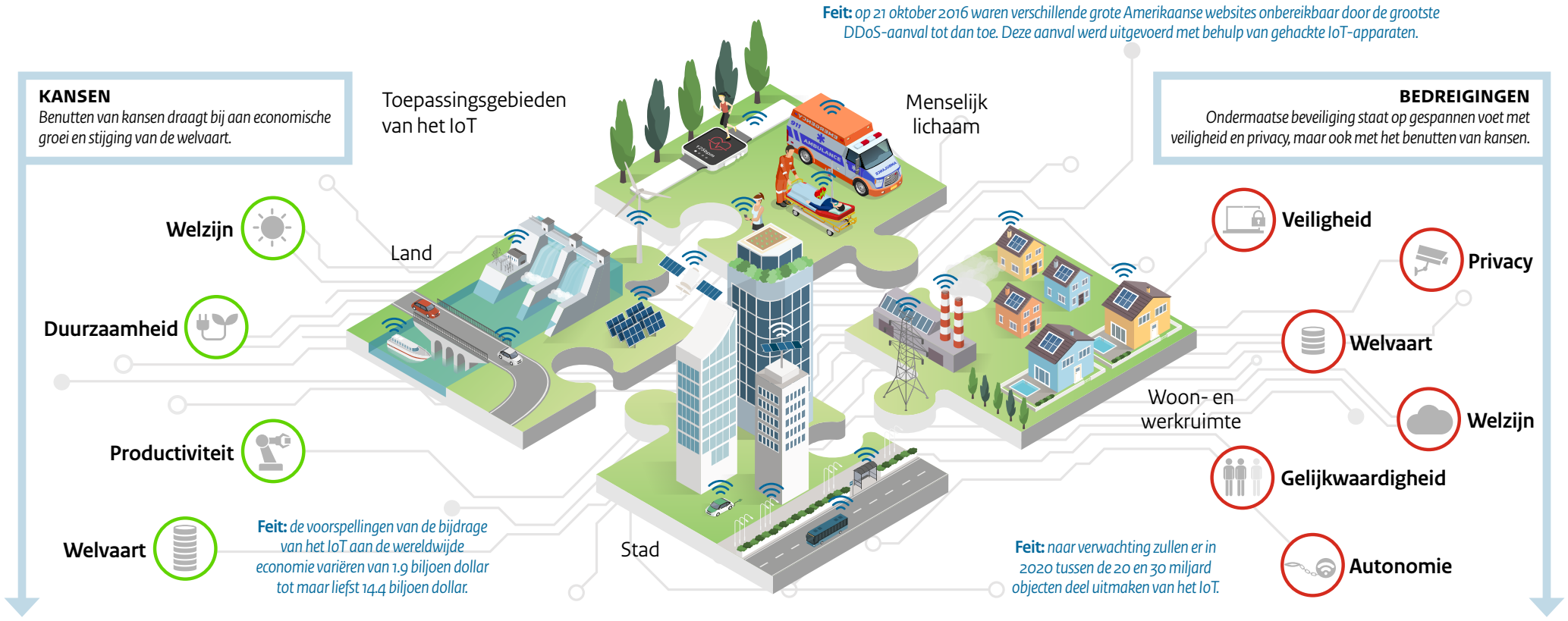
Het Internet of Things
kansen, bedreigingen en maatregelen

Wetenschappelijk Onderzoek- en Documentatiecentrum
Ministerie van Veiligheid en Justitie

Het Internet of Things (IoT) is een netwerk van 'slimme' apparaten, sensoren en andere objecten die met elkaar en met het internet verbonden zijn. Ze verzamelen gegevens over hun omgeving, kunnen die uitwisselen en op basis daarvan (semi)autonome beslissingen nemen en/of acties uitvoeren die van invloed zijn op de omgeving. Het IoT brengt zowel kansen als bedreigingen met zich mee. Het is van belang dat er nu maatregelen worden genomen zodat het IoT zo min mogelijk schade veroorzaakt en een positieve bijdrage kan leveren aan onze samenleving.



MAATREGELEN: GEEN ONE SIZE FITS ALL MAATREGEL, MAAR EEN COMBINATIE VAN:

1. Creëren van prikkels voor het bedrijfsleven en erop toezien dat de regelgeving gehandhaafd wordt.
2. Vergroten van kennis en bewustzijn door meer te investeren in onderwijs, om- en bijscholing, voorlichting en onderzoek.
3. Faciliteren van publiek-private en internationale samenwerking op basis van een gedragen IoT-overheidsvisie.
4. Benoemen van één hoofdverantwoordelijke die het geformuleerde overheidsbeleid stuurt en coördineert.

Bron *(Verkeerd) verbonden in een slimme samenleving. Het Internet of Things: kansen, bedreigingen en maatregelen (WODC 2017)*

Wetenschappelijk Onderzoek- en Documentatiecentrum
Ministerie van Veiligheid en Justitie

Cahier 2017-8

(Verkeerd) verbonden in een slimme samenleving

Het Internet of Things: kansen, bedreigingen en maatregelen

J.J. van Berkel
R.L.D. Pool
M. Harbers
J.J. Oerlemans
M.S. Bargh
S.W. van den Braak

TERUG

Cahier
De reeks Cahier omvat de rapporten van onderzoek dat door en in opdracht van het WODC is verricht.
Opname in de reeks betekent niet dat de inhoud van de rapporten het standpunt van de Minister van Veiligheid en Justitie weergeeft.

Alle rapporten van het WODC zijn gratis te downloaden van www.wodc.nl.

TERUG

Voorwoord

Moderne technologieën hebben de samenleving ingrijpend veranderd. Een samenleving zonder computers, smartphones en internet is nauwelijks nog denkbaar. De opkomst van het *Internet of Things* (IoT) maakt dat meer en meer alledaagse objecten met elkaar, en het internet, verbonden zullen worden. Het IoT heeft daardoor een steeds grotere invloed, zowel positief als negatief, op de manier waarop wij leven, werken en met elkaar omgaan.

Dit onderzoek, uitgevoerd in opdracht van de Cyber Security Raad, biedt hierop anticiperend een brede inventarisatie van de kansen en bedreigingen van het IoT voor onze maatschappij, op economisch, sociaal en technologisch gebied. Hierbij is tevens onderzocht welke factoren de succesvolle ontwikkeling van veilige en betrouwbare IoT-toepassingen belemmeren en welke maatregelen genomen kunnen worden om dit te ondervangen. Deze inventarisatie is gebaseerd op literatuuronderzoek en gesprekken met experts en stakeholders. Hierbij zijn eerdere, recent verschenen, onderzoeksrapporten op het gebied van digitalisering en cybersecurity van verschillende instituten meegenomen.

De resultaten van dit onderzoek laten zien dat het IoT tal van mogelijkheden biedt om onze levens aangenamer en makkelijker te maken. Op economisch gebied zijn er volop kansen om kosten te besparen en nieuwe verdienmodellen te ontwikkelen. De basis voor veel kansen is dat door het IoT grote hoeveelheden data beschikbaar komen. Het verzamelen en analyseren deze data kent echter ook een keerzijde, vooral met het oog op privacy en dataveiligheid. Onze toenemende afhankelijkheid van IoT-technologie maakt de samenleving daarnaast kwetsbaar voor nieuwe dreigingen: er kan schade of gevaar ontstaan door uitval of misbruik. Op dit moment is de beveiliging van veel IoT-toepassingen nog ondermaats. Recentelijk heeft een IoT-botnet er bijvoorbeeld voor gezorgd dat grote websites als Twitter, PayPal, Amazon en Netflix een tijdlang niet of nauwelijks te bereiken waren.

Het IoT kan een serieuze bedreiging vormen voor essentiële menselijke en publieke waarden: kwetsbaarheden kunnen onze economie, veiligheid en vrijheid in gevaar brengen. Het is daarom van belang dat er nu maatregelen worden genomen. Gebeurt er niets, dan kan een *verkeerd verbonden* IoT ingrijpende gevolgen hebben. Helaas bestaat er geen *one size fits all* oplossing die alle risico's in keer weg kan nemen. Daarom is er een integrale benadering nodig, waarin stakeholders samenwerken en samenhangende maatregelen genomen worden. Ook kennisontwikkeling en aanvullend (wetenschappelijk) onderzoek is hierbij van groot belang. Daarbij dient aandacht te zijn voor technische mogelijkheden (bijvoorbeeld om IoT-apparaten beter te beveiligen), maar ook voor de beleidsmatige context (bijvoorbeeld de effectiviteit van verschillende maatregelen) en voor gedragswetenschappelijke aspecten.

Het voorliggende onderzoek had niet afgerond kunnen worden zonder de waardevolle bijdrage van vele deskundigen. Mijn dank gaat, mede namens de auteurs, uit naar alle geïnterviewde personen en alle deelnemers van de rondetafelgesprekken. Bijzondere dank wil ik ook graag uitspreken aan de voorzitter en de leden van de begeleidingscommissie.

Prof. dr. Frans Leeuw
Directeur WODC

Inhoud

Samenvatting

Aanleiding, vraagstelling en scope

Het *Internet of Things* (IoT) is een netwerk van 'slimme' apparaten, sensoren en andere objecten die met elkaar en met het internet verbonden zijn. Nu al worden verschillende IoT-toepassingen veelvuldig gebruikt in onze samenleving en in de toekomst zal de adoptie van het IoT alleen nog maar verder toenemen. Het IoT biedt enerzijds kansen door nieuwe technologische mogelijkheden. Anderzijds brengt het ook bedreigingen met zich mee, bijvoorbeeld op het gebied van cybersecurity. Om de kansen van het IoT te benutten en de bedreigingen te minimaliseren moet hier tijdig op worden ingespeeld. Om deze reden heeft het WODC, in opdracht van de Cybersecurity Raad (CSR), een onderzoek uitgevoerd naar het IoT, de impact ervan op de maatschappij en de handelingsperspectieven van relevante stakeholders.

De centrale vraagstelling in dit onderzoek is: *Wat zijn de kansen en bedreigingen van het IoT en hoe kunnen verschillende stakeholders de ontwikkeling van het IoT in Nederland op een positieve manier beïnvloeden?* Om de centrale onderzoeksvraag te beantwoorden zijn de volgende deelvragen geformuleerd.

1 Wat behelst het IoT?
2 Welke kansen biedt het IoT?
3 Welke bedreigingen brengt het IoT met zich mee?
4 Wat zijn de maatregelen die verschillende stakeholders kunnen nemen om de kansen van het IoT te benutten en de bedreigingen ervan te beperken?

Dit onderzoek is een verkenning met als doelstelling een breed overzicht te geven van relevante vraagstukken op het gebied van het IoT, daardoor wordt per deelonderwerp slechts beperkt de diepte in gegaan.

Methodologie

De onderzoeksvragen zijn beantwoord aan de hand van een literatuurstudie, interviews en rondetafelgesprekken. Voor de literatuurstudie is gebruikgemaakt van wetenschappelijke literatuur, vakliteratuur en mediaberichten over het IoT. Naast de literatuurstudie zijn er in totaal zes interviews gehouden met experts en stakeholders uit relevante sectoren. Hiervoor is gebruikgemaakt van semigestructureerde vragenlijsten. Tot slot zijn er twee rondetafelgesprekken georganiseerd met de thema's *Smart City* en *Smart Industry*. Bij beide gesprekken waren verschillende experts en stakeholders op het gebied van het betreffende thema aanwezig.

De kansen en bedreigingen van het IoT zijn in kaart gebracht, beschreven en geanalyseerd aan de hand van menselijke waarden zoals privacy, veiligheid en duurzaamheid. Het uitgangspunt hierbij is dat technologie impact heeft op menselijke waarden, zowel positief als negatief. De belangrijkste waarden die door het IoT worden beïnvloed zijn bepaald op basis van de literatuur, interviews en rondetafelgesprekken. Op basis van deze waarden zijn de belangrijkste kansen en bedreigingen geïdentificeerd, die vervolgens als uitgangspunt hebben gediend voor het bepalen van mogelijke maatregelen.

Resultaten

Kenmerken

Het IoT behelst een netwerk van objecten (vaak verbonden met het internet), die gegevens verzamelen over hun omgeving, deze kunnen uitwisselen en op basis daarvan (semi)autonome beslissingen nemen en/of acties uitvoeren die van invloed zijn op de omgeving. De belangrijkste kenmerken van het IoT zijn: 1) communiceren, 2) waarnemen, 3) data analyseren, en 4) (semi)autonome acties uitvoeren. Het eerste kenmerk van het IoT is dat IoT-objecten met elkaar en vaak ook met het internet verbonden zijn, waardoor zij met elkaar kunnen communiceren en gegevens kunnen uitwisselen. Een tweede kenmerk van IoT-objecten is dat ze, door middel van sensoren, hun omgeving of interne toestand kunnen waarnemen. Hierbij kan bijvoorbeeld worden gedacht aan: geluid, temperatuur en (lucht)vochtigheid. Een derde kenmerk van het IoT is dat er grote hoeveelheden data verzameld en geanalyseerd worden. Enerzijds zijn dit data verzameld door de sensoren van het IoT-object zelf, anderzijds zijn dit data die door andere objecten zijn verzameld en verstuurd. Verschillende data-analysemethoden maken het mogelijk hieruit betekenisvolle, nieuwe informatie te deduceren. Het vierde kenmerk van het IoT is dat objecten acties kunnen uitvoeren die van invloed zijn op de omgeving of het object zelf, bijvoorbeeld door het zenden van geluid, licht of radiogolven. Deze acties kunnen handmatig worden geïnitieerd (door de gebruiker zelf), maar (in toenemende mate) kan het object ook autonoom beslissingen nemen en acties uitvoeren.

Kansen

De komst van het IoT biedt verschillende kansen. De basis voor veel kansen is dat door het IoT relevante (sensor)data steeds vaker snel en overal beschikbaar zijn. Door het combineren, analyseren en interpreteren van deze data, kunnen processen transparanter worden en kunnen nieuwe inzichten worden verkregen. Inzicht en transparantie kunnen bijdragen aan betere en weloverwogen beslissingen (zowel door overheden, bedrijven als burgers). Als gevolg hiervan kan het IoT een sterke positieve invloed hebben op de volgende waarden: welzijn, duurzaamheid, productiviteit en welvaart. Voor al deze kansen geldt dat ze kunnen bijdragen aan economische groei, het maken van winst of het behalen van kostenbesparingen. IoT-toepassingen op het gebied van welzijn kunnen bijvoorbeeld leiden tot kostenbesparing doordat ouderen langer thuis kunnen wonen of doordat zorgkosten dalen omdat gezondheid wordt verbeterd. Het ontwikkelen van duurzame IoT-toepassingen leidt tot nieuwe producten en diensten waarmee winst gemaakt kan worden.

Bedreigingen

De komst van het IoT brengt ook bedreigingen met zich mee. Het verzamelen van grote hoeveelheden data en het steeds meer inzetten van verbonden apparaten kan namelijk ook een negatief effect hebben op de volgende waarden: veiligheid, privacy, welvaart, welzijn, gelijkwaardigheid en autonomie. De meest urgente bedreigingen van het IoT worden gevormd door risico's op het gebied van veiligheid en privacy. Veiligheidsrisico's liggen onder meer op het gebied van cybercriminaliteit, zoals het inbreken in en overnemen van IoT-apparaten en het stelen van data. Daarnaast kunnen disfunctionerende IoT-apparaten veiligheidsrisico's met zich meebrengen. Bedreigingen op het gebied van privacy zijn het risico op privacyschending, bijvoorbeeld door het gebruik van (gevoelige) gegevens voor andere doel-

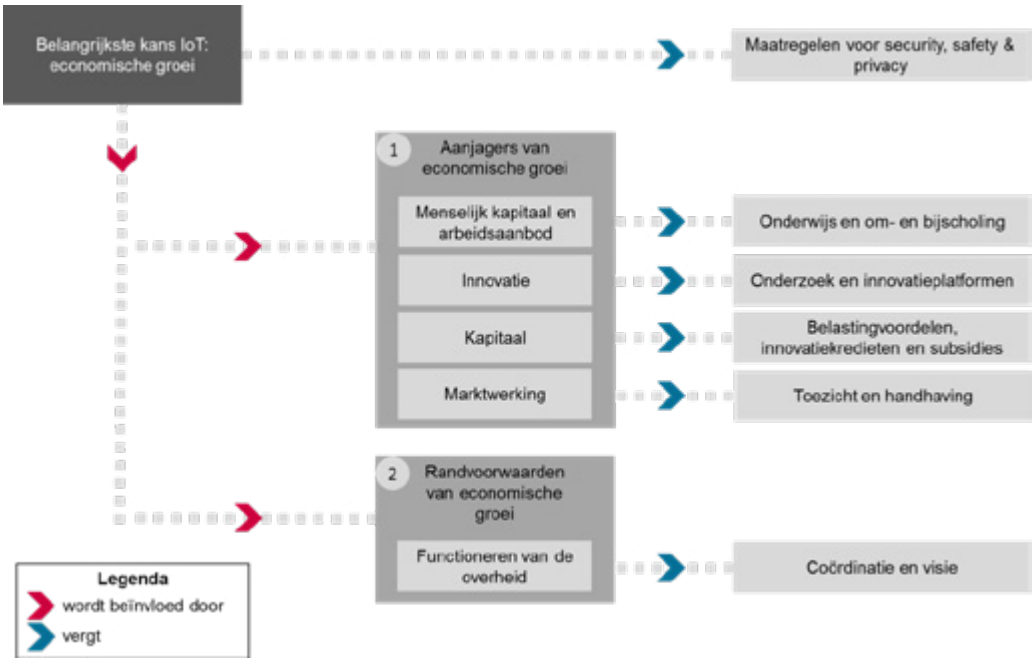
einden dan waarvoor ze verzameld zijn. Deze bedreigingen hangen sterk samen met veiligheidsrisico's. Wanneer de beveiliging van IoT-toepassingen niet op orde is, wordt de kans dat kwaadwillende personen toegang krijgen tot persoonsgegevens groter. Ook bedreigingen op het gebied van andere waarden brengen veiligheidsrisico's met zich mee. Hoe afhankelijker we bijvoorbeeld worden van technologie en grote (buitenlandse) bedrijven, des te groter de gevolgen kunnen zijn als er iets misgaat.

Maatregelen

Er zijn verschillende factoren die van invloed zijn op de kansen op het gebied van economische groei en de bedreigingen aangaande veiligheid en privacy. Hoewel het initiatief met name bij het bedrijfsleven ligt, kan de overheid bedrijven stimuleren door maatregelen te treffen.

Figuur S1 geeft een overzicht van de factoren en bijbehorende maatregelen die economische groei door het IoT positief kunnen beïnvloeden. Allereerst is het tegengaan van risico's op het gebied van veiligheid en privacy een belangrijke vereiste voor het bevorderen van economische groei. De factoren die economische groei beïnvloeden kunnen worden onderverdeeld in aanjagers van economische groei en factoren die samen de randvoorwaarden voor economische groei bepalen.

Figuur S1 Factoren en maatregelen die economische groei door het IoT bevorderen



Economische groei wordt aangejaagd door de beschikbaarheid van kapitaal, daarbij kan het onder meer gaan om menselijk kapitaal en financieel kapitaal. Dit vergt dus een beroepsbevolking met voldoende kennis en vaardigheden, en uiteraard ook investeringen in de betreffende technologie. Innovatie behelst het ontwikkelen van nieuwe processen en producten, die bijvoorbeeld de productiviteit van bedrijven verhogen en de welvaart vergroten. Voor innovatie moet wel ruimte worden gebo-

den, ook als dit bestaande verdienmodellen uitdaagt. Marktwerking is verder een belangrijke aanjager van economische groei. Oneerlijke concurrentie dient daarom zo veel mogelijk worden tegengegaan, iets wat met de komst van digitale platformen mogelijk in toenemende mate onder druk zal komen te staan.

De volgende maatregelen dragen bij aan het positief beïnvloeden van aanjagers van economische groei.

- Overheid en bedrijven: moderniseer het onderwijs zodat er meer aandacht is voor ICT-vaardigheden en biedt ruimte voor het om- en bijscholen van de beroepsbevolking.
- Overheid, bedrijven en kennisinstellingen: investeer in kennis en onderzoek om te komen tot nieuwe IoT-technologieën en -innovaties.
- Overheid: biedt ruimte voor partijen om te kunnen innoveren, dit kan onder meer in de vorm van een *regulatory sandbox*, waarin toezichthouders, in overleg met betrokken partijen, speelruimte creëren om nieuwe toepassingen te onderzoeken.
- Overheid: laat een deel van de verstrekte belastingvoordelen, innovatiekredieten en subsidies voor topsectoren ten goede komen aan de ontwikkeling van topsector-gerelateerde IoT-toepassingen. Houd daarnaast rekening met het ondersteunen van start-ups, bijvoorbeeld door het verstrekken van subsidies.
- Overheid: geef toezichthouders voldoende middelen om toezicht te houden op nieuwe ontwikkelingen, zoals de toenemende invloed van digitale platformen.

Het functioneren van de overheid beïnvloedt het ondernemingsklimaat en vormt daarmee een randvoorwaarde voor economische groei. Als wet- en regelgever is een zekere voorspelbaarheid in het optreden van de overheid gunstig voor het ondernemingsklimaat. Daarnaast is voor de ontwikkeling van het IoT samenwerking tussen veel verschillende partijen noodzakelijk. De overheid zou daarin een rol kunnen spelen, maar schiet op het gebied van ICT nu nog vaak tekort.

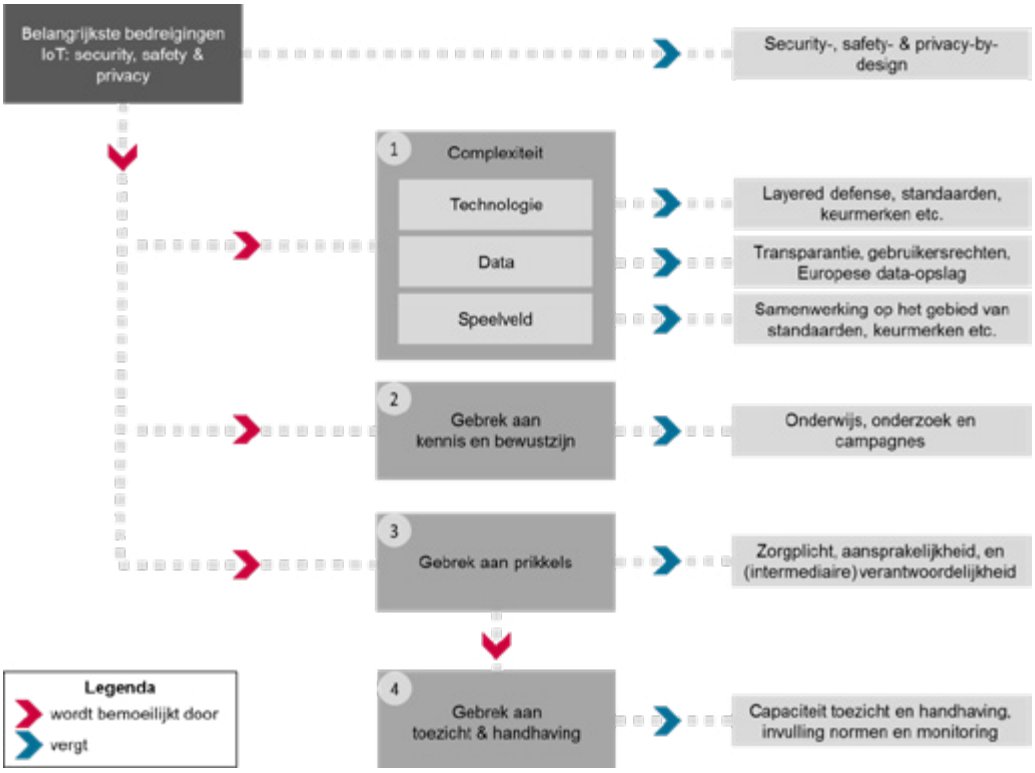
De volgende maatregelen dragen bij aan het positief beïnvloeden van de randvoorwaarden van economische groei.

- Overheid: formuleer een visie voor het IoT, waarbij rekening wordt gehouden met de aanpassingskosten van nieuw beleid. Bedrijven kunnen hierdoor tijdig anticiperen met (het uitstellen of terugschroeven van) eventuele investeringen.
- Overheid: beleg de verantwoordelijkheid voor het sturen en coördineren van de beschreven maatregelen bij één instantie.

Figuur S2 geeft een overzicht van de factoren die de ontwikkeling en het gebruik van veilige en privacygevoelige IoT-toepassingen belemmeren. Dat zijn: 1) complexiteit van het IoT, 2) gebrek aan kennis en bewustzijn, 3) gebrek aan prikkels, en 4) gebrek aan toezicht en handhaving. Per factor kunnen maatregelen genomen worden die het belemmerende effect van deze factoren kunnen verminderen.

De complexiteit van het IoT omvat de technologie zelf, de verwerkte data en het speelveld hieromheen. De heterogeniteit van IoT-technologie maakt het lastig om algemene veiligheidsmaatregelen te formuleren. Dit zorgt ervoor dat lokale oplossingen door hun beperkte reikwijdte aan effectiviteit hebben moeten inboeten. De grote rol van data binnen het IoT draagt bij aan de complexiteit door onduidelijkheid over waar data zijn opgeslagen, wie toegang heeft tot en gebruikmaakt van de data en hoe invulling wordt gegeven aan rechten die aan data kunnen worden ontleend. Het speelveld brengt complexiteit met zich mee door de grote hoeveelheid aan

Figuur S2 Maatregelen om security-, safety en privacyrisico's van het IoT te beperken



(veelal buitenlandse) spelers op de IoT-markt, waardoor het aan overzicht ontbreekt over wie waar verantwoordelijk voor is. Dit probleem wordt verergerd doordat overheden verschillende regels en standaarden hanteren en daarnaast ook andere belangen hebben.

De volgende maatregelen dragen bij aan het omgaan met de complexiteit van het IoT.

- Bedrijven: maak gebruik van *layered defense* bij het treffen van veiligheidsmaatregelen, op deze manier kunnen risico's op verschillende niveaus het hoofd worden geboden.
- Overheid en bedrijven: stel keurmerken en standaarden vast waarin veiligheids- en privacy-eisen staan waaraan fabrikanten van IoT-producten moeten voldoen.
- Bedrijven: vergroot transparantie over het gebruik van data door heldere en begrijpelijke privacyvoorwaarden op te stellen.
- Overheid: verplicht fabrikanten om IoT-apparaten te voorzien van een aan- en uitknop voor gegevensverwerking en gegevensdoorgifte aan derden.
- Overheid en bedrijven: lokaliseer de opslag en verwerking van data van IoT-producten binnen Nederland of Europa.

Het treffen van maatregelen om veiligheids- en privacyrisico's tegen te gaan wordt ook bemoeilijkt door een gebrek aan kennis en bewustzijn over (risico's rondom) het IoT en ICT in het algemeen. Dit geldt voor zowel de overheid, burgers, als het bedrijfsleven.

Een aantal maatregelen kan dit gebrek aan kennis en bewustzijn tegengaan.

- Overheid en bedrijven: investeer in onderwijs, om- en bijscholing en voorlichting om veilig internetgebruik en digitale vaardigheden in Nederland te vergroten.
- Overheid, bedrijven en kennisinstellingen: investeer in onderzoek en monitoring van nieuwe bedreigingen op het gebied van veiligheid en privacy van nieuwe (IoT-)technologie.
- Overheid: investeer verder in het aantrekken en ontwikkelen van (eigen) expertise op het gebied van ICT.

Het nemen van veiligheidsmaatregelen wordt ook sterk belemmerd door een gebrek aan prikkels bij gebruikers en bedrijven. Gebruikers zijn zich vaak niet bewust van veiligheids- en privacyrisico's en ondervinden in veel gevallen ook geen hinder door aanvallen. Voor bedrijven ontbreekt er een economische prikkel om producten voldoende te beveiligen. Beveiliging kost in de meeste gevallen meer dan dat het oplevert. Hoewel bij beide partijen prikkels ontbreken, mogen gebruikers er redelijkerwijs van uitgaan dat fabrikanten deugdelijke producten verkopen.

De volgende maatregelen creëren prikkels voor bedrijven om veiligere en privacyvriendelijkere IoT-toepassingen te fabriceren en aan te bieden.

- Overheid en bedrijven: bedrijven dienen zich beter te houden aan hun zorgplicht. De overheid kan deze zorgplicht aanscherpen op gebieden waar nu soms nog onduidelijkheid over bestaat. Het is nu nog niet altijd duidelijk hoe ver de zorgplicht reikt wat betreft beveiliging. Ook voor aansprakelijkheid geldt dat de overheid nadere regels kan treffen om onduidelijkheden weg te nemen.
- Bedrijven: voer ketenverantwoordelijkheid in om de beveiliging van het IoT te waarborgen, zeker als bij de productie of het gebruik van IoT-producten veel partijen betrokken zijn.
- Verzekeringsmaatschappijen: integreer veiligheidsstandaarden en -keurmerken bij het formuleren van nieuwe (cyber)verzekeringen.
- Overheid: bouw voort op bestaande beleidsmatige initiatieven gericht op ISP's om het ontbreken van marktprikkels tegen te gaan.
- Overheid: geef sturing op het gebied van security via het inkoopbeleid. Dit kan een bijdrage leveren aan kennisopbouw en kan andere partijen ertoe bewegen om te innoveren en investeren op het gebied van cybersecurity.

Het effect van de hierboven beschreven maatregelen wordt beperkt door een gebrek aan toezicht en handhaving. Zonder deze stok achter de deur zijn maatregelen zoals zorgplicht en aansprakelijkheid minder effectief. Middelen voor toezicht en handhaving schieten nu echter (vaak) nog tekort.

De volgende maatregelen dragen bij aan effectief toezicht en effectieve handhaving.

- Overheid: zorg voor voldoende capaciteit bij de betrokken toezichthouders.
- Overheid: geef nadere invulling aan normen voor zorgplicht en aansprakelijkheid, bijvoorbeeld over de levensduur van IoT-apparaten en wat de eindgebruiker mag verwachten van de aanbieder.

Conclusies

Bovenstaande resultaten laten zien dat het IoT een scala aan mogelijkheden verschaft om welzijn, duurzaamheid, productiviteit en welvaart in onze maatschappij te verhogen. Echter blijkt ook dat IoT-toepassingen op dit moment slecht zijn beveiligd en daarmee een bedreiging voor onze veiligheid en privacy vormen. Het Mirai-botnet, bestaande uit gehackte IoT-apparaten, laat zien dat de impact nu al groot is en dit zal in de toekomst alleen nog maar verder toenemen. Het is van belang dat de veiligheids- en privacyrisico's worden aangepakt om schade zo veel mogelijk te beperken en voorkomen. Om te kunnen profiteren van de kansen die het IoT biedt moet er tevens, op een veilige manier, ruimte worden geboden voor nieuwe ontwikkelingen en innovatie.

Als producent van IoT-toepassingen en -infrastructuur zijn bedrijven verantwoordelijk voor het realiseren van nieuwe en innovatieve, maar ook veilige en privacybeschermende IoT-toepassingen. Op dit moment gebeurt dat nog onvoldoende door de grote complexiteit van het IoT en een gebrek aan kennis, prikkels, toezicht en handhaving. Geen van de bovenstaande maatregelen vormt op zichzelf een oplossing voor de bedreigingen van het IoT. In andere woorden, er is geen *one size fits all* maatregel die deze problematiek kan oplossen. In plaats daarvan zijn er verschillende samenhangende maatregelen nodig die pas effectief zijn als zij als geheel worden doorgevoerd. Dit vereist een gedragen overheidsvisie, waarbij er één instantie wordt aangewezen als hoofdverantwoordelijke die dit beleid coördineert en stuurt. Omdat het IoT samenhangt met andere technologische ontwikkelingen en cybersecurity in bredere context, zou een visie ook op deze onderwerpen betrekking moeten hebben.

Discussie en vervolgonderzoek

Dit onderzoek is verkennend en breed van aard, in vervolgonderzoek zou op een aantal thema's dieper kunnen worden ingegaan. Allereerst zou vervolgonderzoek zich erop kunnen richten om de belangrijkste kansen, bedreigingen en handelingsperspectieven van specifieke IoT-toepassingen of toepassingsdomeinen in kaart te brengen. Ten tweede kan er onderzoek worden gedaan naar het kwantificeren van verschillende maatregelen. Een derde aanbeveling is om vervolgonderzoek te doen naar de effecten van verschillende handelingsperspectieven, bijvoorbeeld de haalbaarheid en effectiviteit van een overkoepelend, coördinerend orgaan. Ten vierde zou er dieper in kunnen worden gegaan op de technische details en veiligheid van IoT-producten. Ten vijfde zou er verder onderzoek kunnen worden gedaan naar de benodigde aanpassing van wet- en regelgeving ten aanzien van het IoT. Een laatste aanbeveling is om uitgebreider onderzoek te doen naar de geopolitiek consequenties van het IoT voor de internationale (vrij)handel en het economische verkeer.

