https://www.dewereldmorgen.be/artikel/2021/12/01/digitale-surveillance-made-in-israel-vormt-mondiale-dreiging/

Analyse - soetkin

Digitale surveillance ‘made in Israël’ vormt mondiale dreiging

De afgelopen jaren zette Israël een breed digitaal systeem op om Palestijnen op de bezette Westelijke Jordaanoever permanent te kunnen surveilleren. Uit een onderzoek gebaseerd op getuigenissen van Israëlische ex-soldaten aan de NGO 'Breaking the Silence' blijkt dat het vergaande surveillancebeleid, geïnitieerd door het Israëlisch leger in 2016, gezichtsherkenning integreert in een voortdurend groeiend netwerk van camera's, sensoren en smartphones. Een belangrijk nieuw onderdeel van dit systeem is een gezichtsherkenningsapplicatie, genaamd 'Blue Wolf'.

woensdag 1 december 2021

Elke Palestijn vormt doelwit

Blue Wolf vergelijkt de gezichten van Palestijnen met een uitgebreide foto-databank. Het programma hanteert een kleurcode om aan te duiden of een individu tegengehouden, gearresteerd of met rust gelaten moet worden.

De Blue Wolf-databank is de minder omstandige versie van de zeer uitgebreide ‘Wolf Pack’-databank die profielen bevat van vrijwel elke Palestijn op de Westelijke Jordaanoever, inclusief foto, familiegeschiedenis, opleiding en een veiligheidsclassificatie voor elke persoon. Maar terwijl Wolf Pack alleen toegankelijk is via beveiligde desktopcomputers, is Blue Wolf een gebruiksvriendelijke smartphone-applicatie.

De databank van Blue Wolf wordt samengesteld door Israëlische soldaten gestationeerd in de bezette gebieden die de opdracht krijgen om met gsm’s zoveel mogelijk foto’s te trekken van willekeurige Palestijnen, inclusief kinderen en ouderen – vaak zonder hun toestemming. Er werd vorig jaar zelfs een wedstrijd ingelast, waarbij de militaire eenheden die de meeste foto’s verzamelden prijzen konden winnen, zoals een dagje verlof.

In Hebron, een stad in het zuiden van de Westelijke Jordaanoever waar ook een fanatieke kleine enclave joodse kolonisten woont, installeerde Israël aan de checkpoints camera’s die gezichten scannen zodat Palestijnen geïdentificeerd kunnen worden nog voor ze een identiteitsbewijs voorleggen.

Daarnaast houdt een uitgebreid en gesloten cameranetwerk, genaamd ‘Hebron Smart City’, de Palestijnse bewoners van de oude stad permanent en in realtime in de gaten. Volgens de ex-soldaten die spraken met Breaking The Silence kunnen sommige camera’s zelfs in de huizen van particulieren kijken.

Gezichtsherkenning

In 2019 investeerde Microsoft in 'AnyVision', een Israëlische start-up die samen met het Israëlisch leger (IDF) werkte aan de uitbouw van een smart camera-netwerk dat gebruik maakt van gezichtsherkenningstechnologie. In hetzelfde jaar introduceerde het IDF gezichtsherkenningstechnologie (ontwikkeld door AnyVision) aan de grote checkpoints tussen Israël en de Westelijke Jordaanoever.

Het gebruik van gezichtsherkenningstechnologie is zeer controversieel. Discussies over en bezwaren tegen digitale gezichtsherkenning focussen voornamelijk op privacy-kwesties, maar de bestaande systemen zouden ook een zeer uiteenlopende graad van nauwkeurigheid vertonen. Gevallen van verkeerde identificatie kunnen uiteraard ernstige gevolgen hebben.

Terwijl het debat rond digitale surveillance in verschillende delen van de wereld volop woedt, wordt deze technologie in sommige landen reeds in alle stilte ingezet.

In een heel aantal Amerikaanse steden is het gebruik ervan preventief verboden, maar een studie van de 'Government Accountability Office' in de Verenigde Staten stelde vast dat 20 federale agentschappen reeds gebruik maken van digitale gezichtsherkenningsprogramma's.

Het Europees Parlement keurde vorige maand nog een resolutie goed die de inzet van artificiële intelligentie -waaronder digitale gezichtsherkenning- door politie en justitie, verbiedt.

Ook binnen Israël stuitte een recent voorstel van wetshandhavers om gezichtsherkenningscamera's te installeren in openbare ruimtes, op aanzienlijke tegenstand. De overheidsinstantie die verantwoordelijk is voor de bescherming van de privacy kantte er zich eenduidig tegen. In de bezette gebieden, waar rechten irrelevant blijken, hanteert Israël echter andere normen.

