Stratix

Stratix Rapport

Internetinfrastructuur: standaardisatie, techniek en geopolitiek

RAPPORT

Uitgebracht aan:
Agentschap Telecom

Hilversum, 9-3-2022

Stratix

Managementsamenvatting

Standaardisatie heeft in zijn algemeenheid een positief effect voor de marktwerking. Standaarden maken interoperabiliteit van apparatuur mogelijk, waardoor afnemers meer keuzevrijheid krijgen en concurrentie wordt gestimuleerd. Bovendien maken standaarden het mogelijk om heterogene netwerken aan elkaar te koppelen. Idealiter bevorderen standaarden daarbij – juist door vastleggen van de koppelvlakken – diversiteit en innovatie rond die koppelvlakken.

De opdracht

Agentschap Telecom vroeg Stratix om de huidige technische ontwikkelingen in kaart te brengen rondom internetarchitectuur en standaardisatie daarvan, de maatschappelijke waarden die daarmee gemoeid zijn, en de daarmee gepaarde geopolitieke en governance ontwikkelingen. Agentschap Telecom wil met de uitkomsten van dit onderzoek gesprekken aangaan met stakeholders in binnen- en buitenland over het behoud van een vrij en open internet en over de rol die Agentschap Telecom in de multistakeholder-community kan vervullen.

De scope van deze opdracht was beperkt tot de internet- en transportlagen van de internetarchitectuur. De bekendste standaarden voor deze lagen zijn die voor TCP/IP (de basis van het internet). Daarnaast is ook een klein deel van de standaarden voor mobiele netwerken (zoals UMTS, LTE of 5G) relevant voor deze lagen. Het grootste deel van die mobiele standaarden betreft echter de interne werking van de mobiele netwerken, en valt daarmee buiten de scope van dit onderzoek.

Standaardisatie, maatschappelijke waarden en geopolitiek

Op het gebied van netwerken is een groot aantal standaardisatieorganisaties actief, maar binnen de scope van deze opdracht zijn vooral de Internet Engineering Task Force (IETF) en (voor mobiel) het Third Generation Partnership Program (3GPP) bepalend. De laatste jaren zijn er weinig verschuivingen wat betreft de invloed van standaardisatieorganisaties, al zijn er wel partijen die proberen om via andere standaardisatieorganisaties invloed uit te oefenen op de internet architectuur.

De normen en waarden die de standaardisatie sturen zijn vooral technisch gedreven. Bredere normen en waarden, zoals respect voor de mensenrechten en voor specifieke politieke waarden, spelen wellicht indirect mee, maar worden in het proces meestal niet expliciet benoemd.

Geopolitiek heeft tot nu toe nog weinig invloed op de standaardisatie, ondanks de toenemende participatie vanuit enkele landen die in het verleden minder sterk betrokken waren, zoals China. Deelnemers uit deze landen zijn vooralsnog niet in staat om de richting te bepalen, terwijl de actieve participatie vanuit meer landen in internationale standaardisatie de legitimiteit van standaarden juist versterkt. Daarentegen hebben sommige grote marktpartijen wel bijzonder veel invloed. De standaardisatie van QUIC, een recente ontwikkeling vanuit Google, was bijvoorbeeld alleen mogelijk omdat Google controle had over de grootste browser ter wereld én over een groot Content Distributie Netwerk.

Vraagstukken en oplossingen

Voor het onderzoek heeft Stratix, op basis van gesprekken met experts op dit gebied, een top-tien opgesteld van de belangrijkste vraagstukken (binnen de gegeven scope). Kort geformuleerd zijn dat de volgende vraagstukken, waarbij wij voor meer informatie naar het hoofddocument verwijzen:

1. BGP route hijacking
2. IP-spoofing
3. Traffic shaping/netneutraliteit
4. Weinig zicht op ongewenste content
5. Interceptie van de inhoud
6. Interceptie van metagegevens
7. Zeggenschap op verkeer (soevereiniteit)
8. Innovatie, flexibiliteit en veranderbaarheid van de infrastructuur
9. Gebrek aan mogelijkheden voor duurzaamheid
10. Gebrek aan Quality of Service

Per vraagstuk heeft Stratix vervolgens onderzocht welke waarden relevant zijn, welke oplossingen worden voorgesteld, en hoe kansrijk deze oplossingen zijn.

Voor enkele van de onderzochte vraagstukken is er sprake van conflicterende waarden. Een voorbeeld is het vraagstuk "zicht op ongewenste content": de legitieme behoefte van overheden om bepaalde content te blokkeren of er in elk geval zicht op te hebben (denk bijvoorbeeld aan kinderporno, aanzetten tot haat, of illegale distributie van auteursrechtelijk beschermde werken) is gebaseerd op algemeen erkende waarden, maar conflicteert tegelijkertijd ook met andere erkende waarden zoals privacy en anonimiteit. Een extra complicatie daarbij is dat elk mechanisme dat een overheid in een democratische rechtstaat meer zicht op content geeft, met alle waarborgen die daarbij horen, net zo gemakkelijk door autocratische overheden gebruikt kan worden op manieren die conflicteren met de mensenrechten. Het is feitelijk niet mogelijk om een technische standaard te definiëren die daar onderscheid in kan maken.

Er wordt voor alle onderzochte vraagstukken zowel aan incrementele oplossingen (stapsgewijze wijzigingen of aanvullingen op bestaande standaarden) als aan radicale oplossingen ("clean slate" internet ontwerpen) gewerkt.

Over het algemeen kan gesteld worden dat de genoemde incrementele oplossingen volwassener en kansrijker zijn dan de voorstellen voor meer radicale oplossingen. Zelfs als die radicale oplossingen voldoende schaalbaar zouden zijn, en de gepercipieerde problemen op zouden lossen (wat allebei discutabel is), dan nog is het implementeren van deze oplossingen als vervanging voor het internet door de grote "installed base" effectief niet haalbaar. Deze initiatieven zijn, als de onderzoeksresultaten breed gedeeld worden, wel waardevol voor een beter begrip van de werking van netwerken, en kunnen daardoor leiden tot betere (incrementele) oplossingen in de bestaande standaarden.

Implementatie van standaarden

Het succes van internetstandaarden wordt bepaald door de implementatie in apparatuur, en vervolgens het daadwerkelijke gebruik ervan in netwerken. In sommige gevallen hebben

fabrikanten een standaard wel geïmplementeerd, maar maken de beheerders van netwerken nog niet of nauwelijks gebruik van de standaard. IPv6 is hier een typisch voorbeeld van.

Invloed vanuit de overheid

Voor de Nederlandse overheid, en voor Agentschap Telecom in het bijzonder, is het belangrijk om kennis te behouden omtrent de belangrijkste standaardisatieorganisaties en -processen, en er indirect invloed op uit te oefenen door een dialoog met de diverse betrokkenen. Nederland heeft als geheel al een relatief grote invloed op standaardisatie, maar die invloed vindt, wat betreft de multi-stakeholder organisaties, niet rechtstreeks via de overheid plaats. Juist langs deze indirecte weg kan de overheid de waarden die Nederland belangrijk vindt, in de standaardisatie helpen borgen.

Overheden kunnen daarnaast de implementatie van relevante standaarden stimuleren, door voorlichting, door de standaard voor te schrijven bij de verwerving van systemen, en in sommige gevallen zelfs door standaarden dwingend voor te schrijven in regelgeving.

Management Summary

Standardisation generally has a beneficial impact on markets. Standards make interoperability of equipment possible, thus stimulating user choice and increasing competition. Standards also enable connections between heterogeneous networks. In the ideal case, by defining the interfaces between networks, standards lead to more diversity and innovation around these interfaces.

The assignment

Radiocommunications Agency Netherlands requested a study from Stratix, describing current technical developments with regards to internet architecture and its standardisation, the social values involved, as well as the related geopolitical and governance developments. The agency would like to use the outcome of this study as a basis for discussions with national and international stakeholders regarding the preservation of a free and open internet, as well as the role that Radiocommunications Agency Netherlands can fulfil within the multi-stakeholder community.

The scope of this assignment was limited to the internet and transport layers of the internet architecture. The best-known standards for these layers are those defining TCP/IP (the basis of the internet). A small part of the standards for mobile networks (such as UMTS, LTE or 5G) are also relevant for these layers. The majority of mobile standards apply to the internal working of mobile networks and are therefore out of scope for this study.

Standardisation, social values and geopolitics

A large number of standardisation organisations are active in the field of networks, but for the scope of this study the Internet Engineering Task Force (IETF) and (for mobile) the Third Generation Partnership Program (3GPP) are the most influential. There have not been any significant changes in that respect in recent years, although some players have been trying to influence the architecture of the internet through other standardisation organisations.

The core values that drive standardisation are mostly technical. More generic values, such as respect for human rights or specific political values, may indirectly play a role but are rarely made explicit.

Geopolitics have not had a significant effect on standardisation so far, despite the increasing participation from countries such as China which were less involved in the past. Participants from these countries have not yet been able to fundamentally change the course of standardisation, while active participation from more countries actually strengthens the legitimacy of standards. Some major market players on the other hand, do have significant influence. For instance, the standardisation of QUIC, a recent development started by Google, was only possible because Google controlled the largest browser in the world as well as a significant Content Distribution Network.

Issues and solutions

For this study, Stratix developed a top ten list of the most important issues within the given scope. The list was composed based on discussions with experts in the field. The following list provides a short description of these issues; for more information, please refer to the main document.

1. BGP route hijacking
2. IP spoofing
3. Traffic shaping / net neutrality
4. Limited visibility of undesired content
5. Interception of content
6. Interception of metadata
7. Control over traffic (sovereignty)
8. Innovation, flexibility, and changeability of infrastructure
9. Lack of options to improve sustainability
10. Lack of Quality of Service

For each of these issues Stratix investigated the values that are relevant for each issue, the solutions being proposed and the viability of these solutions.

Some of the issues involve conflicting values. The issue "limited visibility of undesired content" is a good example: the legitimate need for authorities to block or at least detect specific content (such as child pornography, hate speech, or illegal distribution of copyrighted works) is based on generally accepted values, but at the same time conflicts with other accepted values such as privacy and anonymity. An additional complication is that any mechanism giving authorities in a democratic society more control over content, with all relevant assurances, could just as easily be used by autocratic regimes in ways conflicting with human rights. It is in fact impossible to create a technical standard which can differentiate between these two.

For each of the issues listed, there is work being done on incremental solutions (small additions or changes to existing standards) as well as on radical solutions ("clean slate" designs of the internet).

In general, it can be said that incremental solutions are more mature and more viable than the radical solutions. Even if these radical solutions would be sufficiently scalable and if they would solve the issues at hand (both of which are debatable), replacing the internet with these solutions is effectively impossible due to the huge existing "installed base". However, these initiatives can, if the research results are shared widely, provide a valuable contribution to a better understanding of the working of networks, and thereby lead to better (incremental) solutions within the existing standards.

Implementation of standards

The success of internet standards is defined by their implementation in equipment and by their actual use in networks. In some cases, manufacturers have implemented a standard that network operators are so far making little or no use of. IPv6 is a typical example.

Governmental influence

It is important for the Dutch government, in particular Radiocommunications Agency, to maintain knowledge about the main standardisation organisations and processes, and to influence them indirectly through dialogue with the diverse concerned parties. The Netherlands already has as a whole a relatively large influence on standardisation, but at least in the case of the multi-stakeholder organisations this influence is not exerted directly by the government. Through indirect influence the government can help secure those values it considers important in standardisation.

Governments can also encourage the implementation of relevant standards: by providing information; by prescribing the use of standards in systems procurement; and in some cases, even by mandating specific standards in rules and regulations.

Stratix

Inhoudsopgave

1 Aanleiding en achtergrond

1.1 Aanleiding

In meerdere internationale gremia wordt gesproken over de toekomst van de internetinfrastructuur en -architectuur. De Europese Commissie geeft in haar Cybersecurity Strategy aan dat Europa moet streven naar een open internet, terwijl er tegelijkertijd waarborgen nodig zijn; niet alleen om beveiliging mogelijk te maken, maar ook om de Europese waarden en fundamentele rechten voor iedereen te beschermen (EU Commission 2020).

Er vindt in verschillende standaardisatieorganisaties discussie plaats over nut en noodzaak van modernisering van de internet infrastructuur. ETSI voert deze discussie bijvoorbeeld in de Industry Specification Group on Non-IP Networking[1], en in ITU-T wordt gesproken over het Future Generation Net 2030. Er wordt onder meer gekeken naar wijzigingen aan de transportlaag van internet, bijvoorbeeld ter verbetering van efficiëntie in routering, verminderen van header-informatie, of ter verbetering van beveiliging en privacy.

De discussies over modernisering van internetinfrastructuur worden onder andere gevoerd in de Internet Engineering Task Force (IETF), Internet Architecture Board (IAB) en Internet Research Task Force (IRTF). Deze organisaties beschouwen de openheid van het internet als een groot goed.

Een organisatie als International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) raakt meer en meer betrokken bij standaardisatie van internet (zie ook NRC Handelsblad[2]). Anders dan de IETF werkt de ITU-T niet volgens het multi-stakeholdermodel, maar multilateraal[3]. Deze verschuiving of uitbreiding in betrokken gremia leidt dus ook tot een verschuiving in de wijze waarop internationaal consensus wordt bereikt en/of besluiten worden genomen. Via onder andere ITU proberen landen en multinationals hun grip op de infrastructuur van het internet te vergroten. Er worden technische argumenten aangevoerd voor verandering in de internetinfrastructuur (architectuur, standaarden, protocollering), die ten koste zouden kunnen gaan van interoperabiliteit, anonimiteit, privacy en van andere maatschappelijke waarden. Door het geopolitieke component in de discussie valt het niet mee om deze dimensie te scheiden van de puur technische argumenten voor wel of geen gewenste verandering in de internetinfrastructuur.

Samengevat ziet het Agentschap drie veranderingen die aanleiding geven voor dit onderzoek:

1) discussies over nut en noodzaak van nieuwe en alternatieve internetinfrastructuren;
2) een verschuiving in betrokken gremia en de wijze van besluitvorming;
3) een toenemende verwevenheid tussen geopolitiek en technische standaardisatie.

---

[1] https://www.etsi.org/committee/1724-nin

[2] Zie https://www.nrc.nl/nieuws/2020/09/15/help-het-internet-breekt-in-tweeen-a4012056

[3] Een multi-stakeholder model voor een standaardisatie werkt op basis van belanghebbenden die op basis van hun belang (marktpositie, patenten, rol in de markt), kennis, ervaring en belangstelling input leveren in het standaardisatieproces. Bij een multilateraal model spreken overheden gezamenlijk normen af. Zie ook paragraaf 3.2.2.

Deze vraagstukken waren voor het Agentschap Telecom aanleiding om dit onderzoek uit te laten voeren naar "Internetinfrastructuur: standaardisatie, techniek en geopolitiek".

1.2 Vraagstelling

Voor dit onderzoek heeft de opdrachtgever de volgende hoofdvragen en subvragen gesteld:

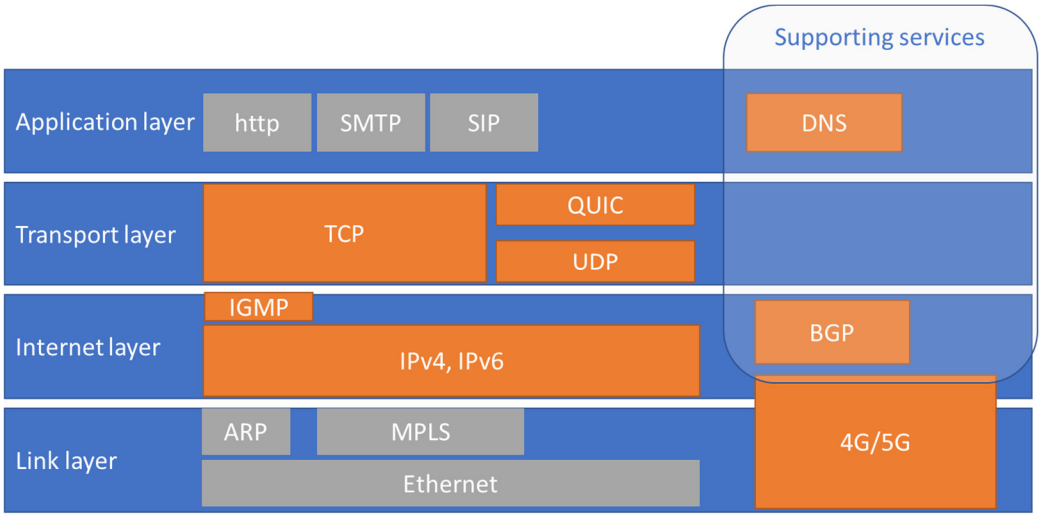
1. *Welke actuele ontwikkelingen in de architectuur en standaardisatie van internet zijn van grote maatschappelijke relevantie (gegeven de scope)?*
    a. *Wat zijn de 10 belangrijkste vraagstukken als gevolg van deze ontwikkelingen en waarom (welke maatschappelijke waarden staan daarbij op het spel)?*
    b. *Welke nationale en internationale gremia hebben momenteel invloed op deze vraagstukken, en welke verschuivingen zijn er in de invloed die deze gremia uitoefenen? Hoe en waar wordt bepaald welke activiteiten elk gremium oppakt? Welke zijn de belangrijkste gremia voor de Rijksoverheid om in te participeren? Staat het multi-stakeholder model zoals door RIPE, IANA, IETF wordt gebruikt onder druk?*
2. *Welke technische oplossingen (in het kader van vraag 1a) worden voorgesteld vanuit de verschillende werelddelen en instanties (gegeven de scope)?*
    a. *Wat zijn de voordelen en nadelen (bijvoorbeeld het risico van fragmentatie van het internet) van deze oplossingen, zowel vanuit de optiek van techniek als vanuit maatschappelijke waarden? Hoe volwassen en kansrijk zijn deze oplossingen?*
    b. *Welke gremia (zie 1b) zijn bij elk van de oplossingen betrokken, en welke oplossingen zijn gremium-overstijgend?*

1.3 Scope

Het onderzoek richt zich, conform de opdracht, op de internet- en transport laag, aangevuld met Domain Name System (DNS), Border Gateway Protocol (BGP) en vergelijkbare protocollen als ondersteunende dienst. Onderstaand lagenmodel (Figuur 1) illustreert deze scope, met een aantal voorbeelden van relevante protocollen per laag. Hiervoor geldt dat DNS en BGP strikt genomen protocollen op de applicatielaag zijn, maar in de praktijk aangrijpen op verschillende lagen[4].

In de analyse ligt de focus op de oranje blokjes in deze figuur. Dat geldt dus ook voor het bepalen van de "top tien" van vraagstukken.

[4] Een toelichting op de verschillende "lagenmodellen" is te vinden in Annex B.



Figuur 1: Scope van dit onderzoek binnen het lagenmodel (scope in oranje)

1.4 Methode

Om antwoord op de gestelde vragen te geven hebben wij voor dit onderzoek de volgende fasen doorlopen:

1.4.1 Fase 1: Desk research naar waarden, ontwikkelingen en actuele vraagstukken

In de eerste fase hebben wij een uitgebreide desk research uitgevoerd naar de verschillende standaardisatieorganisaties en hun rol bij de netwerkstandaarden binnen de hiervoor benoemde scope, naar de raamwerken voor de normen en waarden achter de standaardisatie, en naar relevante en actuele vraagstukken op dat gebied.

Hierbij maakten wij gebruik van wetenschappelijke literatuur, van discussies op mailinglists en in bijeenkomsten van standaardisatieorganisaties en multilaterale organisaties, en van onze eigen kennis en ervaring op dit gebied. De belangrijkste gebruikte literatuur staat in de literatuurlijst benoemd (Annex A).

Voor wat betreft de actuele vraagstukken hebben wij vooral gekeken naar informatie van de laatste drie jaar; voor de overige thema's zijn wij veel verder teruggegaan. De (formele) processen rond standaardisatie zijn in de laatste jaren immers niet veranderd, al kan de invloed van partijen wel veranderd zijn.

De resultaten van de deskresearch werden met de opdrachtgever en de klankbordgroep besproken om de scope verder af te bakenen.

1.4.2 Fase 2: Interviews

Na de desk research hebben wij de relevante ontwikkelingen en bijbehorende vraagstukken verder onderzocht door middel van interviews met experts op het vlak van standaardisatie en implementatie. Daarmee hebben wij de resultaten van Fase 1 verder aangescherpt.

In totaal hebben wij 16 personen geïnterviewd, waarbij wij een zo breed mogelijke selectie van personen hebben gemaakt uit de academische wereld, actieve standaardisatie vanuit bedrijven en instellingen, governance organisaties, standaardisatieorganisaties, relevante Europese organisaties, en vertegenwoordigers van initiatieven die meer radicale veranderingen van de internet architectuur voorstaan. De lijst van geïnterviewde personen is te vinden in Annex E.

Enkele onderwerpen die bij de interviews aan de orde kwamen waren:

a. Standaardisatie en implementatie van standaarden;
b. Relatie tussen standaardisatie en implementatie en ervaringen daarmee;
c. Betrokken (of juist niet betrokken) stakeholders en hun belangen en achterliggende waarden;
d. Reflectie welke vraagstukken actueel en relevant zijn, welke oplossingsrichtingen er zijn met welke kansrijkheid (en waarom) en welke stakeholders daarbij relevant zijn.

De gebruikte generieke vragenlijst staat in Annex F, waarbij wij bij elk interview wel dieper ingingen op de onderwerpen waarin de geïnterviewde gespecialiseerd was en op de vraagstukken die daarbij aan de orde kwamen. De vragenlijst diende dus vooral als "kapstok" voor de interviews.

De informatie uit de interviews werd gebruikt bij het verder aanvullen en beschrijven van de lijst van issues en stakeholders en hun karakteristieken en relaties, en het aanscherpen van de selectie van de top 10 vraagstukken.

1.4.3 Fase 3: Analyse van de opgedane kennis op de geïdentificeerde vraagstukken

In een workshop met een selectie van de geïnterviewde partijen hebben wij de voorlopige observaties toegelicht en de voorgestelde lijst van top 10 vraagstukken met de aanwezigen besproken. De reacties vanuit de workshop hebben wij gebruikt om onze conclusies verder aan te scherpen.

De in de eerdere fases geïdentificeerde stakeholders hebben wij globaal ingedeeld op basis van het model van Mitchell, Agle en Wood (Mitchell et al. 1997).

Voor elk van de top 10 vraagstukken hebben wij een overzicht gemaakt van:

- De eigenschappen van het internet (features) waar het vraagstuk betrekking op heeft;
- Een beschrijving van wat er daarbij (door sommigen) als probleem ervaren wordt;
- Welke incrementele oplossingen mogelijk zijn, met in literatuur en interviews genoemde voor- en nadelen;
- De betrokken standaardisatieorganisaties;
- De kansrijkheid van de oplossingen.

Daarnaast hebben wij een aantal meer radicale oplossingen beschreven die volgens voorstanders verschillende van de benoemde vraagstukken of problemen op zouden kunnen lossen.

Uiteindelijk hebben wij aan de hand van de resultaten van de verschillende fases de onderzoeksvragen beantwoord.

1.5 Leeswijzer

De eerste drie hoofdstukken beschrijven de context van de internet architectuur. Vervolgens wordt in hoofdstuk 4 gereflecteerd op de normen en waarden die aan de architectuur ten grondslag lagen, of zouden moeten liggen. De laatste drie hoofdstukken beschrijven de gesignaleerde problemen en de daarvoor voorgestelde oplossingen, en geven een analyse van voor- en nadelen van deze oplossingen en een reflectie op de relatie met achterliggende normen en waarden, en de mogelijke rol van de overheid bij problemen en oplossingen rond de internet architectuur.

Hoofdstuk 1 beschrijft aanleiding, achtergrond, vraagstelling, scope en methode van dit onderzoek.

Hoofdstuk 2 geeft de historische context van de ontwikkeling van het internet. Hierbij wordt de veranderende kijk geschetst van de telecomwereld en overheden op de mogelijkheden en de rol van internet, en de discussies die ook in het verleden zijn gevoerd over mogelijke fundamentele onvolkomenheden van het internet. Ook gaat het hoofdstuk in op een aantal relevante voorgaande en parallelle ontwikkelingen zoals de opkomst van mobiele netwerken.

Hoofdstuk 3 beschrijft de relevante standaardisatieorganisaties, en hun rol in het maken en onderhouden van de standaarden die de fundamenten van het internet vormen. Ook geeft het inzicht in de processen, cultuur, en deelnemende stakeholders.

Hoofdstuk 4 gaat in op de verschillende achterliggende maatschappelijke, technologische en economische normen en waarden die een rol speelden en spelen bij de standaardisatie. Ook laat het verschillende conflicten en tegenstellingen zien tussen verschillende van deze achterliggende waarden, en vat het de belangrijkste waarden kort samen.

Hoofdstuk 5 geeft een overzicht van de in literatuuronderzoek en interviews genoemde mogelijke vraagstukken en (vermeende) problemen met betrekking tot de huidige standaarden voor geïnterconnecteerde netwerken. Hierbij worden ook de meer radicale voorstellen voor fundamenteel anders inrichten van het internet benoemd, omdat elk van deze voorstellen beoogt om een oplossing te bieden voor een aantal relevante vraagstukken. Uiteindelijk wordt een top 10 bepaald van de op dit moment meest relevante vraagstukken.

Hoofdstuk 6 beschrijft deze top 10 vraagstukken, de bijbehorende voorgestelde incrementele oplossingen met voor- en nadelen, betrokken gremia, en onze inschatting over hoe kansrijk deze oplossingen zijn. Vervolgens geeft het een beoordeling van de meer radicale oplossingen die zijn beschreven in het vorige hoofdstuk.

Hoofdstuk 7 bevat een aantal conclusies met betrekking tot de onderzoeksvragen.

2 Historische context: van bijzaak naar basis

Standaardisatie is net zo oud als telecommunicatie, en gaat al terug tot rooksignalen, trommels en semaforen in de oudheid. Om communicatie op afstand mogelijk te maken was het nodig om afspraken te maken over de betekenis van symbolen en de te gebruiken technieken. Techniek en politiek gingen hierbij vaak hand in hand. In dit hoofdstuk wordt een deel van de historie weergegeven, omdat deze heeft bepaald waar we nu staan. Een groot deel van de actuele vraagstukken rond de architectuur van de internet infrastructuur vindt zijn basis in de historische keuzes achter het internet, die deels weer voortkomen uit een (toenmalig) nieuwe kijk op communicatie ten opzichte van de al bestaande telefonienetwerken.

2.1 Historie van telecom standaardisatie

Communicatietechnologieën hebben altijd een grote rol gespeeld in het vormgeven van relaties binnen en tussen landen. De International Telegraph Union (ITU) werd in 1865 opgericht door 20 landen, waaronder Nederland (Figuur 2 toont als illustratie de voorzijde van het verdrag). Afspraken tussen individuele landen en regionale afspraken bleken niet schaalbaar; daarom was een internationaal gremium noodzakelijk.


LES
GOUVERNEMENTS
des Etats signataires de la
CONVENTION TELEGRAPHIQUE INTERNATIONALE
TITRE PREMIER
du réseau international.
Article 1.

Figuur 2 ITU-verdrag 1865

Het was een wereldwijd telegraaf netwerk dat Groot-Brittannië omvormde van een koloniale tot een imperiale macht (Carey 1983), en het was de lancering van de Sputnik satelliet door de Sovjet-Unie die de Amerikaanse overheid noopte tot het financieren van de voorganger van het internet (Abbate 1999).

Recenter startten de landen van de Europese Gemeenschap de Groupe Speciale Mobile, omdat er meerdere analoge mobiele telefonienetwerken waren in Europa, die niet interoperabel waren. Europa wilde een interoperabel systeem voor mobiele netwerken als basis voor de interne markt, maar ook als alternatief voor Amerikaanse en Japanse mobiele technologie. Kortom: transnationale communicatienetwerken zijn altijd verbonden geweest met industriepolitiek en met geopolitiek.

2.2 Historie van het internet

De discussie over standaardisatie van netwerken is niet nieuw. Al in de jaren '80 van de vorige eeuw werd hierover gesproken. Er waren verschillende gremia waar werd gediscussieerd over hoe de datanetwerken van de toekomst er uit moesten zien.

De wijze waarop computers met elkaar verbonden konden worden was vanaf het begin belangrijk voor de keuze welke computers en netwerken werden gekocht en gebruikt. Telecombedrijven, academici en hun leveranciers discussieerden binnen verschillende gremia over standaarden, zoals X.25, ISDN, OSI en ATM [5], die zij zagen als de basis van intelligente netwerken. De discussies waren zowel wereldwijd als regionaal, waarbij industriepolitiek, nationale standaarden en "eigen" innovaties vaak minstens zo belangrijk waren als interoperabiliteit.

Wetenschappers betrokken bij kernfysica, weermodellen en astronomie waren de eerste grootschalige gebruikers van deze computers en netwerken. Zij bouwden aan academische netwerken, protocollen en standaarden om hun netwerken onderling te verbinden.

Deze academische netwerken gebruikten geen uniforme netwerktechnologieën. Het was daarom nodig om een protocol te gebruiken dat onafhankelijk van het onderliggende netwerk of de gebruikte computer over een veelheid van netwerken kon functioneren. Door informatie op te delen in 'packets' werd het eenvoudiger voor meerdere gebruikers om tegelijkertijd de onderliggende netwerken te delen en te gebruiken. Hiervoor gebruikte men het IP-protocol[6], dat de basis werd van het internet. De universiteit van Berkeley speelde hierbij een belangrijke rol door updates uit te brengen van hun versie van Unix, een operating systeem, dat in de wetenschappelijke wereld veel werd gebruikt. De integratie van IP in Unix BSD (Berkeley Software Distribution) maakte dat IP steeds breder en eenvoudiger beschikbaar werd (Leiner et al 1997).

Om afspraken over protocollen te kunnen maken ontstonden samenwerkingsverbanden als de IETF.

De traditionele staatsbedrijven voor telecommunicatie (de PTT's) zagen de ontwikkelingen op de academische netwerken destijds wel, maar namen ze niet serieus. Zij verwachtten dat de standaarden waar zij aan werkten snel de wereld zouden veroveren.

2.3 Overheden en het succes van internet

In overheidskringen kreeg het internet en de standaardisatie er omheen pas halverwege de jaren negentig aandacht. Overheden hadden tot dusver vooral de ontwikkelingen rond intelligent networks gevolgd in ETSI en ITU, rechtstreeks en via hun PTT's. Zij hadden bijgedragen aan deze intelligent networks door het financieren van Research en Development.

Op hetzelfde moment financierden ze de ontwikkeling van het internet op een indirecte wijze via het financieren van de wetenschap rond kernfysica, klimaatmodellen en astronomie, inclusief de benodigde computers en netwerken.

Dat het internet en de bijbehorende protocollen vanaf 1990 steeds meer tractie kregen was voor velen volkomen onverwacht. Er werd nog wel gepoogd om via druk op de academische netwerken, zoals Surfnet, de "Europese standaarden" (zoals X.25) op te leggen, maar dit bleek weinig effectief. Bij veel experts bestaat de indruk dat het succes van internet voor

[5] Dit rapport bevat vrij veel technische termen en afkortingen; deze staan kort toegelicht in Annex G.
[6] In eerste instantie werd een vorm van TCP gebruikt, die later werd gesplitst in TCP en IP.

consumenten en bedrijven eerder *ondanks* bemoeienis van overheden tot stand kwam, dan *dankzij*. Het succes ontstond vooral door de adoptie binnen wereldwijde academische en onderzoeksinstellingen.

De ontwikkeling van het internet introduceerde het concept van "permissieloze innovatie". Dat wil zeggen: door het open karakter van de onderliggende netwerken kon iedere aangesloten partij nieuwe innovaties introduceren, zonder dat de beheerders van die netwerken daar "toestemming" voor hoefden te geven. Dit was destijds een grote mentaliteitsverandering ten opzichte van de traditionele netwerken, waarbij de beheerders (vaak PTT's) vaak volledige zeggenschap probeerden te houden over de aan te sluiten randapparaten en soms zelfs de daarmee verbonden applicaties.

2.4 Discussies internet versus telecom standaarden

Het internet werd zoals gezegd niet vanaf het begin geaccepteerd als het winnende pad. In die discussie is een aantal fasen te onderkennen, die uiteindelijk leidden tot de acceptatie dat het internet, haar protocollen en bijbehorende gremia de basis vormen waar de digitale samenleving op gebouwd is. De fasen die de discussie doorliep zijn ongeveer:

- *Het internet kan niet werken:* Tot 2001 werd in gremia als ITU-T, ETSI en 3GPP betoogd, dat internet op basis van IP, TCP, en UDP, überhaupt niet kon werken, en al zeker niet voor real-time media. Deze partijen hadden onder andere ISDN en GSM gestandaardiseerd, en zouden dit verder uitbouwen. ATM, 3G, ISDN waren de standaarden die telecombedrijven wereldwijd zouden gaan gebruiken. De discussie stond ook wel bekend als "netheads vs bellheads" of "intelligent networks vs stupid networks" (Isenberg 1998, Odlyzko 1998).
- *IP moet anders, omdat:* Na 2001 werd algemeen geaccepteerd dat IP de basis zou zijn, maar werd in sommige gremia beweerd dat het internet zonder extra functies nooit geschikt zou zijn voor tijdgevoelige applicaties. In ETSI (bv TISPAN), 3GPP en ITU (bv SG-13) werd gewerkt aan protocollen zoals IMS, waarbij IP wel werd gebruikt, maar die een betere Quality of Service zouden leveren dan "het internet".
- *Het internet is onveilig:* Na 2010 ging de discussie in toenemende mate over de beveiliging van het internet, waarbij onder andere beveiligde versies werden voorgesteld protocollen als DNS, BGP en HTTP (DNSSEC, BGPsec, en HTTPS). Uit deze discussie ontstonden ook verschillende pogingen om het internet geheel te vervangen door iets beters (met name RINA en SCION, zie paragraaf 5.1).
- *Het internet moet bijdragen aan:* Inmiddels is het internet algemeen geaccepteerd, maar bestaat nog steeds bij een aantal stakeholders de behoefte om zaken aan te passen zodat het internet het oplossen van bepaalde (maatschappelijke) doelen beter kan ondersteunen, bijvoorbeeld veiligheid, duurzaamheid, of het tegengaan van verspreiding van nepnieuws, racisme, kinderporno, etc. De vraagstukken rond veiligheidsaspecten en tegengaan van ongewenste inhoud speelden en spelen een rol in discussies rond vrijwel alle protocollen waar encryptie een rol speelt. Duurzaamheid is een relatief nieuw thema maar gaat naar verwachting een steeds grotere rol spelen in discussies rond protocollen gerelateerd aan transport en routering.

De genoemde discussies vonden vooral plaats rond techniek en wijze van standaardisatie. De uitkomst werd echter niet in de standaardisatieorganisaties bepaald. Die werd bepaald door

implementatie in hardware en software, en door adoptie in geïnterconnecteerde netwerken en systemen. Implementatie en dan vooral het praktisch gebruik wordt in de discussie nog wel eens vergeten, maar is de bepalende factor.

Veel "standaarden" bestaan vooral op papier en zijn niet omgezet naar software en hardware. Voor zover standaarden omgezet zijn naar hardware en software wordt een groot aantal niet geactiveerd door de beheerders van de netwerken, of niet gebruikt in de interconnectie met andere netwerken[7]. Vooral dat laatste speelt een grotere rol dan gedacht. Het is één ding om de operator van een individueel netwerk te overtuigen om een standaard te gebruiken, maar om die standaard te laten gebruiken in duizenden netwerken en daarmee ook in software en hardware van een veelheid van fabrikanten en ontwikkelaars is vele malen complexer.

Het waren vooral de (financiële/economische) keuzes van bedrijven en dienstverleners in hun lokale netwerken en hun applicaties die de adoptie bepaalden, en niet die van telecombedrijven. In dit rapport zullen we daarom een scheiding maken tussen standaardisatie en implementatie. Standaardisatie is het proces waarbij een groep komt tot gedeelde afspraken over hoe, in deze context, geïnterconnecteerde netwerken moeten werken; implementatie is wat er gebeurt als de afspraken die in een standaard staan, worden omgezet in software, hardware en praktisch gebruik.

2.5 Overheden en het succes van GSM en opvolgers

De historie van de standaardisatie van GSM en zijn opvolgers is bijna tegengesteld aan die van het internet. Beide standaardisatiepaden leidden tot een wereldwijd succes, en ze zijn inmiddels bijna niet meer los van elkaar te zien. Maar hier is de sturing vanuit met name de EC zeer belangrijk geweest.

De opkomst van internet begon vanuit de academische wereld en werd vanuit een wereldwijde 'underground' status bij onderzoeks- en onderwijsinstellingen een voldongen feit. GSM kwam vanuit de telecomwereld, en werd in eerste instantie gestuurd door Europese regulering met de visie dat autotelefoons in heel Europa gebruikt moesten kunnen worden.

Standaardisatie van GSM begon rond 1982 nadat verschillende landen in de wereld analoge mobiele netwerken hadden gelanceerd of op het punt stonden deze te lanceren.