1 Inleiding

1.1 Aanleiding en doelstelling

De groei van het *Internet of Things* (IoT) is een ontwikkeling die haar stempel drukt en in toenemende mate zal drukken op onze maatschappij. Het IoT is een netwerk van 'slimme' apparaten, sensoren en andere objecten die met elkaar en vaak ook met het internet verbonden zijn. De verwachting is dat in de toekomst steeds meer objecten met elkaar verbonden zullen zijn: in 2020 zullen 20 tot 30 miljard objecten deel uitmaken van het IoT (Gartner, 2015; WEF, 2015). Daarbij kan het gaan om kleinere alledaagse objecten zoals lampen en deursloten, maar ook om grotere objecten zoals auto's en gebouwen.

De verwachting is dat het IoT een belangrijke impact zal hebben op de economie en zowel in de consumenten- als industriële markt een aanzienlijk aandeel zal verwerven. De voorspellingen van de bijdrage van het IoT aan de wereldwijde economie variëren van 1,9 biljoen dollar tot maar liefst 14,4 biljoen dollar (Bradley, Barbier, & Handler, 2013; Lund, MacGillivray, Turner, & Morales, 2014; Manyika et al., 2013; GO-Science, 2014). Volgens onderzoeksbureau Gartner (2015) zal het IoT binnen vijf tot tien jaar niet meer weg te denken zijn uit de samenleving. De wereld staat daarmee aan het begin van een nieuwe fase, waarin allerlei dingen steeds meer met elkaar communiceren, grotere hoeveelheden data verzamelen en complexere berekeningen uitvoeren. Het IoT zal een steeds prominentere rol spelen in het dagelijks leven en de digitale en fysieke wereld zullen verder met elkaar vervlochten raken. De opkomst van het IoT zal hierdoor een grote impact hebben op vele aspecten van de samenleving, zoals werkgelegenheid, gezondheidszorg, mobiliteit en welvaart (Bauer, Patel, & Veira, 2014; Ter Welle, Peters, & Sterk, 2015; Ericsson, 2016; Evans, 2012).[1]

De geschetste ontwikkelingen gaan razendsnel en de grootschalige adoptie van IoT-toepassingen in onze samenleving is een gegeven: het IoT is geen toekomstmuziek en is er voor een (groot) deel al. Enerzijds kan het IoT een drijvende kracht zijn voor economische groei en innovatie. Anderzijds zullen de ontwikkelingen ook bedreigingen met zich mee brengen, bijvoorbeeld op het gebied van cybersecurity. Een recent voorbeeld is het Mirai-botnet, dat bestond uit duizenden IoT-apparaten, waarmee verschillende websites eind 2016 onbereikbaar werden gemaakt.[2] Om de kansen van het IoT te benutten en de bedreigingen te minimaliseren moet hier tijdig op worden ingespeeld. De subcommissie Internet of Things van de Cybersecurity Raad (CSR) heeft het WODC daarom gevraagd om een verkenning uit te voeren naar deze kansen en bedreigingen.

De CSR is een nationaal en onafhankelijk adviesorgaan van het Kabinet en is samengesteld uit hooggeplaatste vertegenwoordigers van publieke en private organisaties en de wetenschap. De CSR zet zich op strategisch niveau in om de cybersecurity in Nederland te verhogen. In het Werkprogramma 2016 heeft de CSR

[1] Zie ook: www.gartner.com/newsroom/id/3165317

[2] Zie ook: https://tweakers.net/nieuws/117059/ddos-aanval-op-dns-provider-dyn-werd-uitgevoerd-met-mirai-botnet.html

(2016) een aantal thema's benoemd die aandacht krijgen. Een van deze thema's is: het tijdig en effectief inspelen op nieuwe technologische ontwikkelingen. Voor de CSR is het IoT in dit kader een speerpunt. De CSR heeft zich tot doel gesteld om een advies op te stellen om het IoT op verantwoorde wijze te laten landen in onze samenleving. Het voorliggende onderzoek beoogt hieraan bij te dragen door inzicht te geven in de belangrijkste gevolgen van het IoT voor de samenleving. Daarnaast formuleert dit onderzoek handelingsperspectieven voor de overheid en de samenleving om van de kansen te profiteren en de bedreigingen te minimaliseren.

1.2 Onderzoeksopzet

In deze paragraaf wordt de onderzoeksopzet besproken. Allereerst wordt ingegaan op de definitie van het IoT die ten behoeve van dit onderzoek gehanteerd wordt. Vervolgens komen de onderzoeksvragen en onderzoeksmethode aan bod. Als laatste wordt de scope van het onderzoek toegelicht.

1.2.1 Definitie

Het concept IoT is op veel verschillende manieren gedefinieerd in de literatuur en kent daarmee geen eenduidige definitie (Minerva, Biru, & Rotondi, 2015). De verschillende definities worden beïnvloed door de achtergrond van de auteurs, maar ook door nieuwe technologische ontwikkelingen (Gubbi, Buyya, Marusi, & Palaniswami, 2013; Oriwoh & Conrad, 2015). In dit onderzoek zal de volgende definitie van het Internet of Things worden aangehouden: *Een netwerk van objecten (vaak verbonden met het internet), die gegevens verzamelen over hun omgeving, deze kunnen uitwisselen en op basis daarvan (semi)autonome beslissingen nemen en/of acties uitvoeren die van invloed zijn op de omgeving*.[3]

Het begrip 'object', moet hierbij ruim worden opgevat. Naast apparaten kunnen ook mensen objecten zijn binnen het IoT, bijvoorbeeld door geïmplanteerde sensoren. De focus van dit onderzoek ligt op nieuwe IoT-toepassingen voor een breed scala aan domeinen, zoals bijvoorbeeld *wearables* en *smart-home*-toepassingen. De focus ligt niet op gangbaardere apparaten zoals computers, laptops, tablets en telefoons. Deze apparaten spelen uiteraard wel een belangrijke rol om met het IoT te communiceren en/of objecten in het IoT aan te sturen (en zullen in deze hoedanigheid besproken worden). Ook data spelen een grote rol binnen het IoT en worden in dit onderzoek meegenomen vanuit het oogpunt dat zij kunnen worden gecreëerd of bewerkt door objecten binnen het IoT.

1.2.2 Onderzoeksvragen

De centrale vraagstelling van dit onderzoek is als volgt:

Wat zijn de kansen en bedreigingen van het IoT en hoe kunnen verschillende stakeholders de ontwikkeling van het IoT in Nederland op een positieve manier beïnvloeden?

[3] Deze definitie is onder andere gebaseerd op het werk van Bhabad en Bagade (2015), Caron, Bosua, Maynard, en Ahmad (2016), Davies (2015) en Whitmore, Agarwal en Xu (2015).

Voor de beantwoording van de centrale onderzoeksvraag zijn de volgende deelvragen geformuleerd.

1 Wat behelst het IoT?
2 Welke kansen biedt het IoT?
3 Welke bedreigingen brengt het IoT met zich mee?
4 Wat zijn de maatregelen die verschillende stakeholders kunnen nemen om de kansen van het IoT te benutten en de bedreigingen ervan te beperken?

Deze deelvragen worden in verschillende hoofdstukken behandeld. Het slothoofdstuk van dit rapport beantwoordt vervolgens de centrale vraag. In de hoofdstukken zullen verschillende voorbeelden van IoT-toepassingen worden besproken.

1.2.3 Methodologie

In dit onderzoek is informatie verzameld door middel van een literatuurstudie, interviews en rondetafelgesprekken. Voor de literatuurstudie is gebruikgemaakt van wetenschappelijke literatuur, vakliteratuur en mediaberichten over het IoT. Vanwege de snelle ontwikkelingen op het gebied van het IoT kunnen juist die laatste bronnen soms zeer relevante informatie bevatten. Naast de literatuurstudie zijn er in totaal zes interviews gehouden met experts en stakeholders uit relevante sectoren. Hiervoor is gebruikgemaakt van semigestructureerde vragenlijsten. In bijlage 2 is de lijst van geïnterviewde experts opgenomen. Ten slotte zijn er twee rondetafelgesprekken georganiseerd met de thema's *Smart City* en *Smart Industry*. Bij beide discussies waren verschillende experts en stakeholders met betrekking tot het betreffende thema aanwezig. In bijlage 2 is een lijst met de deelnemers van deze rondetafelgesprekken opgenomen.

Voor het in kaart brengen, beschrijven, en analyseren van de kansen en bedreigingen van het IoT (onderzoeksvragen 2 en 3) zijn diverse benaderingen overwogen. Een voor de hand liggende vorm om de kansen en bedreigingen in kaart te brengen is per toepassingsdomein, waarbij gedacht kan worden aan domeinen als gezondheidszorg, logistiek en landbouw. Een andere vorm is om te kiezen voor een indeling op basis van toepassingsgebied, waarbij bijvoorbeeld onderscheid kan worden gemaakt tussen IoT-toepassingen voor het lichaam, de woon- en werkruimte, de stad en het land.[4] Een nadeel van beide genoemde vormen is dat veel van de kansen en bedreigingen in verschillende toepassingsdomeinen en -gebieden spelen. Veiligheidsrisico's zijn bijvoorbeeld bij vrijwel alle IoT-toepassingen van belang. Een indeling gebaseerd op toepassingsdomein of -gebied leidt daarom al snel tot veel herhaling.

Uiteindelijk is er daarom voor gekozen om de kansen en bedreigingen van het IoT voor de maatschappij te beschrijven aan de hand van menselijke waarden zoals privacy, veiligheid en duurzaamheid. Het uitgangspunt hierbij is dat technologie een impact heeft op menselijke waarden (Kool, Timmer, Royakkers, & Van Est, 2017; Van den Hoven, Van de Poel, & Vermaas, 2014). Een waarde kan hierbij gedefinieerd worden als datgene wat een persoon of een groep personen belangrijk vindt in zijn of haar leven (Friedman, Kahn, & Borning, 2013).

Het IoT maakt een grote diversiteit aan toepassingen mogelijk waardoor het een breed scala aan waarden raakt. Zo kan een slimme lantaarnpaal met sensoren hel-

[4] In hoofdstuk 2 wordt deze onderverdeling overigens wel aangehouden. Hierin wordt het gebruik van IoT-toepassingen geïllustreerd aan de hand van deze niveaus.

pen om onregelmatigheden in een uitgaansgebied sneller te detecteren en zo de waarde veiligheid ondersteunen, een *activity tracker* kan mensen ertoe aanzetten om meer te bewegen en daarmee hun gezondheid bevorderen en een *smart grid* kan ervoor zorgen dat er zuiniger met energie om wordt gegaan en zo duurzaamheid stimuleren. Bovenstaande voorbeelden laten zien hoe IoT-toepassingen menselijke waarden kunnen bevorderen: de kansen. Net als alle (nieuwe) technologieën brengt het IoT naast positieve ook potentiële negatieve effecten met zich mee. Het ondermijnen van menselijke waarden als veiligheid en privacy wordt vaak in verband gebracht met het IoT. Naast veiligheid en privacy kan het IoT nadelige gevolgen hebben voor waarden als welvaart (banen worden overgenomen door technologie) of gelijkwaardigheid in de samenleving (bepaalde groepen hebben beperkt toegang tot de mogelijkheden van het IoT). Deze negatieve effecten van het IoT op menselijke waarden vormen de bedreigingen van het IoT.

De gehanteerde werkwijze voor het in kaart brengen van kansen en bedreigingen aan de hand van waarden is als volgt. Allereerst zijn alle kansen en bedreigingen die gevonden en genoemd zijn in het literatuuronderzoek, de interviews en de rondetafelgesprekken op een rij gezet. Vervolgens zijn overeenkomstige en verwante kansen en bedreigingen geordend in categorieën. Ten slotte is bepaald welke waarde geraakt wordt door de kansen of bedreigingen in een categorie. Bij het categoriseren is rekening gehouden met kansen en bedreigingen die herhaaldelijk naar voren zijn gebracht en die extra werden benadrukt door de geïnterviewde experts en stakeholders. De genoemde waarden vormen dan ook nadrukkelijk niet de enige of de juiste menselijke waarden die beïnvloed worden door het IoT. Wel vormen ze een bruikbare kapstok aan de hand waarvan kansen en bedreigingen van het IoT beschreven kunnen worden, zonder al te veel in de herhaling te vallen.

Voor het beantwoorden van onderzoeksvraag 4, en het in kaart brengen van mogelijke maatregelen, is een vergelijkbare werkwijze gehanteerd. Hierbij zijn de belangrijkste kans en de belangrijkste bedreigingen uit hoofdstuk 3 als uitgangspunt genomen en is eerst bekeken welke factoren deze positief dan wel negatief beïnvloeden. Vervolgens zijn daarbij mogelijke maatregelen gezocht. Hiertoe zijn alle factoren en maatregelen die in de literatuur, interviews en rondetafelgesprekken naar voren zijn gekomen in een lijst geplaatst en vervolgens geordend op basis van overeenkomstigheid. Vervolgens zijn de (belangrijkste) relaties en samenhangen tussen deze factoren en maatregelen in een schema geëxpliciteerd. Hierbij is rekening gehouden met maatregelen die herhaaldelijk naar voren zijn gebracht en extra nadruk kregen in de interviews en rondetafelgesprekken. Voor de beschrijving van de maatregelen is gebruikgemaakt van deze schematische weergaven.

1.2.4 Scope van het onderzoek

Dit onderzoek gaat over het IoT, de impact ervan op de maatschappij en de handelingsperspectieven van relevante stakeholders. Dit is een veelomvattend onderzoeksdoel dat diverse technologieën omvat en vele toepassingsdomeinen en stakeholders raakt. Dit onderzoek is verkennend van aard. Vanwege de grote reikwijdte van dit onderzoek, gecombineerd met een beperkte tijd waarbinnen het onderzoek afgerond moest worden, is ervoor gekozen om een overzicht te geven van het gehele speelveld. De relevante ontwikkelingen, spelers en toepassingen zijn daarbij zo veel mogelijk in kaart gebracht. Een dergelijk brede focus brengt met zich mee dat per deelonderwerp maar beperkt de diepte in kan worden gegaan. Dat is ook niet de doelstelling van het onderzoek. Dit rapport beoogt een brede groep lezers aan te spreken die momenteel nog relatief weinig over het IoT weet. Alleen met

een bredere aanpak is het mogelijk gebleken een zo compleet mogelijk palet aan kansen, bedreigingen, maatregelen en handelingsperspectieven te verschaffen.

Met deze focus onderscheidt dit onderzoek zich op verschillende punten van bestaand onderzoek. Ten eerste richt dit rapport zich op de situatie in Nederland. Diverse andere verkennende onderzoeken beschrijven de kansen, bedreigingen en/of handelingsperspectieven rondom het IoT, maar dan vanuit een internationaal of niet-Nederlands perspectief (bijvoorbeeld, Davies, 2015; GO-Science, 2014; Rose, Eldridge, & Chapin, 2015). Ten tweede richt dit rapport zich specifiek op het IoT. Er bestaan diverse onderzoeksrapporten over onderwerpen die ook in dit rapport aan bod komen, maar die niet specifiek op het IoT gericht zijn, zoals bijvoorbeeld het internet (WRR, 2015), big data (Ministerie van Economische Zaken, 2016; WWR, 2016), cybersecurity (CRS, 2016b; Munnichs, Kouw, & Kool, 2017; NCSC, 2016), waarden in de digitale samenleving (Kool et al., 2017) en digitalisering en werk (van Est & Kool, 2015; SER, 2016; Went & Kremer, 2015). Ten derde bestaat er, voor zover bekend bij de auteurs, geen rapport met zo'n breed, veelomvattend perspectief op het IoT in Nederland als dit rapport, dat ingaat op zowel technologische, maatschappelijke als beleidsmatige aspecten. Een onderzoek uitgevoerd in opdracht van het ministerie van Economische Zaken (EZ) beperkt zich bijvoorbeeld tot de technologische trends en toepassingen van het IoT (Stratix, 2015). Een eerder verschenen rapport van de CSR richt zich juist met name op de handelingsperspectieven (CSR, 2016b). Het voorliggende rapport is daarmee een aanvulling op bestaand onderzoek.

1.3 Leeswijzer

Het rapport is als volgt opgebouwd. In hoofdstuk 2 komt deelvraag 1 aan bod. In dit hoofdstuk wordt ingegaan op de ontwikkeling van het IoT, de belangrijkste kenmerken van het IoT en mogelijke toepassingen van het IoT. Deelvragen 2 en 3 worden in hoofdstuk 3 beantwoord. In dit hoofdstuk worden aan de hand van menselijke waarden de kansen en bedreigingen besproken. De kansen worden besproken aan de hand van de waarden: welzijn, duurzaamheid, productiviteit en welvaart. Vervolgens worden de bedreigingen behandeld aan de hand van de waarden: veiligheid, privacy, welvaart, welzijn, gelijkwaardigheid en autonomie. Vervolgens beschrijft hoofdstuk 4 de maatregelen die stakeholders kunnen nemen om de belangrijkste kans(en) te stimuleren en de belangrijkste bedreiging(en) te mitigeren. Hoofdstuk 5 bevat de conclusie van dit rapport. Daarin worden de bevindingen van dit onderzoek samengevat en de antwoorden op de deelvragen gebruikt om een antwoord op de centrale vraag van dit onderzoek te formuleren.

2 Het Internet of Things

Dit hoofdstuk heeft als doel om meer inzicht te verschaffen in het fenomeen Internet of Things. De opbouw van dit hoofdstuk is als volgt. Paragraaf 2.1 geeft een korte beschrijving van de ontwikkelingen die hebben geleid tot het IoT. In paragraaf 2.2 volgt een analyse van de belangrijkste elementen van het IoT. Ten slotte wordt in paragraaf 2.3 een overzicht gegeven van mogelijke toepassingen van het IoT op verschillende niveaus.

2.1 Ontwikkeling van het Internet of Things

Het idee dat alledaagse objecten voorzien van gegevensverwerkende capaciteiten de omgeving kunnen waarnemen, ermee kunnen interacteren en autonoom beslissingen kunnen nemen is niet nieuw (Whitmore et al., 2015). Sinds de jaren tachtig zijn er vergelijkbare concepten geïntroduceerd, waarbij de nadruk soms op andere aspecten ligt. Enkele voorbeelden hiervan zijn *ambient intelligence*, *calm computing*, *ubiquitous computing*, *pervasive computing* en *cyber physical systems* (Van den Berg, 2010; Kranenburg et al., 2011; Bibri, 2015; Wan, Chen & Leung, 2015). Vaak werden dergelijke concepten geïntroduceerd door bedrijven, zoals Philips en IBM, en vonden vervolgens hun weg naar de bestuurlijke context (Van den Berg, 2010; Kranenburg et al., 2011; Bibri, 2015). Zo werd de term ambient intelligence veel gebruikt in Europa en ubiquitous computing met name in de Verenigde Staten (Bibri, 2015).

De term Internet of Things werd in 1999 geïntroduceerd met de oprichting van het MIT Auto-ID Center (Fletcher, 2015).[5] Het doel van het Auto-ID Center was om identificatietechnologieën te ontwikkelen waarmee de productiviteit en efficiëntie van de industrie kon worden bevorderd. De belangrijkste technologie die daarvoor werd gebruikt was *Radio Frequency Identification* (RFID). Eén van de eerste toepassingen, die nog steeds wordt gebruikt, was de introductie van antidiefstalpoortjes in combinatie met RFID-tags. Deze simpele RFID-tags kunnen aan of uit staan, waarmee kan worden achterhaald of iemand wel of niet heeft betaald. Met de komst van het Auto-ID Center werd deze technologie verder ontwikkeld en toegepast voor logistieke doeleinden. Door gebruik te maken van goedkope RFID-tags werd het mogelijk (en rendabel) om producten individueel in de bevoorradingsketen te volgen (Fletcher, 2015; Roberti, 2015). RFID wordt nog steeds (en in toenemende mate) toegepast in sectoren zoals de logistiek, industrie en detailhandel (Li, Xu & Zhao, 2015), om bijvoorbeeld verstuurde pakketjes online te volgen met behulp van een Track & Trace-code.

Het IoT is dus ontstaan uit een evolutie van bestaande technologieën en concepten (Gubbi et al., 2013). De term IoT wordt daarnaast vaak als synoniem gebruikt voor 'slimme' systemen, zoals *smart homes*, *smart cities* (Thierer, 2015) en het *Industrial Internet of Things* (Jeschke, Brecher, Meisen, Özdemir & Eschert, 2016). Het IoT lijkt als term breed te worden gedragen, mede vanwege de toegankelijkheid van de term door de associatie met het internet (Bibri, 2015). In dit rapport wordt dan ook de (verzamel)term IoT gebruikt. Wat dat concept behelst wordt hieronder verder toegelicht.

[5] Zie ook: www.autoidlabs.org

2.1.1 Aanverwante technologische ontwikkelingen

Zoals eerder aangegeven hebben (andere) technologische ontwikkelingen de reikwijdte van het IoT verbreed: van objecten in de bevoorradingsketen naar vrijwel alle alledaagse objecten (Fletcher, 2015; Gubbi et al., 2013; Santucci, 2010). De ontwikkeling dat sensoren, actuatoren en communicatiemiddelen in vrijwel ieder object passen en betaalbaar zijn geworden, verklaart mede waarom het IoT nu zo sterk in opkomst is. Andere technologische ontwikkelingen die daarbij een belangrijke rol (gaan) spelen zijn: *5G-netwerken*, *cloud computing*, *big data, datamining*, *machine learning* en *kunstmatige intelligentie.* Deze ontwikkelingen dragen met name bij aan de manier waarop data worden verzameld en geanalyseerd en de manier waarop data kunnen worden gebruikt voor IoT-toepassingen. Zij worden hieronder kort toegelicht.

Op dit moment spelen 4G-netwerken al een belangrijke rol bij IoT-toepassingen, bijvoorbeeld door het faciliteren van netwerkverkeer van slimme energiemeters. 5G is de beoogde opvolger van het huidige 4G-netwerk en belooft een hogere doorvoersnelheid met minder vertragingen. 5G-netwerken zijn met name gericht op IoT-apparaten die draadloos verbonden zijn. Ze zullen daarom een belangrijke bijdrage gaan leveren aan het versturen en uitwisselen van data door IoT-apparaten en zo tal van nieuwe toepassingen mogelijk maken. Doordat er niet of nauwelijks vertraging is kunnen dokters bijvoorbeeld procedures op afstand uitvoeren. Een chirurg kan een robot gebruiken om op honderden kilometers afstand te opereren. Door middel van sensoren in de robot kan de dokter realtime feedback ontvangen over de operatie, alsof hij zelf in de kamer aanwezig is.[6] De ontwikkeling van een 5G-netwerk wordt door de Europese Commissie gezien als een belangrijke pijler voor de verdere ontwikkeling van het IoT in de Europese Unie en investeert hier dan ook veel in.[7]

Cloud computing draagt bij aan de mogelijkheid om data in een netwerk op te slaan en te analyseren. Via cloud computing worden middelen (zoals software, hardware en data) op aanvraag beschikbaar gesteld via het internet, ook wel de *cloud* genoemd (Koops, Leenes, Hert, & Olislaegers, 2012). De cloud biedt het IoT een betaalbare oplossing voor het opslaan van data; dit hoeft niet meer lokaal te gebeuren (Al-Fuqaha, Guizani, Mohammadi, Aledhari & Ayyash, 2015; Farooq, Waseem, Mazhar, Khairi & Kamal, 2015). Dit heeft als voordeel dat de opslagruimte vaak onbeperkt is en dat de data op ieder moment en op iedere locatie beschikbaar zijn. Naast het opslaan van data kan de cloud ook gebruikt worden voor rekenkracht. Snelle en krachtige externe servers worden dan bijvoorbeeld ingezet voor dataverwerking en -analyse.

Data die worden verzameld door middel van het IoT kunnen in veel gevallen worden gekwalificeerd als big data. Big data kenmerkt zich door een grote hoeveelheid aan data, een variëteit van data uit verschillende databronnen en een hoge snelheid van dataverzameling en -analyse (Gandomi & Haider, 2015; Laney, 2001; WRR, 2016). Dit type data vormt de basis voor veel IoT-toepassingen, doordat verschillende sensoren realtime een grote hoeveelheid (ongestructureerde) data produceren. Big data kenmerkt zich daarnaast door het gebruik van data uit één domein voor beslissingen in een ander domein (WRR, 2016). In een IoT-context kan bijvoorbeeld sensordata over de luchtkwaliteit worden gecombineerd met medische data, zodat

[6] Zie ook: www.cnet.com/news/5-amazing-things-youll-be-able-to-do-with-5g

[7] Zie ook: https://ec.europa.eu/digital-single-market/en/5g-europe-action-plan

kan worden geadviseerd wanneer iemand met astma het best naar buiten kan.[8] De term big data wordt verder ook gebruikt om specifiek te verwijzen naar *datagedreven* analysemethoden. Hierbij wordt gezocht naar patronen in data zonder dat daarover vooraf een hypothese is opgesteld. De verzameling van analysemethoden die hiervoor wordt gebruikt, wordt vaak onder de noemer big data geschaard.

Voorbeelden van datagedreven analysemethoden zijn datamining en machine learning. Met behulp van datamining kan worden gezocht naar patronen of correlaties in data, op basis waarvan conclusies kunnen worden getrokken of gebeurtenissen kunnen worden voorspeld (Hand, Mannila & Smyth, 2001; Larose, 2014; Witten & Frank, 2005). Slimme thermostaten zoals Nest[9] gebruiken dataminingtechnieken bijvoorbeeld om patronen te herkennen in voorkeuren van gebruikers. Nest leert welke temperaturen gebruikers prettig vinden, herkent wanneer gebruikers aanwezig zijn en programmeert aan de hand van deze informatie de gewenste temperatuur in huis. Machine learning kan gebruikt worden om patronen te herkennen en voorspellende modellen te maken. Het onderscheidt zich met name door zelflerend vermogen, waardoor computers dingen leren te doen waarvoor ze niet expliciet zijn geprogrammeerd (WRR, 2016). Computers kunnen bijvoorbeeld steeds beter spraak en beelden herkennen. Dit maakt het onder andere mogelijk om IoT-producten via gesproken commando's aan te sturen, denk bijvoorbeeld aan de Apple Homekit[10] of de virtuele assistent Siri[11].

Bovengenoemde analysemethoden vallen binnen het bredere onderzoeksveld van de kunstmatige intelligentie. Dit vakgebied gaat over computers die, al dan niet met behulp van zelflerend vermogen, zelfstandig (de juiste) beslissingen kunnen nemen en uitvoeren om een bepaald doel te bereiken (Russell & Norvig, 2010). Kunstmatige intelligentie was begin 2016 prominent in het nieuws door de Googlecomputer AlphaGo, die vier van de vijf Go-wedstrijden won van de regerend wereldkampioen. Lange tijd werd dit onmogelijk geacht voor computers, omdat het spel complex is en intuïtie vereist. Met name dit laatste aspect leek lang voorbehouden aan de mens.[12] Dergelijke ontwikkelingen in kunstmatige intelligentie bieden daarmee ook kansen om IoT-toepassingen nog slimmer te maken. Een mate van zelfdenkend vermogen speelt namelijk ook een rol bij veel innovatieve IoT-toepassingen. Een goed voorbeeld hiervan is de zelfrijdende auto die zelfstandig keuzes moet maken, bijvoorbeeld over de te nemen route of wat te doen in gevaarlijke situaties. In paragraaf 2.2.5 wordt de zelfrijdende auto in de context van het IoT nader toegelicht.

2.2 Onderscheidende kenmerken van het IoT

In hoofdstuk 1 is het IoT gedefinieerd als een netwerk van objecten (vaak verbonden met het internet), die gegevens verzamelen over hun omgeving, deze kunnen uitwisselen en op basis daarvan (semi)autonome beslissingen nemen en/of acties uitvoeren die van invloed zijn op de omgeving. Om meer inzicht te verschaffen in

---

8 Eerste stappen zijn hierin gezet met een app die patiënten informeert over de luchtkwaliteit, zie ook: www.longfonds.nl/nieuws/app-%E2%80%98mijn-luchtkwaliteit%E2%80%99-informeert-snel-over-smog

9 Zie ook: https://nest.com/nl

10 Zie ook: www.apple.com/ios/home

11 Aan de hand van wat de gebruiker zegt kan Siri bijvoorbeeld apparaten aan- of uitzetten. Zie ook: www.apple.com/nl/ios/siri

12 Zie ook: www.volkskrant.nl/tech/googlecomputer-wint-vijfde-en-laatste-partij-tegen-wereldkampioen-go~a4263455

wat het IoT concreet behelst, worden hieronder de volgende kenmerken uit de definitie verder toegelicht: 1) communiceren, 2) waarnemen, 3) data analyseren, en 4) (semi)autonome acties uitvoeren. Deze kenmerken zijn, zoals ook aangegeven in hoofdstuk 1, op zich niet nieuw, maar samen vatten ze de essentie van het IoT. Het IoT voegt deze combinatie van kenmerken op grote schaal aan objecten toe die deze kenmerken voorheen niet hadden. IoT-objecten en -toepassingen geven verschillend invulling aan deze kenmerken en bezitten soms niet alle kenmerken in dezelfde mate. Sommige objecten zullen bijvoorbeeld direct verbonden zijn met het internet, terwijl andere objecten onderling verbonden zijn via een lokaal netwerk en daardoor alleen indirect in verbinding staan met het internet.

De kenmerken komen overeen met de verschillende lagen van een IoT-architectuur die in meerdere bronnen worden onderscheiden: een sensorlaag, netwerklaag, middleware-laag en toepassingslaag (Al-Fuqaha et al., 2015; Cvitić, Vujić & Husnjak, 2016; Farooq et al., 2015; Li et al., 2015). Om beter inzicht te geven in de werking van het IoT wordt hieronder bij de beschrijving van de kenmerken waar mogelijk vastgehouden aan dit (meer technische) referentiekader.

2.2.1 Communiceren

Zoals de naam al suggereert, is het eerste belangrijke kenmerk van het IoT dat objecten met elkaar en vaak ook met het internet verbonden zijn en daardoor gegevens kunnen uitwisselen. Er zijn verschillende communicatietechnologieën die dit mogelijk maken. IoT-objecten zijn vaak verbonden in lokale netwerken die specifiek hiervoor zijn ontwikkeld zoals RFID[13], Zigbee[14] en LoRa[15]. Deze objecten zijn dan niet direct verbonden met het internet. De netwerklaag functioneert in deze gevallen als een router die de koppeling vormt tussen de IoT-objecten en het internet. Het doel van de netwerklaag is om de informatie verkregen uit de sensorlaag (deze wordt beschreven in paragraaf 2.2.2) door te sturen naar de middleware-laag (zie paragraaf 2.2.3.), waar de informatie kan worden verwerkt.

Om met elkaar te kunnen communiceren is de mogelijkheid om objecten uniek te identificeren cruciaal. Op deze manier kan worden afgeleid waar gegevens van afkomstig zijn en kunnen objecten individueel worden aangestuurd. Apparaten die verbonden zijn met het internet maken hiertoe gebruik van het Internet Protocol (IP). De meest gebruikte versie is op dit moment IPv4. Deze versie is echter niet

---

[13] Met RFID-technologie is het mogelijk om objecten uniek te identificeren en te laten communiceren. Dit gebeurt door gebruik te maken van RFID-tags. Deze tags kunnen gebruikt worden om informatie op te slaan en kunnen vervolgens van afstand uitgelezen worden. Dergelijke RFID-tags kunnen actief of passief zijn. Actieve tags bevatten een batterij en zenden constant informatie. Passieve tags worden pas geactiveerd als zij een signaal ontvangen en zij kunnen uit dit signaal voldoende energie halen om te functioneren zonder batterij (Atzori, Iera & Morabito, 2010; Fuhrer & Guinard, 2006).

[14] ZigBee is een open standaard voor draadloze verbindingen gebruikt voor IoT-apparaten op korte afstand. Het is langzamer, maar energiezuiniger dan andere standaarden (zoals Bluetooth) en wordt daarom veel gebruikt voor IoT-toepassingen. Zie ook: www.zigbee.org/what-is-zigbee

[15] LoRa is een netwerk technologie die in Nederland sterk in opkomst is. Door middel van LoRa is het mogelijk om IoT-objecten op grote afstand met elkaar te verbinden. KPN heeft inmiddels een volledig dekkend LoRa-netwerk opgezet in Nederland. Hierop zijn onder andere spoorwissels aangesloten en in de haven van Rotterdam zijn dieptemeters aangesloten op het netwerk. Daarnaast zijn er lokale initiatieven zoals The Things Network (zie: www.thethingsnetwork.org), waarin mensen via crowdsourcing zelf een LoRa-netwerk kunnen opzetten in hun stad of omgeving. Zie ook: http://nos.nl/artikel/2114462-kpn-heeft-landelijk-netwerk-voor-dingen-af.html.

toekomstbestendig omdat het maximumaantal uit te geven adressen nu al bijna is bereikt. De opvolger IPv6 bevat in principe oneindig veel adressen en biedt daarmee een oplossing voor het groeiende aantal objecten die met de opkomst van het IoT een uniek adres dient te krijgen. Speciaal voor het IoT is er daarnaast een speciale versie van IPv6 ontwikkelt genaamd 6LoWPAN, die ook gebruikt kan worden voor energiezuinige objecten (Atzori et al., 2010).

