Drones, Kalashnikov's en tanks. Allemaal wapens waar je wel eens van hebt gehoord.
Maar van je weet hoe ze eruitzien. Maar overheden beschikken ook over zeer schadelijke digitale wapens. Ook de Nederlandse geheimedienst. Een belangrijk en bekend wapen is spyware.
En binnen die categorie is er eigenlijk maar één het meest berucht. Pegasus. Deze spyware is bewust vernoemd naar het paard met vleugels uit de Griekse mythologie. Het computervirus kan namelijk vliegend door de lucht worden afgevuurd om mobiele telefoons te infecteren, data te verzamelen en om je af te luisteren. Een beetje het gevoel als of je in je blootje staat.
Als of iemand in je badkamer, in je bed binnenkomt. In Israel is de NSO group gevestigd. Zij zijn een groot ontwiklaar van cyberwapens en de eigenaar van Pegasus. Overheden gebruiken het om criminele
of terroristen op te sporen. Maar soms ook om activisten, journalisten en de oppositie in de gaten te houden. Het enige dat nodig is om Pegasus te activeren is een telefoonnummer. In je kuntje voorstellen dat wanneer dit met verkeerde motieven wordt ingezet het ramsalige gevolgen kan hebben. Dus het kan gebruikt worden om iemand te bespioneren, iemand te trekken en die vervolgens
naar een ambassade bijvoorbeeld toe te lokken en in stukjes te hakken, want dat is wat er met hem gebeurd is. Ik ben Daniel Verlaan en als techjournalist onderzoek ik het internet. In deze podcast hoor je waar gebeurde verhalen die zich online en vaak recht onder je neus afspelen.
Maar toch onzichtbaar zijn. Je luistert naar ik weet gewachtwoord. Dit is aflevering 5 van seizoen 2.
Ik praat even wat zachter omdat ik in een volle trein naar Brussel zit. Ik heb een afspraak met Peter Verlinde. Hij is een Vlaamse onderzoekjournalist en geïnfecteerd door de allersterkste spyware
die je ken. Pegasus. En niet of cybercriminele, maar door de overheid van Rwanda. We hebben afgesproken
in een hotelkamer in het centrum van de stad. Het zijn wel in ieder geval een beetje dicht in moet praten. Dank je wel dat je ons wil moeten hier in het hotel in Brussel. We zitten hier eigenlijk met een hele duidelijke reden en dat jij bent gehakt met denk ik het meest gevaarlijke digitale wapen dat er bestaat. Pegasus. Pegasus van een israelisch firma. En het blijkt inderdaad in van de meest gesoffisticeerde vormen van spyware te zijn. Peter schrijft al sinds de jaren 90 kritische reportages over het Rwandese regime. Hij is eerlijk en hard in zijn stukken. Twee eigenschappen die door
de Rwandese machthebbers niet worden gewaardeerd. Ik denk dat heel veel mensen nu luisteren en niet denken dit is mijn grootste nachtmerrie om daarmee geïnfecteerd te worden. Ja, ik heb natuurlijk als journalist hier nogal met delicaten dossiers ons bezig is ook wel wel meegemaakt.
Niet dat ik dit zo'n fijne ervaring vond. Maar het is inderdaad wel een als je er goed
over door denkt en op het moment dat we, ik zeg we omdat ook de telefoon van mijn echtgenoten gehekt geweest is. Als je daar even over door denkt, dan is het natuurlijk inderdaad een bijzonder akelig idee en realiteit. Het feit dat iemand in je telefoon kruipt en die volledig in bezit neemt, also dat die jezelf is, also dat die gewoon alles kan doen wat ik normaal met mijn telefoon
doe. Spyware zijn eigenlijk gewoon cyberwapens, dus het zijn metoden om mensen hun telefoons eigenlijk over te nemen en daarmee te bespioneren, dus die specifieke persoon te bespioneren.
Het voordeel van mobieltjes is dat, dat kennen we allemaal wel, die dragen we altijd bij ons.