Er waren verschillende concurrerende analoge standaarden wereldwijd. In de Scandinavische landen was de standaard Nordic Mobile Telephone (NMT). Het systeem werd in 1981 gelanceerd en werd in veel landen buiten Scandinavië gebruikt, onder andere in Nederland, België en Zwitserland. Het onderscheidde zich omdat het ook internationale roaming ondersteunde, iets wat de meeste systemen niet konden. Het Verenigd Koninkrijk gebruikte TACS (Total Access Communication System), gebaseerd op het Amerikaanse AMPS-systeem. Frankrijk en Duitsland werkten een tijd lang aan een gezamenlijke standaard, maar dat project viel uit elkaar en elk land creëerde zijn eigen standaard. Duitsland gebruikte C-Netz van Siemens. In Frankrijk gebruikte France Telecom vanaf 1986 het Franse Radio2000, maar de nieuwe

[7] Een bekend voorbeeld is IP Multicast: vrijwel alle apparaten ondersteunen het, en het wordt binnen individuele netwerken gebruikt, maar niet tussen geïnterconnecteerde netwerken.

toetreder SFR lanceerde haar netwerk in 1988 op basis van NMT. Spanje gebruikte TMA en Italië had RTM.

Al deze systemen waren niet interoperabel, en roaming tussen landen was slechts in enkele gevallen mogelijk. Ieder systeem bleek echter wel in een behoefte te voorzien, want er waren tienduizenden tot honderdduizenden gebruikers per land.

NMT was een relatief succesvol systeem omdat de specificaties open waren, en dit het eenvoudiger maakte voor nieuwe toetreders om toestellen en netwerkapparatuur te bouwen. NMT werd om die reden in een groot aantal landen toegepast. De andere systemen waren minder open, en vaak gekoppeld aan een specifieke aanbieder in een land, zoals bijvoorbeeld het Radio2000 systeem in Frankrijk of C-Netz van Siemens en Deutsche Telekom. De verschillende nationale systemen en implementaties beperkten de markt, waardoor er weinig concurrentie tussen fabrikanten van toestellen en netwerkapparatuur.

Vanuit de Europese Gemeenschap kwam er een roep naar CEPT[8] om met een uniforme standaard te komen. Hiertoe werd in 1982 de Groupe Spécial Mobile opgericht. De eerste paar jaar kwamen er vooral veel ideeën voor een nieuw netwerk vanuit wetenschap, standaardisatieorganisaties, bedrijven en netwerken. Lange tijd werden er concurrerende oplossingen besproken. In 1987 werden echter in een paar maanden tijd, onder druk van de overheden van Duitsland, Frankrijk, Italië en het Verenigd Koninkrijk, de cruciale technische keuzes gemaakt voor het toekomstige netwerk[9].

Om die keuzes te valideren werd er een aantal praktijktesten gedaan met concurrerende implementaties en voorstellen, binnen de gemaakte keuzes. Een team van de Universiteit van Trondheim presenteerde uiteindelijk de best werkende van alle concurrerende voorstellen, en deze versie werd geselecteerd.

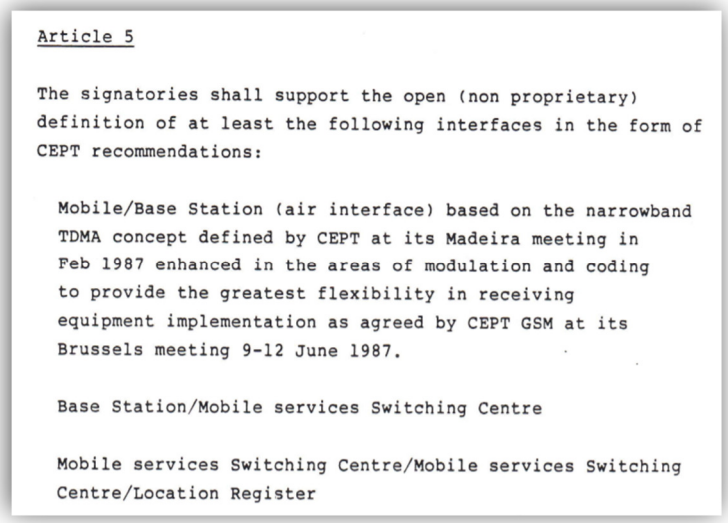
Dit alles leidde in september 1987 tot het GSM Memorandum of Understanding (zie Figuur 3), met daarin de bepaling dat alle deelnemers zich voor een aantal specifieke interfaces aan de afgesproken standaarden zou houden[10]. Iedere partij die apparatuur voor GSM ging ontwikkelen of die van GSM gebruik ging maken werd geacht de MoU te ondertekenen en zich eraan te conformeren. Een belangrijke eis was dat er in 1991 in alle twaalf deelnemende landen commerciële GSM-netwerken moesten zijn. Dit zette druk op de ondertekenaars om te werken aan standaarden, die geïmplementeerd konden worden en geactiveerd in netwerken.

Voor dit rapport is het vooral interessant om te zien hoe de nadruk lag op “non-proprietary” voor alle belangrijke onderdelen van het netwerk. Er mochten geen onderdelen nodig zijn die alleen maar door één partij geleverd konden worden (zoals in eerdere netwerken wel gebruikelijk was). Dat zorgde voor een open markt, waar veel partijen op instapten.

[8] CEPT: Europese organisatie voor post en telecom (oorspronkelijk: Conférence Européenne Postes et Télécommunications), zie CEPT.org

[9] Een origineel hiervan staat online (met handgeschreven annex A en B) http://www.gsmhistory.com/wp-content/uploads/2013/01/3.-1st-GSM-Tech-Spec.pdf

[10] http://www.gsmhistory.com/wp-content/uploads/2013/01/5.-GSM-MoU.pdf



Article 5

The signatories shall support the open (non proprietary) definition of at least the following interfaces in the form of CEPT recommendations:

Mobile/Base Station (air interface) based on the narrowband TDMA concept defined by CEPT at its Madeira meeting in Feb 1987 enhanced in the areas of modulation and coding to provide the greatest flexibility in receiving equipment implementation as agreed by CEPT GSM at its Brussels meeting 9-12 June 1987.

Base Station/Mobile services Switching Centre

Mobile services Switching Centre/Mobile services Switching Centre/Location Register

Figuur 3: Artikel 5 van MoU voor ontwikkeling van een PanEuropees mobiel netwerk: standaard, open interfaces als basis voor o.a. roaming

Extra flexibiliteit ontstond door de invoering van de SIM-kaart, die de gebruiker de mogelijkheid gaf om van mobiel netwerk en toestel te veranderen. Doordat GSM door een veelheid van fabrikanten werd ondersteund, werd GSM uiteindelijk wereldwijd de meest ondersteunde standaard.

Om de standaardisatie en implementatie werkzaamheden voor GSM vaart te geven richtte de CEPT in opdracht van de Europese Gemeenschap de European Telecommunication Standards Institute (ETSI) op. In tegenstelling tot datacommunicatienetwerken was er geen gradueel proces en mogelijkheid voor experimenten en concurrerende oplossingen, maar een big bang scenario waarbij alle onderdelen in 1991 klaar moesten zijn en met elkaar moesten kunnen samen werken. Om die reden werd binnen ETSI veel tijd besteed aan het testen van de onderlinge interoperabiliteit van de verschillende delen van het netwerk en van de producten van verschillende fabrikanten.

2.6 Conclusies

Overheden spelen van oudsher een belangrijke rol in standaardisatie van communicatienetwerken. De ontwikkeling van het internet laat echter zien dat standaarden ook in de luwte, zonder directe bemoeienis van overheden, tot stand konden komen.

Voor de andere grote verandering op telecomgebied, de opkomst van mobiele netwerken, speelde in Europa de overheid (met name op Europees niveau) wel een belangrijke rol bij de totstandkoming van het succes.

Een overeenkomst tussen de ontwikkeling van de fundamenten van internet en die van met name GSM is dat ze allebei in betrekkelijke luwte door een breed team van experts konden worden ontworpen, zonder veel druk van grote bestaande markten en marktbelangen. Want evenals voor het internet gold ook voor de mobiele telefoon: ze werden beide lang beschouwd als een kleine nichemarkt voor een beperkte groep gebruikers.

Een andere overeenkomst is het open karakter van de standaarden. Daarbij stond het gemakkelijk in kunnen zetten van apparatuur van verschillende leveranciers vanaf het begin centraal, terwijl netwerkbeheerders wel zo veel mogelijk autonomie op het eigen netwerk behielden. Hierdoor werd het voor aanbieders mogelijk om wereldwijd apparatuur en diensten te leveren, en kregen afnemers een tot die tijd ongekende keuze tussen aanbieders, en een grote flexibiliteit in wereldwijde inzetbaarheid (inclusief roaming).

In het volgende hoofdstuk gaan wij verder in op de huidige standaardisatiewereld, met deze lessen in het achterhoofd.

3 De wereld van standaardisatie

Om netwerken en systemen te bouwen die op elkaar aansluiten en op een voorspelbare manier samenwerken – ook als onderdelen door verschillende fabrikanten worden gebouwd, door verschillende partijen worden beheerd, en verschillend zijn qua leeftijd en mogelijkheden – is het essentieel dat er standaarden zijn waarop deze netwerken en systemen gebaseerd kunnen worden.

De traditionele telefonienetwerken zijn hier een goed voorbeeld van: toen de opkomende telefonienetwerken eerst landelijk, en later internationaal aan elkaar gekoppeld werden was er een noodzaak om die netwerken goed en eenduidig op elkaar aan te laten sluiten. De daarvoor benodigde standaarden werden in die tijd vastgesteld door de ITU (International Telecommunications Union[11]). Naast interoperabiliteit van netwerken zorgde deze standaardisatie ervoor dat er geleidelijk meer apparatuur beschikbaar kwam die overal ingezet kon worden. De ITU houdt zich al lang niet alleen maar met telefonienetwerken bezig en specificeert en beheert standaarden in het hele telecom domein.

Inmiddels zijn er veel meer verschillende netwerktechnologieën, waarbij TCP/IP (de basis van het internet) en GSM/3G/4G/5G (voor mobiele netwerken) de meest bekende zijn[12]. De standaardisatie van die technologieën vindt in verschillende fora plaats.

3.1 Standaardisatieorganisaties

Deze paragraaf licht de voor dit onderzoek belangrijkste standaardisatieorganisaties toe.

Tabel 1: Relevante standaardisatieorganisaties

Organisatie *(paragraaf)*	**Standaarden (voorbeelden)**	**Vertegenwoordiging**
IETF *(3.1.1)*	IPv4, IPv6, DNS, BGP, SIP, QUIC, TLS	Personen
ETSI *(3.1.2)*	GSM(2G), DECT, eTLS	Bedrijven en overheden
3GPP *(3.1.3)*	UMTS(3G), LTE(4G), 5G	Bedrijven (met name telecomfabrikanten en operators), overheden
ITU-T *(3.1.4)*	E.212 (IMSI), Q.931 (ISDN), DSL, optical standards	Overheden en bedrijven, alleen overheden stemrecht

Bovenstaande tabel geeft een globaal en beknopt overzicht van de betreffende organisaties; hieronder worden deze organisaties kort beschreven.

[11] Tot 1934 heette de ITU nog "International Telegraph Union".
[12] Althans op de lagen die voor dit onderzoek relevant zijn; op andere lagen zijn Ethernet, wifi, en HTTP net zo bekend.

3.1.1 IETF (Internet Engineering Task Force)

Het IETF is vooral gericht op internet (IP) gebaseerde protocollen. In theorie is er een laagdrempelige participatiedrempel voor iedereen, vertegenwoordiging is op basis van persoon en niet op basis van bedrijf. In de praktijk werken de meest invloedrijke personen voor IT gerelateerde bedrijven of instituten.

De IETF kent als belangrijkste communicatievormen:

- "Drafts", die op mailinglijsten gepubliceerd en besproken worden, en een naam hebben die begint met "draft-ietf-";
- Genummerde Requests For Comments (RFC).

Documenten krijgen nooit een definitiever predicaat dan 'RFC', maar er kunnen wel nieuwere versies van dezelfde RFC verschijnen. Hoewel de benaming impliceert dat er nog opmerkingen en verbeteringen mogelijk zijn, worden RFC's wel als wereldwijde standaarden gehanteerd.

3.1.2 ETSI (European Telecommunication Standards Institute)

ETSI is een door de Europese Unie (EU) en Europese Vrijhandelsorganisatie (EFTA) erkende Europese standaardisatieorganisatie, en één van de drie Europese standaardisatieorganisaties (naast CEN[13] en CENELEC[14]). Van deze drie is ETSI de organisatie die zich met de standaardisatie van ICT bezighoudt. ETSI kent een vertegenwoordiging van bedrijven (apparatuur producenten en telecommunicatiebedrijven), overheden, en instellingen, waarbij het meeste technische werk door vertegenwoordigers van bedrijven wordt gedaan.

ETSI is van oorsprong Europees, en heeft ook nu nog de taak om Europese ICT standaarden te ontwikkelen en onderhouden. Inmiddels zijn echter bijna alle grote wereldspelers in de telecommunicatie lid van ETSI, en actief bij de standaardisatie betrokken.

ETSI is één van de oprichters van 3GPP (Third Generation Partnership Program) waarin de verdere standaardisatie van GSM en zijn opvolgers naar toe is verhuisd.

Maar ETSI is ook verantwoordelijk voor andere standaarden zoals DECT (draadloze thuistelefoons) en TETRA (mobilofoons/portofoons).

3.1.3 3GPP (Third Generation Partnership Program)

3GPP is een samenwerkingsverband tussen de standaardisatieorganisaties ETSI (Europa), ATIS (Verenigde Staten), ARIB en TTC (Japan), TTA (Korea), CCSA (China) en (sinds 2015) TSDSI (India). 3GPP richt zich op standaarden voor mobiele breedbandcommunicatie (oorspronkelijke voor de zogenaamde 'derde generatie'-telecomnetwerken zoals UMTS, maar ook voor de daaropvolgende generaties zoals LTE). 3GPP standaardiseert ook IMS, een IP-netwerkarchitectuur voor telefonietoepassingen, oorspronkelijk voor mobiele netwerken bedoeld maar ook breder bruikbaar.

[13] European Committee for Standardisation (www.cen.eu), hierin participeren de Europese landelijke standaardisatieorganisaties

[14] European Committee for Electrotechnical Standardisation (www.cenelec.eu), standaarden rond elektrotechniek

3GPP kent een vertegenwoordiging van bedrijven (producenten van telecomapparatuur en netwerkoperators), overheden en andere instellingen. Deelnemers moeten lid zijn van een van de partner standaardisatieorganisatie om deel te mogen nemen. De meeste input komt van de bedrijven.

De wijze van werken van de 3GPP kenmerkt zich door een focus op generaties van netwerken. Deze generaties zijn ieder weer opgesplitst in een aantal releases. Een release bevat nieuwe functionaliteit en incrementele verbeteringen.

Oorspronkelijk werkte de 3GPP aan de derde generatie van mobiele netwerken, het netwerk dat GSM zou opvolgen, namelijk UMTS. Daarna werkte de 3GPP aan 4G en 5G. Op dit moment werkt het aan de releases die 5G moeten vervolmaken. De specificaties voor de basiskenmerken van een nieuwe generatie mobiele netwerken komen, via de research en development afdelingen van de deelnemers en besluitvorming in ITU en de partnerorganisaties, in het werkprogramma van de 3GPP, die deze uitwerkt tot nieuwe standaarden. Terwijl 5G wereldwijd nog lang niet overal beschikbaar is en er nog druk gewerkt aan verbeteringen in nieuwe releases, wordt er alweer nagedacht over wat er mogelijk in een toekomstige 6G-standaard moet komen.

3.1.4 ITU-T (International Telecommunication Union's Telecommunication Standardization Sector)

De ITU heeft een groot aantal taken, maar is vooral bekend vanwege de wereldwijde coördinatie van spectrum afspraken en vanwege de standaarden voor vaste telefonienetwerken. In de ITU kunnen uitsluitend landen lid worden, maar de onderliggende sectoren (waaronder de ITU-T, de sector voor telecommunicatie) staan open voor zowel landen als bedrijven. Bij formele stemmingen hebben alleen de landen echter stemrecht.

ITU-T publiceert handbooks, tutorials en technical papers, maar de belangrijkste documenten zijn de Recommendations, die in tegenstelling tot de suggestie die de naam wekt standaarddocumenten zijn. Ze zijn gerubriceerd door een letter gevolgd door een cijfer, de letter geeft het werkveld aan.

ITU-T heeft voor elke generatie van mobiele technologie de kaders aangegeven, waarna 3GPP op basis daarvan de technologie heeft gestandaardiseerd. In principe kunnen er meerdere, concurrerende technologieën bestaan die binnen de kaders vallen, maar de 3GPP standaarden krijgen de laatste jaren steeds meer de overhand.

Binnen ITU is ook een werkgroep die zich bezighoudt met de toekomst van wereldwijde netwerken: ITU-T Focus Group on Technologies for Network 2030. De activiteiten van deze groep worden verder beschreven in paragraaf 5.1.3.

3.1.5 Voor dit onderzoek minder relevante standaardisatieorganisaties

Er zijn een groot aantal standaardisatieorganisaties die geen of een beperkte rol spelen bij de ontwikkeling van geïnterconnecteerde netwerken op de internetlaag. De standaarden die voortkomen uit deze organisaties zijn vaak wel essentieel voor het functioneren van netwerken of toepassingen over netwerken. Deze standaarden werken dus op de lagen onder de internetlaag of juist erboven, en zijn voor dit onderzoek buiten scope.

NEN: Nederlands Normalisatie Instituut

NEN is een onafhankelijk instituut dat zich bezighoudt met het formuleren van normen op internationaal, Europees en nationaal niveau. Naast het beheren van deze normen ondersteunen ze ook het gebruik van normen door onder andere trainingen. Het instituut is onder andere actief in IoT apparaat standaardisatie, maar niet zozeer in de standaardisatie van de elementen die in scope zijn van deze studie.

IEEE: Institute of Electrical and Electronics Engineers

Het IEEE is met name gericht op transmissiestandaarden zoals Ethernet, wifi, en Bluetooth. Vertegenwoordiging is op basis van professionals die lid zijn van het IEEE.

Transmissiestandaarden (dus onderin het lagenmodel uit Figuur 1) en daarmee het IEEE zijn minder relevant voor de scope van dit onderzoek.

W3C: World Wide Web Consortium

Dit consortium stelt zich tot doel een aantal standaarden te onderhouden en te ontwikkelen die gerelateerd zijn aan het World Wide Web, zoals HTML en HTTP, de protocollen die door webbrowsers worden gebruikt om informatie op te vragen en af te beelden. Aangezien dit protocollen op de applicatielaag zijn, is ook W3C minder relevant voor dit onderzoek.

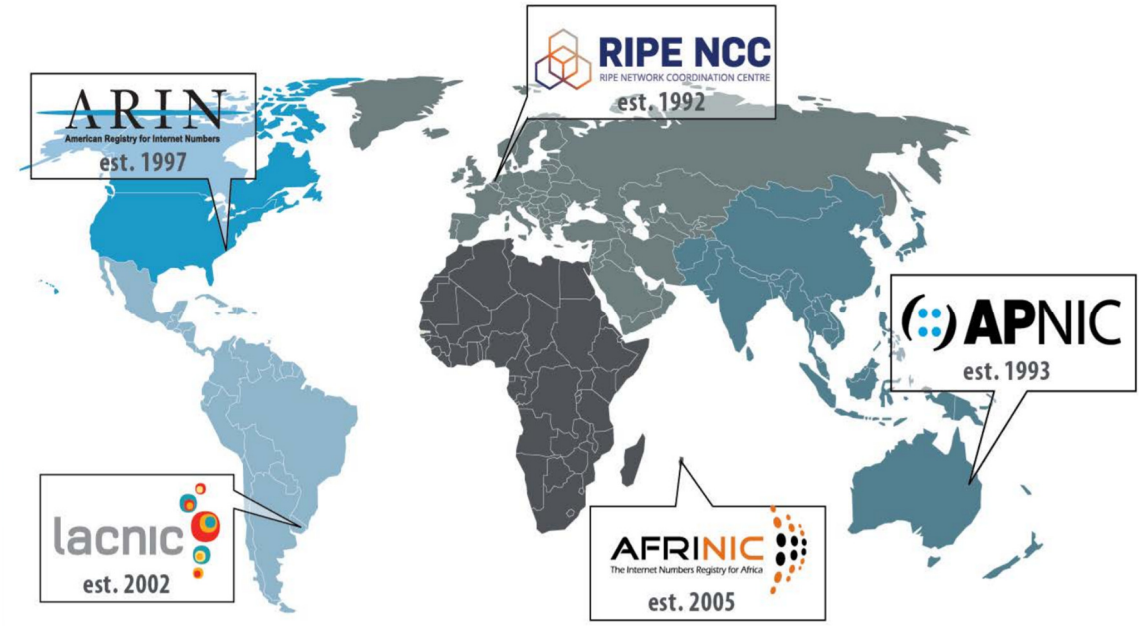
3.1.6 Beheerdersorganisaties van het internet

ICANN

De Internet Corporation for Assigned Names and Numbers (ICANN) is een non-profit organisatie die als doel heeft het internet veilig, stabiel en interoperabel te houden. Ze houden zich onder ander bezig met het toewijzen van domeinnamen en IP-adressen. Hierdoor spelen ze een belangrijke coördinerende rol binnen het internet. ICANN is van mening dat het bestuurlijke gedeelte van het internet op een soortgelijke manier dient te werken als de structuur van het internet, met de nadruk op de openheid en toegankelijkheid. Onderdeel van de ICANN is de IANA, de Internet Assigned Numbers Authority, die o.a. de toplevel domeinen beheert (zie hieronder in het paragraafje over Domain Name Registries) en toeziet op gebruik van aantal standaardnummers zoals poorten voor standaard protocollen. Operationeel doet PTI, een dochterbedrijf van ICANN, het beheer.

Regional Internet Registry (RIR) zoals RIPE NCC

Deze organisaties kennen IP-adresblokken en nummers voor netwerken (Autonomous Systems) toe, die onder andere gebruikt worden bij routering en het BGP-protocol. RIPE NCC is de RIR voor Europa, het Midden-Oosten en Centraal Azië (zie Figuur 4). Dit Network Coordination Centre is organisatorisch onderdeel van het Réseaux IP Européens (RIPE). Het RIPE NCC heeft vestigingen in Amsterdam en Dubai.



Figuur 4: Overzicht van de Regional Internet Registries (RIRs) en de bijbehorende regio's (bron: ICANN)

Domain name registries zoals IANA en SIDN

Deze organisaties beheren de op internet gebruikte domeinnamen. IANA beheert de lijst van topdomeinen; elk van die topdomeinen wordt door een Registry beheerd. Stichting Internet Domeinregistratie Nederland (SIDN) beheert de domeinnamen onder het .nl topdomein.

3.1.7 Special interest groups en andere relevante organisaties rond standaarden

NLnet/ NLnet Labs

NLnet Labs houdt zich voornamelijk bezig met Open Source software en (open) internetprotocollen op het gebied van DNS en routering. Naast het ontwikkelen van standaarden werken ze ook aan juist gebruik en implementatie van deze standaarden. Zo werken ze aan een RPKI toolset. Verder dragen ze bij aan de IETF, mede door de ontwikkeling van een aantal veelgebruikte RFC's.

DNS-OARC

DNS-OARC vormt een platform voor samenwerking op het gebied van DNS. Door onder andere informatie-uitwisseling, analyse en workshops dragen ze bij aan beter en veiliger gebruik van DNS.

Internet Society (ISOC)

De Internet Society is een internationale organisatie gericht op het mogelijk maken van een open, wereldwijd, veilig en betrouwbaar internet. Dit doet het vanuit de kernwaarde dat een dergelijk internet voor iedereen moet zijn te gebruiken. Om dit te bereiken werken ze aan governance, standaarden en innovaties binnen het internet. Op deze manier dragen ze bij aan

de groei van het internet, het robuuster maken van het internet en het doorontwikkelen van het internet. De Internet Society is een wereldwijd platform met ongeveer 85.000 leden en afdelingen en partners vanuit de gehele wereld.

Forum Standaardisatie binnen overheid

Forum Standaardisatie is binnen de Nederlandse overheid een adviescommissie met deskundigen uit de overheid, het bedrijfsleven en de wetenschap. Ze houden zich bezig met het toetsen en voorschrijven van open standaarden aan publieke organisaties, met als doel betere en veiligere uitwisseling en toegankelijkheid van digitale gegevens.

CA/Browser forum

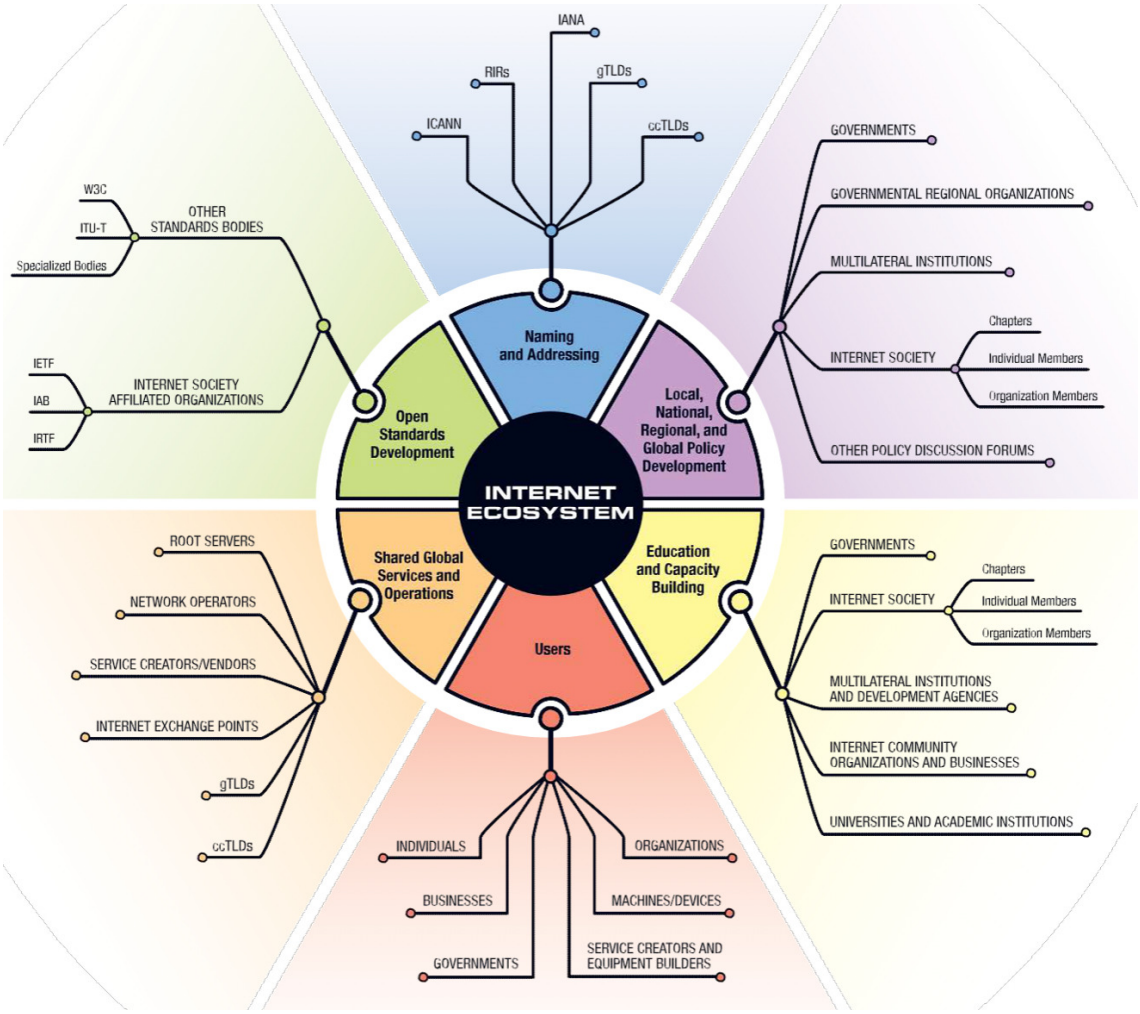
Het Certification Authority Browser Forum (CA/Browser forum) is een samenwerkingsverband tussen uitgevers van certificaten en ontwikkelaars en uitgevers van internetbrowsers software. Het is ontstaan met het doel standaarden en richtlijnen te formuleren voor SSL-certificaten. Door middel van werkgroepen bestaande uit verschillende soorten leden werken ze aan een verbetering van de wijze waarop certificaten worden gebruikt met als doel het internet veiliger te maken voor gebruikers.

3.2 Werking van standaarden: theorie en praktijk

Interoperabiliteit tussen verschillende technische implementaties is een van de belangrijkste drijvende consequenties van standaarden. Hierdoor zijn standaarden een grote vormende macht in het vormen van markten en technologieën.

3.2.1 Deelnemers en stakeholders in standaardisatieprocessen

Wie de deelnemers zijn aan standaardisatieprocessen is afhankelijk van de context van de standaard. Fabrikanten en afnemers spelen in alle gevallen een rol, maar soms is de participatie breder. Overheden, toezichthouders, eindgebruikers, consumentenorganisaties, wetenschappers en ethici kunnen allemaal een bijdrage leveren aan de standaarden. Hoe breder de (verwachte) maatschappelijke effecten, hoe breder de groep van deelnemers meestal is.



Figuur 5: Het internet ecosysteem van stakeholders (bron: ISOC)

Enkele bekende indelingen voor deze brede groep van participanten zijn het overzicht van het internet ecosysteem[15] van ISOC (zie Figuur 5), en de "taxonomy for Future Internet stakeholders" van SESERV[16] (zie Figuur 6). Niet alle getoonde organisaties zijn echter relevant voor de standaardisatie van geïnterconnecteerde netwerken.

Deelnemers in technische standaardisatie rond geïnterconnecteerde netwerken zijn onder andere:

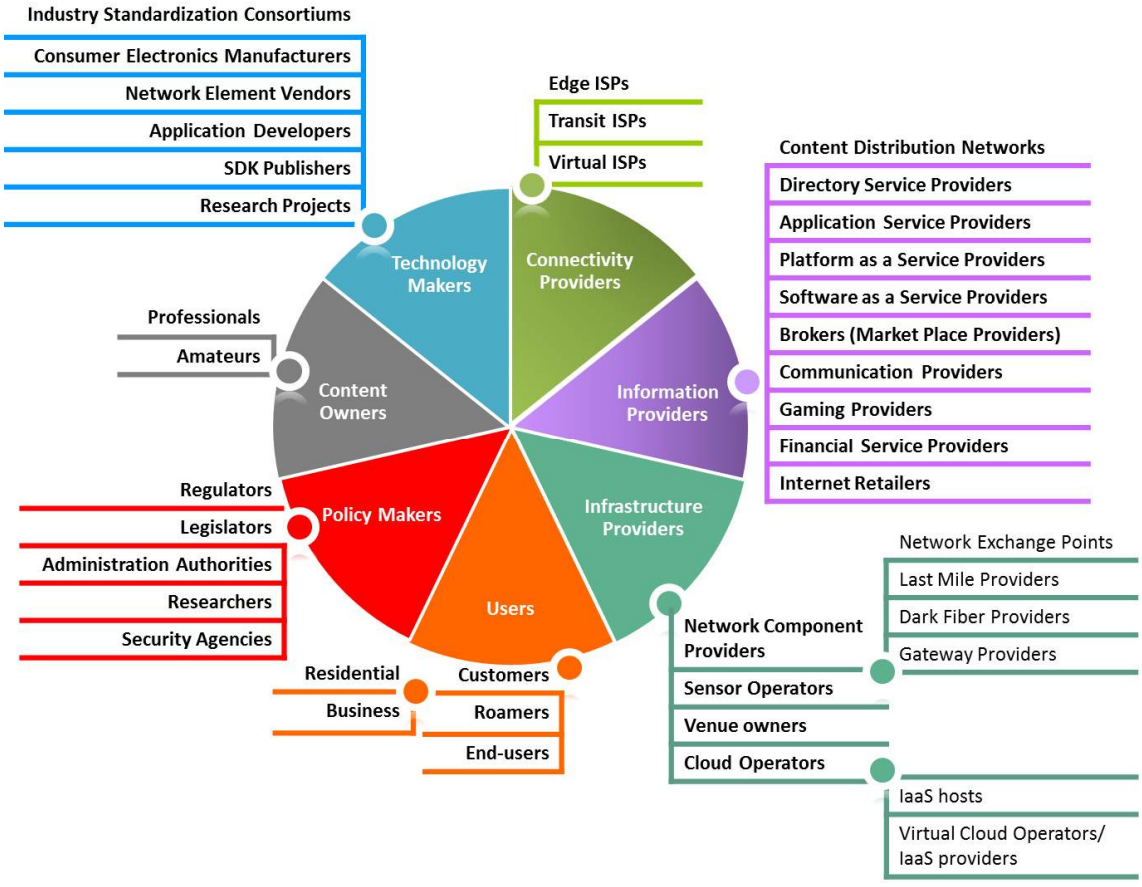
- Fabrikanten van netwerkapparatuur
- Fabrikanten van apparatuur van eindgebruikers
- Fabrikanten van chips/chipsets en andere specifieke hardware (bijvoorbeeld om hardware acceleratie mogelijk te maken.

[15] https://www.internetsociety.org/wp-content/uploads/2017/09/factsheet_ecosystem.pdf en https://www.internetsociety.org/wp-content/uploads/2016/04/IG-MultiStakeholderApproach.pdf

[16] http://www.seserv.org/fise-conversation/ataxonomyforfutureinternetstakeholders

- Ontwikkelaars van software (operating systemen, generieke software, zoals browsers en specifieke software voor specifieke toepassingen) die geïnstalleerd worden op apparatuur van derden
- Ontwikkelaars van diensten geleverd over de netwerken, zoals websites, videoconferencing, gaming etc.
- Ontwikkelaars van generieke infrastructuur (zoals CDN's, cloud computing etc.) die gebruikt worden door dienstverleners
- Aanbieders van telecommunicatienetwerken en diensten
- Beheerders van private netwerken en diensten, bijvoorbeeld academische netwerken, militaire netwerken, overheidsnetwerken, groot zakelijke gebruikers, multinationals etc.
- Academici
- Research and Development organisaties
- Consultants (zowel bedrijven als individuen)
- Overheden (beleidsmakers, toezichthouders)
- NGO's

De lijst is lang. Afhankelijk van de dynamiek zijn er meer of minder partijen bij de standaarden betrokken.



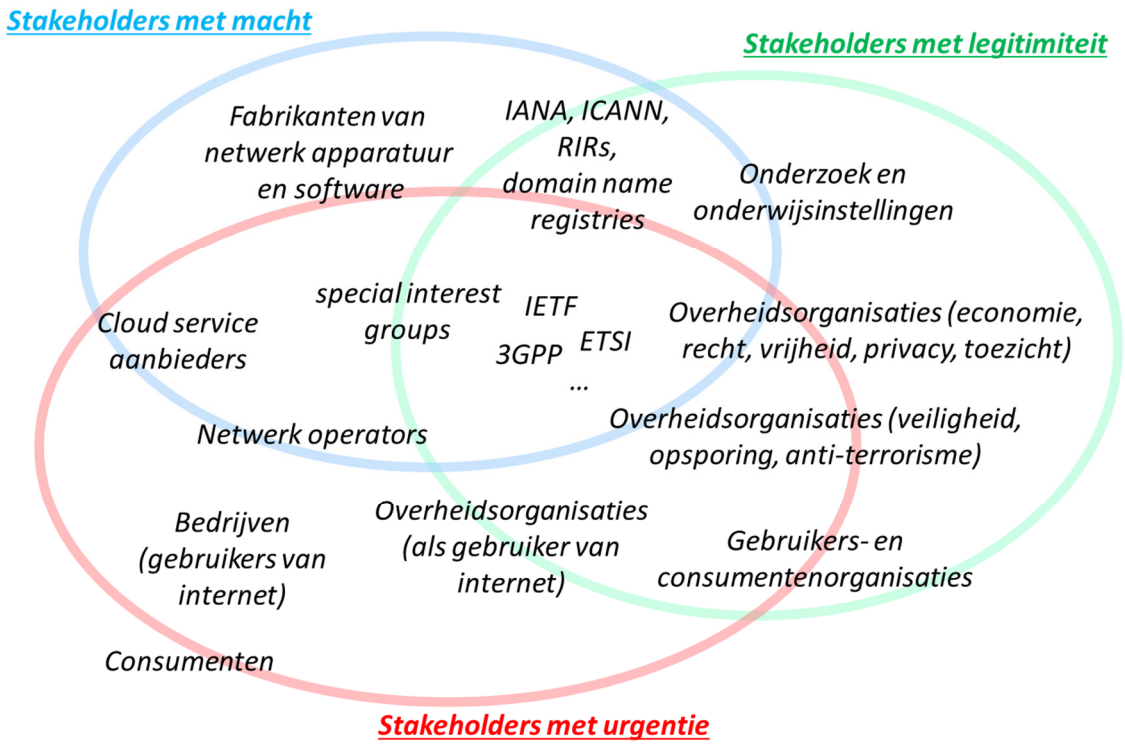
Figuur 6: Mogelijke taxonomie voor stakeholders van het internet van de toekomst (bron: SESERV)

Uit de interviews werd duidelijk dat zelfs ervaren deelnemers aan standaardisatieprocessen niet alle facetten en mogelijke gevolgen van een standaard kunnen doorgronden. De ideale deelnemer is niet alleen bekend met standaardisatie en implementatie van techniek, maar ook met bedrijfsprocessen, ethiek, economische speltheorie, etc.

