

Palantir: Judgment Day Protocol

Een kritische analyse van surveillance, macht en de toekomst van menselijke zelfbeschikking

Editie: 2026 — Eerste Druk

Taal: Nederlands

ISBN: 9789083688817

Auteur: Roy Mikes

Omvang: Inleiding, 18 hoofdstukken, Conclusie en Tweesprong

Pagina's: 205

Thema's: Surveillance, Pre-Crime, IoT, Cognitieve oorlog, AI-singulariteit

© 2026 Roy Mikes. Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopiën, opnamen of op enige andere manier, zonder voorafgaande schriftelijke toestemming van de auteur, met uitzondering van korte citaten in recensies of artikelen.

INHOUDSOPGAVE

Inleiding	De Steen die Alles Ziet	3
H 1	De Geboorte van een Idee — PayPal, 9/11 en de Oorsprong (2004)	9
H 2	In-Q-Tel: De CIA als Durfkapitalist	19
H 3	Gotham — Het Platform dat Terroristen Opspoort	28
H 4	Afghanistan, Irak en de Slagvelden van Data	37
H 5	Schokgolven van de Geschiedenis — 80-jaar cyclus en het Digitale Tijdperk	43
H 6	De Digitale Infrastructuur — IoT, Cloud en de Data-Oceaan	52
H 7	Pre-Crime: Van Minority Report naar Werkelijkheid	64
H 8	Sensor Fusion — Wanneer Alles Kijkt	73
H 9	ICE, Surveillance en de Erosie van de Rechtsstaat	82
H 10	Van Overheid naar Wall Street — Foundry en de Commerciële Sprong	90
H 11	De Beursgang van 2020 en de Waarderingsparadox	96
H 12	Oekraïne, Iran en de AI-Oorlog	102
H 13	Warp Speed — De Digitale Gevangenis & Skynet	108
H 14	AIP — De Kunstmatige Intelligentie Revolutie	129
H 15	Cognitieve Oorlogsvoering — Jouw Brein als Slagveld	137
H 16	Neuralink, Transhumanisme en de Mens als Machine	144
H 17	De Matrix, Zelfbeschikking en de Toekomst van de Mens	159
H 18	Het Uur van de Waarheid — Palantir in april 2026	169
Conclusie	Het Oog sluit nooit — Maar Wij Kunnen Waken	179
Tweesprong	De Tweesprong van de Beschaving — Doemscenario en Hoopvol Scenario	195

INLEIDING

De Steen die Alles Ziet

Er bestaat een bedrijf dat weet waar terroristen zich schuilhouden, dat migranten opspoort voordat ze de grens oversteken, dat generaals in real-time van doelwitinformatie voorziet, dat weet welke buurten morgen crimineel zullen zijn — nog vóórdát iemand ook maar iets heeft gedaan. Het werkt vrijwel onzichtbaar. Het heet Palantir.

De naam is ontleend aan de palantíri — de 'ziende stenen' uit J.R.R. Tolkiens *Lord of the Rings*. In Tolkiens fictieve wereld zijn het kristallen bollen waarmee koningen en tovenaars over grote afstanden kunnen kijken, verbindingen kunnen maken en de wereld kunnen aanschouwen. Dat Peter Thiel, medeoprichter van Palantir Technologies, bewust voor deze naam koos, zegt alles over de ambitie die hij in 2004 in zijn bedrijf legde.

Maar Tolkiens verhaal bevat een waarschuwing. De palantíri konden worden misbruikt. Sauron — de Duistere Heer — gebruikte ze om zijn vijanden te bespioneren, hun wil te breken, hen te misleiden. Slechts de sterksten en wijsten konden erin kijken zonder te worden gecorrumpeerd. Het is een metafoor die precies de spanning benoemt die in het hart van dit bedrijf leeft.

Dit boek gaat verder dan het verhaal van één bedrijf. Het is een poging om de architectuur van een nieuwe wereld bloot te leggen: een wereld waarin miljarden verbonden apparaten constant data genereren, waarin kunstmatige intelligentie die data verwerkt tot patronen die de menselijke geest niet meer kan volgen, en waarin een kleine groep mensen — met toegang tot die technologie — een macht heeft vergaard die in de menselijke geschiedenis geen precedent kent.

"Wij zijn de AI-wapenhandelaar van de 21ste eeuw."

— Jacob Helberg, nationaal-veiligheidsadviseur, over Palantir, *Time Magazine* 2024

Van de eerste CIA-investering in 2004 tot de 430-miljard-dollar-onderneming van 2025 is Palantir de meest zichtbare incarnatie van een fundamentele verschuiving: de fusie van commerciële technologie, staatsmacht en militaire capaciteit in één enkel

platform. Dit boek volgt die reis — kritisch, gefundeerd, en zonder de illusie dat de waarheid eenvoudig is.

Wat dit boek behandelt

In achttien hoofdstukken worden de meest cruciale dimensies van de Palantir-wereld geanalyseerd. Van de historische context van technologische schokgolven tot de filosofische vraag over menselijke zelfbeschikking. Van de praktische werking van sensor fusion tot de dystopische mogelijkheden van pre-crime. Van de IoT-revolutie die alles verbindt tot de cognitieve oorlogsvoering die jouw eigen denken als slagveld ziet — en van Neuralink tot de uiteindelijke vraag: wie is de mens nog in een wereld waar alles data is?

Sommige hoofdstukken zijn ongemakkelijk. De verbanden die hier worden gelegd zijn niet altijd comfortabel, en ze zijn ook niet altijd zeker. Maar ze verdienen een serieuze, open discussie — omdat de beslissingen die nu worden genomen over AI, surveillance en staatsmacht, beslissingen zijn die onze kinderen en kleinkinderen zullen moeten leven met hun gevolgen.

