ARTIKEL

Grenzeloos: rechtsstaat en vertrouwen in een verbonden wereld

Marietje Schaake

Online bestaat er nog geen 'rule of law'-traditie; er is veel onduidelijkheid over welke regels er gelden wanneer staten het internet als een wapen of middel van onderdrukking inzetten. Maar de rechtsstaat moet ook online zijn betekenis houden; daarbij dienen de rechten en vrijheden van de internetgebruiker, waar die zich ook bevindt, centraal te staan.

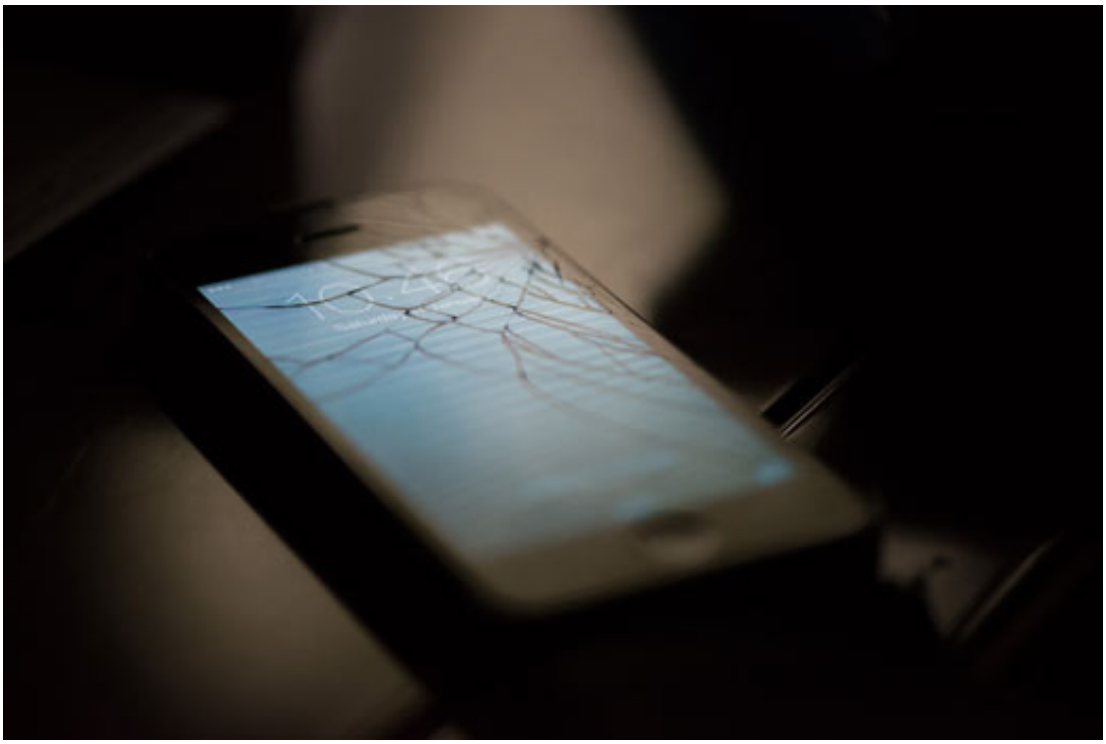
Tijdens de afgelopen presidentsverkiezingen in de Verenigde Staten werd de Democratische partij gehackt en verschenen gevoelige gegevens via WikiLeaks in de media. Al snel wezen Amerikaanse officials met de vinger naar Rusland. Ze beschuldigden het Kremlin ervan te proberen de presidentsverkiezingen te manipuleren. Er moet nog worden bewezen of en in hoeverre dat is gelukt. De vraag is ook welke consequenties deze ongekende aantijging zal hebben en vooral hoe dit soort hacks in de toekomst kunnen worden voorkomen. Inmiddels zei Angela Merkel dat zij vreest voor 'social bots' die de verkiezingen in Duitsland kunnen manipuleren, en is er een levendig debat over 'nep nieuws' en propaganda losgebarsten.

