Inhoud

De belangrijkste in de tekst gebruikte afkortingen

AI	Artificiële Intelligentie
ASML	Advanced Semiconductor Materials Lithography
AU	Afrikaanse Unie
AVG	Algemene Verordening Gegevensbescherming
AWS	Amazon Web Services
BIB	Bank voor Internationale Betalingen
CBDC	Central Bank Digital Currency
CCC	Chaos Computer Club
CCP	Chinese Communistische Partij
CDA	Communications Decency Act
CIA	Central Intelligence Agency
CISA	Cybersecurity and Infrastructure Security Agency
CNI	Clean Network Initiative
CPI	CyberPeace Institute
COO	Chief Operating Officer
CZI	Chan Zuckerberg Initiative
DFI	Declaration for the Future of the Internet
DHS	Department of Homeland Security
DNS	Domain Name System
FDA	Food and Drug Administration
FOIA	Freedom of Information Act
FTX	Futures Exchange
FTC	Federal Trade Commission
GGO	Genetisch gemodificeerd organisme
GPS	Global Positioning System

ICANN	Internet Corporation for Assigned Names and Numbers
ICE	Immigration and Customs Enforcement
LLM	Large Language Model
IEBC	Independent Electoral and Boundaries Commission
NCSC	Nationaal Cyber Security Centrum
NSA	National Security Agency
NSO Group	Israëlisch technologiebedrijf (NSO: Niv Karmi, Shalev Hulio, Omri Lavie, de oprichters)
NTIA	National Telecommunications and Information Administration
OESO	Organisatie voor Economische Samenwerking en Ontwikkeling
OTA	Office of Technology Assessment
RESTRICT	Restricting the Emergence of Security Threats that Risk Information and Communications Technology
RFOB	Real Facebook Oversight Board
SEC	Securities and Exchange Commission
TSMC	Taiwan Semiconductor Manufacturing Company
USAID	United States Agency for International Development
VN	Verenigde Naties
WOB	Wet Openbaarheid van Bestuur
WOO	Wet Open Overheid
ZTE	Zhongxing Telecommunications Equipment

Inleiding
De strijd

Begin 2010 ontmoette ik in een café in het oosten van Turkije een jonge man; laat ik hem Ali noemen. Hij vertelde me over zijn ontsnapping uit Iran.

Ali was de zomer daarvoor gearresteerd tijdens de Groene Beweging, een reeks demonstraties in Iran die uitbrak als protest tegen de uitslag van de presidentsverkiezingen. Terwijl Ali met aan elkaar gebonden polsen op de stoep zat te wachten tot de politie hem kwam halen en zich angstig afvroeg wat hem te wachten stond, kwam er toevallig een vrouw langsgereden. Ze was zo moedig om te stoppen, sleurde hem de auto in, ging er snel vandoor en zette hem thuis af. De opluchting was van korte duur, want Ali wist dat de 'Basiji', de beruchte Revolutionaire Garde, binnenkort bij zijn ouders voor de deur zou staan. Die avond nog vluchtte hij naar een afgelegen gebied in het noorden van het land, waar zijn familie een stukje grond bezat.

Ali was een van de miljoenen Iraniërs die protesteerden tegen de overwinning van Mahmoud Ahmadinejad bij de presidentsverkiezingen. Op 20 juni 2009 werd een andere moedige demonstrante, Neda Agha-Soltan, gedood door een sluipschutter. Ze zakte op straat in elkaar en stierf vrijwel meteen, terwijl het bloed uit haar mond stroomde en omstanders het van schrik en afschuw uitschreeuwden.[1] We weten dit omdat de dood van Agha-Soltan, anders dan de vele wreedheden die autoritaire regimes meestal in donkere gevangeniscellen begaan, werd opgenomen door een ooggetuige met een mobiele telefoon. Video's van dit incident, en van andere gevallen van staatsgeweld tegen vreedzame demonstranten, werden over de hele wereld gedeeld en leidden

tot woede en verontwaardiging. Demonstranten van de Groene Beweging plaatsten hun ooggetuigenverslagen op sociale media met de hashtag #iranelection, waardoor de hele wereld kon zien hoe een revolutie zich ontvouwde in een van de meest repressieve landen ter wereld.

