INTERNET Autocraten gebruiken steeds vaker onlinemiddelen om hun bevolking eronder te houden. Soms met hulp van ‘cyberhuurlingen’. ‘Het wordt bekender bij regimes dat ze dit soort dingen kunnen doen.’

tekst **Arjen van der Ziel** illustratie **Studio Vonq**

Dictators halen de **digitale teugels** *aan*

Mexico was in de zomer van 2016 in de rest van de wereld vooral in het nieuws vanwege de muur die de Amerikaanse presidentskandidaat Donald Trump langs de grens met de zuiderbuur van plan was te bouwen. Maar de Mexicaanse academicus en mensenrechtenactivist Santiago Aguirre had andere, urgentere zorgen. Want Aguirre deed onderzoek naar de mysterieuze verdwijning van 43 studenten in de stad Iguala twee jaar eerder. Zij waren waarschijnlijk vermoord en het werd steeds duidelijker dat uit Aguirre’s naspeuringen iets heel anders zou blijken dan uit het officiële regeringsonderzoek.

Desondanks was de Mexicaanse activist zich van geen onraad bewust toen hij op zijn telefoon een serie berichtjes ontving met internetlinkjes. ‘Help me alsjeblieft met mijn broer, de politie heeft hem meegenomen omdat hij leraar is’, luidde een van de berichtjes. Een andere: ‘Professor, ik stuit op een probleem. Ik stuur u mijn scriptie terug, gebaseerd op uw proefschrift, zodat u commentaar kunt geven.’ “Die berichten bevatten persoonlijke informatie”, vertelde Aguirre later aan het Israëlische dagblad *Haaretz*, dat zijn geval beschreef. “Informatie die het bericht voor mij interessant maakte, zodat ik erop zou klikken.”

Maar toen de activist inderdaad op de linkjes klikte, maakte hij, zonder het te weten, van zijn smartphone een zeer geavanceerd afluisterapparaat van de overheid. Op zijn telefoon was in het geniep Israëlische software geïnstalleerd, waardoor de autoriteiten in staat waren om zijn mobiel vrijwel onbeperkt te bespioneren.

Ze konden niet alleen de locatie van zijn telefoon volgen, ze konden ook zijn gesprekken afluisteren, geluiden in zijn omgeving opnemen, de camera aanzetten, zijn contacten bekijken, alle e-mails en berichtjes lezen, foto’s bekijken en zijn kalender overnemen.

Het geheimzinnige Israëlische bedrijf NSO Group had dit zogenoemde Trojan horse-systeem aan de Mexicanen geleverd, officieel om hen te helpen in hun strijd tegen drugsbaronnen. Maar computerexperts van het Canadese onderzoeksinstituut Citizen Lab, verbonden aan de Universiteit van Toronto, achterhaalden dat Mexico het systeem ook gebruikte om mensenrechtenactivisten en kritische journalisten te volgen.

“Zij zijn de ergste van de ergste”, aldus de Amerikaanse klokkenluider en oud-inlichtingenman Edward Snowden laatst tegenover Israëlische journalisten over NSO Group. “Ze zeggen dat ze levens redden, maar bewijzen laten zien dat ze juist levens kosten.”

De gang van zaken in Mexico is illustratief voor een wereldwijde ontwikkeling. Mensenrechtenorganisaties en pro-democratieactivisten constateren dat regeringen steeds vaker online-middelen inzetten om hun bevolking in de gaten te houden en zo nodig de mond te snoeren. Volgens de Amerikaanse denktank Freedom House, die het democratische gehalte van samenlevingen monitort, neemt de vrijheid op internet hierdoor de laatste jaren gestaag af. Freedom House inventariseerde voor zijn jaarlijkse rapport over internetvrijheid in 2018 de ontwikkelingen in 65 landen en constateerde in 27 daarvan een verslechtering. De grootste teruggang deed zich voor in Egypte, Sri Lanka, Cambodja, Kenia, Nigeria, de Filippijnen en Venezuela.

“Het wordt bekender bij autocratische regimes dat ze dit soort dingen kunnen doen”, zegt de Nederlandse cybersecurity-expert Ronald Prins. Hij werkte ooit bij de inlichtingendienst AIVD en leidde jarenlang het computerveiligheidsbedrijf Fox-IT, dat onder meer de AIVD en de militaire inlichtingendienst MIVD als klant heeft. “Vroeger luisterden regimes gewoon de telefoons van hun onderdanen af. Maar mensen gaan anders communiceren, dus gaan de machthebbers ze ook anders in de gaten houden.”

