Undercover op het dark web

UNDERCOVER OP HET DARK WEB

Wapens, huurmoordenaars, seksuele afpersing, complotdenkers en drugs op het 'verborgen internet'

BORGERHOFF & LAMBERIGTS

Joppe Nuyts

INHOUD

Vooraf 9

Inleiding 11

Welkom op het dark web 15

Aangenaam, Suskewiet 22

De kwaadaardige tweeling 28

Duistere AI 39

Shadowgame 51

De zwarte markt 57

Tor als redding 72

De schaduwbibliotheek 83

Opgelicht 93

De wapenprinter 107

Ransomware 118

Moreel kompas 133

Strijd tegen demonen 139

Handleiding voor misbruik 158

Dark web-mythes 168

De dodenlijst 175

Offline 183

Dankwoord 189

VOORAF

In dit boek lees je over criminele netwerken en de platformen waarop illegale activiteiten plaatsvinden. Om te voorkomen dat mensen deze fora opzoeken of contact leggen met de betrokkenen, zijn de namen van fora, daders, tussenpersonen en chatgebruikers vervangen door schuilnamen. Deze zijn in de tekst telkens herkenbaar aan een asterisk (*). Omdat sommige online pseudoniemen een verhaal op zich vertellen, leunen de schuilnamen inhoudelijk zo dicht mogelijk aan bij het origineel. Uit privacyoverwegingen is ook de identiteit van kwetsbare getuigen en slachtoffers onherkenbaar gemaakt, tenzij zij er expliciet voor gekozen hebben om onder hun eigen naam te getuigen.

INLEIDING

'What's up peeps!'

Een donderdagavond in maart, net voor middernacht. Ik drop deze begroeting in een anoniem chatkanaal op het dark web. Het voelt onwennig, misschien beklemmend, verscholen achter mijn laptop in de lege lobby van een Antwerps hotel. Zou de vrouw achter de receptie dat ook vinden? Ik werp een blik in haar richting, maar ze kijkt niet op. Ze is zelf diep verzonken in haar smartphone.

'Hey man.' Er verschijnt een reactie op mijn scherm. '*Sup fuckface*', typt een andere, duidelijk minder genuanceerde gebruiker. Ik moet erom glimlachen. Zijn grofgebekte begroeting typeert de dynamiek in dit soort chatgroepen. Ik wil iets terugtypen, maar zie dat ik een gesprek tussen twee Amerikanen dreig te onderbreken. Een van hen pocht over zijn studentenleven aan de University of Michigan, waar hij chemie studeert.

'Dus je zou eigenlijk je eigen drugs kunnen maken?' vraagt de andere chatter. 'Zou kunnen? Hehe, je hebt geen idee *bro*.' Als een vlieg op de muur volg ik hun conversatie. Dit is de laatste maanden mijn Netflix geworden. Mijn vaste avondritueel.

Een nieuwe gebruiker meldt zich aan. Hij begroet niemand. Zonder één woord van introductie dropt hij een willekeurige link in de groep. Ik twijfel een seconde, maar de nieuwsgierigheid wint het. Ik klik. De browser laadt tergend traag, zoals alles op dit netwerk. Dan springt er plots een groot, pikzwart scherm open. In strakke, witte letters staat rechts bovenaan één woord: *Shadowgame**.

Het eerste wat ik zie, zijn namen. Honderden, duizenden namen van vrouwen, netjes gerangschikt onder tabbladen waar ik schijnbaar

eindeloos doorheen kan scrollen. Sommigen staan er enkel met hun voornaam, anderen zijn volledig geïdentificeerd. Ik klik op een willekeurig profiel. De overzichtspagina transformeert in een digitaal portfolio van een jonge vrouw. Naast haar voor- en achternaam zie ik tientallen tegeltjes met naaktbeelden. Volgens de teller meer dan duizend stuks. De foto's zijn gebrekkig afgeschermd met een knullig icoontje van een hangslot en een wazige filter eroverheen, maar je ziet in één oogopslag dat het om uiterst intieme, kwetsbare momenten gaat.