Er zit een microfoon in, er zit een camera in, er zit een trucking device in,

dus het beste spyware middel dat je kan bedenken. Je hoort Ricky Gevers,
hij is ethisch hacker en volgt de ontwikkelingen van Pegasus op de voet. Ja, dat is echt
een softwarepakket, zo moet je het echt zien en dus jij gaat op jouw laptop, kan je van alles
uitkiezen en vanaf die laptop eigenlijk kan jij mobieltjes gaan infecteren en dat kan op basis
bijvoorbeeld van een nummer, dus als ik jouw nummer heb, kan ik van alles jouw kant opsturen,
zodat ik die telefoon uiteindelijk kan overnemen. Vanuit die telefoon wordt allerlei informatie
vervolgens via allerlei servers weer terug naar jou gecommuniceerd zodat je kan zien wat er
in de hand is en de dingen die je bijvoorbeeld kan doen is de microfoon afluisteren of de camera
aanzetten maar ook precies zien waar die telefoon zich bevindt. Alles wat jij met jouw telefoon
kan, kan die personen ook, dus ik kan al jouw foto's bekijken, ik kan al je foto's downloaden,
ik kan al je films bekijken, al jouw video's downloaden, etc. etc. De verhaal van Peter is
gevlucht uit Rwanda. Ook zij heeft zich kritisch geuit over het regime. Peter is met haar vakantie
wanneer hij ontdekt dat er iets aan de hand is. We waren op vakantie in Frankrijk en ik kreeg een
telefoon van een nummer en een man die ik niet kende die zich aan de telefoon voorstelde als
iemand van de Belgische justitie. Dat klinkt op zich al een beetje vreemd. Wij noemden ook geen
naam, we noemden ook geen dienst en vroeg eigenlijk alleen bent u in België. En ik zei nee, we zijn
op vakantie in Frankrijk. Wanneer zijn jullie terug? Die datum zijn we terug, eind augustus was
het toen. Zou ik dan opnieuw contact mogen opnemen? Ik zei, ja, uiteraard, doe maar. Hij zei
niet waar het over ging. En toen we terug waren in België, dan belde hij en dan opnieuw en
zegt hij zijn jullie nu in België, ik zou graag langskomen. Hij zei dan nog altijd niet
waarover het ging. En die man spreekt nooit aan de telefoon over dingen waar het over gaat.
En dan hebben we een bepaald moment afgesproken en toen, gewoon thuis, dan het eerste wat hij
vroeg
dat is, hij toonde zijn legitimatie, dat hij inderdaad van de Militaire Inlichtingendienst was.
Hij zag er ook voor mij niet kwaadardig uit, dus ik had al een spontaan vertrouwen. En dan kwam,
dan heb ik die man ontvangen en dan vroeg die man van waar zijn jullie telefoons. En dan heb ik
gezegd
ja, ik heb de vermijnen op zak en die van mijn vrouw daar, zou je die telefoons even willen uitzetten,
op vliegtuigstand of uitzetten. En dan pas heeft hij gezegd van, kijk, daarom kom ik. En dan heeft
hij dus gezegd, kijk, we hebben een sterk vermoeden, maar we moeten het nu uitzoeken, maar we
hebben een
sterk vermoeden dat jullie op de shortlist staan van Rwanda voor Pegasus. De medewerker van de
Belgische Militaire Inlichtingendienst vraagt of Peter en zijn vrouw hun telefoons bij hem willen
inleveren voor naderonderzoek. En nog geen dag later krijgen ze reactie. Er is inderdaad Pegasus
aangetroffen op allebijen telefoons. Het lijkt me best wel een eng idee dat er iemand anders een
tijd heeft meegekeken met je telefoon. Kan je dat soms schrijven wat je dan voelt als je door de
Militaire Inlichtingendienst wordt benaderd met zeg, hey. Je hebt zo een beetje het gevoel,
misschien
gek om het zo uit te drukken, een beetje het gevoel als of je in je blootje staat, als of iemand in je
badkamer, in je bed binnenkomt. Je moet weten, telefoon is, maar ik denk dat iedereen dat in
tussen ook wel weten en ervaart. Een telefoon is tegenwoordig een telefoon meer, dat is eigenlijk
gewoon dat waarmee je zo wat al je communicatie voert, zowel privé. Bijvoorbeeld ik heb
voortdurend
berichtjes met mijn vrouw, ik ben nu daar, ik kom straks terug, ik tegen Damus met de kindjes.