2.2.2 Waarnemen

Een tweede belangrijk kenmerk van het IoT is dat 'zintuigen' aan objecten worden toegevoegd waardoor ze in staat zijn hun omgeving waar te nemen. Dit gebeurt in de sensorlaag die als doel heeft om informatie te verzamelen die vervolgens geanalyseerd kan worden. Met behulp van sensoren is het mogelijk om een grote diversiteit aan parameters te meten. Hierbij kan gedacht worden aan: geluid, beeld, beweging, temperatuur, (lucht)vochtigheid, locatie en chemische samenstelling. Sensoren kunnen zo de staat van een omgeving of object waarnemen. Objecten kunnen deze informatie uiteindelijk gebruiken om beslissingen te nemen en acties uit te voeren (met behulp van actuatoren).

In deze context is het interessant om op te merken dat er op dit moment al veel sensoren en regelsystemen zitten in apparaten die nog niet verbonden zijn met een netwerk. Zo kunnen koffiemachines bijvoorbeeld al de temperatuur, waterdruk en aanwezigheid van bonen meten. Bij auto's is het mogelijk om snelheid, binnenklimaat en verschillende eigenschappen van de motor te meten. Op het moment dat deze data worden gecombineerd, geanalyseerd en mogelijk uitgewisseld, kunnen daar interessante bevindingen en toepassingen uitkomen. Door het combineren van sensordata worden auto's bijvoorbeeld in staat gesteld om zelfstandig te rijden. Dit wordt verder toegelicht in de casus in paragraaf 2.2.5.

2.2.3 Data analyseren

Een ander kenmerk van het IoT is dat er grote hoeveelheden data verzameld worden. Enerzijds worden er veel data verzameld met de sensoren die in de objecten zelf aanwezig zijn. Anderzijds kunnen, doordat de objecten *connected* zijn, data verzameld worden van externe (internet)bronnen of, door het uitwisselen van data. met andere IoT-objecten. De middleware-laag verzamelt, filtert en transformeert deze data naar één standaard. Dit maakt het mogelijk om de data te combineren en vervolgens ook te analyseren. Dit gebeurt met behulp van algoritmen die bijvoorbeeld gebaseerd zijn op datamining en machine learning (zie paragraaf 2.1.1). Dergelijke algoritmen maken het mogelijk betekenisvolle informatie en kennis te deduceren uit de verzamelde data en zo tot nieuwe inzichten te komen.

Een voorbeeld van een toepassing van data-analyse in een IoT-object kan gevonden worden in de *CowManager SensOor*, een chip die in het oormerk van een koe zit verwerkt. Onder andere bewegingssensoren in deze chip bepalen welke bewegingen de koe maakt met zijn kop. Door middel van een algoritme kan worden berekend wanneer en hoeveel gras er door de koe wordt gegeten, aan de hand waarvan de gezondheid en productiviteit van de koe kan worden bepaald (Castermans, Feijth, Verheij, Beekhuizen & Wong-A-Tjong, 2014).

2.2.4 (Semi)autonome acties uitvoeren

Het IoT draait niet alleen maar om het krijgen van inzicht, maar heeft ook toegevoegde waarde doordat het de omgeving (indirect) kan beïnvloeden. Het laatste kenmerk van het IoT is dan ook dat objecten acties kunnen uitvoeren. IoT-objecten bevatten vaak actuatoren die acties uitvoeren die van invloed zijn op de omgeving of het object zelf, bijvoorbeeld door het zenden van geluid, licht of radiogolven (Whitmore et al., 2015). Enerzijds kunnen dergelijke acties geïnitieerd worden door een gebruiker die het object van afstand bedient en anderzijds door het object zelf of een andere object (doordat het zelf beslissingen kan nemen). Het gaat hier dus om zowel handmatige als automatische acties. Beiden worden hieronder toegelicht.

In het geval van handmatige bediening wordt de beslissing voor het uitvoeren van een actie genomen door de gebruiker. De gegevens die door sensoren worden gemeten worden dan teruggekoppeld naar de gebruiker met behulp van een toepassingslaag, bijvoorbeeld via een applicatie op een smartphone. De gebruiker kan vervolgens beslissen of het gewenst is om actie te ondernemen. In sommige gevallen kan de gebruiker dan via een smartphone of tablet het IoT-object op afstand besturen. Bekende voorbeelden zijn slimme lampen en andere IoT-objecten in en om het huis.

In sommige IoT-apparaten zijn deze acties geautomatiseerd en zijn de apparaten in staat om autonome beslissingen te nemen. Een goed voorbeeld is slimme straatverlichting die automatisch uitgaat op het moment dat er geen verkeer is. Een andere toepassing kan gevonden worden in de systemen van waterschappen. Deze systemen zijn in staat om realtime complexe infrastructuren te monitoren en besturen, zodat er op ieder moment van de dag autonoom kan worden gereageerd. Zo is het mogelijk om sluizen en pompen automatisch te bedienen, wat de reactiesnelheid bij calamiteiten verhoogt (Castermans et al., 2014).

2.2.5 Casus: zelfrijdende auto's

Hieronder worden de verschillende beschreven kenmerken met een concreet voorbeeld nogmaals toegelicht. Er is gekozen voor de zelfrijdende auto aangezien dit een sprekend voorbeeld is van de integratie van alle kenmerken van het IoT in een alledaags product.

Een zelfrijdende auto is een auto die van A naar B kan rijden, zonder dat de inzittende iets hoeft te doen. Experts geven aan dat het niet lang meer zal duren voordat auto's de eerste grote wearable computers vormen (Gitlin, 2014; Thierer, 2015). Op dit moment vinden er al verschillende testen en pilots plaats met (semi-) zelfrijdende auto's.[16] Bekende voorbeelden zijn de zelfrijdende auto van Google[17] en de (deels) zelfrijdende auto's van Tesla[18]. Om volledig zelfstandig te kunnen rijden moet een auto alle kenmerken van het IoT bevatten: hij moet kunnen communiceren en waarnemen, data kunnen analyseren en zelf autonome acties kunnen uitvoeren.
Een zelfrijdende auto is verbonden met andere auto's binnen een netwerk en daarnaast bijvoorbeeld met de smartphone van de gebruiker en met stoplichten op de route. Sensoren (zoals camera's) op de auto nemen de omgeving waar en meten

[16] Zie ook: http://nos.nl/artikel/2093139-succesvolle-test-met-zelfrijdende-auto-s-op-de-a2.html en http://nos.nl/artikel/2126659-uber-klant-kan-zelfrijdende-taxi-krijgen-met-iemand-achter-het-stuur.html

[17] Zie ook: www.google.com/selfdrivingcar

[18] Zie ook: www.tesla.com/autopilot

allerlei relevante parameters. Bij de Google Car wordt de gehele omgeving bijvoorbeeld gescand door een camera op de auto die vijf keer per seconde om zijn as draait. Op deze manier wordt de omgeving digitaal in beeld gebracht en kan de auto zich aanpassen aan de omgeving. Deze grote hoeveelheid data wordt vervolgens realtime gedeeld met andere auto's en apparaten. Dit maakt het voor de auto mogelijk om te bepalen waar hij zich bevindt ten opzichte van de omgeving en waar andere objecten zich bevinden ten opzichte van de auto. Hierdoor zal de auto binnen zijn baan op de weg blijven en niet botsen met andere auto's. Deze eigenschappen zorgen ervoor dat de zelfrijdende auto volledig autonoom, veilig kan rijden. De auto onderneemt zelfstandig acties, zoals gas geven en remmen. Daarnaast kan de auto reageren op informatie van buitenaf of impulsen van de omgeving. Hij kan bijvoorbeeld op basis van gegevens uit de agenda van de gebruiker de auto van tevoren opwarmen en de ruiten ontdooien. Als een andere auto te dichtbij komt, kan hij remmen en hem proberen te ontwijken indien nodig. Een zelfrijdende auto kan naast (gebruiks)gemak daarom ook een vorm van veiligheid aan de gebruiker bieden.

2.3 Toepassingen van het IoT

De voorbeelden in dit hoofdstuk hebben al laten zien dat het IoT op veel verschillende manieren kan worden gebruikt. In de literatuur zijn verschillende classificaties voorgesteld om deze toepassingen in te delen (Atzori et al., 2010; Manyika et al., 2015; Oriwoh & Conrad, 2015; Stratix, 2015; Vermeulen, 2016). In dit rapport wordt een indeling gehanteerd die gerelateerd is aan de verschillende niveaus waarop het IoT kan worden toegepast. Hierbij gaat het daarbij om 1) het lichaam, 2) de woon- en werkruimte, 3) de stad en 4) het land. Dit wordt in figuur 2.1 schematisch weergegeven. Deze indeling laat zien hoe het IoT in alle lagen van de samenleving geïntegreerd kan worden en illustreert bovendien dat het potentieel verstrekkende gevolgen kan hebben.

Figuur 2.1 Toepassingen van het IoT verdeeld op het niveau van het lichaam, de woon- en werkruimte, de stad en het land

Het eerste niveau bevat IoT-toepassingen die op of om het lichaam worden gebruikt. Hierbij gaat het om *wearables* die op het lichaam worden gedragen, zoals een *fitness tracker* of een *smartwatch*, die informatie geven over vitale functies zoals iemands hartslag.[19] IoT-toepassingen kunnen zich ook in het lichaam bevinden, zoals pacemakers die verbonden zijn met het internet om zowel de gebruiker als behandelend arts te waarschuwen als er onregelmatigheden zijn.[20]

Het tweede niveau wordt gevormd door toepassingen die zich in en om woon- en werkruimtes bevinden. In het huis kan het gaan om smart-home-toepassingen zoals slimme verlichting die via het internet aan of uit te zetten is.[21] Een ander voorbeeld zijn sensoren die lekkages kunnen waarnemen en gebruikers hierover kunnen waarschuwen op afstand.[22] Om het huis kan het gaan om zonnepanelen verbonden met slimme meters, waardoor leveranciers inzicht krijgen in hoeveel stroom er moet worden bijgeproduceerd (Borgia, 2014; Yan, Qian, Sharif & Tipper, 2013). Soortgelijke toepassingen kunnen ook in kantoorruimtes worden ingezet. In de industrie (in deze context vaak aangeduid als smart industry) kunnen met behulp van het IoT, processen effectiever worden ingericht. Sensoren in machines maken het bijvoorbeeld mogelijk om preventief onderhoud uit te voeren (Atzori et al., 2010; Al-Fuqaha et al., 2015; Borgia, 2014).

Het derde niveau omvat toepassingen die binnen een stad worden gebruikt (in deze context vaak aangeduid als smart cities). Het idee achter dit concept is dat informatie – verzameld door sensoren in de stad – wordt gebruikt om steden schoner, veiliger, beter bereikbaar en aantrekkelijker te maken voor burgers en bedrijven. Hierbij gaat het om concrete toepassingen zoals slimme straatverlichting die zich aanpast aan de omstandigheden.[23] Een ander voorbeeld zijn slimme vuilniscontainers die kunnen waarnemen dat ze vol zijn en dit kunnen communiceren naar de gemeente. Hierdoor kunnen vuilnisophaalroutes worden geoptimaliseerd en kunnen ongemakken voor omwonenden worden verkleind (Whitmore et al., 2015; Zanella, Bui, Castellani, Vangelista & Zorzi, 2014).

Het vierde niveau bevat toepassingen die op landsniveau (en eventueel ook grensoverschrijdend) worden gebruikt. Hier kan worden gedacht aan sensoren die informatie verzamelen over de staat van de infrastructuur, zoals dijken en wegen. Sensoren in dijken kunnen onder andere de waterspanning, temperatuur en meteorologische informatie meten en doorgeven via het internet. Met deze informatie kan worden bepaald hoe stabiel de dijken zijn, zodat tijdig maatregelen genomen kunnen worden.[24] Sensoren in het wegdek kunnen onder andere waarnemen hoe druk het is en hoe zwaar beladen auto's zijn (Brous & Janssen, 2015). Met deze data kunnen met het internet verbonden auto's hun routes optimaliseren en kan door Rijkswaterstaat effectief worden opgetreden tegen te zwaar beladen auto's.

Een aantal IoT-toepassingen en –diensten beslaat meerdere niveaus. De zelfrijdende auto zal bijvoorbeeld zowel op stads- als landsniveau worden gebruikt. Daarnaast kan de auto in de toekomst ook dienen als opslag van duurzame energie voor het

[19] Zie ook: www.apple.com/nl/apple-watch-series-2

[20] Zie ook: www.pandasecurity.com/mediacenter/security/internets-new-heartbreak

[21] Zie ook: www.meethue.com/nl-nl

[22] Zie ook: www.homewizard.nl/homewizard-watermelder

[23] Zie ook: www.tudelft.nl/onderzoek/thematische-samenwerking/delft-research-based-initiatives/delft-energy-initiative/innovatie/intelligente-straatverlichting/

[24] Zie ook: www.floodcontrolijkdijk.nl/

huis (Van Soest, 2015). Een toepassing op het niveau van wearables is zelfs denkbaar, namelijk wanneer via een smartwatch het commando gegeven kan worden om een auto te laten voorrijden. De indeling op deze niveaus illustreert hoe het IoT ons leven op meerdere aspecten ingrijpend kan beïnvloeden. Het laat bovendien zien hoe IoT-toepassingen zich niet eenvoudig in één domein of niveau laten indelen. Dit maakt het lastiger om het IoT te reguleren en om rekening te houden met de belangen van alle verschillende stakeholders. Mogelijke handelingsperspectieven voor het IoT worden beschreven in hoofdstuk 4. Maar eerst worden in het volgende hoofdstuk de kansen en bedreigingen van het IoT besproken.

3 Kansen en bedreigingen

Zoals al beschreven in de voorgaande hoofdstukken, zal de opkomst van het IoT economische en maatschappelijke veranderingen veroorzaken. Dit hoofdstuk geeft een overzicht van de kansen en bedreigingen die de groei van het IoT met zich meebrengt. Zoals besproken in de inleiding van dit rapport (zie hoofdstuk 1) is ervoor gekozen om de kansen en bedreigingen van het IoT voor de maatschappij in kaart te brengen aan de hand van menselijke waarden zoals privacy, veiligheid en duurzaamheid. Hierbij vormen kansen positieve effecten van IoT-toepassingen op menselijke waarden en bedreigingen de negatieve effecten op deze waarden. De daarbij gehanteerde methodologie is beschreven in het eerste hoofdstuk (paragraaf 1.2.3). De verschillende gebieden en domeinen waarin het IoT wordt toegepast, kennen hun eigen kansen en bedreigingen en ook de impact van deze kansen en bedreigingen zal verschillen. Veiligheidsrisico's zullen bij slimme lampen bijvoorbeeld een minder grote rol spelen dan bij zelfrijdende auto's. In dit hoofdstuk worden de kansen en bedreigingen echter in brede context beschreven en wordt niet ingegaan op de individuele impact van verschillende IoT-toepassingen.

De opbouw van dit hoofdstuk is als volgt. In paragraaf 3.1 worden de kansen besproken aan de hand van de waarden: welzijn (gemak, gezondheid en veiligheid), duurzaamheid, productiviteit en welvaart. In paragraaf 3.2 worden vervolgens de bedreigingen behandeld aan de hand van de waarden: veiligheid, privacy, welvaart, welzijn, gelijkwaardigheid en autonomie. Ten slotte wordt in paragraaf 3.3 een samenvatting van de belangrijkste kansen en bedreigingen gegeven.

3.1 Kansen

Met een groeiende hoeveelheid aan verbonden IoT-apparaten die sensoren bevatten, zullen er steeds meer gegevens worden uitgewisseld en verzameld. Er komt informatie beschikbaar die voorheen niet voorhanden was en metingen zullen ook nog eens in realtime plaatsvinden. Relevante informatie is daardoor steeds vaker snel, altijd en overal beschikbaar. Dit maakt dat het IoT kan profiteren van ontwikkelingen op het gebied van big-data-analysemethoden en tegelijkertijd zelf ook kan zorgen voor impulsen voor deze ontwikkelingen. Met deze methoden kan er slimmer gebruik worden gemaakt van de data verkregen uit IoT-apparaten. Door het combineren, analyseren en interpreteren van deze data, kunnen processen transparanter worden en kunnen nieuwe inzichten worden verkregen. Een voorbeeld hiervan is dat metingen van onder andere luchtkwaliteit, weer en verkeer hebben geleid tot meer inzicht in de effecten van verschillende gebeurtenissen op luchtkwaliteit.[25]

Inzicht en transparantie hebben op zichzelf grote waarde, maar ze kunnen op hun beurt ook bijdragen aan betere en weloverwogen beslissingen (zowel door IoT-apparaten zelf, als door overheden, bedrijven en burgers) en zijn daarmee ook voorwaarde voor het succes van verschillende IoT-toepassingen. In deze paragraaf worden inzicht en transparantie daarom niet als opzichzelfstaande waarden besproken, maar in relatie tot de waarden die door toenemende inzicht en transparantie worden bevorderd, namelijk: welzijn (gemak, gezondheid en veiligheid), duurzaamheid, productiviteit en welvaart.

[25] Zie ook: www.knmi.nl/kennis-en-datacentrum/dossier/luchtkwaliteit

3.1.1 Welzijn

Zoals hierboven gezegd, bieden IoT-apparaten toegang tot informatie die voorheen niet altijd even gemakkelijk toegankelijk was. Met behulp van deze informatie kunnen levens gemakkelijker, gezonder en veiliger gemaakt worden en op die manier het welzijn van individuen vergroten. Soms stellen IoT-toepassingen mensen in staat om dingen te doen die ze voorheen niet (zelf) konden doen. Op deze manier heeft de komst van het IoT ook invloed op het welzijn van mensen in de zin dat ze onafhankelijker worden. Uit onderzoek van de EU blijkt bijvoorbeeld dat een samenwerkingsverband tussen GreenPeak en ZTE Health het mogelijk maakt dat ouderen in Nederland langer thuis kunnen blijven wonen doordat verzorgers en familie ze op afstand in de gaten kunnen houden.[26]

Het IoT kan bijdragen aan een verhoogd levensgemak in diverse toepassingsgebieden. In huis zijn er verschillende processen die geautomatiseerd kunnen worden. Slimme systemen kunnen bijvoorbeeld 's ochtends het licht aandoen, de douche aanzetten en koffie klaarmaken. Ook kunnen deze systemen zelf leren wanneer ze de verwarming aan moeten zetten, wat de favoriete tv-programma's van de gebruiker zijn en hoe ze met muziek en licht de juiste sfeer kunnen creëren (Hsu & Lin, 2016; Cook et al., 2003). Uit onderzoek blijkt dat automatisering van huishoudelijk werk in een gemiddeld huishouden een tijdsbesparing van ongeveer honderd uur per jaar kan opleveren (Manyika et al., 2015). Daarnaast kunnen smartwatches bijdragen aan gemak doordat ze het mogelijk maken om direct via een horloge om de pols te reageren op binnengekomen berichten of telefoontjes. Een ander voorbeeld van een comfort verhogende wearable is het door Microsoft en MIT ontwikkelde DuoSkin plakplaatje dat kan functioneren als tijdelijke touchpad of bedieningspaneel.[27] Het IoT kan ook bijdragen aan welzijn en gemak op stadsniveau. Sensoren kunnen onder andere worden ingezet om steden beter bereikbaar en aantrekkelijker te maken voor burgers. Een IoT-toepassing die zich richt op het gemak van de burger is het herkennen en tonen van lege fietsparkeerplaatsen om het vinden van een plek te vergemakkelijken.[28]

Ook op het gebied van gezondheid kan het IoT op verschillende toepassingsniveaus een bijdrage leveren. De eerder genoemde wearables, zoals smartwatches, activity trackers en *smart glasses*, kunnen een positieve invloed hebben op gezondheid. Het bieden van informatie en coaching op het gebied van bewegings-, slaap-, of eetpatronen kan namelijk helpen om een gezondere levensstijl aan te meten (Beaudin, Intille & Morris, 2006; Kong, Beresford & Alfano, 2012; Silver, Wallenstein & Levy, 2012; Swan, 2013). Dit sluit aan bij de bredere *Quantified Self*-beweging, waarin individuen via wearables gegevens vastleggen over zichzelf en hun omgeving om hiervan te leren en hun gedrag te optimaliseren (Swan, 2013). Om gebruikers daarbij te helpen, kunnen activity trackers bijvoorbeeld doelstellingen aanbieden bij het fitnessen die gebruikers ertoe aanzetten om meer te bewegen. In huis kunnen systemen de kwaliteit van leven voor mensen met beperkingen of chronische ziektes verbeteren en zo gezondheid bevorderen. Mensen met een visuele, auditieve of fysieke beperking kunnen bijvoorbeeld door middel van sensoren en automatisering worden geholpen bij hun dagelijkse activiteiten (Domingo, 2012). Daarnaast profiteert de gezondheidzorg van verschillende IoT-toepassingen. Door patiënten in

[26] Zie ook: www.greenpeak.com/Company/PressReleases/PR201503ContractZTEHealth.html

[27] Zie ook: www.nu.nl/tech/4308282/microsoft-en-mit-ontwikkelen-aanrakingsgevoelige-huidstickers.html en http://duoskin.media.mit.edu

[28] Zie ook: www.smartdatacity.org/axis-slim-fietsparkeersysteem-via-netwerkcamera

ziekenhuizen beter in de gaten te houden kunnen risicovolle situaties veel eerder van tevoren voorspeld worden (Healey, Pollard & Woods, 2015).

Ten slotte kan het IoT bijdragen aan welzijn door het veiliger maken van de directe leefomgeving en het publieke domein. Zo zijn er verschillende IoT-toepassingen die gericht zijn op het veiliger maken van woningen. IoT-sensoren en -camera's kunnen bijvoorbeeld gevaren en inbraken detecteren. Daarnaast zijn er ook al slimme rook- en koolmonoxidemelders op de consumentenmarkt beschikbaar.[29] Ook wearables kunnen bijdragen aan veiligheid, bijvoorbeeld door middel van babyfoons die dankzij wearables het slaappatroon, de lichaamstemperatuur en slaappositie van een baby monitoren, en notificaties daarover naar de smartphone van de ouders sturen (Stratix, 2015). Een voorbeeld van een IoT-toepassing op stadsniveau gericht op veiligheid is het uitrusten van lantaarnpalen met sensoren zodat zij zich kunnen aanpassen aan de behoefte van dat moment.[30] In dit kader is het ook relevant dat de Nationale Politie, ten behoeve van de uitvoering van de politietaak, voornemens is gebruik te maken van de data die worden gegenereerd door dergelijke sensoren.[31] Dat betekent dat de data zullen worden gebruikt ten behoeve van handhaving, opsporing en hulpverlening.

3.1.2 Duurzaamheid

Een andere waarde die IoT-toepassingen kunnen bevorderen is duurzaamheid. De VN-commissie Bruntland heeft duurzame ontwikkeling destijds gedefinieerd als een 'ontwikkeling die aansluit op de behoeften van het heden zonder het vermogen van toekomstige generaties om in hun eigen behoeften te voorzien in gevaar te brengen' (Bruntland et al., 1987, p. 41). Het gaat dus om een evenwicht tussen ecologische, economische en sociale belangen. Uit onderzoek van PwC (2014) blijkt dat de energiesector het IoT omarmt. In de VS investeert bijvoorbeeld 32% van de bedrijven in de energiesector in IoT-oplossingen. Dergelijke ontwikkelingen zien we ook in Nederland. Hieronder wordt nader ingegaan op het effect van het IoT op duurzaamheid, gerelateerd aan smart homes, smart grids, smart cities en de circulaire economie.

Hoewel het IoT in huis nu vaak nog een groot 'gadget-gehalte' heeft (zie ook de voorgaande paragraaf) kan het wel degelijk bijdragen aan besparingen van bijvoorbeeld energie en water. Op basis van klantgegevens van Google Nest in Nederland blijkt naar eigen zeggen dat een besparing van 11,9% tot 19,9% mogelijk is door gebruik van de slimme Nest thermostaat.[32] Met het oog op de milieudoelstellingen is het inmiddels een streven om in 2020 alle huishoudens te voorzien van een slimme meter.[33] Deze slimme energiemeters zijn verbonden met het netwerk van de netbeheerder en kunnen in principe op afstand uitgelezen worden. Door deze meters te koppelen aan applicaties, websites, een afleesbaar scherm in huis, of een (slimme) thermostaat kan realtime inzicht verkregen worden in het energieverbruik van een consument (of klein bedrijf). Een bekend voorbeeld van een applicatie die gebruikt maakt van slimme meters is Toon. Deze applicatie van Eneco combineert het monitoren van het energieverbruik van verschillende individuele producten (gas en elektra) met een slimme thermostaat die de temperatuur in huis kan meten en

[29] Zie ook: https://nest.com/nl/smoke-co-alarm/meet-nest-protect

[30] Zie ook: www.eindhoven.nl/inwonersplein/leefomgeving/slim-licht.htm

[31] Tweede Kamer 2015–2016, 29 628, nr. 594, Bijlage Beleidsvisie Sensing.

[32] Zie ook: https://nest.com/nl/support/article/eu-savings

[33] Zie ook: http://nos.nl/artikel/2011515-meer-mensen-krijgen-een-slimme-energiemeter.html

aanpassen. Andere IoT-toepassingen in smart homes die bijdragen aan duurzaamheid zijn bijvoorbeeld apparaten die waterlekkages detecteren (Farooq et al., 2015) en waterkwaliteit monitoren (Gubbi et al., 2013).

Een andere ontwikkeling gerelateerd aan het IoT en duurzaamheid is die van de zogenoemde smart grids. Een smart grid is een intelligent energienet waaraan een meet- en regelsysteem is toegevoegd om vraag en aanbod beter op elkaar af te stemmen. Met de komst van elektrische auto's kan bijvoorbeeld het moment van opladen worden aangepast aan de belasting van het net (als alle auto's tegelijk opladen is dit in één keer een (te) grote belasting). Auto's kunnen ook stroom (tijdelijk) opslaan en terugleveren zodat overbelasting wordt voorkomen en ingespeeld wordt op variabele prijzen (Yan et al., 2013). Een smart grid maakt het daarnaast mogelijk om variabele prijzen aan te bieden, afhankelijk van het gebruik en aanbod (Stratix, 2015). Intelligent gebruik van de door de sensoren in de smart grid verzamelde informatie maakt het tevens mogelijk om het netwerk te optimaliseren en effectief onderhoud te plannen (Wang, Lin, Zhang & Ma, 2012). Daarnaast kan de belasting van het netwerk beter worden beheerd, op tijd op problemen worden gereageerd en dus overbelasting worden voorkomen (Borgia, 2014; Yan et al., 2013).

Ook smart cities kunnen een bijdrage leveren aan duurzaamheid. Het gebruik van het IoT in smart cities kan een hulpmiddel zijn om de klimaatdoelstellingen te verwezenlijken.[34] Allereerst kan het IoT inzichtelijk maken wat het energiegebruik is van lokale diensten, denk bijvoorbeeld aan straatverlichting, transportdiensten en camera's. Op basis hiervan kan geprioriteerd worden welke diensten efficiënter kunnen worden ingericht (Zanella et al., 2014). Daarnaast kan het gebruik van IoT-toepassingen in publieke diensten, zoals slimme straatverlichting, directe energiebesparing opleveren. Slimme lantaarnpalen met ledlampen kunnen bijvoorbeeld het licht dimmen als er niemand in de buurt is, wat een energiebesparing kan opleveren van 50 tot 80 procent.[35] Verder kunnen sensoren in de stad de luchtkwaliteit meten, zodat gepaste maatregelen kunnen worden genomen als deze te ver achteruit gaat (Farooq et al., 2015; Miorandi, Sicari, De Pellegrini & Chlamtac, 2012; Zanella et al., 2014). Auto's zouden dan bijvoorbeeld automatisch kunnen worden geweerd of omgeleid uit een gebied.

Ten slotte speelt het IoT een belangrijke rol bij het realiseren van een circulaire economie. In een circulaire economie wordt geen afval of vervuiling geproduceerd en worden materialen volledig hergebruikt. Doordat in het IoT steeds meer apparaten aan het internet gekoppeld zijn, wordt het mogelijk om informatie te krijgen over energiegebruik en stromen van grondstoffen en producten. Hiermee kunnen bedrijven en overheden verspilling tegengaan en middelen effectiever inzetten (Ellen Macarthur Foundation, 2016). Het kabinet heeft de ambitie uitgesproken dat Nederland in 2050 een volledig circulaire economie heeft (Dijksma, 2016).

3.1.3 Productiviteit

In het bedrijfsleven vormt het maximaliseren van productiviteit een belangrijke sleutel voor het verbeteren van de concurrentiepositie. Arbeidsproductiviteit gaat over het aantal eenheden (producten of diensten) dat per werknemer per tijdseenheid wordt geproduceerd. Het IoT kan op verschillende manieren bijdragen aan het verhogen van productiviteit. Een grote meerwaarde van het gebruik van IoT-toe-

[34] Zie ook: www.rijksoverheid.nl/onderwerpen/klimaatverandering/inhoud/klimaatbeleid

[35] Zie ook: www.volkskrant.nl/archief/slimme-lantaarnpaal-dimt-als-er-niemand-is~a1827057

passingen voor bedrijven is dat er veel meer informatie verzameld kan worden over bedrijfsprocessen dan voorheen. Dit kan helpen bij het optimaliseren van processen, het doen van voorspellingen en het nemen van besluiten. Hieronder wordt stilgestaan bij een aantal toepassingen die processen verbeteren of versnellen in de logistiek, productie en landbouw.

Met name in de logistieke sector wordt het IoT al veelvuldig toegepast om processen te optimaliseren. Het gebruik van het IoT binnen de logistiek is niet nieuw, maar kan sinds kort op veel grotere schaal worden toegepast (Whitmore et al., 2015). Met behulp van RFID kunnen producten door de hele bevoorradingsketen worden gevolgd. Hierdoor wordt het mogelijk om voorraadbeheer efficiënter in te richten, bijvoorbeeld door kleinere voorraden aan te houden (Atzori et al., 2010; Whitmore et al., 2015).

Met behulp van sensoren en RFID-tags kunnen ook productieprocessen worden geoptimaliseerd. Onderdelen worden daarbij gekoppeld aan processen zodat machines automatisch weten welke handelingen uitgevoerd moeten worden bij een bepaald onderdeel. Daarnaast is het mogelijk om realtime de voortgang van het productieproces en problemen daarin te monitoren. Hierdoor kunnen bijvoorbeeld snel defecte onderdelen worden opgespoord en bijgemaakt, zodat het productieproces niet wordt verstoord (Atzori et al., 2010; Stratix, 2015). Daarnaast is het mogelijk om het functioneren van machines op afstand te monitoren en eventueel preventief onderhoud uit te voeren. Machines kunnen indien nodig zichzelf automatisch uitschakelen, terwijl een monteur op de hoogte wordt gesteld van het functioneren van de machine (Atzori et al., 2010; Al-Fuqaha et al., 2015; Borgia, 2014).

In de landbouw kan het IoT bijdragen aan de ontwikkeling van precisielandbouw, waarbij gewassen en dieren nauwkeurig gemonitord en behandeld kunnen worden. Door gebruik te maken van sensoren kunnen bijvoorbeeld verschillen in bodem- en gewaseigenschappen, gewasmicroklimaat en dichtheden van onkruiden, ziekten en plagen worden waargenomen (Bos & Munnichs, 2016; Kempenaar, 2010). Veehouders kunnen via een smartphone of tablet nauwkeurig bijhouden wat de prestaties zijn van individuele dieren (bijvoorbeeld de melkgift, vruchtbaarheid en aanwezigheid van dierziekten), groepen van dieren (bijvoorbeeld de groei van biggen) en hun fysieke omgeving (zoals het binnenklimaat in de stal en de kwaliteit van het grasland) (Bos & Munnichs, 2016). Dit kan eraan bijdragen dat opbrengsten verhoogd worden, terwijl de milieueffecten kleiner worden. Deze ontwikkeling draagt daarom, naast productiviteit, ook bij aan de eerder beschreven waarde duurzaamheid.

3.1.4 Welvaart

Zoals beschreven in hoofdstuk 1, zijn de verwachtingen van het positieve effect van het IoT op de economie hooggespannen. Hoewel deze voorspellingen flink uiteen lopen, is het duidelijk dat het IoT economische kansen biedt voor Nederland. Hierbij valt onder andere te denken aan het ontwikkelen van nieuwe producten, diensten, verdienmodellen (bijvoorbeeld product-dienstcombinaties) en banen. Hieronder worden deze economische kansen kort besproken.

Allereerst levert het ontwikkelen en produceren van nieuwe producten, die onderdeel uitmaken van het IoT, mogelijkheden op voor het bevorderen van de welvaart. Bekende IoT-producten voor consumenten die in Nederland zijn ontwikkeld, zijn Philips Hue (slimme lampen) en Toon (slimme thermostaat). Ook voor de industrie en landbouw worden IoT-producten ontwikkeld door Nederlandse bedrijven (Smit,

Peters, Kemps, Vos & Sterk, 2016).[36] Daarnaast biedt het IoT kansen voor de software-industrie. De softwaresector droeg in 2014 al 3,4% bij aan het bruto binnenlands product (BBP) van Nederland (Te Velde, Veldkamp & Janswhitmaasen, 2014). De komst van het IoT biedt kansen om deze markt verder te laten groeien, bijvoorbeeld door besturingssystemen of software te ontwikkelen voor IoT-producten of, zoals hieronder nog zal worden besproken, door het aanbieden van *software as a service*.