Voor zover ik kan zien, staat hier een mix van echte foto's en zogenaamde *deepnudes* – naaktbeelden die door artificiële intelligentie gemaakt zijn. Maar het stopt niet bij de foto's. Bij sommige vrouwen staat een verzameling aan persoonlijke data. Rechtstreekse links naar hun Instagram- of Facebook-accounts, inclusief hun exacte woonplaats, contactgegevens en geboortedatum. Ik besef plots waar ik naar kijk: dit is geen simpel forum. Dit is een kant-en-klare database met al het nodige materiaal om deze vrouwen te stalken, te chanteren en hun leven systematisch te verwoesten. Dit is een lijst van slachtoffers.

De schaal van deze database is angstaanjagend. Via een keuzemenu kun je doelgericht filteren op nationaliteit. Het overgrote deel van de slachtoffers komt uit de Verenigde Staten: 4.061 profielen. Maar ook de Lage Landen ontsnappen niet. Uit Nederland staan er 190 slachtoffers online. Uit België 28. Stuk voor stuk meisjes en jonge vrouwen van wie de waardigheid hier te grabbel wordt gegooid.

De commerciële machinerie achter het platform Shadowgame is pervers. Voor 249 dollar, af te rekenen in bitcoin, trek je in één klap de volledige, wereldwijde database binnen. Heb je geen geld? Geen probleem. De site stimuleert gebruikers om zelf naaktbeelden te uploaden onder de noemer *'Leak & Earn'*. Als je zelf unieke naaktfoto's van een nieuw meisje aanlevert, kun je ook gratis toegang krijgen tot de rest van de site.

Het dieptepunt is een speciale knop gericht op de slachtoffers zelf. Zij krijgen de mogelijkheid om hun eigen foto's offline te laten halen. Tegen betaling, uiteraard. De bende achter de site passeert zo twee keer langs de kassa: ze incasseren geld van hitsige voyeurs, en ze persen de wanhopige vrouwen af die hun leven proberen terug te kopen.

Hoe gruwelijk ook, dit platform leeft duidelijk. Als ik op andere darkwebfora zoek naar de naam van deze database, zie ik dat er actief naar gevraagd wordt. 'Heeft iemand de link van Shadowgame? Zijn die foto's wel echt?', vraagt iemand op een populair berichtenbord. 'Jazeker', antwoordt een andere gebruiker, die blijkbaar al betaald heeft. 'Regelmatig nieuwe foto's. Check ook de video's op de andere pagina. Ik ben een tevreden klant.' *Een tevreden klant.* Alsof hij net een stofzuiger heeft gerecenseerd.

Ik sla mijn laptop dicht. Inmiddels is het al even voorbij middernacht. De stilte van de hotellobby overvalt me. Aan de overkant van de ruimte zit de receptioniste nog steeds argeloos op haar scherm te scrollen. Wat vanavond begon als onschuldig meelezen in een chatkanaal, is geëindigd in een donkere uithoek van het internet. Ik wrijf over mijn gezicht. Waar ben ik in hemelsnaam terechtgekomen?

WELKOM OP HET DARK WEB

Al zes jaar lang misleid ik mensen doelbewust. Als onderzoeksjournalist, welteverstaan. Undercover. Ik lieg over wie ik ben, omdat het soms de enige manier is om de waarheid aan het licht te brengen.

Ik infiltreer op plekken waar journalisten normaal gezien niet welkom zijn. Of waar ze nooit hetzelfde verhaal krijgen wanneer ze aankomen met een camera op de schouder en een microfoon in de hand. Zo liet ik me via Snapchat ronselen als mensensmokkelaar om voor duizenden euro's migranten op te halen in Oost-Europa. Ik mengde me onder de illegale straatraces op afgelegen industrieterreinen. En ik werkte wekenlang als pakjesbezorger voor PostNL, waar ik met een verborgen camera in mijn kleding grootschalige fraude en kinderarbeid vastlegde.

Dat zo'n infiltratie gepaard gaat met een shot adrenaline, zal ik niet ontkennen. Al is die kick nooit het doel. Aan undercoverjournalistiek – of 'aliasjournalistiek' – doe je uit noodzaak. Veel maatschappelijke verhalen spelen zich af achter gesloten deuren, waar niemand uit zichzelf uit de biecht klapt. Dat is hun goed recht, maar het blijft mijn taak om die feiten toch boven tafel te krijgen. Zolang ik me maar strikt aan de spelregels houd, zoals vastgelegd in de Code van de Raad voor de Journalistiek.