Dus de meest persoonlijke zelfs ook bij momenten intieme communicatie, tot en met de meest professionele
in het voerige communicatie, via mail of bijlagers die je via WhatsApp stuurt. Het gevoel dat iemand aan alles aankan waar jij zelf eigenlijk voortdurend mee bezig bent, want ik ben professioneel, nog altijd zeer actief, hoewel ik eigenlijk met pensioen ben bij de openbare omroep, maar ik ben nog zeer actief. Dat geeft je zo een beetje het gevoel als of je nergens meer veilig bent.
Dat gevoel van onveiligheid begrijp ik nog beter als Peter me meeneemt naar de Afrikaanse buurt hier in Brussel. De avond is inmiddels gevallen en we lopen in het schemer donker door een wijk waar hij in zijn eentje echt niet naar toe gaat. We stoppen voor een café. Daar links het is hier, die larchipel. Dat zit vol met mensen die hier door de Anders-Ade naartoe gehaald worden, omdat ze hand en span dienst te verlenen zullen we maar zeggen.
Oké, hand langers. Zeg maar hier zou je niet naar binnen gaan?
Nee, nee, dat is niet...
Wat zou er dan gebeuren?
Over mij, onder elkaar gesproken worden, en gaat er een of andere ding naar Kigali en verschijnt er in de lokale pers, alle leiddingen, die hebben voorbeeld het feit dat ik met jou aan het praten ben en dan wordt er gezegd van verlinden is weer slechte dingen aan het zeggen over het regionale...
Er zitten ook echt veel mensen ons te kijken overigens. Ik weet niet of dat komt, dat we met de microfoon hier staan of dat jij wordt ergens.
Ik kan wel zeggen dat er bij de Rwandese zelfs een kans heel groot is dat ze mee herkennen.
Mijn collega Steven is ook in Brussel. Hij heeft een afspraak in het Europees Parlement met Sophie in het veld. Zij is Europarlementarier van D66 en geeft een belangrijke persconferentie over spionage-software.
Voorbidden Stories is een non-profit organisatie voor journalisten. Het helpt bij de coördinatie van risicovolle onderzoeksprojecten rond onderwerpen als schending van mensenrechten, milieuschandalen en corruptie bij regeringen.
Samen met mensenrechtenorganisatie Amnesty publiceerden ze in 2021 een lijst met 50.000 telefonummers van mensen die mogelijk waren gehackt met Pérasus. De personen op deze lijst bestonden voornamelijk uit journalisten, activisten en politici. De naam van de Franse president Macron wordt ook genoemd. Sophie in het veld is toen begonnen met een politiek onderzoek. Zij vindt dat er vanuit Europa veel meer toezicht en transparantie moet komen op spyware. Na afloop van de persconferentie stelt Steven haar nog een aantal vragen.
Waarom is dan zo'n spyware die in Israel wordt ontwikkeld en op de markt wordt gebracht?
Waarom is dat dan zo'n aanval op de democratie?
De kritische journalisten, kritische politici, klokkenluiders zijn de zuurstof van onze democratie. Democratie gaat over checks and balances. Democratie gaat over macht en tegenmacht. Dat is de kern van democratie. Als je de tegenmacht uitschakelt door misbruik van spyware, dan heb je dus geen democratie meer. En die democratie hebben wij allemaal nodig. Wij hebben democratie nodig voor onze kwaliteit van leven. Dus laten we die democratie een beetje koesteren. In Ukraine geven ze hun leven ervoor en op heel veel andere plekken van deze aardbol. Ik vind dat we daar zorgvuldiger mee moeten omgaan, minder achterloos.
