Een open, toegankelijk en betrouwbaar Internet

SURF Position paper op het gebied van Internet Governance

Utrecht, april 2016
Versienummer: 1.3

Colofon

Een open, toegankelijk en betrouwbaar Internet

SURF
Postbus 19035
NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl
www.surf.nl

SURF is de ICT-samenwerkingsorganisatie van het Nederlandse hoger onderwijs en onderzoek.
Deze publicatie is digitaal beschikbaar via de website van SURF: www.surf.nl/publicaties

Inhoudsopgave

Inleiding

SURF zorgt ervoor dat studenten, docenten, onderzoekers en medewerkers eenvoudig, betrouwbaar en grenzeloos kunnen werken en samenwerken met de best mogelijke ICT-voorzieningen. In de visie van SURF versterken excellente ICT-voorzieningen toponderzoek en onderwijs. Het Internet speelt hierbij een belangrijke rol en heeft zich ontwikkelt tot een onmisbaar instrument. SURF wil ervoor zorgen dat de mogelijkheden van het Internet voor onderzoek en onderwijs zich zo goed mogelijk ontwikkelen en beschikbaar blijven.

SURFnet is de werkmaatschappij binnen de SURF-coöperatie die onder andere de internetdiensten voor haar leden verzorgt. De inrichting van de internetdienst en daarmee de waarde van deze dienst voor de leden wordt niet alleen bepaald door de keuzes die SURF zelf maakt maar hangt samen met de positie van het Internet in groter verband. Vanuit deze optiek spreekt het vanzelf dat SURF namens haar leden actief deelneemt aan de discussie rondom Internet Governance en haar visie en standpunten daar inbrengt. SURF behartigt in deze discussie de belangen van de leden door een open, toegankelijk en betrouwbaar Internet voor iedereen voor te staan waarbij de rechten van gebruikers, zoals op het gebied van privacy, gerespecteerd worden. SURF werkt op dit gebied samen met Europese NRENs (National Education and Research Network), met GÉANT (Europese vereniging van NRENs) en netwerken wereldwijd.

Het is van belang dat er draagvlak is onder de leden over de visie die SURF uitdraagt. Deze position paper dient als basis voor dat draagvlak en maakt duidelijk welke positie SURF in zal nemen in het maatschappelijk debat rondom Internet Governance (beheer, beheersing, besturing en regulering van het Internet).

1. Positiebepaling

SURF wil excellente en geavanceerde diensten aan haar leden leveren door continue te investeren in innovatie en verbetering van netwerken. In de visie van SURF kunnen onderzoekers en docenten op hun vakgebied het meest vooruitstrevend zijn als ze gebruik maken van de meest geavanceerde ICT-voorzieningen. Het gaat hier niet alleen om een technisch geavanceerd netwerk, maar ook om een netwerk dat je als student, docent of onderzoeker kunt vertrouwen en dat waarborgen biedt met betrekking tot privacy.

SURF streeft naar een zo open, toegankelijk en betrouwbaar mogelijk Internet, waar onderzoekers, studenten en docenten in alle vrijheid veilig hun werk kunnen doen. Hierbij is het belangrijk dat SURF haar netwerk, dataverwerking en diensten kan blijven optimaliseren door in vrijheid beslissingen te kunnen nemen over de inrichting van haar netwerk en diensten.

Op basis van bovengenoemd uitgangspunt kiest SURF voor de volgende positie:

- **Werk continu aan een veilig en betrouwbaar Internet waar de privacy van de gebruiker gerespecteerd wordt:**

  Bij de ontwikkeling van haar internetdiensten speelt veiligheid en betrouwbaarheid een cruciale rol, SURF verzet zich tegen ontwikkelingen die het internet minder veilig en betrouwbaar maken.

  SURF heeft als aanbieder van diensten een zorgplicht jegens haar gebruikers. Een zorgplicht met betrekking tot de veiligheid en betrouwbaarheid van onze diensten inclusief grondrechten van onze gebruikers zoals privacy.

  SURF werkt waar mogelijk samen met overheden en bedrijfsleven aan het veilig houden van Internet en bestrijden van cyberterrorisme en cybercriminaliteit. De samenwerking zorgt ervoor dat kennis en capaciteiten gebundeld kunnen worden, en snel en effectief kan worden gereageerd op grootschalige cybersecurity-incidenten. SURF doet dit zowel binnen Nederland, als met Europese NRENs (National Education and Research Network) in GÉANT en netwerken wereldwijd. SURF draagt bij met kennis en middelen binnen de kaders van de Nederlandse wet en met een oog voor de proportionaliteit wat betreft de impact op de leden en de gebruikers.

