[Transcript] DS Vandaag / Predator Files: Geen enkele smartphone lijkt nog veilig voor spionnen

Dit is Vandaag, de dagelijks podcast van de standaard.
Ik ben Alexander Lippenveld.
De spionageapparatuur Predator die in Europa ontwikkeld is,
wordt over de hele wereld verkocht.
Ook aan dictators, met wie volgens de Europese regels,
geen handel gedreven mag worden.
En Europese toplui waren zelfs het doelwit van die spionage-software.
Dat blijkt allemaal uit de Predator files.
Hoe komt die Europese spionage-software in slechte handen terecht?
Onze collega's zijn de laatste weken diep in de Predator files gedoken
samen met een heel aantal andere journalisten van het onderzoeksconsortium IJK.
En hun resultaten kan je lezen op onze website standaard.be.
De Predator files, je vindt het wel, is een heel interessant dossier.
Als je als min 26-jarige nog geen abonnement hebt,
dan hebben we een heel interessant aanbod.
Want voor amper 1 euro per week kan je de standaard al lezen.
Alle info vind je op standaard.be.
En nu een fragmentje over de spionage-software Pegasus.
Dat waren twee onderzoekers van de onderzoeksgroep
Forensic Architecture in een video van Vice News.
In 2021 publiceerden ze een groot onderzoek naar het wijtverspreidegebruik
van de israelische spionage-software Pegasus,
Nikolas van Hekken en Roelander Mote.
Jullie hebben de voorbijdagen ook al een paar opvallende spionageverhalen
aan onze lezers voorgeschoteld.
Het gaat over Predator, een andere spionagesysteem.
Het jongste verhaal slaat misschien wel alles.
Vietnam heeft geprobeerd de telefoons
te hekken van onder meer Europees parlements,
voorzitter Roberta Metzola,
met die Predator-software die in Europa werd ontwikkeld.
Vertel eens.
Ja, toen wij dat voor het eerst vernamen waren,
waren we er ook zelf verrast.
Zoals je daar net al vertelde,
Alexander gaat het allemaal om de spionageware die Predator heet.
Heel eenvoudig gesteld.
Als die terechtkomt op je smartphone, dan ben je gezien,
letterlijk en figuurlijk.
Dan is praktisch alles wat erop passeert leesbaar voor wie jou aanvalt.
Nu, of dat ook zo is geweest bij Metzola, is het nog niet duidelijk,
maar wel heel wel zeker is,
is dat zij het doel is geweest daarvan.

En dat ging als volgt in zijn werk,
van op een Twitter-account,
pardon, van op een X-account moeten we dus tegorens zijn,
genaamd Joseph Gordon XVI,
werd een berichtje en een link gestuurd naar haar X-account.
De tekst in dat berichtje was wel eens waar in Tengels.
En daar was er ook een link bij,
die leek op een nieuwsartikel van de South China Morning Post,
een belangrijke krant in Hongkong.
En wie daarop klikte, met Zola of iemand anders,
die besmetten dan eigenlijk zijn of haar toestel met die Predator spyware.
Ja, oké, een soort van Trojan Horse virus,
die tactiek, zo is het.
En waarom wou Vietnam Europa bespioneren?
Wel, behalve met Zola,
waren er ook heel veel Europese instanties die daarmee te maken kregen,
met die besmettingspogingen.
Heel concreet was het een Europees project
rond propere oceanen en waterlopen.
Ook de directeur-generaal voor maritime zaken
werd in de val gelokt,
net zoals de directoraal-generaal voor klimaatactie,
waarover er een belg aan het hoofd staat.
Wat er vaak terugkomt bij die doelwitte,
is dat zij iets te maken hebben met de visserij of met de maritime sector.
Tussen de EU en Vietnam is er sinds een paar jaar
een conflict bezig over illegale visserij,
want de commissie vindt dat Vietnam te weinig doet
om die visserij te bestrijden.
Dus ja, dat is mogelijk een van de aanleidingen
voor die pogingen tot hekking.
We hebben het zo meteen over die Predator en die herkomst daarvan,
maar wordt het ook nog door andere regimes gebruikt dan Vietnam, Roeland?
Het wordt door een vrij stevige reeks regimes gebruikt.
En wat je ziet, is dat er kopers van Predator die we onderzocht hebben
dat hij het probeerde uit te voeren naar verschillende regimes,
of het nu in Afrika uit de Middle East of Asia is.
Maar ook in Europa werd ook Griekenland ervan beschuldigd
om Predator gebruik te hebben ook.
Ik weet niet of jullie het je herinneren,
maar in de afgelopen jaren was er een flink schandaal in Griekenland,
want daar bleek plot dat zowel journalisten
als de leider van de oppositie, van de sociaal-democratische oppositie,