Ethisch hacker Ricky ziet ook gevaar in de spyonage software als hij in 2018 in de

krant leest over de toot van een Saudi-Arabisch journalist.
Ja, een van de meest bloedige voorbeelden verder is die en de meest bekende ook tegelijkertijd, die van Jamal Khashoggi. Die werkt er voor de Washington Post, dus dat is een journalist. En de enkele maanden voordat hij vermoord is in de ambassade van Saudi-Arabi in Turkije zijn vrouw geïnfecteerd met pechasses. Nou kan je die twee natuurlijk niet direct met elkaar relateren, maar het is echt wel hoog waarschijnlijk dat die met elkaar enigszins te maken hebben. En dat geven we bijvoorbeeld aan hoe verkeerd deze apparatuur ook ingezet kan worden, dus het kan gebruikt worden om iemand te bespioneren, iemand te tracken en die vervolgens naar een ambassade bijvoorbeeld toe te locken en in stukjes te hakken, want dat is wat er met hem gebeurd is.
Dit verhaal raak mij ook persoonlijk. Als journalist vind ik het belangrijk om mijn bronnen altijd te beschermen. Ik zou het heel heftig vinden als mijn overheid mee kan lezen met al mijn berichten, mijn contactenlijst kan inzien en privégesprekken kan volgen.
Eigenlijk precies dat, want Peter is overkomen. Nadat Peter weet dat hij is gehakt, komt hij in een hele lastige situatie terecht. Hij kan zijn Rwandese contacten niet zomaar een bericht sturen om te laten weten dat ze voorzichtig moeten zijn, want ja, wie leest er nog meer mee?
Hij verzint het volgende. In verschillende talen geeft hij interviews aan kranten en nieuwsites in de hoop dat zijn bronnen de waarschuwing op die manier zullen lezen. Ik zie de koppen ook zelf langskomen. Vlaamse onderzoekjournalist gehakt met Pegasus.
Heb jij enig idee dat er bronnen zijn, die jij hebt gebruikt, die na de Pegasusinfectie waar je nooit meer van hebt gehoord, die van de radar zijn verdwenen?
Zeker twee die we bij een naam kennen, maar ik ga die naam natuurlijk niet noemen, maar die we bij een naam kennen waar we sinds die niets meer van gehoord hebben. En dat waren dus mensen waar wij mee in contact waren. En die dus met de Mozambikaansnummer in dat geval. Heeft dat iets te maken met ons Pegasus verhaal, dat kunnen we niet weten. Ik denk daar eerlijk gezegd liever niet te veel over na.
Je telefoon is privé toch? Er staan berichten op, foto's en gegevens die echt niet voor andere bestemd zijn. Niet per se omdat je iets te verbergen hebt, maar gewoon omdat je recht hebt op privacy. Je hebt vast wel eens gedacht, het is maar goed dat niemand mee kan kijken.
Maar is dat er reële angst bij mensen, dat ze gevolgd worden door een overheid?
Ja ik vind het wel een veilig idee als de AIVD toegang heeft tot telefoon gegevens. Natuurlijk helemaal binnen een bepaalde context met veiligheidsaspecten.
Omdat de dingen op mijn telefoon wel gewoon privé zijn en voor mij zijn. En ik vind het niet veilig als andere mensen dat mee kunnen lezen of kijken. Nee.
Ik vind het een beetje eng dat ze zoveel macht hebben om dat te kunnen doen. Ik vind dat eigenlijk enger dan het idee dat iemand op zijn telefoon wil ik voor iets kan doen. Dat gaat net iets te ver, denk ik.
Moet jij je als burger ook zorgen maken om met Pegasus geïnfecteerd te worden?