- **Bescherm de publieke kern tegen politieke en commerciële invloeden:**

  De centrale protocollen en infrastructuren van het Internet moeten als een mondiaal publiek goed beschouwd worden. Deze publieke kern van het Internet moet gevrijwaard blijven van oneigenlijke interventies van overheden en andere partijen die schade toebrengen en het vertrouwen in het Internet eroderen. Het recente rapport van de Wetenschappelijke Raad van het Regeringsbeleid (WRR)[1]onderkent het belang van een universele, interoperabele en toegankelijke kern van het Internet. De WRR stelt dat de vrijheid en openheid van Internet voor iedereen die mee wil doen geborgd moet blijven. SURF onderschrijft de WRR-conclusie dat vertrouwen in de publieke fundamenten van het Internet essentieel is:

  "Het Internet als publiek goed functioneert alleen als het de kernwaarden universaliteit, interoperabiliteit en toegankelijkheid garandeert en als het de kerndoelen van informatieveiligheid, te weten vertrouwelijkheid, integriteit en beschikbaarheid ondersteunt."

[1] *De publieke kern van het Internet*, publicatie van de Wetenschappelijke Raad voor het Regeringsbeleid, 2015

Gebruikers moeten op de werking van de meest fundamentele protocollen van het Internet kunnen vertrouwen omdat daar ook het vertrouwen van afhangt dat we hebben in het sociaaleconomische bouwwerk dat daarbovenop gebouwd is.

In lijn hiermee concludeert het WRR-rapport dat overheden uiterst terughoudend moeten zijn met beleid, wetgeving en operationele activiteiten die ingrijpen in de kernprotocollen van het Internet. Dit geldt eveneens voor de private partijen die ten aanzien van deze publieke kern een spilfunctie vervullen. Een belangrijk uitgangspunt hierbij moet gevonden worden in proportionaliteit van de maatregelen die getroffen worden, in vergelijking van de gevaren waar tegen deze maatregelen moeten beschermen.

2. Wat gaat SURF doen?

SURF wil zich actief opstellen bij de thema's gerelateerd aan de positiebepaling die de komende jaren actueel zijn. SURF agendeert deze thema's in haar projecten, bij de ondersteuning van haar leden en in haar overleg met andere organisaties over verdere ontwikkeling van het Internet. Dit betekent:

- Deelname aan het publieke debat en consultaties namens de leden
  SURF zal participeren in debatten met overheden en andere partijen opdat die zich onthouden van, of tenminste terughoudend zijn bij, activiteiten die ingrijpen op de publieke kern van het Internet of die consequenties hebben voor de betrouwbaarheid van het Internet en de privacy van gebruikers. Indien wetvoorstellen relevantie hebben voor bovengenoemde thema's zal SURF zal alles in het werk stellen haar invloed aan te wenden.

- Aangaan van samenwerkingsverbanden
  SURF zal participeren in samenwerkingsverbanden die bijdragen aan een open, toegankelijk en betrouwbaar internet waartoe zeker ook behoort het meewerken aan de noodzakelijke bescherming van het Internet tegen cybercriminaliteit en –terrorisme, in balans met respect voor grondrechten van gebruikers (zoals privacy, toegankelijkheid, keuzevrijheid etc.). Voorbeelden van dergelijke samenwerkingsverbanden zijn: DINL (Digitale Infrastructuren Nederland), ISOC (Internet Society), ICANN (Internet Cooperation for Assigned Names and Numbers), NCSC Stakeholders overleg, enzovoorts.

Bijvoorbeeld

In de zomer van 2015 publiceerde het ministerie van BZK een wetsvoorstel voor Inlichtingen en Veiligheidsdiensten (WIV) en biedt middels een consultatie burgers en organisaties de mogelijkheid om te reageren op het voorstel. In het wetsvoorstel staan vergaande bevoegdheden voor Inlichtingendiensten die de privacy van Internetgebruikers en de bescherming van databestanden aantasten. Samen met 556 anderen reageerde SURF op het wetvoorstel namens haar leden.