De rol van sociale media (met name Facebook, YouTube en Twitter) en het gebruik van technologie (mobiele telefoons en internetverbindingen) werd al snel bepalend voor hoe journalisten en politici wereldwijd de protesten in Iran duidden. Deze online platforms vulden een belangrijk gat dat was ontstaan door de harde onderdrukking van de pers door het Iraanse regime. Kort na de start van de protesten verboden de autoriteiten journalisten om op straat verslag te doen, in een wanhopige poging grip te krijgen op de situatie.[2] Ahmadinejad sloot twaalf kranten en liet meer dan honderd journalisten oppakken.[3] Twitter (tegenwoordig opererend onder de naam X) ontpopte zich tot essentieel platform waarop mensen aan informatie konden komen over de protesten en het overheidsgeweld, en als gevolg daarvan werd de Groene Beweging zelfs tot 'Twitter-revolutie' bestempeld.[4] Het was een moment van enorme hoop over het democratiserende potentieel van opkomende technologieën; actievoerders konden sociale media en mobiele telefoons niet alleen gebruiken om mensenrechtenschendingen vast te leggen en te delen, maar ook om hun acties te coördineren en mensen te mobiliseren. De regering-Obama vroeg Twitter zelfs om een geplande systeem-update uit te stellen om te voorkomen dat de Iraanse demonstranten tijdelijk geen toegang zouden hebben.[5]

Deze verwachtingsvolle houding ten opzichte van technologie als partner in de revolutionaire vrijheidsstrijd werd het jaar daarop versterkt toen er volksprotesten uitbraken in Tunesië en Egypte. De opstand van Egyptenaren tegen het regime van Mubarak werd door westerse media uitgeroepen tot een 'Facebookrevolutie', een referentie aan de gigantische Facebookgroepen die jeugdige demonstranten aanmaakten om hun acties te coördineren.[6] Veel mensen geloofden (en hoopten) dat jongeren in Noord-Afrika en het Midden-Oosten met behulp van in de vs gemaakte technolo-

gieën beter in staat zouden zijn om rechten en rechtvaardigheid af te dwingen.

Terwijl westerse media en politici enthousiast waren over het democratiserende potentieel van de nieuwe technologieën, was het beeld in Teheran, Caïro en Tunis minder eenduidig. Zoals de Iraanse journaliste Golnaz Esfandiari later zou uitleggen, communiceerden actievoerders bij het organiseren van protesten vooral via mond-tot-mondberichtgeving, sms'jes, mailtjes en blogposts, in plaats van via sociale media.[7]

Zoals Ali ook zou ontdekken, bleek het gebruik van mobieltjes voor de demonstranten ook enorme risico's met zich mee te brengen. Toen hij zijn schuilplaats in het noorden van Iran had bereikt, belde hij zijn moeder om haar te vertellen dat hij veilig was. Haar opluchting duurde niet lang: Ali's telefoonsignaal werd opgepikt door een landelijk monitoringsnetwerk en niet lang daarna werd hij aangehouden op de afgelegen plek waar hij zich bevond. Hij belandde in de beruchte Evin-gevangenis, die bekendstaat om de brute verkrachting en wrede marteling van gevangenen.[8] Nadat hij daar een aantal vreselijke maanden had doorgebracht, wist hij tijdens een verlof te ontsnappen naar Oost-Turkije. Zelfs toen ik hem in 2010 ontmoette, veranderde hij nog elke dag van adres, omdat hij wist dat de Iraanse veiligheidsdiensten ook over de grens actief op dissidenten joegen.

Mensen die de democratiserende mogelijkheden van technologie en sociale mediaplatforms ophemelden, leken niet te beseffen dat ook autoritaire regimes de laatste innovaties slim gebruikten. In Iran, en later in Syrië, waren de autoriteiten zo sluw om het verbod op het gebruik van sociale media op te heffen, en de geplaatste berichten vervolgens als bewijs te gebruiken tegen degenen die ze hadden geplaatst. Dezelfde technologieën die spam op kunnen sporen, hielpen het staatsapparaat te identificeren wie kritische berichten op sociale media plaatste. Militaire inlichtingendiensten gebruikten locatiesignalen van online platforms om mensen te traceren die zich aan het verzamelen waren op een straathoek – realtime informatie die erg handig kan zijn als je mensen uiteen wilt drijven nog voordat zich grotere massa's vormen.