Hoewel de verkoop van nieuwe IoT-producten op zichzelf kansen voor het Nederlandse bedrijfsleven oplevert, zal de grootste meerwaarde voor bedrijven liggen in de (nieuwe) diensten die gepaard gaan met deze producten. Door het aanbieden van aanvullende diensten (al dan niet door middel van een abonnement), kan ook na verkoop van het product geld verdiend blijven worden. Voor de slimme thermostaat Toon geldt bijvoorbeeld dat een groot deel van de functionaliteit niet wordt geleverd door het product zelf, maar wordt verkregen met behulp van een aanvullend abonnement.[37] Ook kan worden gedacht aan machinebouwers die machines met sensoren produceren en niet alleen de machine zelf verkopen, maar ook aanvullende diensten leveren zoals *predictive maintaince* en onderhoud op afstand (Smit et al., 2016). Een ander voorbeeld is het aanbieden van diensten of abonnementen gericht op het monitoren en beveiligen van IoT-apparaten. Daarmee verschuift met de opkomst van het IoT de nadruk van het periodiek verkopen van nieuwe (vaak dezelfde) producten aan consumenten naar het binden van consumenten voor langere tijd (Langley, 2015).

De komst van het IoT kan tevens bestaande dienstverlening verbeteren. Eerder werden al predictive maintenance en onderhoud op afstand genoemd. Een ander voorbeeld is te vinden in de detailhandel, waar producten en diensten geïndividualiseerd kunnen worden aangeboden. Zo kunnen gepersonaliseerde aanbiedingen worden gedaan in de winkel, maar kan ook meer informatie worden gegeven over de beschikbaarheid en locatie van producten via zogenaamde *smart shelves* (Gregory, 2015).

Het groeiende belang van dienstverlening neemt verschillende vormen aan (Castermans et al., 2014) en uit zich in een aantal verdienmodellen die een beweging van bezit naar gebruik van producten laten zien. Hieronder worden, zonder uitputtend te zijn, drie van deze verdienmodellen besproken. Het eerste verdienmodel sluit aan bij de ontwikkelingen op het gebied van *product as a service* en de 'deeleconomie' (CPB & PBL, 2015; Frenken, 2015). Een bekend voorbeeld van een platform voor deeleconomie is Airbnb, waar mensen hun huis tijdelijk kunnen verhuren, of Peerby, waar spullen kunnen worden uitgeleend aan buurtbewoners. Met de komst van het IoT zal het makkelijker worden om dit concept ook op andere gebieden toe te passen. Als voorwerpen verbonden zijn met het internet kan makkelijker worden bepaald wie wel of geen gebruik van deze voorwerpen kan maken en ook transacties kunnen eenvoudig worden afgehandeld via digitale platformen. Specifiek voor het IoT kan worden gedacht aan het delen van (zelfrijdende) auto's, waarbij vervoer centraal komt te staan en niet het bezit van een vervoersmiddel. Een tweede verdienmodel draait om de gegevens die worden verzameld door de apparaten en sensoren binnen het IoT. Door middel van de dienst *data as a service* wordt toegang geboden tot deze data. Een bedrijf of gebruiker hoeft dan niet zelf sensoren te plaatsen en metingen te verrichten. Een voorbeeld hiervan is een slimme koelkast

[36] Zie ook: www.connecterra.io

[37] Zie ook: www.eneco.nl/toon-thermostaat/abonnement-toon

die bedrijven, bijvoorbeeld supermarkten, inzicht verschaft in de productvoorkeuren van gebruikers. In ruil daarvoor zouden gebruikers bijvoorbeeld korting kunnen krijgen op producten. Ten derde zal ook *software as a service* met de komst van het IoT een belangrijkere rol gaan spelen. Voor het aanbieden van diensten zal veelvuldig gebruik worden gemaakt van de data die het IoT genereert. Het verzamelen en verwerken van deze data kan een grote investering vergen wat betreft hardware (bijvoorbeeld de infrastructuur van servers) en software (bijvoorbeeld op het gebied van (big-)data-analysemethoden). Deze infrastructuur kan door een bedrijf als een dienst (bijvoorbeeld een *webbased* applicatie) worden aangeboden, waarmee andere bedrijven en gebruikers gegevens kunnen opslaan, verwerken en analyseren, zonder zelf deze investeringen te hoeven doen. Deze ontwikkeling hangt nauw samen met de ontwikkeling van cloud computing, zoals beschreven in paragraaf 2.1.1.

De opkomst van het IoT zal ook nieuwe kansen opleveren voor de arbeidsmarkt. Historisch gezien hebben technologische revoluties, zoals de stoommachine, elektriciteit en ICT, ertoe geleid dat oude functies verdwenen en nieuwe functies ontstonden (Van Est & Kool, 2015; Went & Kremer, 2015). Voor het IoT kan dit ook gelden. Nieuwe banen kunnen enerzijds ontstaan doordat er een toenemende vraag ontstaat naar IoT-producten en daaraan gerelateerde diensten. Anderzijds kan een toenemende vraag naar bestaande goederen en diensten, die door de opkomst van het IoT goedkoper kunnen worden geproduceerd door een stijgende productiviteit (zie ook paragraaf 3.1.3), leiden tot nieuwe banen (Went & Kremer, 2015). Daarnaast zullen de ontwikkelingen op het gebied van het IoT vragen om nieuwe en andere expertise van (huidige) werknemers van bedrijven (SER, 2016). Zo komen er meer en nieuwe banen beschikbaar voor bijvoorbeeld data-analisten, veiligheidsexperts, en softwarespecialisten en -ontwikkelaars. Van Est & Kool (2015) concluderen in hun rapport *Werken aan de robotsamenleving* dat technologische ontwikkelingen tot op heden niet tot structurele crises hebben geleid op de arbeidsmarkt. Zij vervolgen dat: 'de inzet van nieuwe technieken op de arbeidsmarkt (…) wel heeft geleid tot de noodzaak om vraag en aanbod van arbeid, bijvoorbeeld via het onderwijs, beter op elkaar af te stemmen' (Van Est & Kool, 2015, p. 85). Het afstemmen van vraag en aanbod door middel van onderwijs of omscholing zal dan ook belangrijk zijn voor de arbeidsmarkt. Bedrijven die het juiste personeel in dienst hebben, hebben een voorsprong op andere bedrijven en kunnen zo kansen beter benutten en makkelijker producten en diensten op de markt brengen. Andere bedrijven (bijvoorbeeld uitzendbureaus) kunnen op deze vraag inspelen door gekwalificeerd personeel aan te bieden en op deze manier hiervan profiteren. Andere ontwikkelingen waardoor het IoT een positieve invloed kan hebben op de arbeidsmarkt zijn de krimpende beroepsbevolking en toenemende vergrijzing. Om economische groei te bewerkstelligen is Nederland daardoor aangewezen op groei van de arbeidsproductiviteit (Van Est & Kool, 2015). Het IoT kan hieraan, zoals ook beschreven in paragraaf 3.1.3, een bijdrage leveren door taken te automatiseren en efficiënter in te richten. Om deze redenen hoeft banenverlies als gevolg van de opkomst van het IoT (zie ook paragraaf 3.2.3) niet direct problematisch te zijn.

3.2 Bedreigingen

In de voorgaande paragraaf zijn verschillende toepassingen beschreven die de kansen en voordelen die het IoT biedt benadrukken. Deze zijn vooral gericht op het verkrijgen van inzicht en transparantie door het verzamelen van grote hoeveelheden (sensor)data, en het op basis daarvan beter beslissingen nemen. Het verzamelen

van grote hoeveelheden data en het steeds meer inzetten van verbonden apparaten heeft echter ook een schaduwzijde. In deze paragraaf wordt dit toegelicht aan de hand van de menselijke waarden die door de opkomst van het IoT bedreigd worden: veiligheid, privacy, welvaart, welzijn, gelijkwaardigheid en autonomie.

3.2.1 Veiligheid

De maatschappij wordt steeds afhankelijker van ICT (zie ook paragraaf 3.2.6). Het is daarom essentieel om te zorgen voor een veilig IoT. Uit de literatuur en interviews met experts en stakeholders blijkt echter dat gebrek aan een voldoende veiligheidsniveau de belangrijkste zorg over het IoT is (Goodman, 2015; FTC, 2015; Peppet, 2014). Het aantal objecten dat is verbonden met het IoT zal met een veelvoud toenemen (zie ook paragraaf 1.1). Als gevolg hiervan zullen ook het aantal veiligheidsrisico's en de impact daarvan met een veelvoud toenemen. Deze risico's kunnen vanzelfsprekend van invloed zijn op de virtuele wereld, maar met de komst van het IoT ook in toenemende mate op de fysieke wereld.[38] In deze paragraaf worden allereerst mogelijke veiligheidsrisico's van IoT-toepassingen en -apparaten besproken, vervolgens worden hieraan gerelateerde IoT-specifieke risicovergrotende factoren besproken.

Veiligheidsrisico's zijn onder te verdelen in *security*- en *safety*risico's (Aoyama, Koike, Koshijima & Hashimoto, 2013). Securityrisico's worden intentioneel veroorzaakt, bijvoorbeeld wanneer systemen gericht worden aangevallen of aangetast door kwaadwillende personen. Safetyrisico's ontstaan zonder expliciete intenties, bijvoorbeeld door menselijke fouten, ontwerpfouten of storingen. Voor beide typen risico's geldt dat ze veroorzaakt kunnen worden door een IoT-apparaat zelf, maar ook door de achterliggende infrastructuur, zoals het communicatienetwerk of de servers van de dienstverlener.

Om risico's op het gebied van security te duiden wordt vaak gebruikgemaakt van een BIV-classificatie, waarbij gekeken wordt naar de 1) beschikbaarheid, 2) integriteit en 3) vertrouwelijkheid van ICT-systemen (Whitman & Mattord, 2014). Deze classificatie wordt hieronder toegepast om securityrisico's van het IoT in kaart te brengen.

Bij beschikbaarheid gaat het erom dat gebruikers zonder obstructie toegang kunnen krijgen tot de functionaliteit van het IoT-apparaat of de daarmee verzamelde data. Securityrisico's op dit vlak zijn bijvoorbeeld het op afstand uitzetten van de motor van een auto (Greenberg, 2016) of het overnemen van slimme verlichting (McCarthy, 2016). In het Cybersecuritybeeld Nederland (NCSC, 2016) wordt daarnaast *ransomware* als een belangrijke bedreiging genoemd. Hierbij wordt een IoT-apparaat versleuteld met zogenaamde *cryptoware*, waarna losgeld geëist wordt om het apparaat weer te ontsleutelen (Goodman, 2015; Williams, 2016). Ook *denial-of-service*-aanvallen kunnen het netwerk van gebruikers behoorlijk ontregelen. Dit zijn aanvallen waarbij een grote hoeveelheid netwerkverkeer naar een computersysteem (meestal een webserver) wordt verstuurd waardoor de dienst niet meer beschikbaar is voor de gebruiker. IoT-netwerken kunnen zo platgelegd worden, in toenemende mate ook voor militaire doeleinden.[39] Kwetsbare IoT-apparaten kunnen ook zelf

[38] Zie ook: www.cio.com/article/3143094/security/iot-attacks-could-bring-real-world-damage.html

[39] Nu steeds meer objecten verbonden raken met het IoT kunnen aanvallen een nog grotere impact hebben op het functioneren van een land, bijvoorbeeld op de (met het IoT verbonden) kritieke infrastructuur van een land. Voorafgaand aan het conflict tussen Rusland en Georgië zijn DDoS-aanvallen onder meer ingezet om de

onderdeel worden van een dergelijk botnet[40] en gebruikt worden voor het uitvoeren van denial-of-service-aanvallen (FTC, 2015; Ashford, 2016; Mimoso, 2016).

Bij integriteit gaat het om het risico dat instellingen van IoT-apparaten worden aangepast en (sensor)data van IoT-toepassingen worden gewijzigd of verwijderd. Kwaadwillende personen kunnen bijvoorbeeld door de instellingen van een slimme pacemaker (een IoT-actuator) aan te passen iemands hartslag gevaarlijk verhogen, het apparaat uit schakelen of de batterij laten leeglopen (Koebler, 2015). Daarnaast kunnen sensordata worden gewijzigd waardoor een gebruiker of arts geen signaal krijgt als de hartslag onregelmatig is. Doordat IoT-toepassingen in toenemende mate autonoom (potentieel gevaarlijke) beslissingen zullen nemen is integriteit van data extra belangrijk. Zoals reeds genoemd geldt dit gevaar in grote mate voor zelfrijdende auto's (FTC, 2015).

Bij vertrouwelijkheid gaat het om het risico van ongeautoriseerde toegang van derden tot (data van) IoT-apparaten. Hier kan het bijvoorbeeld gaan om het breken van de beveiliging van een slim slot (Thomson, 2016), of het overnemen van en meekijken met slimme beveiligingscamera's (Pauli, 2016) of babyfoons (Leyden, 2016). Deze (gevoelige) gegevens kunnen worden gestolen of worden gebruikt als chantagemiddel. Ook digitale spionage door statelijke actoren zal met de komst van het IoT mogelijk een nog grotere dreiging worden dan het nu al is (NCSC, 2016). Het IoT vergroot dit risico doordat IoT-toepassingen veelal worden geleverd door buitenlandse producenten die ook de gegevens in het buitenland beheren.[41]

Zoals eerder aangegeven ontstaan veiligheidsrisico's op het gebied van safety non-intentioneel. Dergelijke risico's ontstaan bijvoorbeeld door ontwerpfouten. Daarnaast kan de kwaliteit van gebruikte onderdelen slecht zijn; IoT-apparaten met inaccurate sensoren kunnen bijvoorbeeld beslissingen nemen op basis van foutieve data. Ook disfunctionerende actuatoren van IoT-apparaten kunnen veiligheidsrisico's veroorzaken. Bij de gevolgen hiervan wordt uitgebreider stil gestaan in paragraaf 3.2.6. Een ander safetyrisico betreft de infrastructuur. Doordat IoT-oplossingen vaak worden geïmplementeerd binnen bestaande infrastructuren kunnen compatibiliteits- en interferentieproblemen ontstaan. Geïnterviewde experts geven bijvoorbeeld aan dat de slimme energiemeter in eerste instantie interfereerde met andere 4G-apparaten. Ten slotte kan er onvoorspelbaar, emergent gedrag ontstaan door interactie tussen verschillende apparaten, waarvan de mogelijke risico's niet bij voorbaat te voorspellen zijn (Roca, Nemirovsky, Nemirovsky, Milito & Valero, 2016).

Op dit moment worden er nog weinig mitigerende maatregelen genomen om bovenstaande veiligheidsrisico's te verkleinen. Basale veiligheidsmaatregelen zoals het vermijden van standaard gebruikersnamen en wachtwoorden worden nu vaak niet genomen door bedrijven, waardoor het hacken van IoT-apparaten aanzienlijk makkelijker wordt. Het Mirai-botnet bestond bijvoorbeeld uit duizenden IoT-apparaten die waren gehackt dankzij deze kwetsbaarheid.[42] In sommige gevallen is het lastig

---

communicatie van de overheid in Georgië te verstoren, zie ook: www.nytimes.com/2008/08/13/technology/13cyber.html.

[40] Zie ook: www.security.nl/posting/483530/Malware+infecteert+1+miljoen+Internet+of+Things-apparaten

[41] Zie bijvoorbeeld het in paragraaf 3.1.1 genoemde ZTE Health, wat onderdeel is van het Chinese staatsbedrijf ZTE.

[42] Zie ook: http://nos.nl/artikel/2139025-aanvallen-op-internetbedrijf-via-babyfoons-en-beveiligingscamera-s.html en https://tweakers.net/nieuws/117059/ddos-aanval-op-dns-provider-dyn-werd-uitgevoerd-met-mirai-botnet.html.

om maatregelen hiertegen te treffen. Zo hebben zeer kleine IoT-apparaten (voorals nog) beperkte computerkracht en accuduur waardoor de verbinding niet altijd met een goed wachtwoord en sterke encryptie te beveiligen is (Peppet, 2014; WP29, 2014).

Een ander probleem is dat IoT-apparaten niet altijd van updates worden voorzien, waardoor ze in de loop der tijd vatbaar worden voor nieuwe veiligheidslekken (Schneier, 2014). Doordat gebruikersinterfaces vaak ontbreken kan het lastig zijn om IoT-apparaten op een gebruiksvriendelijke manier te voorzien van nieuwe software-updates. *Over-the-air* updates worden gezien als mogelijke oplossing voor dit probleem, maar ook deze methode is vatbaar voor misbruik door kwaadwillende personen.[43] Ook als voor deze problematiek een oplossing wordt gevonden, bestaat er het risico dat de ondersteuning van IoT-apparaten na een aantal jaar afloopt. Sommige smart-tv's zijn bijvoorbeeld gebaseerd op het Android-besturingssysteem en zullen slechts een aantal jaar updates ontvangen (Libbenga, 2014). Daarna zijn ze vatbaar zijn voor de uitbuiting van kwetsbaarbaarheden (Peppet, 2014).[44]

3.2.2 Privacy

IoT-toepassingen kunnen op verschillende manieren de privacy van mensen bedreigen. Hieronder worden eerst de belangrijkste risico's met betrekking tot het verzamelen, bewerken en gebruiken van (persoons)gegevens door IoT- toepassingen besproken. Vervolgens wordt ingegaan op moeilijkheden en aandachtspunten rondom privacybescherming.

Zoals hierboven al beschreven, genereren IoT-toepassingen grote hoeveelheden gegevens. Vaak gaat het hierbij om persoonsgegevens, die gevoelig van aard kunnen zijn. Een voorbeeld hiervan zijn gezondheidsgegevens die verzameld worden door smartphones, wearables of interne sensoren in het lichaam. Het anonimiseren van persoonsgegevens die worden gegenereerd door IoT-toepassingen blijkt problematisch te zijn (Peppet, 2014). Daarnaast kunnen door het combineren en bewerken van ogenschijnlijk 'onschuldige' gegevens nieuwe, soms gevoelige, persoonsgegevens ontstaan (Rose et al., 2015; Hildebrandt, 2008; WRR, 2016). Het combineren en analyseren van gegevens over hartslag en bewegingssnelheid kan bijvoorbeeld resulteren in gegevens over het stressniveau, geluksniveau en de algehele gezondheid van gebruikers (Peppet, 2014).

Een groot risico van het verwerken van persoonsgegevens (afkomstig uit IoT-toepassingen) is dat op basis van (bewerkingen) van deze gegevens beslissingen worden genomen door mensen of machines. Dit kan gaan om het bieden van meer gerichte advertenties[45], maar ook om situaties waarbij mensen op basis van een gegenereerd profiel worden uitgesloten van deelname aan een overheidsprogramma of een dienst die wordt geleverd door een bedrijf. Het verwerken van persoonsgegevens kan dus leiden tot onderscheid en discriminatie op basis van gedrag (WRR, 2016). Dit is niet altijd wenselijk. Peppet (2014) wijst er bijvoorbeeld op dat prijsdiscriminatie vanuit economisch perspectief efficiënt en wenselijk kan zijn, maar dat consumenten dit vaak als onwenselijk ervaren. Verschillende andere auteurs mer-

[43] Zie ook: www.newelectronics.co.uk/electronics-blogs/over-the-air-updates-to-iot-devices-will-bring-huge-security-challenges/149124

[44] Zie ook: https://duo.com/blog/duo-analytics-android-device-security-article

[45] Zie bijvoorbeeld het in paragraaf 3.1.2. genoemde NEST, wat onderdeel uitmaakt van Google en waarvan de data mogelijk kunnen worden ingezet voor advertentiedoeleinden.

ken daarnaast op dat indien IoT-systemen en big-data-analyses vaker worden ingezet in bijvoorbeeld achterstandswijken of locaties waar veel overlast is, het systeem mogelijk bevooroordeeld raakt en sociale uitsluiting en discriminatie in de hand werkt (Custers, Calders, Schermer & Zarsky, 2013; Zarsky, 2014, 2016).

Een ander belangrijk hieraan gerelateerd risico is dat mensen ten onrechte in een gegevensset kunnen worden opgenomen, waarna beslissingen worden genomen die nadelig uitpakken voor de betrokkenen. Daarbij kan worden gedacht aan een factuur voor het gebruik van een dienst die op basis van onjuiste gegevens tot stand is gekomen of opname op een zwarte lijst van overheidsinstellingen of bedrijven op basis van onjuiste gegevens. Daar komt bij dat IoT-toepassingen en de daarop volgende big-data-analyses door gebruikers als een *black box* kunnen worden ervaren, omdat voor hen vaak onduidelijk blijft voor welke doeleinden de toepassingen in gebruik zijn, welke besluiten op basis daarvan worden genomen en welke organisatie de verantwoordelijkheid over het gebruik draagt (zie ook WRR, 2016). Hierbij wordt nadrukkelijk opgemerkt dat dergelijke analyses, en de op basis daarvan genomen beslissingen, ook binnen het bedrijfsleven plaatsvinden.

Naast bedrijven en kwaadwillende personen, biedt het IoT ook mogelijkheden voor overheidsinstanties om gegevens te verzamelen (Ackerman & Thielman, 2016). In de memorie van toelichting van de laatste versie van het voorstel voor een nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten wordt op p. 76 bijvoorbeeld expliciet opgemerkt dat 'de diensten ook slimme apparaten (zoals koelkasten, horloges, auto's e.d. die zijn uitgerust met computerfuncties) zouden kunnen hacken. Het is immers niet uitgesloten dat dergelijke slimme apparaten op enig moment gegevens verwerken die voor een goede taakuitvoering van de diensten noodzakelijk kunnen zijn'.[46] Mogelijk ontstaat ook bij de politie op den duur de wens om IoT-apparaten te kunnen hacken voor opsporings- en handhavingsdoeleinden.

Gerelateerd hieraan, maken IoT-toepassingen continue monitoring van (onder andere de bewegingen en handelingen van) individuen mogelijk en lenen deze zich daarom uitstekend voor surveillance- en spionagedoeleinden. Het IoT maakt het bijvoorbeeld mogelijk om in een winkelgebied het aantal mensen dat aan het internet verbonden apparaten bij zich heeft te tellen met sensoren die wifi- en bluetoothsignalen meten. Deze gegevens kunnen mogelijk gecombineerd worden met gegevens uit het openbaar vervoer en van verkeerscamera's (WRR, 2016). Tevens kunnen met behulp van een microfoon in een CCTV camera stemverheffingen van mensen binnen de openbare ruimte worden gemeten om een daad van agressie vroegtijdig te signaleren met behulp van speciale software (Flight, 2016). Zoals al beschreven in paragraaf 3.1.1, heeft de Nationale Politie kenbaar gemaakt dat het voornemens is sensordata te gaan gebruiken voor de uitvoering van de politietaak op eenzelfde manier als het gebruik van camerabeelden.[47]

Bovenstaande toepassingen kunnen op verschillende wijze inbreuk maken op het recht op privacy. Betrokkenen kunnen het gebruik (en misbruik) van persoonsgegevens als een ongewenste inmenging in hun persoonlijke levenssfeer ervaren. Het gevoel van mensen dat zij constant op een of andere wijze door het IoT 'bespied' worden kan een *chilling effect* met zich meebrengen. Dat wil zeggen dat mensen hun gedrag aanpassen naar aanleiding van een ingezette (of een vermeende) maatregel. Daarbij kan het gaan om mensen die publieke ruimtes zullen mijden

[46] Tweede Kamer 2016–2017, 34 588, nr. 3.

[47] Tweede Kamer 2015–2016, 29 628, nr. 594, Bijlage Beleidsvisie Sensing.

omdat daar een IoT-toepassing wordt gebruikt om de openbare orde te handhaven. Het ligt namelijk voor de hand dat in de nabije toekomst steeds meer sensoren de signalen van bijvoorbeeld mobiele telefoons zullen uitpeilen. Of mensen als gevolg daarvan daadwerkelijk bepaalde plekken of overheidsdiensten zullen vermijden is nu nog niet in te schatten.

Hildebrandt (2016) waarschuwt in haar preadvies voor de Nederlandse Juristen Vereniging dat in de nabije toekomst IoT-systemen zich als *agents* kunnen gaan gedragen die hun omgeving niet alleen waarnemen maar ook kunnen ingrijpen. Daarbij zal niet altijd tijd zijn voor het maken van een menselijke afweging (WRR, 2016). Dat kan consequenties hebben voor de vraag of iemand terecht als 'overtreder' of 'verdachte' door een dergelijk systeem wordt aangemerkt. IoT-toepassingen zullen echter niet alleen in de publieke ruimte worden ingezet, maar ook binnenshuis en mogelijk in het lichaam. Mogelijke privacyschendingen zullen daarbij per ruimte of, anders gezegd, per context van elkaar verschillen (Rose et al., 2015).

Om bovenstaande privacyschendingen tegen te gaan, bestaat er wet- en regelgeving zoals de Wet bescherming persoonsgegevens (Wbp),[48] maar deze blijkt er niet altijd toe in staat om privacy te beschermen. IoT-toepassingen en de daaraan gerelateerde big-data-toepassingen verhouden zich namelijk niet altijd goed tot bestaande wetgeving. Het doelbindingsprincipe uit de Wbp gaat bijvoorbeeld het gebruik van gegevens voor een ander doel dan waarvoor de gegevens oorspronkelijk zijn verzameld, zogenoemde *function creeps*, tegen (WRR, 2016). Bij IoT-toepassingen is het doel van de verwerking van gegevens echter niet altijd van tevoren helder, zeker als het verdienmodel berust op big-datatoepassingen. Juist het analyseren van eindeloos veel combinaties van gegevens levert een grote meerwaarde op (WRR, 2016). Het noodzakelijkheidsvereiste uit de Wbp stelt onder andere dat gegevensverwerking noodzakelijk moet zijn voor de uitvoering van een overeenkomst met de betrokkene. Dit staat op gespannen voet met de praktijk van big-data-analyses, waar in principe alle beschikbare data worden geanalyseerd en de uitkomst van de analyse van tevoren vaak niet helder is (Zwenne, 2015).

Naast het doelbindingsprincipe en noodzakelijkheidsvereiste is er regelgeving over het informeren van betrokkenen. Betrokkenen moeten worden geïnformeerd over de wijze waarop de verwerking van persoonsgegevens plaatsvindt en zij moeten daar expliciet toestemming voor geven (*informed consent*). Echter, omdat veel IoT-apparaten geen scherm bevatten is het voor gebruikers lastig om zicht te hebben op de privacyinstellingen (Peppet, 2014) en om ondubbelzinnig toestemming te verlenen voor gegevensverwerking (Zwenne, 2015). Daarnaast zullen IoT-apparaten regelmatig gegevens verzamelen van mensen die hier niet expliciet mee instemmen. Een zelfrijdende auto zal bijvoorbeeld de locatie van alle inzittenden meten en delen, ook al willen sommige inzittenden dit niet. Individuele privacyvoorkeuren zullen dus niet altijd in te willigen zijn (Rose et al., 2015). Ook camera's kunnen gemakkelijk beelden maken van personen op straat die daar geen toestemming voor hebben gegeven. Met de enorme toename van het aantal IoT-apparaten is het de vraag in hoeverre het haalbaar en wenselijk is om voor ieder individueel appa-

[48] De Wet bescherming persoonsgegevens is geïmplementeerd naar aanleiding van de Europese Privacyrichtlijn (95/46/ EG). Deze is recentelijke geactualiseerd in de Algemene Verordening Gegevensbescherming (Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 (PbEG L 119 van 4 mei 2016)). De bepalingen in de Algemene Verordening Gegevensbescherming moeten op 25 mei 2018 in de Wet bescherming persoonsgegevens zijn vervangen.

raat toestemming te verlenen en zicht te hebben op de privacyinstellingen (Rose et al., 2015).[49]

Eigendomsrecht ten slotte regelt het recht op eigendom van een bestaansmiddel en de opbrengst die ermee wordt behaald. Bij het verwerken van data kunnen echter gemakkelijk onduidelijkheden over eigendom ontstaan, bijvoorbeeld wanneer meerdere databronnen worden gecombineerd en hier analyses op worden uitgevoerd. Nog ingewikkelder wordt het wanneer verschillende databronnen en -verwerkers uit verschillende landen komen, met elk een eigen wet- en regelgeving. In hoofdstuk 4 zal dieper op de problematiek rondom deze complexiteit van data worden ingegaan.

3.2.3 Welvaart

Technologische ontwikkelingen hebben de afgelopen twintig jaar een belangrijke bijdrage geleverd aan de welvaart en economische groei (Van Est & Kool, 2015). Zoals in paragraaf 3.1.4 beschreven biedt het IoT voldoende kansen voor verdere groei, maar dit gaat tegelijkertijd gepaard met een aantal risico's. Deze negatieve effecten zullen met name zichtbaar zijn op het gebied van werkgelegenheid, concurrentie en de manier waarop bedrijven zaken doen.

In de media verschijnen geregeld berichten dat er banen gaan verdwijnen door nieuwe technologische ontwikkelingen (Heijne & Witteman, 2014).[50] Historisch gezien is deze vrees maar deels terecht; op de zeer korte termijn gaan technologische ontwikkelingen ten koste van banen, maar binnen één tot twee jaar zijn hier tot nu toe altijd nieuwe banen voor in de plaats gekomen (Van Est & Kool, 2015). De meningen verschillen over hoe dit zich in de toekomst zal ontwikkelen. Onderzoek binnen OECD-landen laat zien dat de effecten van robotisering en het IoT op de werkgelegenheid mogelijk beperkt zullen zijn (Arntz, Gregory & Zierahn, 2016). Onderzoek van onder andere het Rathenau Instituut (Van Est & Kool, 2015) en Deloitte[51], daarentegen, toont juist aan dat de effecten groter zullen zijn.

Technologische ontwikkelingen, waaronder de opkomst van het IoT, zullen ook de concurrentieposities van bedrijven veranderen. Het IoT creëert nieuwe markten en kansen, maar als Nederlandse bedrijven hier niet tijdig op inspelen kunnen zij mogelijk niet meer concurreren met (internationale) bedrijven die dit wel doen. Sommige bedrijven hebben moeite om in te spelen op de nieuwe 'online werkelijkheid', wat met de komst van het IoT waarschijnlijk niet minder zal worden.[52] Het IoT zal binnen iedere sector worden toegepast, wat in veel gevallen zal leiden tot inmenging van (technologie)bedrijven van buiten de sector. Bedrijven die IoT-toe-

---

[49] Een soortgelijk dilemma doet zich ook voor omtrent de Nederlandse cookiewetgeving, waardoor mensen veelvuldig te maken krijgen bij pop-ups op websites over het cookiebeleid van websites. Zie bijvoorbeeld Zwenne & Mommers (2010) hieromtrent.