als mensen binnen de partijen van premier Mitsotakis,
de centrum-next premier Mitsotakis, zouden afgeluisterd zijn.
Vaak ging het om interne rivale van Mitsotakis.
En een aantal van die mensen bleken ook links ontvangt te hebben,
waar het bleek, dat zij ook wel echt de doel werd waren van Predator,
wat de Grieken ontkennen.
Ze ontkennen dat ze Predator gebruikt hebben,
maar we weten wel dat die mensen afgeluisterd zijn met telefoons
en dat ze het doel werd waren van de overheid.
Dat is nu nog op schandaal geweest in Griekenland,
maar dat heeft een beperkt staartje gehad
in de zin dat een aantal van de verantwoordelijke onder meer Mitsotakis neef.
Die een belangrijk luid- en antwoord van Mitsotakis
en verantwoordelijk voor eerlichtingendiensten moest afscheid nemen.
Het Griekse schandaal werd ook besproken in het Europees Parlement.
We luisteren even naar het eerste Parlementslit Claire Daily.
De truth is that this scandal really is just the tip of an iceberg.
The design, sale and use of spying technologies doesn't happen by accident.
It's a business, a branch not only of Israel,
but also of the European arms industry.
Ja, we hoorden het net.
Die Spionage-software is eigenlijk een Europese uitvinding, vertel.
Het is ontwikkeld in Europa.
Het is ook verkocht vanuit Europa.
Wat doet zo'n Spionage-software?
Dat wordt ook gebruikt voor legitime doelijnen.
In Europa gebruiken veiligheidsdiensten dat bijvoorbeeld zo'n spy werd,
daarom niet precies pruiter,
maar die gebruiken dat om de communicatie van drugsbarron en mafiabasis
en terroristen zwaar crimineelen kort om,
om dat allemaal op te kunnen volgen.
Maar om te voorkomen dat die software in verkeerde handen terechtkomt,
dus en bij dubieus regimes, heeft de EU de verkoper van welstrikt gereglementeerd.
Dus dat dat ook zo vroepant is aan ons onderzoek,
de pruiterfiles die software is ontwikkeld in Europa,
ook de financiers en verkopers werken vanuit de EU.
En ondanks die reglementering rond de verkoop,
is dat toch ja, wereldwijd verspreid geraakt.
Hoe dan?
Eén van de bedrijven die we onderzochten, die het NEXA,
dat is een Fransbedrijf,
dat ook heel veel leverd aan de Franse staat,
die goed genetwerkd zijn in Frankrijk

en dat al toppers binnen NEXA blijken,
bijvoorbeeld over het telefoonnummer van president Emmanuel Macron,
te beschikken.
Ze zijn niet alleen leverd als hier zijn Franse staat,
maar wat ze ook doen,
is via een zusterbedrijf in de verenigde Arabische Emiraten,
leveren een heel aantal andere landen.
En wat je ziet, is dat afhankelijk van het land,
waar predator bijvoorbeeld moeten recht komen,
dat ze vaak liever opteren
om hun vestiging een zusterbedrijf in de Emiraten te gebruiken,
om wel even omdat ze in de Emiraten
nu eenmaal minder export beperkingen zijn,
de Emiraten die doen veel minder lastig dan de Europese Unie,
over wat je wel en niet kan uitvoeren.
Dus die vestiging in de Emiraten biedt een achterpoortje
en op die manier zie je dat Europese bedrijven,
in dit geval gevestigd in Frankrijk,
via dit achterpoortje,
plots toegeven tot een hele wereldmarkt.
En die gaat van, ik zeg maar,
wat Vietnam tot Egypte,
waar ook een dictator aan de macht is,
of Libye waarom Wapen en Bargo heerst.
Wie zit er achter dat bedrijf, achter die NEXA?
Eén van de belangrijkste figuren daar is de zikresteef van Salius.
Hij is medeoprichter van NEXA
en werkte ook mee aan het bondgenoodschap IntelXA.
Hij had dan die preutersoftwerter eens begonnen verspijden.
Hij is een 59-jarige man,
die fysica heeft gestudeerd in Parijs en Silicon Valley,
maar eigenlijk draait hij al jaren mee
in de sector van de espionagetechnologie.
Hij was manager bij een voorlopper van NEXA.
Dat heette Amazis voor de Feyenproevers.
En dat bedrijf wagen zich in 2007
alle aan een zeer riscante deel,
namelijk een verkoop aan het regime van de Libese dictator,
Mohamad Gaddafi.
Die verkoop legte vier jaar later in 2011 uit
en dan is er ook een onderzoek opgestart
door het Franse gerecht naar die verkoop.
En dat onderzoek draait zelfs