Deze berichten, en de vrijwel dagelijkse stroom nieuws over hacken, lekken, cyberaanvallen en data-inbreuken, dragen niet bij aan het vertrouwen onder burgers. Het staat in schril contrast met de belofte van het open internet dat democratisering zou moeten brengen en mensen over de hele wereld meer mogelijkheden zou geven, zoals toegang tot universele mensenrechten. Maar het vertrouwen in het gebruik van online-diensten neemt af, staten monitoren wat internetgebruikers zeggen en terreurorganisaties gebruiken sociale media en chat apps om gruwelijke beelden te delen en mensen te ronselen voor een zogenaamd heilige oorlog.

Om het internet open, betrouwbaar, vrij en veilig te houden, moeten de rol en verantwoordelijkheid van verschillende actoren wier gedrag de meeste invloed heeft, worden belicht. Niet alleen staten hebben een belangrijke rol als het gaat om wetten en regels die gelden op het wereldwijde internet. Van de technische infrastructuur tot de diensten die eroverheen gestuurd worden, de private sector wordt steeds invloedrijker. We moeten over grenzen heen kijken en zoeken naar nieuwe oplossingen die ervoor zorgen dat de rechtsstaat ook online zijn betekenis houdt. Daarbij moeten de rechten en vrijheden van de internetgebruiker, waar die zich ook bevindt, centraal staan.

Grenzeloos

Dat is gemakkelijker gezegd dan gedaan in de verschuivende realiteit tussen soevereiniteit van staten en een grenzeloos internet, dat zowel leidt tot kansen als bedreigingen. Vanuit het perspectief van democratisering en mensenrechten, kunnen Iraniërs bijvoorbeeld worden geholpen om toch toegang tot informatie te krijgen, ondanks de zeer restrictieve wetten in dat land. Maar vanuit het perspectief van de Islamitische Republiek is de beschikbaarheid en toegang tot het wereldwijde web juist een reden om een nationaal internet aan te leggen: gecensureerd en centraal gecontroleerd.



© Flickr / Faris Algosaibi

'De immateriële schade van het beperken van toegang tot informatie en vrije meningsuiting is groot'.

De beweging richting een gesloten 'splinternet', waarbij landen een eigen, controleerbaar internet prefereren boven het open internet, past in een bredere trend (http://www.economist.com/news/leaders/21702750-farewell-left-versus-right-contest-matters-now-open-against-closed-new) waarbij staten de grip op mensen versterken via het controleren van het internet en wat erover wordt verstuurd. De drang naar meer controle gaat ook gepaard met het door staten steeds actiever inzetten van nieuwe technologieën als een middel voor controle op hun burgers, of zelfs als middel van nieuwe oorlogsvoering.

Uitschakelen van het internet door staten gebeurt steeds vaker.....

Een drastische manier om controle over burgers te behouden, is het volledig uitschakelen van het internet. Dat gebeurde in Egypte tijdens de massale opstanden tegen het regime van Hosni Mubarak, maar ook Turkije sluit regelmatig toegang tot het internet af in het zuidoosten van het land. Bangladesh sloot apps, zoals WhatsApp, Facebook Messenger en Twitter, gedurende 22 dagen af om protesten te voorkomen nadat een rechtbank doodstraffen had uitgesproken tegen twee politieke leiders die beschuldigd werden van oorlogsmisdaden. In Oeganda werden internet serviceproviders (ISP's) door de overheid gedwongen WhatsApp, Facebook en Twitter te blokkeren in de aanloop naar de presidentsverkiezingen. Algerije bedacht dat het afsluiten van sociale media zelfs een goede remedie was tegen spieken bij examens, en China hanteert een 'great firewall' en houdt daarmee zowel zijn bevolking in toom als westerse bedrijven buiten de virtuele deur. De lijst met dergelijke voorbeelden wordt steeds langer.