ARTIKEL 17 VAN DE JOURNALISTIEKE CODE

Aliasjournalistiek – waarbij de journalist bewust een andere hoedanigheid aanneemt – is slechts verantwoord indien de informatie niet op een andere manier kan verkregen worden en wanneer er voldoende maatschappelijk belang is. Er moet steeds zorgvuldig worden afgewogen of er geen overdreven risico's worden genomen voor de veiligheid van de journalist en de omstanders.

Precies dat maatschappelijk belang vormt ook de drijfveer voor dit boek. Een zoektocht naar het ware gelaat van het verborgen internet: het dark web. De sensationele verhalen zijn bekend: een digitale vrijplaats vol harddrugs, wapenhandel en andere lugubere praktijken. Een schuilkelder waar criminelen zogezegd onschendbaar zijn. Maar klopt dat beeld wel? Wat speelt zich daar echt af? En wanen misdadigers zich hier terecht onkwetsbaar?

Tegelijk wil ik begrijpen wie uit onze eigen achtertuin stiekem inlogt op het dark web – en met welke agenda. We bestempelen de figuren op zulke criminele fora graag – en vaak volkomen terecht – als onverbeterlijk slecht. Maar wie het daarbij laat en weigert te graven naar hun motieven, werkwijzen en systemen, gooit de deur dicht naar belangrijke inzichten. In dit boek spreek ik met misdadigers. Niet om hun daden goed te praten en hen een podium te bieden, maar om in hun hoofd te kijken. Hoe gaan oplichters, drugsdealers of wapenhandelaars op het dark web te werk? Pas als je die criminele mechanismen blootlegt, kun je als samenleving een dam opwerpen en nieuwe slachtoffers voorkomen.

Voor ik die vragen kan beantwoorden, moeten we terug naar de basis: wat is het dark web precies? De naam alleen al trekt een scherpe grens met het 'normale' internet. We zijn gaan geloven dat er op dat verborgen internet uitsluitend monsters ronddwalen. Dat beeld danken we niet alleen aan sommige krantenkoppen of Hollywoodfilms; ook op sociale media scoren theatrale video's erover miljoenen views. Amusant? Soms. Realistisch? Meestal niet.

Om uit te leggen wat het dark web dan wel is, wordt vaak dezelfde klassieke metafoor gebruikt: een ijsberg. Een gigantische klomp ijs waarvan het overgrote deel zich onzichtbaar onder de zeespiegel bevindt.

Het topje van de ijsberg, boven de zeespiegel, is het *clear web*. Dat is je vertrouwde digitale omgeving: de zoekresultaten op Google, de nieuwspagina's of de website van de lokale voetbalclub. Alles wat openbaar toegankelijk is en door zoekmachines wordt opgevist, zonder dat je ergens hoeft in te loggen.

Daaronder ligt de massieve onderlaag van het internet: het *deep web*. Dit is de afgeschermde onderwatermassa die volgens experts het overgrote deel van het wereldwijde netwerk beslaat. Het omvat alle pagina's die achter een inlogscherm schuilgaan. Denk aan je online bankomgeving, je medisch dossier, de interne databank van je werkgever of een besloten WhatsApp-groep.

En helemaal onderaan vind je het verborgen internet: het *dark web*. Een afgesloten netwerk dat volledig losstaat van de rest. Het staat bekend om zijn anonimiteit. Precies daardoor is het net zo goed een toevluchtsoord voor activisten en vrijheidsstrijders als voor criminelen.

In tegenstelling tot wat de naam doet vermoeden, is het 'verborgen internet' eigenlijk niet zo moeilijk te vinden. Je hebt er geen ingewikkelde apparatuur of persoonlijke uitnodiging voor nodig, alleen een speciaal programma: de Tor-browser. Iedereen kan die software in een paar muisklikken gratis downloaden via *The Tor Project*, de organisatie die het netwerk onderhoudt.