Naast de actieve deelnemers zijn er ook nog stakeholders die bewust of onbewust indirect invloed uitoefenen. De verschillende typen stakeholders die relevant zijn voor dit onderzoek kunnen globaal volgens de "Mitchell stakeholder typologie" (Mitchell et al. 1997) worden getypeerd. Hierbij worden stakeholders voorzien van een drietal attributen ten aanzien van een bepaald thema, in dit geval het veranderen van de fundamenten van internet:

- Urgentie die een stakeholder voelt om onmiddellijke aandacht te vragen;
- Macht om een andere stakeholder te bewegen om iets te doen wat ze uit zichzelf niet zouden doen;
- Legitimiteit: algemene perceptie dat de stakeholder acties gepast zijn binnen een systeem van normen, met andere woorden wordt de stakeholder gezien als de partij die hier aandacht aan moet geven?

Stakeholders die meer van deze attributen vertegenwoordigen zijn succesvoller in het realiseren van hun prioriteiten ten aanzien van het thema. De methodiek helpt bij het maken van stakeholder overzichten, het bepalen van relevantie van stakeholders en het nadenken over of en hoe stakeholders te bewegen zijn tot meer aandacht voor het thema.



Figuur 7: Globaal overzicht stakeholders (indeling volgens Mitchell typologie (Mitchell et al. 1997))

Leveranciers van netwerkapparatuur en software zorgen uiteindelijk voor implementatie en succes van bepaalde veranderingen, maar hebben niet altijd urgentie en worden vanwege

afzonderlijke bedrijfsbelangen ook niet altijd vertrouwd als zij in hun eentje oplossingen voorstellen.

Meer verticaal georganiseerde bedrijven zoals cloud service aanbieders voelen voor een aantal issues meer urgentie (of zien meer voordelen van veranderingen doordat afhankelijkheden tussen functionele lagen in hun praktijk zichtbaarder zijn). Dit geldt met name voor bedrijven die zowel aan de devicezijde (bijvoorbeeld operating systemen) als aan de netwerkzijde meerdere functies vertegenwoordigen.

Overheden kennen hier verschillende gezichten: als gebruiker of aanjager van economie en bewaker van de vrijheden van de rechtsstaat hebben ze soms andere belangen en prioriteiten dan als veiligheidsbewaker.

Netwerk operators vormen een belangrijke schakel in uitrol van veranderingen maar hebben verschillende belangen die de urgentie kunnen beïnvloeden: Is bijvoorbeeld het kunnen monitoren van inhoud of bepaalde metadata een bedrijfsmatige behoefte, wordt het door overheden geëist, of levert het bedrijfsmatige voordelen en/of overheidsgoedkeuring op om dit juist niet te (kunnen) doen?

De academische wereld is de bakermat van veel van de huidige internetfundamenten maar is steeds minder bij machte om het internet fundamenteel bij te sturen, gewoonweg omdat er al zo veel bestaande apparatuur en programmatuur aanwezig is, en er veel gevestigde belangen zijn.

De eindgebruikers zijn zeer beperkt bij machte om invloed uit te oefenen, en veel consumentenorganisaties voelen hier ook niet of nauwelijks noodzaak toe. De zaken waar consumenten direct mee te maken hebben spelen zich voornamelijk af op hogere lagen. De basis van het internet wordt veelal gezien als voldongen feit[17].

Een deel van de organisaties die het internet draaiende houden hebben wel de macht en legitimiteit maar vaak niet grote urgentie met betrekking tot fundamentele veranderingen. Wel zijn zij betrokken bij het signaleren van de noodzaak voor een aantal meer incrementele oplossingen.

Daarnaast zijn er voor een aantal thema's special interest groups zoals beschreven in 3.1.7. Dergelijke groepen zijn vaak belangrijk omdat er bepaalde issues worden gesignaleerd en mogelijke oplossingen besproken.

De verschillende standaardisatieorganisaties combineren urgentie, macht en legitimiteit het best. Maar per issue kan met name de gevoelde urgentie en de macht verschillen per standaardisatieorganisatie (bijv. door belangen van deelnemende organisaties).

3.2.2 Multilateraal of multi-stakeholder

Standaardisatieorganisaties worden vaak grofweg ingedeeld in twee categorieën:

i. Multilaterale (ook wel intergouvernementele) organisaties:

[17] Uitzonderingen zijn de netneutraliteitsdiscussie en de privacy discussie, waarin vaak ook consumentenorganisaties deelnemen.

organisaties waarin landen hun soevereine rechten om bepaald telecombeleid uit te voeren op elkaar afstemmen; dit kan leiden tot wereldwijde bindende en door overheden verplichte standaarden,

ii. Multi-stakeholder organisaties:

organisaties waarin verschillende private (en in sommige gevallen ook publieke) organisaties zoals fabrikanten van netwerkapparatuur, fabrikanten van smartphones en netwerkoperators, toezichthouders, en soms ook individuele experts (Apache, IETF) samenwerken om een doel te bereiken, in dit geval een telecom standaard. Dit kan – zeker bij wereldwijd grootschalig gebruik – in de praktijk leiden tot (de-facto) wereldwijd bindende standaarden.

Tabel 2 geeft de belangrijkste verschillen tussen de twee categorieën weer.

Tabel 2: verschillen multilaterale en multi-stakeholder organisaties (bron World Bank Group 2016)

Dimension	Multistakeholder	Multilateral/intergovernmental
Leading principle	Collaborative leadership among stakeholders, with a commitment to resolving particular problems	Sovereign right of governments to determine internet policy and regulation
Representation of stakeholders	Direct engagement of private business and industry, governments, bilateral and multilateral international institutions, civil society and academia, NGOs	National government agency represents interests of all in bilateral and multilateral treaties and agreements, anchored in advice and consultation with all stakeholders
Role of governments	Governments are a key stakeholder, with legitimacy to make decisions	National governments represent other interests in an intergovernmental entity
Process	• Bottom-up participatory • Horizontal across stakeholders • Generally open and transparent	• Top-down consultative • Hierarchical within states and through international agreements and treaties • Intergovernmental negotiations, with open consultation
Examples of relevant bodies and processes	ICANN, Internet Society, World Summit on the Information Society, Internet Governance Forum	ITU, UN, WIPO, WTO

3.2.3 Standaarden en markten

In standaardisatieprocessen werken organisaties, die soms concurrenten zijn, aan een gezamenlijke set van afspraken. Rond een standaard ontstaan markten van vraag en aanbod. Standaarden verminderen de concurrentie op specifieke functionaliteit, maar vergroten de concurrentie op implementaties van de afgesproken standaard.

Standaarden kunnen worden ontwikkeld en vastgesteld door:

- Globale multilaterale gremia, (bijv. ISO, CEN/CENELEC, ITU-T) of multi-stakeholder gremia (bijv. IEEE, 3GPP);
- Regionale multilaterale gremia, men spreekt dan van regionale standaarden (bv ETSI in de rol van Europese standaardisatieorganisatie);
- Nationale standaardisatieorganisaties, men spreekt dan van nationale standaarden (bv NEN standaarden);

- Standaarden van organisaties specifiek voor een industrie of samenwerkingsverband, men spreek dan van industriestandaarden. Dit zijn over het algemeen multi-stakeholder organisaties.

Standaarden kunnen op verschillende manieren "open" of "gesloten" zijn[18].

Standaarden kunnen officieel gesanctioneerd zijn. Men spreekt dan van *de jure* standaarden. Dit zijn bijvoorbeeld de Europese *geharmoniseerde normen*, vastgesteld door één van de drie Europese standaardisatieorganisaties. Lidstaten worden geacht het gebruik van deze normen te bevorderen, bijvoorbeeld door er in regelgeving en in aanbestedingen naar te verwijzen. Een bedrijf kan de norm dan gebruiken om te bewijzen dat een product of dienst aan de wettelijke eisen voldoet, maar kan er ook voor kiezen om op een andere manier aan die eisen te voldoen.

Waar nodig, bijvoorbeeld om de interoperabiliteit te borgen, kan de Europese Commissie het gebruik van deze normen zelfs verplichten[19]. Een typisch voorbeeld is de bekende "SCART" connector, waarbij een verplichte Europese norm[20] er destijds voor heeft gezorgd dat analoge tv-toestellen, decoders en videorecorders van verschillende merken correct samen konden werken.

Als een oplossing de markt domineert en de markt zich daar vervolgens naar schikt, zonder een formeel door een standaardisatieorganisatie vastgestelde norm, dan ontstaat wat men noemt een *de facto* standaard. Soms wordt een dergelijke *de facto* standaard in een later stadium alsnog als formele standaard vastgesteld.

3.2.3.1 Creëren van markten

Als een standaard wordt bepaald en vervolgens door een groot deel van de markt wordt geïmplementeerd kan dit significante organiserende impact hebben op markten, het concentreert competitie rondom een standaard. Een voorbeeld hiervan is de Europese afspraak rond oplaadadapters voor mobiele telefoons[21], hetgeen ertoe leidde dat de meeste fabrikanten van mobiele telefoons (behalve Apple) kozen voor micro-USB en later voor USB-C. Voor consumenten en fabrikanten betekende dit een vereenvoudiging in type opladers en kabels. Het gaf consumenten meer keuze en betere opties om over te stappen van telefoonfabrikant en bestaande opladers (bijvoorbeeld in auto of een extra oplader op werk of vakantieadres) te blijven gebruiken, waardoor de concurrentie tussen deze fabrikanten werd versterkt. Een voorbeeld van een markt waarin dit niet gelukt is, is die van stekkers en wandcontactdozen. Zelfs binnen de EU zijn hier verschillende versies voor in gebruik.

Het falen van standaardisatie heeft er vaak mee te maken dat er al te veel geïnvesteerd is in bepaalde implementaties en daarom ofwel geen consensus meer kan worden bereikt voor een afwijkende versie, ofwel niet genoeg steun in de markt is om deze daadwerkelijk te implementeren.

---

[18] De verschillende varianten van proprietary, non-proprietary, open, free ("(speech vs beer")) licensed, non-licensed etc worden hier niet besproken.
[19] Conform artikel 39 (lid 3 en 4) van de Richtlijn (EU) 2018/1972
[20] CENELEC EN 50049-1, in Nederland (impliciet) vastgelegd in de Regeling breedbeeldtelevisiediensten en normen digitale consumentenapparaten
[21] https://www.dw.com/en/companies-agree-on-standard-mobile-phone-charger/a-4441089

De literatuur laat zien dat gestandaardiseerde markten efficiënter zijn dan niet-gestandaardiseerde markten, en dat standaardisatieorganisaties daarom een beter middel zijn in het formeren van efficiënte markten dan de markt zelf (Yates 2019, Berg 1989).

3.2.3.2 Standaarden als publiek goed

Technische standaarden worden veelal gezien als publiek goed omdat de implementatie van een standaard door een bepaalde actor niet de waarde van de implementatie van een andere actor vermindert (Berg 1989). Dit nodigt andere actoren uit om ook van de standaard gebruik te maken, en organiseert zo een markt die aantrekkelijk is voor zowel de producent van apparatuur, informatie, of diensten als voor de consumenten.

3.2.3.3 'Switching costs'

In niet gestandaardiseerde markten, of markten waarin standaardisatie heeft gefaald, is er vaak sprake van inefficiënties omdat gebruikers niet eenvoudig kunnen wisselen vanwege hoge wisselkosten (Matzler et al 2015). Hierdoor worden gebruikers 'ingesloten' in (mogelijk proprietaire) productseries van een bepaalde fabrikant die niet interoperabel zijn met andere implementaties. Dit remt innovatie omdat het wisselen van product(serie) hoge kosten met zich meebrengt. Hoewel een consument wel zou *willen* wisselen van product houden deze 'switching costs' het vormen van een efficiënte markt tegen. Dit stimuleert op korte termijn voordeel voor fabrikanten die (een deel van) de markt domineren, maar is slecht voor het stimuleren van concurrentie en productinnovatie.

Standaard interfaces tussen componenten verlagen deze kosten. Maar dit is niet alleen op het fysieke vlak een voordeel (denk aan de 220 volt stekker). Gestandaardiseerde netwerkprotocollen (IP) en standaarden voor identificatie van een mobiel apparaat (SIM) waarbij de identificatie niet permanent fysiek gekoppeld is aan een apparaat hebben grote bijdrages geleverd aan een situatie waarin je apparatuur wereldwijd kan gebruiken.

3.2.3.4 Netwerkeffecten

Rondom standaarden, en vooral telecommunicatie standaarden, is er vaak sprake van netwerk-effecten. Dit betekent dat ieder die de standaard adopteert, bijdraagt aan de toename van de waarde van alle anderen in het netwerk die de standaarden ook implementeren. Vervolgens profiteren alle gebruikers en producenten die deel zijn van het netwerk van de groei van het netwerk. Standaarden omtrent veiligheid zijn hier goede voorbeelden van. Zo is HTTPS een standaard die voor aanbieders van web content maar ook voor gebruikers waarde oplevert bij implementatie.

3.2.3.5 Padafhankelijkheid

Het creëren van standaarden vormt niet alleen markten, maar stimuleert ook de ontwikkeling van technologie in een bepaalde richting, en beperkt mogelijk de ontwikkeling van technologieën in een richting die niet goed bij de standaard past. Dit betekent dat bepaalde technologieën en technologieontwikkelingen 'weggeorganiseerd' worden door standaarden. Dit heeft tot gevolg dat beslissingen in de toekomst afhangen van beslissingen die in het verleden zijn gemaakt. Een relatief kleine keuze kan in de toekomst grote impact hebben op keuzemogelijkheden (Cowan en Gunby 1996). Zo leidde de keuze van het aantal bits in een IPv4 adres (32 bits) enkele decennia later tot een tekort aan IPv4 adressen, en daardoor tot oplossingen

voor hergebruik van IP-adressen (Carrier Grade NAT). Een meer structurele oplossing in de vorm van IPv6, met 128-bit adressen, is veel lastiger te implementeren gebleken (zie 3.2.6.3).

Padafhankelijkheid kan leiden tot suboptimale oplossingen, maar is in een complexe ontwikkeling nooit helemaal te vermijden. Wel kunnen deelnemers aan standaardisatieprocessen proberen om zo goed mogelijk rekening te houden met de lange termijn gevolgen van voorgestelde keuzes.

3.2.4 Institutionele processen en cultuur

Behalve de technische en economische prikkels en drijfveren speelt ook de institutionele configuratie van organisaties die standaarden definiëren een rol: welke stakeholders kunnen en mogen meedoen, wat zijn de toegangsdrempels, hoe zijn de rollen verdeeld, welke procedures moeten gevolgd worden, etc. Vaak wordt hier de werking van een infrastructuur bepaald door de meest invloedrijke spelers. Wie er wat en wanneer te zeggen heeft, en hoe dit wordt uitgevoerd kan een serieuze invloed hebben op het standaardisatieproces.

Een van de organisaties die achtergrond en verschillende smaken van de standaardisatieprocessen het meest uitgebreid heeft beschreven is de ETSI. In het document "Understanding ICT standardization: principles and practice" (Abdelkafi et al. 2019) wordt de relatie beschreven tussen standaardisatieproces, achterliggende doelen, en de rol voor innovatie en het strategisch, business en economisch perspectief op standaardisatie.

3.2.4.1 Processen

Bij 3GPP (en sommige werkgroepen binnen ETSI) bestaat een set standaarden uit een aantal 'Stages' die eerst na elkaar en daarna parallel worden uitgewerkt en bijgewerkt. Hierbij vullen standaarden uit de verschillende stages elkaar aan en zijn ieder op hun eigen manier belangrijk in het standaardisatieproces:

- Stage 1 is een opsomming van de (functionele) eisen en service aspecten
- Stage 2 omschrijft de architectuur en rollen
- Stage 3 omschrijft de protocolimplementatie

Bij het maken en onderhouden van standaarden kunnen documenten uit de 3 stages steeds met elkaar worden vergeleken om de consistentie van de standaarden te waarborgen.

Deze wijze van werken is vergelijkbaar met de waterval methode voor softwareontwikkeling. Een voordeel van deze methode is dat de werkwijze erg gestructureerd is. In principe zet de voorgaande stage de kaders waarin een volgende stage kan werken. Als er in een volgende stage vragen zijn over de kaders, mogelijke complicaties of nieuwe wensen, dan leidt tot een wijzigingsverzoek in de voorgaande stage of stages. Het nadeel is dat proces langdurig en formalistisch kan zijn. Hoe goed specificaties ook zijn, bij de implementatie komen de praktische vragen, problemen en onduidelijkheden naar boven. Dat kan leiden tot langdurige trajecten voor wijzigingen of inconsistenties tussen verschillende implementaties.

Bij de andere genoemde organisaties is er geen scherp onderscheid tussen deze "stages"; met name binnen de IETF is het gebruikelijker om de functionele eisen, architectuur en protocolimplementatie in hetzelfde document te presenteren. De IETF manier van werken wordt wel omschreven met "rough consensus en running code". Hiermee wordt bedoeld dat de

ervaringen tijdens de implementatie (het schrijven van werkende software die de standaard implementeert) de keuzes ten aanzien van functionele eisen, architectuur en protocol-implementatie moet voeden. Door een aantal proefimplementaties te maken wordt duidelijk wat in de praktijk kan werken. Deze manier van werken is vergelijkbaar met de "agile" methodes van softwareontwikkeling. Het voordeel van deze manier van werken zijn korte feedback loops. Nadeel kan wel zijn dat de grote architectuur uit het oog wordt verloren en er wordt gewerkt aan deeloplossingen.

3.2.4.2 Specificaties, standaarden en normen

Het verschil tussen een 'norm', een 'standaard', en een 'specificatie' is niet altijd even duidelijk. Verschillende standaardisatieorganisaties gebruiken deze termen verschillend. Soms worden deze termen als synoniem gebruikt, maar waar dit niet zo is, is een norm meestal het zwaarst (meest dwingend), en een specificatie het lichtst. Bij de ETSI bijvoorbeeld is er een verschil tussen:[22]

- EN-documenten (European Standard) die bedoeld zijn om aan Europese regelgeving te voldoen, of naar aanleiding van een verzoek van de EC zijn gemaakt. Deze kunnen, na goedkeuring door de EC, leiden tot een geharmoniseerde standaard;
- ES-documenten (ETSI Standard). Hierbij is het document ter goedkeuring voorgedragen aan alle ETSI leden;
- TS-documenten (Technical Specifications) die door Technical Bodies (werkgroepen op een bepaald gebied) worden uitgebracht, en nog geen formele norm vormen. Een TS-document is vaak een voorloper op een latere EN versie;
- TR-documenten (Technical Reports) zijn geen standaarden, maar kunnen de opmaat vormen naar een standaard (bijvoorbeeld door de gebruikersbehoefte vast te leggen).

De IETF hanteert een wat afwijkend documentgebruik. Genummerde RFC's (Request For Comments) zijn voorstellen voor (veranderingen in) standaarden. RFC's kunnen de status 'Proposed Standard' krijgen, vervolgens 'Draft Standard, en als de standaard volwassen en stabiel geacht wordt krijgt deze de status 'Internet Standard'. Vaak bereikt een document pas de 'Internet Standaard' status als de standaard al breed wordt toegepast.

IPv6 werd bijvoorbeeld in 1995 voor het eerst voorgesteld, in 1997 gepubliceerd in RFC 2460 als 'Draft Standard' en werd eind 2017 (met al behoorlijke implementatie) pas als RFC 8200 gepromoveerd tot 'Internet Standard'.

In ETSI en 3GPP wordt per Release (met een bepaalde feature set) een hele nieuwe set standaarden gepubliceerd, ook van zaken die er in vorige releases ook al waren. Bij de IETF bestaat een dergelijk systeem niet, en wordt alleen een nieuwe versie opgesteld voor standaarden waar een verandering nodig is. Maar mogelijk juist daardoor moet er goed nagedacht worden over compatibiliteit en interoperabiliteit tussen verschillende generaties.

3.2.4.3 Participatie

Per standaardisatieorganisatie zijn de regels anders wie er mee mag doen en onder welke voorwaarde. Mogen alleen staten participeren, of mensen die bij een door staten erkend of

[22] https://www.etsi.org/standards/types-of-standards

aangewezen standaardisatiebureau werken? Mag iedereen meedoen maar moet er wel een contributie betaald worden, of mag iedereen gratis meedoen? En als mensen mee mogen doen, wat is dan hun rol in het standaardisatieproces, voor wie zijn de documenten beschikbaar, welke talen worden gesproken en geschreven en is er vertaling beschikbaar?

Onderzoek laat zien dat de organisaties met de grootste *staying power,* kortom de organisaties met de mensen die het langst in de standaardisatieorganisatie participeren, de meeste invloed hebben (Balzarova en Castka 2012). Dat komt omdat zij belangrijke posities in de organisatie bezetten, de meeste mensen kennen, en de regels en procedures van binnenuit kennen. Dit kan ervoor zorgen dat organisaties op deze manier onevenredig grote invloed uitoefenen via directe invloed, via de sleutel- en leiderschapsposities die zij bezetten, of via indirecte invloed door het domineren van discussies.

3.2.4.4 Stemmen en consensus

Standaardisatiesprocessen duren gemiddeld tussen drie en zeven jaar, maar kunnen ook veel korter of langer duren. In deze periode moeten veel beslissingen genomen worden. Hoe vaak en door wie deze beslissingen worden genomen, en hoe hier op wordt toegezien verschilt per standaardisatieorganisatie. Vaak zijn de processen uitvoerig beschreven, maar kennis van de processen wil nog niet betekenen dat men er ook meteen kunde in heeft.

Vaak wordt er binnen werkgroepen informeel gepeild welk voorstel door de meeste leden gesteund wordt. Als een bepaalde coalitie of organisatie veel mensen in de werkgroep heeft kan dit eenvoudig in hun voordeel uitpakken.

Uiteindelijk zeggen de meeste standaardisatieorganisaties uit te zijn op consensus beslissingen, maar wat dit precies betekent is verschillend. Sommige organisatie, zoals de 3GPP, kiezen er zelfs liever voor om dit helemaal niet te definiëren. Consensus hoeft dus niet noodzakelijkerwijs te betekenen dat iedereen het eens is, maar komt neer op een besluit waarbij alle deelnemers afzien van een formele procedure. Soms is het simpelweg dat minderheidsmeningen uitgebreid zijn gehoord, maar door de overgrote meerderheid te licht zijn bevonden of geen steun hebben gekregen, waarna de partijen met de minderheidsmening afzien van verdere promotie ervan.

3.2.4.5 Openheid

In zijn boek ‘Open standards and the digital age’ (Russell 2014) beschrijft Russell hoe *de jure* standaarden plaats lijken te hebben gemaakt in de 21ste eeuw voor een ideologie van vrijwillige open standaarden die gebaseerd zijn op consensusbeslissingen (zie ook paragraaf 3.2.2 over multilateraal versus multi-stakeholder organisaties). Hiermee lijken standaarden gedepolitiseerd te zijn doordat de directe invloed van overheden lijkt te zijn afgenomen, maar dit betekent eerder dat standaarden opgenomen zijn in een globale kapitalistische economie waar multinationale bedrijven en overheden wedijveren om macht en controle over informatiestromen. Dus zijn standaarden hiermee in feite nog steeds niet gedepolitiseerd.

3.2.4.6 Transparantie

Het is niet altijd eenvoudig om standaarden te vinden, toegang tot ze te krijgen, of om vervolgens erachter te komen welke beslissingen aan een bepaalde standaard ten grondslag liggen en welke actoren hieraan hebben bijgedragen. Dit ondermijnt de legitimiteit van

standaarden en bemoeilijkt de participatie van nieuwe deelnemers, en bevoordeelt de partijen die al lang deelnemen.

ETSI en IETF geven iedereen gratis toegang tot hun standaarden, terwijl IEEE en ISO hier geld voor vragen. Bij de IETF zijn ook alle eerdere drafts voor iedereen beschikbaar; bij ETSI is dat in de meeste gevallen beperkt tot de versies die formeel zijn aangenomen.

3.2.4.7 Generaties, Version release, achterwaartse compatibiliteit, en 'flag days'

In veel standaarden worden versienummers gebruikt om verbeterde versies van een document te kunnen onderscheiden van oudere versies. Sommige standaardisatieorganisaties zoals de ETSI en 3GPP gebruiken daarbij het verschil tussen Releases, waarbij alle apparatuur die een bepaalde Release ondersteunt, met elkaar en met apparatuur die vorige Releases ondersteunt zou moeten kunnen interacteren. Binnen elke Release worden vervolgens weer versies onderkend, waarin verbeteringen worden aangebracht. Ook oude, bestaande standaarden, worden soms herzien om fouten of onduidelijkheden op te lossen.

Standaardisatieorganisaties hebben met de manier waarop zij versies inrichten een grote invloed op hoe een markt zich kan vormen, maar actoren in een markt kunnen ook weerbarstig zijn en zich niet conformeren aan de (nieuwere) standaard.

In het vroege internet was er nog wel eens sprake van 'flag days', specifieke dagen waarop een bepaald protocol, of een versie daarvan, niet meer ondersteund zou worden en men overal tegelijk over zou gaan op een nieuwe methode. Dit mechanisme kon helpen om de eerdergenoemde padafhankelijkheid te doorbreken.

Inmiddels is het internet te groot geworden om dat gecoördineerd te doen, en wordt in het algemeen gepoogd om standaarden achterwaarts compatibel te houden (backwards compatability) zodat iedereen zelf kan kiezen wanneer zij een nieuwe versie introduceren. Maar als men backwards compatability continu in acht moet nemen, betekent dit dat de toekomst er altijd een beetje als het verleden uit blijft zien.

Een aantal protocollen rond adressering zijn in de loop van de tijd relatief stabiel gebleven met hier en daar incrementele verbeteringen. Een belangrijk aspect van netwerkstandaarden op de link laag, zoals Ethernet, wifi, Bluetooth, PON en LTE, is dat deze standaarden veranderen naarmate door snellere en goedkopere rekenkracht de dragers (koperleidingen, glasvezelkabels, frequentiegebieden voor radioverbindingen) beter benut kunnen worden. Dat betekent dat eens in de zoveel jaar er een nieuw type transmissie mogelijk wordt die daarvoor nog te duur was waarbij er significant hogere datasnelheden kunnen worden bereikt door data op een andere manier te verzenden en te ontvangen. Die ontwikkeling gaat over het algemeen in generaties, waarbij apparatuur van dezelfde generatie optimaal met elkaar samen werkt, maar waarbij er ook teruggevallen kan worden op standaarden uit eerdere generaties als één van de participerende apparaten de nieuwe standaard nog niet implementeert. Voor Ethernet is de aanduiding veelal via de bandbreedte, 10Gbps, 40 Gbps, 100Gbps etc. Voor wifi wordt er nu in de marketing gebruik gemaakt van cijfers, "Wi-Fi 5", "Wi-Fi 6" en binnenkort "Wi-Fi 7". In mobiele netwerken 2G, 3G, 4G met eventueel tussentijdse updates[23]. Dit zorgt voor een

[23] Strikt genomen werkt 3GPP met releases, een generatie beslaat vaak meerdere releases. Documenten binnen dezelfde release werken samen met apparatuur die aan deze en

dynamiek van cyclussen. De cyclussen in de 3GPP zijn ruwweg 10 jaar. Ieder nieuw decennium heeft zijn eigen nieuwe generatie mobiele technologie.

De nieuwe generaties worden mogelijk omdat de technologische ontwikkeling in ICT gedreven wordt door continue verbeteringen in hardware en software. Hierdoor zijn er na een aantal jaren technisch en functioneel nieuwe mogelijkheden die niet of niet efficiënt te realiseren waren in een voorgaande versie. Voor de participanten in de standaardisatie zijn cyclussen nodig, omdat zowel antennes, core netwerkapparatuur als terminals in hardware en software aan de nieuwe specificatie moeten voldoen. Als een element ontbreekt, dan werkt het niet. Dit zet druk op deelnemers om er onderling uit te komen.

Deadlines zorgen voor focus, maar ook tot conflictmijding. Focus zorgt ervoor dat alleen haalbare elementen in de standaard komen, terwijl conflictmijding leidt tot acceptatie van elementen die later niet (of niet goed) worden geïmplementeerd. Alhoewel de leveranciers klaar moeten zijn voor een nieuwe generatie technologie, betekent dit niet dat de gebruikers direct deze nieuwe generatie moeten implementeren. Bedrijven, telecomaanbieders en consumenten wachten vaak met het vernieuwen van het netwerk en activatie van een nieuwe generatie, tot een moment dat voor hen relevant is.

In de hogere netwerklagen, zoals die van het internet en de applicaties hier overheen, zijn updates incrementeel in plaats van in generaties. Er wordt gewerkt met versies die naast elkaar en met elkaar kunnen functioneren. Het functioneren en de functionaliteit op deze lagen wordt minder bepaald door vernieuwing in chips en software. Het zijn afspraken die werken over een veelheid van netwerken heen.

3.2.4.8 Ossificatie

Tegenstanders van incrementele standaardisatie stellen vaak dat incrementele oplossingen tot ossificatie leiden. Met ossificatie wordt een verstarring bedoeld, waarbij er geen fundamenteel nieuwe standaarden meer gerealiseerd kunnen worden, maar moet worden doorgebouwd op bestaande protocollen, mede vanwege de achterwaartse comptabiliteit (zie hierboven).

Het doorbouwen op bestaande oplossingen leidt daarbij tot steeds complexere protocollen, zoals bij DNS dat inmiddels duizenden pagina's aan RFC's beslaat die allemaal van elkaar afhankelijk zijn.

De ossificatie wordt met name veroorzaakt door de grote "installed base" van de bestaande standaard en het gebrek aan prikkels om daar iets aan te veranderen. Het feit dat 5G New Radio (de nieuwste generatie van 3GPP radio standaarden) bijvoorbeeld nu al breed geïmplementeerd is, komt omdat 5G NR daadwerkelijk grote voordelen biedt ten opzichte van 4G LTE (dus een prikkel om te veranderen), en bovendien selectief per netwerk of per locatie geïmplementeerd kan worden (dus een beslissing per aanbieder, onafhankelijk van anderen). De "core" van het netwerk kan daarentegen ook 4G blijven, zonder al te grote nadelen, en daardoor zijn er nog vrijwel geen 5G core implementaties in de grote mobiele netwerken.

---

voorgaande releases voldoet. Binnen releases zijn updates van hetzelfde document (bug fixes) en interne verbetervoorstellen weer apart genummerd zodat ze uit elkaar te houden zijn.

Een ander voorbeeld van een "verstard" protocol is het signaleringsprotocol SS7. Het laat zien hoe complex vervangen is, wanneer er geen overweldigende druk is vanuit bijvoorbeeld een technische vernieuwing. SS7 stamt uit 1975 en verzorgt de signalering binnen en tussen telefoonnetwerken, waaronder mobiele netwerken. Het heeft wel veel uitbreidingen gekregen voor 3G en 4G, maar is in de basis onveranderd, en veelal compatibel met voorgaande versies. Het protocol beval een veelheid aan bekende kwetsbaarheden die fraude, spam en afluisteren mogelijk maken (Pelman 2020).

Het vervangen van SS7 blijkt zo goed als onmogelijk, omdat er te veel voorgaande en regionale varianten van de implementatie zijn, waar nationale afspraken en bedrijfsmodellen van afhankelijk zijn. Zo zijn nummerplannen en de bijbehorende implementatie van nummerportabiliteit nationaal georganiseerd. In het ene land gebruiken mobiele telefoons lokale geografische nummers en in het andere land een specifieke reeks, zoals 06 in Nederland. Nummerportabiliteit wordt in het ene land geïmplementeerd door het verkeer voor een nummer altijd via het oorspronkelijke netwerk te routeren (bv. in VK) en in andere landen, zoals Nederland direct naar het ontvangende netwerk. Het uitfaseren en beveiligen van SS7 is een langgekoesterde wens van overheden en operators, maar lijkt de komende jaren niet waarschijnlijk, sterker nog het is ook weer de basis voor 5G.

3.2.4.9 Standaardisatieculturen

Organisaties hebben hun eigen cultuur – zo is dit ook met standaardisatieorganisaties. In de IETF zal men weinig mensen met mantelpak of kostuum tegenkomen, bij ITU-T studiegroepen is het tegenovergestelde het geval, en vind je juist minder mensen die meer casual gekleed gaan. Ook de communicatie- en omgangsstijlen kunnen sterk verschillen. Dit maakt het voor mensen met bepaalde culturele achtergronden eenvoudiger of complexer om deel te nemen in het standaardisatieproces. Veruit de meeste standaardisatieprocessen worden gedomineerd door bedrijven en deelnemers uit Europa en de VS, alhoewel hier nu verandering in lijkt te komen door de toenemende participatie vanuit Koreaanse en Chinese bedrijven. Deze bedrijven lopen qua invloed en leiderschapsposities echter nog steeds achter bij hun concurrentie uit de VS en Europa (Baron en Kanevskaia 2021).

3.2.5 Grillige werkelijkheid

3.2.5.1 Standaardisatie versus Implementatie

Als men nu een nieuwe implementatie zou maken van het Domain Name System (DNS), grofweg het telefoonboek van het internet, en dat zou doen op basis van de RFC's die het DNS beschrijven, dan zou deze implementatie niet werken op het moderne internet. Standaarden beschrijven een perfecte wereld zoals men deze voor zich zag ten tijde van standaardisatie. Maar de implementatie werkelijkheid is vaak weerbarstig. Er worden innovaties gedaan, en de markt beweegt verder. Soms vinden deze verbeteringen hun weg terug naar de RFC's, maar vaak ook niet: mensen in het veld weten hoe ze iets moeten implementeren zonder dat het formeel gedocumenteerd wordt.

Een voorstel tot standaardisatie is nog geen garantie op standaardisatie, en standaardisatie is ook geen garantie voor implementatie. Er zijn meer gefaalde dan succesvolle voorstellen, en voor het succes van een standaard hoeft de implementatie niet noodzakelijkerwijs helemaal 'standard compliant' te zijn.

In de IETF wordt getracht de verbinding tussen standaardisatie en implementatie te leggen door te eisen dat er werkende implementaties zijn van de standaard, voordat deze in een RFC wordt vastgelegd. Toch is dit lang niet altijd voldoende voor een goed werkende standaard. Een voorbeeld is het toevoegen van extension headers in IPv6. Deze zijn bedoeld om in de toekomst nieuwe informatie in de headers van een packet op te kunnen nemen voor nieuwe diensten, standaarden of functionaliteiten in netwerken. Het blijkt dat juist deze extension headers implementatie van IPv6 in hardware van routers moeilijk maakt. Door de verwerking van IP-headers in specialistische router chips te laten plaatsvinden, kan een router veel sneller en efficiënter werken dan in software op een normale CPU. Zo kan een nieuwe Cisco router chip 25 Terabit/s verwerken (ruwweg net zoveel als alle data op het netwerk van KPN en VodafoneZiggo samen). Maar in hardware nieuwe instructies toevoegen die de extension headers verwerken is echter niet eenvoudig, of zelfs niet mogelijk, daarvoor is nieuwe hardware nodig. Extension headers bieden in de praktijk dus veel minder flexibiliteit voor nieuwe diensten, standaarden of functionaliteiten dan was beoogd.

Implementatie staat in de 3GPP wereld op grotere afstand van de standaardisatie dan bij de IETF. De waterval methode waar de 3GPP mee werkt, en de veel meer aanwezige vertegenwoordiging door bedrijven, leidt er vaak toe dat er in de standaard een verzameling opties is die onderling niet of niet voldoende samenwerken. Het samenwerken van twee apparaten van verschillende fabrikanten die volgens de standaard werkt kan dan soms leiden tot het netjes onderhandelen over een bepaald subprotocol, om er vervolgens achter te komen dat alleen een oud protocol door beide apparaten wordt ondersteund. De strijd welke opties uiteindelijk gemeengoed worden wordt zo vaak na standaardisatie nog in implementatie en daadwerkelijke deployment uitgevochten, waarbij standaardisatieorganisaties en GSMA uiteindelijk bepaalde ‘profielen’ van opties promoten.

3.2.5.2 Monopolies en oligopolies

In monopolies en oligopolies zijn er één of enkele partijen die de markt domineren. Dit kan innovatie verstoren, een drempel veroorzaken voor nieuwkomers en zorgen voor hoge prijzen door oneerlijke concurrentie. De vorming van monopolies en oligopolies heeft een negatief effect op open standaardisatie omdat een monopolist de *de facto* standaard bepaalt. Op dit moment tekent zich een situatie af in de internetmarkt waarin er zich steeds verdere sectoroverschrijdende consolidatie plaatsvindt. Zo beheerst Google zowel de zoekmachine (en andere platformen) als de browser, en is bijvoorbeeld Facebook ook ondersteuner van Magma, een softwareoplossing voor het management van 5G netwerken.

Hier komt nog bij dat standaardisatie op de lagere lagen van het internet steeds ingewikkelder wordt, voornamelijk vanwege de complexe implementatie realiteit. Dit betekent dat uitvoerige testen nodig zijn voor een protocol op schaal te kan werken op het internet. Hiervoor is controle en inzicht over grote delen van het internet nodig (bijvoorbeeld zoals Google deed bij QUIC, door testen te draaien tussen Google Chrome browsers en Google-servers over de hele wereld). Dit is niet voor veel actoren weggelegd, wat innovatie alleen nog maar mogelijk maakt voor een steeds kleinere groep bedrijven die daardoor nog meer marktmacht krijgen.