De wereld voor en na Palantir

Om Palantir te begrijpen, moet men begrijpen in welke wereld het werd geboren. De jaren na 9/11 waren jaren van angst, van verwarring, van een machtige natie die zich plotseling kwetsbaar voelde. Amerika had de grootste militaire macht ter wereld, maar was toch niet bij machte geweest een aanslag van negentien mannen met vliegtuigtickets te voorkomen.

Die kwetsbaarheid leidde tot een fundamentele herschikking van prioriteiten. Surveillance werd veiligheid. Privacy werd luxe. Transparantie — maar dan voor de burger tegenover de staat, niet andersom — werd norm. De Patriot Act, goedgekeurd slechts 45 dagen na de aanslagen, breidde de bevoegdheden van de inlichtingendiensten dramatisch uit. NSA-programma's als PRISM en XKeyscore, later onthuld door Edward Snowden, begonnen te draaien.

Het is in deze context dat Palantir werd geboren. Niet als een bedreiging voor de vrijheid — zo zagen de oprichters het zeker niet — maar als een oplossing voor een urgent probleem: hoe verbind je de verspreide datapunten die terrorisme kunnen voorspellen en voorkomen? Het morele kader was helder: meer verbinding betekende meer veiligheid, betere analyse betekende minder dode soldaten, slimmere targeting betekende minder burgerslachtoffers.

Of dat kader klopte, is een vraag die dit boek probeert te beantwoorden. Maar laten we beginnen met te erkennen dat er mensen van goede wil waren — en zijn — die oprecht geloofden en geloven dat Palantirs technologie de wereld beter maakt. Die erkenning is essentieel: het makkelijkste wat men kan doen, is dit verhaal reduceren tot een verhaal van kwade opzet. Maar de werkelijkheid is ingewikkelder en daardoor gevaarlijker.

Het tijdperk van de data-economie

We leven in een tijdperk dat historici later waarschijnlijk de Data-Revolutie zullen noemen — een periode die qua transformatieve kracht vergelijkbaar is met de Industriële Revolutie van de 18e en 19e eeuw. Net zoals stoommachines de verhouding tussen menselijke arbeid en productie fundamenteel veranderden, veranderen datanetwerken de verhouding tussen informatie en macht.

De cijfers zijn duizelingwekkend. In 2025 werd elke dag meer dan 120 zettabytes aan data gegenereerd. Ter vergelijking: één zettabyte is een miljoen petabyte, een petabyte is een miljoen gigabyte. Alle woorden die ooit zijn gesproken door alle mensen die ooit hebben geleefd, beslaan naar schatting ongeveer 5 exabyte aan opslag — dat is 0,005 zettabyte. Wij genereren dit volume dus in een paar uur.

Deze data heeft een eigenschap die data vóór het digitale tijdperk niet had: ze is permanent, doorzoekbaar, koppelbaar en schaalbaar. Een gesprek dat men in 1850 voerde was weg zodra het was uitgesproken, tenzij iemand het opschreef. Een bericht dat men in 2026 verstuurt via WhatsApp, iMessage of Signal — zelfs versleuteld — laat metadata na: wanneer, van wie naar wie, hoe lang, via welk apparaat, vanaf welke locatie. Die metadata is waardevoller dan men denkt.

Het is precies dit soort metadata waarop Palantirs systemen zijn gebouwd. Niet de inhoud van een gesprek — althans niet in de eerste instantie — maar de patronen. Wie praat met wie? Hoe vaak? Wanneer verandert het patroon? Wie zit in het netwerk van wie? Het zijn dezelfde vragen die Peter Thiel — de PayPal-medeoprichter en Palantir-investeerder die als eerste geloofde dat data-analyse misdaad kon voorspellen — al in 2001 stelde om PayPal-fraude te detecteren. Diezelfde logica past Palantir nu toe op terrorisme, misdaad, ziekte-uitbraken, supply chains, financiële markten en uiteindelijk op iedereen.

Palantir als metafoor voor macht en controle

Dit is geen toevallige parallel. In een wereld waar data de grondstofdefinitie van macht herdefiniëert, is de vraag wie de data ziet — en wie bepaalt wat de data betekent — een politieke vraag van de hoogste orde. Palantir biedt zijn klanten de mogelijkheid om te zien. Maar het bedrijf bepaalt ook, via zijn algoritmen, zijn interfaces en zijn trainingdata, wat er te zien is en hoe het wordt geïnterpreteerd.

"Macht is niet wie de sterkste troepen heeft. Macht is wie het verhaal vertelt."

— Yuval Noah Harari, *Sapiens*, 2011

Dit boek is ook een poging om het verhaal te vertellen. Niet het verhaal dat Palantir zelf vertelt — van redding, van bescherming, van democratische waarden — en niet het verhaal van simpele demonisering. Maar het verhaal van een technologie die fundamenteel is voor hoe macht in de 21e eeuw wordt georganiseerd, en die fundamentele vragen stelt over wat wij als samenleving willen zijn.

Het digitale panopticon: een nieuwe vorm van macht

De filosoof Jeremy Bentham ontwierp in 1785 het Panopticon: een gevangenis waarbij een centrale bewaker alle gevangenen kon observeren zonder dat zij konden zien of ze werden geobserveerd. De bewaker hoeft niet altijd te kijken — de mogelijkheid van observatie is genoeg om gedrag te disciplineren. Michel Foucault gebruikte dit concept in zijn meesterwerk *Surveiller et punir* (1975) om te beschrijven hoe moderne samenlevingen macht uitoefenen via zichtbaarheid en zelfcensuur.