.....maar heeft grote economische gevolgen

Toch schieten regeringen zichzelf met deze maatregelen in de voet. Want het afsluiten van het internet heeft grote economische gevolgen. Zo toonde een studie van de denktank Brookings aan, dat 81 afsluitingen van het internet in totaal een verlies van 2,4 miljard euro voor de

wereldhandel tot gevolg hadden. In Egypte werden de voor het afsluiten van het internet en mobiele verkeer verantwoordelijke ministers wel veroordeeld voor economisch verlies, maar niet voor de gevolgen voor mensen zelf, die in angst zaten over hoe het met hun dierbaren verging of niet in staat waren een ambulance te bellen in geval van gewonden. De immateriële schade van het beperken van toegang tot informatie en vrije meningsuiting is vele malen groter.

Nieuwe soevereinen

Een analyse van restricties van het open internet kan zich niet alleen beperken tot het gedrag van staten. Grote technologiebedrijven ontpoppen zich als de nieuwe soevereinen. Door de belangrijke rol die zij wereldwijd spelen, worden ze steeds vaker geconfronteerd met uitdagingen die voorheen alleen op het bord van diplomaten of politici lagen. Dit werd onder andere duidelijk in de commotie over 'The Innocence of Muslims' op YouTube. Moeten bedrijven censuur toepassen onder druk van regeringen van landen, omdat rellen met dodelijke slachtoffers uitbreken? Kunnen regeringen radicalisering wel effectief tegengaan *zonder* samenwerking met sociale mediagiganten? Maar hoe wordt gecontroleerd of informatie wel binnen de grenzen van de wet wordt verwijderd? Wat is de maatschappelijke impact van algoritmen die vooral ontworpen zijn om steeds grotere winst te verwezenlijken, als het gaat om toegang tot informatie, non-discriminatie en media-pluralisme?

In het vacuüm van ontbrekende wereldwijde wetgeving, springen grote technologie- en sociale mediabedrijven. Zij ontwikkelen *de facto* al normen die niet altijd in lijn zijn met de beginselen van de rechtsstaat. Ook zijn staten steeds afhankelijker van bedrijven als het gaat om het ontwikkelen en beschermen van kritieke infrastructuur. De vraag dringt zich op waar beslissingen worden genomen en wie uiteindelijk verantwoordelijk is.

'Inlichtingendiensten mogen nu ook zonder gerechtelijk bevel zien welke websites iemand bezoekt, waarmee de geloofwaardigheid van democratische landen ten opzichte van landen met repressieve regeringen wordt aangetast'.

Helaas wordt de rechtsstaat, d.w.z. het effectief juridisch en democratisch toezicht op het handelen van staatsorganen, niet altijd nageleefd in democratische landen. Zo wil – zelfs na de onthullingen over de praktijken van de NSA door Edward Snowden – de nieuwe CIA-directeur opnieuw op grote schaal metadata gaan verzamelen, ook nadat een Amerikaanse rechtbank die praktijk eerder al illegaal had beschouwd. En een nieuwe wet in het Verenigd Koninkrijk legaliseerde het op grote schaal aftappen van communicatie van burgers door Britse inlichtingendiensten. Inlichtingendiensten mogen nu ook zonder gerechtelijk bevel zien welke websites iemand bezoekt. Behalve de vraag of deze wetten voor een veiligere of onveiligere samenleving zorgen, wordt hiermee de geloofwaardigheid van democratische landen ten opzichte van landen met repressieve regeringen aangetast.

> Staten zijn steeds afhankelijker van bedrijven als het gaat om het ontwikkelen en beschermen van kritieke infrastructuur

Eerder werd al duidelijk hoe specialisten van de NSA onder de codenaam ‘GENIE’ inbreken in buitenlandse netwerken zodat die door de NSA kunnen worden gecontroleerd. De schaal van die operaties ging veel verder dan al werd aangenomen.