Techno-dystopie

China spant de kroon. Volgens Freedom House is het grote Aziatische land op weg een ‘techno-dystopie’ te worden. De autocratische president Xi Jinping heeft een soort digitale Chinese Muur opgetrokken, die ervoor moet zorgen dat burgers nauwelijks toegang hebben tot kritische buitenlandse media. En achter die muur intensiveert Xi de online-censuur. Geregeld worden mensen gearresteerd die – via digitale sluipwegen – toch proberen kritiek te spuien.

Zo vertelde een 47-jarige Chinese bouwvakker onlangs aan *The New York Times* hoe hij werd opgepakt nadat hij het had gewaagd om een spotprent en enkele berichten over mensenrechtenschendingen te posten op het in China geblokkeerde Twitter. Hij werd twintig uur verhoord en twee weken vastgehouden in een cel met tien anderen, waar propaganda-video’s werden vertoond. “We zijn als lammeren”, aldus de bouwvakker huilend in een telefoongesprek met de Amerikaanse krant. “Ze pakken ons een voor een. We kunnen niet terugvechten.”

China exporteert zijn repressieve model ook. De machthebbers in Peking hebben de afgelopen jaren voor regeringsfunctionarissen van tientallen landen wekenlange seminars georganiseerd over manieren om het web onder controle te houden. De deelnemers krijgen les over het monitoren en managen van de publieke opinie en het herkennen van online-bedreigingen van de openbare orde.

Maar ook zonder dit soort Chinese hulp worden autocratische regimes bedrevener in digitale repressie. Ze beroepen zich er daarbij vaak op dat hun maatregelen nodig zijn om verspreiding van ‘nepnieuws’ te voorkomen.

Zo heeft de Venezolaanse sterke man Nicolás Maduro de laatste tijd draconische maatregelen genomen om de vrijheid verder aan banden te leggen op internet, waar zijn burgers door de economische crisis toch al beperkt

‘Repressieve regeringen gebruiken het gevaar van nepnieuws vaak als excuus om de online-onderdrukking op te voeren’

toegang tot hebben. Sites van oppositiemedia zijn in het Zuid-Amerikaanse land geblokkeerd en kritische online-journalisten riskeren lange celstraffen.

Ook in Egypte heeft de president, generaal Abdel Fattah al-Sisi, de online-repressie verder opgevoerd. Egyptenaren kregen het afgelopen jaar lange celstraffen voor misdrijven zoals het delen van een satirisch online-bericht of het aankaarten van seksueel misbruik.

En in Rwanda kreeg blogger Joseph Nkusi tien jaar cel voor het verspreiden van geruchten en het aanzetten tot burgerlijke ongehoorzaamheid. Hij had het gewaagd om het officiële verhaal over de genocide in 1994 in twijfel te trekken en kritiek te uiten op het gebrek aan politieke vrijheid.

“Nepnieuws is iets heel dubbelzinnigs”, zegt Bart Jacobs, hoogleraar computerbeveiliging aan de Radboud Universiteit in Nijmegen. “Repressieve regeringen gebruiken het gevaar van nepnieuws vaak als excuus om de online-onderdrukking op te voeren. Maar tegelijk verspreiden ze zelf meestal ook nepnieuws, om opponenten in diskrediet te brengen en om hun burgers eronder te houden. Want nepnieuws maakt apathisch. Waarom zou je je nog druk maken over dingen, als je niet meer weet wat waar is? Zulke regimes zijn vaak heel blij met een apathische bevolking.”

Al het hacken, spioneren en manipuleren brengt grote gevaren met zich mee, want het internet heeft een spilfunctie in democratieën. “Sociale media en zoekmachines hebben een enorme macht en een zware verantwoordelijkheid om ervoor te zorgen dat hun platforms het publieke belang dienen”, waarschuwt Freedom House dan ook in zijn laatste rapport. “Als anti-democratische entiteiten in feite het internet veroveren, verliezen burgers een forum waar ze tot gedeelde waarden kunnen komen, beleidskwesties kunnen bediscussiëren en conflicten in de samenleving op vreedzame wijze kunnen oplossen.”

