Een ‘responsible internet’: meer vertrouwen in het fundament van de digitale samenleving; een nieuwe manier van internet-communicatie

*Dr. ir. C.E.W. Hesselman**

120

Samenlevingen zijn in toenemende mate afhankelijk van digitale diensten, maar organisaties en individuen hebben steeds minder inzicht in en controle over hoe de onderliggende systemen met hun gegevens omgaan en wie ze beheert en produceert. Om dit probleem van afnemende ‘digitale soevereiniteit’ te helpen oplossen, ontwikkelen onderzoekers van verschillende universiteiten en internetorganisaties het nieuwe concept van een ‘responsible internet’. Dit is een fundamentele verandering van de internetinfrastructuur die gebruikers meer inzicht geeft in en controle over hun internetcommunicatie, in het bijzonder voor vitale diensten zoals ‘slimme’ energienetwerken.

Dit artikel is een herpublicatie van de blog ‘Een “responsible internet”: Meer vertrouwen in het fundament van de digitale samenleving’ van november 2020.[1] Het onderzoek vond plaats in het kader van het 2STiC[2]-onderzoeksprogramma (Security, Stability and Transparency in internetwork Communications). Het doel van 2STiC is het ontwikkelen en evalueren van mechanismen om de veiligheid, stabiliteit en transparantie van internetcommunicatie te vergroten, bijvoorbeeld door te experimenteren met en bij te dragen aan opkomende internetarchitecturen. Wetenschapsfinancierder NWO honoreerde de onderzoekers in april 2021 met 1.9 miljoen euro om een eerste versie van het responsible internet te starten vanuit Nederland.[3]

In dit artikel wordt het concept van een ‘responsible internet’ besproken, waarvan de auteurs verwachten dat het internetcommunicatie fundamenteel zal veranderen. Beargumenteerd wordt waarom een dergelijke beveiligingsuitbreiding nodig is om het probleem van de afnemende digitale soevereiniteit op te lossen. En tot slot worden de voordelen geschetst die het zal opleveren voor beleidsmakers, netwerkoperators en individuen. ‘Een verantwoord internet is de volgende fase in de evolutie van internet en het concept is ook bruikbaar voor schone internetsystemen’, volgens de onderzoekers. De auteurs hebben een achtergrond in technisch, policy- en business-modellen-onderzoek en zijn daarom erg geïnteresseerd in feedback vanuit de juridische gemeenschap.

1 Het maatschappelijke probleem: toenemende afhankelijkheid, afnemende soevereiniteit

Economieën en samenlevingen zijn in toenemende mate afhankelijk van digitale diensten. Dit omvat ‘gewone’ diensten zoals videovergaderen, dataopslag en ‘connected homes’, maar ook opkomende veiligheidskritische diensten zoals slimme energienetwerken, zelforganiserende bevoorradingsketens en ambulances die sensordata vooruitsturen naar het ziekenhuis.

Hoewel van dit soort diensten wordt verwacht dat ze de samenleving veiliger, slimmer en duurzamer maken, bestaat er over de hele wereld ook steeds meer bezorgdheid over de manier waarop ze de ‘digitale soevereiniteit’ van de samenleving aantasten. Dit komt doordat de onderliggende computersystemen en -netwerken (bijvoorbeeld algoritmen, DNS-diensten en netwerkapparatuur) steeds vaker elders worden gefabriceerd of beheerd, terwijl organisaties en individuen slechts een beperkt inzicht hebben in en controle hebben over hoe ze afhankelijk zijn van deze systemen. Dit is een probleem omdat het uiteindelijk de mogelijkheden van samenlevingen beperkt om autonoom te beslissen en te handelen over hoe ze hun digitale infrastructuur gebruiken, ervan afhankelijk zijn en hoe ze het inrichten. Dit vormt een risico voor publieke waarden als veiligheid, transparantie, privacy en democratie.