De digitale equivalent van ‘sleeper cells’

We spreken nu vaak over ‘sleeper cells’ van terreurnetwerken als Al-Qaida of de zogenaamde Islamitische Staat. Het zijn mensen die gedurende lange tijd nietsdoen, en dan gericht worden geactiveerd om een aanslag te plegen. Inmiddels zien we de digitale equivalent van ‘sleeper cells’. Door eerst stilletjes toegang te verschaffen tot een computersysteem, kan die toegang op een bepaald moment worden geactiveerd om ervoor te zorgen dat een computer de verkeerde berekeningen gaat maken, uitvalt of de controle verliest over een essentiële functie. De gevolgen kunnen desastreus zijn, en in het uiterste geval zelfs als oorlogsdaad worden bestempeld.

Staten of criminelen die een dergelijke aanval plegen, laten meestal geen sporen achter, of ´vermommen´ zich. Zo kan een Amerikaans gestuurde aanval via Duitse computers worden uitgevoerd. Het feit dat het ingewikkeld is om precies te weten wie een cyberaanval aanstuurt, maakt het lastig om de daders verantwoordelijk te houden, of te weten tegen wie een tegenaanval zich moet richten.

Nationale veiligheid *versus* cyberveiligheid

Hoewel solide nationale veiligheid niet kan bestaan zonder een weerbare digitale infrastructuur, zijn nationale veiligheid en cyberveiligheid geen synoniemen. Wanneer het internet een instrument wordt voor nationale veiligheidsdoelen, kan de cyberveiligheid zelfs verzwakt worden.

Dat is de belangrijkste les als het gaat om het verzwakken van versleutelingstechnieken (encryptie). Terwijl veel inlichtingendiensten hiervoor pleiten, zodat zij gegevens uit zoveel mogelijk telefoons en computers kunnen ophalen, waarschuwen computerexperts voor de gevolgen daarvan. Je kunt via een digitale achterdeur niet gericht toegang geven en degenen die kwaad willen, buiten de deur houden. Een gaatje in een softwaresysteem kan door

iedereen worden uitgebuit. Wie de essentiële methode om data te beveiligen – versleuteling – verzwakt, stelt zich bloot aan grote veiligheidsrisico's, die niet opwegen tegen de vermeende voordelen voor inlichtingendiensten.

Voorts is het boemerangeffect dat overheden over zichzelf afroepen, door bijvoorbeeld zelf te hacken, software-kwetsbaarheden niet te melden maar voor zichzelf te houden, of cyberaanvallen op staten uit te voeren, enorm. Onlangs werd nog aangetoond dat door *reverse engineering* de Islamitische Republiek Iran juist grote kennis over de gebruikte technologieën opdeed, terwijl het door de Verenigde Staten met Stuxnet werd aangevallen.

Ook de recente DNS-hack van Dyn en de razendsnelle groei van 'slimme apparaten' tonen aan dat voorkomen veel en veel belangrijker is dan genezen. Vaak is een systeem slechts zo sterk of veilig als de zwakste schakel. Dat kunnen ijskasten of verwarmingsthermostaten zijn, minimaal beveiligd met standaard paswoorden, maar die wel hele netwerken kwetsbaar maken. Wetgeving die minimale veiligheidsstandaarden en aansprakelijkheid oplegt aan fabrikanten, zou al een stap in de goede richting zijn. Wanneer keurmerken op producten staan weten consumenten beter hoe goed hun apparaten zijn beveiligd. Die standaarden moeten internationaal gemaakt worden om impact te hebben.

> Wereldwijd leiderschap door open democratieën is essentieel om te voorkomen dat gesloten, top-down gecontroleerd bestuur de norm wordt

In het publieke debat wordt vaak in zeer algemene termen over een 'cyber' gesproken. Het is belangrijk in te zoomen op verschillende typen aanvallen en niveaus van risico, op het zo precies mogelijk aanwijzen van verantwoordelijken om vervolgens naar oplossingen te zoeken. Waar mogelijk moet worden voortgebouwd op huidige wetten en regels. Het is tenslotte al lastig genoeg om het tempo van technologische ontwikkelingen bij te houden met het tempo van het maken van wet- en regelgeving in een democratie.