3.2.6 Praktijkvoorbeelden

Enkele praktijkvoorbeelden die hier onder worden geschetst tonen zeer beknopt de geschiedenis van een aantal protocollen, en de processen rond de ontwikkeling ervan. Waar geen organisatie is vermeld gaat het steeds om ontwikkelingen binnen de IETF.

3.2.6.1 Verbetering van veilig, betrouwbaar en efficiënt gegevenstransport

Over het internet vond end-to-end gegevensuitwisseling oorspronkelijk plaats via TCP (data versturen in pakketten met ontvangstbevestiging) en later, voor sommige applicaties, via UDP (data versturen in pakketten zonder ontvangstbevestiging). Daaroverheen kwamen protocollen op als HTTP (versturen van webpagina's, in eerste instantie ontwikkeld door CERN en later W3C, nu samen met IETF). De behoefte groeide om dergelijke informatie op een standaard manier te kunnen versleutelen zodat niemand tussen bron en eindpunt de gegevens zou kunnen inzien.

Dit leverde protocollen als HTTPS (veilige HTTP), dat weer gebruik maakt van TLS (of vroeger SSL). Een nieuwer alternatief voor HTTPS is HTTP via QUIC. QUIC maakt nog steeds gebruik van TLS, maar vult een deel van de functies van TCP zelf in, waardoor het gebruik kan maken van UDP. Gebruik van QUIC is in de meeste gevallen efficiënter dan HTTPS en TCP.

QUIC is voor een groot deel door Google ontwikkeld, en vervolgens ingebracht bij de IETF waar het verbeterd werd voordat het een internet standaard werd.

3.2.6.2 Verbetering van het opzoeken van DNS

DNS, het Domain Name System dat op internet namen zoals www.stratix.nl vertaalt naar IP-adressen, is een gedecentraliseerd systeem van apparaten (DNS servers). Elk apparaat op internet kan een DNS server instellen waardoor deze namen kan laten opzoeken. Niet bekende namen (of delen van namen) worden door doorverwijzingen naar andere DNS servers opgezocht. Om het systeem efficiënter te maken wordt op veel plaatsen opgezochte informatie een tijdje bewaard (caching) zodat niet bij elke opzoekactie veel servers hoeven te worden benaderd.

Dit systeem werkte heel lang prima maar heeft mogelijke nadelen: DNS servers moeten elkaar vertrouwen dat ze de goede informatie doorsturen, en de eindgebruiker moet erop kunnen vertrouwen dat bij de naam uiteindelijk het goede IP-adres wordt geleverd. Het is mogelijk om malafide antwoorden te sturen, en daarmee de gebruiker (bijvoorbeeld) naar de verkeerde website te sturen. Dit risico kan voorkomen worden met DNSSEC, maar dat vereist wel dat beide kanten (de vragende partij en de eigenaar van de zone) het geïmplementeerd hebben.

Verder zijn bij DNS de opgevraagde namen en geleverde IP-adressen op veel plaatsen door derden in te zien, waardoor het mogelijk wordt om te zien met welke systemen gebruikers informatie uitwisselen. Oplossingen hiervoor DNS over HTTPS (ook wel DoH genoemd), en DNS over TLS. DNS over HTTPS is tegenwoordig in veel browsers aanwezig; bij sommige staat het zelfs standaard aan. Er is veel discussie hierover, want tegenover de privacyverbetering die het oplevert staat ook dat degene die de DNS over HTTPS-server beheert (bijvoorbeeld Cloudflare) juist meer privacygevoelige informatie krijgt.

3.2.6.3 IPv6 als verbetering van IPv4

IP werd bedacht in een tijd waarin efficiënt netwerkgebruik nog belangrijk werd gevonden, en onnodig verzenden van bits als verspilling werd gezien. De in IP versie 4 (IPv4) gebruikte adresgrootte van 32 bits leek bij introductie zeer ruim gedimensioneerd om alle denkbare IP-apparatuur ter wereld te kunnen adresseren. Maar het grote succes van internet en de inzet van steeds meer goedkope apparaatjes met een eigen adres zorgde ervoor dat men zich eind vorige eeuw realiseerde dat IP-adressen schaars zouden gaan worden, en dat IPv6 werd gestandaardiseerd[24].

IPv6 vergroot niet alleen de adresruimte uit van 32 naar 128 bits, waardoor het aantal mogelijke adressen van 4,3 miljard naar 3,4 x 10^{38} wordt uitgebreid, maar er werden ook een aantal nieuwe eigenschappen geïntroduceerd zoals meer ingebouwde features ten behoeve van multicast, versleuteling en mobiliteit.

Ondanks dat het aantal IPv4 adressen steeds schaarser werd, verloopt grootschalige introductie van IPv6 moeizaam: wereldwijd is nog maar zo'n 35% van de eindpunten[25] IPv6, en Nederland zit hierbij ongeveer op dit gemiddelde.

3.3 Rol van overheden

Overheden kunnen verschillende rollen vervullen in standaardisatieprocessen:

- Overheden kunnen kaders stellen middels regelgeving (bijvoorbeeld via de Algemene Verordening Gegevensbescherming, AVG, en de aanstaande Digital Markets Act);
- Overheden kunnen zelf actief participeren in standaardisatie;
- Overheden kunnen stimuleren dat bedrijven en wetenschappelijke instellingen actief participeren in standaardisatie, en contact onderhouden met de betrokkenen (bijv. via verband van Platform Internetstandaarden);
- Overheden kunnen zelf standaarden gebruiken (via Forum Standaardisatie);
- Overheden kunnen waarschuwen voor ongewenste effecten van bepaalde standaarden (zoals het Nederlandse Nationaal Cyber Security Centrum)
- Overheden kunnen het gebruik van standaarden stimuleren (zoals de factsheet over routing security van AT) en in sommige gevallen zelfs verplichten voor (een deel van) de markt (een voorbeeld is de huidige discussie over IoT en security: Nederland en de Europese Commissie willen daar naar een geharmoniseerde standaard toe, in het kader van de Radio Equipment Directive[26]).

Uiteraard zijn er enkele gebieden waar overheden de enige, of de belangrijkste gebruiker is. Voorbeelden daarvan zijn Legal Interception (aftappen) en TETRA (zoals C2000 in Nederland). In die gevallen moet de overheid wel participeren om de stem van de gebruiker binnen de standaardisatie te laten horen. Voor de standaardisatie van aftapmogelijkheden werken belanghebbenden vanuit overheden samen met fabrikanten en operators in ETSI[27] en 3GPP[28].

[24] Draft standaard in ietf in 1998, internet standard in 2017.
[25] Zie https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption
[26] Zie https://www.agentschaptelecom.nl/onderwerpen/handel-en-apparatuur/digitale-veiligheidseisen-aan-iot-apparaten
[27] Zie https://www.etsi.org/technologies/lawful-interception
[28] Zie https://www.lawfulinterception.com/explains/3gpp-sa3-li/

Voor TETRA vindt de standaardisatie geheel plaats binnen ETSI[29], waarbij de openbare orde- en veiligheidsdiensten (politie, brandweer en ambulance) de belangrijkste gebruikers zijn.

Uit de literatuur blijkt dat het in andere gevallen direct participeren van overheden in standaardisatieprocessen in multi-stakeholder standaardisatielichamen significante negatieve invloed kan hebben op het wereldwijde vertrouwen in standaarden (deNardis 2014, Yates en Murphy 2019). Er bestaat dan een reële kans op het ondergraven van reputaties, met negatieve impact op mogelijkheid van toekomstige interventies en het ondergraven van vertrouwen in het standaardisatieproces in het algemeen. Een bekend voorbeeld daarvan is de poging van de Amerikaanse NSA om invloed uit te oefenen op de kwaliteit van de encryptiestandaarden binnen IETF (Rogers en Eden 2017).

Recenter werd binnen ETSI, onder andere op aandringen van het Britse NCSC[30], met eTLS (zie ook 6.2.5), een onveiliger encryptievorm gestandaardiseerd dan de IETF-versie. De reacties hierop laten zien dat een overheid er weliswaar toe kan bijdragen dat een standaard tot stand komt, maar dat het resultaat twijfelachtig is en het vertrouwen in die overheid (en de betreffende standaard) kan schaden.

Van overheden wordt daarentegen wel verwacht dat zij scherpe randvoorwaarden stellen aan standaarden en implementatie wat betreft veiligheid, beschikbaarheid en soevereiniteit. Het Nederlandse NCSC (Nationaal Cyber Security Centrum) waarschuwt bijvoorbeeld uitdrukkelijk tegen het gebruik van de bovengenoemde eTLS variant (NCSC 2019).

Maar om randvoorwaarden te stellen hoeft de overheid niet in de multi-stakeholder standaardisatie te participeren; dit kan efficiënter worden bereikt door regulering waaraan de markt (en waar nodig, de standaard) zich kan aanpassen. Een bekend voorbeeld is de privacywetgeving, die indirect leidt tot standaarden waarmee bedrijven en instellingen beter in staat stellen om deze wetgeving na te leven.

De Nederlandse overheid kan onder meer signalen geven over het belang van Europese en mensenrechtenwaarden, ook in het kader van standaardisatie, en waar mogelijk tegenwicht bieden als landen proberen oneigenlijk gebruik te maken van 'forum shopping'. Het bevestigen van de relatie tussen technische normen, sociale en legale normen en maatschappelijke waarden en het ontwikkelen van een geïntegreerde visie hierop zou hieraan kunnen bijdragen.

Voor de geloofwaardigheid van een dergelijke geïntegreerde visie is het van belang dat de overheid de ontwikkeling van standaarden volgt, en een helder beleid voert op navolging van specifieke standaarden binnen de overheid en de Nederlandse kritieke infrastructuren. Dat geldt met name voor standaarden die belangrijk zijn voor de beveiliging, zoals TLS, DNSSEC, BGPsec, en RPKI. In Nederland gebeurt dit al via het Forum Standaardisatie.

[29] Zie https://www.etsi.org/technologies/tetra
[30] Zie https://www.ncsc.gov.uk/blog-post/tls-13-better-individuals-harder-enterprises

3.4 Conclusies

Om de onderzoeksvragen te kunnen beantwoorden, is enige achtergrondinformatie over standaardisatie essentieel. Deze achtergrondinformatie is in dit hoofdstuk behandeld. Met name de hieronder genoemde conclusies zijn relevant voor de beantwoording.

Standaardisatie heeft in zijn algemeenheid een positief effect voor de marktwerking. Standaarden maken interoperabiliteit van apparatuur mogelijk, waardoor afnemers van deze apparatuur niet meer aan één leverancier vastzitten. Voor geïnterconnecteerde netwerken stimuleren standaarden bovendien de interoperabiliteit tussen die netwerken.

Op het gebied van de telecommunicatie is een groot aantal standaardisatielichamen actief, maar voor de lagen binnen de scope van deze opdracht zijn vooral IETF en 3GPP relevant. Deze twee zijn zeer verschillend georganiseerd, maar er zijn ook belangrijke overeenkomsten: beide streven naar open standaarden (voor maximale interoperabiliteit), en naar standaarden die wereldwijd ingezet kunnen worden.

Het succes van een standaard wordt bepaald door de implementatie. Veel standaarden, of onderdelen daarvan, blijven ongeïmplementeerd omdat fabrikanten en afnemers er geen behoefte aan hebben en er sprake is van vrijwilligheid.

Ook als standaarden wel geïmplementeerd worden kan het lange tijd duren voordat ze gemeengoed zijn. IPv6 is bijvoorbeeld al ruim twintig jaar beschikbaar maar is nog slechts op 35% van de eindpunten actief, voornamelijk omdat de meeste partijen er geen directe noodzaak toe zien om het te implementeren.

Slechts weinige partijen hebben de benodigde marktmacht om implementatie van een nieuwe standaard af te dwingen; Google is (met QUIC als voorbeeld) een dergelijke partij.

Overheden kunnen een rol spelen in standaardisatie. Voor de multi-stakeholder standaardisatieorganisaties zoals de IETF is het effectiever om die invloed op afstand uit te oefenen, door contact te houden met mensen en instituten die bij de standaardisatie betrokken zijn.

Overheden kunnen bovendien een rol spelen bij de implementatie van standaarden, door zelf het voortouw te nemen, door te stimuleren en voor te lichten, en waar nodig zelfs via regelgeving.

4 Waarden en netwerken

The Internet isn't value-neutral, and neither is the IETF.

— Mission Statement of the IETF (Alvestrand 2004)

Aangezien de onderzoeksvragen onder andere ingaan op de maatschappelijke waarden in relatie tot standaardisatie, is het belangrijk om deze maatschappelijke waarden eerst te benoemen. Dit hoofdstuk identificeert daarom de normen en waarden die expliciet of impliciet achter het ontwerp van diverse geïnterconnecteerde netwerken schuilen, om daar in de volgende twee hoofdstukken naar te kunnen refereren.

Het hoofdstuk gaat in op de achterliggende idealen en hun internationale context (paragraaf 4.1), mensenrechten (paragraaf 4.2), belangrijke maatschappelijke politieke waarden in Nederland en Europa (paragraaf 4.3) en de ontwerpprincipes van het internet (paragraaf 4.4).

De laatste paragrafen (4.5 en 4.6) reflecteren op de verschillende typen waarden, en geven een samenvatting.

4.1 Normen en Waarden

Sociale en technische normen tonen veel gelijkenissen. Normen zijn 'breed geaccepteerde en geïnternaliseerde principes of gedragscodes die aangeven welke gedrag gezien wordt als toegestaan, verboden of verwacht van leden van een bepaalde gemeenschap' (Erskine en Carr 2016). Normen reguleren dynamische systemen zoals de samenleving en het internet door het creëren van gemeenschappelijke verwachtingen zonder het voorschrijven van specifiek gedrag voor iedere situatie. Hoe normen worden toegepast in specifieke situaties wordt overgelaten aan individuen (Okuyama, Bordini, en da Rocha Costa 2011). Dit is wat normen bij uitstek geschikt maar voor het aansturen van gedistribueerde architecturen.

Waarden zijn de achterliggende idealen die als waardevol worden aangeduid. Waarden hebben weer overeenkomsten met normen; net als normen zijn waarden fenomenen op groepsniveau gebaseerd op gezamenlijke instemming. Waarden beschrijven echter niet wat mag of wat niet mag en voorzien dus niet in een evaluatieve beschrijving van gewenst gedrag. Normen beschrijven wat er wordt verwacht terwijl waarden eerder een persoonlijke of cultureel ideaal beschrijven.

Omdat het internet een wereldwijd netwerk van netwerken is, is het van belang om een normen en waardenraamwerk te vinden met een gelijke scope. Er zijn echter maar weinig van dergelijke morele globale raamwerken te vinden, en daarom komt men al snel uit op de mensenrechten. Dit is immers de meest wereldwijd verbreide internationale norm die is geratificeerd door bijna alle landen ter wereld. Bovendien is toen het internet initieel werd ontwikkeld niet eerst een normen- en waardenraamwerk vastgesteld, afgesproken of ontstaan. Wel zijn er – deels achteraf – een aantal ontwerpprincipes te onderscheiden (zie paragraaf 4.4).

Naast maatschappelijke normen en waarden spelen er bij de standaardisatie natuurlijk ook technische en bedrijfseconomische aspecten een rol. Deze zijn de ene keer duidelijker dan de andere keer te koppelen aan bredere maatschappelijke waarden.

4.2 Mensenrechten

Als raamwerk gebruiken we het EU Handvest van grondrechten en de VN Principes voor bedrijfsleven en mensenrechten. Universele mensenrechten zijn: Vrijheid van Meningsuiting, Non-discriminatie, Gelijkwaardige bescherming, Participatie in politiek, maatschappij, cultuur, kunst en wetenschap, Onderwijs, Vrijheid van samenkomst en vereniging en Veiligheid. De VN Principes zijn neergelegd in 2011 in de United Nations Guiding Principles on Business and Human Rights (hierna: de UN Guiding Principles). Deze principes zijn in juni 2011 unaniem door de VN-Mensenrechtenraad bekrachtigd. De principes bevestigen:

- De bestaande verplichtingen van staten om mensenrechten en fundamentele vrijheden te beschermen en te realiseren (1e pijler, State Duty to Protect);
- De verantwoordelijkheid van bedrijven om mensenrechten te respecteren (2e pijler, Business Responsibility to Respect);
- De noodzaak te voorzien in effectieve maatregelen voor herstel en/of verhaal bij inbreuken hierop (3e pijler, Access to Remedy).

De verantwoordelijkheid van bedrijven om mensenrechten te respecteren is onder Nederlands voorzitterschap in de Richtlijnen voor Multinationale Ondernemingen van de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO-richtlijnen) opgenomen.[31]

Een gezaghebbende lijst van de belangrijkste internationaal erkende mensenrechten wordt geboden door het Internationaal Statuut van de Rechten van de Mens (bestaande uit de Universele Verklaring van de Rechten van de Mens[32] in samenhang met de belangrijkste instrumenten waarmee zij is gecodificeerd: het Internationaal Verdrag inzake burgerrechten en politieke rechten en het Internationaal Verdrag inzake economische, sociale en culturele rechten), aangevuld met de principes betreffende fundamentele rechten van de acht belangrijkste IAO[33]-conventies vastgelegd in de verklaring inzake de fundamentele beginselen en rechten op het werk. Deze instrumenten vormen de benchmark die andere maatschappelijke actoren hanteren bij het beoordelen van de impact van bedrijfsactiviteiten op de mensenrechten. De verantwoordelijkheid van bedrijven om de mensenrechten te respecteren staat los van kwesties inzake juridische aansprakelijkheid en wetshandhaving, die grotendeels onder de bepalingen van de nationale wetgeving in de betreffende jurisdicties blijven vallen. Afhankelijk van de omstandigheden kan het voor bedrijven nodig zijn nog andere normen in aanmerking te nemen.

Vanuit de Verenigde Naties is er een groeiende interesse in de relatie tussen mensenrechten en standaarden. David Kaye, de voormalige speciale gezant voor het recht op de vrijheid van meningsuiting heeft in 2017 zelfs een rapport geschreven over de relatie tussen infrastructuur, standaarden en mensenrechten, dat vervolgens is aangenomen door de generale assemblee[34].

[31] Nationaal Actieplan bedrijfsleven en mensenrechten, MinBuza
[32] Zie de verkorte versie in Annex D
[33] Internationale Arbeids Organisatie, International Labour Organization
[34] https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/SR2017ReporttoHRC.aspx en https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/22/Add.4

Tevens is er een recentelijk nieuw verzoek gedaan vanuit de mensenrechtenraad om de relatie tussen mensenrechten en standaardisatie verder te onderzoeken[35].

De relatie tussen internetstandaarden en maatschappelijke normen en waarden zoals mensenrechten is uitgebreid wetenschappelijk bestudeerd (zie Cath 2019 voor een overzicht), en is in toenemende mate een onderwerp van discussie binnen de gremia die zich met standaardisatie bezighouden. Zo is er RFC 8280[36] die het verband legt tussen specifieke mensenrechten en internet standaarden, en een suggestie doet hoe deze beter op elkaar afgestemd zou kunnen worden.

4.3 Belangrijke maatschappelijke en politieke waarden in Nederland en Europa

In Nederland en Europa zijn er een aantal aanvullende maatschappelijke en politieke waarden die van invloed zijn op hoe we naar normen en waarden rond standaardisatie kijken. Voorbeelden hiervan zijn:

1. Concurrentie: We leven in een marktgebaseerde economie, waarbij zoveel mogelijk gestreefd wordt naar standaarden die concurrentie bevorderen, en niet op voorhand de uitkomst bepalen. Dit betekent ook dat toetreding tot de markt mogelijk moet zijn.
2. Digitale Soevereiniteit: Deze waarde is redelijk nieuw in het debat, maar stelt dat Nederland en Europa zelf willen kunnen bepalen wat er mogelijk is op netwerken in Europa en dat standaarden en implementaties niet tot een ongewenste afhankelijkheid van andere economische machtsblokken met tegengestelde waarden mogen leiden.
3. Decentralisatie: Deze waarde zorgt ervoor, dat er geen machtsconcentratie plaatsvindt. Macht over de verschillende aspecten van hoe het netwerk functioneert en kan worden gebruikt. Macht zorgt ervoor dat innovatie en keuzevrijheid worden belemmerd, door oligopolies en monopolies. Privacy, veiligheid, redundantie, soevereiniteit zijn ook waarden die bij een concentratie van macht worden bedreigd. Om die reden wordt het van belang geacht decentralisatie en distributie te realiseren in zowel economische, geografische, als technische zin.
4. Transparantie: Om de rechten en vrijheden van gebruikers van diensten en infrastructuurgebruikers te kunnen beschermen, is het van belang dat het kenbaar is hoe systemen werken.

Deze waarden zijn gedeeltelijk een invulling van de Universele mensenrechten. Concurrentie is een uitdrukking van participatie in de maatschappij, gelijkwaardige bescherming en nondiscriminatie. Niet alle landen en gedachtensystemen zien dat op dezelfde wijze en maken vergelijkbare afwegingen in het gewicht van deze waarden. Dit blijkt ook in discussies over internet governance en mensenrechten op en rond internet. Digitale soevereiniteit is voor sommige landen van zo groot belang, dat ze transparantie, concurrentie en decentralisatie eraan ondergeschikt achten. In Europa wordt juist benadrukt dat digitale soevereiniteit, transparantie, decentralisatie en transparantie niet zonder elkaar kunnen en elkaar versterken. Dus

[35] https://undocs.org/A/HRC/47/L.12/Rev.1
[36] https://datatracker.ietf.org/doc/html/rfc8280

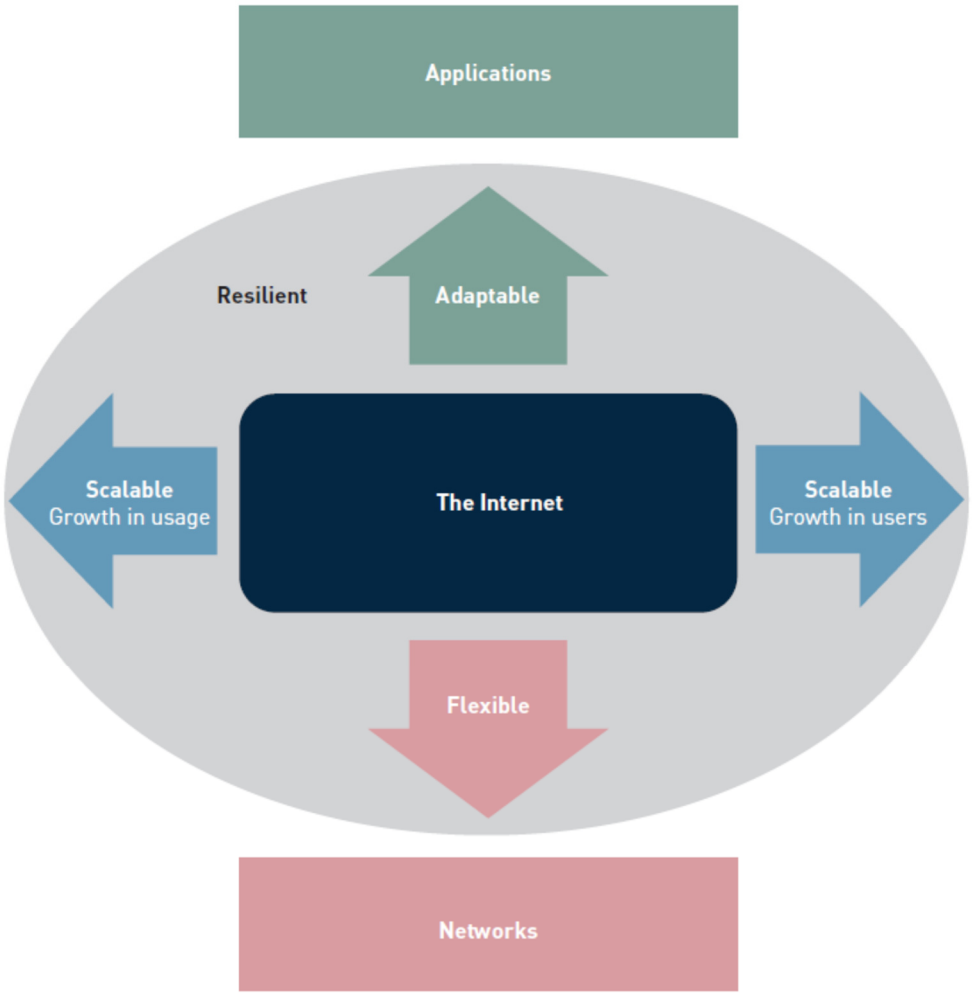
wil je transparantie, dan heb je concurrentie, soevereiniteit en decentralisatie nodig en vice versa.

4.4 Ontwerpprincipes van het internet

Binnen de standaardisatie van netwerken zijn er verschillende "waarden" of basisprincipes geformuleerd. Dit zijn op zichzelf geen maatschappelijke waarden, maar eerder ontwerpprincipes. Wel lijkt er vaak impliciet een aantal maatschappelijke waarden achter deze principes te liggen, maar dit wordt zelden expliciet gemaakt. In deze ontwerpprincipes zijn er grote verschillen te zien tussen die van "het internet" en die van "de telecom". Deze ontwerpprincipes zijn ook al lang elkaars tegenstelling geweest.

De ontwerpprincipes van het internet werden al in 1973 geformuleerd door Robert Kahn toen hij de lessen van de eerste ARPAnet implementatie probeerde toe te passen op een draadloos packet radionetwerk waar door het Amerikaanse defensie onderzoeksbureau DARPA-studie naar werd gedaan. Doordat radionetwerken inherent problemen konden hebben met fouten en problemen in transmissie werden ideeën als best effort transmissie en retransmissie bij verlies van data belangrijke principes. Net zoals dat wijzigingen in een deel van het netwerk geen wijzigingen elders in het netwerk mochten vereisen, waarbij gateways en routers zo weinig mogelijk informatie moesten hebben en bewaren over de communicatie en er geen besturing mocht zijn die over het hele netwerk reikte. Deze principes waren de basis van en nog steeds vergelijkbaar met de ontwerpprincipes die nu nog steeds de basis zijn van het internet.

In het rapport Study on the Internet's Technical Success Factors voor APNIC en LACNIC van Analysys Mason (Analysys Mason 2021) worden de succesfactoren samengevat in vier succesdimensies: het internet zorgt ervoor dat een veelheid en verscheidenheid aan applicaties kan communiceren over een veelheid en verscheidenheid van netwerken. Daarbij blijkt het internet flexibel met betrekking tot de eigenschappen en kwaliteiten van de onderliggende netwerken en transmissie technieken, is aan te passen voor het gebruik door zeer uiteenlopende applicaties (adaptable) en is gemakkelijks schaalbaar met betrekking tot de aantallen gebruikers en de hoeveelheid verkeer.



Figuur 8: De vier succesdimensies van het internet (bron: Analysys Mason, 2021)

4.4.1 RFC 1958

RFC 1958 (Architectural Principles of the Internet) vat een aantal design principes van het internet samen. RFC 3439 (Some Internet Architectural Guidelines and Philosophy) licht deze principes verder toe.

RFC 1958 opent met de observatie dat er niet zozeer een achterliggende architectuur is, maar meer een traditie. Er zijn wel verschillende uitgangspunten te herkennen, die in het verleden goed gewerkt hebben:

- De kern is **interconnectiviteit.**
- De ideale situatie is **één protocol** op internet level.
- End-to-end functionaliteit kan het beste worden ondersteund door **end-to-end protocollen.**
- Niemand is de eigenaar of de baas op internet, niemand kan het internet uitzetten: er is **geen gecentraliseerd beheer**.

Vervolgens wordt een aantal ontwerpprincipes beschreven die ten grondslag liggen aan het huidige internet (zie Annex C voor een samenvatting).

4.4.2 ISOC

Internet Society publiceerde een document (Internet Society 2020) waarin vijf essentiële eigenschappen worden benoemd van het internet:

1. Een toegankelijke infrastructuur met een gemeenschappelijk protocol: open, met lage toegangsdrempels;
2. Een open architectuur van samenwerkende en herbruikbare bouwblokken;
3. Gedecentraliseerd beheer en één gedistribueerd, schaalbaar, robuust routeringssysteem;
4. Gemeenschappelijke wereldwijde identificatie en adresseerbaarheid;
5. Een technologie neutraal, algemeen bruikbaar netwerk.

Deze eigenschappen omvatten een aantal breed uitlegbare begrippen zoals 'openheid', 'lage toegangsdrempels', 'herbruikbaarheid', 'samenwerking', 'robuustheid', 'wereldwijd', 'neutraal' en 'algemeen bruikbaar'. Maar achteraf gezien heeft hebben juist deze eigenschappen er in de praktijk daadwerkelijk voor gezorgd dat vele fabrikanten onderdelen en applicaties voor dit netwerk hebben kunnen maken die door bijna elk bedrijf of consument in de wereld gebruikt kunnen worden, waarbij onderdelen vrijwel probleemloos kunnen worden aangesloten op een thuis-, bedrijfs- of operator netwerk en kunnen communiceren met en via andere onderdelen, afhankelijk van de mogelijkheden die op hogere lagen zijn ingesteld (zoals bereikbaarheid en toegangsauthenticatie).

In de praktijk is er een zeer grote mate van portabiliteit van eindapparatuur, onderdelen en applicaties, die voor de komst van het internet en voor de revolutie van mobiele netwerken vrijwel onmogelijk was: je kunt in principe alle onderdelen loshalen, meenemen en elders weer gebruiken. En het netwerk is totaal agnostisch ten aanzien van de aansluitingen, toepassingen, mediatypen en inhoud.

Dit betekent in de praktijk zowel enorme mogelijkheden en voordelen, als grote uitdagingen: want alles wat fout kan gaan, kan overal fout gaan. Het betekent ook bijna automatisch dat allerlei achterliggende economische, politieke en ethische overwegingen achter een applicatie, onderdeel of eindapparaat heel moeilijk te isoleren zijn tot een bepaalde plek of een bepaald land, maar aan de andere kant ook heel lastig wereldwijd zijn op te leggen. Tenzij je de fundamenten aanpast, met het gevaar dat je de basis van het internet met de beste bedoelingen zodanig aanpast, dat de universele bruikbaarheid op termijn juist minder wordt. De regelmatig terugkerende discussies over encryptie zijn hier een voorbeeld van.

Critical Property	Benefits
1 An Accessible Infrastructure with a Common Protocol that is open and has low barriers to entry	Unrestricted access and common protocols deliver global connectivity and encourage the network to grow. As more and more participants connect, the value of the Internet increases for everyone.
2 Open Architecture of Interoperable and Reusable Building Blocks based on open standards development processes voluntarily adopted by a user community	Open architecture creates common interoperable services, which deliver fast and permissionless innovation everywhere. The inclusive standardization process and demand-driven adoption ensures that useful changes are adopted, while unnecessary ones disappear.
3 Decentralized Management and a Single Distributed Routing System which is scalable and agile	Distributed routing delivers a resilient and adaptable network of autonomous networks, allowing for local optimizations while maintaining worldwide connectivity.
4 Common Global Identifiers which are unambiguous and universal	A common identifier set delivers consistent addressability and a coherent view of the entire network, without fragmentation or fractures.
5 A Technology Neutral, General-Purpose Network which is simple and adaptable	Generality delivers flexibility. The Internet continuously serves a diverse and constantly evolving community of users and applications. It does not require significant changes to support this dynamic environment.

Figuur 9: De Internet Society beschrijft 5 essentiële eigenschappen die de 'Internet way of networking' definiëren de groei en het aanpassingsvermogen van het internet ondersteunen. De voordelen van deze eigenschappen hebben volgens de Internet Society gezorgd voor de economische en technologische ontwikkeling die het internet wereldwijd gebracht heeft.

4.4.3 RFC 1925

RFC 1925 is een bekende 1 april RFC die op humoristische wijze een deel van de waarden van het internet uitlegt. Dit humoristisch bedoelde stuk bevatte een groot aantal serieuze, onderliggende kernwaarden, die nog steeds worden aangehaald. De belangrijkste waardes die hier uit volgen zijn:

1. Het moet werken;
2. Het moet implementeerbaar zijn;
3. Het is beter deelproblemen aan te pakken, dan in 1 grote oplossing te bouwen;
4. De beste oplossing zit soms ergens anders in het netwerk of op een andere laag
5. Elke keuze is een economische of politieke afweging (goed, snel of goedkoop, je kunt maar twee tegelijk kiezen);
6. Complexiteit moet worden beperkt (het is al complex genoeg);
7. Realiseer je dat iedereen maar beperkt middelen heeft;

8. Realiseer je dat de technische vernieuwing van hardware en software veel problemen kan oplossen;
9. Het moet in zoveel mogelijk netwerken werken;
10. Of iets een goed idee is wordt bepaald door of het werkt;
11. Een goed protocol doet zo weinig mogelijk aannames.

Wat deze humoristische beschrijving laat zien is dat het ontwerpprincipes combineert met implementatie principes. Zoals bijvoorbeeld onder 8, waarbij de schrijver eigenlijk zegt tegen standaarden makers en degenen die het moeten implementeren: over 18 maanden verdubbelt de wet van Moore het aantal schakelingen op een chip en kan een implementatie van een standaard, die nu nog (te) langzaam is, snel genoeg zijn voor praktisch gebruik. Dat betekent dus ook dat optimalisatie van een standaard en de tijd die dat kost soms beter kan worden gelaten, omdat het te veel tijd kost en de ontwikkeling van de ICT de nieuwe standaard wel mogelijk maakt.

4.5 Conflicten en tegenstellingen over waarden en effecten op standaardisatie

Er zijn niet alleen grote verschillen tussen processen en procedures in verschillende standaardisatieorganisaties, maar ook in de culturen en de waarden van de participanten. Een bekend voorbeeld is de aanwezigheid van surveillance mogelijkheden in standaarden. Binnen de IETF is de heersende mening dat dit structureel ongewenst is[37,38], terwijl het integreren van 'lawful intercept' mogelijkheden binnen de 3GPP een standaard onderdeel van de standaardisatie is.

Hoewel bijna alle standaardisatieorganisaties het "dienen van het algemeen goed" in hun strategie en doelstellingen hebben staan (Yates and Murphy 2019), is het niet altijd duidelijk hoe dit wordt geoperationaliseerd. Vaak worden standaarden zelf gezien als een publiek goed, maar een publiek goed hoeft niet altijd te werken in het publieke belang (Kindleberger 1983).

Waarden in standaardisatieorganisaties zijn te onderscheiden op verschillende niveaus. Ten eerste zijn er proceswaarden. Deze gaan vaak over openheid, participatie, transparantie, verantwoordingsstructuren (Russell 2014). Deze waarden beschrijven het proces waarin standaarden ontwikkeld worden. Ten tweede zijn er uitkomstwaarden, die beschrijven wat de status is van de standaarden die ontwikkeld worden, of ze bijvoorbeeld vrijwillig of verplicht zijn, hoe ze verkrijgbaar zijn, en hoe er omgegaan wordt met patenten. Ten derde zijn er impactwaarden, deze beschrijven wat de beoogde impact is van de standaarden die geproduceerd worden. En hoewel er al sinds vroege standaardisatie van het internet over de sociale impact van het internet is gesproken (Braman 2011), is de analyse maatschappelijk impact nooit structureel geïncorporeerd in het standaardisatieproces (ten Oever 2021b; Cath 2021).

Onderzoek laat zien dat steeds als er oproepen zijn om de maatschappelijke impact van standaarden te analyseren als deel van het ontwikkelingsproces van standaarden, dit wordt afgewezen (Morris en Davidson 2003; Cath 2019). De reden hiervoor is wellicht dat de standaarden voornamelijk geproduceerd worden in private organisaties die gedomineerd worden door de

[37] https://datatracker.ietf.org/doc/html/rfc2804
[38] https://www.iab.org/documents/correspondence-reports-documents/2013-2/montevideo-statement-on-the-future-of-internet-cooperation/

private sector, die geen direct belang hebben in dergelijke analyses die het standaardisatiesproces duurder en complexer kunnen maken (ten Oever 2021a).

Dit is waarom veel onderzoekers in internationale betrekkingen en de studie van wetenschap en technologie, standaardisatieprocessen vaak beschrijven als een proces met grote maatschappelijke invloed maar weinig democratische legitimiteit. Shapiro en Varian zeggen zelfs: 'standaardontwikkeling is een wilde mix van politiek en economie' (Shapiro en Varian 1998).

De vraag hoe waarden in het proces van standaardisatie geborgd kunnen worden is een vraag van continue wetenschappelijke discussie die langzaam meer weerklank begint te krijgen in standaardisatieorganisaties. Voor een overzicht van de wetenschappelijke discussie, zie bijvoorbeeld het volgende overzicht (Cath 2019). Echter is het de vraag in hoeverre dergelijke maatschappelijke en sociale waarden structureel geïntegreerd gaan worden in het standaardisatieproces zonder een sterke interventie van overheden of het maatschappelijk middenveld. Tot op zekere hoogte is dit precies wat men nu kan waarnemen: overheden ontwikkelen wet- en regelgeving omdat ze bepaalde voorstellen niet gerealiseerd krijgen via internet governance en standaardisatieprocessen (Cohen 2019). Hier ligt een belangrijke keuze voor: accommoderen de standaardisatieorganisaties de behoeftes van overheden *tijdens* het standaardisatieproces, of moeten ze hun standaarden later aanpassen aan het mozaïek van wetgeving van verschillende landen en mogendheden.