Het standpunt van SURF is dat de aantasting van de privacy proportioneel moet zijn met de maatschappelijke opbrengst van de maatregelen. SURF maakt zich ook sterk voor een goede bescherming van databestanden (zonder gerechtelijk bevel geen toegang), zodat onderzoekers die werken met gegevens van (proef)personen zich verzekerd weten van een goede bescherming van die gevoelige gegevens. Tot slot neemt SURF het standpunt in dat het in vrijheid een optimale architectuur voor haar netwerk moet kunnen implementeren dat onderzoekers, docenten en studenten op de beste wijze bedient. Het mogelijk beperken van die vrijheid ten behoeve van de werkzaamheden van de Inlichtingen en Veiligheidsdiensten brengt onnodige beperkingen en hoge kosten met zich mee.

3. Kansen en bedreigingen voor een open, toegankelijke en betrouwbaar Internet

De ontwikkeling van het Internet biedt kansen en bedreigingen. De belangrijkste kansen zijn samen te vatten in de volgende vier ontwikkelingen:

- *Internet of People*: Door toenemende toetreding van nieuwe gebruikers kan er nog breder kennis gedeeld worden en nieuwe inzichten verkregen worden; al deze gebruikers genereren ook data en hebben toegang tot kennis die online beschikbaar is;

- *Internet of Things*: Door steeds meer connected 'things' (sensoren, actoren) wordt er steeds meer gemeten in onze omgeving en komen nog meer data beschikbaar, en kan het Internet direct bijdragen aan een leefbaarder en veiliger samenleving op een manier die voorheen niet (meer) betaalbaar was door inzet van gekoppelde systemen;

- *Internet of Data:* Door bovenstaande ontwikkelingen en door betere ontsluiting komen meer data voor onderzoek en ontwikkeling beschikbaar. Belangrijk is hierbij de mens centraal te laten staan;

- *Awareness:* Steeds meer gebruikers zijn zich bewust van de gevaren van het Internet. Onthullingen zoals die van Snowden betreffende de praktijken van de Amerikaanse overheid en rondom gegevensgebruik door Facebook hebben geleid tot een toenemende bewustwording. Dat heeft vervolgens er toe geleid dat ook bedrijven zich steeds meer bewust zijn van hun rol in het betrouwbaar houden van het Internet, dus ook het netjes omgaan met persoonsgegevens. De recente rechtszaak in de VS tussen de FBI en Apple over het ontsleutelen van een iPhone is daar een voorbeeld van. Hierdoor ontstaan nieuwe innovaties, zoals b.v. die van privacy-enhanced technology, die het Internet betrouwbaarder maken.

Deze ontwikkelingen, gebaseerd op openheid en toegankelijkheid, maken het Internet sterk, maar ook kwetsbaar. Vertrouwen in het Internet is belangrijk, maar er zijn ontwikkelingen die dat ondermijnen. Oorspronkelijk werd het Internet ontwikkeld om samen te kunnen werken op niet-commerciële basis, maar vandaag de dag wordt het Internet in alle lagen en sectoren van de samenleving gebruikt, voor allerlei toepassingen. Door het toenemende sociale, economische en politieke belangen van het Internet in de samenleving neemt de druk op het Internet aan alle kanten toe. Bedreigingen die zich ontwikkelen en die ten koste gaan van de betrouwbaarheid en het vertrouwen in het Internet zijn:

- *Criminaliteit en terrorisme*: zowel cyber-criminaliteit als "gewone" criminaliteit maakt steeds meer gebruik van het Internet. Je kunt vanaf bijna elke fysieke locatie verbinding maken met het Internet waardoor het mogelijk wordt misdrijven en misdaden te begaan zonder fysiek aanwezig te moeten zijn. Nieuwe criminaliteit komt op, waaronder identiteitsdiefstal, cyberspionage, cyberpesten en cyberafpersing (ransomware). Maar ook het 'storen' van Internet of diensten op het Internet door zogenaamde Distributed Denial of Service (DDoS) aanvallen worden steeds meer gemeengoed;

- *Commerciële activiteiten:* door de nieuwe mogelijkheden ontstaan nieuwe bedrijfsmodellen die soms voorbijgaan aan menselijke waarden zoals privacy en keuzevrijheid. Surfgedrag, voorkeuren en meningen worden door allerhande bedrijven in kaart gebracht, gericht op commercieel gewin. Daarnaast ligt er een hoge nadruk op "time-to-market" van nieuwe producten, diensten en bijvoorbeeld software releases. Dat gaat ten koste van kwaliteit en betrouwbaarheid van hard- en software, wederom zonder dat de gebruiker hierover goed geïnformeerd wordt. De hieruit voortkomende kwetsbaarheden kunnen tot teleurstellingen bij gebruikers leiden, en kunnen door criminelen misbruikt worden;

- *Regulering en optreden door de overheid*: door gebruik te maken van massa-surveillance en aantasten van de technische integriteit van het Internet (door het inbouwen van “achterdeurtjes” waardoor beveiligingen omzeild kunnen worden). Door het invoeren van allerlei vormen van wetgeving die de vrijheid van het inrichten en vormgeven van netwerken disproportioneel vermindert en bijvoorbeeld encryptie tracht te verbieden, of de exploitatiekosten onevenredig opdrijft.