Het Europees Agentschap voor Cybersecurity (ENISA) onderstreepte onlangs in haar verslag over de digitale soevereiniteit van Europa het belang en de urgentie van

---

* **Cristian Hesselman is directeur van SIDN Labs. De overige auteurs staan vermeld aan het eind van het artikel. De oorspronkelijke tekst is in het Engels.**

1 sidnlabs.nl/nieuws-en-blogs/een-responsible-internet-meer-vertrouwen-in-het-fundament-van-de-digitale-samenleving.
2 2stic.nl.
3 nwo.nl/onderzoeksprogrammas/nationale-wetenschapsagenda-nwa/thematische-programmering-nwa/cybersecurity-0.

het probleem.[4] Ze benadrukte bijvoorbeeld dat de 15 grootste internetbedrijven ter wereld (bijv. Google, Facebook en Alibaba) afkomstig zijn uit de VS of China en niet uit Europa, en dat Europese technologiebedrijven vaak worden overgenomen door niet-Europese bedrijven (53 werden er tussen 2011 en 2016 bijvoorbeeld gekocht door Amerikaanse 'tech giants'). De risico's die het agentschap identificeert zijn onder meer dat Europa niet langer in staat is om aan de waarden en verwachtingen van haar burgers te voldoen, afnemende concurrentiekracht en het wegvloeien van technische expertise. De Australische regering heeft soortgelijke zorgen en gaat de afhankelijkheden van hun vitale IT-infrastructuur in kaart brengen in het kader van de 'Security of Critical Infrastructure Act'. Ze kijken daarbij bijvoorbeeld naar wie de eigenaren van bedrijven zijn, samenstelling van de toeleveringsketens en uitbestede projecten.[5]

2 Relevant in meerdere technische gebieden

Het probleem van afnemende digitale soevereiniteit wordt op verschillende manieren en in verschillende technologische gebieden aangepakt. Zo hebben Artificial Intelligence (AI)-onderzoekers ontwerprichtlijnen ontwikkeld om de beslissingen van AI-algoritmen transparanter en verklaarbaarder te maken door middel van wat zij 'responsible AI' noemen.[6] Op een vergelijkbare manier stimuleert de Europese Commissie de ontwikkeling van een Europese federatieve clouddienst met de naam 'GAIA-X', die de datasoevereiniteit van Europa moet verbeteren.[7] De Europese Commissie heeft onlangs ook verschillende beleidsinstrumenten in kaart gebracht voor gebieden als 5G-mobiele toegangsnetwerken en het 'internet of things'.[8]

Daarnaast vindt er op verschillende niveaus een intensiverend publiek debat plaats over digitale soevereiniteit, zoals te zien is aan recente publicaties in de reguliere media over publieke beleidsvorming, AI en datasoevereiniteit.[9]

3 De internetinfrastructuur is de leemte

Hoewel deze ontwikkelingen aangeven dat digitale soevereiniteit een algemeen erkend en urgent probleem is, stellen wij vast dat in deze discussie de internetinfrastructuur grotendeels ontbreekt: de technische systemen (zoals routers, switches en DNS-servers) die het mogelijk maken dat internetapparaten met elkaar kunnen communiceren en waar alle andere 'lagen' (beleidsvorming, AI, data) van afhankelijk zijn. De uitzondering is het debat over vermeende veiligheidskwetsbaarheden in 5G-apparatuur. Die vormen volgens de Europese Commissie een risico voor de strategische autonomie van de Europese Unie, maar 5G-netwerken omvatten alleen het mobiele toegangsgedeelte van de internetinfrastructuur.[10]

Het specifieke soevereiniteitsprobleem in de internetinfrastructuur is dat gebruikers geen inzicht hebben in of controle hebben over hoe zij afhankelijk zijn van netwerkoperators en hun systemen, wat uiteindelijk een ernstige beperking vormt voor overheden, instellingen, bedrijven en individuen om te beslissen hoe zij veilig kunnen communiceren. Dit is vooral relevant voor vitale dienstverleners (zoals elektriciteitsnetwerken, transportsystemen, mobiele netwerken en productiefaciliteiten), die steeds afhankelijker zijn geworden van computernetwerken. Dergelijke providers willen bijvoorbeeld weten of internet hun verkeer via netwerken routeert waarvan de apparatuur mogelijk backdoors heeft. Backdoors zijn mechanismes die bewust worden toegevoegd om (op afstand) toegang te krijgen tot apparatuur.

Tegelijkertijd zijn internetgebruikers 'by design' afhankelijk van derden, omdat internet een enorm gedistribueerd en mondiaal systeem is van zo'n 70.000 autonome netwerken. Zo maken gebruikers tijdens een typisch websitebezoek, zonder dat ze het weten, gebruik van de diensten van verschillende DNS-operators, transitproviders, clouddiensten en contentdistributie-aanbieders. Deze kunnen allemaal verschillende geografische locaties en verschillende jurisdicties hebben.