4.6 Conclusies

4.6.1 Synthese van de belangrijkste waarden

De belangrijkste waarden voor dit onderzoek zijn een samenstel van de waarden die in de vorige paragrafen genoemd zijn. Omdat dit onderzoek beperkt is, zijn er ook beperkingen in de keuze. Niet alles heeft dezelfde prioriteit, terwijl alles uiteindelijk belangrijk is. In de implementatie zullen deze waarden bovendien met elkaar gebalanceerd moeten worden. Zo kan het recht op vrije demonstratie en vrije associatie op gespannen voet staan met het recht op de vrijheid van meningsuiting, als degenen die het ergens niet mee eens zijn een website blokkeren via een DDoS aanval. In dergelijke gevallen is een afweging die noodzakelijkheid en proportionaliteit in acht neemt essentieel. Dit soort dilemma's zijn dus ook belangrijk bij het zoeken van een adequate oplossing bij veel van de vraagstukken geschetst in het volgende hoofdstuk. Of bij de vraag: is het eigenlijk wel een probleem, of is het juist een onvermijdelijk gevolg van een gewenste eigenschap van hoe internet zou moeten werken om de achterliggende waarden te ondersteunen?

Samenvattend zien we, op basis van de genoemde waarden en ontwerpprincipes, de volgende algemeen erkende principes met betrekking tot standaardisatie van de fundamenten van internet:

1. Het moet werken, over een veelheid van geïnterconnecteerde netwerken, in een veelheid van situaties, en met tientallen of miljarden deelnemers;
2. Concurrentie en innovatie moeten bevorderd worden. Standaarden mogen niet leiden tot verstarring en het bevoordelen van bestaande of dominante spelers;
3. Het moet veilig zijn (security);

4. Het moet de privacy en bescherming van (bedrijfs)vertrouwelijke informatie bevorderen;
5. Het moet digitale soevereiniteit helpen behouden (niet afhankelijk zijn van derden);
6. Gebruikers moeten zelf kunnen beslissen wat er met hun data gebeurt en wie er toegang tot heeft;
7. Het netwerk moet stabiel zijn en niet fragiel;
8. Het moet schaalbaar zijn;
9. Het netwerk moet innovatie en verandering kunnen faciliteren;
10. De werking van netwerken moet begrijpelijk en inzichtelijk zijn voor toezichthouders en gebruikers.

4.6.2 Spanningen tussen waarden

Maar daarnaast zien we dat er spanning bestaat tussen een aantal uitgangspunten, of tussen uitgangspunten en doelen van belangrijke stakeholders. De belangrijkste spanningsvelden zijn:

- Het belang van afscherming van informatie (privacy/bedrijfsvertrouwelijkheid) versus het belang van (gecontroleerde) inzage in informatiestromen door overheden (terrorismebestrijding, oplossen misdaden, etc). Dit speelt bij veel discussies rond encryptie een rol.
- Het belang van een open en laagdrempelig internet, waar iedereen op aan kan sluiten, overal ter wereld, versus de noodzaak voor alle bij de routering betrokken partijen om elkaar te vertrouwen.
- Het belang van gegarandeerde servicegaranties versus het uitgangspunt dat internet in de basis een 'best effort' karakter heeft waarbij geen sessies met gegarandeerde verbindingen worden opgezet, en waarbij alle pakketverkeer in principe gelijkwaardig is. Dit speelt onder andere in de netneutraliteitsdiscussie een rol.
- Het belang van internet als enabler van duurzaamheid versus discussies over het verkleinen van de ecologische footprint van het internet zelf. Dit speelt onder andere een rol bij discussies over routering.
- Het belang van het bevorderen van innovatie versus het belang van (stabiliteit van de) interoperabiliteit. Goede standaarden zorgen veelal voor innovatie en concurrentie aan beide kanten van de gestandaardiseerde interface, maar dit gaat soms ten koste van innovatie van de interface zelf. Denk hierbij bijvoorbeeld aan de nog steeds gebruikte stekkers en stopcontacten voor het aansluiten van apparatuur.

Het volgende hoofdstuk laat de inventarisatie van vraagstukken zien uit literatuurstudie en interviews. Vele van deze vraagstukken hebben een relatie met één of meer van bovengenoemde spanningsvelden.

5 Vraagstukken rond de huidige netwerken

Op dit moment zijn er verschillende initiatieven om de architectuur en basisprotocollen van het internet te herzien, verbeteren of zelfs te vervangen. Dat impliceert dat het huidige internet volgens sommigen herziening, verbetering of vervanging behoeft omdat er – volgens de initiatiefnemers - problemen zijn met de bestaande standaarden die opgelost dienen te worden. Sommige van die problemen zijn technisch en/of operationeel van aard, maar vele hebben (ook) achtergronden in maatschappelijke vraagstukken zoals fraudebestrijding, bestrijding van criminaliteit of het beschermen van bedrijfsvertrouwelijkheid en privacy.

Paragraaf 5.1 beschrijft een aantal voorstellen voor radicale vernieuwingen van internet, en welke vraagstukken de voorgestelde oplossingen willen adresseren. Paragraaf 5.2 geeft een overzicht van vraagstukken en problemen in de huidige basisprotocollen die het internet dragen, zoals die verschillende partijen ervaren worden. Deze vraagstukken komen naar voren in de beschrijving van de radicale initiatieven uit de eerste paragraaf, maar ook in actuele discussies in standaardisatieorganisaties, literatuur, internetdiscussies en tijdens de interviews. In 5.3 wordt vervolgens een 'top 10' van vraagstukken opgesteld op basis van de observaties in de literatuurstudie en de interviews. Vervolgens worden deze top 10 vraagstukken en hun oplossingen en hun kansrijkheid verder besproken in hoofdstuk 6. Ook wordt daar gereflecteerd over de discussies rond en kansrijkheid van de meer radicale voorstellen.

5.1 Radicale voorstellen internetvernieuwing en wat ze adresseren

Er is een veelheid van voorstellen voor een nieuw internet, waarbij de verbeteringen variëren van kleine, incrementele verbeteringen tot opnieuw beginnen met een schone lei ("clean slate"). Deze paragraaf behandelt de meer radicale "clean slate" voorstellen, waarbij substantiële delen van de internetprotocollen volledig worden vervangen[39].

Een analyse van deze voorstellen maakt duidelijker welke vraagstukken met betrekking tot het huidige internet volgens de initiatiefnemers belangrijk zijn. In de onderstaande paragrafen worden enkele initiatieven benoemd, met daarbij kort de vraagstukken die deze initiatieven pogen op te lossen. Vervolgens worden deze en andere vraagstukken in de volgende paragraaf afzonderlijk behandeld.

Paragraaf 6.3 reflecteert op de kansrijkheid van deze initiatieven.

5.1.1 Recursive InterNetwork Architecture (RINA)

RINA[40] is gebaseerd op de ideeën van John Day, een ARPAnet en OSI-standaardisatie veteraan uit de Verenigde Staten, die hij publiceerde in 2008. Het gaat uit van het principe dat een netwerk een serie van inter-proces communicatie (IPC) is, vergelijkbaar met de processen in een besturingssysteem, maar dan schaalbaar door gedistribueerde inter-proces faciliteiten (DIF). Ieder proces in een operating systeem heeft een aantal functies die het kan uitvoeren,

[39] Zie ook https://courses.sidnlabs.nl/anet-2021/ voor meer informatie over een aantal van deze architecturen

[40] Zie http://csr.bu.edu/rina/about.html en (Grasa 2019)

inputs die het kan verwerken met bepaalde kwaliteitsparameters en outputs die het kan verzenden. Netwerkcommunicatie is ook zo'n proces, tussen een apparaat en een randapparaat, tussen twee computers in een ruimte of op een wereldwijde schaal. In principe zou het niet nodig moeten zijn om te weten waar in de wereld of op een netwerk of computer het proces zich bevindt en of dit op 1 of op een miljoen computers is. Applicaties roepen processen aan en RINA zorgt ervoor dat dit wordt verwerkt, lokaal of internationaal met de juiste kwaliteitsparameters, zoals beveiliging, toegangscontrole en Quality of Service en bepaalt een pad over de IPC/DIF's die hiervoor nodig zijn. Dit is fundamenteel anders dan het perspectief dat een netwerk een serie van best-effort lagen is waar de communicatie tussen specifieke eindpunten over gaat, zoals in het internet en OSI-model (beschreven in Annex B).

De website van Boston University waar Day werkzaam is, noemt de volgende issues met het huidige internet:

"By making the choice for a rudimentary "best-effort" service, the Internet has ***not been able to effectively respond to new requirements security, manageability, wireless, mobility, etc.)*** *Today, Internet Service Providers (ISP's) may be willing to provide better than best-effort service to their customers or their peers for a price or to meet a Service Level Agreement (SLA). The lack of a structured view of how this could be accomplished, given the current IP model, has led to numerous ad hoc solutions that are either inefficient or incomplete. Shortcomings of the current internet are:*

- ***Naming and addressing interfaces*** *rather than nodes****,***
- ***exposing addresses*** *to applications,*
- ***artificially isolating functions of the same scope****: transport and routing/relaying are split into two layers: Data Link and Physical layers over the same domain/link, and Transport and Network layers internet-wide, and*
- *artificially* ***limiting the number of layers (levels).****"*

In Europa liep er een aantal onderzoeksprojecten, mede gefinancierd door de Europese Commissie, die onderzoek doen of hebben gedaan naar RINA.[41] De resultaten zijn tot nu toe beperkt tot een aantal referentie implementaties, maar geen productie. Er is een organisatie, de Pouzin Society, die ontwikkelingen rond RINA volgt en updates geeft over nieuw onderzoek.

5.1.2 Scalability, Control, and Isolation on Next-Generation Networks (SCION)

SCION[42] is een "clean slate" design van ETH Zürich, dat zich richt op een hoge mate van vertrouwen in het netwerk. Hiertoe geeft het afzenders, ontvangers en ISP's grotere controle over de routering van verkeer, zowel de wijze waarop het verkeer gerouteerd wordt als het pad waarover het verkeer gerouteerd wordt. Als de data niet via een bepaald netwerk (Autonomous System) mag, bijvoorbeeld omdat dit netwerk onder controle van een bepaald land staat, dan kan hier rekening mee worden gehouden in de routering. De eindgebruiker bepaalt in principe de routering en geeft deze mee aan het packet. In principe kunnen alleen gebruikers die toegelaten zijn tot een bepaalde groep (Isolation Domain, ISD), waarbinnen partijen elkaar vertrouwen, onderling met elkaar communiceren. Er kan ook over ISD's met elkaar gecommuniceerd worden, maar alleen via een hiërarchisch systeem waarbij een 'Core Autonomous Systems' binnen een ISD's het contact met een andere ISD verzorgt. Met dit systeem kunnen

[41] https://pouzinsociety.org/research/projects
[42] https://www.scion-architecture.net/, en (Barrera et al, 2017)

gebruikers expliciet controle krijgen over welke netwerken hun communicatie wel en niet overheen mag, zodat bijvoorbeeld communicatie niet door een bepaald specifiek ander land gaat.

SCION noemt de volgende issues met het huidige internet:

*"The Internet was **not designed as a high-security network**. Security improvements primarily address specific attacks, but do not solve the fundamental problems and often introduce new undesirable consequences e.g.*

- *BGPSEC prevents route hijacking but causes delayed route convergence, and*
- *does not support prefix aggregation which contributes* to **reduce scalability**.

With a clean-slate design, we can fundamentally improve the security to a level that is unlikely to be achievable through incremental changes."

SCION is op dit moment in onderzoek, onder andere in Nederland op het 2StiC[43] Testbed van o.a. NInetlabs, SIDN Labs, Universiteit Twente, Universiteit van Amsterdam en SURF. In Zwitserland is een project om het in te zetten in de communicatie tussen de Zwitserse Banken[44]. Er zijn ook voorstellen om de routering in SCION zo te maken dat informatie over bijvoorbeeld energieverbruik/CO2 uitstoot invloed kan hebben op de keuzes ten aanzien van routering. Bijvoorbeeld door verkeer tussen Zürich en Londen via Frankrijk te sturen vanwege de lage CO2 uitstoot van Frankrijk's elektriciteitsproductie, behalve op dagen met veel zon en/of wind, want dan stoot de route via Duitsland en Nederland het minste CO2 uit[45].

Er is veel discussie over de vraag of SCION een betere basis voor de beveiliging biedt dan BGP, in combinatie met alle verbeteringen die beogen BGP veiliger te maken[46].

5.1.3 ITU-T Focus Group on Technologies for Network 2030

ITU-T Network 2030 Focus Group (FG NET-2030)[47] noemt de volgende issues met het huidige internet:

"Current internetworking infrastructure provides network services that are fundamentally built on the basis of "best effort". While differentiated services allow for the prioritization of traffic and the reservation of resources, and while transport-layer protocol can add reliability via retransmission schemes, all of these mechanisms are associated with significant trade-offs and limitations. In order to support new applications, Network 2030 services need to move beyond best effort and support a new concept of "high precision": high precision in terms of quantifiable latency guarantees, in terms of synchronization of packet flows across multiple communication channels and communicating parties, in terms of behaviour in face of congestion and resource contention.

The following applications areas are seen among the primary drivers for new Network 2030 services:

---

[43] https://www.sidnlabs.nl/nieuws-en-blogs/experimenteren-met-nieuwe-internet-infrastructuren-scion

[44] https://scion-architecture.net/pages/scion_day_2022/slides/SCiON_day_2022_Boye_Steinmann.pdf

[45] https://www.weforum.org/agenda/2021/03/internet-carbon-emissions-data-path-scion/

[46] https://www.weforum.org/agenda/2021/06/internet-connectivity-border-gateway-protocol-scion

[47] https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/Deliverable_NET2030.pdf, https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx, https://www.huawei.com/en/technology-insights/industry-insights/innovation/new-ip

1. ***Industrial & Robotic automation:*** *Machine-to-machine communication for industrial and robotic automation requires very fine-grained timing accuracy for the dispersion of control commands and for the collection of telemetry data.*
2. ***Emergence of holographic media and other advances in multimedia technology:*** *Holograms, haptics, and other sensory data will provide immersive and "real" user experience. For this to happen, very high data throughput involving tight coordination across bundles of streams among multiple stream sources and sinks will be necessary, as well as the ability to rapidly prioritize data items within and between streams per guidance from applications.*
3. ***Autonomic and critical infrastructures:*** *Network services that enable mission-critical applications such as self-driving vehicles, drones, automated traffic control systems, all communicating with one another and their environment, need to be failsafe so that infrastructure can rapidly adapt and react to unexpected events. Without it, such applications might quickly devolve from a perceived blessing into a safety hazard. For autonomic and mission-critical applications, time-guaranteed packet delivery is often required and/or favoured.*
4. ***Diversity of applications and their needs:*** *An explosion of new applications that consume networking services can be expected. Many of those applications may be driven by Artificial Intelligence (AI) and depend on myriads of data feeds; they may also involve novel mixes of humans, machines, and IT systems communicating with one another. This will require the ability to not just deliver but also to dynamically adapt associated network services.*
5. ***Accountability for services delivered:*** *Often stringent service requirements directly impact operational and maintenance costs as seen through managed service models. Accountability in the form of evidence that actions were taken in delivering a service in conformance with the agreement benefits both functional and business aspects of a service. It incentivizes service providers to offer new type of service delivery models and allow innovations in applications to incorporate such capabilities.*
6. ***Expectations for varying degrees of distortion tolerance:*** *Applications that can absorb intermittent or partial loss of data and still function normally are said to be distortion tolerant. While many Network 2030 applications are characterized by their need for high precision networking services, other classes of applications may in fact be distortion tolerant to a degree. In some such cases, applications may demand novel abilities to differentiate contents that is tolerant to loss, and articulate more sophisticated ways to deal with such loss than is the case today."*

Er worden hier wel enkele drijfveren benoemd, maar de achterliggende problemen (waar we in dit hoofdstuk naar op zoek zijn) blijven enigszins impliciet. Samengevat lijken de gepercipieerde problemen te liggen op de vlakken die ITU ook al eerder zag voor internet: onvoldoende schaalbaarheid, onvoldoende mogelijkheden voor QoS, onvoldoende ondersteuning voor lokale missiekritische of autonome toepassingen en netwerken, onvoldoende mogelijkheden voor diverse applicaties en onvoldoende mogelijkheden voor specifieke billing en accounting.

5.1.4 Named Data Networking (NDN)

Het NDN-project[48] streeft ernaar om de zwaktes van het bestaande internet op te lossen. Volgens het NDN-project is het huidige IP vooral bedoeld voor conversaties tussen gelijkwaardige eindpunten, terwijl het internet voor het grootste deel gebruikt wordt om informatie op te halen. Het project ziet daardoor de volgende zwaktes in het huidige model:

- De gebruiker vraagt om een specifiek stukje informatie, maar internet werkt alleen met IP-adressen. Er is daarom een reeks van vertaalslagen nodig tussen de naam van (bijvoorbeeld) een videofragment, de server waarop dat fragment beschikbaar is, en uiteindelijk het IP-adres van een specifieke netwerkinterface van die server.
- IP gaat er van uit dat elk pakketje apart gerouteerd wordt, terwijl de gevraagde informatie meestal integraal dezelfde route kan volgen.
- Bij IP moet de beveiliging (versleuteling en authenticatie) apart geregeld worden.

NDN adresseert deze zwaktes door de "naam" van de gevraagde gegevens of de gevraagde dienst direct als adres te gebruiken, en door op elk apparaat op de route zowel de verzoeken om gegevens als de gegevens zelf voor enige tijd te bewaren. Het netwerk functioneert daardoor impliciet ook als een "Content Distribution Network" (CDN), en hoeft dus elk stukje informatie maar één keer op te halen om het aan meerdere vragende partijen te kunnen leveren. In tegenstelling tot de bestaande CDN's vindt de adressering bij NDN echter plaats via de (naam van) de inhoud en niet via een IP-adres.

NDN is als idee ontstaan in 2001, en is vooralsnog een experimenteel concept. Er wordt veel onderzoek aan gedaan, en er zijn kleinschalige testnetwerken beschikbaar, maar het is nog niet duidelijk in hoeverre het concept voldoende schaalbaar is voor een wereldwijd netwerk.

5.1.5 "New IP"

Een aantal Chinese partijen (aangevoerd door Huawei) heeft binnen de ITU voorgesteld om een geheel nieuw internetprotocol te definiëren. Er gaan veel geruchten rond over de visie van deze partijen, en met name over de mate van centrale controle die in deze visie centraal zou staan, maar het formele voorstel aan de ITU[49] noemt slechts drie (gepercipieerde) problemen, zonder al een oplossingsrichting aan te geven:

- Steeds meer verschillende types apparaten, met verschillende eisen;
- Steeds meer losstaande technologieën, waardoor er complexe gateways nodig zouden zijn;
- Gebrekkige security en trust.

De bijbehorende presentatie en de latere "tutorial" (Huawei 2019) noemen echter nog enkele andere (vermeende) probleemgebieden, en meer aspecten van het security vraagstuk:

- Te grote en te onvoorspelbare end-to-end vertraging (latency);
- Niet geschikt als tijdbasis (synchronisatie) voor tijd-kritische applicaties;
- Niet geschikt voor nieuwe netwerken (o.a. via satellieten, met continu veranderende netwerktopologie);

[48] Zie https://named-data.net/ en (Zhang et al, 2014)
[49] ITU TSAG-C83 bijdrage, september 2019

- IP-spoofing, geen mogelijkheid om het IP-adres van de afzender te verifiëren;
- Kwetsbaarheden in encryptie, met name door gecentraliseerd beheer van sleutels (CA's);
- Applicaties hebben geen invloed op routering (bv. Keuze tussen pad met meer bandbreedte of met betere latency garanties).

Het "New IP" voorstel is binnen de ITU afgewezen, maar verschillende Chinese partijen proberen nu om, in diverse ITU-werkgroepen, specifieke onderdelen van het voorstel afzonderlijk als standaard vastgesteld te krijgen (Voo en Creemers 2021).

5.2 "Long list" vraagstukken

Uit het bovenstaande, uit de verdere literatuur en uit de interviews zijn we de volgende vraagstukken tegengekomen die een relatie hebben met het bestaande internet, en die bovendien een relatie hebben met de lagen die in scope van de opdracht zijn. De vraagstukken zijn hieronder per thema gesorteerd.

Bij een deel van de vraagstukken zijn er enkele bestaande of voorgestelde oplossingen (vaak deeloplossingen, of pogingen daartoe) bij het vraagstuk benoemd. Voor de "top tien" vraagstukken gaan wij in hoofdstuk 6 verder in op de bestaande en voorgestelde oplossingen.

5.2.1 Security issues:

- BGP-spoofing[50], waarbij een kwaadwillende partij de routing tables van anderen probeert te beïnvloeden door foute informatie in een BGP-sessie tussen andere partijen te stoppen (oplossingen: BGPsec, RPKI).
- BGP route hijacking, waarbij een kwaadwillende (of gehackte) ISP foute informatie in zijn eigen BGP-sessies stopt (oplossingen: BGPsec, RPKI).
- DNS-spoofing[51], waarbij een kwaadwillende partij plausibele DNS-antwoorden stuurt zonder ooit een DNS-verzoek gekregen te hebben, en daarmee verkeer naar een verkeerde bestemming routeert (oplossingen: DNSsec, DoT, DoH).
- IP-spoofing, waarbij een kwaadwillende partij pakketjes verstuurd met een incorrect afzenderadres, zodat de reactie naar een ander toe gaat (als onderdeel van een DdoS attack) en/of zodat de afzender moeilijker te vinden is (oplossing: BCP 38 en 84).
- DdoS op de infrastructuur zelf, waarbij er massaal pakketjes naar componenten binnen de infrastructuur (bijvoorbeeld de DNS-servers) gestuurd worden met als doel deze te overbelasten (oplossingen: voorkomen van IP-spoofing, beperken en afremmen van te grote verkeersstromen van internetverkeer, authenticatie van regelmechanismen tussen ISP's).

[50] BGP, het Border Gateway Protocol, wordt gebruikt om het verkeer tussen netwerken van verschillende eigenaren te routeren. Netwerken geven elkaar routeinformatie, maar beslissen zelf hoe daar mee om te gaan om hun verkeer via bepaalde andere netwerken te routeren.

[51] DNS, het Domain Name System wordt gebruikt om namen van internetbestemmingen (zoals www.stratix.nl) naar IP-adressen te convergeren, die gebruikt worden bij adressering en routering van IP-pakketten.

5.2.2 Neutraliteit:

- Traffic shaping, waarbij een partij op de route een eigen dienst, groep, of organisatie bevoordeelt, bijvoorbeeld door concurrerende diensten van anderen kunstmatig te vertragen (oplossing: QUIC).

5.2.3 Ongewenste content (haatzaaien, kinderporno, cyberpesten, phishing/malware etc.):

- Weinig zicht op ongewenste content: hoewel de content zich altijd op het niveau van de applicatie bevindt (en dus buiten scope voor deze opdracht), is er vaak wel een behoefte om ongewenste content op de onderliggende lagen aan te pakken. De applicatie en de content kunnen zich immers in een ander land bevinden, buiten de eigen jurisdictie, terwijl de routing meestal tenminste deels via een ISP in het eigen land plaats vindt. Het "probleem" is dan dat ISP vaak geen zicht heeft op de content, zeker als deze versleuteld is. En dit is weer het gevolg van de scheiding tussen netwerk en de applicaties en informatie die daarover vervoerd worden; deze scheiding is inherent aan hoe het internet is opgebouwd. Elke poging om dit probleem op te lossen leidt echter weer tot nieuwe problemen op het gebied van privacy en vrije meningsuiting, iets waarbij die scheiding tussen netwerk en inhoud juist goed van pas komt. (oplossingen: blokkeren van IP-adressen of van DNS namen).
- Behoefte aan rechtvaardigheid en rechtshandhaving. Bij stalking of bedreiging wil de maatschappij dat de dader wordt gevonden en bestraft. Aftapbaarheid dient ook een maatschappelijk belang.

5.2.4 Privacy:

- Interceptie van de inhoud (legaal of illegaal), waarbij een partij op de route het verkeer tussen andere partijen uitleest (oplossing: TLS, HTTPS)
- Interceptie van metagegevens (legaal of illegaal), waarbij een partij informatie over het verkeer uitleest (oplossingen: header encryption, Ipsec, DNS over HTTPS, ODNS, …)
- Onzekerheid over routering: net zoals de overheid geen zicht heeft op de routering van verkeersstromen, heeft de gebruiker dat zelf ook niet. Het is dus mogelijk dat verkeer gerouteerd wordt via landen waar minder stringente privacyregels gelden, zonder dat de gebruiker zich daarvan bewust is (oplossingen: TLS, separate netwerken).

5.2.5 Gebrek aan soevereiniteit:

- Nationale overheden hebben veelal behoefte aan mogelijkheden om zeggenschap over het verkeer te hebben, of in ieder geval te kunnen hebben, bijvoorbeeld om in bepaalde gevallen gelegitimeerde interceptie te doen, of zelfs om bepaald verkeer te kunnen stoppen. Doordat er op het internet geen zekerheid is dat al het verkeer via het eigen land of groep van landen gerouteerd wordt (zelfs als begin- en eindpunt wel daarbinnen liggen) is dit niet altijd mogelijk.
- Tegelijkertijd willen overheden voorkomen dat andere overheden, en bedrijven buiten hun eigen jurisdictie, zeggenschap over het verkeer kunnen krijgen. Ook dit is niet altijd mogelijk, om diezelfde reden.

- Het is zelfs niet altijd mogelijk om te weten of het verkeer wel of niet door een ander land heen zal gaan, aangezien de routering van moment tot moment kan verschillen.

5.2.6 Gebrek aan zeggenschap voor eindgebruikers:

- Niet alleen bij overheden bestaat er behoefte aan zeggenschap over hun datastromen, ook bij bedrijven en burgers bestaat een groeiende behoefte controle te hebben over hun data en hun datastromen. Dit is ingewikkeld in de huidige netwerkarchitectuur, omdat alleen op AS-niveau er zeggenschap is over de routering. Een bedrijf kan er bijvoorbeeld niet makkelijk voor zorgen dat zijn verkeer alleen binnen jurisdicties blijft waar vergelijkbare privacyregels gelden als in het eigen land.
- Net als voor overheden is het ook voor de eindgebruiker niet of nauwelijks mogelijk om zeker te weten hoe het verkeer gerouteerd zal worden.

5.2.7 Trage of incorrecte implementatie van standaarden:

- Hoewel er consensus lijkt te bestaan over de invoering van bepaalde standaarden (IPv6, RPKI, VoLTE), laat de implementatie vaak lang op zich wachten. Sommige standaarden (zoals IPv6) zijn na twintig jaar nog steeds niet volledig uitgerold.
- Daarnaast bevindt zich in de netwerken een grote hoeveelheid apparaten die niet volgens standaard werken. De interoperabiliteit tussen deze apparaten en de apparaten die wel conform de standaard werken is vaak slechts met veel “trial and error” tot stand gekomen. Dit bemoeilijkt de implementatie van nieuwe versies van de standaard, omdat de interoperabiliteit van de aangepaste apparaten met deze niet-conforme apparaten niet gegarandeerd kan worden.

5.2.8 Gebrek aan innovatie, flexibiliteit en veranderbaarheid van de infrastructuur:

- Het gebruik van communicatienetwerken verandert in de loop der jaren, en daarmee veranderen ook de verwachtingen van en eisen aan de netwerken weer. Het succes van het internet is verbonden met het concept van permissieloze innovatie en het flexibele en modulaire en gelaagde karakter van de internetarchitectuur. Het is echter steeds moeilijker geworden om te innoveren, vooral op de IP en transportlagen. De standaardisatie van QUIC (zie 3.2.6.1), een recent protocol dat gegevenstransport betrouwbaarder maakt, was alleen mogelijk omdat Google controle had over de grootste browser ter wereld én over een groot deel van de inhoud. Voor andere, vooral kleinere, partijen is het veel lastiger om nieuwe ideeën te implementeren of substantieel te reflecteren op de voorstellen die vanuit de grote internetpartijen worden gelanceerd. De vraag is dus of het internet nog wel innovatie op het gebied van netwerken kan faciliteren, en of kleinere partijen nog in staat zijn daar invloed op uit te oefenen.

5.2.9 Gebrek aan duurzaamheid:

- Zoals het internet nu is vormgegeven is alle verkeer gelijk, en is er in de meeste gevallen weinig stimulans om minder verkeer te versturen (het tegengestelde lijkt soms het geval: meer is beter, duplicatie, redundantie, ontvangstbevestigingen en hertransmissies zijn inherent onderdeel van concepten op vrijwel alle lagen). Dit druist in tegen duurzaamheidsprincipes, want het transport, verwerken en bufferen of cachen van meer gegevens kost (op den duur) wel extra energie en grondstoffen.

5.2.10 Onzekerheid over end-to-end performance:

- Quality of service: het huidige internet biedt slechts beperkt mogelijkheden om de end-to-end prestaties van een dienst te garanderen. Voorzieningen op de hogere lagen om gegevensverlies te voorkomen leiden altijd tot meer onzekerheid over de vertraging tussen de eindpunten. Dit is een direct gevolg van het gebrek aan "quality of service" features in het huidige internet (oplossing: DiffServ).

5.2.11 Mobiliteit/ continuïteit van sessies:

- Een endpoint dat voor toegang tot het internet overstapt naar een andere verbinding krijgt in de meeste gevallen een ander IP-adres, waardoor bestaande sessies op de applicatielaag verbroken worden en opnieuw moeten worden opgebouwd. Een voorbeeld: een gesprek via WhatsApp of Skype stopt even men bijvoorbeeld binnen een gebouw met slechte dekking overgaat van een mobiele verbinding naar een wifi verbinding, waarna de applicatie het gesprek opnieuw opstart (oplossingen: Mobile IP, Mobile IPv6, multipath TCP, QUIC).

5.2.12 Performance en beheer:

- Load sharing via multi-homing is beperkt mogelijk; een IP-adres is (in het algemeen) op elk moment aan één interface gekoppeld, dus een machine met meerdere interfaces (wellicht via verschillende ISP's) krijgt voor een gegeven IP-adres slechts verkeer op één interface. Het is op zich wel mogelijk om verkeer te spreiden, maar dat maakt het beheer ingewikkelder.
- Routing tables worden steeds groter, omdat (bijna) elke routerende partij alle aangekondigde prefixes moet bewaren. De tabel heeft nu (midden 2021) circa 890.000 regels voor IPv4 en 110.000 voor IPv6, en het aantal groeit nog steeds.

5.3 Selectie van een "top tien" van vraagstukken

Vanuit de in de vorige paragrafen aangegeven lijst met relevante vraagstukken hebben wij een "top tien" bepaald, om voor deze top tien van vraagstukken verder te kijken naar de mogelijke oplossingen en de rol van standaardisatie daarbij. Deze top tien is een enigszins subjectieve keuze van de onderzoekers. De selectie is gebaseerd op de signalen uit de interviews en uit de literatuur, en op de inzichten van de onderzoekers zelf, op basis van overwegingen als:

- Hoe fundamenteel is het vraagstuk?
  - Heeft het een relatie met de fundamenten van het internet?
  - Heeft het vraagstuk verband met erkende waarden en principes?
- Wordt het vraagstuk nu en in de komende tijd als belangrijk gezien door stakeholders?
  - Wat is de actualiteit van het vraagstuk?
  - Zijn er op dit moment veel activiteiten rond dit vraagstuk in de standaardisatieorganisaties en andere gremia, of in discussiegroepen, nieuwsartikelen, etc.?
- Is het vraagstuk niet al onderdeel van een ander vraagstuk?
- Is er aandacht bij overheden met betrekking tot dit vraagstuk?

De ‘top tien’ bevat vraagstukken waarvan we verwachten dat die nu en in de komende jaren de discussies rond de fundamenten van internet zullen blijven bepalen. In een expert workshop met leden van de klankbordgroep zijn de overwegingen gedeeld en besproken, en is de voorgestelde ‘top 10’ verder aangescherpt.

De laatste twee gebieden uit de ‘long list’ uit paragraaf 5.2 (mobiliteit, zie paragraaf 5.2.11, en performance/beheer, zie paragraaf 5.2.12) zien wij niet als belangrijke probleemgebieden die conflicteren met maatschappelijke waarden, of waarvoor de oplossingen tot dergelijke conflicten kunnen leiden. Het zijn primair technische issues, waar wel veel aandacht voor is, maar die uiteindelijk vooral technisch afgewogen moeten worden. Een voorbeeld: een oplossing voor IP-mobiliteit kan op de IP-laag geïmplementeerd worden (zoals met Mobile IP), maar het is ook mogelijk om de bovenliggende lagen robuuster te maken tegen discontinuïteit in de onderliggende lagen.

Van de rest van de genoemde vraagstukken zien wij de volgende “top tien”. Bij elk genoemd vraagstuk staat een verwijzing naar de eerdere paragraaf met beschrijving.

1. BGP route hijacking (5.2.1)
2. IP-spoofing (5.2.1)
3. Traffic shaping/netneutraliteit (5.2.2)
4. Weinig zicht op ongewenste content (5.2.3)
5. Interceptie van de inhoud (5.2.4)
6. Interceptie van metagegevens (5.2.4)
7. Zeggenschap op verkeer (soevereiniteit) (5.2.5, 5.2.6)
8. Innovatie, flexibiliteit en veranderbaarheid van de infrastructuur (5.2.8)
9. Gebrek aan mogelijkheden voor duurzaamheid (5.2.9)
10. Gebrek aan Quality of Service (5.2.10)

5.4 Conclusies

Er is veel discussie over aspecten van het internet die wellicht beter of in elk geval anders zouden moeten. Vanuit deze discussies hebben wij een “long list” opgesteld van mogelijke vraagstukken. Ook de bestaande “clean slate” initiatieven geven een goed beeld van mogelijke vraagstukken, aangezien deze de motivatie vormden om de genoemde initiatieven te starten.

Vanuit de “long list” van vraagstukken hebben wij uiteindelijk een selectie van een “top tien” gemaakt. Deze “top tien” lijst vormt de basis voor de analyse in het volgende hoofdstuk.

6 Uitwerking: vraagstukken en oplossingen

6.1 Algemeen

In het vorige hoofdstuk is de "top tien" van vraagstukken geïdentificeerd. Paragraaf 6.2 geeft voor elk van deze vraagstukken een korte omschrijving, en de voorgestelde (en vaak deels al geïmplementeerde) *incrementele* verbetervoorstellen. Dit zijn oplossingen die ontworpen worden bovenop bestaande protocollen, of door kleine wijzigingen aan bestaande protocollen.

Per vraagstuk wordt steeds een korte beschrijving gegeven met daarin op welke eigenschap van het internet deze betrekking heeft, het vraagstuk of probleem zelf, en kort de belangrijkste gerelateerde afwegingen rond waarden. Vervolgens worden de voorgestelde of mogelijke oplossingen beschreven, bijbehorende gremia, voor- en nadelen en kansrijkheid.

Daarnaast zijn er *radicale* voorstellen; deze pogen om een groot aantal vraagstukken tegelijk op te lossen, en passen daardoor minder goed in deze structuur. Paragraaf 6.3 beschrijft een aantal van deze radicale voorstellen en de vraagstukken waar deze bij passen.

6.2 Uitwerking per vraagstuk

6.2.1 BGP route hijacking

Omschrijving

Feature

Netwerken geven elkaar voorkeursroutes door. Daardoor hoeft ieder individueel netwerk niet zelf de route te bepalen naar elke mogelijke bestemming, maar vertrouwt het op informatie die het vanuit andere netwerken krijgt.

Vraagstuk

De feature wordt misbruikt door derden om (algemeen of specifiek) verkeersafhandeling te storen, bijvoorbeeld om een bestemming onbereikbaar te maken of om verkeer naar een ander netwerk toe te trekken, om het daar vervolgens af te tappen of te beïnvloeden.

Ook is het mogelijk dat een foute configuratie binnen één netwerk ervoor zorgt dat andere netwerken verkeerde BGP-informatie krijgen. Van buitenaf is niet altijd duidelijk of een "route hijacking" gebeurtenis bewust of per ongeluk veroorzaakt is[52].

BGP route hijacking is mogelijk omdat de routering door een steeds bredere groep partijen wordt verzorgd, terwijl het mechanisme uitgaat van vertrouwen tussen al deze partijen. Door

[52] Zie https://www.zdnet.com/article/russian-telco-hijacks-internet-traffic-for-google-aws-cloudflare-and-others/ voor een voorbeeld waarbij het ook achteraf niet goed vast te stellen was of er opzet in het spel was.

de grootte van de groep is niet meer mogelijk om zeker te stellen dat alle betrokken partijen betrouwbaar zijn.

Gerelateerde afwegingen rond waarden

Een belangrijke eigenschap van het internet is dat het open is, met lage toegangsdrempels (zie punt 1 in 4.4.2). Dat betekent dat iedere gebruiker, waar ook ter wereld, erop aan moet kunnen sluiten. Om dat mogelijk te maken, is vertrouwen in de ISP's in alle landen ter wereld essentieel, maar tegelijkertijd blijkt dat vertrouwen niet altijd gerechtvaardigd.

Incrementele oplossing: RPKI/BGPsec

Wat is de oplossing:

Het is, binnen de bestaande standaarden, mogelijk om BGP veiliger te maken. We noemen hier twee belangrijke componenten van de oplossing; voor een uitgebreidere discussie over het beveiligen van BGP verwijzen wij naar aanbevelingen vanuit NIST (Sririram en Montgomery 2019).