Deze kansen en bedreigingen leiden tot de huidige maatschappelijke discussies rondom Internet Governance en zijn daarmee de reden dat SURF namens haar leden een positie wil innemen in die debatten.

4. Het publieke debat

Bovengenoemde ontwikkelingen brengen een aantal concrete thema's met zich mee die onderdeel zijn van het publieke debat of dat zouden moeten zijn. Hieronder zijn de actuele thema's weergegeven waar SURF vanuit haar positiebepaling aan bijdraagt:

- *De organisatie van de Internet Governance zelf:* Hoe wordt de governance geregeld? Welke organisaties krijgen daarin een stem? In lijn met de WRR zet SURF hier in op een multi-stakeholder benadering. Niet één organisatie of één groep van belanghebbenden, maar alle belanghebbenden moeten een stem hebben;

- *Open data, big data, data analytics*: bij het delen van data moet een evenwicht gevonden worden tussen het belang van individuele personen (bescherming van privacy en keuzevrijheid) en het belang van de maatschappij om commercieel en/of maatschappelijk voordeel te halen bijvoorbeeld in onderzoek of onderwijs;

- *Toenemende digitalisering van de samenleving*: Steeds meer objecten worden gekoppeld aan het Internet. Deze 'dingen' worden gebruikt om data te verzamelen, te delen, en om taken uit te voeren die data- en/of signaal gestuurd zijn. Zo ontstaan "lerende omgevingen" die ervoor zorgen dat onze wereld en het handelen in onze wereld in toenemende mate gedigitaliseerd wordt. Dit biedt ongekende mogelijkheden voor nieuw onderzoek en onderwijs die zo min mogelijk moeten worden beperkt;

- *Aantasting van privacy*: Voorgaande twee punten leiden tot een toenemende druk op privacy van gebruikers, maar ook van mensen over wie onderzoekers data verzamelen. Door de digitalisering van gegevens worden data eenvoudig in een andere context gebruikt dan waarvoor ze oorspronkelijk verzameld waren. Daarmee wordt mogelijk de privacy aangetast. Het ontwerpen van diensten en databeheer met een oog voor privacy is dus van belang ("*privacy by design*") naast het investeren in Privacy Enhancing Technologies en het aanbieden van assessment tools;

- *Beperkingen aan de groei van het Internet*: bijvoorbeeld door een schaarste aan adressen. Groei van Internet moet zo ongehinderd mogelijk voortgang kunnen vinden. Dat is o.a. noodzakelijk voor toepassing van Internet of Things binnen onderzoek;

- *Zekeren van beveiliging (security)* van toegang tot data, datastromen en van toegang tot systemen die taken uitvoeren is uitermate belangrijk, waarbij de veiligheid steeds verder moet verbeteren – hierbij wordt onderkend dat "aanvallen" steeds geavanceerder worden, en systemen zo ingericht zullen moeten worden dat de beveiliging steeds verder verbeterd kan worden;

- *Zekeren van veiligheid (safety)* van instituten, gebruikers en systemen die via en dankzij het Internet functioneren.

5. Omgang met dit Position paper

Over de ontwikkelingen op het gebied van Internet Governance zal SURF regelmatig het gesprek aangaan met de leden, waaronder in ieder geval:

- 1 keer per jaar in de ledenraad;
- 1 a 2 keer per jaar met de Coördinerend SURF Contactpersonen (CSCs).

Verder zal het onderwerp aan bod komen tijdens de reguliere bijeenkomsten van de Programma Advies Raad (PAR) van het programma Betrouwbare en Veilige Omgeving. Dit position paper is bedoeld als een document dat waar nodig zal worden geüpdatet. Als zodanig biedt het een helder en actueel uitgangspunt wanneer nieuwe ontwikkelingen op het gebied van Internet Governance beschouwd (moeten) worden die SURF, haar leden en/of haar eindgebruikers raken.