Het digitale tijdperk heeft het Panopticon van Bentham gerealiseerd op een schaal die noch Bentham noch Foucault kon voorzien. De bewakingstoren is niet meer één centrale locatie maar een gedistribueerd netwerk van sensoren, databases en algoritmen. De gevangenen — burgers — zijn niet opgesloten achter muren maar bewegen vrij, terwijl hun bewegingen, communicaties en gedragingen continu worden geregistreerd.

Het meest radicale aspect van het digitale panopticon is dat de gevangenen het zelf hebben gebouwd. Mensen dragen hun smartphone vrijwillig. Ze installeren smart-speakers in hun slaapkamers. Ze plaatsen camera's bij hun voordeur. Ze posten hun locatie, hun gedachten, hun foto's op sociale media. Het digitale panopticon is geen door de staat opgelegde infrastructuur — het is een vrijwillig gecreëerd systeem dat staatsactoren en commerciële actoren vervolgens kunnen exploiteren.

Palantir is de organiserende laag van dit panopticon. Het is het systeem dat de data van de vrijwillige sensoren integreert, analyseert en bruikbaar maakt voor machtsuitoefening. Het heeft de bewakingstoren gebouwd voor een samenleving die al lang zijn eigen cellen had ingericht.

Wat dit boek niet is

Dit boek is geen complottheorie. Het beschrijft geen geheime organisatie die in het verborgene werkt aan een plan voor wereldheerschappij. Alle feiten die hier worden gepresenteerd — de CIA-investering in Palantir, de contracten met ICE, de betrokkenheid bij Oekraïne, de Bilderberg-deelname van Thiel — zijn publiekelijk gedocumenteerd in mainstream journalistiek, bedrijfsregistraties en officiële overheidsdocumenten.

Dit boek is ook geen anti-technologie-manifest. Technologie is een menselijk instrument. De vraag is niet of we technologie moeten gebruiken, maar hoe, onder welke omstandigheden en met welk toezicht. Een mes is een nuttig keukeninstrument en een potentieel moordwapen: de context en het toezicht bepalen wat het is.

Dit boek is een poging tot doorzichtigheid: het in kaart brengen van een systeem dat bewust ondoorzichtig is gehouden, zodat burgers en beleidsmakers geïnformeerde keuzes kunnen maken over de samenleving die ze willen zijn. Informatie is de voorwaarde voor vrijheid.

Het probleem van het vertrouwen in systemen

Een van de meest urgente vragen van het digitale tijdperk is niet technologisch maar psychologisch: hoe gaan mensen om met systemen die ze fundamenteel niet kunnen begrijpen? De meeste mensen begrijpen niet hoe hun auto werkt, hoe het elektriciteitsnet functioneert of hoe hun bank zijn kredietbeoordeling berekent. Toch vertrouwen ze die systemen dagelijks — en dat vertrouwen is grotendeels gerechtvaardigd, omdat die systemen gereguleerd, gecertificeerd en geauditeerd zijn.

AI-systemen — en in het bijzonder grote taalmodellen en predictieve algoritmen — zijn fundamenteel anders: ze zijn niet deterministisch, hun gedrag is niet volledig voorspelbaar, en ze zijn doorgaans niet onderworpen aan de certificeringseisen die andere kritieke systemen moeten doorstaan. Een vliegtuig mag de lucht niet in zonder Type Certificate. Een medicijn mag niet op de markt zonder klinische trials. Een AI-systeem dat bepaalt over iemands kredietwaardigheid of zijn visa-aanvraag mag dat doen op basis van een intern bedrijfsbesluit.

Dit gat in de regulering is geen toeval: het weerspiegelt de snelheid waarmee AI-systemen zijn gedeployeerd versus de snelheid waarmee regulering kan worden ontwikkeld. De EU's AI Act is een poging dit gat te dichten — maar zelfs die wet zal jaren nodig hebben om volledig geïmplementeerd en gehandhaafd te worden.

In de tussentijd worden systemen als Palantir ingezet in kritieke contexten — rechtspraak, grenscontrole, militaire targeting — zonder de certificering en het externe toezicht die andere kritieke systemen vereisen. Het vertrouwen dat wordt gesteld in die systemen, is grotendeels gebaseerd op de reputatie van het bedrijf, de kwaliteit van zijn sales-pitch en de tevredenheid van zijn klanten — niet op onafhankelijk bewijs van betrouwbaarheid, nauwkeurigheid en rechtvaardigheid.

Van data naar beslissing: de verantwoordelijkheidsvraag

In de klassieke rechtsstaat is verantwoordelijkheid individueel: een persoon neemt een beslissing, en die persoon is aansprakelijk voor de gevolgen. In de data-gestuurde staat is verantwoordelijkheid gedistribueerd: de data is verzameld door X, verwerkt door Y, geanalyseerd door Z, aanbevolen door het algoritme, beoordeeld door een analist, goedgekeurd door een commandant, en uitgevoerd door een operator. Wie is er aansprakelijk?

Dit is niet een louter theoretisch probleem. In 2024 werd voor het Internationaal Strafhof (ICC) een onderzoek gestart naar de betrokkenheid van AI-systemen bij targeting-beslissingen in het Gaza-conflict. De vraag: als bewijsmateriaal voor aanklachten deels is gegenereerd door of gefilterd door AI-systemen — is dat bewijsmateriaal aanvaardbaar? En wie is strafrechtelijk aansprakelijk voor een AI-aanbeveling die heeft geleid tot een aanval op een beschermd object?