- RPKI: een stelsel van digitale handtekeningen en certificaten, waarmee partijen binnen het internet vast kunnen stellen dat routeringsinformatie voor een IP-blok afkomstig is van de partij die daadwerkelijk dat IP-blok beheert;
- BGPsec: een mechanisme om de uitgewisselde routeringsinformatie digitaal te ondertekenen.

Pro/con:

+ De combinatie van RPKI en BGPsec zou BGP route hijacking kunnen voorkomen, mits alle betrokken partijen deze standaarden daadwerkelijk implementeren. Dat wil niet alleen zeggen dat alle partijen de relevante "handtekeningen" op de verstuurde informatie zetten, maar dat alle partijen die handtekeningen ook valideren en alleen correct ondertekende informatie gebruiken.

- Met name BGPsec creëert nieuwe risico's, omdat voor het uitwisselen van certificaten een IP-verbinding nodig is; dat betekent dat er een "kip en ei" probleem kan ontstaan waarbij IP-routering correct moet werken om de informatie uit te wisselen die voor IP-routering nodig is.
- De implementatie komt (mede hierdoor) langzaam op gang, waardoor het probleem nog lange tijd aanwezig zal zijn.

Gremia:

BGP is afkomstig uit de IETF, en de genoemde oplossingen worden ook in de IETF besproken. Veel andere instituten (zoals NLnet Labs en SIDN Labs) doen onderzoek naar de adoptie, de problemen, en de mogelijke oplossingen.

Kansrijk:

Oplossingen gebaseerd op RPKI en BGPsec lijken ondanks de nadelen wel goede kansen te maken. Er wordt veel onderzoek gedaan naar de beste manier om ze te implementeren en om de nadelen te omzeilen. Voor een deel kunnen de nadelen ondervangen te worden door niet alles geautomatiseerd uit te voeren, maar deels te werken met handmatige processen (met name om het "kip en ei" probleem te voorkomen). De uitdaging is daarbij om de juiste balans

van handmatige en geautomatiseerde processen te implementeren, zodat de genoemde risico's ondervangen worden maar de schaalbaarheid van het internet daarbij niet aangetast wordt.

6.2.2 IP-spoofing

Omschrijving

Feature

De bestaande protocollen laten toe dat elk apparaat dat aan het internet hangt voor elk pakketje zelf het afzender-IP-adres invult. Dat maakt het internet flexibel; gebruikers kunnen vrij bepalen welke van de aan hen toegekende adressen zij voor welke toepassing gebruiken.

Vraagstuk

Apparaten kunnen een afzender-IP-adres invullen dat niet bij de betreffende gebruiker hoort. Dat maakt verschillende vormen van aanvallen mogelijk. Een bekend voorbeeld hiervan is een "Denial of Service" aanval, waarbij een aanvaller een groot aantal verzoeken aan een server stuurt met verschillende afzenderadressen, om daarmee de server zwaar te belasten. Doordat de adressen verschillend zijn is het lastig om het verkeer van legitiem verkeer te onderscheiden. Als de aanvaller dit vanuit een groot aantal apparaten tegelijk doet dan ontstaat een "Distributed Denial of Service" oftewel DDoS aanval.

Gerelateerde afwegingen rond waarden

Het vraagstuk is vooral gerelateerd aan de afweging tussen afscherming van informatie en inzage van informatie ten behoeve van veiligheid, maar ook aan de afweging tussen een open netwerk (iedereen kan aan iedereen pakketjes sturen) en vertrouwen (als je de ISP niet kunt vertrouwen, kun je ook niet weten of het IP-adres klopt).

Incrementele oplossingen: BCP 38 en 84

Wat is de oplossing:

In veel gevallen kan IP-spoofing voorkomen worden doordat elke ISP op elke router aan de randen van zijn netwerkverkeer blokkeert met een afzender adres dat niet kan horen bij de verzendende partij. Voor een ISP met consumenten of klein-zakelijke klanten is dat relatief eenvoudig: de ISP kent IP-adressen aan de klanten toe, en verifieert dat alle pakketjes die van de klant komen één van de toegekende adressen als afzender bevatten. De klant heeft daarbij nog steeds de flexibiliteit om verschillende toegekende adressen voor verschillende doelen te gebruiken. Voor deze oplossing is geen nieuwe standaard nodig; de methode is beschreven in BCP[53] 38 (RFC 2827).

Het wordt ingewikkelder als een gebruiker (vaak een groot-zakelijke gebruiker of een ISP) meerdere routes naar het internet heeft, en zelf IP-adressen regelt buiten de ISP om. Om desondanks te voorkomen dat de gebruiker "foute" IP-adressen als afzenderadres kan hanteren zijn er verschillende mechanismen mogelijk; deze zijn beschreven in BCP 84 (RFC 3704).

[53] Een BCP (Best Current Practice) beschrijft geen afwijkende protocollen maar een aanbevolen manier om de bestaande protocollen in te zetten.

Ook de eerdergenoemde NIST-aanbeveling SP 800-189 benoemt deze mechanismen, en geeft enkele praktische aanwijzingen voor de implementatie,

Pro/con

+ De genoemde mechanismen zijn in de meeste gevallen afdoende om IP-spoofing geheel te voorkomen.
+ BCP 38 is voor een ISP vrij eenvoudig te implementeren; BCP 84 is iets complexer maar nog steeds goed mogelijk.

- De genoemde mechanismen kunnen IP-spoofing alleen volledig voorkomen als alle betrokken partijen ze implementeren.
- Voor complexe routeringen is BCP 84 ingewikkelder om te implementeren, waardoor de kans op fouten toeneemt. Door dergelijke fouten kan er legitiem verkeer geblokkeerd worden.
- De partij die de mechanismen implementeert heeft daar de kosten van, maar niet de voordelen (want de voordelen zijn voor het hele internet). Er is dus weinig prikkel voor partijen om de oplossing te implementeren.

Betrokken gremia

De genoemde oplossingen worden in de IETF besproken. Veel andere instituten (zoals NLnet Labs en SIDN Labs) doen onderzoek naar de adoptie, de problemen, en de mogelijke oplossingen.

Kansrijk?

De meeste ISP's hebben in elk geval BCP 38 geïmplementeerd (Lone et al 2020), waardoor IP-spoofing al een stuk lastiger is geworden dan een aantal jaren geleden.

Zolang er echter ISP's zijn die, uit desinteresse of om andere redenen, geen stappen willen zetten zal IP-spoofing niet volledig uitgebannen kunnen worden. Daarom zullen systemen en netwerken additionele maatregelen moeten nemen om de aanvallen die via IP-spoofing mogelijk worden, te voorkomen of in elk geval de consequenties te beperken.

6.2.3 Traffic shaping/netneutraliteit

Omschrijving

Feature

De tot nu toe gebruikelijke protocollen op het internet, op de lagen die in scope zijn (met name TCP, UDP, en IP), geven inzicht in de diensten en applicaties waar de verkeersstromen bij horen. Zo kan een aanbieder bijvoorbeeld besluiten IP-pakketten voor streaming video op een andere manier af te handelen dan die voor e-mails; voor e-mails is het immers belangrijk dat ze aankomen, maar komt het niet op een seconde aan, terwijl streaming video best een keer een pakketje kan missen zolang de rest van de pakketjes tijdig aankomt.

Vraagstuk

Als een aanbieder (ISP) onderscheid kan maken tussen verschillende diensten of applicaties, dan kan hij daar ook oneigenlijke concurrentie mee introduceren. Een ISP die zelf videodiensten aanbiedt zou bijvoorbeeld videodiensten van zijn concurrenten naar zijn klanten toe

kunnen vertragen, om die klanten aan te moedigen zijn videodiensten te gebruiken. Ook als hij zelf geen videodiensten aanbiedt, zou hij aan een aanbieder van deze diensten kunnen voorstellen om zijn diensten voorrang te geven en die van anderen te vertragen – tegen betaling, uiteraard.

Dergelijke constructies kunnen de concurrentie beperken (bijvoorbeeld tussen de dienst van de ISP en die van concurrenten) en bovendien de innovatie afremmen (doordat alleen gevestigde partijen voorrang kunnen bedingen, waardoor nieuwe partijen niet dezelfde kwaliteit van diensten kunnen leveren).

Gerelateerde afwegingen rond waarden

Dit vraagstuk is vooral gerelateerd aan de afweging tussen het belang van gegarandeerde servicegaranties versus het uitgangspunt dat internet in de basis een 'best effort' karakter heeft waarbij geen sessies met gegarandeerde verbindingen worden opgezet, en waarbij alle pakketverkeer in principe gelijkwaardig is.

Incrementele oplossingen: wetgeving en encryptie

Wat is de oplossing:

In veel jurisdicties, waaronder in de Europese Unie, is dit probleem via wetgeving aangepakt, waarbij het hierboven beschreven gedrag verboden of beperkt wordt.

Verordening (EU) 2015/2120 bepaalt bijvoorbeeld (art. 3 lid 3):

"Aanbieders van internettoegangsdiensten behandelen bij het aanbieden van internettoegangsdiensten alle verkeer op gelijke wijze, zonder discriminatie, beperking of interferentie, en ongeacht de verzender en de ontvanger, de inhoud waartoe toegang wordt verleend of die wordt verspreid, de gebruikte of aangeboden toepassingen of diensten, of de gebruikte eindapparatuur."

De verordening geeft vervolgens enkele uitzonderingen, met name voor redelijke verkeersbeheersmaatregelen, wettelijke verplichtingen, de integriteit en veiligheid van het netwerk, en het voorkomen van congestie.

Er zijn echter ook technische mogelijkheden om het probleem aan te pakken. Steeds meer diensten maken gebruik van encryptie, waardoor het al lastiger wordt om onderscheid tussen specifieke diensten te maken. Met QUIC gaat dit nog een stap verder, aangezien QUIC ook een groot deel van de metagegevens van de dienst verbergt.

Pro/con

+ Zowel de juridische als de technische maatregelen kunnen het lastig of onmogelijk maken om verschillende diensten verschillend te behandelen, en daarmee de concurrentie en de innovatie te hinderen.

- De juridische maatregelen vereisen extra toezicht, en gedetailleerde richtlijnen over wanneer een verschillende behandeling wel of niet legitiem is. Dit kan tot grote "grijze gebieden" leiden waarbinnen de aanbieder toch nog ongewenst gedrag kan vertonen. De aanbieder kan bijvoorbeeld door handig gebruik van routing protocollen, het

beperken van capaciteit op specifieke routes, of door het al dan niet toelaten van Content Delivery Networks verschil in content maken zonder expliciet de regels te overtreden.
- De juridische maatregelen kunnen het lastig maken om onderscheid tussen verkeerstromen te maken wanneer daar wel goede redenen voor zijn, maar deze niet expliciet onder de uitzonderingen vallen. Er is bijvoorbeeld veel discussie of de verschillende use cases voor "slicing" in 5G wel of niet strijdig zijn met de regels rond netneutraliteit (Koers 2019).
- De technische maatregelen (encryptie en met name QUIC) maken ook legitieme maatregelen voor het netwerkbeheer lastiger.

Betrokken gremia

De juridische maatregelen vallen buiten het thema "standaardisatie", en de betrokken gremia verschillen per jurisdictie[54].

De technische maatregelen worden grotendeels gestandaardiseerd binnen de IETF. Een bijzonder geval is eTLS, dat door ETSI is gestandaardiseerd. eTLS wordt behandeld onder 6.2.5.

Kansrijk?

De beschreven juridische maatregelen bestaan al enige tijd, en lijken grotendeels te werken (al blijft er zoals gezegd een grijs gebied over). Er zijn wel nog regelmatig discussies over het verschillend tariferen van verkeer (waaronder "zero rating" om eigen diensten te bevoordelen), en ook de opkomst van 5G introduceert weer nieuwe discussies over netneutraliteit (Koers 2019).

Encryptie wordt al op het meeste verkeer toegepast, en ook QUIC (dat onderscheid tussen diensten lastiger maakt) wordt steeds meer gebruikt.

6.2.4 Weinig zicht op ongewenste content

Omschrijving

Feature

Encryptie maakt het mogelijk om privacygevoelige of anderszins vertrouwelijke informatie te beschermen tegen afluisteren op de route tussen de eindpunten.

Vraagstuk

In veel gevallen zijn er legitieme redenen om bepaalde content te weren. Gebruikers willen beschermd worden tegen malware, phishing, etc., overheden willen voorkomen dat gebruikers illegale content zoals kinderporno uit kunnen wisselen, en rechthebbenden willen hun auteursrechten kunnen beschermen.

[54] De juridische aspecten zijn buiten de scope van dit onderzoek. In Nederland zijn hierbij onder andere het Ministerie van Economische Zaken en Klimaat, de ACM, en Agentschap Telecom relevant, en in Europa onder andere de EC (DG Connect) en BEREC.

Encryptie maakt het voor de ISP moeilijk, of zelfs onmogelijk om deze content te blokkeren of te signaleren, zelfs al zouden ze hiertoe verplicht worden. Dit kan dan alleen nog bij de bron of bij de bestemming.

Het recht op privacy conflicteert in dit geval met andere algemeen erkende waarden, zoals de bescherming van kinderen tegen seksuele exploitatie via kinderporno.

Zoals in paragraaf 5.2.3 aangegeven bevindt dit vraagstuk zich op de applicatielaag, en zou het dus buiten de scope moeten vallen.

Omdat de eindpunten vaak buiten het zicht van de ISP en van de overheid vallen (met name als de server in het buitenland staat), is er desondanks een sterke wens vanuit veel overheden om via de onderliggende lagen toch ongewenste content te kunnen blokkeren.

Gerelateerde afwegingen rond waarden

Het vraagstuk is vooral gerelateerd aan de afweging tussen het belang van afscherming van informatie en het belang van inzage van informatie ten behoeve van veiligheid.

Incrementele oplossingen: bronnen blokkeren, encryptie (wetmatig) beperken

Wat is de oplossing:

Aangezien het vrijwel onmogelijk is om de encryptie te doorbreken waarmee de content beschermd is (in elk geval in "real time"), wordt er vaak gezocht naar oplossingen op de lagen eronder. Oplossingen die regelmatig worden voorgesteld zijn:

- Encryptie verbieden, of encrypted content blokkeren;
- Encryptie afzwakken of voorzien van "achterdeurtjes";
- Specifieke IP-adressen blokkeren waarvan bekend is dat die ongewenste content aanleveren;
- Specifieke hostnames in de DNS blokkeren.

Pro/con

- Encryptie verbieden of afzwakken heeft grote nadelen voor de privacy en andere gegevensbescherming, en zet de deur open voor schendingen van mensenrechten in landen waar die toch al bedreigd worden[55]. Achterdeuren of universele sleutels inbouwen levert het risico op dat ook verkeerde partijen toegang krijgen[56]. Dergelijke ingrepen kunnen (op termijn) het vertrouwen in de veiligheid en betrouwbaarheid schaden.
- Specifieke IP-adressen blokkeren werkt, totdat de aanbieder van de ongewenste content van IP-adres wisselt, of totdat de gebruiker de verbinding via een buitenlandse VPN-provider opzet. Tegelijkertijd kan een IP-blokkade ook veel andere (legitieme) content blokkeren, aangezien er zelden een één op één relatie is tussen diensten en IP-adressen.

[55] Zie https://ecp.nl/wp-content/uploads/2021/11/Argumentenkaart-inperking-encryptie2.pdf

[56] Zie bijvoorbeeld http://www.slaw.ca/2020/01/15/encryption-backdoors-a-very-bad-idea/ voor een uitgebreidere beschrijving van de nadelen.

- Hostnames in de DNS blokkeren werkt beperkt, aangezien de gebruiker ook op andere manieren bij de content kan komen. Bovendien wordt steeds vaker gebruik gemaakt van DNS servers in andere jurisdicties, bijvoorbeeld via Google DNS, of via DNS over HTTPS (DoH). Alle browsers kunnen inmiddels DoH gebruiken, en bij Firefox is het in de Verenigde Staten zelfs de default instelling (met Cloudflare als DNS provider). Dat maakt het voor een overheid lastig om blokkades via DNS af te dwingen.

Betrokken gremia

Mogelijkheden voor het blokkeren van ongewenste content zijn in het verleden wel binnen de IETF besproken, zonder dat dit tot nieuwe standaarden heeft geleid. IETF is voorzichtig met dit thema, omdat elke mogelijkheid om content te blokkeren ook door autoritaire regimes gebruikt kan worden om kritiek op het regime te blokkeren.

In de IETF-draft "draft-elkins-hrpc-ifilter-00" (Elkins 2018) beschreef de auteur verschillende redenen om content te blokkeren, waarbij duidelijk werd dat sommige niet compatibel zijn met westerse waarden en andere wel. Tegelijkertijd is het niet mogelijk om technische mechanismen te ontwerpen die dat onderscheid zouden kunnen maken. Om die reden is er verder niets meer mee gedaan[57].

Omdat verzwakking van encryptiemogelijkheden niet goed binnen IETF te standaardiseren blijkt, proberen belanghebbenden dit soms via andere organisaties te organiseren. Een voorbeeld is eTLS (binnen ETSI), zie 6.2.5.

Kansrijk?

Er zijn voor dit vraagstuk geen kansrijke, internet-brede oplossingen, althans niet op de lagen die in scope van deze opdracht zijn. Alle genoemde oplossingen hebben grote nadelen.

Om zicht op de content te krijgen moet een oplossing zich richten op de eindpunten, dat wil zeggen de bron en de bestemming van de communicatie. Dat is lastig, omdat het ene eindpunt vaak een server in het buitenland is, en het andere eindpunt een device van een consument. Toch zijn dat de enige plekken waar er überhaupt een structurele oplossing mogelijk is.

6.2.5 Interceptie van de inhoud

Omschrijving

Feature

Er kunnen veel partijen betrokken zijn bij het routeren van pakketten over het internet: de lokale ISP, de verschillende "upstream" ISP's, internet exchanges etc.

Vraagstuk

Elk van de betrokken partijen kan in principe in de pakketten kijken, en de inhoud zien of zelfs manipuleren. Aangezien de protocollen algemeen bekend zijn, is het eenvoudig om de pakketten te analyseren en de inhoud eruit te halen of te wijzigen.

[57] Zie ook RFC 7754 en RFC 7258.

Gerelateerde afwegingen rond waarden

De betrokken partijen hebben vaak een legitieme reden om zicht op de inhoud te willen (wettelijke verplichtingen, netwerkmanagement etc.) maar de gebruiker heeft ook recht op privacy.

Incrementele oplossingen: encryptie

Wat is de oplossing:

De meest gebruikelijke oplossing is encryptie: door de inhoud te versleutelen wordt het voor de partijen op de route moeilijk of onmogelijk om de inhoud eruit te halen. Waar een aantal jaren geleden het meeste verkeer onversleuteld was, wordt het steeds gebruikelijker om de inhoud te versleutelen. De gebruiker hoeft hier meestal niets voor te doen; de browsers selecteren bijvoorbeeld waar mogelijk de versleutelde versie van een website (https:) en geven een waarschuwing als er alleen een onversleutelde versie beschikbaar is. Ook voor mail en andere veelgebruikte diensten zijn er versleutelde versies beschikbaar.

Ook het nieuwe transport protocol QUIC maakt gebruik van TLS, niet alleen voor de inhoud maar ook voor een deel van de metadata.

Pro/con

+ Versleuteling maakt het moeilijk voor een partij op de route om kennis te nemen van de inhoud of om deze te wijzigen.

- Versleuteling kan een verwachting van privacy leveren, terwijl het soms (door zwaktes in de algoritmes of door brute-force) voor een actor met voldoende middelen toch mogelijk is om de inhoud te lezen. Ook kan het voorkomen dat versleuteling niet end-to-end is maar bijvoorbeeld termineert bij een Content Distribution Network (CDN).
- Versleuteling van inhoud maakt het lastiger voor bedrijven en instellingen om controles op de in- en uitgaande datastromen uit te voeren.

Betrokken gremia

De bekendste vorm van versleuteling is TLS; deze wordt door de IETF gestandaardiseerd. De technologie is steeds in ontwikkeling, en daarom worden er ook geregeld nieuwe versies van TLS vastgesteld. Op dit moment is de actuele versie TLS 1.3.

Voor veel van de gebruikelijke protocollen op het internet heeft de IETF versleutelde versies gedefinieerd, meestal gebaseerd op TLS. Zo zijn er “secure” versies van POP3 en SMTP (mail), van SIP (onder andere voor telefonie), en van veel andere protocollen.

TLS 1.2 en eerdere versies hadden echter een risico in zich: het was mogelijk om een “statische” sleutel te gebruiken, waardoor een aanvaller met kennis van de sleutel de inhoud kon lezen (ook achteraf nog). Dit is opgelost in TLS 1.3.

Voor sommige instellingen leverde dit een probleem op, aangezien zij in hun eigen infrastructuur juist gebruik maakten van deze zwakte in TLS 1.2. Met name banken gebruikten deze zwakte om toezicht te houden op het in- en uitgaande verkeer. Feitelijk was dit een vorm van interceptie, maar dan op hun eigen inhoud. Met TLS 1.3 is dit niet mogelijk.

Onder druk van deze instellingen is binnen ETSI daarom een variant van TLS ontwikkeld (formeel bekend als TS 103 523, maar algemeen aangeduid als “eTLS”). De ontwikkeling werd

gesteund door het Britse NCSC (National Cyber Security Centre, onderdeel van de inlichtingendienst GCHQ).

De eTLS variant van TLS heeft alle eigenschappen van TLS 1.3, maar laat wel statische sleutels toe. Voor de betreffende banken is dat een voordeel (ze hoeven geen grote wijzigingen in hun infrastructuur uit te voeren), maar in het algemeen wordt het als een belangrijke zwakte gezien.

Het Nederlandse NCSC (Nationaal Cyber Security Centrum) waarschuwt daarom uitdrukkelijk tegen het gebruik van de eTLS variant (NCSC 2019).

Kansrijk?

Encryptie wordt zeer veel gebruikt, vaak zonder dat de gebruiker er iets voor hoeft te doen.

Ondanks de geregeld terugkerende discussies over het verbieden of verzwakken van encryptie (zie 6.2.4) lijkt het waarschijnlijk dat steeds meer inhoud versleuteld zal worden met steeds sterkere encryptie mechanismen. Dat zien we nu al: de meeste webpagina's worden nu versleuteld opgehaald, de meeste mail wordt versleuteld, videoconferentie-diensten zoals Microsoft Teams versleutelen al het verkeer, en ook veel telefoniediensten over internet (VoIP) worden inmiddels versleuteld aangeboden. Het verkeer van Netflix en andere videoproviders is ook versleuteld, zowel om de privacy van de gebruiker te borgen als om de verstuurde inhoud tegen kopiëren te beschermen.

6.2.6 Interceptie van metagegevens

Omschrijving

Feature

Iedere partij die bij de routering van IP-pakketten betrokken is (van de eigenaar van een wifi hotspot tot de ISP's op de route) heeft de mogelijkheid om de pakketten te analyseren en die informatie voor de afhandeling van de pakketten te gebruiken.

Vraagstuk

Zelfs als de content versleuteld is, kan de metadata al veel informatie over de gebruikte dienst geven. Vanuit het oogpunt van privacy en bedrijfsvertrouwelijkheid is dat ongewenst.

Als een gebruiker bijvoorbeeld een website bezoekt, dan kan de lokale ISP al uit de DNS query afleiden welke site (hostname) het betreft. Vervolgens kan elke aanbieder op de route diezelfde informatie ook uit de eerste pakketten van de verbinding halen, zelfs als de gebruiker een versleutelde verbinding gevraagd heeft (via https:).

Andere protocollen hebben soortgelijke problemen: de encryptie werkt pas als de gebruiker toegang tot de server heeft, dus is uit de eerste pakketten wel al duidelijk welke hostname en vaak ook welke dienst het betreft.

Gerelateerde afwegingen rond waarden

Ook dit vraagstuk is vooral gerelateerd aan de afweging tussen het belang van de ISP om aan wettelijke verplichtingen te voldoen en om zijn netwerk efficiënt te beheren, en het recht van de gebruiker op privacy.

Incrementele oplossingen: encryptie van (een deel van) de metagegevens

Wat is de oplossing:

Voor de privacy van het DNS protocol zijn er meerdere oplossingen; de meest relevante is DNS over HTTPS (DoH). Bij DoH wordt de DNS query in HTTPS verpakt, en dus via een encrypted tunnel (TLS) aan een server gestuurd; ook de reactie komt via diezelfde tunnel. Daarmee wordt het vrijwel[58] onmogelijk voor de partijen op de route naar die server om de hostnaam in te zien.

Ook voor de privacy van TLS (en daarmee HTTPS) zijn er oplossingen, zoals Encrypted Client Hello (ECH) dat het mogelijk maakt om de naam van (bijvoorbeeld) de website te verbergen.

Pro/con

+ DoH: alle informatie in het DNS verzoek wordt versleuteld, waardoor de lokale ISP (maar ook bijvoorbeeld de eigenaar van een wifi hotspot) geen zicht meer op de gebruikte dienst heeft.
+ ECH: de naam van de site (hostname) wordt versleuteld, waardoor de partijen op de route alleen nog het IP-adres van de server kunnen zien. Aangezien servers vaak een groot aantal websites hosten is een deel van het privacy probleem daarmee al opgelost

- DoH: de partij die de DoH dienst aanbiedt ziet wel de volledige DNS query. Vaak bevindt deze partij zich in een andere jurisdictie, waardoor toezicht op de privacy alleen maar lastiger wordt. DoH verschuift feitelijk het privacy probleem van de lokale ISP naar een andere partij, vaak een grote wereldwijde speler. Er zijn wel ontwikkelingen om dit nadeel tegen te gaan (onder andere Oblivious DoH, dat de afzender van de query verbergt).
- Bijkomend nadeel van DoH is dat de authorative DNS server (de server die uiteindelijk het antwoord geeft) geen informatie heeft over de regio waar de gebruiker zich bevindt, en dus niet meer de dichtstbijzijnde server aan kan geven. Daar is weliswaar ook weer een oplossing voor beschikbaar (EDNS Client Subnet), maar die levert weer nieuwe privacy issues.
- Geen van de genoemde oplossingen kan verhinderen dat een partij op de route inzicht krijgt in de betrokken IP-adressen, de hoeveelheid data, of de tijdstippen van de communicatie. Daarmee is een deel van de metadata dus altijd zichtbaar[59]. Een VPN kan de IP-adressen wel voor de ISP afschermen, maar verplaatst feitelijk het probleem van de lokale ISP naar de aanbieder van het VPN.

[58] Theoretisch kun je aan de hand van een interceptie van een IP-adres van de server daar een reverse lookup op uitvoeren en zo de domeinnaam achterhalen.
[59] en deze wel zichtbare informatie kan de partij soms via reverse lookups of andere intelligentie meer informatie verschaffen zoals één of meer mogelijke hostnamen

Betrokken gremia

De genoemde verbeteringen worden allen binnen de IETF gestandaardiseerd. Voor VPN's zijn er naast IETF-protocollen ook andere protocollen beschikbaar, bijvoorbeeld van Microsoft.

Kansrijk?

De genoemde oplossingen zijn al op enige schaal in gebruik, en relatief eenvoudig te implementeren. Ondanks de genoemde nadelen lijkt het erop dat met name DoH snel zal groeien, wellicht met uitbreidingen die deze nadelen ondervangen (zoals Oblivious DoH).

6.2.7 Zeggenschap op verkeer (soevereiniteit)

Omschrijving

Feature

Het internet is zeer flexibel ontworpen; er zijn geen vaste routes maar elk deel van het internet (AS, Autonomous System) bepaalt de beste route voor dat moment aan de hand van informatie van andere AS'en. Daardoor kan het internet stabiel werken, terwijl de onderliggende verbindingen vaak niet stabiel zijn.

Vraagstuk

Aangezien de routes dynamisch zijn, kan de afzender van een pakket niet weten welke route het pakket zal volgen, en er geen invloed op uitoefenen. Voor de meeste gebruikers is dat ook niet relevant, maar een partij die bijvoorbeeld vertrouwelijke data verwerkt loopt hierdoor het risico dat die data door jurisdicties loopt met regelgeving die strijdig is met zijn eigen verplichtingen.

Een voorbeeld: als beide eindpunten van een verbinding binnen de EU staan, zou de route voor pakketten door landen kunnen lopen die niet voldoen aan de regels van de Algemene Verordening Gegevensbescherming (AVG). De gebruiker heeft hier geen invloed op, en kan dus niet garanderen dat alle partijen op de route aan de AVG gebonden zijn.

Ook instellingen die zich bezighouden met de staatsveiligheid hebben er vaak behoefte aan om controle te hebben over de routes die pakketten volgen, om te voorkomen dat deze door andere mogendheden afgeluisterd, gemodificeerd of geblokkeerd kunnen worden.

Gerelateerde afwegingen rond waarden

Hier speelt met name de afweging tussen het belang van efficiënte routering (soms loopt de handigste route via een andere jurisdictie), het belang van gebruikers om zich aan de wet te houden, en het belang van overheden om de voor hen belangrijke waarden via wetten af te kunnen dwingen (zoals in het voorbeeld van de AVG).

Incrementele oplossingen (theoretisch): toevoegen routeinformatie

Hoewel het in principe mogelijk is om de huidige routeringsprotocollen te gebruiken om routes met specifieke eigenschappen te selecteren, zijn er momenteel geen werkbare oplossingen die een gebruiker garanderen dat de route binnen een bepaalde jurisdictie blijft (bijvoorbeeld binnen de EU of binnen Nederland), of binnen de groep landen met een set gezamenlijke uitgangspunten of waarden (bijvoorbeeld de groep van landen waar de AVG geldt dan wel die als

gelijkwaardig beschouwd mogen worden). In theorie is dit wel mogelijk via de bestaande routeringsprotocollen; een voorstel voor een dergelijke oplossing stuitte eerder echter op veel weerstand (zie ten Oever, Niels. 2021a).

Het is wel mogelijk om regelmatig te controleren welke route pakketten nemen, maar dat geeft geen enkele garantie dat dat zo blijft.

De meeste oplossingen zijn daarom defensief van aard: accepteren dat de route wellicht door andere jurisdicties loopt, en de integriteit en vertrouwelijkheid van de gegevens op de hogere lagen borgen, bijvoorbeeld via sterke encryptie.

Pro/con

- Elke oplossing die afdwingt dat een route binnen een bepaalde jurisdictie blijft, sluit daarmee automatisch routes uit die daar niet aan voldoen, waardoor de beschikbaarheid van de verbinding minder kan worden.
- Routeren op een andere basis dan alleen de technische eigenschappen van de betrokken routes verhoogt de complexiteit van de routering en van de onderliggende configuraties.

Betrokken gremia

Hoewel er wel discussies binnen IETF en RIPE zijn geweest, is er op dit moment in geen van de betrokken gremia een oplossing in ontwikkeling.

Kansrijk?

Er is binnen de internetgemeenschap veel weerstand tegen het inperken van routes, en met name tegen het verbinden van de wensen op applicatieniveau met de routering op de onderliggende lagen. Dat zou de gelaagdheid van het internet verstoren, waardoor de complexiteit uiteindelijk toeneemt en de beschikbaarheid moeilijker te borgen wordt.

Het lijkt dan ook niet waarschijnlijk dat er uit deze hoek de komende tijd een oplossing zal komen (en er is zelfs geen consensus over de vraag of er wel een probleem is). Veel betrokkenen zien het internet als een inherent mondiaal fenomeen, waarbinnen het zinloos is om onderscheid tussen jurisdicties te willen maken.

6.2.8 Innovatie, flexibiliteit en veranderbaarheid van de infrastructuur

Omschrijving

Feature

Door het grote succes van het internet is er een enorme “installed base” van hardware en software die gebruik maakt van internetprotocollen. Hetzelfde geldt voor de mobiele netwerken, die gebruik maken van de 3GPP protocollen.

Vraagstuk

Terwijl de stabiliteit van de internetprotocollen een enorme hoeveelheid innovatie *over* het internet mogelijk heeft gemaakt, is het lastiger geworden om in het internet zelf te innoveren. De protocollen zijn zo complex geworden dat kleine veranderingen vaak onverwachte effecten teweegbrengen, en de hoeveelheid apparatuur en software die op basis van de bestaande

protocollen is gebouwd is zo groot dat het bijna onmogelijk is om die protocollen nog aan te passen. Dat geldt met name op de IP-laag, die in alle operating systems en routers is ingebouwd. De moeite die het kost om IPv6 geïmplementeerd te krijgen is wat dat betreft tekenend.

Ook op de transportlaag is innovatie erg lastig. TCP en UDP zijn de laatste tientallen jaren niet meer wezenlijk aangepast; wel zijn er voor TCP verbeterde mechanismen geïntroduceerd om met congestie om te gaan. QUIC is het eerste nieuwe transport protocol sinds lange tijd, en levert werkelijke innovatie op de transportlaag. QUIC zou echter nooit tot stand gekomen zijn zonder druk vanuit Google, aangezien andere partijen niet dezelfde schaalgrootte en dezelfde mate van toegang tot browsers én servers hebben als Google.

Voor mobiele netwerken is de innovatie iets makkelijker: de meeste 3GPP protocollen kunnen binnen een specifiek netwerk geïmplementeerd worden, zonder te hoeven te wachten tot anderen hetzelfde doen. Generaties van 3GPP (3G, 4G, 5G) kunnen naast elkaar opgebouwd worden, totdat alle eindgebruikers apparatuur hebben gekocht die de nieuwste versie aan kan zodat de oudere opgedoekt kunnen worden.

Gerelateerde afwegingen rond waarden

Dit vraagstuk is vooral gerelateerd aan de afweging tussen innovatie versus interoperabiliteit.

Incrementele oplossingen: compatibiliteit combineren met vernieuwing

Een belangrijke "oplossing" is achterwaartse compatibiliteit. Door nieuwe versies van protocollen te definiëren die probleemloos samenwerken met de oude, is het mogelijk de nieuwe versies geleidelijk te introduceren.

De andere veel gebruikte oplossing is om de bestaande protocollen intact te laten, maar nieuwe protocollen te definiëren die bovenop of in plaats van de oude te gebruiken zijn. QUIC komt bijvoorbeeld naast TCP (en op UDP).

Pro/con

+ De genoemde oplossingen laten de mogelijkheid open om nog heel lang met de oude versie van de protocollen te werken (in tegenstelling tot bijvoorbeeld 3GPP generaties, waarbij apparatuur in elk geval op de air interface alleen werkt als het de juiste generatie implementeert).

- Een gevolg van de genoemde oplossingen is dat de complexiteit steeds verder toeneemt. Doordat er steeds meer protocollen gedefinieerd worden die op elkaar voortbouwen, wordt het alleen maar nog moeilijker om de oorspronkelijke protocollen aan te passen. Een goed voorbeeld is DNS, dat inmiddels duizenden pagina's aan standaarden omvat[60]. Dit nadeel is enigszins te ondervangen door oudere versies van protocollen vanaf enig moment niet meer te ondersteunen.
- Een ander aandachtspunt is dat de bedrijven achter verschillende lagen van het internet meer geconsolideerd zijn en het voor kleinere stakeholders in standaardisatiegremia niet altijd gemakkelijk is om voorstellen van grote internetspelers, en de implicaties daarvan – op waarde te schatten en er substantieel tegenwicht aan te bieden.

[60] Zie https://www.ietf.org/blog/herding-dns-camel/

Betrokken gremia

De genoemde voorbeelden komen uit de IETF en 3GPP, maar het onderliggende probleem raakt eigenlijk aan alle gremia waar standaardisatie een rol speelt.

Kansrijk?

Het hier beschreven model van incrementele ontwikkeling blijkt tot nu toe, ondanks de nadelen, goed te werken. De hoeveelheid apparatuur die volgens bestaande standaarden werkt maakt elke andere benadering feitelijk onhaalbaar.

Ondanks alle commentaren dat het internet "stuk" zou zijn, zien wij op dit moment geen aanwijzingen dat het model van incrementele verbeteringen op termijn niet houdbaar zou zijn. Wel zullen de standaardisatieorganisaties (met name IETF) nog meer dan nu aandacht moeten geven aan de toenemende complexiteit, en daarbij regelmatig verouderde standaarden op moeten schonen. Op een aantal deelgebieden zien we hier al verbeteringen, bijvoorbeeld op het gebied van DNS[61].

6.2.9 Gebrek aan mogelijkheden voor duurzaamheid

Omschrijving

Feature

Elektronische communicatie heeft als alternatief voor fysieke contactmomenten enorme duurzaamheidsvoordelen. Daarbij is opslag en vervoer van data zeer veel efficiënter geworden dan voor de introductie van internet, en hebben intelligentie en informatie-uitwisseling en daarop gebaseerde meet- en regeltechniek mede gezorgd voor enorme efficiencyverbeteringen in zo ongeveer alles wat energie gebruikt.

Het internet heeft echter ook gezorgd voor een enorme toename van gecommuniceerde, opgeslagen en verwerkte data. Er worden in wetenschap en maatschappelijk debat dan ook veel vragen gesteld over de duurzaamheid van IT in het algemeen, en de datatransmissie in het bijzonder.

Het internet en de applicaties daarboven op kennen features om de hoeveelheid datatransport te beperken zoals caching. Maar vanwege het best effort karakter en de wens om meer plaatsen back-up informatie te hebben (redundantie) wordt heel veel data gedupliceerd, dicht bij de eindbestemming toch weggegooid, of meerdere malen herzonden naar dezelfde bestemming als niet zeker is dat het is aangekomen.