Tor is de afkorting van *The Onion Router*. Vandaar dat IT-experts het netwerk vergelijken met de schillen van een ui. Dat werkt zo: als je naar een website surft, verpakt de Tor-browser je internetverkeer vooraf in meerdere versleutelde lagen. Vervolgens reizen je data via een omweg langs verschillende computers – zogenaamde Tor-*nodes* – die door vrijwilligers wereldwijd worden beheerd. Elke computer pelt één laagje af om het adres van de volgende computer te lezen, waardoor niemand in de keten het volledige traject kent. Zelf vind ik die technische ui-metafoor wat abstract. Ik bekijk het liever als een postpakket.

In de normale wereld is logistiek overzichtelijk: je laat een pakket ophalen dat je wilt verzenden. Een chauffeur rijdt vanaf jouw voordeur rechtstreeks naar het adres van de ontvanger. Op het etiket staat precies waar de doos naartoe moet, en de chauffeur weet exact wie jij bent en bij wie hij aflevert. Op het dark web gooien we die logica volledig overboord. Een digitaal pakketje wordt daar niet door één chauffeur bezorgd, maar via een estafette van drie 'blinde koeriers' die elkaar niet kennen:

- De eerste koerier haalt het pakketje bij jouw voordeur op. Hij weet wie jij bent, maar op zijn etiket staat uitsluitend het adres van een anoniem tussenstation ergens ter wereld. Wat de inhoud of de uiteindelijke eindbestemming is? Hij heeft geen flauw idee.
- De tweede koerier neemt de doos halverwege over. Hij ziet alleen van wie hij hem kreeg en naar welk volgend tussenstation hij moet rijden. Jij bent voor hem al lang uit beeld verdwenen; hij is niets meer dan een blind doorgeefluik.
- De derde koerier levert de doos af bij de website die je wilt bezoeken. Hij ziet wie het pakketje in ontvangst neemt, maar kan onmogelijk achterhalen wie de oorspronkelijke afzender was.

Omdat duizenden van deze 'blinde koeriers' voortdurend miljoenen pakketjes over de hele wereld aan elkaar doorgeven, raakt het spoor naar jouw eigen woonkamer al bij de allereerste stap bijster. Jij bent onzichtbaar geworden, maar je pakketje komt wel aan.

Dat je internetverkeer anoniem verloopt, betekent niet dat je automatisch in een crimineel netwerk bent beland. Het gebruik van de Tor-browser is volkomen legaal. Sterker nog: de technologie werd oorspronkelijk ontwikkeld door de Amerikaanse marine om hun spionnen in vijandig gebied onzichtbaar te laten communiceren. Om die militaire anonimiteit echt te laten werken, moesten ze het netwerk wel openstellen voor het grote publiek. Want als uitsluitend Amerikaanse spionnen die specifieke browser gebruiken, valt elke gebruiker alsnog

meteen op. Het was dus nooit bedoeld als crimineel netwerk, maar als een digitaal massacommunicatiekanaal.

In de praktijk kun je met Tor exact hetzelfde doen als met alledaagse browsers: het nieuws lezen, recepten opzoeken of de actuele treinuren bekijken. Het grote verschil? Reguliere browsers zoals Chrome of Safari laten toe dat je gegevens worden verzameld en dat je IP-adres je exacte locatie verraadt. Tor weigert dat pertinent door je internetverkeer volledig te anonimiseren. Om die privacy extra te waarborgen, werkt Tor standaard met de privacyvriendelijke zoekmachine DuckDuckGo, die je surfgedrag niet bijhoudt en geen gepersonaliseerde advertenties voorschotelt.

Niet elke website is blij met die anonimiteit. Veel reguliere pagina's blokkeren Tor-gebruikers uit voorzorg, omdat ze hun surfgedrag niet kunnen monitoren. Het maakt de browser voor alledaags gebruik minder populair: je stuit voortdurend op geblokkeerde sites of irritante captcha-puzzels – typische opgaves als 'duid alle foto's met zebrapaden aan'. Ook autoritaire regimes doen er alles aan om het netwerk te weren. Landen als Iran en China eisen immers totale controle over het surfgedrag van hun burgers – en precies daar steekt Tor een stokje voor.