Deze vragen zijn niet opgelost. Het internationaal humanitair recht is geschreven in een tijdperk van menselijke commandanten die menselijke beslissingen nemen. De introductie van AI in de beslissingsketen creëert een juridisch vacuüm dat dringend moet worden gevuld — maar dat vergt internationale onderhandeling en consensus die moeilijk te bereiken is in een tijdperk van geopolitieke concurrentie.

HOOFDSTUK 1

De Geboorte van een Idee

PayPal, 9/11 en de geboorte van een surveillance-imperium (2004)

Het verhaal van Palantir begint niet met een visie voor een bedrijf. Het begint met een fraude-epidemie die PayPal bijna ten onder bracht — en een inzicht over data dat de wereld zou veranderen.

PayPal en de kunst van patroonherkenning

In de vroege jaren 2000 worstelde PayPal met een existentieel probleem: georganiseerde online fraude. Fraudeurs uit Oost-Europa, velen van hen actief in netwerken gekoppeld aan de georganiseerde misdaad, hadden systematische methoden ontwikkeld om valse transacties uit te voeren. Het PayPal-team gaf één van de meest consistente patronen intern de codenaam 'Igor' — een samengesteld profiel, geen echte persoon, maar een analytisch ankerpunt voor het anti-fraudealgoritme dat ze bouwden.

Peter Thiel begreep iets fundamenteels: de sleutel tot het stoppen van Igor was niet meer data verzamelen, maar de verbanden zien in bestaande data. Wanneer honderden transacties dezelfde kenmerken deelden — vergelijkbare tijdstippen, bedragen, geografische clusters — kon een algoritme automatisch ingrijpen. Dit klinkt vandaag vanzelfsprekend. In 2001 was het revolutionair.

De les bleef Thiel bij: dezelfde logica — patronen herkennen in chaos — kon op veel grotere schaal worden toegepast. Fraude. Terrorisme. Criminaliteit. Ziekte-uitbraken. Supply chain-verstoringen. Overal waar grote hoeveelheden schijnbaar onsamenvhangende data aanwezig waren, lagen verborgen patronen te wachten.

9/11: de katalysator

Op 11 september 2001 werden vier gekaapte vliegtuigen ingezet als wapens tegen Amerika. Bijna 3.000 mensen stierven. Voor de inlichtingengemeenschap was het een catastrofe — niet omdat er geen informatie was, maar omdat de informatie die er was niet werd verbonden. De CIA en de FBI werkten in silo's. Databases waren gescheiden. Analisten deelden hun inzichten niet.

Achteraf bleek dat sommige van de kapers al in de databases van de inlichtingendiensten stonden. De verbindingen waren er — maar niemand had ze gelegd. De tragische ironie: het was geen tekort aan informatie die 9/11 mogelijk maakte. Het was een tekort aan integratie.

"De vraag na 9/11 was niet: kunnen we meer data verzamelen? We hadden al te veel data. De vraag was: kunnen we de verbanden zien die al in die data verborgen zitten?"

— Peter Thiel, 2013

De oprichting in 2004: vijf mensen, een idee en de CIA

Palantir Technologies werd formeel opgericht in mei 2003, maar begon operationeel te worden in 2004. Thiel benoemde Alex Karp — een filosoof die promoveerde in sociale theorie aan de Goethe Universiteit in Frankfurt, onder invloed van Jürgen Habermas — als CEO. Het was een bijzondere keuze: een denker, geen ingenieur, aan het hoofd van een technologiebedrijf.

De eerste investeerder was In-Q-Tel, de durfkapitaalarm van de CIA. De investering was bescheiden — circa 1,3 miljoen pond — maar bood iets waardevollers: toegang tot de problemen en behoeften van de Amerikaanse inlichtingengemeenschap. Twee jaar lang kwamen CIA-analisten naar Palantirs kantoor in Palo Alto om samen met de engineers het product te bouwen.

TOLKIEN ALS IDENTITEIT

Palantirs kantoren dragen tot op de dag van vandaag namen uit Tolkiens universum. Palo Alto = The Shire. McLean (Virginia, nabij CIA-hoofdkwartier) = Rivendell. Washington D.C. = Minas Tirith. Het is geen toeval: Thiel positioneerde zijn medewerkers bewust als de helden van Midden-Aarde die het goede verdedigden.

Silicon Valley was sceptisch. Sequoia Capital weigerde. Kleiner Perkins weigerde. Thiel financierde de eerste jaren grotendeels zelf — naar schatting 30 miljoen dollar.

Het was een gok op een markt die anderen te moeilijk, te politiek en te onzeker vonden: de combinatie van overheid, inlichtingen en complexe software.

Peter Thiel: de man achter het idee

Peter Andreas Thiel werd op 11 oktober 1967 geboren in Frankfurt am Main, West-Duitsland. Zijn vader, een mijnbouwingenieur, bracht het gezin naar de VS toen Peter jong was. Hij groeide op in diverse plaatsen — Ohio, Michigan, Noord-Californië — als kind van een gereformeerde protestantse familie. Hij studeerde filosofie en rechten aan Stanford, en leerde daar de mensen kennen die zijn leven zouden bepalen: onder wie Elon Musk, Reid Hoffman en David Sacks.

Thiel behoort tot wat men de 'PayPal Mafia' noemt — een groep vroegere PayPal-medewerkers en -oprichters die na de verkoop aan eBay in 2002 elk op eigen kracht monumentale bedrijven opbouwden of investeerden. Musk richtte Tesla en SpaceX op. Hoffman richtte LinkedIn op. Sacks investeerde in tientallen tech-bedrijven. Thiel richtte Palantir op en investeerde als eerste externe investeerder in Facebook.