De onderdrukking en het lijden van de moedige Iraanse demonstranten raakten me diep. Ik was ook onder de indruk van hun moed. Neda Agha-Soltan was destijds maar vier jaar jonger dan ik. In dezelfde zomer waarin een golf van jonge Iraniërs hun vrijheid eisten, was ik als lid van het Europees Parlement gekozen door kritiek te leveren op de Nederlandse regering, terwijl mensen die in Iran precies hetzelfde deden door hun regering werden doodgeschoten. Ik was ook geschokt, niet zozeer doordat autoritaire staten mensen onderdrukten; ik had weinig anders verwacht, maar door onze eigen dubbele moraal. De door deze regimes gebruikte monitoringtechnologie en spyware kwamen uit Europa. Italiaanse hackingapparatuur was favoriet bij het Assad-regime in Syrië, terwijl Franse technologieën Gaddafi hielpen in Libië, en Britse systemen het Mubarak-regime in Egypte ondersteunden.[9]

Waar Europese regeringen de schendingen van mensenrechten veroordeelden, exporteerden Europese bedrijven geavanceerde spyware naar machthebbers in het Midden-Oosten. Zoals Nokia Siemens Networks in 2010 zou toegeven, had dit bedrijf monitoringsystemen voor mobiele telefoonnetwerken verkocht aan de Iraanse autoriteiten. Die konden daarmee demonstranten volgen; mensen die op vreedzame wijzen vroegen om vrijheden die iedere Europeaan als vanzelfsprekend beschouwt.[10] Tijdens een hoorzitting voor de mensenrechtencommissie van het Europees Parlement probeerde het hoofd marketing van Nokia Siemens het bedrijf te distantiëren van de Iraanse misstanden met als argument dat uiteindelijk 'degenen die deze technologie gebruiken om mensenrechten te schenden verantwoordelijk zijn voor hun eigen handelen'.[11] Hoewel dit natuurlijk waar is – niemand betwist dat de Iraanse regering verantwoordelijk is voor haar handelen – ontslaat dit het bedrijf niet van zijn morele plicht om te voorkomen dat het onderdrukking faciliteert. Ingenieurs van bedrijven met dergelijke contracten moeten meerdere keren naar Iran gereisd zijn om daar mensen te trainen op een zo effectief mogelijk gebruik van hun systemen, of om ze te repareren. Waarschijnlijk hebben ze ook nog extra salaris ontvangen omdat ze onder 'zware arbeidsomstandigheden' moesten werken. Bovendien waren de

mensenrechtenschendingen in Iran al bekend en goed gedocumenteerd voordat het neerslaan van de protesten in 2009 begon.

Als pas gekozen lid van het Europees Parlement was ik woedend na het horen van Ali's verhaal en de verhalen van de andere Iraanse vluchtelingen die ik tijdens mijn reis naar Turkije ontmoette. Welke betekenis hadden Europese steunbetuigingen aan de mensenrechten van demonstranten nog als de nieuwste repressiemiddelen ook in Europa werden geproduceerd? Deze dubbele moraal legde de grondslag voor een groot deel van mijn werk als volksvertegenwoordiger. In de tien jaar dat ik Europarlementariër was zou ik elk denkbaar beleidsinstrument aangrijpen in mijn pogingen om een einde te maken aan de inzet van wat ik destijds 'digitale wapens' noemde, software die gegarandeerd tot schendingen van mensenrechten leidt en onschuldige mensen schaadt.[12] Helaas is er nog veel meer werk te doen. Tegenwoordig zijn de nieuwste versies van commerciële hackingsystemen er alleen maar krachtiger en grootschaliger op geworden. Erger nog, naarmate ik meer te weten kwam over de digitale wapenhandel die zich de afgelopen tien jaar steeds verder heeft verbreid, realiseerde ik me dat de Iraanse Groene Beweging slechts één veldslag was in de oorlog om de democratie te beschermen tegen machtsmisbruik met behulp van technologie.

De onthulling

Toen het 'Pegasus Project' in de zomer van 2021 een reeks artikelen publiceerde met onthullingen over overheidsspionage, las ik die met een mix van verontwaardiging en hoop.[13] Pegasus is het belangrijkste spywareproduct van de NSO Group – een Israëlisch technologiebedrijf dat vooroploopt in commerciële hackingtechnologie, een markt waarin wereldwijd miljarden omgaan. Spyware wordt over de hele wereld verkocht als wapen tegen terrorisme en misdaad, maar wordt uiteindelijk vaak gebruikt als een private inlichtingendienst waarmee kritische stemmen kunnen worden geïntimideerd en onderdrukt. De onderzoeksjournalisten van het

Pegasus Project publiceerden de lijst met gelekte doelwitten van de NSO Group: meer dan vijftigduizend telefoonnummers van potentiële slachtoffers die de organisatie in opdracht van haar klanten zou hacken.[14] Veel mensen werden zich door het Pegasus Project voor het eerst bewust van de ingrijpende gevolgen van hack- en spionagetechnologieën.