[50] Sommige voorspellingen hebben het zelfs over 1 op de 3 banen die verloren gaan door 'robots' (Verbeek, 2016). Zie ook: www.ad.nl/economie/robotisering-kost-tot-3-miljoen-banen~a7a108dc

[51] Zie ook: www.deloitte.com/nl/nl/pages/data-analytics/articles/arbeidsmarkt-resultaten-2015-state-of-the-state.html

[52] Uit onderzoek van TNS NIPO blijkt bijvoorbeeld dat het MKB moeite heeft om aansluiting te vinden bij het online consumentengedrag, zie ook: www.dtg.nl/over-dtg/persberichten/archief/kloof-online-consumentengedrag-en-inzet-online-lokaal-mkb.aspx Ook de vele retailfaillissementen worden vaak geweten aan het onvoldoende inspelen op de online werkelijkheid, zie ook: www.metronieuws.nl/nieuws/binnenland/2016/02/faillissement-winkelketen-waar-gaat-het-mis

passingen willen gebruiken lopen daarmee het risico belangrijke delen van hun waardeketen weg te geven.[53]

Van veel grotere invloed zijn de technologiebedrijven die met nieuwe IoT-toepassingen bestaande sectoren zullen binnentreden. General Electric bijvoorbeeld heeft met Predix een industrieel IoT-platform ontwikkeld dat industriële apparaten verbindt met het internet en realtime data-analyses uitvoert. Ook andere nieuwe bedrijven springen in op de mogelijkheden van het IoT. Een rapport van het Rathenau Instituut zegt hierover: 'door middel van digitale platformen betreden ze snel nieuwe markten, integreren ze producten en diensten, laten ze andere partijen mee innoveren en betrekken ze gebruikers bij innovaties' (Van Est & Kool, 2015, p. 60). Dit kan leiden tot oneerlijke concurrentie. Bedrijven als Uber en Airbnb hoeven bijvoorbeeld niet te voldoen aan de eisen die aan taxidiensten en hotels worden gesteld. Hierdoor kunnen zij goedkoper en flexibeler opereren dan bestaande organisaties (Bijlsma, Overvest & Straathof, 2016). Dergelijke regels zijn echter ingevoerd om de consument te beschermen, denk bijvoorbeeld aan brandvoorschriften. Consumenten kunnen hierdoor dus een hoger veiligheidsrisico lopen. Ook het innen van belasting en het mogelijk mislopen daarvan is een nieuwe uitdaging die deze nieuwe platformen met zich meebrengen.[54]

Een mogelijke bedreiging van deze digitale platformen is dat het kan leiden tot *platformkapitalisme.* Deze platformen hebben vaak een *winner takes all* karakter, waarbij één product veruit het grootste marktaandeel heeft (Van Est & Kool, 2015; Bijlsma et al., 2016).[55] Veel van deze platformen werken dit ook in de hand doordat een groter aanbod leidt tot meer vragers en omgekeerd (mensen zullen gebruikmaken van het platform waarop de meeste mensen actief zijn). Binnen het IoT is deze 'strijd' nu volop gaande, zo werkt Samsung op dit moment aan het platform Artik[56] en Apple aan Homekit[57]. Daartegenover staat de AllSeen Alliance[58], een consortium van bedrijven zoals Microsoft, Philips en Sony, die streven naar een open standaard voor het IoT.[59] Welk platform de overhand krijgt zal moeten blijken, maar het gebrek aan standaarden zorgt tot die tijd voor beperkingen op het gebied van interoperabiliteit en levensduur van IoT-apparaten. Het risico bestaat dat IoT-apparaten worden aangeschaft waarvan een standaard na een aantal jaar niet meer wordt ondersteund, waardoor ze op termijn onbruikbaar worden. Het zal daarnaast de keuzevrijheid van consumenten beperken. Als consumenten optimaal gebruik willen maken van hun IoT-apparaten kunnen zij het beste producten van één fabri-

---

[53] In de auto-industrie maakt elektronica nu al bijna 40% uit van de totale kosten van de auto, deze elektronica en de functies die het biedt worden vaak door derden gemaakt. Met de komst van het IoT en zelfrijdende auto's zal dit percentage verder stijgen (Scuro, z.j.). Sommige bedrijven spelen hier dan ook al op in, zoals Ford die een 'start-up' heeft opgericht om te kunnen concurreren met andere tech bedrijven (Ziegler & Patel, 2016).

[54] De online platformen bieden mogelijk ook uitkomst, omdat alle transacties online worden geregistreerd. Zie ook: http://nos.nl/artikel/2130175-belastingdienst-worstelt-met-interneteconomie.html

[55] De zoekmachine-markt wordt bijvoorbeeld gedomineerd door Google, sociale netwerken door Facebook en online retail door Amazon (Bijlsma et al., 2016).

[56] Zie ook: www.artik.io

[57] Zie ook: www.apple.com/ios/home

[58] Zie ook: https://allseenalliance.org

[59] Zie ook: www.forbes.com/sites/janakirammsv/2015/10/29/google-brillo-vs-apple-homekit-the-battleground-shifts-to-iot/#1965efc94cac

kant aanschaffen.[60] Als gevolg hiervan kan ook de concurrentie op de markt afnemen, de kosten van het gebruik van bepaalde platformen toenemen en innovatie afnemen. Dit aspect van keuzevrijheid en afhankelijkheid van fabrikanten wordt ook nog toegelicht in paragraaf 3.2.6 onder de waarde autonomie. Bovenstaande dynamiek speelt zich af op internationaal niveau en vereist daarmee ook een mondiale aanpak.

3.2.4 Welzijn

Een groeiend IoT kan het menselijk welzijn op een aantal punten bedreigen. Hieronder worden de gevolgen besproken van de steeds grotere hoeveelheden beschikbare informatie, van technologie die bepaald gedrag voorschrijft, en van de steeds grotere rol van technologie in ons dagelijks leven.

Het IoT zal met zijn vele sensoren steeds meer data verzamelen en informatie genereren die met computers, smartphones, tablets of andere media te raadplegen zijn. Hoewel, zoals in paragraaf 3.1 beschreven, de vergaarde informatie voor verschillende nuttige doelen kan worden ingezet, kent de veelheid aan informatie ook een keerzijde. Uit onderzoek blijkt dat mensen niet altijd in staat zijn om goed om te gaan met grote hoeveelheden informatie (Bawden & Robinson, 2009). Te veel informatie kan bijvoorbeeld leiden tot *information overload*, concentratieproblemen, angst en keuzestress. De steeds grotere beschikbaarheid van data maakt dat mensen zich steeds bewuster zijn van wat zij niet weten en niet begrijpen en dat veroorzaakt stress (Wurman, 1989).

Een tweede bedreiging van het IoT voor welzijn is dat het keuzevrijheid mogelijk beperkt. Des te meer het IoT in de dagelijkse omgeving is verweven, des te meer invloed het heeft op de levens van mensen. Zo kunnen steeds complexere algoritmes gaan bepalen wanneer de verwarming en het licht in huizen aan- en uitgaan, op welke manier er auto wordt gereden, hoe mensen door een stad navigeren en welke (persoonlijke) informatie er met wie gedeeld wordt. Bij veel toepassingen bestaat de mogelijkheid wel om gebruikersvoorkeuren in te stellen, maar de keuzemogelijkheden die er zijn liggen vaak vast en zijn soms erg beperkt (Amichai-Hamburger, 2002). Verder zal het voor mensen steeds lastiger worden om zich volledig te onttrekken aan IoT-toepassingen en om geen persoonlijke informatie te delen (Peppet, 2014). Dit is dus sterk gerelateerd aan wat hierboven al is geschreven over privacy (zie paragraaf 3.2.2). Daarnaast heeft het te maken met het afhankelijk worden en zijn van technologie, dat nog aan de orde komt in de paragraaf over autonomie (paragraaf 3.2.6).

Ten slotte gaat de groei van het IoT gepaard met een aantal ontwikkelingen waarvan niet goed bekend is wat de gevolgen daarvan zullen zijn. Eén van die ontwikkelingen is dat technologie steeds meer wordt ingezet voor taken die voorheen door mensen werden uitgevoerd, waardoor menselijk contact vermindert. Mensen doen bijvoorbeeld steeds vaker online inkopen in plaats van dat ze naar een winkel gaan, bij de dokter krijgen ze een automatische diagnose in plaats van een consult en in een verzorgingstehuis worden ze verzorgd door robots in plaats van door verplegers. Dit roept vragen op als: Wat doet verminderd contact bij het afnemen van diensten met het vertrouwen in andere mensen? Welke gevolgen heeft dit voor de

[60] Zie ook het voornemen van Philips om de ondersteuning van producten van derde partijen bij Hue in te trekken; dit is na veel kritiek teruggedraaid: https://tweakers.net/nieuws/106882/philips-draait-enkele-wijzigingen-uit-hue-upgrade-terug.html

manier waarop mensen met elkaar omgaan? De antwoorden op deze vragen zijn nog onduidelijk. Een hieraan gerelateerde ontwikkeling is dat technologie steeds zelfstandiger en proactiever wordt, bijvoorbeeld in de vorm van een zelfrijdende auto of een zorgrobot. Ook dit roept vragen op zoals bijvoorbeeld: Hoe moeten mensen met robots omgaan die steeds menselijker worden? Wanneer mensen steeds meer interactie hebben met robots, verandert dit dan de manier waarop ze met andere mensen omgaan? In de literatuur wordt beargumenteerd dat bij verhoogde zelfstandigheid van technologie, moraliteit verdeeld raakt over mens en technologie (Van den Berg & Keymolen, 2013). Hierbij neemt technologie een deel van de morele beslissingen over die voorheen door mensen werden gemaakt. Dit zou ertoe kunnen leiden dat kritische reflectie op ons handelen afneemt en het moreel besef van mensen vermindert (Keymolen, 2014). Techniekfilosofen merken verder op dat mensen steeds meer versmolten zijn met technologie en dat de grens tussen mens en technologie daardoor vervaagt (Floridi, 2015; Verbeek, 2011). Ook raken de virtuele wereld en de realiteit steeds meer met elkaar vervlochten (Floridi, 2015). Pokémon Go is hiervan een recent voorbeeld (Malik, 2016). Ook bij deze ontwikkelingen is onduidelijk wat ze betekenen voor mens-zijn en menselijk contact. De mogelijke gevolgen zullen hoogstwaarschijnlijk sterker zijn voor jongeren dan voor ouderen. Het opgroeien in een wereld vol digitale en netwerktechnologieën heeft namelijk invloed op de constructie en expressie van identiteit (De Mul, 2015; Van den Berg, 2009). Jongeren van nu zijn bijvoorbeeld al vanaf jonge leeftijd bezig met het vormen van een online identiteit (Thomas, 2007). Het is nog niet bekend wat de gevolgen daarvan op latere leeftijd zullen zijn.

3.2.5 Gelijkwaardigheid

Het IoT kan ook een bedreiging vormen voor gelijkwaardigheid in de samenleving. Hierboven is al een aantal voorbeelden van discriminatie en stigmatisatie gegeven op basis van (gegevens afkomstig uit) IoT-toepassingen. Deze laten zien dat het risico bestaat dat bepaalde groepen uit de samenleving niet of onvolledig deel kunnen nemen aan het maatschappelijke leven. Hieronder wordt specifiek ingegaan op de risico's van het IoT voor gelijkwaardigheid in de samenleving die gerelateerd zijn aan de volgende onderwerpen: digitale geletterdheid, woonomgeving, arbeidsmarkt en digitale profilering.

Technologische vooruitgang heeft geleid tot een kloof tussen diegenen die kunnen profiteren van digitale technologie en zij die dit niet kunnen (Norris, 2001). Deze laatste groep dreigt in toenemende mate te worden afgesloten van (publieke) diensten, omdat zij niet in staat is om gebruik te maken van digitale middelen. Een voorbeeld hiervan is de Wet elektronisch berichtenverkeer Belastingdienst (met als doel om alle correspondentie tussen burger en belastingdienst digitaal te laten verlopen), die het voor sommige mensen onmogelijk maakt om belastingaangifte te doen.[61] Deze digitale kloof kan leiden tot een gevoel van eenzaamheid en buitensluiting. De komst van het IoT dreigt de digitale kloof verder te vergroten. Zo is het niet ondenkbaar dat verzekeringspremies omlaag gaan voor mensen met een smart home of *smart car*. Naast het feit dat een deel van de bevolking geen gebruik zal kunnen maken van deze toepassingen wegens digitale ongeletterdheid, zullen deze mensen ook nog eens meer moeten betalen voor bepaalde diensten in vergelijking met mensen die wel van IoT-toepassingen kunnen profiteren.

[61] Zie ook: www.nationaleombudsman.nl/nieuws/2015/ombudsman-onderzoekt-verdwijnen-blauwe-envelop-belastingdienst

De opkomst van het IoT kan tevens leiden tot grotere verschillen tussen bewoners van het platteland en de stad. Op dit moment wordt er op grote schaal geïnvesteerd in smart cities,[62] waardoor steden in de nabije toekomst een groot aantal objecten met sensoren zullen hebben. De informatie die hiermee verzameld wordt, zal in toenemende mate worden gebruikt om diensten aan te bieden, bijvoorbeeld op het gebied van gezondheidszorg, afvalverwerking of openbaar vervoer, die in niet-stedelijke gebieden niet of beperkter worden aangeboden (CLTC, 2016). Daarnaast zal met de komst van smart cities (landelijke) besluitvorming steeds meer gebaseerd worden op verzamelde data. Mensen in gebieden waar het IoT nog niet (vergaand) is doorgevoerd, kunnen hierdoor benadeeld worden.

Het IoT kan er daarnaast toe leiden dat er banen verloren gaan (zoals reeds genoemd in paragraaf 3.2.3) en dat arbeidsomstandigheden onzekerder worden. Uit onderzoek van het Rathenau instituut blijkt dat technologie vooral geschikt is om cognitief routinewerk over te nemen zoals administratief werk, het maken van berekeningen of het beoordelen van producten, en dat het daarmee vooral middelbaar geschoold werk raakt (Van Est & Kool, 2015). Dit kan leiden tot een grotere kloof tussen hoog- en lageropgeleiden in Nederland. Zoals al genoemd in paragraaf 3.1.4 speelt IoT naast deze ontwikkeling ook een rol in de opkomst van de deeleconomie, met platformen zoals bijvoorbeeld Airbnb en Uber (Frenken, 2016). Deze platformen creëren nieuwe vormen van werkgelegenheid, doorgaans zonder vaste contracten en onder flexibele omstandigheden. Daarmee kan de deeleconomie leiden tot grotere ongelijkwaardigheid op de arbeidsmarkt, onder andere wat betreft loon, arbeidsvoorwaarden en kans op werk (Roose, 2014).

Zoals beschreven in paragraaf 3.2.2. kunnen bedreigingen omtrent gelijkwaardigheid ook ontstaan bij big-data-analyses gericht op profilering, dat wil zeggen, het destilleren van categorieën op basis van gegevens over personen of groepen. Zo past de Nederlandse overheid profilering toe voor veiligheidsdoeleinden, bijvoorbeeld in analyses door politie en justitie, de inlichting- en veiligheidsdiensten en verschillende organisaties op het gebied van fraudebestrijding (WRR, 2016). Een risico hierbij is dat het toepassen van profilering leidt tot onterechte verdenkingen, uitspraken en conclusies over personen of groepen. Dit geeft een nadeel (discriminatie) voor bepaalde groepen in de maatschappij en kan leiden tot een ongelijke verhouding tussen maatschappelijke groepen (WRR, 2016).

3.2.6 Autonomie

Voor alle technologie, dus ook voor het IoT, geldt dat er een risico bestaat op uitval of niet naar behoren functioneren. Des te nauwer technologie in onze dagelijkse omgeving verweven raakt, des te afhankelijker de samenleving raakt van technologie en des te groter de gevolgen van storingen van technologie zullen zijn. Dit bedreigt onze autonomie. De toenemende afhankelijkheid van technologie is geen nieuwe ontwikkeling, maar wordt wel versterkt door de opkomst van het IoT. Hieronder worden verschillende oorzaken en gevolgen van deze bedreiging besproken.

Allereerst bestaat de kans op uitval van IoT-technologie door internet- en stroomstoringen of overbelasting van communicatienetwerken. Wanneer steeds meer apparaten en technologieën verbonden zijn met het IoT, bestaat de mogelijkheid dat zij een deel van hun functionaliteit verliezen of zelfs helemaal niet meer functio-

[62] Zie ook: https://eu-smartcities.eu/content/european-commision-invest-%E2%82%AC200m-smart-cities-next-two-years

neren zonder internetverbinding. Dit kan vervelend zijn, bijvoorbeeld wanneer een smart home niet meer naar behoren functioneert (Balta-Ozkan, Davidson, Bicket & Whitmarsh, 2013). Het kan zelfs ernstige gevolgen hebben, bijvoorbeeld als op termijn zelfrijdende auto's niet meer kunnen rijden zonder internetverbinding. De website allestoringen.nl laat zien dat internet- en telefoonstoringen met enige regelmaat voorkomen[63] en cijfers over stroom- en gasuitval van brancheorganisatie Netbeheer Nederland geven aan dat een Nederlands huishouden in 2015 gemiddeld 33 minuten geen stroom had[64].

Het IoT neemt steeds meer taken en activiteiten van mensen over. Zoals beschreven in paragraaf 3.1.1, maakt deze ontwikkeling het voor sommige mensen mogelijk om werkzaamheden uit te voeren waar ze voorheen niet toe in staat waren. Toenemende automatisering leidt er echter ook toe dat bepaalde kennis en vaardigheden niet meer nodig zijn en daardoor verloren kunnen gaan (Pereira, Benessia & Curvelo, 2013). Hierdoor groeit de afhankelijkheid van technologie, wat met name risico's oplevert als IoT-toepassingen niet naar behoren functioneren. Een voorbeeld is diagnostisering in de zorg. Tot voor kort werden diagnoses gemaakt op basis van jarenlange ervaring en kennis van de arts. Echter, doordat technologie in toenemende mate een rol speelt bij het maken van diagnoses wordt het voor jonge artsen steeds lastiger om deze ervaring op te doen (Lu, 2016).

Naast het risico van technische storingen, creëert een groeiend IoT ook nieuwe afhankelijkheden van fabrikanten die in veel gevallen niet in Nederland gevestigd zijn. Zo kunnen producten of diensten foutief gedrag vertonen of kan de ondersteuning van een bepaald product door een bedrijf worden stopgezet. Dit kan (zoals beschreven in paragraaf 3.2.1) veiligheidsrisico's met zich meebrengen, bijvoorbeeld doordat bepaalde lekken in het apparaat niet langer worden gedicht. Daarnaast kan het betekenen dat apparaten niet meer functioneren of dat apparaten niet (langer) kunnen werken met andere IoT-apparaten. Deze risico's zullen zich met name voordoen als er gebruik wordt gemaakt van gesloten standaarden, wat mede het belang van open standaarden onderstreept (zie ook paragraaf 3.2.3). De afhankelijkheid van fabrikanten kan ook nationale belangen schaden. Het CLTC (2016) schetst een toekomst waarin landen IoT-productie nationaliseren om mogelijke spionage of sabotage uit andere landen tegen te gaan. De eerste tekenen hiervan zijn nu al zichtbaar, bijvoorbeeld bij de verkoop van telefoons.[65] Een wereldwijd IoT-netwerk lijkt daarmee onwaarschijnlijk. Vanwege schaalvoordelen voorspelt het CLTC (2016) dat een aantal grote netwerken zullen ontstaan van landen zoals China en de Verenigde Staten. Hierdoor zullen met name kleine landen een keuze moeten maken tot welke invloedsfeer zij willen behoren. Dit roept allerlei vragen op, bijvoorbeeld over de invloed die deze landen zullen hebben op de geproduceerde (privacygevoelige) IoT-data.

3.3 Deelconclusie

Dit hoofdstuk heeft laten zien dat het IoT vele kansen in verschillende domeinen creëert, maar dat het ook een aantal serieuze bedreigingen met zich meebrengt.

---

[63] Zie ook: www.allestoringen.nl

[64] Zie ook: www.netbeheernederland.nl/nieuws/nieuwsbericht/?newsitemid=2051244033

[65] Zie ook de discussie over Huawei telefoons, die mogelijk een achterdeurtje bevatten waarmee de Chinese overheid in de Verenigde Staten kan spioneren: www.zdnet.com/article/is-it-safe-for-americans-to-buy-a-huawei-built-nexus-phone

Figuur 3.1 geeft een overzicht van de kansen en bedreigingen die in dit hoofdstuk zijn besproken. Samenvattend kan geconcludeerd worden dat het IoT grote impact op onze samenleving zal hebben met zowel positieve als negatieve gevolgen. De precieze impact van de genoemde kansen en bedreigingen is afhankelijk van hoe het IoT zich verder ontwikkelt. Op dit moment lijkt de grootste kans te liggen in het realiseren van economische groei en vormen veiligheids- en privacyrisico's de belangrijkste bedreigingen.

Figuur 3.1 Overzicht van de kansen en bedreigingen van het IoT

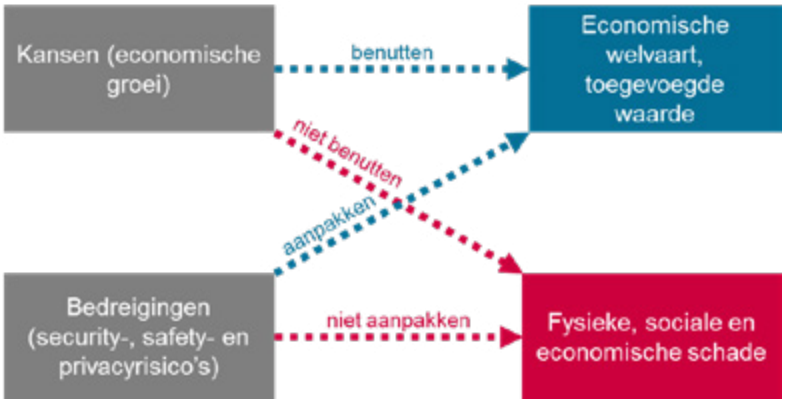
Economische groei speelt in meer of mindere mate een rol bij de beschreven kansen in dit hoofdstuk. Kansen op het gebied van welzijn kunnen, naast het vergroten van gemak, gezondheid en veiligheid, ook bijdragen aan economische groei. Hierbij gaat het met name om kostenbesparing, bijvoorbeeld doordat ouderen langer thuis kunnen wonen of doordat zorgkosten dalen omdat gezondheid wordt verbeterd. Ook voor duurzaamheid geldt dat, naast de bijdrage aan het milieu, de genoemde kansen kunnen bijdragen aan economische groei. Bijvoorbeeld door nieuwe, duurzame IoT-producten of -diensten aan te bieden. Het ministerie van EZ spreekt in dit kader dan ook van een 'groene groei' van de economie, waarbij de focus ligt op het benutten van economische kansen bij de transitie naar een duurzame samenleving (Kamp

& Mansveld, 2013). Kansen op het gebied van productiviteit dragen met name bij door het optimaliseren van bestaande bedrijfsprocessen. Kansen op het gebied van welvaart leveren een bijdrage aan economische groei doordat er nieuwe producten, diensten, verdienmodellen en banen zullen ontstaan.

De belangrijkste bedreigingen liggen op het gebied van veiligheid (security en safety) en privacy. Securityrisico's zijn bijvoorbeeld risico's op het gebied van cybercriminaliteit en safetyrisico's zijn risico's veroorzaakt door disfunctionerende IoT-apparaten. Bedreigingen rondom privacy zoals het risico op privacyschending hangen sterk samen met securityrisico's. Wanneer de beveiliging van IoT-toepassingen niet op orde is, wordt de kans dat kwaadwillende personen toegang krijgen tot persoonsgegevens groter. Ook bedreigingen genoemd in de andere paragrafen bevatten veiligheidsrisico's. In het stuk over welzijn (paragraaf 3.2.4) worden bedreigingen op economisch vlak genoemd, zoals het verlies van werkgelegenheid en het verslechteren van de concurrentiepositie van bedrijven door nieuwe (vaak ook buitenlandse) technologiebedrijven. Bedreigingen voor autonomie (paragraaf 3.2.6) brengen ook veiligheidsrisico's met zich mee. Hoe afhankelijker we worden van technologie en grote (buitenlandse) bedrijven, des te groter de gevolgen kunnen zijn als er iets misgaat.

Figuur 3.2 laat zien wat de gevolgen zijn van het al dan niet benutten van de kansen en het al dan niet aanpakken van de bedreigingen. Dit zal leiden tot fysieke, sociale en/of economische schade. Echter, wanneer de kansen en bedreigingen van het IoT wel worden benut en aangepakt, dan kan dat bijdragen aan economische welvaart en toegevoegde waarde voor diverse toepassingsdomeinen. Er is dus sprake van een wisselwerking. Als er alleen oog is voor de kansen, en de bedreigingen op het gebied van veiligheid en privacy niet adequaat worden aangepakt, zal er niet of slechts beperkt geprofiteerd kunnen worden van de kansen die het IoT biedt.

Figuur 3.2 Relatie kansen en bedreigingen



In het volgende hoofdstuk wordt een aantal maatregelen en handelingsperspectieven besproken die eraan bijdragen dat Nederland de veiligheids- en privacyrisico's kan beperken en tegelijkertijd kan profiteren van economische groei.

4 Handelingsperspectieven

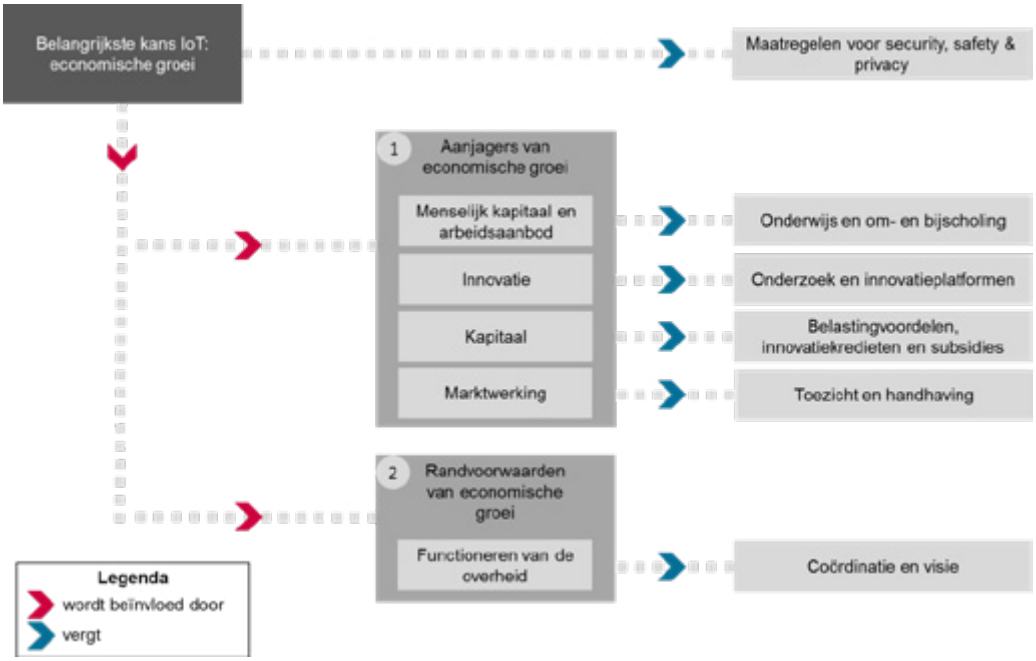
Dit hoofdstuk geeft een overzicht van de belangrijkste maatregelen die enerzijds bij kunnen dragen aan het bevorderen van economische groei en het creëren van toegevoegde waarde en anderzijds aan het voorkomen van fysieke, sociale en economische schade. Allereerst wordt in paragraaf 4.1 ingegaan op maatregelen die economische groei kunnen stimuleren. Paragraaf 4.2 bespreekt vervolgens de belangrijkste maatregelen die de veiligheid kunnen bevorderen. Beiden worden geïllustreerd door middel van een concrete casus. Ten slotte worden in paragraaf 4.3 de belangrijkste conclusies van dit hoofdstuk besproken. Hieruit volgt een overzicht van handelingsperspectieven voor verschillende betrokken stakeholders.

4.1 Economische groei

Het CBS identificeert in een conceptueel model een aantal factoren die bijdragen aan economische groei (CBS, 2013). Daarbij gaat het enerzijds om factoren die gelden als aanjagers van economische groei: innovatie, ondernemerschap, marktwerking, menselijk kapitaal en arbeidsaanbod, en kapitaal. Anderzijds gaat het om factoren die samen de randvoorwaarden voor economische groei en de maatschappelijke context bepalen: de maatschappelijke situatie, de macro-economische condities, het functioneren van de overheid en de kwaliteit van de infrastructuur. Een deel van deze factoren beïnvloedt ook de economische groei veroorzaakt door het IoT. Om deze factoren positief te beïnvloeden kunnen verschillende maatregelen genomen worden. In deze paragraaf wordt dit model gebruikt als structuur om de maatregelen te beschrijven die kunnen bijdragen aan economische groei door het IoT. Alleen die factoren waarvoor relevante maatregelen zijn beschreven in het kader van het IoT worden besproken.

Figuur 4.1 geeft een overzicht van de belangrijkste kans van het IoT, factoren die daar invloed op hebben en de maatregelen die deze factoren op een positieve manier beïnvloeden. Zoals aangegeven in de figuur vergt economische groei ook dat risico's op het gebied van veiligheid en privacy worden gemitigeerd. Als het IoT niet naar behoren functioneert, zal het vertrouwen in het gebruik afnemen en daarmee ook de voordelen die hiermee gepaard gaan. Het tegengaan van deze risico's wordt besproken in paragraaf 4.2. De overige maatregelen worden hieronder toegelicht in relatie tot hun onderliggende factoren.

Figuur 4.1 Factoren en maatregelen die economische groei door het IoT bevorderen



4.1.1 Menselijk kapitaal en arbeidsaanbod

Menselijk kapitaal en arbeidsaanbod gaan over de kennis en vaardigheden van de beroepsbevolking (CBS, 2013). De komst van het IoT en de verdere digitalisering van de economie leidt ertoe dat er in toenemende mate behoefte is aan mensen met ICT-competenties. Het IoT zal vragen om werknemers met nieuwe, gespecialiseerde kennis zoals data-analisten, veiligheidsexperts, en softwarespecialisten en -ontwikkelaars. Op dit moment bestaat er al een tekort aan ICT-specialisten en is ingrijpen noodzakelijk om dit kennisgat in de toekomst te dichten (CSR, 2016b; Van Lakerveld et al., 2014; SER, 2016). Daarnaast zullen ook voor traditioneel werk ICT-vaardigheden in toenemende mate vereist zijn (CSR, 2016c).

Om economische groei te bevorderen is het daarnaast van belang dat er bij bedrijven voldoende kennis aanwezig is om nieuwe producten en diensten op de markt te brengen die concurreren met het aanbod van andere (internationale) bedrijven. Ook mensen die bij de overheid werken dienen voldoende kennis over het IoT en andere technologische ontwikkelingen in huis te hebben. Verschillende van de geïnterviewde experts gaven aan dat er op dit moment een tekort aan kennis en bewustzijn aangaande het IoT bij beleidsmakers is. Dit maakt het lastiger om beleid op te stellen en uit te voeren dat bijdraagt aan het benutten van de kansen aangaande het IoT.

Maatregelen
Om in te spelen op de groei van het IoT moeten toekomstige werknemers op de juiste manier worden opgeleid en zullen huidige werknemers moeten worden bij- of omgeschoold. Zowel bedrijven als de overheid zullen werknemers hiervoor ruimte moeten bieden.

Om de digitale geletterdheid van toekomstige werknemers te waarborgen, zal er meer aandacht moeten worden besteed aan ICT-vaardigheden in het basis-, middelbaar- en voortgezet onderwijs. Dit kan door het invoeren van nieuwe vakken, zoals programmeren, of het toespitsen van bestaande vakken op deze vaardigheden (CSR, 2016b). In Nederland is een eerste stap in deze richting gezet met het uitkomen van het adviesrapport 'Ons onderwijs 2032', waarin digitale vaardigheden als één van de pijlers wordt gezien van het toekomstige onderwijscurriculum (Platform Onderwijs 2032, 2016).

4.1.2 Innovatie

Door middel van innovatie kunnen nieuwe processen en producten worden ontwikkeld die de productiviteit van bedrijven en de welvaart kunnen vergroten. Uiteraard is het daarbij van belang om toegang tot kennis te hebben (zoals hierboven beschreven), maar daarnaast zal deze kennis ook moeten leiden tot daadwerkelijke innovaties. Landen of regio's die hierin slagen kunnen qua concurrentie voorop (blijven) lopen (CBS, 2013).

Maatregelen
Het doen van onderzoek naar nieuwe IoT-technieken en –toepassingen kan economische groei bevorderen. Dit onderzoek kan zowel uitgevoerd worden door kennisinstellingen zoals (hoge)scholen, universiteiten en onderzoeksinstituten als door bedrijven, bijvoorbeeld binnen R&D-afdelingen. Samenwerkingen tussen kennisinstellingen en bedrijven zijn ook mogelijk. Daarbij kan het gaan om spin-offs op basis van onderzoek dat op universiteiten is verricht (Zeemeijer, 2016), maar ook om samenwerkingsverbanden tussen bedrijven en universiteiten om nieuwe technologieën te ontwikkelen, bijvoorbeeld in de gezondheidszorg.[66]

Daarnaast is het van belang dat er ruimte is voor bedrijven om te experimenteren en innoveren. De expertgroep Big Data en privacy van het ministerie van EZ stelt in dit kader voor om de mogelijkheid te onderzoeken tot het creëren van een *regulatory sandbox*. Hierin kunnen toezichthouders, in overleg met bedrijven, speelruimte creëren om nieuwe big-data-toepassingen te onderzoeken (Ministerie van Economische Zaken, 2016). Dit kan doorgetrokken worden naar IoT-toepassingen, zeker omdat daar in veel gevallen ook big-data-analyses worden uitgevoerd. Een ander voorbeeld hiervan is het National Cyber Testbed (NCT) waarin met nieuwe toepassingen op het gebied van cybersecurity kan worden geëxperimenteerd (Remerie & te Brake, 2017).

4.1.3 Kapitaal

Kapitaal is een belangrijke productiefactor, daarbij kan het gaan om fysiek kapitaal (zoals gebouwen en machines) en financieel kapitaal. De beschikbaarheid ervan bepaalt of bedrijven willen investeren in Nederland of uitwijken naar het buitenland (CBS, 2013). Om hier op in te spelen steunt de overheid innovatieve bedrijven in negen topsectoren via belastingvoordeel, innovatiekrediet en/of subsidie.[67] Dit zijn sectoren waarin het Nederlandse bedrijfsleven en onderzoekscentra internationaal uitblinken.[68] Technologie vormt geen aparte topsector, maar het IoT zal (zoals geïl-

[66] Zie ook: www.tue.nl/universiteit/nieuws-en-pers/nieuws/03-06-2014-philips-en-tue-nemen-initiatief-voor-digitale-innovatie-voor-gezondheidszorg-verlichting-en-datawetenschap

[67] Zie ook: www.rijksoverheid.nl/onderwerpen/ondernemen-en-innovatie/inhoud/rijksoverheid-stimuleert-innovatie

[68] Zie ook: www.topsectoren.nl/topsectoren

lustreerd met voorbeelden in hoofdstuk 3) in toenemende mate een rol gaan spelen in meerdere van de topsectoren, zoals de landbouw-, energie- en logistieksector.