Jordi Scharlow is van onze partner KPM.
Als doodnormale burger heb je gelukkig niet zoveel te vrezen. Pegasus is iets wat heel toegericht, specialistisch wordt ingezet. Het maakt gebruik van hele kostbare beveiligingslekken waarvan de fabrikant niet wil dat ze bekend worden en gedicht worden. Het leent zich dus niet echt voor de massa. Ik zou zeggen dat Pegasus het is wel een

dreiging voor de democratie, maar als doodnormale burger heb je niet zoveel te vrezen.
KPM zet zich op veel manieren in voor ondernemers. KPM werkt 24-7 aan het veilig houden van bedrijven
en hun data en biedt overzichtelijke oplossingen om de cybersecurity binnen jouw bedrijf te verbeteren.
Als ondernemer ben je al druk genoeg, dus laat KPM je helpen om jouw bedrijf veilig te houden.
Wil je weten hoe dat kan? Kijk dan op kpn.com slash veiligheid.
De Pegasus software maakt gebruik van lekken die gezocht worden in de beveiliging van iPhone en Android. Om de lekken op te sporen, worden digitale onderzoekers flink betaald.
Je moet het zo zien dat die kwetsbaarheden in die telefoonsystemen, dus in een Android of in een Apple iPhone, die vind je niet zomaar. Dat is echt een vakgebied op zichzelf en daar zijn specifieke onderzoekers daarin gespecialiseerd. Dan moet je denken dat die echt enkele maanden
op zoek zijn en zeker niet iedereen kan dat. Die zijn maanden op zoek naar zoiets en die vinden zo'n kwetsbaarheid en die kunnen ze vervolgens verkopen. Dan heb je bijvoorbeeld een platform dat heet Zerodium. Daar kan je naartoe gaan en als die kwetsbaarheid goed is, die jongens testen dat dan, dan krijg jij binnen drie dagen geld voor je noem. Het kan soms een miljoen zijn bijvoorbeeld, dus dat kan heel lucratief zijn als je daar goed in bent.
Nochmal is het echt heel gespecialiseerd, dus echt niet iedereen kan dat zomaar. Maar je kan ook naar een NSO-group zelf toegaan en het daar direct bijvoorbeeld verkopen.
De manier waarop ze lekken vinden is zelfs zo slim dat het slachtoffer nergens op hoeft te klikken, oftewel het zero-klik-principe. Eerder in deze aflevering vertelde ik al dat Pegasus gemaakt en verkocht wordt door de israelische NSO-group. Maar wat is dit voor groep en wat voor mensen werken er?
Ja, het zijn dus vooral mensen die uit de inlichtingendienst komen en uit de israelische inlichtingendienst, dus dan moet je aan de monsat bijvoorbeeld denken. Het vervelende is, dit zijn nieuwe bedrijfjes, dus die krijgen eigenlijk extra aandacht en we begrijpen allemaal dat je of eenvoudig een verkeerde afslag met dit soort apparatuur kan maken. Dus daardoor is er eigenlijk extra focus op van wat gebeurt hier en wat wordt er mee gedaan. En als dat doen, dan wordt deze NSO-group eigenlijk door mensen uit mijn vakgebied goed in de gaten gehouden om te kijken of ze niet hele voulte dingen eigenlijk aan het doen zijn.
