

'De informatiesnelweg.' Zo noemden we het internet in de jaren 90. En we meenden het nog ook! Aan een halsbrekende vaart zou informatie zich over dit wereldwijde netwerk verspreiden onder de wereldbevolking. En dan, ja dan was alles mogelijk. Hoe zouden dictators hun bevolking nog dom kunnen houden? Hoe zouden grote bedrijven het nog halen tegen een handvol jonge creatievelingen met een website?

Een van de uithangborden van dat optimistische idee was Wikipedia: een schat aan informatie, gratis ter beschikking van iedereen. En steeds *up to date*. Elke leemte werd meteen opgevuld, elke fout meteen gecorrigeerd door *the crowd*.

Natuurlijk was dat nooit helemaal waar. Wikipedia is alleen écht helder en betrouwbaar als het over ontegensprekelijke wetenschappelijke feiten gaat. Zodra er een beetje politiek of, erger nog, religie mee gemoeid is, wordt Wikipedia een zootje: honderden auteurs proberen de tekst hun eigen draai te geven, zodat het resultaat uiteindelijk vier keer te lang en amper coherent is.

Maar het kan veel erger, leerden we de jongste maanden. Het internet kan worden gebruikt om valse informatie te verspreiden. En, wie weet, heeft dat de democratie zelfs ontworcht. Dat is mogelijk geworden door een fundamentele verandering in de manier waarop we het internet gebruiken. Weet u nog dat we het ooit hadden over 'surfen' op het web? Die uitdrukking suggereerde dat je een stukje meereed op één golf, en dan oversprong op de volgende. Waarbij je zelf – min of meer – de richting kon bepalen. Vandaag drijven we in een vlotje de Facebook-rivier af. Wat we zien voorbijkomen, en wat niet, wordt bepaald door 'het algoritme': een vorm van zwarte magie die ontwikkeld is om ons zo lang mogelijk op Facebook te houden en ons daar zo veel mogelijk advertenties te tonen.

In de bubbel

Sociale netwerken en Google hebben de neiging ons 'meer van hetzelfde' te laten zien, stelde Eli Pariser in 2011 vast. Hij noemde dat fenomeen de 'filter bubbel'. Maar dat werd pas een acuut gevaar toen het onderzoeksinstituut PEW constateerde dat een zorgwekkend grote groep Amerikanen haar nieuws net put uit die bubbel. Die nieuwe realiteit zette de deur open voor misbruik door mensen die het Facebook-algoritme weten te manipuleren. Bij een heel nipte verkiezingsstrijd – en elke presidentsverkiezing in de VS is per definitie nipt – kon dat misschien zelfs een doorslaggevend verschil geven.

Op Facebook ziet een nieuwsbericht van, pakweg, *The New York Times* en één van *The Denver Guardian* er ongeveer hetzelfde uit. Maar *The New York Times* is een krant

Vals nieuws verdringt het echte op Facebook. Racisme en seksisme tieren welig, terwijl een blote borst wordt gecensureerd. Cybercriminelen stelen miljoenen euro's en, via een paar gehackte mailboxen, misschien wel een presidentsverkiezing. En de jacht op terroristen doet ons laatste beetje privacy wegsmelten. Wanneer werd het internet zo'n duistere plek?

met honderden van de allerbeste journalisten. *The Denver Guardian*? Die bestaat niet. Er is wel een website met die naam, maar die is gebouwd om één bericht te lanceren, in volle verkiezingsstrijd. Namelijk dat Clinton een FBI-agent en zijn gezin heeft laten vermoorden. Dat bericht is niet waar. En zonder Facebook had het zich maar moeilijk kunnen verspreiden. Ja, ik had u een e-mail kunnen versturen met een link naar het bericht, en de vraag om het dringend naar al uw vrienden door te mailen. Maar op Facebook staat het gewoon tussen de echte verhalen, en daar ontleent het geloofwaardigheid aan. In enkele seconden gaat het de wereld rond.

Is daar iets aan te doen? We kunnen laag opgeleide, oudere blanke arbeiders in het Amerikaanse binnenland moeilijk verplichten om een goede krant te lezen of naar NPR te luisteren. Evenmin kunnen we deze mensen opleggen om op Facebook ook bevriend te worden met een paar linkse intellectuelen uit Manhattan, kwestie van wat meer verschillende stemmen te horen. En dus eisen we nu dat Facebook en Google vals nieuws detecteren en uit hun respectieve bubbels verwijderen. Maar dan hebben we Facebook aangesteld tot officiële instantie die bepaalt wat waar is en wat niet.