Wat Thiel onderscheidt van zijn tijdgenoten is zijn ideologische coherentie. Waar de meeste Silicon Valley-ondernemers zich presenteren als politiek neutraal, is Thiel uitgesproken libertarisch-rechts. Hij heeft publiekelijk gesteld: 'Ik geloof niet meer dat vrijheid en democratie compatibel zijn.' Een uitspraak die door critici wordt geciteerd als bewijs van anti-democratische overtuigingen, maar door Thiel zelf wordt verdedigd als een pleidooi voor constitutionele beperkingen op de staatsmacht.

Thiels wereldvisie is diepgeworteld in het werk van Leo Strauss — de conservatieve filosofische traditie die stelt dat samenlevingen worden geregeerd door een kleine, verlichte elite die de bevolking leidt, soms via misleiding, naar het goede. Dit 'Straussiaanse' gedachtegoed loopt als een rode draad door zijn academische achtergrond, zijn politieke netwerk en de manier waarop hij Palantir positioneert: als een patriottische elite die de democratie beschermt tegen haar eigen kwetsbaarheden.

Alex Karp: de onwaarschijnlijke CEO

Als Thiel het strategische brein van Palantir is, is Alex Karp het publieke gezicht. En wat een gezicht. Karp past op geen enkel stereotype van een Silicon Valley-CEO. Hij woont deels in Zwitserland, waar hij skiet en traint. Hij draagt zijn haar in een wilde bos. Hij promoveerde in sociale theorie aan de Goethe Universiteit in Frankfurt. Hij heeft een hond die hij meeneemt naar vergaderingen.

Maar achter het excentrieke imago schuilt een scherp denker die bewust de frontman is van een bedrijf dat zijn imago zorgvuldig beheert. Karp is de man die naar Zelensky reist, die voor Senaatscommissies getuigt, die in Davos spreekt over de plicht van de tech-industrie om de westerse beschaving te verdedigen. Zijn boek 'The Technological Republic' (2025), co-geschreven met journalist Nicholas Zamiska, is een provocatief manifest dat Silicon Valley bekritiseert voor zijn gebrek aan patriottisme.

Karp is ook eerlijk over de controversiële aard van Palantirs werk op een manier die zijn meeste collega's vermijden. 'Wij zijn het meest gecontroleerde technologiebedrijf ter wereld,' heeft hij meerdere keren gezegd — niet als apologie, maar als badge of honor. 'Onze producten werken. Dat is wat ertoe doet.'

De vroege jaren: onzekerheid en doorzettingsvermogen

De beginjaren van Palantir waren allesbehalve triomfantelijk. Het team van vijf mensen werkte in een bescheiden kantoor in Palo Alto. De eerste prototypes waren ruw. De CIA-analisten die met het team werkten, stelden eisen die de engineers nauwelijks konden bijbenen. Sequoia Capital lachte hen de deur uit. De overheidsmarkt was voor Silicon Valley-normen traag, bureaucratisch en onbegrijpelijk.

Thiel financierde de eerste 30 miljoen dollar grotendeels zelf. Hij geloofde in het idee, in het team, en in de markt — ook als niemand anders dat deed. Twee jaar lang was In-Q-Tel de enige externe geldschieter, en zelfs die investering was meer strategisch dan substantieel. De echte test was: kon het team een product bouwen dat CIA-analisten werkelijk wilden gebruiken?

Het antwoord bleek ja — maar het kostte tijd. Twee jaar van intensieve samenwerking met analisten in Langley en Washington produceerden een versie van Gotham die aantoonbaar werkte. Mond-tot-mondreclame verspreidde zich door de inlichtingengemeenschap. Nieuwe agentschappen vroegen om toegang. De markt die niemand wilde bedienen, bleek enorm.

De filosofie van de oprichting: vrijheid en veiligheid verzoenen

Palantir werd opgericht met een bewust paradoxale missie: technologie bouwen die overheden in staat stelt terrorisme te bestrijden zónder de burgerrechten te schenden. Dit was Thiels antwoord op de post-9/11 paradox. In zijn woorden: 'De vraag was niet óf we meer surveillance-technologie zouden bouwen. De vraag was wie die technologie zou bouwen — en met welke waarborgen.'

Palantir bouwde privacybeschermende mechanismen rechtstreeks in de software in: elke zoekopdracht werd gelogd, elke analist-toegang werd geregistreerd, elk gebruik was traceerbaar. Het systeem was zo ontworpen dat misbruik zichtbaar zou zijn voor interne en externe toezichthouders. In theorie was dit elegant. In de praktijk hing alles af van de vraag of die toezichthouders daadwerkelijk toezicht uitoefenden.

Historisch oordeel op die vraag is gemengd. De NSA-programma's die via Palantir-tools werden ondersteund en door Snowden werden onthuld, bevatten weinig bewijs van effectief intern toezicht. De ICE-contracten leverden een systeem op dat werd ingezet voor doeleinden — massadeportaties, familieseparatie — die de oorspronkelijke ontwerpers van het 'privacy-first' kader misschien niet hadden voorzien.

Alex Karp: de filosoof als CEO

De keuze voor Alex Karp als CEO was onorthodox, zelfs voor Silicon Valley-maatstaven. Karp is geen ingenieur. Hij heeft geen MBA. Hij promoveerde in 1998 aan de Goethe Universiteit Frankfurt met een proefschrift over sociale theorie, onder begeleiding van Jürgen Habermas — een van de meest invloedrijke Europese filosofen van de twintigste eeuw, grondlegger van de communicatieve rationaliteitstheorie.