Maatregelen
Gezien het belang van de topsectoren in Nederland ligt het voor de hand om een deel van de verstrekte belastingvoordelen, innovatiekredieten en subsidies ten goede te laten komen aan de ontwikkeling van topsector-gerelateerde IoT-toepassingen. Daarnaast geven meerdere van de geïnterviewde experts aan dat kleine subsidies een goede motivatie kunnen zijn voor start-ups om IoT-diensten te gaan en blijven ontwikkelen.

4.1.4 Marktwerking

Marktwerking is een belangrijke voorwaarde voor de ontwikkeling van het IoT en economische groei. Marktwerking moet bedrijven ertoe aanzetten om efficiënt te opereren, economische waarde te creëren en deze waarde te delen met afnemers (CBS, 2013). Verschillende instrumenten kunnen hiervoor worden ingezet, zoals wet- en regelgeving die de spelregels van de markt bepalen. Hier kan het bijvoorbeeld gaan om regels omtrent arbeid, maar ook regels die ervoor zorgen dat er een eerlijk speelveld ontstaat voor zowel binnenlandse als buitenlandse bedrijven. Het stimuleren van innovatie (zoals hierboven beschreven) kan in dat kader soms botsen met het stimuleren van marktwerking.

Marktwerking moet het daarnaast voor nieuwe bedrijven mogelijk maken om de IoT-markt te betreden en het moet keuzevrijheid voor consumenten en andere afnemers bieden. De Autoriteit Consument en Markt (ACM) houdt toezicht op de markt en waakt voor oneerlijke concurrentie. De mededingingswet wordt overtreden op het moment dat er kartelafspraken worden gemaakt of misbruik wordt gemaakt van een economische machtspositie. In paragraaf 3.2.3 is beschreven hoe de groei van digitale platformen in veel gevallen heeft geleid tot één dominante aanbieder. Met de komst van het internet is de invloed van digitale platformen enorm toegenomen en deze invloed zal met de komst van het IoT nog verder toenemen.

Maatregelen
Zowel op nationaal als Europees niveau is het van belang dat er ook in de toekomst voldoende middelen beschikbaar zijn om te zorgen voor een eerlijk speelveld. De ACM (of een andere aan te wijzen partij) moet daartoe voldoende middelen hebben om toezicht te houden op nieuwe platformen en waar nodig de mededingingswet te handhaven.

4.1.5 Functioneren van de overheid

Het functioneren van de overheid beïnvloedt het ondernemingsklimaat op verschillende manieren (CBS, 2013). Allereerst legt de overheid als wet- en regelgever rechten en plichten op aan bedrijven. Als dienstverlener ondersteunt de overheid deze rechten en plichten door het verstrekken van vergunningen, subsidies en het heffen van belasting. Daarnaast kan de overheid ook nog afnemer zijn van bepaalde producten of diensten. Voor het ondernemingsklimaat is een zekere voorspelbaarheid van de overheid in haar optreden belangrijk (CBS, 2013), dit verkleint risico's voor bedrijven wanneer zij willen investeren.

De ontwikkeling van het IoT wordt beïnvloed door veel verschillende stakeholders (zie ook paragraaf 4.2.1). Om nieuwe IoT-toepassingen te ontwikkelen en succesvol uit te bouwen zullen deze partijen met elkaar moeten samenwerken. De overheid zou daarin een rol kunnen spelen, maar schiet op het gebied van ICT nu nog vaak tekort.[69]

Maatregelen
Het uitspreken van een overheidsvisie kan bedrijven helpen om in te schatten waar ruimte is om te innoveren en investeren. Dit gaat zeker op als deze innovaties bestaande verdienmodellen uitdagen. Wanneer het in de toekomst bijvoorbeeld mogelijk wordt om zelfrijdende auto's te delen, zal dat van grote invloed zijn op de verdienmodellen in de autoverhuur- en taxisector. Dit kan mogelijk leiden tot weerstand binnen de sectoren en een roep naar strengere wetgeving. Als bedrijven in een dergelijke situatie weten wat de visie van de overheid is kunnen zij daar tijdig op anticiperen met (het uitstellen of terugschroeven van) eventuele investeringen. Zoals beschreven in de casus (zie paragraaf 4.1.6) draagt de overheid nu al een visie uit over zelfrijdende auto's door ruimte te bieden om te experimenteren en eventuele obstakels weg te nemen (denk aan het aanpassen van wet- en regelgeving)[70].

In het verlengde hiervan stelt het CPB dat als er veel technologische onzekerheid is, een technologieneutraalbeleid de voorkeur geniet (Bijlsma et al., 2016). Indien de aanpassingskosten van nieuwe wetgeving laag zijn voor bedrijven dan loont het als de overheid experimenten met nieuwe producten of diensten faciliteert.[71] Als de aanpassingskosten echter hoog zijn, dan is wachten op nieuw beleid juist te kostbaar (Bijlsma et al., 2016).

Verschillende rapporten en eerdere onderzoeken concluderen dat het nuttig is om een overkoepelend orgaan in te stellen dat meewerkt aan het opstellen van een visie en de uitvoering hiervan coördineert (GO-Science, 2014; Kool et al., 2017).[72] Sommigen van de geïnterviewde experts zien het instellen van een nieuw orgaan echter juist als inefficiënt, doordat het een extra overheidslaag creëert. Op basis van dit onderzoek is niet te concluderen of er al dan niet een overkoepelend orgaan opgericht moet worden. Voor de meerderheid aan maatregelen in dit hoofdstuk is het wel van belang dat één instantie deze kan coördineren en sturen. Dit kan een overkoepelend orgaan zijn, een nieuw ministerie, maar ook een afdeling binnen een bestaand ministerie.

4.1.6 Casus: zelfrijdende auto's

In hoofdstuk 2 is al kort stilgestaan bij de wereldwijde opkomst van zelfrijdende auto's. In deze casus wordt de Nederlandse situatie beschreven en hoe dit zich verhoudt met aanjagers en randvoorwaarden van economische groei. Daarbij wordt

---

[69] In het onderzoek van de Tijdelijke Commissie ICT van de Tweede Kamer wordt onder meer geconcludeerd dat het door het ontbreken van centrale sturing kostenbesparing en maatschappelijke opbrengsten van het ICT-beleid moeilijker inzichtelijk te krijgen zijn. Zie ook: Tweede Kamer 2014–2015, 33 326, nr. 5.

[70] Zie ook: www.rijksoverheid.nl/onderwerpen/mobiliteit-nu-en-in-de-toekomst/inhoud/zelfrijdende-autos

[71] Deze aanpak past binnen het beleidsperspectief *van permissionless innovation*, waarbij nieuwe technologie en verdienmodellen in beginsel alle ruimte krijgen, tenzij er overtuigende argumenten zijn om dat niet te doen (Thierer, 2015).

[72] Zie ook: www.surf.nl/nieuws/2016/11/brede-coalitie-wil-meer-actie-van-kabinet-rond-digitalisering.html

aangegeven welke maatregelen de ontwikkeling hiervan in Nederland mogelijk maken.

In 2014 stelde Minister Schultz van Haegen van Infrastructuur en Milieu (I&M) voor om Nederland wereldwijd een koploper te maken op het gebied van de ontwikkeling en het testen van zelfrijdende auto's. Het ministerie van I&M heeft daartoe samen met Rijkswaterstaat en de Dienst Wegverkeer (RDW) onderzocht hoe testen op de openbare weg veilig kunnen plaatsvinden. Dit bleek mogelijk door een aanpassing van de Algemene Maatregel van Bestuur die partijen, die met zelfrijdende voertuigen willen testen op de openbare weg, in staat stelt om onder bepaalde omstandigheden ontheffing aan te vragen bij de RDW. Het voornemen is om het in de toekomst bij wet mogelijk te maken auto's zonder bestuurders de openbare weg op te laten gaan.[73]

Deze casus laat zien dat de economische kansen van deze IoT-toepassing worden gestimuleerd door verschillende factoren.

1 *Aanjagers van economische groei: Deze casus laat zien dat de overheid ruimte kan creëren voor innovatie. Bestaande wetgeving laat het niet toe dat een voertuig zonder bestuurder de openbare weg opgaat. Door maatregelen van de minister wordt het met behulp van ontheffingen, en in de toekomst een aanpassing van de wet, mogelijk gemaakt te experimenteren met zelfrijdende auto's.*
2 *Randvoorwaarden van economische groei: Vanwege de onzekerheid en grote investeringen die met innovatie gepaard gaan, kan het uitspreken van een visie door de overheid helpen deze onzekerheid te verkleinen. Wat betreft zelfrijdende auto's heeft Minister Schultz van Haegen de ambitie uitgesproken dat Nederland wereldwijd een koploper op dit gebied wordt en mogelijke obstakels wegneemt. Deze casus toont daarnaast aan hoe met een duidelijke, gedeelde doelstelling verschillende overheidsdiensten kunnen samenwerken om de ontwikkeling van (specifieke) IoT-toepassingen te bevorderen.*

4.2 Veiligheid en privacy

In de literatuur worden verschillende maatregelen beschreven om security-, safety- en privacyrisico's te mitigeren.[74] Het rekening houden met security, safety en privacy tijdens het ontwerpproces wordt respectievelijk ook wel *security-by-design*, *safety-by-design* en *privacy-by-design* genoemd (Langheinrich, 2001). Wanneer bestaande systemen veiliger of privacygevoeliger worden gemaakt is er sprake van security-, safety-, of privacy-by-*re*design (Lee, Girgensohn & Schlueter, 1997). Het toepassen van deze ontwerpstrategieën leidt tot concrete maatregelen, zoals mechanismes voor het automatisch kunnen wijzigen van standaardwachtwoorden, het vereenvoudigen van updates (bijvoorbeeld door over-the-air updates aan te bieden), of het toevoegen van een delete-knop om (verwerkte) gegevens te wissen. Daarbij wordt ook rekening gehouden met de beveiliging gedurende de levenscyclus van het desbetreffende product. Daarnaast kunnen procedurele maatregelen worden getroffen, zoals het toepassen van *best practices* en risicomanagement. Het Amerikaanse Department of Homeland Security (DHS) heeft in dit kader een handreiking uitgebracht, waarin procedurele maatregelen staan beschreven om de veiligheid van IoT-toepassingen te vergroten (DHS, 2016). Op dit moment worden er door bedrij-

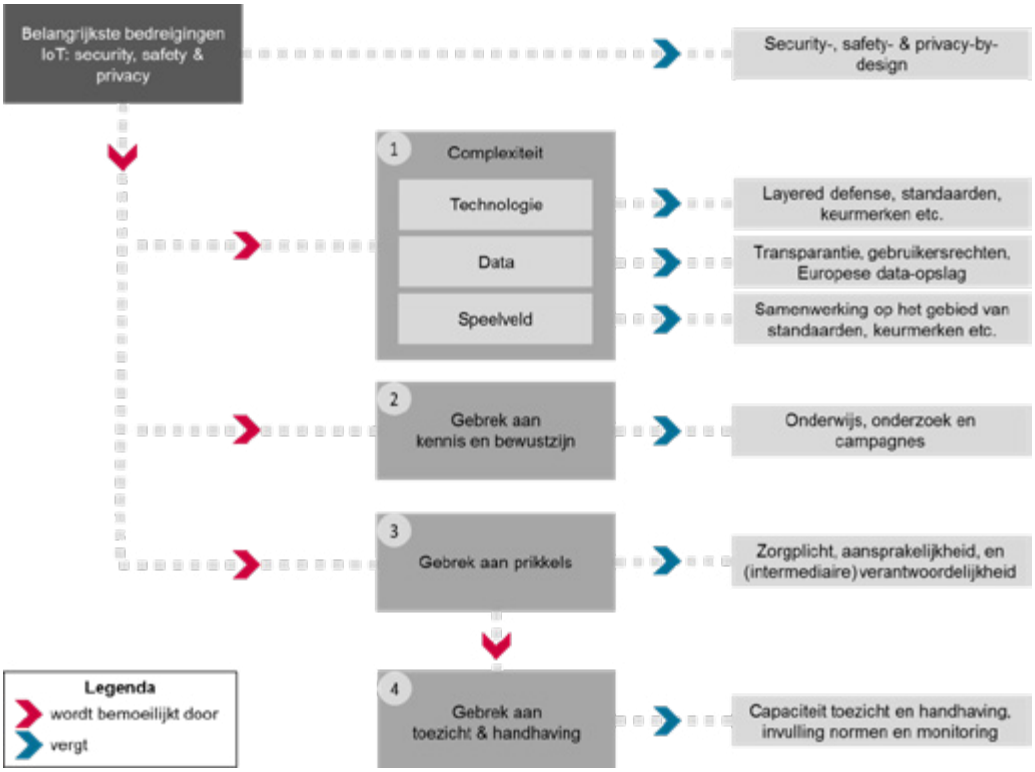
[73] Zie ook: www.rijksoverheid.nl/ministeries/ministerie-van-infrastructuur-en-milieu/nieuws/2017/02/24/voertuigen-zonder-bestuurder-aan-boord-de-weg-op

[74] Voor een uitvoerige discussie zie bijvoorbeeld: BITAG (2016).

ven echter onvoldoende maatregelen getroffen om de veiligheid en privacy van het IoT te vergroten. Dit kan verklaard worden door een combinatie van verschillende factoren.

Figuur 4.2 geeft een overzicht van de belangrijkste bedreigingen van het IoT, factoren die het tegengaan van deze bedreigingen belemmeren en maatregelen die getroffen kunnen worden om het effect van deze belemmerende factoren te verminderen. De figuur bevat niet alle mogelijke relaties tussen de blokken (gebrek aan bewustzijn maakt het bijvoorbeeld ook lastiger om prikkels te creëren), maar wel de belangrijkste. Hieronder worden de verschillende onderdelen van de figuur toegelicht.

Figuur 4.2 Maatregelen om security-, safety- en privacyrisico's van het IoT te beperken



4.2.1 Complexiteit

Interconnectiviteit is, zoals beschreven in hoofdstuk 2, een belangrijk kenmerk van het IoT. Via het IoT zijn een groot aantal heterogene objecten en gebruikers met elkaar verbonden die zich in verschillende landen kunnen bevinden. Deze interconnectiviteit vormt een nieuw complex geheel, wat meer is dan de som van de afzonderlijke delen. Deze complexiteit kan dan ook worden gezien als één van de belemmerende factoren bij het veiliger en privacygevoeliger maken van IoT-toepassingen. Dit geldt in het bijzonder voor 1) de grote diversiteit aan IoT-technologie, 2) de verwerking van (big) data en 3) het grote speelveld.

Complexiteit IoT-technologie
Het IoT omvat verschillende hard- en softwarecomponenten en raakt vele toepassingsdomeinen en stakeholders. Zoals in paragraaf 2.2 is beschreven, bestaat de IoT-architectuur uit een sensorlaag, netwerklaag, middleware-laag en toepassingslaag. De rol van deze lagen en de risico's die hiermee gepaard gaan zijn afhankelijk van de IoT-toepassing. Naast de toepassingen zelf spelen dienstverleners ook een steeds grotere rol bij het functioneren van IoT-toepassingen. Ook de hard- en software die deze partijen gebruiken is daarom van invloed op de veiligheid van het IoT.

Deze heterogeniteit van het IoT maakt het lastig om algemene veiligheidsmaatregelen te formuleren. Dit zorgt ervoor dat lokale oplossingen door hun beperkte reikwijdte aan effectiviteit inboeten.

Maatregelen
Keurmerken en standaarden kunnen bijdragen aan de veiligheid door het harmoniseren van IoT-technologie. Met behulp van keurmerken en standaarden kunnen veiligheids- en privacy-eisen worden vastgelegd waaraan fabrikanten van IoT-producten moeten voldoen. Dit kan het ook gemakkelijker maken om veilige IoT-technologie te ontwikkelen waarbij privacy geborgd is. Het National Cyber Testbed (NCT) zou mogelijk een rol kunnen vervullen bij het formuleren en certificeren van keurmerken (Remerie & te Brake, 2017).

Om te kunnen omgaan met de complexiteit van individuele systemen pleiten verschillende auteurs daarnaast voor het inzetten van een *layered defense*, waarbij maatregelen worden getroffen op basis van mogelijke risico's op verschillende niveaus (Easttom II, 2012; Wolff, 2016; Talbot, 2010). Bij het falen van de beveiliging zijn hierdoor nog verschillende andere *safeguards* aanwezig. Layered defense kan als uitgangspunt dienen voor de hierboven beschreven ontwerpstrategieën.

Complexiteit (big) data
Data, en big data in het bijzonder, vormen een relatief nieuw soort handelswaar, waardoor er soms onduidelijkheden ontstaan en bestaande wet- en regelgeving soms lastig toepasbaar zijn (voor een uitgebreidere beschouwing zie paragraaf 3.2.2). Hieronder worden kort de belangrijkste factoren besproken die de complexiteit van data vergroten.

Betrokkenen waarvan persoonsgegevens worden verwerkt hebben verschillende rechten. Zij hebben bijvoorbeeld het recht om hun gegevens in te zien, aan te passen of te verwijderen.[75] Dit is in de praktijk echter niet altijd eenvoudig. Er kan bijvoorbeeld onduidelijkheid ontstaan over waar data zich bevinden. Het komt voor dat een IoT-dienst als app wordt aangeboden in één land, terwijl de data van gebruikers worden opgeslagen en bewerkt in een ander land. Het is niet altijd duidelijk hoe in andere landen met data wordt omgegaan. Extern opgeslagen data kunnen daarnaast worden gedeeld met andere partijen, zonder dat de eindgebruiker daar bewust van is (WP29, 2014). Dit gebrek aan transparantie belemmert betrokkenen gebruik te maken van hun rechten. Daarnaast kunnen er ook persoonsgegevens ontstaan door het combineren van dataverzamelingen, die op zichzelf staand geen persoonsgegevens bevatten. Hierdoor kan het gebeuren dat de verwerking van deze gegevens onrechtmatig is of de genomen veiligheidsmaatregelen ontoereikend zijn (zij het onbedoeld). Ook informed consent is minder effectief door deze complexi-

[75] Artikel 35 en 36 Wbp.

teit. Informed consent dient ertoe om betrokkenen te informeren over waar de verzamelde data voor gebruikt gaan worden, maar in de praktijk zijn privacyvoorwaarden erg complex waardoor het onduidelijk is waarvoor betrokkenen toestemming geven (Madrigal, 2012).[76] Daarbij leidt toestemming voor het één soms tot toestemming voor het ander, waardoor gegevens voor andere doeleinden worden gebruikt dan waarvoor ze verzameld zijn (ook wel function creep genoemd).

Ook voor andere type gegevens, zoals bedrijfsdata, zijn er uitdagingen. Verschillende auteurs en geïnterviewde experts spreken hun zorgen uit over het punt dat de verwerking van data binnen het IoT tot onduidelijkheid kan leiden over wie de verwerker is van de (bedrijfs)data, met als gevolg dat er onduidelijkheid kan bestaan over wie deze data bezitten en hoe deze data worden gebruikt (Mashhadi, Kawsar & Acer, 2014; Weinberg, Milne, Andonova & Hajjat, 2015).

Maatregelen
Transparantie kan worden vergroot door bedrijven te verplichten heldere en begrijpelijke privacyvoorwaarden bij IoT-toepassingen op te stellen. Hierover zijn in Europees verband afspraken gemaakt. De algemene verordening gegevensbescherming (AVG) verplicht bedrijven informatie in een beknopte, transparante en begrijpelijke taal aan de betrokkenen te presenteren.[77] De AVG stelt verder dat gebruikers recht hebben op uitleg van beslissingen op basis van big-data-algoritmes. Het vergroten van transparantie kan ook bijdragen aan het bewustzijn van gebruikers (Van den Berg, Pötzsch, Leenes, Borcea-Pfitzmann & Beato, 2011). De effectiviteit van deze maatregel zal afhangen van de naleving (zie ook paragraaf 4.2.4).

Een manier om bij IoT-apparaten invulling te geven aan het recht op verwijdering, is door deze te voorzien van een aan- en uitknop voor gegevensverwerking en gegevensdoorgifte aan derden. Tenslotte kan het lokaliseren van dataopslag het gemakkelijker maken om dataverwerking en -gebruik in de hand te houden. In Europees verband is bijvoorbeeld gesproken over het oprichten van een Europees communicatienetwerk, daarnaast zijn in Duitsland verdergaande voorstellen gedaan om een nationale *cloud service* op te richten en buitenlandse bedrijven te weren die niet kunnen garanderen dat data niet met andere partijen worden gedeeld (Maurer, Skierka, Morgus & Hohmann, 2015; WRR, 2015).

Complexiteit speelveld
Diverse stakeholders spelen een rol in de ontwikkeling van het IoT. In de literatuur worden 1) overheid, 2) bedrijfsleven, 3) kennisinstellingen en 4) burgers aangewezen als de belangrijkste sleutelactoren voor technologische innovatie (Carayannis & Campbell, 2012).

Op *overheidsniveau* krijgen verschillende instanties en organen met het IoT te maken. Hierbij kan het gaan om instanties en organen zoals gemeentes, provincies, ministeries, agentschappen, zelfstandige bestuursorganen en toezichthouders. Uiteraard houden ook steeds meer *bedrijven* zich bezig met het IoT en op termijn zal ieder bedrijf in meerdere of mindere mate gebruik gaan maken van het IoT. Ten eerste zijn er bedrijven die IoT-producten maken. Hieronder vallen zowel fabrikan-

[76] Zie ook: www.bright.nl/39-accept-or-decline-het-eindrapport

[77] Artikel 12, Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

ten die IoT-hardware en IoT-apparaten produceren, als bedrijven die IoT-software ontwikkelen. Ten tweede zijn er bedrijven die (nieuwe) diensten aanbieden met behulp van het IoT. Ook kunnen dienstverleners invloed hebben op het IoT zonder daar zelf direct iets mee toe doen. Verzekeraars kunnen bijvoorbeeld bepaalde eisen stellen (zie ook paragraaf 4.2.3). *Kennisinstellingen* doen onderzoek naar nieuwe IoT-technologieën en de mogelijke gevolgen daarvan. Daarnaast verzorgen zij (basis)onderwijs en om- of bijscholing over technologie. *Burgers* hebben verschillende rollen, bijvoorbeeld als consument, kiesgerechtigde en cliënt. In deze verschillende rollen hebben zij invloed op de ontwikkeling van het IoT door wel of niet gebruik te (gaan) maken van een IoT-toepassing of -dienst.

Door de grote hoeveelheid aan (veelal buitenlandse) spelers op de IoT-markt ontbreekt het aan overzicht. Hierdoor is het onduidelijk wie waar verantwoordelijk voor is en wie waar op kan worden aangesproken. Dit probleem wordt verergerd doordat overheden verschillende regels en standaarden hanteren en daarnaast ook andere belangen hebben. In Europa zit Nederland in de kopgroep wat betreft het gebruik van digitale technologie (CSR, 2016c), maar desondanks kan Nederland slechts beperkt invloed uitoefenen op ontwikkelingen aangaande het IoT. Het creëren van standaarden zal bijvoorbeeld op internationaal niveau moeten plaatsvinden en de invloed van Nederland hierop is beperkt. Zelfs als Nederland (al dan niet in Europees of bilateraal verband met de Verenigde Staten) bepaalde ontwikkelingen afkeurt of tegen probeert te houden zal hun toepassing in het buitenland gevolgen kunnen hebben voor Nederland. Op geopolitiekniveau zal de invloed van Nederland en andere westerse landen wat betreft het internet en het IoT kleiner worden (Dommering et al., 2014; WRR, 2015).

Maatregelen
In dit complexe, grensoverschrijdende speelveld kan de samenwerking op het gebied van veiligheid en privacy (op EU-niveau en daarbuiten) nog worden vergroot, bijvoorbeeld op het gebied van keurmerken en standaarden. Zo kunnen in EU-verband en daarbuiten makkelijker veiligheidseisen worden afgedwongen. Producenten hebben de voorkeur om één versie van hun product te maken die voor alle markten geschikt is. Daarmee bepaalt de grootste afzetmarkt indirect de veiligheids- en privacy-eisen die aan een product worden gesteld. Ook voor veel van de maatregelen besproken in de voorgaande subparagrafen geldt dat deze het meest effectief in internationaal verband kunnen worden gerealiseerd.

4.2.2 Kennis en bewustzijn

Het treffen van maatregelen om veiligheids- en privacyrisico's tegen te gaan wordt ook bemoeilijkt door een gebrek aan bewustzijn en kennis over (risico's rondom) het IoT en ICT in het algemeen. Dit geldt zowel voor de overheid, burgers, als het bedrijfsleven. Door dit gebrek aan kennis en bewustzijn zullen deze partijen niet altijd de meest effectieve maatregelen treffen.

Veel van de geïnterviewde experts geven aan dat beleidsmakers onvoldoende kennis van en bewustzijn hebben over het IoT en de daarbij horende veiligheids- en privacyrisico's. Ook uit het rapport van de commissie Elias blijkt dat er een groot probleem ligt wat betreft kennis over ICT en technologische ontwikkelingen bij de overheid – er wordt zelfs gesproken van een 'bijna onoverbrugbare kloof' tussen ICT'ers en beleidsmakers.[78] Bovendien is een groot gedeelte van de aanwezige

[78] Tweede Kamer 2014–2015, 33 326, nr. 5., p. 16.

kennis extern ingehuurd en om deze reden niet geborgd binnen de organisatie (Algemene Rekenkamer, 2016).

Veel consumententoepassingen zullen de komende jaren deel uit gaan maken van het IoT. Voldoende kennis over mogelijke privacy- en veiligheidsrisico's onder burgers draagt dan ook bij aan een veilig(er) gebruik van deze toepassingen. Ook voor bedrijven is het van belang dat zij zich bewust zijn van de mogelijke nadelige gevolgen van onveilige producten, zoals recente inbraken op IoT-apparaten in ziekenhuizen (Gallagher, 2016) en bij overheidsinstanties (Goodman, 2015). Voldoende kennis kan fabrikanten helpen om bij het ontwerpen van hun IoT-producten en -diensten rekening te houden met beveiliging en bescherming van persoonsgegevens (Ministerie van Economische Zaken, 2016).

Het beperken van veiligheids- en privacyrisico's is extra lastig doordat er continu nieuwe ontwikkelingen plaatsvinden. Voor traditionele auto's geldt bijvoorbeeld dat, zolang de natuurwetten niet veranderen, het duidelijk is aan welke veiligheidseisen een auto moet voldoen om het risico op auto-ongelukken te minimaliseren. Voor zelfrijdende auto's veranderen de 'natuurwetten' echter voortdurend doordat er iedere dag nieuwe beveiligingslekken kunnen ontstaan of worden ontdekt (Farooqui, 2015). Het op peil houden van de kennis van stakeholders is daarom een belangrijke voorwaarde om in te kunnen spelen op nieuwe ontwikkelingen en de juiste maatregelen te treffen.

Maatregelen

Investeren in onderwijs is een belangrijk instrument om veilig internetgebruik en digitale vaardigheden in Nederland te vergroten (CSR, 2016c; Munnichs et al., 2017). Dit geldt voor het basis- en voortgezet onderwijs, maar ook voor het om- en bijscholen van werknemers. Ook kunnen kennisinstellingen in onderzoek en onderwijs meer aandacht geven aan kritische reflectie over veiligheid en privacy bij het ontwikkelen en gebruiken van IoT-toepassingen. Informatiecampagnes over cyberveiligheid en cyberhygiëne kunnen daarnaast het bewustzijn en daarmee de digitale weerbaarheid van burgers vergroten. Hier kan aansluiting worden gezocht bij al lopende initiatieven op dit gebied, zoals Alert Online (CSR, 2016c).

Door het doen van onderzoek kan de kennis over de huidige stand van zaken wat betreft technologie, cybersecurity en -privacy worden bijgehouden en vergroot (bijvoorbeeld op het gebied van zero-days[79]). Publiek-private samenwerkingen kunnen daarbij helpen door het monitoren en delen van informatie over actuele dreigingen. Deze samenwerking vindt nu al plaats, maar kan verder worden geïntensiveerd (CSR, 2016c).

Om veiligheidsrisico's van het IoT te beperken is het van belang dat de overheid over voldoende ICT-kennis beschikt. Op dit gebied lopen al enkele initiatieven. De minister van Wonen en Rijksdienst (W&R) heeft bijvoorbeeld aangegeven dat de komende jaren wordt geïnvesteerd in personeel op het gebied van ICT om kennis en kunde binnen de organisatie te borgen (Blok, 2016).

[79] Een zero-day is een lek in software dat ontdekt wordt door derden, buiten de maker van de software om, waarvoor nog geen patch voorhanden is. Hackers die misbruik maken van zo'n kwetsbaarheid, die razendsnel kan worden rondgedeeld, kunnen via het gat bijvoorbeeld gevoelige informatie ontvreemden. Zie ook: http://computerworld.nl/security/74895-wat-is-een-zero-day-exploit

4.2.3 Prikkels

Het nemen van veiligheidsmaatregelen wordt ook belemmerd door een gebrek aan prikkels bij gebruikers en bedrijven. Gebruikers zijn zich vaak niet bewust van veiligheids- en privacyrisico's en ondervinden in veel gevallen ook geen hinder als hun IoT-apparaten worden gehackt (Van Voorst, 2016). Een slimme thermostaat die deel uitmaakt van een botnet zal bijvoorbeeld niet noodzakelijkerwijs zijn functionaliteit verliezen (Schneier, 2016a). Hierdoor is er voor veel gebruikers geen noodzaak om hun gedrag aan te passen.

Er zijn verschillende redenen waarom prikkels voor bedrijven ontbreken. Allereerst bestaat er een economische prikkel om een product, met of zonder adequate beveiliging, als eerste naar de markt te brengen (Wolters & Verbruggen, 2016). Als het apparaat eenmaal verkocht is, is de motivatie beperkt om de beveiliging nog te voorzien van updates (Jacobs, 2016). Beveiliging kost in een dergelijke situatie tijd en geld, en levert in de meeste gevallen niets extra's op (Munnichs et al., 2017). Daarbij kan beveiliging haaks staan op functionaliteit, compatibiliteit en gebruiksvrijheid (Bauer & Van Eeten, 2009). Voor start-ups, die verantwoordelijk zijn voor veel nieuwe IoT-producten, zijn er nog minder prikkels omdat er voor hen minder op het spel staat dan voor bestaande (grote) bedrijven (Haas, Haas & Weinert, 2015).

Bij het produceren van IoT-producten zijn verschillende partijen betrokken. Fabrikanten combineren of *re-branden* verschillende hard- en software van andere fabrikanten. Zij werken vaak met kleine winstmarges, zijn gericht op het ontwikkelen van volgende producten en voor hen is er dan ook geen prikkel om onderhoud te plegen aan oude apparatuur en software (Schneier, 2014, 2016b). ISP's kunnen een belangrijke partner zijn om risico's te mitigeren[80], maar ook voor hen geldt dat er weinig prikkels zijn om dit te doen. Daarom vermijden ze vaak de extra kosten die hiermee gepaard gaan (Asghari, Van Eeten & Bauer, 2015; Bauer & Van Eeten, 2009).

Maatregelen
Prikkels ontbreken bij zowel gebruikers als fabrikanten. In principe mag de gebruiker er echter van uitgaan dat fabrikanten deugdelijke producten verkopen[81]. Het ligt daarom voor de hand om maatregelen te treffen die prikkels voor fabrikanten genereren. Eén van die maatregelen is het verder versterken van de zorgplicht. Een zorgplicht is een plicht 'tot het rekening houden met, en eventueel handelen ten behoeve van, de belangen van een ander' (Tjong Tjin Tai, 2006, p. 376). Onder deze zorgplicht kan ook de beveiliging van IoT-producten vallen. Aansprakelijkheid op basis van schade veroorzaakt door IoT-producten kan ook een belangrijke prikkel zijn voor bedrijven en daarnaast ook dienen als grond voor de zorgplicht. Voor beide maatregelen geldt dat deze nu al van toepassing zijn op IoT-toepassingen, maar voor beiden gelden nog wel beperkingen die in paragraaf 4.2.4 nader worden toegelicht.

Doordat er veel partijen betrokken zijn bij het produceren van IoT-producten, kan het invoeren van ketenverantwoordelijkheid eraan bijdragen dat de beveiliging van IoT-producten wordt gewaarborgd. Betrokken partijen kunnen elkaar regels opleg-

[80] ISP's spelen bijvoorbeeld een belangrijke rol bij het bestrijden van botnets (Asghari et al., 2015).

[81] Zie ook: www.acm.nl/nl/onderwerpen/consumentenrecht/garantie-en-conformiteit/recht-op-een-deugdelijk-product

gen, eisen stellen aan de beveiliging en indien nodig elkaar aansprakelijk stellen voor eventuele schade (CSR, 2016c).