De opmars van sociale netwerken, en met name Facebook, heeft de aard van het internet fundamenteel veranderd. 'Het internet' is van iedereen (hoewel: een beetje meer van Google en Amazon dan van u en mij). Maar Facebook is van één man, Mark Zuckerberg. Via een speciaal soort supra aandelen is hij amper verantwoording verschuldigd aan de andere aandeelhouders – laat staan aan een of andere overheid. Het is Facebook, dus Zuckerberg, die bepaalt dat een historisch

belangrijke nieuwsfoto zoals die van het napalm-meisje weg moet, terwijl dat 'nieuws' over een door Clinton vermoorde FBI-agent wel mag worden gedeeld. Gaat het protest hard genoeg klinken, dan corrigeert hij zijn oordeel wel eens. Maar niet altijd. Hoe belangrijker Facebook wordt en hoe meer tijd we er doorbrengen, hoe meer dat een probleem wordt.

Gesponsord of niet

Als *fake news* de doorslag niet gaf op 8 november, dan waren het misschien de (Russische?) hackers die gênante mails van de Democratische partij verspreidden. Mails van de Republikeinse partij hebben ze blijkbaar achtergehouden – wat meteen ook betekent dat 'iemand' nog over cybermunitie beschikt die op een geschikt tijdstip kan worden bovengehaald.

Het zijn de VS, waarschijnlijk in samenwerking met Israël, die de grenzen voor cyberspionage en cyberoorlog hebben verlegd. In 2010 werd Stuxnet ontdekt, een virus dat speciaal was ontworpen om de nucleaire opwerkingscentrifuges van Iran te saboteren. Stuxnet was een succes: het heeft het (nucleaire) machtsverval in de wereld beïnvloed. Maar je zou ook kunnen zeggen dat de VS toen zelf het politieke cybermonster hebben verwekt dat ze op 9 november in hun eigen bed aantroffen.

Cybercriminelen heb je voortaan in twee variëteiten: met en zonder 'state sponsorship', zoals dat heet. Ook de 'gewone' cyberboeven zijn gevaarlijker dan ooit. Dit jaar kwamen we te weten dat de database van Yahoo niet één maar twee keer volledig leeggeroofd is. Dat zou weliswaar al in 2013 en 2014 zijn gebeurd. Gegevens van 1 miljard gebruikers zijn gepikt.

Ook via onze inbox staan we on-

der vuur. Een gevaarlijke *phishing mail* kon je vroeger gewoon herkennen aan de schabouwelijke spelling. In 2016 niet meer. En de bedrieglijke link in die mail leidt je misschien naar *ransomware*: een virus dat je harde schijf versleutelt. Je krijgt je gegevens alleen terug, als je meteen geld overschrijft. Eind oktober nog moesten drie Amerikaanse hospitalen hun computersystemen afsluiten, nadat ze werden getroffen door *ransomware*.

Andere hackers slaagden erin het Swift-betaalsysteem te kraken en zo tientallen miljoenen te roven van de Centrale Bank van Bangladesh. En op 21 oktober ging een flink stuk van het internet urenlang plat, na een bombardement door een zogenoemd 'botnet'. De verrassing was dat het Mirai-botnet niet bestaat uit traditionele computers, maar uit onder meer beveiligingscamera's, digitale videorecorders en andere zogenoemde 'Internet of Things'-apparaten. Die trend om allerlei toestellen van een handige internetverbinding te voorzien, heeft dus ook een keerzijde – maar dat kwamen we pas in de laatste weken van dit jaar te weten.

Nooit meer anoniem

'Op het internet weet niemand dat je een hond bent', zo grapte een beroemde cartoon in 1993 in *The New Yorker*. In 2016 zijn er nog maar een paar wilde uithoeken van het net waar je anoniem kunt zijn. Twitter is daar één van. We zagen dit jaar meer dan ooit tot wat voor wansmakelijk seksistisch en racistisch geraas dat kan leiden. En dus zal er in 2017 nog minder plaats zijn voor anonimiteit.

Dat is geen onverdeelde zegen, want het alternatief leerden we dit jaar ook heel intiem kennen: op het nieuwe internet zijn we voortdurend zichtbaar en herkenbaar – voor Facebook, voor adverteerders, voor inlichtingendiensten uit binnen- en buitenland. Voorvechters van onze online privacy behaalden in het begin van het jaar nog een belangrijke overwinning: de Europese privacy-verordening werd uiteindelijk toch aangenomen. Maar nog voor ze van kracht is, wordt ze alweer uitgehold, omdat de wereld inmiddels andere prioriteiten heeft. Zoals de strijd tegen het 'terrorisme', een begrip dat in deze context steeds breder wordt geïnterpreteerd. Met terrorisme als argument, eiste de FBI een achterpoortje op elke iPhone (voorlopig zonder succes). Groot-Brittannië keurde een wet goed die zowat alle overheidsdiensten toegang geeft tot het surfgedrag van de Britten, op eenvoudig verzoek.

Het internet droeg natuurlijk al sinds zijn ontstaan dit kwalijke potentieel in zich. Wie geen dromerige utopist was, heeft dat altijd geweten. En toch. Dat we het in 2016 allemaal zo ongenadig over ons heen gekieperd zouden krijgen, wie zag dat twaalf maanden geleden aankomen?

We surfen niet meer op het internet, we drijven in een vlot de **Facebookrivier** af