Het gebruik van gezichtsherkenningstechnologie is duidelijk een zoveelste wapen van de bezetting, een instrument ter onderdrukking van het Palestijnse volk.

'Geen commentaar'

Volgens de digitale burgerrechtenorganisatie 'AccessNow' is Israëls gebruik van digitale surveillance en gezichtsherkenning het meest uitgebreid van alle landen die dergelijke technologieën inzetten om een bevolking te controleren. Men kan spreken van een totale schending van de privacy van een heel volk.

Naast Blue Wolf, lanceerde Israël nog een andere smartphone-applicatie, genaamd 'White Wolf', die speciaal ontwikkeld werd voor de joodse kolonisten op de Westelijke Jordaanoever. Hoewel de bewoners van deze internationaalrechtelijk illegale nederzettingen zelf geen Palestijnen mogen vasthouden, kunnen 'veiligheidsvrijwilligers' de White Wolf-app gebruiken om de identiteitskaarten te scannen van Palestijnen die de nederzettingen betreden om er te werken (voornamelijk in de bouw).

De technologie stelt kolonisten in staat om persoonsgegevens te controleren aan de hand van een databank van de IDF, de Israëlische inlichtingendienst en de veiligheidsdepartementen van de nederzettingen

Het Israëlisch leger schildert zijn uitgebreide surveillancenetwerk in de bezette gebieden in een statement af als "routine veiligheidsoperaties" die deel uitmaken van "de strijd tegen terrorisme en de inspanningen om de levenskwaliteit van de Palestijnse bevolking in Judea en Samaria te bevorderen". (Judea en Samaria is de officiële Israëlische benaming voor de Westelijke Jordaanoever.) Het statement vervolgt: "We kunnen uiteraard geen commentaar geven op de operationele capaciteiten van de IDF".

Toch werd het bestaan van zowel de Blue Wolf-technologie, het Hebron Smart City-programma als de White Wolf-app officieus erkend door het Israëlisch leger (respectievelijk in een online brochure, een artikel op de IDF-website en een interview met een legerchef in een rechts blad).

NSO

Israël hanteert niet alleen zelf een technologisch hoogstaand digitaal surveillancebeleid, het staat mondiaal ook op het voorfront wat de ontwikkeling van digitale defensie- en surveillancetechnologie betreft.

Vorig jaar kwam het spywareprogramma 'Pegasus', ontwikkeld door het Israëlische tech-bedrijf 'NSO Group', nog uitgebreid in het nieuws toen onderzoek uitwees dat het heimelijk en vanop afstand geïnstalleerd werd op de mobiele telefoons van honderden activisten, journalisten, politieke dissidenten, advocaten, enz. door de veiligheidsdiensten van een resem landen met autoritaire regimes, waaronder Saoedi-Arabië, Marokko en de Verenigde Arabische Emiraten.

De spyware (die toegang geeft tot tekstberichten, camera, microfoon, paswoorden en geo-locatie) werd door NSO verkocht (alleen aan regeringen en mits goedkeuring van het Israëlisch Ministerie van Defensie) als "technologie om terreur en zware misdaad te voorkomen en te onderzoeken". Pegasus werd echter systematisch en al vele jaren misbruikt om op grote schaal mensenrechtenschendingen te faciliteren over heel de wereld.

VS-president Biden zette NSO op 3 november op de 'Entity List' -een lijst met buitenlandse personen, entiteiten of regeringen waarvoor handelsrestricties gelden- wegens het opereren "in strijd met de belangen van de VS op het gebied van de nationale veiligheid of het buitenlands beleid". De verkoop van hardware, software en diensten aan het

bedrijf vanuit de VS is nu feitelijk verboden. Dat belemmert NSO op zich niet enorm, maar het is zeker een symbolisch signaal.

Vorige week spande Apple bovendien een rechtszaak aan tegen NSO in een poging om de verspreiding van door de Israëlische staat gesponsorde spyware in te dammen. Pegasus slaagde er namelijk in om ook de doorgaans veilig geachte mobiele telefoons van Apple te hacken.

Zelfs als NSO onder druk van de controverse en rechtszaken failliet zou gaan, zal noch Pegasus noch de ontwikkeling van gelijkaardige technologieën plots verdwijnen.

Aanval op Palestijnse activisten

Uit een pas uitgekomen onderzoek van de Ierse mensenrechtenorganisatie 'Front Line Defenders' (FLD) blijkt dat de mobiele telefoons van zes Palestijnse activisten gehackt werden met de gesofistikeerde Pegasus-spyware van de NSO Group.