Hoe beland je dan wél in die online schaduwwereld? Via de Tor-browser kun je niet alleen gewone websites bezoeken, maar ook surfen naar zogenaamde *onion-links*. Dit zijn de echte adressen van het dark web. Verwacht geen overzichtelijke domeinnamen zoals *google.com*, maar ellenlange, cryptische ketens van letters en cijfers die eindigen op onion. Omdat er in die webadressen geen herkenbaar woord staat, kun je er niet zomaar naar gissen. Je moet die links dus letterlijk verzamelen. Sommige van die onion-links vind je eenvoudig via het clear web. Om een paar voorbeelden te noemen:

DuckDuckGo
Duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion

De anonieme zoekmachine waarmee Tor standaard opstart.

De Amerikaanse inlichtingendienst CIA
Ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion

Een anonieme digitale brievenbus van de Amerikaanse inlichtingendiensten, waar klokkenluiders wereldwijd gevoelig materiaal kunnen dumpen zonder hun leven te riskeren.

The New York Times
ej3kv4ebuugcmuwxctx5ic7zxh73rnxt42soi3tdneu2c2em55thufqd.onion

Een afgeschermde omgeving voor journalisten om hun anonieme bronnen te beschermen en tips te ontvangen. Ook VTM Nieuws en HLN hadden in 2015 zo'n initiatief onder de naam 'Nieuwsleaks', maar dat bestaat niet meer.

Dat activisten, veiligheidsdiensten en journalisten deze technologie kunnen gebruiken om anoniem te opereren, betekent echter ook dat dezelfde technologie beschikbaar is voor mensen met slechte intenties. Precies daar begint de echte schaduwwereld van het dark web. Criminelen maken dankbaar gebruik van diezelfde anonimiteit.

Een jaar lang infiltreren op het dark web voelde als wandelen door een mijnenveld met je ogen dicht. Er zijn momenten geweest waarop ik met één verkeerde klik zaken te zien kreeg die op mijn netvlies gebrand blijven. Tegelijk waren het mijnen die bijzonder laat tot ontploffing kwamen. Omdat je data een wereldreis maken, duurt het laden van

een pagina soms bijzonder lang, om je vervolgens te laten landen op een site met het klungelige design uit de jaren negentig. Toch trekt Tor een gigantische massa aan: ruim zeven miljoen mensen maken er dagelijks gebruik van. Onder hen bevinden zich duizenden criminelen die zich verschuilen achter afgeschermde onion-links, in de overtuiging dat geen enkele opsporingsdienst hen ooit kan raken.

Dat een bezoek aan het Tor-netwerk op zich legaal is, betekent echter niet dat ik vrij spel had. Als onderzoeksjournalist ben ik gebonden aan strikte wettelijke en ethische spelregels. Een perskaart is immers geen vrijgeleide: ik mag onder geen beding zelf strafbare feiten plegen of illegale goederen aanschaffen. Daarnaast is uitlokking streng verboden. Als een crimineel uitsluitend door mijn toedoen een strafbaar feit pleegt, ga ik mijn boekje te buiten. En ten slotte moet ik bij elk undercovercontact de afweging maken of de misleiding ethisch verantwoord is, en of iemand me niet exact hetzelfde zou vertellen als hij wel wist dat er een journalist aan de andere kant van het scherm zat.

Die regels onderschrijf ik volledig; ze vormen het fundament van integere onderzoeksjournalistiek. Binnen dit kader wilde ik het echte gelaat van het dark web blootleggen: de hardnekkige fabeltjes ontkrachten, het Hollywoodbeeld nuanceren en de theatrale influencers ontmaskeren. Mijn doel was om de fictie van de feiten te scheiden, maar ook om te onderzoeken welke impact dark web-verhalen hebben op de bovenwereld. Dat vele ervan verzonnen blijken te zijn, betekent immers niet dat ze geen schade aanrichten.

AANGENAAM, SUSKEWIET

Zaterdag 4 oktober 2025. Buiten raast storm Amy door de Antwerpse straten, met felle windstoten en striemende regen. Achter in een koffiebar zit ik weggedoken aan een tafeltje. Ik staar naar het scherm van de tweedehandse laptop die ik twee weken geleden kocht. Wat ik zie, wil ik onder geen beding met de rest van de klanten delen: drugs. Cannabis, xtc en MDMA – netjes gecategoriseerd en te koop aangeboden alsof het alledaagse koopjes op Amazon zijn. Sporadisch kijk ik even rond om er zeker van te zijn dat niemand meekijkt.