Gelekte documenten lieten zien hoe geavanceerd spyware tegenwoordig is; het doet de methoden verbleken waarmee Ali's bewegingen in Iran werden nagegaan. Door op afstand microfoons en camera's in te schakelen zonder dat een slachtoffer het weet, kan Pegasus hun telefoon of laptop veranderen in een live-spionage-instrument. Deze zogenaamde *zero-click*-aanvallen zijn zeer effectief omdat je niets hoeft te doen – op een geïnfecteerde link klikken of wat dan ook – om de infiltratie in gang te zetten. Zodra NSO toegang krijgt, kunnen diens klanten iemands contacten, gesprekslogs, berichten, foto's, browsegeschiedenis en software-instellingen inzien en informatie verzamelen uit populaire communicatie- en chatapps.[15] Het is niet verrassend dat autoritaire landen overal ter wereld enthousiaste afnemers zijn. Voordat het Pegasus Project de praktijken van het bedrijf openbaarde, bedroeg de waarde van de NSO Group 2,3 miljard dollar.[16]

De publicaties legden niet alleen bloot wat deze technologie kan en wie de slachtoffers waren, maar ook wie er bij het bedrijf waren betrokken. Zo hadden voormalige officials van de Franse regering en de regering-Obama lucratieve functies als 'Senior Advisors' – terwijl intussen de telefoons van de Franse president, de hoofdredacteur van de *Financial Times* en Hongaarse oppositieleiders werden gehackt en afgeluisterd.[17] Het faciliteren van Ali's arrestatie door Nokia Siemens en de transacties van de NSO Group met dictaturen roepen de vraag op waarom de democratische landen vanwaaruit deze bedrijven opereerden niet méér hebben gedaan om de ontwikkeling en verkoop van deze technologieën aan banden te leggen.

Eén reden, al is het zeker niet de enige, is dat onze politieke leiders te lang in de greep zijn geweest van een veel te optimistische kijk op nieuwe technologie. De datagedreven aanpak in de succes-

volle verkiezingscampagne van Barack Obama in 2008 werd door politici over de hele wereld met ongekend enthousiasme gevolgd. Ze stonden te trappelen om ook op nieuwe manieren met kiezers te communiceren. Dat weet ik ook uit eigen ervaring. Mijn activiteiten op sociale media hebben me ongetwijfeld geholpen om mijn zetel in het Europese Parlement te veroveren. Zonder Twitter en Facebook had ik als nieuwkomer in de politiek mijn potentiële kiezers misschien nooit kunnen bereiken. Toen ik eenmaal was gekozen, boden deze platforms me ook een handige manier om mensen op de hoogte te houden van activiteiten die de krant of tv niet haalden. In mijn eerste jaren als Europarlementariër werd technologische disruptie vooral gezien als een positieve ontwikkeling.

Maar ook toen duidelijker werd wat de ware aard en schaduwzijden van deze technologieën waren, en toen de techbedrijven een enorme groei doormaakten, deden politieke leiders er weinig aan. Tegen de tijd dat de onthullingen van het Pegasus Project in 2021 de voorpagina's haalden, streed ik al tien jaar lang tegen spyware, en nog was deze gevaarlijke industrie geen halt toegeroepen. Ja, we hadden het voor elkaar gekregen dat de EU exportcontroles invoerde, waardoor de uitvoer van spyware werd beperkt; maar de import en dus het gebruik binnen de EU kon ongehinderd doorgaan.

Aanvankelijk was ik zo naïef om te denken dat mijn politieke collega's niets deden omdat de technologie zich snel ontwikkelde, en ze de ingewikkelde systemen gewoon niet begrepen. Hoewel die onwetendheid vast heeft bijgedragen aan hun passieve houding, was de belangrijkste reden veel cynischer: regeringen wilden deze spyware zelf ook gebruiken om hun eigen bevolking in de gaten te kunnen houden. Destijds waren Europeanen woedend omdat Amerikaanse inlichtingendiensten Europese leiders bleken af te luisteren, onder wie de Duitse bondskanselier, Angela Merkel.[18] EU-lidstaten drongen aan op nieuwe wetgeving om mensen te beschermen tegen Amerikaanse spionagepraktijken. Maar ondanks die publieke verontwaardiging kochten Europese politiekorpsen in het geheim de meest geavanceerde infiltratiesystemen