Rechtsstaat in een verbonden wereld

Online bestaat er nog geen 'rule of law'-traditie, en is er veel onduidelijkheid over welke regels er gelden wanneer staten het internet als een wapen of middel van onderdrukking inzetten. Juridische duidelijkheid ontbreekt nu vaak omdat verschillende wetten van toepassing zijn, maar er ook sprake is van een juridisch vacuüm en nieuwe vragen over aansprakelijkheid, rechten en plichten. Het is belangrijk om helder inzichtelijk te maken hoe bestaande wetgeving op het gebied van mensenrechten, internationale handel, strafrecht of contractenrecht zodat het kan worden gehandhaafd over grenzen heen. Wanneer er geen afspraken worden gemaakt over normen waaraan staten zich houden, maar waaraan ook bedrijven gebonden zijn, dan dreigt een 'race to the bottom' en zelfs een digitale wedloop.

Ondanks technologische ontwikkelingen moeten het publieke belang, en principes zoals verantwoordlijkheden voor nationale veiligheid of het garanderen van mensenrechten, maar ook eerlijke concurrentie en democratische controle, worden gewaarborgd. Die principes en fundering van democratie en rechtsstaat zouden technologische revoluties moeten kunnen doorstaan. Wereldwijd leiderschap door open democratieën is essentieel als we willen voorkomen dat gesloten, top-down gecontroleerd bestuur de norm wordt.

In het kader van de Verenigde Naties wordt door staten onderling over normen gesproken die, vergelijkbaar met de regels voor de ruimte, de zee of oorlogsrecht, ervoor moeten zorgen dat er ten tijde van oorlog en vrede minimale afspraken over het gedrag van staten bestaan. Die afspraken zijn nu nog vrijwillig. Een van de belangrijkste gevolgen van het wereldwijd verbonden internet is de enorm grote wederzijdse afhankelijkheid van het functioneren van de basisinfrastructuur. Voor bedrijven en staten – of die nu democratisch zijn of niet – is het functioneren van het internet van grote waarde.

'Voor bedrijven en staten is het functioneren van het internet van grote waarde.'

Het vastleggen van internationale normen, waarin de centrale protocollen van het internet beschouwd worden als een neutrale zone die overheden niet mogen betreden of verstoren, kan een belangrijke eerste stap zijn naar een goed functionerend en veerkrachtig internet. Het verbieden van misbruik van de kernprotocollen van het internet is in het belang van alle staten en bedrijven, en natuurlijk van internetgebruikers. Het vertrouwen van gebruikers in de talloze *services* die op het internet worden aangeboden, van online-betalingen tot chatten, is immers van die veilige kernprotocollen afhankelijk. De Wetenschappelijke Raad voor het Regeringsbeleid adviseerde de Nederlandse regering dit tot speerpunt in ons buitenlandsbeleid te maken.

De rechtsstaat is geworteld in de natiestaat, plaatsgebonden door rechtsgeldigheid binnen de grenzen van een land. Regeringen kiezen in specifieke gevallen voor internationale afspraken, zoals op het gebied van handel en mensenrechten. Het vinden van antwoorden op de vraag over welk gebied rechtsmacht of jurisdictie geldt, in de context van een wereldwijd verbonden internet, is een enorme uitdaging. Daarbij moeten staten zowel nationaal als internationaal regels aanpassen en, misschien nog wel het belangrijkste, ze moeten het goede voorbeeld geven. Terwijl wetgeving vaak nog afwezig of niet volledig dekkend is, zijn ethische keuzes en moreel leiderschap des te belangrijker. Niets staat de machtige spelers op het internet in de

weg hun eigen verantwoordelijkheid te nemen om het gedeelde belang van het open internet te onderstrepen en mensen en hun welzijn voorop te stellen. Alleen dan is er een kans dat de belofte van het open internet ook in de toekomst wordt verwezenlijkt.

Auteurs

Marietje Schaake
Lid van het Europees Parlement namens D66
(https://www.marietjeschaake.eu/nl)