4 De visie: een responsible internet

Om deze leemte in de digital soevereiniteitsdiscussie op te vullen hebben we onlangs het concept van een 'responsible internet' ontwikkeld, een nieuwe 'security-by-design'-uitbreiding van internet (of toekomstige netwerken) die de gebruikers (zoals aanbieders van vitale diensten of individuen) extra securitygerelateerde mogelijkheden biedt waarmee ze meer grip krijgen op hun afhankelijkheden van internet en zo hun vertrouwen in en hun soevereiniteit over internetcommunicatie verhogen.[11]

Een responsible internet bereikt dit door zijn netwerken transparanter, verantwoordingsplichtiger en beter controleerbaar te maken. Dit betekent dat gebruikers een responsible internet kunnen vragen om hoog-niveaubeschrijvingen van de ketens van netwerkoperators (bijv. ISP's, datacenters en DNS-operators) die mogelijk hun

4 enisa.europa.eu/publications/enisa-position-papers-and-opinions/eu-ict-industry-consultation-paper.
5 homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf.
6 itu.int/en/journal/001/Documents/itu2017-1.pdf.
7 data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-the-european-project-kicks-of-the-next-phase.pdf?__blob=publicationFile&v=6.
8 eitdigital.eu/newsroom/news/archive/article/new-report-on-european-digital-infrastructure-and-data-sovereignty.
9 foreignaffairs.com/articles/world/2020-10-13/lawless-realm en nrc.nl/nieuws/2018/04/27/eu-dreigt-digitale-kolonie-te-worden-a1601157 en vpro.nl/programmas/tegenlicht/kijk/afleveringen/2019-2020/herover-je-data.html.
10 eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0534.
11 sidnlabs.nl/downloads/2v6sEqlLniF GTWbbKqTvhx/ee9f96134c0607c67 efe40940039cd76/Hesselman_et_al-2020-Journal_of_Network_and_Systems_Management.pdf.

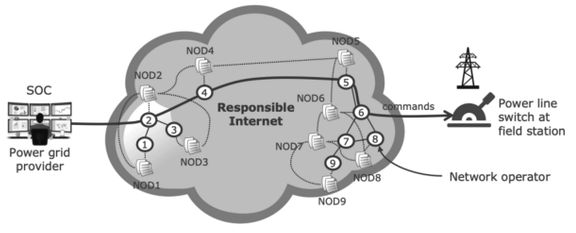
datastromen afhandelen, bijvoorbeeld in termen van hun beveiliging en administratieve eigenschappen, onderlinge relaties en beheerswerkzaamheden die ze hebben uitgevoerd (transparantie). Een responsible internet stelt gebruikers in staat om te controleren of deze gegevens accuraat zijn (verantwoordingsplicht) en om vervolgens de infrastructuur opdracht te geven hun datastromen op een specifieke manier te behandelen, bijvoorbeeld door ze alleen via netwerkoperators met bepaalde verifieerbare beveiligingseigenschappen te laten lopen (controleerbaarheid).

Onze notie van een responsible internet is geïnspireerd op responsible AI, een ontwerpparadigma dat zich erop richt om mensen meer inzicht te geven in hoe AI-systemen tot beslissingen komen en waarom, bijvoorbeeld voor vrijlatingen op borgtocht en luchtvervuilingsbeslissingen.[12]

5 Illustratief voorbeeld: smart grid

Figuur 1 laat een voorbeeld zien waarin een aanbieder van een 'smart' grid (links) zijn diensten bouwt op een responsible internet (de grijze wolk in het midden).[13] De gridaanbieder gebruikt een Security Operations Center (SOC) om zijn elektriciteitsfaciliteiten in het veld (rechts) op afstand te bedienen, bijvoorbeeld om stroomleidingen aan of af te sluiten.

In een responsible internet kan het SOC details tonen over de veiligheidskenmerken van de keten van netwerkoperators die de commando's transporteren waarmee het SOC de veldstations bedient (netwerkoperators 2, 4, 5 en 6) of die deze mogelijkerwijs kunnen transporteren (1, 3, 7, 8 en 9), zelfs als de gridaanbieder geen zakelijke relatie met hen heeft. Zo koopt de gridaanbieder in figuur 1 internetconnectiviteit van netwerkoperator 2 voor zijn SOC en van operator 6 voor de connectiviteit in de elektriciteitsstations, maar het SOC kan van de andere netwerkoperators ook een beschrijving opvragen.