rond medeplichtigheid aan voltering.
Dus de verdenkmaking draait daar rond.
Omdat dan de zaakvoers van dat bedrijf
tegen het onder de voeten werd,
erachtte ze een nieuw bedrijf op
waar ze wel diezelfde software,
diezelfde espionage software,
verder begon te verkopen.
En in de jaren, dus ja,
in de jaren 2010 en daarna
breiden ze ook een arsenal uit.
Dat leverde die groep miljoenen op.
Opvallend is ook,
dus in de hondere documenten die we hebben kunnen bestuderen,
zit ook een handgeschreven notitie
van een soort teambuilding-sessie
bij dat espionagebedrijf NEXA
een handgeschreven notitie van die saliës.
En daarin schrijft hij letterlijk zelf
dat zijn drijf weer is rijk worden
om tussen aandachtstekens op een grote boot te zeilen.
Dus geld was zijn drijf weer
en de verkoop van die zeer omstreede producten
heeft hem dus ook echt wel veel geld opgebracht
toen hij tijdelijk door de politie werd verhoord,
heeft hij daar verklaren
dat hij €50.000 per maand verdiende,
dat hij met een Porsche Macan en Mercedes GT reed
toch enorme luxevoertuigen.
Hij pocht ook met een huis van €4 miljoen
in de buurt van Parijs,
een villa in Dubai van €1,5 miljoen.
Dus het heeft hem zeker geen windtijden gelegd
die dubbeuse handel.
Hoe zijn jullie dat allemaal te weten gekomen, Roland?
Wel, we maken deel uit van een Europees onderzoeksnetwerk.
Daar hebben we eerder al projecten mee ten huidvoer gebracht.
Het ging zowel over Congo en de kleptocratie
die daar heerstende links naar België
als over rivierspionnen die mensen in Europa
zwart maken of het levenzeur maakt
en inclusief een aantal België.
En wat we vaak doen is, als er een grote ciris is,

dan gaan we dat samen uitspitten met de collega's van dat netwerk.
In dit geval hebben media partners en de Spiegel
onze partners een aantal vertrouwlijke documenten in handen gekregen
en die gedeeld met een heel aantal andere partners,
ook een aantal media van buiten het netwerk,
die bewerkte omdat zij zich bewond op een relevant plaats.
Israël, Griekenland, ik zeg maar wat.
En al die partners van het netwerk,
die zijn samen door de documenten gegaan
en die zijn ook uit de plekken gegaan als dat nodig was,
bijvoorbeeld bij het huis van de sommigen van de mensen die we onderzochten.
En ja, we hebben ook geprobeerd om al die mensen te bereiken.
Dus samen zijn we eigenlijk tot uiteindelijk de conclusie gekomen
dat er inderdaad vanuit Europa,
ondanks de geweldige Europese regulering op papier,
Jaaspionagebedrijven, werkzaamzijden
die een spyware uitvoeren naar de hele wereld.
Straks vragen we ons af wat Europa kan doen
om te vermijden dat die software naar opskure regimes gaat,
maar eerst gaan we er even uit voor reclame.
Stop, wie zit er nog met vragen?
Vragen als elektrisch laden, hoe doe ik dat invoudig?
Slim, voordelig.
Ontdek al onze laatere plossingen opmaat,
want bij Angie willen we dat iedereen mee is.
Angie, al onze energie gaat met jou.
Nicolas en Roland, terug naar jullie.
We hadden het over dat Franse bedrijf Nexa en die topman Salies,
maar hij doet het niet alleen.
Klopt.
De Franse waren nooit zover geraakt,
zonder hulp van een israelische partner
die een heel belangrijke rol heeft gespeeld,
omdat hij hen geholpen heeft aan predator te raken,
dus de beruchte spyware,
waarover een groot deel van het verhaal gaat.
De man in kwestie, die heet Tel Dilyan.
Tel Dilyan is een fascinerend figuur,
een ex Farakomando,
die ook heel lang de bevelen hebben geweest van 1heid 81.
1heid 81 is een beetje van een enigmatische enheid
van het israelische leger.
Je kan die eigenlijk beschouwen als de speelgoedwerkplaats