Habermas' werk gaat over de vraag hoe democratische samenlevingen kunnen functioneren in een tijdperk van complexe systemen en gespecialiseerde kennis. Zijn centrale begrip — de communicatieve rationaliteit — stelt dat legitieme beslissingen alleen genomen kunnen worden via vrije, open en gelijke communicatie. Het is een filosofie die in bijna alles haaks staat op wat Palantir doet: systemen bouwen die beslissingen nemen op basis van informatie die de meeste mensen niet kunnen zien, laat staan beoordelen.

Karp zelf erkent deze spanning. In interviews beschrijft hij zichzelf als iemand die 's nachts wakker ligt van de ethische implicaties van het werk dat zijn bedrijf doet. Hij is uitgesproken over zijn aversie tegen ongecontroleerde AI, over de noodzaak van

menselijk toezicht, over het gevaar van techno-utopisme. Tegelijkertijd bouwt zijn bedrijf de infrastructuur voor precies de systemen die hij beschrijft als gevaarlijk.

Dit is geen hypocrisie — of niet alleen hypocrisie. Het is het fundamentele dilemma van iedereen die met transformatieve technologie werkt: als jij het niet bouwt, bouwt iemand anders het. En liever iemand die nadenkt over de ethiek, zo luidt de redenering, dan iemand die dat niet doet.

De vroege jaren: overleven op overheidsgeld

De eerste vier jaar van Palantirs bestaan waren financieel een nachtmerrie. Het bedrijf had geen commercieel product. Het had één klant: de CIA. En die klant betaalde relatief weinig. Thiel pompt jaar na jaar zijn eigen geld in het bedrijf — naar later schattingen meer dan 30 miljoen dollar van zijn eigen vermogen.

Wat het bedrijf overeind hield, was de steun van In-Q-Tel en de overtuiging dat de technologie werkte. CIA-analisten die met Palantir werkten, rapporteerden dramatische verbeteringen in hun analytische capaciteit. Verbanden die voorheen weken kostten om te leggen, konden nu in uren worden gevonden. Het product was ruw, de interface primitief, maar de belofte was echt.

In 2007 begon Palantir zijn eerste grote doorbraak. Het Pentagon hoorde over de resultaten in de CIA-analyses en vroeg om toegang. De Special Operations Forces in Irak en Afghanistan begonnen het systeem te gebruiken om IED-netwerken — netwerken van berymbommen — in kaart te brengen. De resultaten waren opmerkelijk: in sommige regio's daalde het aantal IED-aanvallen met meer dan 60 procent nadat Palantir werd ingezet.

Dit succes transformeerde het bedrijf. Niet alleen financieel, maar ook qua identiteit. Palantir presenteerde zichzelf niet langer als een data-analysebedrijf. Het presenteerde zichzelf als een bedrijf dat levens redde. En dat verhaal — van technologie als de redder van soldatenlevens — was krachtig genoeg om kritische vragen over toezicht en privacy jaren achter te houden.

Palantir is niet het product van één persoon. Het netwerk dat Thiel meebracht vanuit zijn PayPal-jaren — Reid Hoffman, David Sacks, Max Levchin, Keith Rabois — leverde zowel kapitaal als verwijzingen naar vroege klanten. De Silicon Valley-credibiliteit die dit netwerk uitstraalde, was voor overheidsbeslissers een signaal: dit waren geen hobbyisten, dit waren serieuze operators.

De naamkeuze als bedrijfsstrategie

De naam Palantir was geen nostalgisch gebaar van een Tolkien-fan. Het was een strategische positionering. In de wereld van overheidscontracten, inlichtingendiensten en defensie, waar bedrijven normaal gesproken neutrale namen als 'Booz Allen Hamilton' of 'Leidos' dragen, stak een naam als Palantir er bewust en provocatief uit.

Tolkien-kenners in de inlichtingengemeenschap — en die waren er; de cultuur van de NSA en CIA heeft een opmerkelijk groot overlap met fantasy- en sci-fi-literatuur — begrepen de verwijzing onmiddellijk. De palantiri zijn niet alleen almachtige bollen: ze zijn ook gevaarlijk. Ze kunnen worden omgedraaid. Ze kunnen worden gebruikt om hun bezitters te misleiden. Sauron gebruikte ze als werktuig van bedrog. De naamkeuze erkende impliciet de dubbele aard van het product.

Dit is niet de verdediging die je verwacht van een bedrijf dat zijn technologie wil verkopen als neutraal instrument. Het is de verdediging van een bedrijf dat zich positioneert als bewust van het risico dat het introduceert — en dat vertrouwt op de morele kwaliteit van zijn klanten om dat risico te beheersen. In een sector waar iedereen neutraliteit pretendeert, was dat een opmerkelijk eerlijk standpunt.

De filosofische wortels van Palantir

Palantir's intellectuele DNA is ongebruikelijk voor een technologiebedrijf. Terwijl de meeste Silicon Valley-ondernemers hun filosofische inspiratie halen uit Ayn Rand's objectivisme of het pragmatisme van Silicon Valley-cultuur, put Thiel uit een rijkere en meer gelaagde traditie.

Leo Strauss — de politieke filosoof wiens conservatieve denken de neoconservatieve beweging in de VS sterk beïnvloedde — is een belangrijke referentie voor Thiel. Strauss geloofde dat samenlevingen worden geleid door een kleine elite van filosofen-koningen die de waarheid kennen maar die waarheid moeten verbergen voor de massa, die er niet klaar voor is. Dit esoterische principe — waarheid voor de elite, nuttige mythen voor het volk — is een terugkerend thema in Thiels denken.