Figuur 1. Voorbeeld: gridaanbieder die een responsible internet gebruikt. NOD is een afkorting van Network Operator Description (bijv. NOD4 voor operator 4).

Een netwerkoperatorbeschrijving is een automatisch te verwerken elektronisch document dat betrekking heeft op de eigenschappen van een operator die van invloed kunnen zijn op de manier waarop de operator met datastromen omgaat. Voorbeelden hiervan zijn beveiligingseigenschappen (bijvoorbeeld als de operator het mogelijk maakt om op afstand de veiligheid van zijn routersoftware te verifiëren), administratieve eigenschappen (zoals jurisdictie en geolocatie), relaties met andere netwerkoperators (bijvoorbeeld outsourcingrelaties) en wijzigingen die de operator aan zijn infrastructuur heeft doorgevoerd (bijvoorbeeld beveiligingspatches van routers). Het SOC in figuur 1 zou bijvoorbeeld de beschrijvingen van operators 2, 4, 5 en 6 kunnen gebruiken om te controleren of de routersoftware op het pad naar het veldstation geen backdoors bevat (transparantie) en om te controleren of al deze 4 operators de nieuwste beveiligingspatches op hun routers hebben geïnstalleerd (verantwoordingsplicht).

Het SOC-team gebruikt vervolgens de beschrijvingen van de netwerkoperators om het responsible internet te instrueren de commando's voor veldstations te transporteren via een keten van netwerkoperators die voldoen aan de eisen van het SOC, zoals dat de routers op het pad geen bekende kwetsbaarheden bevatten en gecontroleerd zijn op backdoors.

6 Een nieuwe manier van internetcommunicatie

Een responsible internet verandert de manier waarop organisaties en individuen over internet communiceren fundamenteel, omdat internet momenteel niet de mogelijkheden ondersteunt die het SOC uit figuur 1 ter beschikking staan. In plaats daarvan is internet een 'black box' die gebruikers alleen toestaat om het eindpunt te specificeren waar het netwerk de gegevens naartoe moet sturen. Het pad wordt bepaald door mechanismen buiten de controle van de gebruiker en zelfs buiten de controle van de netwerkoperators. In het voorbeeld van figuur 1 betekent dit dat de gridaanbieder meestal niet weet van welke netwerkoperator zijn diensten afhankelijk zijn en dat hij weinig controle heeft over welke soorten operators hij zijn verkeer het liefst zou laten transporteren (bijvoorbeeld op basis van de veiligheidseigenschappen van de netwerkoperators).

Tegelijkertijd blijft een responsible internet zoals wij dat voor ons zien het open, bottom-up en multistakeholderkarakter van internet volgen. Ons concept van soevereiniteit gaat over serviceproviders en individuen die meer controle hebben over hun afhankelijkheden van de internetinfrastructuur. Het gaat uitdrukkelijk niet om het creëren van door de overheid gecontroleerde of zelfs geïsoleerde nationale netwerken (zoals het 'Pekingse internet' of het 'Moskouse internet'), of om het uitsluiten van technologieën uit specifieke regio's.[14]

7 Een responsible internet komt ten goede aan een breed scala van gebruikers

Het verbeterde palet van veiligheidsgerelateerde mogelijkheden van een responsible internet biedt niet alleen

12 itu.int/en/journal/001/Documents/itu2017-1.pdf.
13 research.utwente.nl/en/publications/process-aware-scada-traffic-monitoring-a-local-approach.
14 dl.acm.org/doi/pdf/10.1145/3341722.

voordelen voor vitale dienstverleners zoals de gridaanbieder in figuur 1, maar ook voor beleidsmakers, netwerkoperators en uiteindelijk ook individuele personen.

Beleidsmakers: de netwerkbeschrijvingen die een responsible internet biedt, maken een meer datagestuurde en proactieve manier van beleidsvorming, bemiddeling en handhaving mogelijk. Ze stellen nationale beleidsmakers bijvoorbeeld in staat om risicogebieden in hun lokale internetinfrastructuur (bijvoorbeeld machtsconcentraties) te analyseren op basis van historische gegevens.[15] Ook kunnen beleidsmakers netwerkbeschrijvingen invoeren in een platform dat aanbieders van vitale infrastructuren (bijvoorbeeld gridaanbieders en transportsystemen) in staat stelt feedback te geven over de veiligheid van de netwerkoperators op basis van empirische data.