van israelische spionnen,
waar alle high-tech verwaardigd wordt
voor inlichtingendiensten,
maar ook om op het terrein gebruikt te worden
door de soldaten van één van de meest gavanceerde legerste wereld.
En Dilyan, na zijn vertrek uit het leger,
heeft hij eigenlijk een tweede leven opgebouwd
als spyware-entrepreneur.
Een van de dingen die hij deed is eigenlijk de makers van Pegasus,
een ander beruchte spyware,
die ook uit israel kwamen naar de kroonsteken
door zelf zijn eigen toelsten te gaan ontwikkelen.
En door de kracht te buddelen met de Fransen,
kon hun alliantie,
een Europees, grote Europees spyware-bondgenotenschap
plots allemaal producten aanbieden
die ze daarvoor niet konden aanbieden.
En bovendien, leuk voor Dilyan,
hadden de Fransen een enorm adresboekje
dankzij jaren na een ervaring in Afrika,
met een oostenbevoerbeeld.
Dus plots konden ze die producten ook aan de man brengen
op plaatsen waar Dilyan voor dien geen toegen had.
Je zegt dat Roulant
concurrentie met die Pegasus, die andere
speionage-software,
is dit dan een beter product,
die Predator of niet?
Wel, in de eerste versie was Predator geen beter product,
in zekere zin, want de heilige graal
in de hacking-software heet Zero Click.
En in Zero Click's systeem,
dat is een systeem dat jouw telefoon kan infecteren
zonder dat je op een link hoeft te klikken.
Vaak, en dat hebben we ook gezien
in aantal van de mensen die we beschrijven in onze stukken,
die krijgen een link toegestuurd,
dan klikken ze erop, dan krijgt een telefoon geïnfecteerd
en dan kan die leeggezo geworden door de hackers.
Dat is een oude versie, die ook door Predator ingezet werd.
Maar wat Dilyan eigenlijk wilde, is een Zero Click systeem.
Je telefoon kan gewoon in je zak blijven
en toch kunnen we je telefoon leeghalen zonder dat jij iets hoeft te doen.

En een van de dingen waar Dilyan in geslaagd is,
dankzij zijn alliantie met de Franse,
is om ook dat Zero Click systeem eigenlijk in te brengen in Predator.
En op die manier heeft er van Predator
één van de meest moderne hacking-toels gemaakt,
die helemaal mee is met de wereldwijde spionagemarkt.
Ja, hoe deed is dat dan?
Met een hacking-busje.
Oké, dat klinkt IT-machtig.
Ja, dat klinkt ook vooral gewoon zoals het is, namelijk.
Dat is een zwart busje dat volgestuid zit met hacking-apparatuur eigenlijk.
De bedoeling daarvan is om telefoons
binnen een bepaalde straal van 500 meter tot een kilometer
van de sterkte van de golven die het kan uitzenden
om dit te besmetten met de Predator Spyware.
Dus vanuit dat busje worden dan radio-golven uitgestuurd.
Het ene programma heet Spearhead.
Dat gebeurt dan via wifi-golven
zoals onze telefoonverbinding zou maken met een wifi-netwerk.
Daar komt dan die Spearhead tussen gefietst
om ons zo te besmetten met de Predator Spyware.
Een andere mogelijkheid is misbrek maken van het GSM-netwerk.
Dat programma heet dan AlphaMax.
Dat werkt via een antenne die de master van mobiele operatoren eigenlijk imiteert.
En wanneer dan een doelwit in de buurt is,
wordt het, zoals dat dan in de brochure beschreven staat van Intellexa,
wordt dat doelwit discreet losgemaakt van het netwerk.
En dan worden alle vormen van communicatie opgenomen en bewaard
en wordt het doelwit gelokaliseerd.
Dus er eigenlijk misbreuk te maken van de wifi-signalen
of het GSM-signal worden die toestellen besmet.
Kost 9 miljoen euro voor wie je geïnteresseerd zou zijn.
Dat is niet te weinig geld natuurlijk,
maar het is wel een zeer gevaarlijke hacking-toel.
Naast de hacking-bushen,
niet iedereen heeft meteen 9 miljoen vuil voor een hacking-bushen,
maar het houdt ook wel een aantal andere oplossingen,
namelijk ook hacking-software die verstopt dat in een rugzak
of heidingapparatuur die kon verbonden worden aan een drone.
Ook op die manier kan je dichtbij een doelwit raken.
Iets handiger.
Ja, materiaal voor alle terreinen.
Het magazine Forbes kreeg een paar maanden geleden