René Girard — de Franse antropoloog en literatuurwetenschapper die de theorie van mimetisch verlangen ontwikkelde — is een andere centrale referentie. Girard stelde dat menselijk gedrag wordt gedreven door het verlangen om te willen wat anderen willen, niet door autonome preferenties. Conflicten ontstaan wanneer rivaliserend verlangen escaleert. Thiel heeft zich uitvoerig uitgesproken over Girards invloed op zijn denken — en dat denken kleurt zijn visie op concurrentie, de technologiesector en geopolitiek.

Deze filosofische wortels zijn niet academisch irrelevant. Ze verklaren waarom Thiel fundamenteel anders denkt over concurrentie (hij gelooft dat monopolies goed zijn voor innovatie), over democratie (hij gelooft dat democratie en vrijheid niet per se compatibel zijn) en over de rol van een elite in het sturen van de toekomst (hij gelooft dat visionaire individuen het recht hebben om de wereld te vormen).

De Thiel Fellowship en de toekomst van het onderwijs

In 2010 startte Thiel de Thiel Fellowship: een programma dat jaarlijks twintig jongeren onder de 23 jaar 100.000 dollar geeft om de universiteit te verlaten en een bedrijf te starten. De impliciete boodschap: universitair onderwijs is een zeepbel die mensen opzadelt met schulden voor een credential die steeds minder waard is.

Thiel Fellows hebben indrukwekkende bedrijven opgericht: Vitalik Buterin (Ethereum), Dylan Field (Figma), Ritesh Agarwal (OYO Hotels). Maar de Fellowship heeft ook kritiek gekregen: het werkt alleen voor mensen die al uitzonderlijk getalenteerd zijn en die het zich kunnen veroorloven om te falen. Het ondermijnt het principe van gelijke toegang tot onderwijs als basis voor sociale mobiliteit.

De onderliggende filosofie — dat conventionele instituties als de universiteit overbodig zijn geworden en dat individueel genie de motor van de toekomst is — contrasteert scherp met het egalitaire ideaal van publieke educatie. Het is ook consistent met Thiels bredere visie: een kleine elite van uitzonderlijke individuen die de toekomst vormgeeft, in plaats van democratische instituties die collectieve beslissingen nemen.

Peter Thiel en de PayPal-oorsprong van data-denken

De intellectuele doorbraak die Palantir mogelijk maakte, ontstond niet bij een overheidsopdracht maar bij een praktisch fraude-probleem. PayPal, het betalingsbedrijf dat Thiel mede oprichtte, werd in de vroege jaren nul geplaagd door massale fraude: criminele netwerken die valse accounts aanmaakten, gestolen creditcards gebruikten en miljoenen dollars per dag wegsluisden voordat het bedrijf het door had.

Het anti-fraude-team van PayPal — waaronder de jonge ingenieurs die later Palantir zouden oprichten — ontwierp een systeem dat relaties tussen accounts analyseerde in plaats van individuele transacties. Als vijf accounts allemaal geld stuurden naar dezelfde ontvanger op hetzelfde moment, was dat een sterker signaal van fraude dan elke transactie afzonderlijk. Netwerkanalyse, niet transactie-analyse, was de sleutel.

Dit inzicht — dat de patronen in netwerken meer informatie bevatten dan de afzonderlijke datapunten — is het kernprincipe achter Palantir's architectuur. Gotham analyseert geen individuen: het analyseert relaties, patronen en netwerken. Dat maakt het zo krachtig en zo anders dan traditionele databeheertools.

Na de verkoop van PayPal aan eBay hadden Thiel en zijn team het kapitaal, de technische expertise en — cruciaal — het conceptuele framework dat ze nodig hadden. De vraag was alleen: welke markt was groot genoeg en urgent genoeg om deze aanpak te rechtvaardigen? Het antwoord, in de nasleep van 9/11, was duidelijk: inlichtingen en nationale veiligheid.

De cultuur van Palantir: forward deployed engineers

Palantir heeft een ongebruikelijk bedrijfsmodel: het stuurt zijn eigen ingenieurs — 'forward deployed engineers' (FDE's) — naar de kantoren van zijn klanten om ter plaatse systemen te bouwen en te onderhouden. In plaats van software te leveren en de klant te laten uitzoeken hoe hij het moet gebruiken, leeft een deel van Palantirs personeel feitelijk bij zijn klanten in.

Dit model heeft voordelen: Palantir begrijpt de problemen van zijn klanten beter dan welke andere softwareleverancier, kan snel aanpassen en heeft diepere institutionele kennis. Maar het heeft ook implicaties: FDE's weten precies hoe klanten hun systemen gebruiken, welke vragen ze stellen, welke datastructuren ze hebben. Die kennis is proprietary en maakt de klant nog afhankelijker van Palantir.

In de inlichtingengemeenschap — waar Palantir zijn meest gevoelige werk doet — zijn FDE's ook een veiligheidsrisico: ze hebben toegang tot gerubriceerde systemen en data. Het is een ongebruikelijk arrangement dat vereist dat Palantir-medewerkers veiligheidsmachtigingen hebben op het niveau van de klant — een uitzonderlijke positie voor een private contractor.

Thiel en het libertarische project

Peter Thiel's politieke filosofie is het best te begrijpen als radicaal libertarianisme: een diep wantrouwen van de staat als ordenende actor, gecombineerd met een geloof in de capaciteit van individueel genie om de menselijke conditie te verbeteren. Dit is geen gewoon Amerikaans conservatisme: Thiel heeft de Democraten en Republikeinen beide bekritiseerd als vertegenwoordigers van gevestigde belangen die echte verandering blokkeren.