Waarom neem ik het risico om in een volle koffiebar te zitten met zulke criminele beelden op mijn scherm? En dat nota bene met een laptop die bij momenten klinkt als een haardroger? Wie niet wil opvallen, kiest namelijk een andere strategie. Mijn bizarre werkplek is de schuld van Gemini, de AI-assistent en chatbot van Google. Het principe is vergelijkbaar met ChatGPT: je stelt een vraag en de software beantwoordt ze op basis van miljarden online gegevens. De eerste weken van mijn nog prille onderzoek was Gemini mijn digitale mentor.

Mijn vraag aan Gemini was simpel: 'Hoe surf ik veilig en volstrekt onvindbaar op het dark web?' Ik vroeg het programma om mijn vraag bloedserieus te behandelen, alsof ik met een doorgewinterde privacy-expert sprak. Het is altijd een risico om AI blind te vertrouwen – taalmodellen kunnen immers hallucineren en feiten verdraaien – maar ze bundelen wel razendsnel informatie. En belangrijker: ik wilde mijn plannen nog niet aan de grote klok hangen bij menselijke experts.

Het antwoord van Gemini móést wel waterdicht zijn. Het dark web staat immers bekend als een broedplaats voor cybercriminaliteit. De hackers en oplichters die er rondzwerven spelen Champions League. Ik daarentegen? Zelfvertrouwen genoeg, maar ik ben geen whizzkid, geen techneut en geen IT-expert. Ik ben zeker geen leek, maar ik speel

in een heel andere divisie. Als een van die criminelen niet gediend is met mijn vragen en jacht maakt op mijn identiteit, maak ik zonder ijzersterke voorbereiding geen schijn van kans.

Ik verwachtte dat dit onderzoek redelijk comfortabel zou verlopen. Gewoon vanuit mijn eigen zetel of aan mijn vertrouwde bureau, 's avonds na de uren. Gemini maakte snel korte metten met dat luie plan. Mijn eigen laptop en wifi-netwerk gebruiken kan ik wel vergeten. Dat is namelijk ontzettend dom en ronduit gevaarlijk. Met één verkeerde klik lekt mijn IP-adres – de unieke stempel die mijn woonadres verklapt – of raakt mijn computer geïnfecteerd met kwaadaardige software. Dat zou mijn ander journalistiek werk in gevaar brengen. Volstrekt uit den boze, oordeelde Gemini. In plaats daarvan krijg ik een boodschappenlijstje voorgeschoteld: een goedkope, tweedehandse laptop, een blanco USB-stick, een besturingssysteem waar ik nog nooit van heb gehoord, een anoniem e-mailadres en een handvol locaties met een openbaar wifi-netwerk waar ik me voortaan na de uren zou moeten installeren.

De zoektocht naar de spullen op dat lijstje begint in een volkse wijk in Puurs, vlak bij de afrit van de A12. Daar heb ik afgesproken met Damien*, een Franstalige man die ik de avond ervoor via Facebook Marktplaats had gecontacteerd. Ik zou Damien omschrijven als een 'laptopboer'. Hij koopt oude, afgeschreven bedrijfstoestellen in bulk, lapt ze op en verkoopt ze contant door. Voor 120 euro cash werd ik eigenaar van een Dell Latitude E5570 uit 2016 – een digitaal fossiel uit een tijd dat AI-programma's als Gemini nog niet in de steigers stonden.

'Zo goed als nieuw', glundert Damien, terwijl hij de laptop bovenhaalt. Je merkt aan alles dat hij verstand van zaken heeft. Trots laat hij me zien hoe hij het systeem grondig heeft opgeschoond. 'Een oud beestje, maar de nieuwste Windows staat erop. Je kunt er zo mee aan de slag.' Terwijl hij de lader bij de laptop in een plastic zakje propt, bekijkt hij me nieuwsgierig. 'Gebruik je hem voor je werk?' 'Soort van', antwoord