Europa is verbaasd dat zijn spyware door dictators wordt misbruikt

Nikolas Vanhecke Roeland Termotein samenwerking met EIC

De EU heeft regels voor de uitvoer van Europese spionage-software, maar slaagt er niet in die te laten naleven. Daardoor gaat spyware naar autoritaire regimes als Egypte en Vietnam.

Het is pijnlijk ironisch: de Europese Unie, die al jaren timmert aan regels om te voorkomen dat spionagesoftware in verkeerde handen terechtkomt, is uitgegroeid tot een paradijs voor bedrijven die dergelijke software ontwikkelen.

‘Landen als Nederland, Frankrijk, Ierland, Luxemburg, Cyprus en Bulgarije helpen andere landen om mensen te bespioneren’, zegt Europarlementslid Sophie in ’t Veld (Renew). ‘Ze bieden niet alleen een thuis aan de ontketende surveillance-industrie, maar ondersteunen die ook via financiële systemen en belastingvoordelen. Europa is daaraan medeplichtig.’ Een van de spionage-allianties die floreren in de EU heet Intellexa. Het is een bondgenootschap van Franse en Israëlische ondernemingen, met als bekendste product de beruchte Predator-spyware. Wie Predator loslaat op de smartphone van een doelwit, kan diens digitale doen en laten volgen.

Op basis van vertrouwelijke data die Mediapart en Der Spiegel verkregen en deelden met de European Investigative Collaborations (EIC), laten De Standaard en zijn internationale partners zien hoe Predator werd verkocht aan autoritaire regimes als Egypte en Vietnam, zonder dat Europese regels dat konden verhinderen. Binnen Intellexa is het Franse bedrijf Nexa een belangrijke poot. Dat kon jarenlang surveillance-systemen aan de man brengen bij dictators over de hele wereld, zelfs al liepen er in Frankrijk twee gerechtelijke onderzoeken tegen het bedrijf. De Franse speurders verdachten het van medeplichtigheid aan foltering.

Praktisch geen controle

De deals die de leden van de Intellexa-alliantie sloten met autoritaire regimes, tonen hoe de EU geen grip krijgt op de uitvoer van spionagesoftware. Dat ligt niet aan een gebrek aan regels rond de verkoop van software als Predator. Zo valt spionagesoftware sinds 2013 onder de Wassenaar-overeenkomst, die de export van ‘dual-usegoederen’ aan banden moet leggen. Dat zijn producten, technologieën of materialen die zowel voor burgerlijke als militaire doeleinden kunnen worden gebruikt.

Tweeënveertig landen, waaronder de VS, Rusland en EU-landen (maar níét EU-lidstaat Cyprus) ondertekenden de overeenkomst. China en Israël doen niet mee. Volgens Wassenaar moet elke uitvoerder van dual-usegoederen daarvoor de toestemming vragen aan de eigen nationale overheid. Maar doordat elk land daarover eigen criteria hanteert, is dat een slag in het water. ‘Het

is duidelijk dat deze overeenkomst misbruiken niet tegengaat', zegt Katia Roux, beleidsmedewerker bij Amnesty International, dat meewerkt aan de Predator Files. Ook van de VN kreeg Wassenaar een onvoldoende: 'Het is een understatement om te zeggen dat dit controlemechanisme niet werkt. In werkelijkheid is het praktisch onbestaand.' Europa probeerde in 2021 zelf de gaten te dichten met regels waar jarenlang over onderhandeld is. Daarin staat dat landen zelf kunnen beslissen of er een uitvoervergunning nodig is voor surveillance-systemen, bijvoorbeeld als er twijfel is of ze onder dual-useregels vallen. Fabrikanten moeten ook spontaan een vergunning aanvragen als ze denken dat hun product kan leiden tot een schending van de mensenrechten. Als een lidstaat die vergunning weigert, moeten de andere landen daarvan op de hoogte gebracht worden. Op papier klinkt dat goed. Maar: 'In de praktijk zijn geharmoniseerde controles alleen van toepassing als alle staten het eens zijn. De lidstaten hebben dus veel speelruimte als het om de implementatie gaat', zegt Lena Riecke, die aan de universiteit van Leiden onderzoek doet naar dit onderwerp. Die speelruimte verklaart waarom Griekenland groen licht gaf voor de export van Predator aan Madagaskar en Soedan.

Lobby's aan het werk

Ook van de beloofde Europese transparantie over het aantal exportvergunningen is weinig in huis gekomen. Een eerste overzicht dat in september vorig jaar verscheen, bleef hangen in algemene statistieken en sloeg op het jaar 2020. In een branche die technologisch constant evolueert en waarin bedrijven komen en gaan, zijn data van achttien maanden oud amper relevant.