Europarlementarier Sophie Innetveld vindt het op z'n zacht gezegd opmerkelijk dat de NSO-group vrijwel geen weerstand vragen of kritiek van de Europese Commissie krijgt bij het verkopen van hun spyware. Ze doen hun bankzaken via Luxemburg, ze doen hun export via Cyprus en Bulgarije, daar zit ook nog een ontwikkelingstak dus dat is gewoon vanuit Europa. Zij hebben wel het spul geleverd waarmee Kamal Yajouki is gehekt. Die man die vermoord is door de zaudische autoriteiten en in stukken is gehakt in de Turkse ambassade. En in zo heeft dat spul gewoon aan Saudi-Arabië verkocht. Dus wij moeten ons dan toch ook afvragen als Europa waar zijn we
eigenlijk mee bezig. Eén van de redenen waarom jij niet echt bang hoeft te zijn voor een aanval met Pegasus is vanwege het geld. Het aanschaffen van de software is namelijk fucking duur. Samen met Ricky duik ik in de actuele prijzenlijst. Ik pak hier nu eventjes de prijzenlijstvormen van in dit geval Zerodium, dat is een van de meest bekende bedrijven, er zijn er veel meer trouwens die dat doen, maar dat is naar de meest gangbare. Op hun website hebben ze ook echt

gewoon een prijzlijst staan van hoe duur al die dingen zijn of hoeveel geld jij ervoor krijgt als je dat meldt bij ze. De duurste op dit moment is een Android full chain with persistence. Dus wat dat op het moment dat je zo'n Android telefoon hekt, dan blijft die mal waar daar zitten. Dus dan kan je eigenlijk voor de rest van de tijd zo'n Android device volgen en dat is 2,5 miljoen waard. Dus daar kan je tegelijkertijd opmaken dat de hoeveelheid exploits voor Android dat die het meest celte zijn. Dat is gewoon marktwerking in feite. De tweede prijs die je daar hebt is de iOS full chain persistence, dus dat is dezelfde als de Android maar ietsje goedkoper is die, die is 2 miljoen. Dus kan je 2 miljoen euro vervangen als jij een lek daarin vindt op dit moment. Stel dat ik dus weet van jij bent een high value target voor mij en jij hebt een iPhone en ik wil jou, je bent een terrorisme voorbeeld en ik wil jou over hele lange tijd gewoon trekken om precies te weten wat jij doet. Nou dan moet ik 2,5 miljoen op tafel gaan leggen om dat te kunnen doen. Dus die marktwerking zorgt er gelijkertijd voor dat het niet zomaar behadbaar voor alles en iedereen is. Tegelijkertijd mensen met voldoende geld of overheden met voldoende geld die hebben
hier vrije toegang tot en die kunnen dit vrij eenvoudig dus overal inzetten. Hoeveel, hoeveel denk je dat jij waard was voor deze overheid? Dat vind ik eigenlijk een hele mooie vraag want dat is precies wat wij onszelf ook bedachten. Wij hebben onze bedenking gemaakt, de buulen mijn echtgenoten en ik zelf hebben onze bedenking gemaakt. Zijn wij nu echt zo veel waard? We voelden
ons op bepaald moment zo'n beetje verheven. Zijn wij nu echt zo belangrijk? Er circuleren bedragen, ik ken ze niet uit mijn hoofd van wat Pegasus kost, wat men ons wel vertelt heeft bij de militaire inlichtingendienst. Dat is dat het gebruik van Pegasus, dat dat niet alleen een kost is per telefoon maar ook voor de duurtijd dat die besmetting gebeurt. En dus als men een uur volgt of iemand een week volgt, dat maakt wel heel wat uit. En dus inderdaad, dat is een dure aangelegenheid en ik denk dat er want als een geld beter kan besteden. Heel veel overheden beschikken over Pegasus, ook de Nederlandse overheid, zo bleek uit onderzoek van de volkskrant. Of ze die spy weer ook dat werkelijk inzetten? En als we het over ons eigen land hebben dus we weten dat het dat wij het zelf ook gekocht hebben, is er enig zicht op of wij dat ook gebruikt hebben? Nou ja, er is dat een de beroemde geval dus van Riddo Antaghi, die met Pegasus opgespoord
zou zijn, dat kan. Kijk, uiteindelijk vind ik dat overheden gewoon veel opener over dit soort dingen moeten zijn, of dat het in ieder geval controlerbaar moet zijn. Al was het maar door een toezichthouder of door een parlement of wat ook, maar dat het gewoon helemaal zich aan een soort
aan de openbaarheid onttrekt, dat vind ik gewoon niet in de haak. Ik vind het ook heel raar, want als burger ben je een beetje een beetje soort vogelvrij, want als je kritisch uitgeproken bent, actief bent, wat dan ook, dan zou je dus het risico kunnen lopen dat je, en dan moet je maar hopen dat je regering hebt van fatsoenlijke mensen of zo, maar daar kan het toch niet vanafhankelijk zijn. Nee, en dus onze eigen regering is net zo gesloten als al die andere lidstaten, die hebben het vast. Maar dat zijn ze allemaal, maar ik heb dat gericht, dat is de Omerta, gewoon zwijgen. Ja, en Nederland hoort ook bij die Omerta. Ja. Als ik Peter was geweest, had ik meteen een nieuwe telefoon gekocht en het gehackte apparaat laten vernietigen, maar Peter denkt er
anders over. Dus jij gebruikt nog steeds dezelfde telefoon? Ik gebruik nog steeds dezelfde telefoon.