In een beruchte passage uit 2009 schreef Thiel: 'Ik geloof niet langer dat vrijheid en democratie compatibel zijn.' Hij doelde op zijn observatie dat demografische expansie — meer kiezers, inclusief mensen die voor herverdeling stemmen — structureel vrijheidsverkleining in de hand werkt. Zijn alternatief: technologische escape-routes uit de democratische staat, via zee-steads, ruimtekolonies of het cyberspace.

Dit is de ideologische kern van waaruit men Palantir moet begrijpen: het is niet een bedrijf dat de democratische staat wil versterken — het is een bedrijf dat de staat wil instrumentaliseren voor de bescherming van de westerse beschaving zoals Thiel die definieert. Als de staat toevallig democratisch is, prima. Als de uitkomsten van de democratie hem niet bevallen, zoekt hij alternatieven.

Dit verklaart ook waarom Thiel zo vrij was om Trump te steunen in 2016, terwijl veel Silicon Valley-figuren zich distantieerden. Thiel zag in Trump geen bedreiging voor de democratische orde maar een mogelijkheid om de democratische orde te hervormen — of te omzeilen — ten gunste van een sterkere, meer daadkrachtige staat die zijn agenda van technologische en militaire suprematie kon uitvoeren.

HOOFDSTUK 2

In-Q-Tel: De CIA als Durfkapitalist

Hoe de geheimste opdrachtgever ter wereld de technologiesector vormde

In-Q-Tel is misschien de meest invloedrijke investeerder die de meeste mensen nog nooit van hebben gehoord. Opgericht in 1999 door de CIA, heeft het bedrijf in stilte mede de basis gelegd voor technologieën die nu de dagelijkse basis van onze digitale wereld vormen.

Wat is In-Q-Tel?

In-Q-Tel (IQT) is een non-profit durfkapitaalonderneming die in 1999 door de CIA werd opgericht om de kloof te overbruggen tussen de snelle innovatie in de private sector en de behoeften van de nationale veiligheidsinfrastructuur. De naam verwijst naar 'Q', het fictieve personage uit de James Bond-films dat technologische uitvindingen maakt voor de geheime dienst.

Het model is vernuftig: IQT investeert kleine bedragen — doorgaans 500.000 tot 3 miljoen dollar — in veelbelovende startups. In ruil daarvoor krijgt IQT toegang tot de technologie en een positie als 'board observer'. De CIA krijgt vroege toegang tot baanbrekende technologieën en kan die direct testen in operationele contexten. De startups krijgen geloofwaardigheid, kapitaal en een eerste klant die goed betaalt.

De bedrijven die uit In-Q-Tel zijn voortgekomen

De portfolio van In-Q-Tel leest als een wie-is-wie van de moderne technologiesector. Keyhole — een geospatiale data-visualisatietool — werd in 2004 overgenomen door Google en werd de basis voor Google Earth. Via dat overnamebedrag ontving IQT Google-aandelen ter waarde van meer dan 2,2 miljoen dollar.

Amazon verwierf twee IQT-gesteunde bedrijven: AppThwack (later AWS Device Farm) en Elemental Technologies, betaald voor 500 miljoen dollar. Ook Palantir zelf begon met IQT-geld. De suggestie die hieruit voortkomt — dat de CIA mede aan de

basis stond van Google Earth, Amazon Web Services en Palantir — is niet overdreven. Ze is feitelijk.

Bedrijf	Investing	Uitkomst
Keyhole	\$527.500	Overgenomen door Google → Google Earth
Palantir	~£1,3 mln	Huidige beurswaarde \$430+ mrd (2025)
AppThwack	\$610.000	Overgenomen door Amazon → AWS Device Farm
Elemental Tech.	\$45,7 mln	Overgenomen door Amazon (\$500 mln)
Acalvio	Niet pub.	AI-cyberbeveiliging (actief 2026)

Selectie van bekende In-Q-Tel portfolio-bedrijven. Bron: Crunchbase, Grey Dynamics

Waarom er geen goed alternatief is voor Microsoft, AWS en Google

Er is een vraag die zelden gesteld wordt maar cruciaal is: waarom gebruiken vrijwel alle grote bedrijven ter wereld óf Microsoft Azure, óf Amazon Web Services, óf Google Cloud? Er zijn tientallen kleinere cloudproviders — maar de markt is volledig gedomineerd door drie Amerikaanse giganten. Is dat toeval?

Een deel van het antwoord ligt in de enorme kapitaalinvesteringen die nodig zijn voor hyperscale cloudinfrastructuur. Een ander deel ligt in de netwerkeconomieën: hoe meer gebruikers, hoe meer diensten, hoe aantrekkelijker het platform. Maar er is ook een derde factor: de Amerikaanse overheid — via In-Q-Tel, via directe contracten, via JEDI en JWCC — is de grootste en meest loyale klant van al drie.

Het is geen complottheorie om te stellen dat de CIA, het Ministerie van Defensie en de NSA een belang hebben bij het vermijden van Europese of Chinese alternatieven. Europese alternatieven zoals Deutsche Telekom Cloud, OVHcloud of Nederlandse providers kunnen die schaal gewoon niet bieden — en worden ook niet actief bevoordeeld door overheidsbeleid.

DATASOEVEREINITEIT

Wanneer een Nederlands bedrijf zijn data opslaat in Microsoft Azure of Amazon AWS, slaat het die data feitelijk op in een Amerikaans-gecontroleerde infrastructuur. De CLOUD Act (2018) geeft de Amerikaanse overheid het recht om toegang te eisen tot die data, ongeacht waar de servers fysiek staan — ook als ze in Europa staan.