Een andere mogelijke prikkel voor bedrijven is de komst van cyberrisicoverzekeringen. Doordat cyberrisico's steeds groter worden kan het voor bedrijven aantrekkelijk zijn om dit soort verzekeringen af te sluiten. Een belangrijke voorwaarde bij het afsluiten van deze verzekeringen is de mitigerende maatregelen die betrokkenen zelf al hebben genomen. Om het risico in te schatten wordt door verzekeraars vaak gebruikgemaakt van bestaande veiligheidsstandaarden. Daarmee kunnen verzekeringen als prikkel dienen om bepaalde beveiligingsmaatregelen te treffen en beveiligingsstandaarden in te voeren.

Voor ISP's worden nu al beleidsmatig prikkels gecreëerd. Een voorbeeld hiervan is het Nederlandse anti-botnet centrum AbuseHub dat deels gefinancierd wordt door de overheid en waarin verschillende ISP's samenwerken. Dit creëert enerzijds druk op ISP's om maatregelen te nemen en anderzijds verlaagt het de mitigatiekosten voor ISP's (Asghari et al., 2015).

Ten slotte kan de overheid ook sturing geven via hun eigen inkoopbeleid. De overheid neemt ongeveer dertig procent af van alle beveiligingsproducten en -diensten in Nederland (Munnichs et al., 2017). Hiermee vervult de overheid een voorbeeldrol, en kan het als *launching customer* bijdragen aan kennisopbouw en andere partijen ertoe bewegen te innoveren en investeren op het gebied van cybersecurity (Munnichs et al., 2017). In het inkoopbeleid kan ook als voorwaarde worden opgenomen dat alleen producten en diensten worden afgenomen die aan bepaalde standaarden of keurmerken voldoen, waardoor dit ook als prikkel voor het gebruik van standaarden en keurmerken kan dienen.

4.2.4 Toezicht en handhaving

Het effect van prikkels beschreven in de vorige paragraaf wordt beperkt door een gebrek aan toezicht en handhaving. Zonder deze stok achter de deur zijn maatregelen zoals zorgplicht en aansprakelijkheid minder effectief. Ook het Rathenau Instituut concludeert dat toezicht en handhaving essentieel zijn voor de naleving van de zorgplicht (Munnichs et al., 2017). Bestaande regelgeving wordt vaak moeizaam of niet gehandhaafd. De meldplicht datalekken laat bijvoorbeeld zien dat de dreiging van boetes voor bedrijven (vooralsnog) beperkt is. Deze meldplicht bestaat sinds januari 2016 en verplicht bedrijven datalekken te melden en maatregelen te treffen. Indien dit niet gebeurt kan de Autoriteit Persoonsgegevens (AP) een boete opleggen van maximaal € 820.000 per overtreding of 10% van de jaaromzet.[82] In het eerste jaar zijn er 5.500 meldingen gemaakt en zijn er aanvullende onderzoeken uitgevoerd. Dit heeft echter nog niet geleid tot boetes, maar wel tot enkele waarschuwingen.[83] Naar verwachting zijn er 18.500 datalekken niet gemeld (Pb7 Research, 2017). Voor sommige organisaties lijkt het vooralsnog dan ook voordeliger om datalekken niet te melden in plaats van wel (De Lange, 2016).

---

[82] Zie ook: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

[83] De AP heeft ruim 4.000 binnengekomen meldingen nader bekeken en soms aanvullende vragen gesteld. Ruim honderd organisaties kregen naar aanleiding hiervan een waarschuwing van de AP. In enkele andere tientallen gevallen doet de AP een diepgaander onderzoek. Deze onderzoeken lopen nog. Zie ook: https://autoriteitpersoonsgegevens.nl/nl/nieuws/1-jaar-meldplicht-datalekken

Ook voor keurmerken en standaarden geldt dat deze alleen effectief zijn met toezicht en handhaving. Een voorbeeld hiervan is de CE-markering. De CE-markering dient als middel om aan te tonen dat een product voldoet aan geldende Europese eisen zoals veiligheid, gezondheid en milieu. Desondanks worden er jaarlijks tientallen CE-gemarkeerde producten van de markt teruggetrokken omdat zij een risico vormen voor de gezondheid of veiligheid van gebruikers (Algemene Rekenkamer, 2017). De Algemene Rekenkamer (2017, p. 7) concludeert onder meer dat op dit moment de middelen en capaciteit tekort schieten voor effectief toezicht op de CE-markering. Dit keurmerk is (nog) niet gericht op security, safety of privacy, maar het toont wel aan dat een keurmerk alleen niet voldoende is om te garanderen dat een product voldoet aan bepaalde vereisten.

Voor zorgplicht en aansprakelijkheid geldt daarnaast dat het nog niet altijd duidelijk is wat de reikwijdte ervan is. Voor de zorgplicht is dit in sommige gevallen heel concreet. IoT-toepassingen waarbij persoonsgegevens worden verwerkt hebben bijvoorbeeld zorgplichten op grond van de Wbp (welke verder worden uitgebreid met de komst van de AVG). Op basis van deze zorgplichten worden aanbieders geacht veiligheidsmaatregelen te treffen. Wanneer het gaat om het bijwerken van onveilige software op IoT-toepassingen is dit echter minder concreet en zal de exacte invulling ervan vaak per geval (door de rechter) moeten worden beoordeeld (Tjong Tjin Tai, Koops, Heij, Silva & Skorvánek, 2015; Wolters & Verbruggen, 2016). Wat betreft aansprakelijkheid is het bij disfunctionerende software vaak lastig om aan te tonen waar het probleem ligt en dus wie daarvoor verantwoordelijk is. Hierdoor kan aansprakelijkheid vaak worden ontweken. Daarnaast komt het ook voor dat aansprakelijkheid in de algemene voorwaarden buiten spel wordt gezet (Engelfriet, 2011). Als gevolg van deze onduidelijkheden wordt het ook lastiger om effectief te handhaven.

Maatregelen

Effectief toezicht en effectieve handhaving zijn een belangrijke voorwaarde om prikkels zoals de zorgplicht te realiseren. Daarnaast is het ook een belangrijke voorwaarde voor maatregelen zoals keurmerken en standaarden. Meer investeren in toezicht en handhaving ligt daarom voor de hand, maar het gewenste (acceptabele) niveau en de inrichting van toezicht en handhaving zal nader moeten worden bepaald (WRR, 2013).

Daarnaast schieten de (open) normen van zorgplicht en aansprakelijkheid nu nog tekort. Over de invulling van de zorgplicht voor leveranciers van hard- en software zal verder onderzoek en discussie nodig zijn. Dit wordt ook geconcludeerd in een recent onderzoek van het Rathenau Instituut (Munnichs et al., 2017). Daarnaast zal bij de invulling van de zorgplicht helder moeten worden gemaakt wat de eindgebruiker mag verwachten van de aanbieder (CSR, 2016c). Hierbij zal ook bepaald moeten worden hoe zorgplicht en aansprakelijkheid zich verhouden tot de levensduur van producten. Veel producten worden namelijk slechts enkele jaren ondersteund terwijl ze vele jaren langer meegaan (een thermostaat wordt bijvoorbeeld zelden vervangen).[84] Er zal daarom ook moeten worden nagedacht of bedrijven verplichtingen (zouden moeten) hebben na de levensduur van de producten.

[84] Een mogelijk genoemde oplossing kan zijn dat software die door de fabrikant niet meer wordt onderhouden automatisch open source wordt (Jacobs, z.j.).

4.2.5 Casus: elektronisch sleutelsysteem

Recent zijn er verschillende incidenten geweest die duidelijk maken dat IoT-toepassingen op dit moment niet voldoende beveiligd zijn en daardoor schade kunnen veroorzaken. In deze casus wordt aan de hand van een van deze incidenten geïllustreerd hoe de hierboven beschreven factoren een veilig gebruik van IoT-toepassingen belemmeren en waarom het lastig is om mitigerende maatregelen te treffen.

Kortgeleden hebben criminelen tot drie keer toe het netwerk van een luxueus hotel in Oostenrijk gehackt.[85] Ze maakten het elektronisch sleutelsysteem van het hotel onklaar, waardoor nieuwe hotelgasten hun kamer niet in konden. Hiermee persten de hackers de directeur van het hotel af, die vervolgens de vereiste som van € 1.500 in bitcoins aan losgeld betaalde. Na de derde hack heeft de directeur besloten om terug te gaan naar fysieke sleutels. Het hotel heeft geen geld teruggekregen van de verzekering omdat de schuldigen niet gevonden konden worden. Ook de politie kon niets doen.

Deze casus laat zien dat de beveiliging van deze IoT-toepassing wordt bemoeilijkt door verschillende factoren.

1. *Complexiteit: In deze casus is de fabrikant in principe verantwoordelijk voor de beveiliging van het elektronische sleutelsysteem. Het zou echter kunnen dat de beveiliging van het systeem zelf op orde was, maar dat hackers toch in konden breken doordat het standaardwachtwoord niet gewijzigd was of doordat het netwerk van het hotel niet goed beveiligd was. Vanwege de complexiteit van de technologie is het dus niet evident waar het beveiligingslek precies zit.*
2. *Gebrek aan kennis: Na betaling van losgeld werkt het sleutelsysteem weer, maar dit blijkt slechts een tijdelijke oplossing te zijn. De directeur van het hotel lijkt niet in staat om de kern van het beveiligingsprobleem op te lossen en besluit over te stappen op fysieke sleutels. Dat deze hack tot drie keer toe heeft kunnen plaatsvinden wijst naast de complexiteit hoogstwaarschijnlijk ook op een gebrek aan kennis.*
3. *Gebrek aan prikkels, toezicht en handhaving: Door de complexiteit is het onduidelijk hoe de hack heeft kunnen plaatsvinden. Hierdoor wordt noch de fabrikant van het sleutelsysteem, noch de netwerkbeheerder, in deze casus aansprakelijk gesteld voor de schade die het hotel ondervindt. Het hotel draait zelf op voor de kosten van de afpersing. Voor de fabrikant en provider zijn er dus ook geen prikkels gecreëerd om hun producten en diensten in de toekomst veiliger te maken.*

4.3 Deelconclusie

In dit hoofdstuk zijn verschillende maatregelen besproken die kunnen bijdragen aan enerzijds het aanjagen van de economische groei door het IoT en anderzijds het verkleinen van de veiligheids- en privacyrisico's van het IoT (zie figuren 4.1 en 4.2 voor een overzicht). Het overzicht aan maatregelen laat zien dat het bedrijfsleven primair aan zet is om nieuwe en innovatieve, maar ook veilige en privacybeschermende IoT-toepassingen te realiseren. De overheid kan dit faciliteren door verschillende, met elkaar samenhangende maatregelen te treffen. Dit wordt hieronder nader toegelicht.

[85] Zie ook: www.ad.nl/digitaal/sleutelpasjes-eeuwenoud-oostenrijks-hotel-gehackt~a54de529

Als producent van IoT-toepassingen en -infrastructuur is het *bedrijfsleven* uiteindelijk de partij die ervoor kan zorgen dat kansen van het IoT benut worden en bedreigingen worden tegengegaan. Fabrikanten en dienstverleners kunnen nieuwe, innovatieve IoT-toepassingen op de markt brengen en zij zijn in principe ook verantwoordelijk voor het produceren en leveren van veilige, privacybeschermende IoT-producten en -diensten. Op dit moment schieten zij echter vaak nog tekort in het beveiligen van IoT-apparaten. Dit kan verklaard worden door de belemmerende factoren die zijn besproken in dit hoofdstuk (zie figuur 4.2 en paragraaf 4.2), waarbij met name het gebrek aan prikkels een belangrijke factor is.

Met de verschillende maatregelen zoals genoemd in dit hoofdstuk kan de *overheid* belemmerende factoren wegnemen en hanteerbaarder maken, waardoor bedrijven gestimuleerd worden om kansen te benutten en bedreigingen te beperken. Om het bedrijfsleven in beweging te zetten zijn de juiste prikkels (zie paragraaf 4.2.3) cruciaal. Aangezien de verschillende maatregelen die in dit hoofdstuk zijn besproken sterk met elkaar samenhangen, is het creëren van prikkels alleen niet genoeg. Prikkels zoals zorgplicht en aansprakelijkheid zijn bijvoorbeeld alleen effectief als er voldoende toezicht wordt gehouden en de regels worden gehandhaafd. Ook kunnen bedrijven hun verantwoordelijkheid pas nemen op het moment dat zij hiervoor voldoende kennis in huis hebben. De overheid kan hierop inspelen door lesprogramma's in te richten die huidige en toekomstige werknemers goed voorbereiden op een wereld met het IoT. Tot slot kan de overheid een bemiddelende rol spelen in (internationale) samenwerkingen, die bedrijven zelf soms moeilijk in kunnen nemen. Kortom, de overheid kan omstandigheden creëren waarbinnen bedrijven maximaal kunnen bijdragen aan een positieve, en vooral veilige, ontwikkeling van het IoT.

Op dit moment lopen er al verschillende overheidsinitiatieven en bestaan er verschillende adviesorganen die helpen om de ontwikkeling van het IoT in goede banen te leiden. Het initiatief van minister Schultz van Haegen van I&M faciliteert bijvoorbeeld het ontwikkelen en testen van zelfrijdende auto's in Nederland (zie paragraaf 4.1.6). Echter, deze initiatieven zijn verspreid over verschillende organen en instanties en deze worden niet altijd (goed) op elkaar afgestemd. Daarnaast zijn activiteiten vaak gericht op een deel van de problematiek, bijvoorbeeld specifiek op zelfrijdende auto's of cyberveiligheid, maar ontbreekt een overkoepelend perspectief op het geheel. Dit is zorgelijk aangezien de kansen, bedreigingen en maatregelen rondom het IoT sterk met elkaar samenhangen. De maatregelen genoemd in dit hoofdstuk zijn pas effectief als ze als geheel worden genomen. Hiervoor is visie, coördinatie en sturing nodig.

In meerdere adviesrapporten wordt overheden aangeraden om een visie op het IoT te ontwikkelen en een sturende en coördinerende rol te spelen in de uitvoering ervan (zie ook paragraaf 4.1.5). Verschillende van de geïnterviewde experts hebben ook het belang van een overheidsvisie op het IoT-beleid benadrukt. Het ontwikkelen van een visie en het coördineren en sturen van de uitvoering ervan vereist dat er één instantie wordt aangewezen als hoofdverantwoordelijke op IoT-gebied. Dit kan bijvoorbeeld een overkoepelend orgaan zijn, een nieuw ministerie of een afdeling binnen een bestaand ministerie. Deze centrale instantie kan een sturende en coördinerende rol spelen bij het op elkaar afstemmen van verschillende initiatieven voor zowel het aanjagen van de economische kansen van het IoT als het beperken van veiligheidsrisico's.

5 Conclusie

Dit rapport beschrijft de resultaten van een breed en verkennend WODC-onderzoek naar het IoT in Nederland. Hierin zijn onder andere mogelijke toepassingen van het IoT onderzocht en is nagegaan welke kansen en bedreigingen het IoT met zich meebrengt. Ook is er een aantal handelingsperspectieven uiteen gezet. De hoofdvraag van het onderzoek luidt als volgt:

Wat zijn de kansen en bedreigingen van het IoT en hoe kunnen verschillende stakeholders de ontwikkeling van het IoT in Nederland op een positieve manier beïnvloeden?

In dit hoofdstuk wordt beknopt antwoord gegeven op bovenstaande onderzoeksvraag door de vier deelvragen te beantwoorden (paragraaf 5.1). Vervolgens worden suggesties gedaan voor vervolgonderzoek (paragraaf 5.2) en wordt het rapport afgesloten met een slotwoord (paragraaf 5.3).

5.1 Antwoorden op de onderzoeksvragen

In deze paragraaf worden de antwoorden op de deelvragen samengevat en vervolgens wordt een antwoord gegeven op de hoofdvraag van dit onderzoek.

Hoofdstuk 1 en 2 geven antwoord op de eerste deelvraag: *Wat behelst het IoT?*. In hoofdstuk 1 wordt het IoT gedefinieerd als '*een netwerk van objecten (vaak verbonden met het internet), die gegevens verzamelen over hun omgeving, deze kunnen uitwisselen en op basis daarvan (semi)autonome beslissingen nemen en/of acties uitvoeren die van invloed zijn op de omgeving'*. Deze definitie is gehanteerd in de rest van het rapport. Hoofdstuk 2 bevat vervolgens een overzicht van het ontstaan van het IoT, een bespreking van de (meest) onderscheidende kenmerken van het IoT (communiceren, waarnemen, data analyseren, en (semi)autonome acties uitvoeren) en een beschrijving van de verschillende toepassingsgebieden (lichaam, woon- en werkruimte, stad, en land). Dit alles is geïllustreerd met een aantal voorbeelden.

Hoofdstuk 3 geeft antwoord op de deelvragen: *Welke kansen biedt het IoT?* en *Welke bedreigingen brengt het IoT met zich mee?* In dit hoofdstuk zijn de belangrijkste kansen en bedreigingen van het IoT in kaart gebracht door de positieve en negatieve effecten van het IoT op menselijke waarden te bespreken. Het hoofdstuk laat zien hoe het IoT menselijk welzijn (gemak, gezondheid en veiligheid), duurzaamheid, productiviteit en welvaart kan bevorderen. Dit zijn de kansen van het IoT. Vervolgens zijn de mogelijke negatieve gevolgen van het IoT op veiligheid, privacy, welvaart, welzijn, gelijkwaardigheid en autonomie besproken. Dit zijn de bedreigingen die het IoT met zich meebrengt. Voor zowel de kansen als bedreigingen geldt dat deze veroorzaakt worden door de grote hoeveelheid data die het IoT produceert en gebruikt.

In het slot van het hoofdstuk wordt geconcludeerd dat het IoT een grote impact op onze samenleving zal hebben. De grootste kansen lijken te liggen in het realiseren van economische groei en de belangrijkste bedreigingen worden gevormd door risico's op het gebied van veiligheid en privacy. Hierbij is er geconstateerd dat om

van de economische groei te kunnen profiteren, het nodig is om ook (eerst) de bedreigingen aan te pakken.

Hoofdstuk 4 geeft antwoord op de deelvraag: *Wat zijn de maatregelen die verschillende stakeholders kunnen nemen om de kansen van het IoT te benutten en de bedreigingen ervan te beperken?* Er zijn verschillende factoren die van invloed zijn op de kansen op het gebied van economische groei en de bedreigingen aangaande veiligheid en privacy. Deze factoren vragen om verschillende maatregelen, die het meest effectief zijn als zij in samenhang worden genomen. Hoewel het initiatief met name ligt bij het bedrijfsleven, kan de overheid bedrijven stimuleren door maatregelen te treffen.

Voortbouwend op hoofdstuk 3 zijn diverse maatregelen genoemd die economische groei door het IoT kunnen bevorderen. Deze maatregelen richten zich op 1) factoren die gelden als aanjagers van economische groei en 2) factoren die samen de randvoorwaarden van de economische groei bepalen. Hierbij gaat het onder meer om het investeren in onderwijs en digitale vaardigheden, het stimuleren van onderzoek naar nieuwe innovaties en het bieden van ruimte om hiermee te experimenteren, het opstellen van een visie aangaande het IoT en het coördineren van en sturing geven aan deze visie. Daarnaast zal het nemen van maatregelen om veiligheids- en privacyrisico's te beperken noodzakelijk zijn om volledig te kunnen profiteren van de kansen die het IoT biedt.

Vervolgens is geconstateerd dat het ontwikkelen en gebruiken van veilige en privacyvriendelijke IoT-toepassingen wordt bemoeilijkt door de volgende factoren: 1) de complexiteit van het IoT, 2) gebrek aan kennis en bewustzijn, 3) gebrek en prikkels, en 4) gebrek aan toezicht en handhaving. Per factor zijn maatregelen genoemd die het belemmerende effect van de betreffende factor kunnen verminderen. Hierbij gaat het onder meer om het nemen van gelaagde veiligheidsmaatregelen, het opstellen van standaarden en keurmerken in Europees of internationaal verband, het verbeteren van gebruikersrechten ten aanzien van data, het investeren in onderwijs en onderzoek, het toepassen (of toepasbaar maken) van de zorgplicht en aansprakelijkheid op IoT-producten en het borgen van toezicht en handhaving.

Samen geven deze uitkomsten antwoord op de hoofdvraag van dit onderzoek: *Wat zijn de kansen en bedreigingen van het IoT en hoe kunnen verschillende stakeholders de ontwikkeling van het IoT in Nederland op een positieve manier beïnvloeden?* Samengevat zijn dit de belangrijkste conclusies van dit onderzoek:

- Het IoT verschaft een scala aan mogelijkheden om welzijn, duurzaamheid, productiviteit en welvaart in onze maatschappij te verhogen. IoT-toepassingen zijn op dit moment echter slecht beveiligd en vormen daarmee een bedreiging voor onze veiligheid en privacy, maar ook voor het verwezenlijken van de kansen. Het Mirai-botnet, bestaande uit gehackte IoT-apparaten, laat zien dat de impact nu al groot is. Dit zal in de toekomst alleen nog maar verder toenemen. Het is daarom van belang dat de veiligheids- en privacyrisico's worden aangepakt om schade zo veel mogelijk te beperken en voorkomen. Om te kunnen profiteren van de kansen die het IoT biedt, moet er tevens, op een veilige manier, ruimte worden geboden voor nieuwe ontwikkelingen en innovatie.
- Als producent van IoT-toepassingen en -infrastructuur zijn bedrijven verantwoordelijk voor het realiseren van nieuwe en innovatieve, maar ook veilige en privacybeschermende IoT-toepassingen. Dit gebeurt onvoldoende door de grote complexiteit van het IoT en een gebrek aan kennis, prikkels, en toezicht en handhaving.

- Er is geen *one size fits all* maatregel die deze problematiek kan oplossen; in plaats daarvan zijn er verschillende samenhangende maatregelen nodig die pas effectief zijn als zij als geheel worden doorgevoerd.
- Hoewel het initiatief ligt bij het bedrijfsleven, kan de overheid bedrijven stimuleren door maatregelen te treffen op de volgende gebieden: 1) het creëren van prikkels voor bedrijven en erop toezien dat regelgeving gehandhaafd wordt, 2) het vergroten van kennis en bewustzijn in de samenleving, en 3) het faciliteren van publiek-private en internationale samenwerking. Dit vereist een gedragen overheidsvisie, waarbij er één instantie wordt aangewezen als hoofdverantwoordelijke die dit beleid coördineert en stuurt. Omdat het IoT samenhangt met andere technologische ontwikkelingen en cybersecurity in bredere context, zou een visie ook op deze onderwerpen betrekking moeten hebben.

5.2 Aanbevelingen voor vervolgonderzoek

Dit onderzoek is verkennend en breed van aard. Zoals genoemd in paragraaf 1.2.4 en uitgebreider beschreven in hoofdstuk 2, behelst het IoT niet één bepaalde techniek, één bepaalde toepassing, of één bepaald domein. In tegendeel, het IoT bevat verschillende technieken en technologieën en kent tal van toepassingen binnen velerlei domeinen, met grote onderlinge verschillen tussen de diverse IoT-producten en -diensten. In dit rapport worden vele belangrijke ontwikkelingen en toepassingen op het gebied van het IoT besproken. Door deze focus op breedte gaat het onderzoek slechts in beperkte mate dieper in op die ontwikkelingen. Dit zou in vervolgonderzoek opgepakt kunnen worden. In deze paragraaf wordt daartoe een aantal aanbevelingen gedaan.

Ten eerste zou dieper ingegaan kunnen worden op de verschillende specifieke toepassingen van het IoT. De verschillende producten, domeinen en contexten waarin het IoT wordt toegepast kennen hun eigen kansen en bedreigingen. Bij smart-home-oplossingen om ouderen langer zelfstandig laten wonen, speelt privacy bijvoorbeeld een belangrijke rol, terwijl bij zelfrijdende auto's veiligheid een belangrijke rol speelt. Vervolgonderzoek zou zich erop kunnen richten om de belangrijkste kansen, bedreigingen en handelingsperspectieven van specifieke IoT-toepassingen of toepassingsdomeinen in kaart te brengen. Daarbij kan de opdracht worden gegeven om de economische kansen van bepaalde IoT-toepassingen te proberen te kwantificeren, teneinde de invloed en potentie van de toepassingen beter te kunnen inschatten.

In het verlengde hiervan, is een tweede aanbeveling om onderzoek te doen naar het kwantificeren van de effecten van verschillende maatregelen. Het voorliggende onderzoek beschrijft wel de verwachte gevolgen van verschillende (in)acties, maar gaat niet in op hoe sterk de effecten van verschillende maatregelen zijn. In een vervolgonderzoek kan, zoals hierboven geschetst, geprobeerd worden om eerst de invloed van het IoT op de benoemde waarden te meten (bijvoorbeeld: in welke mate verhoogt het IoT de welvaart?). Vervolgens kan geprobeerd worden te meten in welke mate bepaalde voorgestelde maatregelen invloed hierop hebben. Dit kan weer afgezet worden tegen de verwachte ontwikkelingen als er niet wordt ingegrepen. Hierbij zouden ook de interactie-effecten tussen verschillende handelingsperspectieven meegenomen kunnen worden.

In dit kader kan, als derde aanbeveling, nog dieper ingegaan worden op de handelingsperspectieven. Per toepassing, domein of techniek zouden specifiekere

maatregelen geïdentificeerd kunnen worden. Dit vervolgonderzoek zou zich dan ook kunnen richten op de effecten van verschillende handelingsperspectieven. Daarbij kan bijvoorbeeld worden onderzocht wat de haalbaarheid en effectiviteit is van een overkoepelend orgaan dat ontwikkelingen op het gebied van het IoT coördineert en stuurt. Gegeven de complexiteit van de materie zal het echter slechts beperkt mogelijk zijn om hier gegronde uitspraken over te doen.

Een vierde aanbeveling voor vervolgonderzoek is om dieper in te gaan op de technische details van IoT-producten. Betere kennis over de technische mogelijkheden op het gebied van bijvoorbeeld encryptie, netwerken en machine learning kan erbij helpen om veiligheidsrisico's beter in te schatten en nauwkeurigere en meer adequate handelingsperspectieven te formuleren. Daarbij kan ook worden gedacht aan meer technische onderzoeken waarin de beveiliging van populaire IoT-systemen wordt getest en suggesties voor verbeteringen worden gedaan. Het ministerie van EZ laat in dit kader een onderzoek uitvoeren naar de veiligheid van het Internet of Things (IoT) en hoe deze versterkt kan worden.[86]

Een vijfde aanbeveling is om meer onderzoek te doen naar het aanpassen van wet- en regelgeving. In het rapport wordt genoemd dat principes uit privacywetgeving, de zorgplicht en aansprakelijkheid zich soms lastig verhouden tot IoT-toepassingen. Vervolgnderzoek zou zich kunnen richten op hoe wetgeving aangepast kan worden zodat het ook dit soort toepassingen adresseert. Ook wordt er in het rapport een aantal suggesties gedaan om te komen tot nieuwe veiligheidsnormen van producten. Er worden echter geen concrete aanbevelingen gedaan over hoe dergelijke wetten of regels eruit zouden moeten zien. Ook zou er meer onderzoek gedaan kunnen worden naar de noodzaak tot het nemen van maatregelen en het aanpassen van wet- en regelgeving op Europees en internationaal niveau. Daarnaast zou kunnen worden onderzocht of de huidige wetgeving rondom netneutraliteit voldoende aansluit op het toekomstige IoT.[87]

Een laatste aanbeveling is om uitgebreider onderzoek te doen naar de geopolitieke consequenties van het IoT voor de internationale (vrij)handel en het economische verkeer. Doordat het IoT alle lagen van de samenleving zal beïnvloeden, kan het IoT een ongekende vermenging van politiek, technologie en economie tot gevolg hebben. Dit zal leiden tot nieuwe mondiale machtsblokken. Hierin kan onder andere ook de rol en de gevolgen van IoT in de kritieke infrastructuur worden meegenomen. Dit is in het onderzoek, gezien de scope, alleen zijdelings besproken.

5.3 Tot slot

Het IoT heeft nu al een sterke invloed op hoe we leven en werken en de impact op onze maatschappij zal in de toekomst alleen nog maar groter worden. Het IoT biedt tal van mogelijkheden om onze levens aangenamer te maken, ons werk efficiënter in te richten en op een duurzamere manier met de wereld om te gaan. Echter, op dit moment is de beveiliging van veel IoT-toepassingen ondermaats en vormen IoT-objecten een serieuze bedreiging voor onze veiligheid en privacy. In de komende jaren komt het er dus op aan op welke manier er met deze kansen en bedreigingen wordt omgaan. Gebeurt er niets, dan kan de verdere opkomst van een *verkeerd*

[86] Tweede Kamer 2016–2017, 29 544, nr. 773.

[87] Data afkomstig uit IoT-toepassingen zoals zelfrijdende auto's vragen wellicht andere behandeling dan data afkomstig uit streamingdiensten.

verbonden IoT ingrijpende gevolgen hebben. Door het nemen van de juiste maatregelen daarentegen zal Nederland aanzienlijk van het IoT kunnen profiteren.

Dit rapport laat zien dat de 'dingen' uit het IoT niet alleen met elkaar verbonden zijn, maar dat ze ook samenhangen met allerlei economische, sociale en technologische ontwikkelingen. Mede hierdoor bestaat er geen *one size fits all* maatregel die alle privacy- en veiligheidsrisico's in één keer weg kan nemen. Om de bedreigingen van het IoT tegen te gaan en de juiste voorwaarden te scheppen voor economische groei is een integrale benadering nodig, waarbij meerdere stakeholders met elkaar samenwerken om IoT-gerelateerde en aanverwante technologische ontwikkelingen bij te sturen door een reeks van met elkaar samenhangende maatregelen te nemen. Alleen zo kan een IoT ontstaan met veilige en betrouwbare verbindingen dat een positieve bijdrage levert aan onze samenleving.

Summary

(Mis)connected in a smart society
The Internet of Things: opportunities, threats and measures

Background, research question and scope

The Internet of Things (IoT) is a network of 'smart' devices, sensors and other objects, which are connected with each other and to the Internet. Several IoT applications are widely used in our society and the adoption of IoT will only increase in the coming years. On the one hand, the IoT offers opportunities by introducing new technological possibilities. On the other hand, it also brings new threats, related to cyber security. To seize the opportunities of IoT and minimize the threats we need to respond timely and adequately to these changes. For this reason the WODC has conducted a study on the IoT, its impact on society and the action perspectives for relevant stakeholders.

The key question of this research report is: *What are the opportunities and threats of the IoT and how can various stakeholders influence the development of the IoT in the Netherlands in a positive way?* To answer this research question, the following sub-questions were formulated.

1 What is the Internet of Things?
2 Which opportunities does the IoT present?
3 What challenges, pitfalls and threats does the IoT bring?
4 What measures can stakeholders take to further the opportunities of the IoT and mitigate the threats?

This study ought to be seen as an exploratory survey, aiming to provide a general overview of the relevant issues with respect to IoT. As a result, there was no room for an in-depth analysis of the subtopics.

Methodology

The research questions have been answered using the following methods: 1) desk research, 2) interviews, and 3) round-table discussions. The desk research has been conducted on the basis of an analysis of scientific literature, professional literature, and news articles with regard to developments in IoT. Six semi-structured interviews were held with experts and stakeholders in various relevant disciplines. Finally, two round table discussions were organized with the themes *Smart City* and *Smart Industry*. In both discussions several experts and stakeholders on the topic were present.

The opportunities and threats of the IoT are mapped, described and analysed according to human values, such as privacy, security and sustainability. Generally, technological developments will have both a positive and negative impact on human values. The most prominent values influenced by the IoT were determined on the basis of literature, interviews and the round-table discussions. These values have made it possible to identify the most important opportunities and threats, which in turn have been used to determine possible measures.

Results

IoT characteristics

The IoT involves a network of objects (often connected to the Internet), which collect and exchange data about their surroundings, and based on that take (semi) autonomous decisions and/or perform actions that affect the environment. The main features of the IoT are: 1) communication, 2) observation, 3) data analysis, and 4) conducting (semi) independent operations. The first feature of the IoT is that IoT objects are connected with each other and often to the Internet, so that they can communicate with each other and exchange data. The second characteristic of IoT objects is that they, by means of sensors, can perceive their environment or internal state. One might consider: sound, temperature and humidity. The third characteristic of the IoT is that there are large amounts of data to be collected and analyzed. These are both data that have been collected by the sensors of the IoT object itself, as well as data that have been collected by other objects. Various data analysis methods make it possible to deduce meaningful new information. The fourth feature of the IoT is that objects can perform actions that affect the environment or the object itself, for example by sending sound, light or radio waves. These actions may be initiated manually (by the user), but (increasingly), the object itself can also take autonomous decisions and execute actions.