Netwerkoperators hebben baat bij een responsible internet omdat de netwerkbeschrijvingen hen in staat stellen om grootschalige beveiligingsincidenten proactiever af te handelen. Een netwerkoperator in een responsible internet kan bijvoorbeeld in zijn beschrijving metadata opnemen die aangeven welke metingen hij verricht bij de DDoS-aanvallen die hij heeft opgevangen. Hierdoor wordt het voor andere operators veel gemakkelijker om datasets over dergelijke aanvallen te vinden, waardoor ze betere en tijdigere beveiligingsinformatie kunnen verkrijgen. Uiteindelijk stelt dit netwerkoperators in staat om betere beveiligingsbeslissingen te nemen en de beveiliging en veerkracht van hun diensten en die van hun klanten te vergroten. Een responsible internet bouwt een dergelijke gezamenlijke aanpak van internetbeveiliging in het netwerk in.[16]

Individuen: op de lange termijn verwachten we dat ook individuen baat hebben bij een responsible internet. Gebruikers van videoconferenties zouden bijvoorbeeld een responsible internet kunnen vragen om te laten zien waar hun videostromen terechtkomen en hun eindpunt mogelijk veranderen naar een datacenter in een andere regio. Videoconferencetool Zoom voegde een dergelijke functie pas aan hun dienst toe als reactie op zorgen over de veiligheid van de dienst, zoals over de opslag van cryptografisch materiaal in datacenters buiten 'vriendelijke' jurisdicties.[17] In een responsible internet zouden dit soort faciliteiten integraal onderdeel zijn van de netwerkinfrastructuur en dus beschikbaar zijn voor alle toepassingen, inclusief Zoom.

Meer informatie:

Op de website van SIDN Labs is ook een vervolgblog te vinden over de technische en niet-technische onderzoeksuitdagingen die overwonnen moeten worden om een verantwoord internet te realiseren.[18]

Het gedetailleerde wetenschappelijke artikel (in het Engels) is daar ook te vinden.[19]

De auteurs hebben een achtergrond in technisch, policy- en businessmodellen-onderzoek en zijn daarom erg geïnteresseerd in feedback vanuit de juridische gemeenschap.

Overige auteurs: Paola Grosso (3), Ralph Holz (2), Fernando Kuipers (4), Janet Hui Xue (5), Mattijs Jonker (2), Joeri de Ruiter (1), Anna Sperotto (2), Roland van Rijswijk-Deij (2, 6), Giovane C.M. Moura (1, 4), Abhishta Abhishta (2), Luca Allodi (7), Chrysa Papagianni (3), Bart Nieuwenhuis (2), Aiko Pras (2) en Cees de Laat (3)

1 SIDN Labs, 2 Universiteit Twente, 3 Universiteit van Amsterdam, 4 Technische Universiteit Delft, 5 Wolfson College, Oxford University, UK, 6 NLnet Labs, 7 Technische Universiteit Eindhoven

Dit onderzoek maakt deel uit van het 2STiC-onderzoeksprogramma (Security, Stability and Transparency in internetwork Communications). Website: 2stic.nl.

SIDN en de Universiteit Twente zijn medegefinancierd door het onderzoeks- en innovatieprogramma Horizon 2020 van de Europese Unie in het kader van subsidieovereenkomst nr. 830927. Projectwebsite: concordia-h2020.eu.

De Universiteit van Amsterdam werd gefinancierd door de Nederlandse Stichting voor Wetenschap in het programma Commit2Data (subsidienummer: 628.001.001). Projectwebsite: dl4ld.nl.

15 tandfonline.com/doi/full/10.1080/23738871.2020.1740753.
16 sidnlabs.nl/nieuws-en-blogs/impuls-voor-wetenschappelijk-onderzoek-naar-collectieve-internetbeveiliging.
17 blog.zoom.us/coming-april-18-control-your-zoom-data-routing/.
18 sidnlabs.nl/nieuws-en-blogs/een-responsible-internet-de-uitdagingen.
19 sidnlabs.nl/downloads/2v6sEqlLniF GTWbbKqTvhx/ee9f96134c0607c67 efe40940039cd76/Hesselman_et_al-2020-Journal_of_Network_and_Systems_Management.pdf.