Vraagstuk

Onder andere door de discussies rond datacenters is er steeds meer aandacht voor de ecologische footprint van de digitalisering. Daarbij ontstaat de vraag of digitalisering een duurzaamheidsbevorderaar is of in de toekomst ook een mogelijke duurzaamheidsremmer. De steeds

[61] In 2019 en in 2020 werden "DNS Flag Days" afgekondigd, waarna de betrokken partijen een aantal verouderde DNS constructies niet meer ondersteunden. Dit dwong alle overige partijen om ook van deze constructies af te stappen.

doorgaande miniaturisering en toenemende efficiency van apparaten, netwerken en datacenters zorgde er tot nu toe voor dat ondanks het steeds maar weer toenemende gebruik het totale energieverbruik beperkt bleef. Maar blijft dat zo? En als dit niet het geval is, is dit niet deels te wijten aan de fundamenten van het internet dat toepassing-agnostisch en best effort is georganiseerd en leidt tot flat fees, peering agreements en niet of nauwelijks tot gebruik afremmende of beperkende prijsmodellen?

Gerelateerde afwegingen rond waarden

Hier speelt de afweging tussen internet als enabler van duurzaamheid versus verkleining van de ecologische footprint van het internet zelf een rol. Maar ook hier speelt op de achtergrond de afweging tussen het belang van innovatiebevordering versus interoperabiliteit.

Incrementele oplossingen: toevoegen van routeinformatie

Het is in principe mogelijk om de huidige routeringsprotocollen te gebruiken om routes met specifieke eigenschappen te selecteren. Dit zou dus ook gebruikt kunnen worden om meer duurzamer routes te selecteren boven minder duurzame routes, mits er een algemeen geaccepteerde en gevalideerd systeem ingevoerd zou kunnen worden om (delen van) routes in de gezamenlijke databases[62] te labelen met variabelen die deze selectie ondersteunen. Een partij die een voorkeur heeft voor "duurzame" routes zou dan de mogelijkheid hebben om informatie van andere partijen over de duurzaamheid van hun netwerk te betrekken in zijn routeringsbeslissingen.

Pro/con

+ Partijen kunnen elkaar op een gestandaardiseerde manier laten weten hoe "duurzaam" hun netwerk is, zonder dat anderen (die hier niet aan deelnemen) gedwongen worden om aanpassingen te maken.

- Routes worden nu vooral geselecteerd op de kans van aflevering van het pakket, en routeprotocollen worden onder andere gebruikt voor het balanceren van het verkeer van verschillende mogelijke routes. Dit zou een extra aspect introduceren die dus andere belangen minder prominent maakt. Dit is zowel een voordeel als een nadeel. Een alternatieve route (die bijvoorbeeld sneller, goedkoper of minder bezet is) kan dan toch lager scoren doordat deze minder duurzaam is dan andere routes.
- De oplossing introduceert extra complexiteit in het routeringsmechanisme (maar alleen voor partijen die besluiten hier aan deel te nemen).

Betrokken gremia

Op dit moment wordt dit soort oplossingen alleen nog buiten de traditionele standaardisatieorganisaties geopperd, zoals bij SCION maar het heeft wel politieke aandacht (zoals in een publicatie op de website van het World Economic Forum[63]). Binnen de IETF zijn er wel RFC's te vinden over dit onderwerp maar die zijn niet heel actueel (zoals een voorstel[64] om energiegebruik mee te nemen in de kenmerken van MPLS-paden) of enigszins met een knipoog (zoals

[62] Bijvoorbeeld die van RIPE, zie https://ripe78.ripe.net/presentations/105-Taking-The-High-Route-Routing-WG.pdf voor een vergelijkbaar mechanisme.
[63] Zie o.a. https://www.weforum.org/agenda/2021/03/internet-carbon-emissions-data-path-scion/
[64] https://datatracker.ietf.org/doc/html/draft-li-ospf-ext-green-te-01

een RFC van 1 april 2015[65] die het mogelijk maakt data via de meest milieuvriendelijke route te routeren).

Kansrijk?

Er is op dit moment nog veel discussie over wat precies het probleem is en hoe dit kan worden gekwantificeerd. Een aantal wijdverspreide claims over bijvoorbeeld de ecologische footprint van het bekijken van een Netflix-film blijken bij nader onderzoek niet te kloppen. Betere en meer onafhankelijke monitoring van de daadwerkelijke ecologische footprint (stroomverbruik, ruimtegebruik en watergebruik) van datacenters, netwerken en devices is nodig om duurzaamheid bij de routeringskeuzes te kunnen betrekken.

6.2.10 Gebrek aan Quality of Service

Omschrijving

Feature

Het internet werkt op basis van best effort. Dat betekent dat packets die binnenkomen op een switch, in principe in volgorde worden afgehandeld. Volgens critici betekent dit dat het netwerk voor tijd-kritische communicatie zoals telefonie pakketten zou kunnen vertragen of weggooien, terwijl er ook niet-tijd kritische communicatie verwerkt wordt, zoals een webpagina.

Er zijn verschillende voorstellen om verkeer dat "belangrijk" is een hogere prioriteit te kunnen geven. Het idee is dat deze communicatie dan wel tijdig aankomt bij de gebruiker en dat bijvoorbeeld een telefoniegesprek ongestoord kan worden gevoerd, terwijl het laden van een webpagina even moet wachten.

QoS is een essentieel deel van bijna elke alternatieve architectuur voor het internet. Het was een belangrijk onderdeel van X.25 en ATM-technologieën. In mobiele netwerken is het beschikbaar voor bijvoorbeeld telefonie. Bij het opzetten van een VoLTE verbinding wordt een prioriteitsklasse meegegeven aan het telefonieverkeer, waardoor het netwerk weet dat dit verkeer voorrang heeft op ander verkeer, zoals "gewoon" IP-verkeer.

Proponenten van de huidige structuur van het internet zeggen dat QoS in de praktijk niet veel toevoegt of zelfs ronduit niet werkt. Zij wijzen erop dat de communicatie zich in kabels en door de lucht verplaatst met de snelheid van het licht. Dat betekent dat datapakketten elkaar niet kunnen inhalen. Prioriteit is dus niet als een sirene en zwaailichten op een ambulance. De enige plek waar "winst" gehaald kan worden is in switches en routers. In principe hoort een de uitgang van een router niet overladen te worden, en lopen de buffers dus niet vol. Een prioriteitsklasse zorgt in dat soort gevallen niet voor een verbetering van het netwerk. Zit een verbinding te vol, dan zal een prioriteitsklasse geen effect hebben omdat de switch het inkomende verkeer niet kan verwerken. Dit is als een ambulance die snel een verkeersknooppunt probeert te doorkruisen, dat werkt alleen als het niet te druk is en er nog ruimte is om ruimte te maken voor de ambulance. QoS voegt dus alleen iets toe wanneer de buffer bijna vol zit, maar nog niet overladen is, dan kan de switch mogelijk een pakketten prioriteit geven, maar

[65] https://datatracker.ietf.org/doc/html/rfc7511

als er iets meer data komt, dan de buffer kan verwerken, dan kan de prioriteitsbit niet worden gelezen. QoS implementaties zorgen volgens sommigen daarmee wel voor complexiteit, maar lossen geen problemen op.

Het niet ondersteunen van QoS wordt ook wel gezien als feature, omdat het zou betekenen dat pakketten niet onderling gediscrimineerd worden. Het netwerk is neutraal ten opzichte van het verkeer. Dit is niet alleen een ethisch argument, maar ook een economisch argument. QoS verhoudt zich niet goed met een structuur van netwerk van netwerken; wat prioriteit heeft voor de ene partij heeft mogelijk geen prioriteit voor de ander. Waarom zou een academisch netwerk een prioriteitsbit moeten honoreren die gezet is door een gebruiker op een bancair netwerk of een consument?

Vraagstuk

De interactie tussen verkeersstromen kan voor gebruikers een probleem zijn. Het thuis downloaden van een grote update voor een game kan effect hebben op de kwaliteit van een videovergadering vanuit huis. Vooral interactieve communicatie tussen mensen heeft een constante en ononderbroken stroom aan data nodig. De download mag best een paar minuten langer duren, maar een onderbreking van een seconde in een gesprek maakt conversatie zeer onprettig.

Gerelateerde afwegingen rond waarden

Ook hier spelen vrijwel alle van de in 4.6 genoemde afwegingen mee, maar voornamelijk de afweging tussen het belang van gegarandeerde servicegaranties versus de succesfactor dat internet van oudsher juist is gebouwd met een ‘best effort’ karakter.

Incrementele oplossingen

Er zijn verschillende incrementele oplossingen voorgesteld om het probleem van onderbrekingen in diensten die de gebruiker belangrijk vindt aan te pakken. Een veelgebruikte is om in de switch of router te configureren dat een bepaalde hoeveelheid capaciteit gereserveerd is voor bijvoorbeeld telefonie of video. De verbinding kan dan niet volledig worden gebruikt als er wordt gebeld. De download heeft minder ruimte, maar er wordt capaciteit beschikbaar gehouden voor telefonie. Dit kan eventueel dynamisch, zodat alle capaciteit beschikbaar is op momenten dat de telefoon of de televisie niet wordt gebruikt.

Een variant hiervan in de netwerken van ISP’s en bedrijven is dat verkeer met prioriteit soms over separate verbindingen wordt verzonden. Het “gewone” internetverkeer gaat over de ene poort op de switch en glasvezel en het telefonieverkeer over een andere. In feite worden er dan twee verbindingen gebruikt ieder voor een eigen dienst, in plaat van dat de totale capaciteit van beide verbindingen kan worden gebruikt voor beide diensten.

Er zijn ook een aantal protocollen ontworpen in de IETF voor QoS. DiffServ is daarvan de meest recente implementatie. RFC 2474 is in 1998 gepubliceerd. Het specifieert een QoS klasse die in de header van een IP-packet kan worden meegegeven. Het gebruik ervan heeft zich vooral beperkt tot interne netwerken van ISPs. ISPs honoreren de QoS classificering van andere aanbieders meestal niet. DiffServ classificatie van bijvoorbeeld het VoIP-verkeer in een bedrijfsnetwerk is vaak wel gebruikelijk. Of het echt een significant voordeel oplevert kan een punt

van discussie zijn, maar netwerkbeheerders stellen het in, zodat het in ieder geval aan staat.[66] Sinds 2010 zijn er op dit punt geen nieuwe RFC's verschenen, behalve in 2019 RFC 8622, die voorstelde om bepaald verkeer een expliciete lage inspanningsclassificatie te geven, het tegenovergestelde van hoge prioriteit. Als een verbinding vol zit, dan is dat het eerste verkeer dat weggegooid kan worden.

Voor videostreaming is een alternatief om gebruik te maken van multicast. Het idee is dat 1 stream (bijvoorbeeld een tv-kanaal) naar een locatie wordt verzonden en dat meerdere clients de stream bekijken. Dit bespaart capaciteit in de kern van het netwerk. Multicast wordt onder andere door KPN gebruikt voor de distributie van haar IPTV-signaal naar de set-top boxen van haar klanten. In theorie bespaard deze wijze van distributie veel bandbreedte, omdat in plaats van 100x een stream te versturen er nu maar 1x een stream hoeft te worden verstuurd en de laatste router deze over 100 gebruikers verdeeld.

Pro/con

+ Incrementele oplossingen zoals DiffServ/DSCP helpen soms om de gevolgen voor de gebruiker op te lossen, zoals een download die een video call in de weg zit. Het effect is vooral nuttig op de "last mile" of in het lokale netwerk.

- Kritiek op QoS is vooral dat het in de praktijk te weinig oplevert. Als een verbinding vol zit, dan moet deze worden opgewaardeerd. Met de groei van piekverbruik op netwerken van enkele tientallen procenten per jaar kan QoS maar een beperkte tijd succesvol functioneren, voordat de lijn te vol zit.
- Multicast technieken zijn voor IPTV wel toegepast, maar nu consumenten op steeds meer apparaten en ook vaker uitgesteld kijken, wordt de efficiëntie ervan steeds beperkter. Met steeds meer content aanbieders, televisiekanalen en concurrerende vormen van gebruik van het netwerk, zoals gaming, is de kans dat een groot aantal gebruikers naar hetzelfde "kanaal" kijken steeds kleiner. Multicast is dan een extra complexiteit voor wat in de praktijk toch één stream voor één klant blijkt te zijn. Een lokale cache van bijvoorbeeld Netflix vervult een vergelijkbare rol, maar vereist geen specifieke configuratie van het netwerk.
- Multicast (over meerdere netwerken heen) maakt de afrekening met de rechthebbende ingewikkelder. Tv-platforms die streams individueel naar gebruikers sturen, kunnen exact aangeven hoeveel streams zij versturen en op basis daarvan de rechten betalen. Met multicast heeft het platform deze informatie niet.
- QoS verhoogd de complexiteit. VoLTE in mobiele netwerken is een goed voorbeeld: doordat de 4G VoLTE specificatie ervan uitgaat dat QoS nodig is voor VoLTE moeten alle implementaties er rekening mee houden, terwijl de implementatie niet uniform is over verschillende netwerken, fabrikanten en telecomaanbieders. VoWifi dat dezelfde techniek gebruikt voor telefonie en met dezelfde servers contact heeft werkt ook goed, maar heeft geen QoS omdat er te veel wifi-netwerken zijn om afspraken mee te maken.

[66] Deze blog van Cato networks uit 2021 geeft een voorbeelden hoe DiffServ mogelijk wel aan staat, maar het netwerk van haar klant er geen gebruik van maakt en de klant dat niet bemerkt. https://www.catonetworks.com/blog/voip-diffserv-and-qos-dont-be-held-captive-by-old-school-networking/

Betrokken gremia

- 3GPP: QoS speelt nog steeds een rol in discussies over nieuwe netwerken, zoals 5G. Een nieuwe variant hiervan is slicing (allocatie van capaciteit in een radionetwerk voor een klantengroep of applicatie).
- IETF: DiffServ is een RFC, maar er lijkt weinig nieuw werk te zijn aan QoS in de IETF.

Kansrijk

Het waarborgen van QoS garanties op geïnterconnecteerde netwerken lijkt steeds minder noodzakelijk, en dus – hoewel dit paradoxaal lijkt – zijn oplossingen die QoS garanties waarborgen steeds minder kansrijk. Er is in toenemende mate voldoende capaciteit. Toepassingen als videoconferencing, telefonie en real time gaming zijn meestal mogelijk op bestaande netwerken zonder QoS. Piekverbruik per abonnee is rond de 2mbps rond 's avonds negen uur, waarvan een groot deel wordt afgehandeld via lokale caches van diensten als Netflix en Youtube. Bij elkaar opgeteld zijn dat vele terabits/s aan data, maar verdeeld over het netwerk en daarmee niet in concurrentie met andere toepassingen. Bovendien is een QoS oplossing over verschillende netwerken heen lastig te implementeren: als iedere applicatie zelf zijn prioriteit aan kan geven, wat weerhoudt applicaties er dan van om altijd de maximale prioriteit te eisen?

6.3 Radicale oplossingen

Naast de genoemde incrementele oplossingen zijn er initiatieven om een geheel nieuw internet te definiëren, dat fundamenteel anders werkt en daardoor (een deel van) de genoemde problemen niet kent. Dit zijn de eerdergenoemde "clean slate" voorstellen.

Deze voorstellen komen van een veelheid van initiatiefnemers: internetbedrijven, standaardisatieorganisaties en soms ook (vaak op de achtergrond) overheden. Vooral de recente "New IP" voorstellen vanuit China hebben geopolitieke vragen opgeroepen.

Veel van deze initiatieven werken al in een beperkte omgeving, bijvoorbeeld in een test bed van één of enkele onderzoeksinstellingen. De bekendste initiatieven, die uitgebreider zijn beschreven in paragraaf 5.1, zijn:

- RINA (Recursive InterNetwork Architecture): een alternatieve set van internetprotocollen die veel van de complexiteit van het huidige internet vermijdt (zie ook 5.1.1).
- SCION (Scalability, Control, Isolation on Next-generation Networks): een "clean slate" benadering die het internet op zou delen in "isolation domains" (ISD's), met gevalideerde routes tussen deze ISD's (zie ook 5.1.2).
- Een initiatief van de ITU-T om het internet te vernieuwen door meer aandacht voor QoS in de protocollensuite (zie ook 5.1.3).
- Named Data Networking: een initiatief waarbij niet apparatuur, maar gegevens en diensten via het netwerk geadresseerd worden, ongeacht waar de gegevens zich bevinden (zie ook 5.1.4).
- New IP: een voorstel om een nieuwe set internetprotocollen te definiëren dat meerdere adresschema's parallel kan gebruiken (in plaats van alleen IPv4 en IPv6), waaronder adressen voor heterogene netwerken en voor diensten/inhoud. In dit model zouden

routers tussen netwerken de authenticiteit van pakketten moeten borgen, wat tot kritiek geleid heeft omdat dit de mogelijkheid openzet voor een overheid om onwelgevallige bronnen te blokkeren (zie ook 5.1.5).

In de verschillende interviews werden met name SCION en RINA veel specifiek benoemd, de andere initiatieven meer algemeen.

In tegenstelling tot de eerdergenoemde incrementele oplossingen, wordt de discussie over deze radicale oplossingen meestal niet in de gebruikelijke gremia (IETF en 3GPP) gevoerd, maar juist op andere plaatsen. New IP is bijvoorbeeld bij de ITU-T voorgesteld; andere initiatieven spelen zich vooral af binnen en tussen onderzoeksinstituten. Deze concepten worden in de gebruikelijke gremia in het algemeen niet als serieus alternatief gezien, waardoor de initiatiefnemers op zoek gaan naar andere gremia voor hun ideeën.

6.3.1 SCION

Uit ons onderzoek bleek dat er grote verschillen van inzicht zijn over de haalbaarheid en de voordelen van SCION. Er zijn voorstanders die denken dat het significante problemen oplost in het huidige internet, vooral ten aanzien van de veiligheid van routering. Vanuit betrokkenen bij andere (incrementele) ontwikkelingen rond beveiliging van routering klinkt juist dat de probleemanalyse van SCION niet correct is, en dat het daarom oplossingen als RPKI verkeerd inschat.

Een ander kritiekpunt is dat SCION in principe uitgaat van closed user groups waar een gebruiker lid van wordt, wat ervoor zou moeten zorgen dat alleen geautoriseerde partijen contact met elkaar kunnen leggen. Dat vereist dat vooraf bekend is wie met wie contact mag leggen en onder welke voorwaarden. Ook moeten de clients de routering aangeven in het packet, waardoor ze de staat van het netwerk en storingen of wijzigingen daarin moeten kennen en bijhouden. Dit lijkt complex, want het is moeilijk te voorspellen welke netwerken, diensten, gebruikers etc. met elkaar verbinding willen hebben. Een klant van een bank zal mogelijk ook op zakenreis in het buitenland toegang moeten hebben. In bestaande netwerken zijn er al mogelijkheden met vergelijkbare functionaliteit ten aanzien van afgeschermde groepen en controle over de routering van verkeer. Tussen groepen zakelijke gebruikers bestaan er besloten netwerken waarin de routering bekend is, maar daar worden nu separate glasvezels, MPLS-verbindingen, Ethernet VLANs en dergelijke voor gebruikt. Het is onduidelijk of SCION hier voldoende waarde aan toevoegt.

SCION werkt aan “overlay” mechanismen, waarbij SCION-netwerken deel kunnen worden van het bestaande internet. Daarbij vallen de voordelen van SCION echter grotendeels weg, waardoor ook deze aanpak naar onze mening niet kansrijk is als geleidelijke vervanging voor het internet.

6.3.2 RINA

Ook het enthousiasme voor de RINA lijkt tot nu toe beperkt. Discussies op mailinglists en reflecties van ontwikkelaars van RINA-implementaties[67] laten zien dat er een verschil in perspectief is ten aanzien van de praktische bruikbaarheid van de ideeën. Het idee van interprocess communicatie mag conceptueel wel eenvoudig zijn, de schaalbaarheid ervan is complex. Om de IPC te vinden die kan doen wat de applicatie wil doen, of de communicatie IPC van een andere gebruiker om een videoverbinding op te zetten vergt een veelheid van "kennis" over de staat van andere IPC's die nodig zijn (van tussenliggende nodes, gebruikte technieken, beveiliging, autorisatie etc.). IPC's moeten deze informatie verzamelen, bijhouden, verwijderen en optimaliseren met miljarden gebruikers, apparaten, diensten, processen en toepassingen. Dit is veel complexer dan het initieel lijkt.

6.3.3 Onze opvatting over "clean slate" architecturen

Hoewel elk van de genoemde initiatieven poogt om oplossingen voor meerdere van de genoemde vraagstukken te leveren, is het op dit moment nog niet duidelijk dat de architecturen schaalbaar genoeg zijn om wereldwijd een serieuze rol te spelen.

Zelfs al zou de schaalbaarheid echter geborgd zijn, kunnen deze en andere initiatieven naar onze mening het bestaande internet niet vervangen; in elk geval is het zeer onwaarschijnlijk dat dit in de komende decennia zal gebeuren. De "installed base" is daarvoor simpelweg te groot. Dat is ook meteen het grote verschil met de implementatie van het internet, wat destijds ook een "radicale" verandering was: de installed base was toen zo klein, en zo gefragmenteerd, dat er ruimte was voor een nieuwe oplossing.

De trage implementatie van IPv6 (die veel makkelijker zou moeten zijn dan de implementatie van de genoemde alternatieven) laat goed zien hoe lastig het is om iets nieuws te introduceren, gegeven de huidige omvang van de installed base en het gebrek aan prikkels voor partijen om iets aan te passen. Om überhaupt een kans te maken moet een nieuwe architectuur incrementeel geïmplementeerd kunnen worden in delen van het bestaande internet, en daarbij direct tastbare voordelen opleveren voor alle betrokkenen. Dat lijkt bij deze initiatieven niet het geval te zijn.

De nieuwe initiatieven kunnen echter wel leiden tot eigen netwerken voor specifieke toepassingen of doelgroepen, die vanwege specifieke eisen geen gebruik willen maken van het publieke internet.

Daarnaast levert het onderzoek aan deze nieuwe netwerken veel kennis op; deze kennis wordt op diverse manieren ingezet om de bestaande netwerken te verbeteren.

[67] https://ouroboros.rocks/blog/2021/03/20/how-does-ouroboros-relate-to-rina-the-recursive-internetwork-architecture/#ouroboros-diverges-from-rina en mailinglists waar Stratix auteurs en proponenten van RINA, waaronder John Day actief op zijn.

7 Conclusies

Dit hoofdstuk geeft antwoord op de onderzoeksvragen, in veel gevallen door terug te verwijzen naar eerdere hoofdstukken waar de specifieke vragen werden behandeld.

7.1 Belangrijkste vraagstukken en gerelateerde waarden

Onderzoeksvraag 1: Welke actuele ontwikkelingen in de architectuur en standaardisatie van internet zijn van grote maatschappelijke relevantie (gegeven de scope)?

Onderzoeksvraag: 1a: Wat zijn de 10 belangrijkste vraagstukken als gevolg van deze ontwikkelingen en waarom (welke maatschappelijke waarden staan daarbij op het spel)?

"Belangrijk" is hier een subjectief begrip, maar op basis van interviews, de deskresearch en de input uit de workshop zijn wij tot de volgende "top tien" van vraagstukken binnen de gegeven scope van dit onderzoek gekomen:

1. BGP route hijacking (6.2.1)
2. IP-spoofing (6.2.2)
3. Traffic shaping/netneutraliteit (6.2.3)
4. Weinig zicht op ongewenste content (6.2.4)
5. Interceptie van de inhoud (6.2.5)
6. Interceptie van metagegevens (6.2.6)
7. Zeggenschap op verkeer (soevereiniteit) (6.2.7)
8. Innovatie, flexibiliteit en veranderbaarheid van de infrastructuur (6.2.8)
9. Gebrek aan mogelijkheden voor duurzaamheid (6.2.9)
10. Gebrek aan Quality of Service (6.2.10)

Bij de uitwerking van elk vraagstuk is kort aangegeven aan welke waarden deze raken. In sommige gevallen conflicteren deze waarden, waardoor er geen oplossing bestaat die aan alle waarden recht doet.

Een vraagstuk dat inherent met conflicterende waarden te maken heeft, is nummer 4 in de lijst (weinig zicht op ongewenste content):

De behoefte van overheden om bepaalde content te blokkeren, of er in elk geval zicht op te hebben (denk bijvoorbeeld aan kinderporno, aanzetten tot haat, of illegale distributie van auteursrechtelijk beschermde werken), is gebaseerd op algemeen erkende waarden zoals het recht van kinderen om beschermd te worden (in het geval van kinderporno), of het recht op genot van eigendom (auteursrechten). Tegelijkertijd conflicteert deze behoefte met andere waarden, zoals privacy.

Een extra complicatie daarbij is dat elk mechanisme dat een overheid in een democratische rechtstaat meer zicht op content geeft, met alle waarborgen die daarbij horen, net zo makkelijk door autocratische overheden gebruikt kan worden op manieren die conflicteren met de mensenrechten.

Los van de gebruikte protocollen en standaarden zal hier dus altijd een conflict tussen verschillende waarden bestaan. De regelmatig terugkerende discussies over het al dan niet inperken van encryptie[68] laten dit conflict duidelijk zien.

7.2 Ontwikkelingen in de standaardisatie

Onderzoeksvraag 1b1: Welke nationale en internationale gremia hebben momenteel invloed op deze vraagstukken?

Voor de lagen die in scope van de opdracht zijn worden de meeste vraagstukken en de meeste oplossingen besproken in de IETF, en (voor mobiele netwerken) in de 3GPP. De keuze hiervoor is vooral historisch: de IETF is als gevolg van het wereldwijde succes van TCP/IP verantwoordelijk voor definitie en onderhoud van de protocollen die de basis vormen van het internet. 3GPP is als gevolg van het wereldwijde succes van GSM en de opvolgers daarvan verantwoordelijk voor definitie en onderhoud van de protocollen die de basis vormen van internet via de mobiele netwerken. Daarnaast zijn er special interest groups in diverse vormen die zelf niet de standaarden vaststellen, maar die aan de discussie bijdragen door beter zicht te geven op problematiek en mogelijke oplossingen (zie 3.1.7). NLnet Labs en Internet Society zijn hier voorbeelden van.

[…] en welke verschuivingen zijn er in de invloed die deze gremia uitoefenen?

Er zijn geen grote veranderingen gaande met betrekking tot de structuur en de processen bij IETF en 3GPP. Wel is zichtbaar dat de samenstelling verschuift, waarbij marktpartijen uit landen als China een grotere rol gaan spelen dan voorheen. Dat wil echter niet zeggen dat deze landen nu een dominantie invloed hebben; de (stakeholders uit) "westerse" landen hebben gezamenlijk nog duidelijk de meeste invloed.

Binnen IETF is wel zichtbaar dat de invloed van de grote platform bedrijven zoals Google steeds groter wordt. Het multi-stakeholdermodel werkt nog steeds goed, al is er een risico dat deze grote bedrijven zoveel invloed gaan krijgen dat zij de standaarden naar hun hand kunnen zetten, ook omdat deze partijen veelal over vele functionele lagen en met functionaliteit aan beide kanten van interfaces opereren. QUIC is een goed voorbeeld van een standaard die voornamelijk vanuit Google kwam, maar waarbij door tegenwicht vanuit andere deelnemers uiteindelijk een versie is vastgesteld die voor de meeste partijen acceptabel was.

Hoe en waar wordt bepaald welke activiteiten elk gremium oppakt?

Elk gremium bepaalt zelf welke activiteiten het oppakt, en blijft daarbij meestal bij zijn oorspronkelijke missie. Er is echter wel een tendens dat partijen die hun voorstellen in de betreffende gremia niet geaccepteerd krijgen, overgaan op "forum shopping", door die voorstellen bij andere gremia in te brengen. Een voorstel dat het in IETF of 3GPP niet haalt wordt dan bijvoorbeeld bij ETSI of bij de ITU ingebracht. Dit is onder andere gebeurd met "ETSI TLS"

[68] Zie bijvoorbeeld https://www.rijksoverheid.nl/documenten/kamerstukken/2021/03/09/antwoorden-kamervragen-over-het-verzwakken-van-encryptie-door-de-minister-van-justitie-en-veiligheid

(eTLS) en met "New IP". Vooralsnog heeft dit niet geleid tot grootschalige implementatie van deze alternatieve voorstellen, en het ligt ook niet voor de hand dat dit snel zal gebeuren.

7.3 Technische oplossingen

Onderzoeksvraag 2: Welke technische oplossingen (in het kader van vraag 1a) worden voorgesteld vanuit de verschillende werelddelen en instanties (gegeven de scope)?

Er zijn voor de genoemde vraagstukken zowel incrementele oplossingen (kleine wijzigingen aan bestaande protocollen, of nieuwe protocollen die de bestaande aanvullen) als radicale oplossingen ("clean slate" internet ontwerpen).

De voorgestelde incrementele oplossingen zijn per vraagstuk beschreven in paragraaf 6.2.

Meer radicale voorgestelde oplossingen voor vernieuwing van het internet, waarbij de architectuur fundamenteel op de schop zou moeten, staan beschreven in paragraaf 6.3. Deze oplossingen adresseren steeds een aantal van de genoemde vraagstukken tegelijk.

Onderzoeksvraag 2a: Welke gremia (zie 1b) zijn bij elk van de oplossingen betrokken, en welke oplossingen zijn gremium-overstijgend?

Bij de incrementele oplossingen is in de meeste gevallen de IETF betrokken, en in sommige gevallen 3GPP (voor mobiel). Enkele oplossingen worden in andere gremia zoals ETSI besproken. Vraagstukken die inherent aan maatschappelijke waarden raken (zoals "zicht op ongewenste content") zijn vaak gremium-overstijgend, maar de technische oplossing wordt uiteindelijk meestal in het meest relevante gremium besproken.

Onderzoeksvraag 2b: Wat zijn de voordelen en nadelen (bijvoorbeeld het risico van fragmentatie van het internet) van deze oplossingen, zowel vanuit de optiek van techniek als vanuit maatschappelijke waarden?

De belangrijkste voor- en nadelen van de voorgestelde oplossingen zijn benoemd in hoofdstuk 6. Geen van de incrementele oplossingen heeft grootschalige nadelen zoals fragmentatie van het internet, maar elke oplossing heeft technische nadelen die vaak weer nieuwe technische oplossingen nodig maken.

De radicale oplossingen hebben wel de mogelijkheid om tot een fragmentatie van het internet te leiden. De meeste van deze oplossingen zijn wel zo ontworpen dat nieuwe netwerken aan kunnen sluiten op het bestaande internet, maar dat gaat vaak ten koste van de voordelen van die nieuwe oplossingen.

[…] Hoe volwassen en kansrijk zijn deze oplossingen?

Over het algemeen kan gesteld worden dat de genoemde incrementele oplossingen volwassener en kansrijker zijn dan de voorstellen voor meer radicale oplossingen. Zelfs als de radicale oplossingen voldoende schaalbaar zouden zijn, en de problemen op zouden lossen waarvoor ze ontworpen zijn, dan nog is het implementeren van deze oplossingen als vervanging voor het internet door de grote "installed base" effectief niet haalbaar.

Om veiligheid, privacy, beschikbaarheid, en innovatie te garanderen hebben wij ook geen aanwijzing gevonden dat dit het beste bereikt zou kunnen worden door deze "clean slate architectures". Deze initiatieven kunnen wel leiden tot kleinschalige netwerken voor specifieke doelgroepen, en leveren in elk geval nieuwe kennis die nuttig is voor het ontwerpen van nieuwe aanpassingen in bestaande communicatienetwerken.

7.4 Rol van de Rijksoverheid

Onderzoeksvraag 1b2: Welke zijn de belangrijkste gremia voor de Rijksoverheid om in te participeren?

Zoals aangegeven in paragraaf 3.3 zou een directe participatie van overheden in het standaardisatieproces van de multi-stakeholder standaardisatielichamen de effectiviteit van het proces en het vertrouwen in standaarden kunnen ondermijnen. Dat wil niet zeggen dat de overheid niet moet participeren, maar wel dat zij zorgvuldig moet bepalen in welke gremia, op welke manier en met welk doel zij participeert.

De Nederlandse overheid kan in elk geval het standaardisatieproces beïnvloeden door betrokken te blijven bij de Nederlandse stakeholders die in het proces actief zijn, en daarbij haar beleidsdoelen indirect in te brengen.

Overheden oefenen ook op andere manieren indirecte invloed uit, door regulering (eisen die regulering aan netwerken stelt hebben invloed op standaarden), en door implementatie (overheden kunnen het goede voorbeeld geven en daardoor de implementatie van standaarden bevorderen, bijvoorbeeld via de "pas toe of leg uit" lijst van het Forum Standaardisatie).

Uiteraard moet de overheid wel participeren in de multilaterale gremia, aangezien er anders niemand is die de Nederlandse belangen in die gremia kan behartigen.

Daarnaast zijn er enkele (beperkte) gebieden waar de overheid de enige, of de belangrijkste gebruiker is. Voorbeelden daarvan zijn de standaardisatie van interfaces voor Legal Interception (aftappen) en de standaard voor digitale portofoonnetwerken op basis van TETRA (zoals C2000 in Nederland). In die gevallen moet de overheid wel participeren, om de stem van die gebruiker binnen de standaardisatie te laten horen. Beide genoemde discussies vinden voornamelijk binnen ETSI en 3GPP plaats.

[…] Staat het multi-stakeholder model zoals door RIPE, IANA, IETF wordt gebruikt onder druk?

Voor zover wij kunnen zien staat het multi-stakeholder model op dit moment niet onder druk, voor wat de internet en mobiele standaarden betreft. Pogingen van verschillende overheden om (eventueel via alternatieve gremia) invloed op het standaardisatieproces uit te oefenen hebben uiteindelijk niet of nauwelijks geleid tot daadwerkelijk wereldwijd geaccepteerde implementaties. De Nederlandse overheid kan hier aan bijdragen door zich in de multilaterale gremia actief te verzetten tegen dergelijke pogingen tot "forum shopping".

Annex A Literatuurlijst

Abbate, J (1999). Inventing the Internet. Inside Technology. Cambridge, MA: The MIT Press.

Abdelkafi, N., Bolla, R., Lanting, C. J., et al. (2019). Understanding ICT standardization: principles and practice.

Alvestrand, H. T. (2004). "RFC3935 - A Mission Statement for the IETF." RFC-Series. RFC Editor. https://tools.ietf.org/html/rfc3935.

Analysys Mason (Kende, M., Kvalbein, A., Allford, J., Abecassis, D.) (2021). Study On The Internet's Technical Success Factors. https://blog.apnic.net/wp-content/uploads/2021/12/MKGRA669-Report-for-APNIC-LACNIC-V3.pdf

Balzarova, M. A., en Castka, P. (2012). "Stakeholders' Influence and Contribution to Social Standards Development: The Case of Multiple Stakeholder Approach to ISO 26000 Development." Journal of Business Ethics 111, no. 2 : 265–79. https://doi.org/10.1007/s10551-012-1206-9.

Barrera, D. et al. (2017). "The SCION Internet Architecture", Communications of the ACM, Vol. 60, No. 6, June 2017, https://scion-architecture.net/pdf/2017-SCION-CACM.pdf

Braman, S. (2011). "The Framing Years: Policy Fundamentals in the Internet Design Process, 1969–1979." The Information Society 27 (5): 295–310. https://doi.org/10.1080/01972243.2011.607027

Baron, J., en Kanevskaia, O. (2021). "Global Competition for Leadership Positions in Standards Development Organizations." SSRN. https://doi.org/10.2139/ssrn.3818143.

Berg, S. V. (1989) "Technical Standards as Public Goods: Demand Incentives for Cooperative Behavior." Public Finance Quarterly 17, no. 1: 29–54. https://doi.org/10.1177/109114218901700102

Busch, L. (2011). Standards: Recipes for Reality. 0 edition. Cambridge, Mass: The MIT Press.

Caeiro, C., Jones, K. en Taylor, E. (2021) "Technical Standards and Human Rights: The case of New IP" Oxford Information Labs (preprint)

Carey, J. W. (1983). Technology and ideology: The case of the telegraph. Prospects, 8, 303-325.

Cath, C. (2019). "Internet Governance and Human Rights: A Literature Review." In The 2018 Yearbook of the Digital Ethics Lab, edited by Carl Öhman and David Watson, 105–32. Digital Ethics Lab Yearbook. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-17152-0_8

Cath, C. (2021). "The Technology We Choose to Create: Human Rights Advocacy in the Internet Engineering Task Force." Telecommunications Policy 45 (6): 102144. https://doi.org/10.1016/j.telpol.2021.102144

Cohen, J. E. (2019). Between Truth and Power: The Legal Constructions of Informational Capitalism. Oxford University Press.

Cowan, R., & Gunby, P. (1996). Sprayed to death: path dependence, lock-in and pest control strategies. The economic journal, 106(436), 521-542.

DeNardis, L. (2009). Protocol Politics: The Globalization of Internet Governance. Cambridge, MA: MIT Press.

DeNardis, L. (2014). The Global War For Internet Governance. Yale University Press.

Easterling, K. (2014). Extrastatecraft: The Power of Infrastructure Space. Verso Books.

Elkins, N. (2018). Human Rights Considerations of Internet Filtering, draft-elkins-hrpc-ifilter-00. https://www.ietf.org/archive/id/draft-elkins-hrpc-ifilter-00.txt

Erskine, T. en Carr, M (2016). "Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace." International Cyber Norms: Legal, Policy & Industry Perspectives, NATO CCD COE Publications.