de Israëleertal de leeren zover om zijn espionagebusje
te demonstreren, we luisteren even mee.
We zetten twee mensen uit de van.
We zetten ze, intercepteren ze, infecteren ze.
By exploiting weaknesses in de Android-device
held by de collega's,
we moeten silenlijk installeren een stuk van software
die betere private WhatsApp-messages kunnen sipheren.
Ja, die man maakt reclame voor zijn espionage-software.
U sprak daar net, Nicolas, ook van brochures die ze uitgeven.
Hebben die echt brochures van hun katalentussen?
Zoze zaken worden ook via beursen aan de mannen gebracht, bijvoorbeeld.
Dat is zoals zij beuren hebben op mobielhomes of visserijproducten.
Oké, oké.
Hoe je zei daar net, die Predator-software is in principe niet illegaal,
is dit ook niet illegaal of is dat zo zwart als het maar kan zijn?
Dat hangt eigenlijk ook van de rechtstaat en aanwezig zijn van de rechtstaat waar het wordt toegepast.
In België, in Europa, in andere westerse landen,
gebruiken veiligheidsdiensten dit soort zeer intrusieve software
om toegang te krijgen tot de communicatie van topcriminele.
Dat is een feit.
De Belgische politie, via onze informatie, is bevestigd geraakt
dat die boven het Pegasus gebruiken of gebruiken.
Alles hangt dus af van de context.
Als zo'n apparatuur dan gaat naar Egypte, waar de rechtstaat
heel wat minder voorstelt dan in West-Europa,
dan kom je meteen in een Gelander verhaal terecht
en dan is de vraag, is dat wel correct dat daar wordt gebruikt?
Ja, inderdaad.
En om nog maar eens aan te tonen met welke jongens we hier te maken,
hebben we het bedrijf wilde zelfs verkopen aan Libië.
Klopt.
En meer bepaald aan Veld Marschalk, of zo noemt hij zichzelf toch,
gelief van Haftar, die regeert met zijn troepen over het oosten van Libië.
Hij heeft bijvoorbeeld de Benghazi in handen.
En hij wordt beschuldigd door NGWs, bijvoorbeeld.
Er waren ook onderzoeken naar hem van mensenrechte schendingen.
En hij opereert ook in een land waar sinds 2011
een internationaal wapen en bargo tegen Van Kracht is,
afgekondigd door de Zee- en veiligheidsraad.
Dus dat is op het hoogste niveau afgesproken.
In principe leveren je geen wapens aan iemand als Marschalk Haftar.

En vanuit de meeste Europese landen zou het ook extreem moeilijk zijn
om wapens te leveren aan Marschalk Haftar.
Dat valt gewoon onder exportbeperking.
Blijkt dat de mensen die wij onderzochten hebben dan toch toestaat geweest?
Ja, maar ze zijn wel tegen de lamp gelopen.
Er lopen nog onderzoeken tegen die mensen waarbij de verkoper zijn
uitvinders van die spy weer overigens zelf afgeluisterd door het Franse gerecht.
En in die gesprekken blijkt ook dat ze zichzelf best wel beust waren
over wat ze deden.
Bijvoorbeeld naar Libië wordt verwezen als door Stéphane Salies,
die een van de hoofdhaandeelhouders is van de bedrijven die wij onderzochten
en een van de bedrijven de krachten achter de hele operatie.
Wel die verweest naar Libië als een heel slecht land.
Hij was dus wel degelijk bewust van het feit dat Libië niet zomaar staat
als een Zwitserland of Oosterrijk.
Ja, dan moeten we het natuurlijk nog hebben over de vraag
hoe kan dit allemaal,
dat die Europese software naar het buitenland verscheept wordt.
Ja, Roeland heeft het daar straks al kort vermeld.
Er was een zusterbedrijf van het Franse espionagebedrijf
gevestigd in Dubai, Amis heette dat.
Voormiddels stond dat los van de Franse bedrijf,
maar had dat eigenlijk wel zowel dezelfde aandeelhouders als bewinslui.
Onthoud dat even, want dat is een belangrijke factor in heel het verhaal.
Vanuit de EU is het in theorie niet mogelijk
om zo'n espionage software naar Egypte of Vietnam of Anderlande te exporteren.
Dat is omdat die software valt onderzocht,
gegeten Dual-U's-goedrum.
En dat zijn eigenlijk productentechnologie of materialen
die wel voor burgerlijke als militaire doeleinden kunnen worden gebruikt.
Dat valt ook onder de was naar overeenkomst, heet-ie.
Maar elk land hanteert eigen criteria,
waardoor heel die overeenkomst een slag in het water is.
Dat is ook al met zoveel woorden gezegd eigenlijk door de VN.
Die noemen het een controlemechanisme en dat niet werkt.
In werkelijkheid is het praktisch onbestaand.
Nu is er binnen de Europese Unie wel al jarenlang
een poging bezig om die gaten toch te dichten.
Er is ook een stijlregels daarvoor gekomen in 2021.
En daar staat specifiek dat landen zelf kunnen beslissen
dat er een uitvoervergunning nodig is voor surveillance-systemen.
Bijvoorbeeld als er twijfel is, valt het onder Dual-U's of niet,
dan kan een land als Frankrijk.