Een aantal van de geviseerde mensenrechtenverdedigers werken voor organisaties die eerder dit jaar al onterecht door Israël op de lijst van terroristische groepen werden gezet – een frontale aanval op de Palestijnse mensenrechtenbeweging. Mensenrechtenexperts bij de Verenigde Naties hebben het over "misbruik van de antiterrorismewetgeving door de Israëlische autoriteiten".

De geviseerde organisaties documenteren beschuldigingen van mensenrechtenschendingen door Israël en de Palestijnse Autoriteit. Het gaat om 'Al-Haq', 'Addameer', 'Defense for Children Palestine', het 'Bisan Center', de 'Union of Palestinian Women's Committees' en de 'Union of Agricultural Work Committees'.

Drie van de zes activisten die gehackt werden met Pegasus waren bereid uit de anonimiteit te treden. Salah Hammouri is een Palestijns-Franse rechtenverdediger en advocaat wiens verblijfsstatus in Jeruzalem werd ingetrokken, Ubai Al-Aboudi is de Palestijns-Amerikaanse uitvoerende directeur van het Bisan Center, en Ghassan Halaika is een onderzoeker voor Al-Haq.

Volgens 'The Citizen Lab', een onderzoekscentrum rond cybersurveillance en mensenrechten verbonden aan de Universiteit van Toronto, werden de activisten gehackt (soms lang) voor hun organisaties op de terroristenlijst werden gezet.

Aangezien Pegasus de volledige controle verschaft over de toestellen van de geviseerde individuen, kan volgens The Citizen Lab niet uitgesloten worden dat er vals belastend materiaal op geplaatst wordt door overheidsoperatoren.

Volgens de New York Times ontkennen de Israëlische autoriteiten dat Pegasus gebruikt werd om de gsm's van Palestijnen te hacken. Een woordvoerder van de NSO Group gaf de inmiddels de standaardverklaring van het bedrijf: "Vanwege contractuele en nationale veiligheidsoverwegingen kunnen we de identiteit van onze overheidsklanten niet bevestigen of ontkennen. Zoals we in het verleden al aangaven, bedient NSO Groep de producten niet zelf; het bedrijf geeft [door de Israëlische regering] goedgekeurde overheidsinstanties een licentie en we zijn niet op de hoogte van de details van personen die worden gecontroleerd".

Is misbruik de regel?

Een woordvoerder van Candiru, een andere Israëlische producent van spyware, reageerde gelijkaardig nadat de nieuwswebsite 'Middle Eastern Eye' (MEE) onlangs ontdekte -samen met andere nieuwssites- het slachtoffer geweest te zijn van een cyberaanval die hoogstwaarschijnlijk gelinkt is aan de technologie van dat bedrijf.

"Het product van het bedrijf is bedoeld om wetshandhavingsinstanties te helpen terrorisme en misdaad te bestrijden… Het bedrijf verkoopt zijn producten alleen aan overheidsinstanties, na het ontvangen van alle benodigde vergunningen van het Israëlisch Ministerie van Defensie… Het bedrijf en zijn product hacken geen websites. De licentie en de wet verbieden het bedrijf of zijn werknemers om het product voor de klant te bedienen, of om te worden blootgesteld aan wie het doelwit ook is."

De voorbeelden van NSO en Candiru tonen aan dat Israëlische digitale surveillancetechnologieën, waaronder gezichtserkenning en spyware, een transnationale impact hebben en een wereldwijde dreiging vormen.

Er is in ieder geval een totaal gebrek aan internationale regulering van digitale surveillancetechnologieën. Het tempo van de technologische innovaties maakt regulering op gelijk welk niveau bovendien heel moeilijk. Misbruik, dat streng gesanctioneerd zou moeten worden, blijft ondertussen moeilijk op te sporen. En neigt misbruik in de wereld van cyber-surveillance niet eerder de regel dan de uitzondering te zijn?

Terwijl over de hele wereld verontwaardigde reacties te horen waren na de onthullingen over Pegasus en Candiru, lijken heel wat overheden al te dromen over de mogelijke 'nuttige' manieren waarop zij innovatieve digitale surveillancetechnologieën zouden kunnen inzetten. En dat geldt zeker niet alleen voor landen met autoritaire regimes. Denk maar aan de manier waarop digitale surveillance belangrijker wordt bij de pushback van vluchtelingen en migranten aan de buitengrenzen van de Europese Unie.

Dit artikel verscheen eerder op www.vrede.be