EU Commission. (2020). Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade. JOIN (2020), 18.

Grasa, E. (2019). Next Generation Protocols (NGP); An example of a non-IP network protocol architecture based on RINA design principles. ETSI GR NGP 009 V1.1.1, Feb 2019, Chapters 4 and 5. https://www.etsi.org/deliver/etsi_gr/NGP/001_099/009/01.01.01_60/gr_NGP009v010101p.pdf

Huawei (2019). New IP: Shaping the Future Network. Contribution to ITU-T TSAG. https://www.itu.int/md/T17-TSAG-190923-TD-GEN-0598/en

Huston, G. (2021). Transport protocols and the network. https://blog.apnic.net/2021/05/11/transport-protocols-and-the-network/

Internet Society (2020). The Internet Way of Networking. Defining the critical properties of the Internet. https://www.internetsociety.org/wp-content/uploads/2020/09/IWN-IIAT-Defining-the-critical-properties-of-the-Internet.pdf

Isenberg, D. S. (1998). The dawn of the "stupid network". *NetWorker*, *2*(1), 24-31.

Kindleberger, C. P. (1986). International public goods without international government. The American economic review, 76(1), 1-13.

Koers, A. (2019) "Netneutraliteit en Network Slicing." UvA master scriptie

Lampland, M. en Star, S. L., eds. (2008). Standards and Their Stories: How Quantifying, Classifying, and Formalizing Practices Shape Everyday Life. 1st edition. Ithaca: Cornell University Press.

Leiner, B. M., Cerf, V. G. et al. (1997). A brief history of the Internet.

Lone, Q., Korczyński, M., Gañán, C., en van Eeten, M. (2020). SAVing the Internet: Explaining the Adoption of Source Address Validation by Internet Service Providers. In Workshop on the Economics of Information Security.

Mitchell, R.K., Agle, B.R., en Wood, D.J. (1997) "Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts", Academy of management review, pp. 853-886.

Morris, J. en Davidson, A. (2003). "Policy Impact Assessments: Considering the Public Interest in Internet Standards Development." In Proceedings of the 31st Research Conference on Communication, Information and Internet Policy (TPRC 2003). Washington DC. https://cdt.org/wp-content/uploads/publications/pia.pdf

Matzler, K, Strobl, A., Thurner, N. and Füller, J. (2015). "Switching Experience, Customer Satisfaction, and Switching Costs in the ICT Industry." Journal of Service Management.

NCSC (2019). ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS). https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls/ICT-beveiligingsrichtlijnen-voor-Transport-Layer-Security-v2.pdf

Odlyzko, A. (1998). 'Smart' and 'Stupid' networks: why the Internet is like Microsoft. *net-Worker*, *2*(5), 38-46.

Okuyama, F., Y., Bordini, R. H. and da Rocha Costa, A. C. (2011). "Situated Normative Infrastructures: The Normative Object Approach." Journal of Logic and Computation 23, no. 2: 397–424.

ten Oever, N. (2021a). "Norm Conflict in the Governance of Transnational and Distributed Infrastructures: The Case of Internet Routing." Globalizations, 1–17.

ten Oever, N. (2021b) "'This Is Not How We Imagined It' - Technological Affordances, Economic Drivers and the Internet Architecture Imaginary." New Media & Society 23, no. 2.

Pelman, L. (2020). Technical report on SS7 vulnerabilities and mitigation measures for digital financial services transactions, ITU. https://figi.itu.int/wp-content/uploads/2021/04/Technical-report-on-the-SS7-vulnerabilities-and-their-impact-on-DFS-transactions_f-1-1.pdf

Rogers, M., en Eden, G. (2017). "Digital Citizenship and Surveillance | The Snowden Disclosures, Technical Standards, and the Making of Surveillance Infrastructures." International Journal of Communication 11, no. 0: 22.

Russell, A. L. (2014). Open Standards and the Digital Age. Cambridge University Press.

Shapiro, C., en Varian H. R. (1998). Information Rules: A Strategic Guide to the Network Economy. Boston, Mass: Harvard Business Review Press.

Sriram, K., en Montgomery, D. C. (2019). Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation.

Sowell, J. H. (2012). "Empirical Studies of Bottom-up Internet Governance." In Proceedings of the 40th Research Conference on Communication, Information and Internet Policy (TPRC 2012). Washington DC.

Shin, D., Kim, H. en Hwang, J. (2015). "Standardization Revisited: A Critical Literature Review on Standards and Innovation." Computer Standards & Interfaces 38: 152–57.

Taylor, R. (2017). Making the Internet a Safer (and Better) Place for Children. https://blogs.lse.ac.uk/medialse/2017/12/05/making-the-internet-a-safer-and-better-place-for-children/

Viswanathan, S. (2005). "Competing across Technology-Differentiated Channels: The Impact of Network Externalities and Switching Costs." Management Science 51, no. 3: 483–96.

Voo, J. en Creemers, R. (2021). "China's Role in Digital Standards for Emerging Technologies – Impacts on the Netherlands and Europe." Leiden Asia Centre.

World Bank Group. (2016). World development report 2016: digital dividends. World Bank Publications.

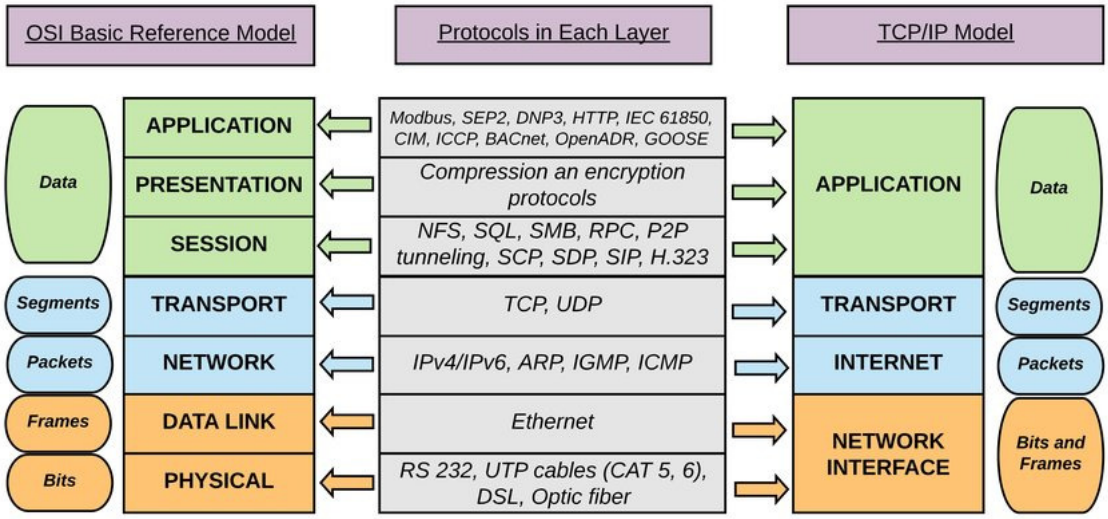
Yates, J. en Murphy, C. N. (2019). Engineering Rules: Global Standard Setting since 1880. JHU Press.

Zhang, L. et al. (2014). Named Data Networking. ACM SIGCOMM Computer Communication Review (CCR), July 2014. https://www.sigcomm.org/sites/default/files/ccr/papers/2014/July/0000000-0000010.pdf

Annex B OSI en TCP/IP lagenmodellen

De uitvraag van het Agentschap Telecom baseerde zich op de indeling in lagen zoals gebruikt in RFC1122. De opdracht is om alleen naar de internet- en transportlagen te kijken, en niet naar de standaardisatie ten aanzien van onderliggende en bovenliggende lagen. Dit betekent dat er niet gekeken wordt naar hoe wifi, of glasvezelkabels worden gestandaardiseerd of naar de specificatie van HTML, besturingssystemen of browsers.

Voor de lezer die niet goed bekend is met de lagen en de terminologie volgt een korte uitleg.



Figuur 10: A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/The-logical-mapping-between-OSI-basic-reference-model-and-the-TCP-IP-stack_fig2_327483011 [opgehaald op 26 nov 2021]

Het TCP/IP model is een schematische weergave van hoe een communicatieprotocollen werken en geeft een logische afbakening, ingedeeld in vier lagen.

Een ander model dat gebruikelijk is, is die van het zogenaamde OSI-lagen model, wat nog steeds veel wordt aangehaald door wetenschappers en beheerders van netwerken.[69] Het OSI model kent zeven lagen, die van beneden naar boven worden geteld.[70] Elk van de bovenliggende lagen stelt eisen aan de onderliggende lagen, bijvoorbeeld aan de capaciteit en de betrouwbaarheid van elke laag.

[69] Netwerkbeheerders, wetenschappers en soms zelfs beleidsmakers gebruiken deze lagen vaak als aanduiding, bv "ik heb een laag 2 verbinding nodig tussen Amsterdam en Rotterdam" (als diegene een verbinding nodig heeft zonder routers ertussen) of "de aftapverplichting richt zich vooral op laag 3 aanbieders." (deze regels rond aftappen betreffen vooral ISP's en niet de dienstverleners over het internet, of de eigenaar van het onderliggende netwerk)

[70] A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/The-logical-mapping-between-OSI-basic-reference-model-and-the-TCP-IP-stack_fig2_327483011 [accessed 26 Nov, 2021]

Laag 1 is het fysieke medium en de eisen die daaraan worden gesteld, het soort kabel of een specifiek deel van het spectrum. De specificatie hiervan vindt voor glasvezel bijvoorbeeld plaats in de ITU, waar gespecificeerd wordt aan welke eisen een glasvezelkabel moet voldoen voor bepaalde classificaties, bv ten aanzien van dikte, brekingsindexen etc. Laag 2 is een lokaal netwerkprotocol tussen apparaten in een netwerk, zoals ethernet, wifi, GSM, LTE, Docsis etc. Het zegt hoe een signaal wordt gemoduleerd, met welk vermogen, hoe apparaten worden geïdentificeerd (bv MAC-adres etc.) Deze twee lagen zijn buiten scope voor dit onderzoek, maar soms wordt er wel naar verwezen. Dit onderzoek richt zich vooral op laag 3 (en 4) de netwerk (en de transport) laag. Op deze laag zit het IP-protocol met de IP-adressen.

De internet laag, laag 3, was de innovatie die het mogelijk maakte om een wereldwijd netwerk te bouwen uit netwerken van verschillende thuisnetwerken, bedrijven, dienstverleners en telecombedrijven. Het is belangrijk om te vermelden dat het Internet Protocol de uiteindelijk succesvolle invulling geworden is van die laag, maar dat er veel voorstellen voor een invulling van deze laag geweest zijn. Het is de laag die het mogelijk maakt om verschillende soorten fysieke netwerken en op basis van verschillende protocollen met elkaar te laten samen werken en er geïnterconnecteerde netwerken van te maken. Het abstraheert onderliggende techniek, of het glasvezel is, mobiel of satelliet en het laat het er voor de bovenliggende lagen, de applicaties, uit zien alsof het een uniform netwerk is. Zonder een dergelijke abstractie zou het nodig zijn om een vertaling te maken van bv ethernet, naar satelliet, naar 4G, naar wifi en weer terug. Een ontwikkelaar van videoconferencing moet dan rekening houden met iedere vertaling en de mogelijke problemen die dat kan geven.

Het OSI-model hanteert laag 5, 6 en 7 (sessie, presentatie en applicatie), die in het internetmodel samengevoegd zijn tot de applicatielaag. Op deze laag zitten de toepassingen. Dit kunnen specifieke toepassingen zijn, zoals een game of een videoconferencing applicatie, waarbij de applicatie zelf interacteert met de transportlaag. Soms werken deze toepassingen vanuit een browser over HTML, en handelt de browser de interacties met de onderliggende lagen af. Hierin is heel veel flexibiliteit.

Figuur 11: OSI-stack + twee extra lagen: financial en political

In het kader van dit rapport is het belangrijk te onderkennen dat de lagen theoretische modellen zijn en niet harde kaders. Het is niet voor niets dat Evi Nemeth al in de jaren 80 twee lagen toevoegde aan het model, een financiële laag en een politieke laag. De onderliggende lagen creëren de parameters waarop de businessmodellen en de politieke context (zowel in standaardisatieorganisaties als door regulering van overheden) werken. De economische en politieke realiteit bepalen deels ook weer hoe de protocollen op de lagere lagen worden ontwikkeld in de standaardisatieorganisaties.

Annex C De ontwerpprincipes uit RFC 1958, kort samengevat

Algemene ontwerp issues

- Heterogeniteit is onvermijdelijk en moet door het design worden ondersteund.
- Als er meerdere manieren zijn om hetzelfde te doen: kies één manier, probeer duplicatie van functionaliteit te voorkomen
- Schaalbaarheid is essentieel
- Performance en kosten zijn belangrijke overwegingen
- Kies altijd de simpelste oplossing
- Modulariteit is goed. Regel zaken apart van elkaar waar mogelijk.
- Wacht niet op de perfecte oplossing maar pas de bijna complete oplossing toe.
- Vermijdt opties en parameters waar mogelijk
- Wees strikt bij het zenden van informatie en tolerant bij het ontvangen en accepteren ervan. Zend alleen foutmeldingen terug als het echt nodig is.
- Wees spaarzaam met verzenden van ongevraagde pakketten.
- Vermijdt circulaire afhankelijkheden (voorbeeld: routering zou niet af moeten hangen van DNS lookups die zelf weer afhankelijk zijn van goede routering)
- Objecten moeten zo veel mogelijk zelf beschrijvend zijn. Waar codes noodzakelijk zijn, gebruik alleen die van de IANA.
- Alle specificaties moeten dezelfde terminologie, notatie en bit en byte volgorde gebruiken
- Er is pas een standaard als er meerdere (verschillende) gecodeerde en werkende oplossingen zijn die samenwerken.

Naam en adres issues

- Vermijdt ontwerpen waarbij apparatuur een vast adres heeft. Applicaties gebruiken bij voorkeur namen in plaats van adressen
- Een eenduidige naamgevingsstructuur moet worden gebruikt
- Publieke namen in niet-hoofdlettergevoelig ASCII-karakters
- Adressen moeten niet ambigu zijn (uniek binnen context en scope waar zij gebruikt worden)
- Hogere lagen protocollen moeten eindpunten duidelijk kunnen identificeren (adres mag bijvoorbeeld niet wijzigen tijdens een transmissie)

Externe issues

- Prefereer ongepatenteerde technologie (tenzij tegen redelijke voorwaarden)
- Alle benodigde technologie moet in principe in alle landen geproduceerd kunnen worden. Export regulering kan hoogstens een secundaire rol spelen
- Implementaties die niet aan alle eisen voldoet kunnen niet conformiteit met de standaard claimen
- Ontwerpen moeten internationaal gebruik ondersteunen (o.a. ondersteuning verschillende karaktersets)

Vertrouwelijkheid en authenticatie

- Alle ontwerpen moeten passen in de IP-security architectuur
- Bewaking van privacy en authenticiteit is wenselijk maar geen architectuur eis: confidentialiteit en authenticatie is de verantwoordelijkheid van eindgebruikers en door hen gebruikte (end-to-end) protocollen en moet niet afhangen van de netwerklaag als drager van de informatie.
- Waar cryptografische algoritmen worden gebruikt moet altijd de mogelijkheid worden gegeven om een alternatief algoritme te kunnen gebruiken. Dergelijke algoritmen dienen expliciet te worden gelabeld met een IANA label.
- Er moet een manier zijn voor eindpunten om te onderhandelen welk gezamenlijk algoritme gebruikt wordt om een veilige verbinding op te zetten.

Annex D Universele verklaring van de rechten van de mens, kort samengevat

Mensenrechten zijn een plicht van iedereen: regering, individu of maatschappelijk orgaan.

1. Iedereen wordt vrij en met gelijke rechten geboren.
2. De mensenrechten gelden voor wie je maar bent, waar je ook bent.
3. Je hebt recht op leven, vrijheid en veiligheid.
4. Slavernij is verboden.
5. Martelen is verboden.
6. Je hebt het recht op erkenning voor de wet.
7. De wet is voor iedereen gelijk.
8. Als je onrecht is aangedaan, moet je rechtsbescherming krijgen.
9. Je mag niet zomaar worden opgesloten, of het land uitgezet.
10. Je hebt recht op een eerlijke en openbare rechtszaak met een onafhankelijke rechter.
11. Je bent onschuldig tot het tegendeel is bewezen.
12. Je hebt recht op privacy en op bescherming van je goede naam.
13. Je mag je vrij verplaatsen in je eigen land. Je mag ieder land (ook je eigen) verlaten.
14. Als je mensenrechten bedreigd worden, mag je in een ander land asiel vragen.
15. Je hebt recht op een nationaliteit.
16. Je mag trouwen met wie je wilt en een gezin stichten.
17. Je hebt recht op bezit, dat mag niemand zomaar van je afnemen.
18. Je mag je eigen godsdienst of overtuiging kiezen en daarnaar leven.
19. Je mag uitkomen voor je mening en je mag overal informatie vandaan halen.
20. Je mag een vereniging oprichten, niemand mag je dwingen ergens lid van te worden.
21. Iedereen mag meedoen aan verkiezingen en zich verkiesbaar stellen.
22. Je hebt recht op maatschappelijke zekerheid.
23. Je hebt recht op werk naar keuze, met een eerlijk loon. Vakbonden zijn vrij.
24. Je hebt recht op rust, vrije tijd en betaalde vakantie.
25. Je hebt recht op voldoende inkomen, zo nodig moet de staat voor je zorgen.
26. Je hebt recht op onderwijs.
27. Je hebt recht om te genieten van kunst en cultuur. Cultuur moet worden beschermd.
28. Alle regeringen moeten ervoor zorgen dat de mensenrechten worden nageleefd.
29. De wetten en de democratie moeten de mensenrechten beschermen.
30. Niets van het bovenstaande mag misbruikt worden om de mensenrechten teniet te doen.

Bron: Amnesty International (https://www.amnesty.nl/encyclopedie/universele-verklaring-van-de-rechten-van-de-mens-uvrm-korte-versie)

Annex E Lijst geïnterviewden

- Adrian Scrase – is vanuit ETSI zeer betrokken geweest in het ontstaan van 3GPP en is de huidige CTO van ETSI. Ook vanuit die rol nog zeer betrokken bij 3GPP.
- Anders Jonsson – vanuit de Zweedse autoriteit voor post en telecom (PTS) betrokken bij de ITU tot en met 2018, als Head of Deputy Head of Delegation voor ITU-conferenties; vanaf 2019 als onafhankelijk adviseur.
- Benno Overeinder – Managing Director bij NLnet Labs. Verder actief in de IETF en DNS-oarc.
- Bert Hubert – oprichter van PowerDNS. Daarnaast betrokken geweest in standaardisatie bij onder andere de IETF en ETSI.
- Ian Brown – binnen de standaardisatie-wereld betrokken bij en bekend met onder andere de IETF, ETSI en ITU. Tevens veel betrokken geweest bij organisaties gericht op digitale burgerrechten.
- Job Snijders – is Principal Engineer bij Fastly. Daarnaast in verschillende rollen betrokken bij de IETF en RIPE.
- Lars Eggert – is de huidige voorzitter van de IETF en daarnaast Technical Director for Networking bij NetApp.
- Maarten Aertsen – werkt binnen het National Cyber Security Center (NCSC-NL). Volgt vanuit die hoedanigheid de IETF. Nationaal ook betrokken bij Forum Standaardisatie.
- Mehwish Ansari – momenteel Digital Program Officer bij ARTICLE 19. Houdt zich daar bezig met (digitale) mensenrechten. Actief in de ITU.
- Michael Kende – econoom, onder andere werkzaam bij APNIC en Analysys Mason. Tevens betrokken geweest bij de Internet Society, volgt de IETF.
- Mirja Kuehlewind – werkzaam bij het Ericsson Research Eurolab. Tevens voorzitter van de Internet Architecture Board binnen de IETF.
- Nicola Rustignoli – research assistent onder Adrian Perrig, bij de Network Security Group bij de ETH Zürich. Werkt daar aan SCION.
- Olaf Kolkman – staat aan het hoofd van de Internet Society. Daarnaast betrokken (geweest) bij NLnet Labs en de Internet Architecture Board van de IETF.
- Olivier Bringer – werkzaam bij de European Commission. Was daar ten tijde van het onderzoek Head of Unit van Next Generation Internet.
- Reinhard Scholl – de huidig Deputy tot he Director van de Telecomunnication Standardization Bureau (TSB) binnen de ITU. Hiervoor ook onder andere gewerkt binnen ETSI.
- Roland van Rijswijk – hoogleraar netwerkbeveiliging bij de Universiteit Twente. Werkt daarnaast bij NLnet Labs.

Annex F Vragenlijst interviews

Onderstaande vragenlijst diende als ondersteuning bij de interviews. Elk interview ging specifieker in op het specialisme van de geïnterviewde en op de vraagstukken die tijdens het gesprek naar boven kwamen.

Interview onderwerpen en vragen

A. Achtergrond geïnterviewde

1. Wat is uw achtergrond in standaardisatie?
2. Kunt u de verschillende standaardisatieorganisaties waar u ervaring mee hebt karakteriseren?
   a. Wat doen ze goed (en wat niet),
   b. hoe werken ze intern,
   c. werken ze zoals ze zeggen dat ze werken of is er een groot verschil tussen formeel en informeel?
   d. Hoe worden de standaarden in praktijk gebruikt door fabrikanten, operators, overheden etc.?
3. In hoeverre zijn de standaarden waar u bij betrokken was uiteindelijk geïmplementeerd in mainstream producten en gebruikt (en waarom)?
4. Welke problemen ziet u in de huidige en toekomstige geïnterconnecteerde netwerken en wat zijn de oplossingen die we moeten gebruiken? Welke waardes hanteert u bij de keuzes van de oplossing?

B. Essentiële internet standaarden en standaardisatieorganisaties

5. Wat zijn volgens u op dit moment de essentiële standaarden en standaardisatieorganisaties voor het geïnterconnecteerde netwerken?
   a. Welke geïnterconnecteerde netwerken ziet u als het belangrijkst in de wereld.
   b. Welke standaardisatie-organisaties en -ontwikkelingen ziet u als essentieel voor de toekomst van het internet en van mobiele netwerken?
   c. Welke rol spelen deze organisaties volgens u bij de ontwikkeling van geïnterconnecteerde netwerken?
   d. Zijn er opkomende organisaties, of innovatieve alternatieve manieren van standaardiseren die in de toekomst mogelijk belangrijk worden?
   e. Wat zijn de positieve elementen van de verschillende organisaties waar de anderen wat van kunnen leren?
6. Hoe zijn we tot de huidige toestand van internetstandaarden en 3GPP standaarden gekomen?
   a. Is dit het gevolg van overheidsbeleid, van economische druk van bedrijven, is het toeval?
   b. Wat is volgens u bepalend geweest voor de huidige situatie m.b.t. internet standaarden?
   c. Bent u blij met de huidige situatie m.b.t. internet standaarden?
   d. Wat kan (en/of moet) er verbeteren? Wat gaat er mis bij de huidige standaardisatie en implementatie van geïnterconnecteerde netwerken?

7. Hoe ziet u de interactie tussen de standaardisatieorganisaties? Werken ze goed samen? Gezonde concurrentie? Strijd? In hoeverre is er sprake van forum shopping?

C. Normen en waarden en andere uitgangspunten

8. Is het succes van internet en 3GPP standaarden te koppelen aan bepaalde achterliggende normen en waarden?
   a. Zo ja welke zijn dit (zie voor voorbeelden bijlage 1)?
   b. Zo nee waaraan is het succes dan te danken?
   c. In hoeverre kunnen 'normen en waarden' worden gestimuleerd of afgedwongen?
9. Hoe spelen normen en waarden een rol in standaardisatie en implementatie?
10. Welke achterliggende problemen of paradoxen zijn te onderscheiden? Denk bijvoorbeeld aan
    a. het bevorderen van privacy versus het tegengaan van terrorisme en kinderpornoverspreiding
    b. Bevorderen van concurrentie tussen marktpartijen vs marktpositie van de standaardiserende partijen
    c. De mate waarin ideeën in de standaard opgenomen worden, vs de implementeerbaarheid (rough consensus vs unanimiteit)
    d. Het ondersteunen (en wellicht zelfs bevorderen) van heterogeniteit en het bevorderen (of wellicht waarborgen) van homogeniteit
11. Ziet u geopolitieke verschillen en zo ja hoe werken die uit?

D. Moet het internetfundament anders en zo ja waarom?

12. Ziet u de huidige stand van zaken rond geïnterconnecteerde netwerken positief of negatief?
    a. Kunt u voorbeelden noemen wat volgens u goed gaat en niet goed gaat?
    b. Welke normen hanteert u voor de beoordeling?
13. Wat zijn volgens u de belangrijkste issues die moeten worden opgelost in nieuwe standaarden of updates van bestaande standaarden? Zie bijlage 2 voor voorbeelden van nieuwe standaarden, zoals RINA, SCION en ITU-T FG NET-2030.
14. Er zijn al veel voorstellen gedaan voor QoS, controleerbare routering, verbeterde security etc. in internetstandaarden, die niet zijn geïmplementeerd. Waarom is dat, is het idee niet goed of ligt het aan de omgeving die moet standaardiseren of implementeren?
15. Hoe ziet u bijvoorbeeld het uitblijven van de (volledige) implementatie van IPv6 in deze context?

E. Geopolitiek en bedrijfsbelangen

16. Welke zijn volgens u de belangrijkste stakeholders m.b.t. de basis inrichting van internet
    a. wat zijn hun belangen en achterliggende drijfveren
    b. welke (maatschappelijke) waarden zijn voor deze stakeholders belangrijk (m.b.t. de problemen genoemd in sectie D.)
    c. (hoe) zijn zij succesvol om hun belangen waarden via de standaarden te verankeren?
17. Zijn er stakeholders die uitgesloten worden?

   a. Wat zijn hiervan achtergronden en mechanismes?
18. Welke geopolitieke context ziet u en hoe belangrijk is deze?
19. Welke overheden spelen volgens u een grote rol?
20. Welke bedrijven spelen een grote rol? Zijn er verschillende groepen aan te wijzen, bv Telco vs Internet. In hoeverre spelen ze een rol bij de standaardisatie en implementatie
21. Bij de standaardisatie en implementatie van het QUIC-protocol, en van 5G, hoe ziet u die tegenstellingen tussen groepen, tussen normen en waarden etc. terugkomen?
22. Wat is uw perspectief op implementatie van standaarden?
   a. Denk bijvoorbeeld implementatie IPv6, BGP-security, VoLTE, QUIC, RPKI, DNSsec, opvolgende releases van 3GPP
   b. In hoeverre speelt de implementeerbaarheid een rol bij standaardisatie
   c. Hoe zorgen organisaties ervoor dat de standaarden ook uniform geïmplementeerd worden (running code, plugfests etc.)
23. Wat is de waarde van voorstellen voor een alternatief ("clean slate") internet, zoals SCION, RINA, "new IP", etc.

F. Lessons learned

24. Welke evoluties en revoluties in het oorspronkelijke internet ontwerp zijn succesvol gebleken en welke niet? Waarom?
   a. Waarom is de implementatie van IPv6 zo moeilijk gebleken?
   b. Wat zijn de ervaringen bij het implementeren van nieuwe internet standaarden, zoals Secure BGP vs RPKI/MANRS, of recente verbeteringen in DNS
25. Wat moeten we niet vergeten in deze analyse?

Annex G Verklarende woordenlijst

3G/4G/5G/6G	Generaties van mobiele telecomstandaarden
3GPP	Third Generation Partnership Program, standaardisatieorganisatie voor mobiele telecommunicatie
5G NR	5G “New Radio”, nieuwste generatie 3GPP radio standaard
AFRINIC	African Network Information Centre, Regional Internet Registry (RIR) voor de regio Afrika
AI	Artificial Intelligence
AMPS	Advanced Mobile Phone System, Amerikaanse standaard voor analoge mobiele telefonie
APNIC	Asia Pacific Network Information Centre, Regional Internet Registry (RIR) voor de regio Azië-Pacific
ARIB	Association of Radio Industries and Business, Japanse standaardisatieorganisatie
ARIN	American Registry for Internet Numbers, Regional Internet Registry (RIR) voor de regio Noord-Amerika
ARPAnet	Advanced Research Projects Agency Network, voorloper van het internet
AS	Autonomous System, deelnetwerk van het internet
ATIS	Alliance for Telecommunications Industry Solutions, Noord-Amerikaanse standaardisatieorganisatie
ATM	Asynchronous Transfer Mode, netwerkprotocol
BGP	Border Gateway Protocol, routeringsprotocol
BGPsec	Border Gateway Protocol Security, veiligheidsextensie voor BGP
CCSA	China Communications Standards Association, Chinese standaardisatieorganisatie
CDN	Content Delivery Network, verspreid netwerk van servers dat gebruikers in staat stelt sneller content binnen te halen.
CEN	European Committee for Standardisation, hierin participeren de Europese landelijke standaardisatieorganisaties
CENELEC	European Committee for Electrotechnical Standardisation, Europese standaardisatieorganisatie rond elektrotechniek
CEPT	European Conference of Postal and Telecommunications Administrations, Europese organisatie voor post en telecom
C-Netz	Funktelefonnetz-C, Duitse analoge mobiele telecomstandaard
Carrier Grade NAT	Mechanisme om IP-adressen te vertalen (NAT) op de schaal van een operator, in plaats van die van een huishouden of bedrijf.
CPU	Central Processing Unit, (computer)processor
DDoS	Distributed Denial of Service, aanval via veel verschillende apparaten een verzoek naar een servers sturen waardoor deze overbelast raakt
DECT	Digital Enhanced Cordless Telecommunications, telecomstandaard
De jure/de facto	De jure standaarden zijn formeel vastgesteld, de facto standaarden ontstaan in de markt (en kunnen later alsnog formeel worden gemaakt)
DIF	Distributed IPC Facility, groep van inter-proces communicatie, gebruikt in RINA
DNS	Domain Name System, netwerkprotocol om (onder andere) namen in IP-adressen om te zetten
DNSSEC	Domain Name System Security, veiligheidsextensie voor DNS
DoH	DNS over HTTPS, extensie voor DNS over een beveiligde verbinding
EC	European Commission
ECH	Encrypted Client Hello, veiligheidsstandaard

EFTA	European Free Trade Association, Europese Vrijhandelsorganisatie
Ethernet	Netwerkstandaard voor verbindingen op laag 2 (Link Layer, zie Figuur 1)
ETNO	European Telecommunications Network Operators association, vertegenwoordigt de Europese telecom operators (voormalige staatsbedrijven)
ETSI	European Telecommunication Standards Institute, standaardisatieorganisatie
GCHQ	Government Communications Headquarters, Britse inlichtingendienst
GSM	Global System for Mobile communications, telecomstandaard
GSMA	GSM Association, vertegenwoordigt mobiele telecom operators wereldwijd
HTML	HyperText Markup Language, opmaaktaal, voornamelijk bedoeld voor websites
HTTP/HTTPS	HyperText Transfer Protocol (Secure), protocol voor communicatie tussen een webclient en een webserver
IAB	Internet Architecture Board, organisatie die internetprotocollen en standaarden overziet
IANA	Internet Assigned Numbers Authority, organisatie die toplevel domeinen beheert
IAO	Internationale Arbeids Organisatie
ICANN	Internet Corporation for Assigned Names and Numbers, beheerdersorganisatie van het internet
IEEE	Institute of Electrical and Electronics Engineers, standaardisatieorganisatie
IETF	Internet Engineering Task Force, standaardisatieorganisatie
IMS	IP Multimedia Subsystem, gestandaardiseerde telecom infrastructuur
Installed base	Term voor de hoeveelheid bestaande installaties van een bepaald product
IoT	Internet of Things, totaal aan apparaten (zonder gebruikersinteractie) die via het internet met elkaar verbonden zijn
IPC	Inter-Process Communication, onderlinge communicatie tussen meerdere processen in een besturingssysteem
IPv6	Internet Protocol versie 6, internetprotocol
IRTF	Internet Research Task Force, organisatie die onderzoek naar het internet promoot en overziet
ISD	Isolated Domains, geïsoleerde domeinen, gebruikt binnen SCION
ISDN	Integrated Services Digital Network, groep telecom standaarden
ISO	International Organisation for Standardisation, internationale standaardisatieorganisatie
ISOC	Internet Society, internationale non-profit organisatie die zich bezighoudt met beleid, standaarden en ontwikkeling van het internet
ISP	Internet Service Provider
ITU	International Telecommunications Union, wereldwijde organisatie voor afspraken rond radio- en telecommunicatie
ITU-T	Onderdeel van de ITU voor telecommunicatie (waaronder standaardisatie)
LACNIC	Latin America and Caribbean Network Information Centre, Regional Internet Registry (RIR) voor midden- en Latijns-Amerika
LTE	Long Term Evolution, bekendste 4G mobiele telecomstandaard
MoU	Memorandum of Understanding
NAT	Network Address Translation, mechanisme om IP-adressen te vertalen waardoor hergebruik mogelijk is.
NCSC (GB)	National Cyber Security Centre, onderdeel van het Britse GCHQ
NCSC (NL)	Nationaal Cyber Security Centrum, onderdeel van het ministerie van J&V
NDN	Named Data Networking, project dat ernaar streeft de zwaktes van het huidige internet op te lossen
NEN	Nederlands Normalisatie-instituut/Nederlandse Norm, beschrijft normen

NIST	National Institute of Standards and Technology, wetenschappelijke instelling die zich onder andere inzet voor standaardisatie
NMT	Nordic Mobile Telephone, Scandinavische telecomstandaard
OESO	Organisatie voor Economische Samenwerking en Ontwikkeling, samenwerkingsverband van landen
OS	Operating System, besturingssysteem
OSI	Open Systems Interconnection model, gestandaardiseerd model voor datacommunicatie
PON	Passive Optical Network, glasvezelnetwerk bestaand uit passieve elementen
Ossificatie	Proces van verstarring, waarbij steeds moet worden doorgebouwd op bestaande protocollen
POP3	Post Office Protocol, e-mailprotocol, derde versie
PTI	Public Technical Identifiers, dochterbedrijf van ICAnn, beheerdersorganisatie
PTT	(Voormalige) staatsbedrijf voor Post, Telegrafie en Telefonie (niet alleen in Nederland; PTT is een generieke term voor een dergelijk staatsbedrijf in veel landen)
QoS	Quality of Service
QUIC	Transportlaag protocol
Radio2000	Franse telecomstandaard
RFC	Request for Comments, communicatievorm gebruikt door de IETF, onder andere voor internet standaarden
RINA	Recursive InterNetwork Architecture, initiatief voor een 'nieuw internet'
RIPE NCC	RIPE Network Coordination Centre, Regional Internet Registry (RIR) voor Europa en het Midden-Oosten
RIR	Regional Internet Registry, kent (onder andere) IP-adresblokken en nummers toe aan netwerken
Roaming	Gebruik maken van (mobiel) internet op andere netwerken dan het 'eigen' netwerk
Routing tables	Data die informatie over de topologie van het netwerk bevat en zodoende de 'route' van de data beschrijft
RPKI	Resource Public Key Infrastructure, manier om BGP-routing veiliger te maken
RTM	Italiaanse mobiele analoge telecomstandaard
SCION	Scalability, Control, and Isolation on Next-Generation Networks, initiatief voor een 'nieuw internet'
SDO's	Standaardisatieorganisaties
SG-13	Study Group-13, genummerde studiegroep binnen de ITU-T, met focus op nieuwe netwerkstandaarden
SIDN	Stichting Internet Domeinregistratie Nederland, beheert domeinnamen eindigend op .nl
SIP	Session Initiation Protocol, communicatieprotocol
Slicing	Opdelen van mobiele netwerkcapaciteit
SMTP	Simple Mail Transfer Protocol, e-mailstandaard
Spoofing	Vervalsen van (bepaalde kenmerken van) data
TCP	Transmission Control Protocol, internetprotocol op de transportlaag
TCP/IP	Reeks netwerkprotocollen die gebruikt worden voor netwerkcommunicatie, grondslag van onder andere het internet
TETRA	Terrestrial Trunked Radio, communicatiestandaard die vooral wordt gebruikt door politie en veiligheidsdiensten
TLS/eTLS	Transport Layer Security, encryptieprotocol
TMA	Spaanse mobiele analoge telecomstandaard

TSDSI	Telecommunications Standards Development Society India, standaardisatieorganisatie
TTA	Telecommunications Technology Association, Koreaanse standaardisatieorganisatie
TTC	Telecommunication Technology Committee, Japanse standaardisatieorganisatie
UDP	User Datagram Protocol, internetprotocol op de transportlaag
UMTS	Universal Mobile Telecommunications System, 3G mobiele telecomstandaard
Unix BSD	Berkeley Software Distribution, besturingssysteem
VoIP	Voice over IP, telefonie en andere spraak via internetprotocollen
VoLTE	Voice over LTE, spraak over 4G IP-gebaseerde netwerken
VoWifi	Voice over wifi, spraak over wifi
VPN	Virtual Private Network
W3C	World Wide Web Consortium, standaardisatieorganisatie
X.25	telecomprotocol

CONTACT

Stratix

Stratix B.V.
Villa Looverhoek - Julianalaan 1
1213 AP Hilversum

Telefoon:	+31.35.622 2020
E-mail:	office@stratix.nl
URL:	http://www.stratix.nl
Reg. no.:	57689326
IBAN:	NL85ABNA0513733922
BIC:	ABNANL2A
VAT:	NL8526.92.079.B.01