De oorspronkelijke regels die de Europese Commissie had voorgesteld, waren nochtans streng. Ook het Europees Parlement was voorstander van een strikte regulering. Waar is het dan verkeerd gelopen? 'De regels zijn opgeofferd aan de belangen van de lobby's', zegt de Duitser Klaus Buchner, die als voormalig Europarlementslid betrokken was bij de onderhandelingen. Het tegenwerk was afkomstig van de lobbygroep DigitalEurope, die de technologiesector verenigt. Ook lidstaten als Frankrijk en Duitsland gingen op de rem staan. Zij vreesden dat er misbruik gemaakt zou worden van te gedetailleerde data over de exportlicenties, of dat dit het concurrentievermogen zou ondergraven. Nederland kantte zich ook uitdrukkelijk tegen het voorstel van het parlement, blijkt uit een document dat EIC verkreeg via de transparantie-ngo FragDenStaat.

'De regels worden ook niet toegepast omdat de overheden niet geïnteresseerd zijn', vindt Europarlementslid Sophie In 't Veld. 'Ze maken zich zorgen over terroristen, pedoseksuelen, georganiseerde misdaad: milieus die gebruikmaken van encryptie en berichten die zichzelf vernietigen. Veel landen kampen daardoor met een dilemma. Ze zeggen tegen spywarebedrijven: "We hebben dit of dat nodig." En de industrie zegt: "Oké, graag zelfs, maar in ruil vallen jullie ons niet lastig als we willen exporteren. Geen toezicht alstublieft." Het is een deal uit de hel, met wereldwijde gevolgen.'

Lees de volledige reeks op www.standaard.be/predator-files

Vrienden in het Elysée

De groep rond Nexa bespeelde handig de internationale regelgeving, maar had ook de beschikking over een indrukwekkend netwerk. In Frankrijk leverde het bedrijf surveillance-software aan de overheid én had het toegang tot de hoogste niveaus van de Franse politiek. In interne documenten van Nexa troffen we het telefoonnummer van de Franse president Emmanuel Macron aan, net als dat van zijn voormalige veiligheidsadviseur Alexandre Benalla. Die laatste werd internationaal bekend nadat hij op een 1 meimanifestatie in 2018, met een politiehelm op het hoofd, demonstranten mishandeld had.

Nadat hij het Elysée moest verlaten, onderhield Benalla nauwe contacten met een van de bestuurders van Nexa, Olivier Bohbot: tussen juni 2020 en juni 2021 wisselde hij 499 Whatsapp-berichten uit met de man. Daaruit komt naar voren dat hij optrad als liaison tussen het spionagebedrijf en Saoedi-Arabië. Zo stelt hij de Nexa-bestuurder voor aan ‘een prins’ die ‘zeer dicht staat bij MBS’, de Saoedische heerser Mohammed bin Salman. Stéphane Saliès en Bohbot, de drijvende krachten achter Nexa, zeggen in een reactie dat ze Benalla nooit betaald hebben, noch contracten aan hem te danken hebben. Tegelijk geven ze aan dat ze in hun transacties met ‘omstreden landen’ slechts ‘de weg van nauwe samenwerking volgden, die Frankrijk met diezelfde landen was ingeslagen’. (rte, vhn)

reactie Europese Commissie

‘Elke poging om illegaal toegang te krijgen tot data van burgers is onaanvaardbaar’

‘De uitvoering van de regulering is een complex proces, waarbij overleg met de relevante stakeholders komt kijken’, reageert de Europese Commissie. ‘De richtlijnen zijn ook zeer technisch, waardoor het proces nog complexer wordt.’

Een update van de regelgeving zal de transparantie verhogen, verzekert de Commissie. ‘Er zal specifieke aandacht zijn voor de publicatie van informatie over technologieën voor cybersurveillance, zowel op het niveau van de EU als van de lidstaten. Dat zal een beter begrip van de controlemechanismes mogelijk maken. Er zal ook meer samenwerking zijn tussen de lidstaten en de Commissie omtrent de vergunningen.’

‘Onze mening over de inzet van spyware in lidstaten is duidelijk: elke poging om illegaal toegang te krijgen tot data van burgers is onaanvaardbaar.’

De zaakvoerders van Nexa zeggen dat ze altijd de regels rond de uitvoer van hun spyware hebben gerespecteerd. (vhn, rte)

Lees ook