Ja, een van onze kinderen is zo wat toe aan een eigen telefoon en ik had aan mijn echtgenote gezegd van jammer weet je wat we doen, we maken een van onze telefoons volledig leeg, we zetten daar een nieuwe batterij in voor 60 euro en dan heeft onze dochter, heeft ze dan een eigen telefoon en dan heeft mijn vrouw gezegd nee dat wil ik niet. Ik wil niet dat een telefoon die ooit besmet is door Pegasus, dat nu een van de kinderen die heeft, want dan kunnen ze dat kind weer gaan volgen, omdat ze dus die code van die telefoon kennen. Maak je wel eens zorgen naar die Pegasus infectie over je kinderen? Ja, natuurlijk, uiteraard. Is dat erg geworden door Pegasus? Tussen je twee oren wel, terwijl het eigenlijk rationeel eigenlijk geen verschil zou mogen maken, want waar onze kinderen op school gaan, wat hun vrijheidsbesteding is en zo, uiteraard weten ze dat gewoon van ons agenda's. En oké, we hebben dan wel die paswoorden veranderd, maar dat is allemaal gemakkelijk te weten te komen. Maar psychologisch, gewoon in je mentaal, in je geest heeft dat wel gealerteerd, omdat je het gevoel hebt, ja, als ze alles over je weten, dan weten ze ook dat je kinderen op dat moment op school zitten, op dat moment thuis komen, ook wil eens een keertje en alleen thuis zijn, dat soort dingen allemaal. Maar om dat in real-time, dus op de huidige moment te kunnen achterhalen, zouden ze eigenlijk daar Pegasus opnieuw moeten opzetten.
Vanaf het Europees Parlement is er nog geen oplossing voor mensen zoals Peter die doelwit zijn of zijn geweest van Pegasus. Ik kan Europa iets voor hem doen dan als het uit Rwanda komt. Dat is heel lastig. Ja, kijk, je kan wel in je buitenlandse betrekking of ook bijvoorbeeld in ontwikkelingshulp of zo, want het is dus heel gek als je ontwikkelingshulp geeft en dat wordt vervolgens door een regering gebruikt om dit soort spul aan te kopen, dat is natuurlijk niet de bedoeling. Maar nee, dat is heel lastig als dat zo van buiten af gaat. Dus daarom denk ik ook, we zullen het dus ook nooit helemaal 100% in de greep krijgen. Maar als je de industrie al voor een heel groot deel kan reguleren, als je tegen bedrijven zegt, jongens, als jullie zaken willen doen in Europa of in de VS, dan mag je niet aan dit soort regimes verkopen. Ja, dan moeten ze dus gaan kiezen van waar zit de grotere markt, Europa in de VS of Rwanda. Nou ja, weet je, zo kan je indirect, kan je wel invloed uitoefenen. Je luisterde naar Ik weet je wachtwoord. Check ook het gelijknamige boek, de documentair op Vierderland of volg op Ets Daniel Vlaan.