Maar niet te zeggen zelf wel bepalen van
ja, maar dit gaan we toch even in de gaten houden
en zien we hier geen aparte vergunning voor nodig is.
Fabrikanten moeten ook spontaan een vergunning aanvragen
als ze zelf denken dat hun product kan leiden tot de schending van de mensenrechten.
Opnieuw, op papier klinkt dat zeer goed,
maar experts die zeggen, ja, dat gaat alleen maar werken als alle lidstaten
het eens zijn over wat er Dual-U's is en wat niet
en wat er moet worden beperkt en wat niet.
En ja, het is al lang een probleem binnen de Europese Unie,
maar als het gaat over samenwerking rond veiligheid,
zowel intern als extern, is er vaak een gespeide slag hoorde
en dat is hier opnieuw het geval.
Er ontstaat veel speelruimte
en dat verklaren we voor het warme land als Griekenland.
Hij heeft toch al een tijdje een lid van de Europese Unie.
Waarom zij toch groenlicht gaven voor de export aan landen als Madagaskar en Soudam?
In het geval van Frankrijk,
waar een aantal van die spyware-producten gefabriceerd werden
of in ieder geval verkocht werden,
ook daar heeft de staat er eigenlijk wel belangrijk
dat er een stevige spyware-industrie is in Europa
want wij concurreren in de ogen van grote Europese overheden
met de VS, met Israël, met China, met Rusland
en zelf wil al die regeringen ook toegang tot goede spyware.
In dat geval is het altijd meer opportun
toch gezien van het gelijkwelke Europese regering
om daar zelf controle over te hebben
over hoe die vervaardigd wordt, wie die vervaardigd heeft
om dus eigenlijk gewoon een spyware-industrie
eigen achtertuin te hebben.
Die spyware-industrie kan dan dienen
om de geopolitieke belangen van jouw land veilig te stellen,
kan ook dienen om pedophile en criminele
allerhande drugstielers en z'n woord op te pakken
en dat zal altijd afgewogen worden
de facto tegen de verstrenging van regelgeving
rond die spyware, tegen het beschermen van burgerlijke vrijheden.
Dus regeringen zitten daar altijd wat geprankt
en ja, zolang heel veel achter de schermen gebeurt
zijn er best ook wel incentives voor die regeringen
om toch het spyware-industrie in Europa
een beetje te laten begaan

om al die Europese regels misschien niet zo nou te nemen
als ze op papier zouden moeten genomen worden.
Ja, bijzondere tegenstelling.
Tot slot, dit zijn dingen die vooral achter de schermen gebeuren
waar we weinig van weten.
Het is wel interessant dat we dit bloot leggen.
Ja, dat vinden wij.
Het is denk ik wel belangrijk om inzicht te geven
in hoe die wereld werkt van de spionage software
omdat in autoriteite regimes zijn dit zeer belangrijke wapens
dat ze zo gerecht iemand's leven over hoop kunnen halen.
En dat is net wat dictators willen
de dissidenten mondoot maken, bang maken, met dit soort spyware.
En het is ook syronisch
dat vanuit Europa, dat wordt verkocht
aan die autoriteite regimes
ook al lijkt Europa de veilige haven voor
voor vrijheden en mensenrechten
dat dan toch tussen de regels door wordt gefietst
omdat de verkopen is zeer pijnlijk
en dat moet gewoon uit de schade worden gehaald.
Ja, absoluut.
Goed, Nicolas van Hekken, noem aan te remoten.
Dank jullie wel.
Dank u.
Reageren kan via podcast adstandaard.be