Helaas voor de voorvechters van internetvrijheid krijgen regimes steeds meer mogelijkheden voor repressie. Want er zijn inmiddels tientallen cyberspionage-bedrijven, die systemen leveren voor onder meer online-surveillance en het hacken van telefoons en computers.

Deze bedrijven hebben, zeker als ze gevestigd zijn in westerse landen, voor de export van zogenoemde ‘offensieve’ cybersystemen vaak een vergunning nodig. En de ondernemingen stellen zelf doorgaans dat ze hun technologie alleen laten gebruiken in de strijd tegen criminaliteit en terrorisme. “De enigen die bang hoeven te zijn, zijn terroristen en misdadigers”, verzekerde directeur Shalev Hulio van het Israëlische cybersecuritybedrijf NSO laatst tegenover de krant *Yedioth Ahronoth*. “De bevolking kan ’s nachts gerust slapen.”

Maar autocratische afnemers hanteren nogal eens hun eigen definitie van ‘terroristen’. En in de praktijk nemen ook lang niet alle cybersecurityfirma’s het even nauw als de dollars of euro’s van de dictators lonken.

Spin-off

Het Brits-Duitse Gamma Group kwam bijvoorbeeld in opspraak omdat het zijn FinFisher-systeem zou hebben geleverd aan onder meer Egypte en Turkmenistan. Toen het Italiaanse bedrijf HackingTeam in 2015 zelf het doelwit werd van een hack bleek de firma facturen te hebben gestuurd naar landen als Soedan, Kazachstan en naar het Libanese leger. En in Israël is, als spin-off van zijn relatief forse veiligheidsapparaat, een waar cluster van cyberspionagefirma’s ontstaan.

Volgens recente onthullingen van Haaretz leveren Israëlische ‘cyberhuurlingen’ hun geavanceerde systemen aan zeer uiteenlopende, niet altijd even fatsoenlijke overheden, variërend van Azerbeidzjan tot Swaziland en van Indonesië tot Saudi-Arabië. De autoriteiten in die landen zetten de snufjes vervolgens, als het zo uitkomt, in voor de jacht op oppositiepolitici, homo’s, etnische en religieuze minderheden en mensenrechtenactivisten

We zijn als lammeren. Ze pakken ons een voor een. We kunnen niet terugvechten.

Chinese bouwvakker die een spotprent op Twitter postte

Zo kreeg een medewerkster van Amnesty International in Londen in juli vorig jaar op haar mobiel een whatsapp-berichtje met een weblinkje over een naderend protest bij de Saudische ambassade in Washington. De mensenrechtenorganisatie voerde op dat moment juist campagne voor de vrijlating van enkele activisten in Saudi-Arabië. De Amnesty-medewerkster besteedde in eerste instantie weinig aandacht aan het berichtje, maar kreeg een dag later toch argwaan en ging met haar telefoon langs bij digitale experts van Amnesty. Die ontdekten dat het een Saudische poging was geweest om ongezien een hoogwaardig software-pakketje genaamd Pegasus, ontwikkeld in Israël, op haar smartphone te installeren. “Dat is heel diep binnendringende software”, vertelt deskundige Danna Ingleton van Amnesty. “Het maakt van je telefoon een spion in je eigen zak. De gebruikers krijgen toegang tot al je contacten. Ze kunnen al je foto’s zien en elke toets registreren waar je op drukt.”

Saudi-Arabië probeerde software op de mobiel van een Amnesty-medewerker te zetten. ‘Die maakt van je telefoon een spion in je eigen zak.’

Ingleton en haar collega’s constateerden dat enkele Saudische dissidenten in het Westen rond die tijd ook met dezelfde Israëlische software waren aangevallen. Onder hen de Saudische activist Omar Abdulaziz, die contact onderhield met de bekende Saudische balling en krantencolumnist Jamal Khashoggi, die twee maanden later in Istanbul zou worden vermoord. Amnesty zegt nog geen bewijs te hebben dat Khashoggi zelf ook met de omstreden Israëlische software werd gevolgd. Maar de mensenrechtenorganisatie ziet in de zaak wel extra reden om beter toezicht te eisen.

“Overheden mogen deze technieken natuurlijk hebben voor de strijd tegen echte terroristen”, zegt Ingleton. “Maar dan wel met alle *checks and balances*, om misbruik te voorkomen. En deze middelen mogen nooit in handen komen van landen als Saudi-Arabië. Regeringen moeten er veel beter op gaan toezien dat autocratische regimes dit soort systemen niet krijgen.”