Opportunities

New IoT technologies allow for various *opportunities*. In part, these developments have been made possible due to IoT (sensor) data that can be acquired increasingly fast. By combining, analyzing and interpreting these data, processes are more transparent and new insights can be obtained. Improved understanding and transparency can contribute to better and informed decisions (whether by governments, businesses or citizens). As a result, the IoT can have a strong posi-tive impact on the following values: well-being, sustainability, productivity and prosperity. In turn, all these opportunities may contribute to economic growth, profit or cost savings. IoT applications in healthcare, for example, lead to cost savings because seniors can live independently longer. Furthermore, developing sustainable IoT applications will lead to profits from new products and services.

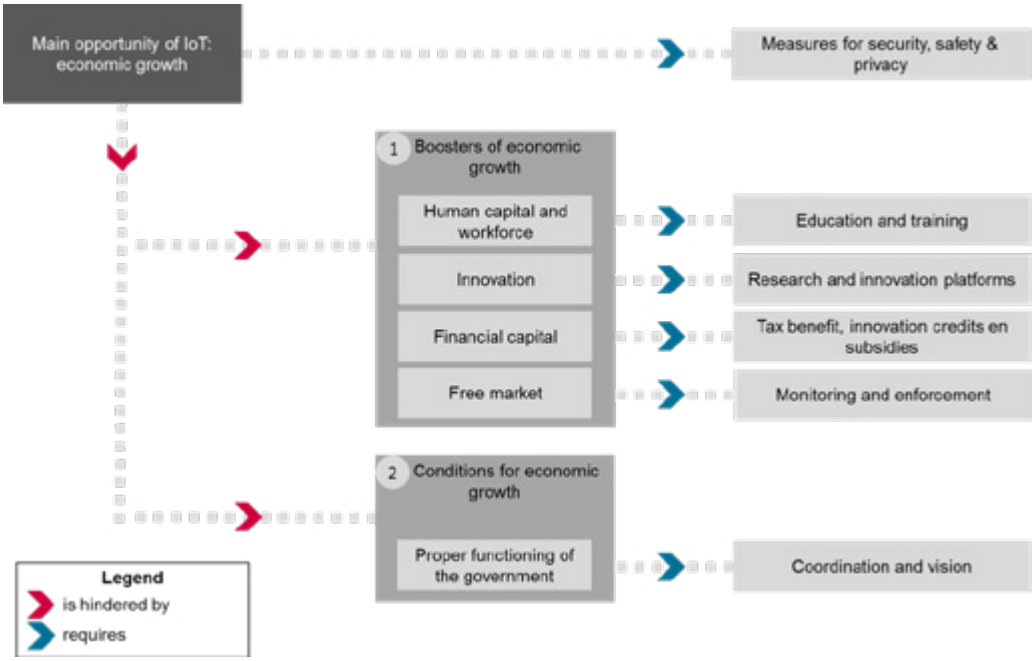
Security threats

The introduction of the IoT also brings some *threats*. Collecting large amounts of data and the increasing deployment of connected devices may have a negative effect on the following values: security, privacy, prosperity, well-being, equality and autonomy. The most prominent threats comprise the security, safety, and privacy of people. Security risks entail cyber crimes such as breaking into and taking over IoT devices, and stealing data. In addition, dysfunctional IoT devices can increase safety risks. The risk of privacy violations, for example through the use of (sensitive) data for purposes other than for which they were collected, increases with IoT devices. These threats are closely related to security risks. When the security of IoT applications is not in order, the chance that malicious people gain access to personal data increases. Of course, threats in other values also bring security risks. The more dependent we become on technology, the greater the consequences could be if something goes wrong.

Measures

There are several factors that affect the chances of economic growth and the threats regarding security and privacy. Although the initiative mainly lies with businesses, the government can certainly encourage companies to take action.
Figure S1 shows a summary of the factors and associated measures, which can positively affect economic growth. First, preventing security and privacy-related risks is an important requirement for promoting economic growth. The factors affecting growth can be divided into boosters of economic growth and factors that together determine the conditions for economic growth.

Figure S1 Factors and measures that foster economic growth through the IoT



Economic growth is driven by the availability of capital, this may include both human and financial capital. Therefore, a labour force with adequate knowledge and skills, as well as investment in the technology is required. Innovation involves developing new processes and products, which, for example, increase the productivity of businesses and bring prosperity. Innovation should be given ample room, even if it challenges existing business models. Market competition is also an important driver of economic growth. It is of particular importance to prevent unfair competition as much as possible.

The following measures help to positively influence boosters of economic growth.
- Government and business: modernise education to put more emphasis on IT skills and provide space for training and retraining the workforce.
- Government, companies and research institutions: invest in knowledge and research to develop new IoT technologies and innovations.
- Government: provide space for parties to innovate, for instance through a regulatory sandbox in which authorities work together with stakeholders to explore new applications.

- Government: ensure that tax benefits, credits and subsidies for innovation benefit the development of top sector-related IoT applications. In addition, pay attention to support for start-ups, for example by providing subsidies.
- Government: give regulators sufficient resources to monitor new developments such as the increasing influence of digital platforms.

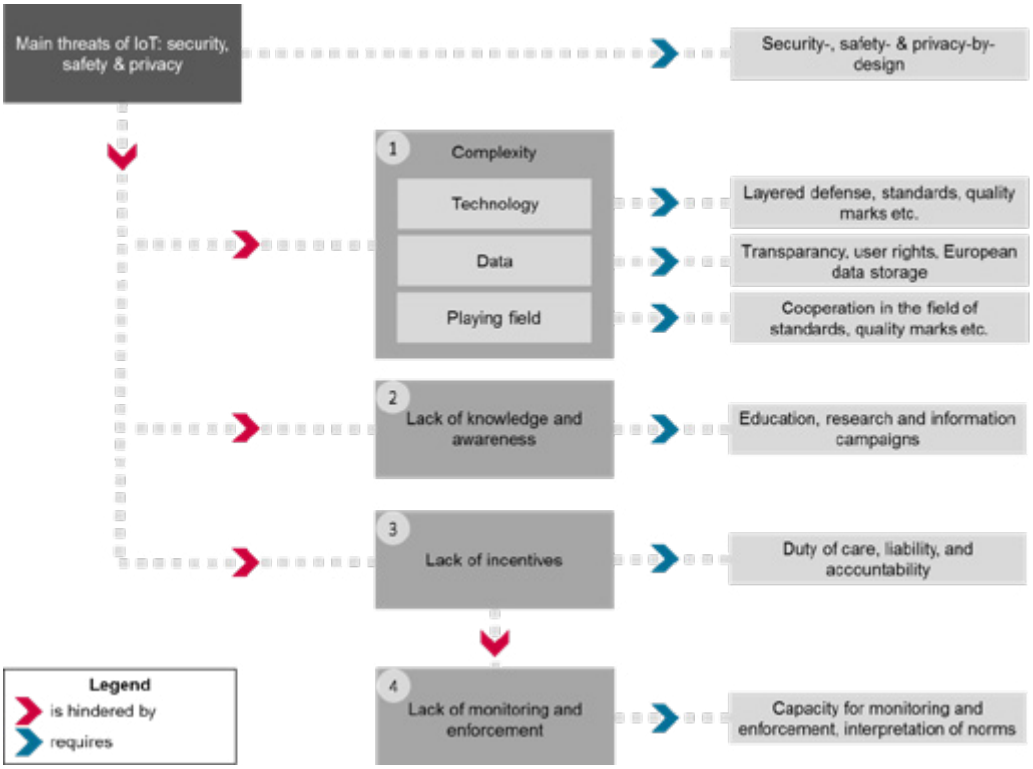
Government procedures affect the business environment, providing a precondition for economic growth. A certain predictability of the government, as legislator, will aid the business climate. In addition, cooperation between many different parties is essential for the development of the IoT. The government ought to play a role in it, but unfortunately knowledge in the field of IT often falls short.

The following measures will contribute to the positive influence of the conditions of economic growth.

- Government: formulate a vision for the IoT, taking into account the costs of new policies. Consequently, companies can use this to decide whether to invest in IoT technology or not.
- Government: siege responsibility for directing and coordinating the measures described in one body.

Figure S2 shows an overview of the factors and associated measures that can hinder the development and use of safe and privacy-sensitive IoT applications. These are: 1) complexity of the IoT, 2) lack of knowledge and awareness, 3) lack of incentives, and 4) lack of surveillance and enforcement. Per factor measures can be taken to reduce the restrictive impact.

Figuur S2Means to mitigate security, safety and privacy risks.



The complexity of the IoT includes the technology itself, the processed data, and the playing field. The heterogeneity of IoT technology makes it challenging to introduce general security measures. The important role of data in the IoT contributes to complexity, because of ambiguity about where data are stored, who has access to and makes use of the data, and the legal interpretation of fundamental rights. Due to the large amount of (mostly foreign) players on the IoT market, the playing field is rather complex and lacks overview of who is responsible for what. This problem is worsened because governments have different rules and standards and also have different interests.

The following measures will contribute to dealing with the complexity of the IoT.

- Businesses: use layered defense when taking security measures, this way risks can be tackled at different levels.
- Government and businesses: set standards and certifications defining security and privacy requirements for manufacturers of IoT products to abide by.
- Businesses: establish transparency about the use of data by clear and understandable privacy policies.
- Government: require manufacturers of IoT devices to provide an on/off switch for data processing and data sharing to third parties.
- Government and business: localise the storage and processing of data of IoT products in the Netherlands or Europe.

Taking measures to mitigate security and privacy threats are also hampered by a lack of awareness and knowledge about (the risks around) the IoT and IT in general. This applies to the government, citizens, as well as businesses.

A number of measures can counteract this lack of knowledge and awareness.

- Government and businesses: invest in education and (re)training to stimulate safe and responsible use of the internet, and improve digital literacy in the Netherlands.
- Government, companies and research institutions: invest in research in and monitoring of new threats to aid safety and privacy of new (IoT) technology.
- Government: invest more in attracting and developing expertise (of public officials) in the field of IT.

Implementing security measures is greatly hampered by a lack of incentives for users and businesses. Users are often not aware of security and privacy risks and, in most cases, are not affected by attacks. For companies, an economic incentive to secure products is missing. Security costs require additional effort and investment, from which in most cases no proportional benefits are gained. Although both parties lack incentives, users may reasonably assume that manufacturers launch decent products.

The following measures could create incentives for companies to manufacture more secure and privacy-friendly IoT applications.

- Government and businesses: businesses should take their duty of care into account more often. The government can sharpen the duty of care rules in areas in which they are unclear. Currently, it is not always clear how far the duty of care reaches regarding security. Also with respect to liability, the government can set out clear rules to eliminate ambiguities.
- Businesses: implement chain responsibility to ensure the security of the IoT, especially in the production or use of IoT products where many parties are involved.

- Insurance companies: integrate security standards and -certification in new (cyber) security insurances.
- Government: build on current policy initiatives involving ISPs to counter the lack of market incentives.
- Government: provide direction and set a good examle through the procurement of security packages. This could contribute to knowledge building and can move other parties to innovate and invest in the area of cyber security.

The impact of the incentives described above is limited by a lack of monitoring and enforcement. Without these, measures such as duty of care and liability are less effective. However, currently allocated resources for monitoring and enforcement leave much to be desired.

The following measures could contribute to a more effective monitoring and enforcement.

- Government: allocate sufficient capacity at involved supervision authorities.
- Government: provide specific standards about duty of care and liability, for example, regarding the durability of IoT devices and what end users can expect from the provider.

Conclusion

The above results show that the IoT provides a range of opportunities to increase welfare, sustainability, productivity and prosperity in our society. However, it appears that IoT applications are currently poorly protected and thus pose a threat to our security and privacy. The Mirai botnet, consisting of compromised IoT devices, shows that the risk is ever-present and this will only continue to grow. It is important that the security and privacy risks are addressed in order to reduce and prevent damage as much as possible. Nevertheless, to take advantage of the opportunities that the IoT offers, a safe environment also needs to be created for new developments and innovation.

As manufacturers of IoT applications and infrastructure, companies are responsible for the realization of new and innovative, but also secure and privacy-protective IoT applications. Currently this happens insufficiently due to the complexity of the IoT and a lack of knowledge, incentives, monitoring and enforcement. None of the above measures is in itself a solution to the threats of the IoT. In other words, there is no one-size-fits-all solution for this problem. Instead, several interrelated measures are required, which are only effective if they are implemented as a whole.This requires a supported government vision, where one body is designated to control and coordinate this policy. Because the IoT is related to other technological developments and cyber security in a broader context, the government vision should also cover these topics.

Discussion and follow-up research

This study is exploratory and broad in nature, in follow-up research a number of topics could therefore be explored. First of all, follow-up research could focus on identifying the main opportunities, threats and perspectives of specific IoT applications or domains. Secondly, research could be done on quantifying different measures. Thirdly, research could be done on the impact of different perspectives, such

as the feasibility and effectiveness of a governing body. Fourthly, one could look into the technical details and safety of IoT products. Fifhly, follow-up research might be conducted to identify necessary amendments of IoT-legislation. A final recommendation is to do extensive research into the geopolitical consequences of the IoT with regard to international (free) trade and economic interaction.

Literatuur

Ackerman, S. & Thielman, S. (2016). *US intelligence chief: we might use the internet of things to spy on you*. Geraadpleegd op 4 april 2017: www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, *17*(4), 2347-2376.

Algemene Rekenkamer (2016). *Staat van de rijksverantwoording 2015: Rijksbrede resultaten verantwoordingsonderzoek.* Den Haag: Algemene Rekenkamer.

Algemene Rekenkamer (2017). *Producten op de Europese markt: CE-markering ontrafeld.* Den Haag: Algemene Rekenkamer.

Amichai-Hamburger, Y. (2002). Internet and personality. *Computers in Human Behavior*, *18*(1), 1-10.

Aoyama, T., Koike, M., Koshijima, I., & Hashimoto, Y. (2013). A unified framework for safety and security. *Safety and security engineering V*, *134*, 67-77.

Arntz, M., Gregory, T., & Zierahn, U. (2016). *The risk of automation for jobs in OECD countries: A comparative analysis* . Parijs: OECD Publishing. OECD Social, Employment and Migration Working Papers, 189.

Ashford, W. (2016). *LizardStresser IoT botnet launches 400Gbps DDoS attack.* Geraadpleegd op 4 april 2017: www.computerweekly.com/news/450299445/LizardStresser-IoT-botnet-launches-400Gbps-DDoS-attack

Asghari, H., Eeten, M.J.van , & Bauer, J.M. (2015). Economics of fighting botnets: Lessons from a decade of mitigation. *IEEE Security & Privacy*, *13*(5), 16-23.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805.

Balta-Ozkan, N., Davidson, R., Bicket, M., & Whitmarsh, L. (2013). Social barriers to the adoption of smart homes. *Energy Policy*, *63*, 363-374.

Bauer, J.M., & Eeten, M.J. van (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, *33*(10), 706-719.

Bauer, H., Patel, M., & Veira, J. (2014). *The Internet of Things: Sizing up the opportunity*. Geraadpleegd op 4 april 2017: www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-sizing-up-the-opportunity

Bawden, D., & Robinson, L. (2009). The dark side of information: Overload, anxiety and other paradoxes and pathologies. *Journal of information science*, *35*(2), 180-191.

Beaudin, J.S., Intille, S.S., & Morris, M.E. (2006). To track or not to track: User reactions to concepts in longitudinal health monitoring. *Journal of Medical Internet Research*, *8*(4), 1-22.

Berg, B. van den (2009). *The situated self: Identity in a world of ambient intelligence*. Erasmus University Rotterdam. Geraadpleegd op 4 april 2017: http://hdl.handle.net/1765/15586

Berg, B. van den (2010). Ambient intelligence: Wat, wie en... waarom?. *Computerrecht*, *2010*(6), 267-272.

Berg, B. van den, & Keymolen, E. (2013). Techniekfilosofie: Het medium is de maat. *Wijsgerig Perspectief*, *53*(1), 8-17.

Berg, B. van den, Pötzsch, S., Leenes, R., Borcea-Pfitzmann, K., & Beato, F. (2011). Privacy in social software. In J. Camenish, S. Fischer-Hübner & K. Rannenberg (red.), *Privacy and identity management for Life* (pp. 33-61). Londen: Springer.

Bhabad, M.A., & Bagade, S.T. (2015). Internet of Things: Architecture, security issues and countermeasures. *International Journal of Computer Applications*, *125*(14), 1-4.
Bibri, S.E. (2015). *The shaping of ambient intelligence and the Internet of Things: historico-epistemic, Socio-cultural, politicoinstitutional and eco-environmental dimensions*. Penryn: Atlantis Press.
Bijlsma, M., Overvest, B., & Straathof, B. (2016). *Marktordening bij nieuwe ICT-toepassingen*. Den Haag: Centraal Planbureau.
Blok, S. (2016, 28 april). *Reactie op het conceptrapport de Staat van de Rijks-verantwoording 2015*. Geraadpleegd op 4 april 2017: www.rekenkamer.nl/dsresource?objectid=24279&type=org
Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, *54*, 1-31.
Bos, J., & Munnichs, G. (2016). *Digitalisering van dieren*. Den Haag: Rathenau Instituut.
Bradley, J., Barbier, J., & Handler, D. (2013). *Embracing the Internet of everything to capture your share of $14.4 trillion*. San Jose: Cisco.
Brous, P., & Janssen, M. (2015, October). A systematic review of impediments blocking Internet of Things adoption by governments. In M. Janssen et al. (red.), *Open and big data management and innovation* (pp. 81-94). Cham: Springer International Publishing.
Bruntland, G.H. et al. (1987). *Report of the World Commission on Environment and Development: Our common future*. Geraadpleegd op 4 april 2017: www.un-documents.net/wced-ocf.htm
Caron, X., Bosua, R., Maynard, S.B., & Ahmad, A. (2016). The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. *Computer law & security review*, *32*(1), 4-15.
Castermans, J., Feijth, H., Verheij, M., Beekhuizen, J., & Wong-A-Tjong, S. (2014). *Internet of Things: Slimme en internet-verbonden producten en diensten.* Utrecht: Kamer van Koophandel.
CBS (Centraal Bureau voor de Statistiek) (2013). *Het Nederlandse ondernemings-klimaat in cijfers 2013.* Den Haag: CBS.
CLTC (Center for Long-term Cybersecurity) (2016). *Cybersecurity futures 2020*. Berkely: University of Carlifornia.
Cook, D.J., Youngblood, G.M., Heierman III, E.O., Gopalratnam, K., Rao, S., Litvin, A., & Khawaja, F. (2003). MavHome: An agent-based smart home. *Proceedings of the First IEEE International Conference on Pervasive Computing and Communi-cations 2003*, 3, 521-524.
CPB & PBL (2015). *Toekomstverkenning welvaart en leefomgeving: Achtergrond-document binnenlandse personenmobiliteit*. Den Haag: CPB/PBL.
CSR (Cybersecurity Raad) (2016a). *Werkprogramma 2016: De toekomst is dichtbij dan je denkt*. Den Haag: CSR.
CSR (Cybersecurity Raad) (2016b). *The opportunities and risks of the Internet of Things: Perspectives for action*. Den Haag: CSR.
CSR (Cybersecurity Raad) (2016c). *De economische en maatschappelijke noodzaak van meer Cybersecurity: Nederland digitaal droge voeten*. Den Haag: CSR.
Custers B.H.M., Calders T., Schermer B. & Zarsky T.Z. (2013). *Discrimination and privacy in the information society: Data mining and profiling in large databases studies in applied philosophy*. Heidelberg: Springer.
Cvitić, I., Vujić, M., & Husnjak, S. (2016). Classification of security risks in the IoT environment. *Proceedings of the 26th DAAAM International Symposium*, 731-740.

Davies, R. (2015). The Internet of Things opportunities and challenges. Geraadpleegd op 4 april 2017: www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf
Dijksma, S. (2016). Rijksbrede programma Circulaire Economie [Kamerbrief]. Geraadpleegd op 4 april 2017: www.rijksoverheid.nl/documenten/kamerstukken/2016/09/14/rijksbrede-programma-circulaire-economie
Domingo, M.C. (2012). An overview of the Internet of Things for people with disabilities. *Journal of Network and Computer Applications*, *35*(2), 584-596.
Dommering, E.J., Ginkel, B.T. van, Goede, M. de, Koops, E.J., Plooij-van Gorsel, P.C., Verrijn Stuart, H.M., & Smallenbroek, J. (2014). *Het internet: Een wereldwijde vrije ruimte met begrensde staatsmacht*. Den Haag: Adviesraad Internationale Vraagstukken.
Easttom II, W.C. (2012). *Computer security fundamentals* (2nd ed.). Indianapolis: Pearson.
Ellen Macarthur Foundation (2016). Intelligent assets: Unlocking the circular economy potential. Geraadpleegd op 4 april 2017: www.ellenmacarthurfoundation.org/publications/intelligent-assets
Engelfriet, A. (2011). *Ben ik aansprakelijk voor de fouten in mijn software?* [Blog post] Geraadpleegd op 4 april 2017: https://blog.iusmentis.com/2011/09/19/ben-ik-aansprakelijk-voor-de-fouten-in-mijn-software
Ericsson (2016). *Ericsson Mobility Report: On the pulse of the networked society.* Stockholm: Ericsson.
Est, R. van, & Kool, L. (2015). *Werken aan de robotsamenleving: Visies en inzichten uit de wetenschap over de relatie technologie en werkgelegenheid.* Den Haag: Rathenau Instituut.
Evans, D. (2012). *The internet of everything: How more relevant and valuable connections will change the world*. San Jose: Cisco.
Farooq, M.U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review on Internet of Things (IoT). *International Journal of Computer Applications*, *113*(1), 1-7.
Farooqui, O. (2015). *Critique of the SPY Car Act of 2015*. Geraadpleegd op 4 april 2017: www.cs.tufts.edu/comp/116/archive/fall2015/ofarooqui-supporting.pdf
Fletcher, D. (2015). Internet of Things. In M. Blowers (red.), *Evolution of cyber technologies and operations to 2035* (pp. 19-32). Cham: Springer International Publishing.
Flight, S. (2016). Politie en beeldtechnologie: Gebruik, opbrengsten en uitdagingen. *Justitiële Verkenningen*, *42*(3), 68-93.
Floridi, L. (2015). *The onlife manifesto: Being human in a hyperconnected era*. Cham: Springer International Publishing.
Frenken, K. (2015). Reflecties op de deeleconomie. Geraadpleegd op 4 april 2017: https://dspace.library.uu.nl/handle/1874/320399
Frenken, K. (2016). *Deeleconomie onder één noemer*. S.l.:Universiteit Utrecht. Geraadpleegd op 4 april 2017: www.uu.nl/sites/default/files/20160211-uu_oratie-frenken.pdf
Friedman, B., Kahn Jr, P.H., & Borning, A. (2013). Value sensitive design and information systems. In K. E. Himma & H. T. Tavani (red.), *Early engagement and new technologies: Opening up the laboratory* (pp. 55-95). Hoboken: John Wiley & Sons, Inc.
FTC (2015). *Privacy & security in a connected world*. Washington: FTC.
Fuhrer, P., & Guinard, D. (2006). Building a smart hospital using RFID technologies: Use cases and implementation. Geraadpleegd op 4 april 2017: http://diuf.unifr.ch/drupal/sites/diuf.unifr.ch.drupal.softeng/files/file/publications/internal/rfidehealth.pdf

Gallagher, S. (2016). *Kentucky hospital hit by ransomware attack*. Geraadpleegd op 4 april 2017: https://arstechnica.com/security/2016/03/kentucky-hospital-hit-by-ransomware-attack
Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, *35*(2), 137-144.
Gartner. (2015). *What's new in Gartner's hype cycle for emerging technologies, 2015*. Geraadpleegd op 4 april 2017: www.gartner.com/smarterwithgartner/whats-new-in-gartners-hype-cycle-for-emerging-technologies-2015
Gitlin, J.M. (2014). *How can cars keep up with gadget innovation?* Geraadpleegd op 4 april 2017: https://arstechnica.com/cars/2014/06/industries-collide-how-automakers-are-adapting-to-consumer-tech-life-cycles
Goodman, M. (2015). *Future crimes: Everything is connected, everyone is vulnerable and what we can do about it*. Londen: Transworld.
GO-Science (The Government Office for Science) (2014). *The Internet of Things: Making the most of the Second Digital Revolution.* Londen: GO-Science.
Greenberg, A. (2016). *The FBI warns that car hacking is a real risk*. Geraadpleegd op 4 april 2017: www.wired.com/2016/03/fbi-warns-car-hacking-real-risk
Gregory, J. (2015). The Internet of Things: Revolutionizing the retail industry: Accenture. Geraadpleegd op 4 april 2017: www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_14/Accenture-The-Internet-Of-Things.pdf
Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645-1660.
Haas, A., Haas, M., & Weinert, M. (2015). The Internet of Things is already here, but who bears the risks? Geraadpleegd op 4 april 2017: www.wriec.net/wp-content/uploads/2015/07/6J3_Haas.pdf
Hand, D.J., Mannila, H., & Smyth, P. (2001). *Principles of data mining*. Cambridge: MIT press.
Healey, J., Pollard, N., & Woods, B. (2015). *The healthcare internet of things: Rewards and risks*. Washington: Atlantic Council.
Heijne, S. & Witteman, J. (2014). Al 154.000 administratieve banen weg door 'robots'. Geraadpleegd op 4 april 2017: www.volkskrant.nl/tech/al-154-000-administratieve-banen-weg-door-robots~a3761685
Hildebrandt, M. (2008). Defining profiling: A new type of knowledge? In M. Hildebrandt, & S. Gutwirth (red.), *Profiling the European citizen* (pp. 17-45). Dordrecht: Springer.
Hildebrandt, M. (2016). Data-gestuurde intelligentie in het strafrecht. In T.E. Tjong Tjin (red.), *Homo Digitalis* (pp. 139-240). Deventer: Wolters Kluwer.
Hoven, J. van den, Poel, I. van de, & Vermaas, P. E. (2014). *Handbook of ethics, values and technological design*. Dordrecht: Springer.
Hsu, C. & Lin, J.C. (2016). An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. *Computers in Human Behaviour, 62*, 516-527.
Jacobs, B. (2016). Aftercare for the Internet of Things. *CSR Magazine*, *2*, 61-62.
Jacobs, B. (z.j.). *Het internet der ondingen*. Geraadpleegd op 4 april 2017: http://pilab.nl/about%20pi%20lab/blog/het%20internet%20der%20ondingen.html
Jeschke, S., Brecher, C., Meisen, T., Özdemir, D., & Eschert, T. (2016). Industrial Internet of Things and cyber manufacturing systems. In S. Jeschke, C. Brecher, H. Song, & D.B. Rawat (red.), *Industrial Internet of Things* (pp. 3-19). Cham: Springer International Publishing.

Kamp, H.G.J., & Mansveld, W.J. (2013). *Groene Groei: Voor een sterke, duurzame economie* [Kamerbrief]. Geraadpleegd op 4 april 2017: www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2013/03/28/kamerbrief-groene-groei-voor-een-sterke-duurzame-economie/kamerbrief-groene-groei-voor-een-sterke-duurzame-economie.pdf

Kempenaar, C. (2010). Precisielandbouw: Slim combineren van nieuwe technologieen. *Syscope Magazine*, *26*, 22-27.

Keymolen, E. (2014). A Moral Bubble: The influence of online personalization on moral repositioning. In J. de Mul (red.), *Plessner's pPhilosophical anthropology: Perspectives and prospects* (pp. 387-406). Amsterdam: Amsterdam University Press.

Koebler, J. (2015). *Hackers killed a simulated human by turning off its pacemaker*. Geraadpleegd op 4 april 2017: https://motherboard.vice.com/en_us/article/hackers-killed-a-simulated-human-by-turning-off-its-pacemaker

Kong, A., Beresford, S.A., & Alfano, C.M. (2012). Self-monitoring and eating-related behaviors are associated with 12-month weight loss in postmenopausal overweight-to-obese women. *Journal of the Academy of Nutrition and Dietetics*, *112*(9), 1428–1435.

Kool, L., Timmer, J., Royakkers, L., & Est, R. van (2017). *Opwaarderen:- Borgen van publieke waarden in de digitale samenleving.* Den Haag: Rathenau Instituut.

Koops, B.J., Leenes, R., Hert, P.D., & Olislaegers, S. (2012). *Misdaad en opsporing in de wolken: Knelpunten en kansen van cloud computing voor de Nederlandse opsporing*. Tilburg: Tilburg Institute for Law, Technology, and Society.

Kranenburg, R. van, Anzelmo, E., Bassi, A., Caprio, D., Dodson, S., & Ratto, M. (2011). *The internet of things. A critique of ambient technology and the all-seeing network of RFID*. Amsterdam: Insitute of Network Cultures.

Lakerveld, J.A. van, Broek, S.D., Buiskool, B.J., Grijpstra, D.H., Gussen, I., Tonis, I.C.M., & Zonneveld, C.A.J.M. (2014). *Arbeidsmarkt voor cybersecurity professionals.* Leiden: PLATO.

Laney, D. (2001). *3-D data management: Controlling data volume, velocity and variety: Application Delivery Strategies by META Group Inc*. Geraadpleegd op 4 april 2017: http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

Lange, R. de (2016). Niet melden cybercrime is vaak verstandiger. Geraadpleegd op 4 april 2017: https://fd.nl/economie-politiek/1172215/niet-melden-cybercrime-is-vaak-verstandiger

Langheinrich, M. (2001). Privacy by design: Principles of privacy-aware ubiquitous systems. In G.D. Abowd, B. Brumitt & S. Shafer (red.), *Ubicomp 2001: Ubiquitous computing* (pp. 273-291). Berlijn: SpringerLink.

Langley, D. (2015). De boeddhistische leer achter het internet of things. *Het Financieele Dagblad*, 24 oktober 2015, p. 9. Geraadpleegd op 4 april 2017: https://fd.nl/morgen/1124267/het-internet-of-things-maakt-eigendom-onzinnig

Larose, D.T. (2014). Discovering knowledge in data: An introduction to data mining. Hoboken: John Wiley & Sons.

Lee, A., Girgensohn, A., & Schlueter, K. (1997). NYNEX portholes: Initial user reactions and redesign implications. *Proceedings of the international ACM SIGGROUP conference on Supporting group work: the integration challenge*, 385-394.

Leyden, J. (2016). *IoT baby monitor style hacks still a threat*. Geraadpleegd op 4 april 2017: www.theregister.co.uk/2016/07/19/baby_monitor_style_hacks

Li, S., Xu, L.D., & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243-259.

Libbenga, J. (2014). *Philips: 'Met Android zijn we toekomstvast'*. Geraadpleegd op 4 april 2017: www.emerce.nl/achtergrond/philips-met-android-toekomstvast
Lu, J. (2016). Will medical technology deskill doctors? *International Education Studies*, *9*(7), 130-134.
Lund, D., MacGillivray, C., Turner, V., & Morales, M. (2014). *Worldwide and regional internet of things (iot) 2014–2020 forecast: A virtuous circle of proven value and demand*. Framingham: International Data Corporation (IDC).
Madrigal, A.C. (2012). *Reading the privacy policies You encounter in a year would take 76 work days*. Geraadpleegd op 4 april 2017: www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851
Malik, O. (2016). *Pokémon go will make you crave augmented reality.* Geraadpleegd op 4 april 2017: www.newyorker.com/tech/elements/pokemon-go-will-make-you-crave-augmented-reality
Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P., & Marrs, A. (2013). *Disruptive technologies: Advances that will transform life, business, and the global economy*. San Francisco: McKinsey Global Institute.
Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). *The Internet of Things: Mapping the value beyond the hype*. San Francisco: McKinsey Global Institute.
Mashhadi, A., Kawsar, F., & Acer, U. G. (2014). Human data interaction in IoT: The ownership aspect. *2014 IEEE World Forum on Internet of Things (WF-IoT)*, 159-162.
Maurer, T., Skierka, I., Morgus, R., & Hohmann, M. (2015). Technological sovereignty: Missing the point? *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, 53-68.
McCarthy, K. (2016). *Osram's Lightify smart bulbs blow a security fuse: isn't anything code audited anymore?* Geraadpleegd op 4 april 2017: www.theregister.co.uk/2016/07/27/osram_smart_lightbulbs
Mimoso, M. (2016). *IoT botnets are the new normal of DDOS attacks.* Geraadpleegd op 4 april 2017: https://threatpost.com/iot-botnets-are-the-new-normal-of-ddos-attacks/121093
Minerva, R., Biru, A., & Rotondi, D. (2015). Towards a definition of the Internet of Things (IoT). Geraadpleegd op 4 april 2017: http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf
Ministerie van Economische Zaken (2016). *Licht op de digitale schaduw: Verantwoord innoveren en met big data: Rapport van de expertgroep Big data en privacy aan de minister van Economische Zaken.* Den Haag: Ministerie van Economische Zaken.
Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497-1516.
Mul, J. de (2015). The game of life: Narrative and ludic identity formation in computer games. In L. Way (red.), *Representations of Internarrative Identity* (pp. 159-187). Londen: Palgrave Macmillan UK.
Munnichs, G., Kouw, M., & Kool, L. (2017). *Een nooit gelopen race: Over cyberdreigingen en versterking van weerbaarheid.* Den Haag: Rathenau Instituut.
NCSC (Nationaal Cybersecurity Centrum) (2016). *Cybersecuritybeeld Nederland 2015*. Geraadpleegd op 4 april 2017: www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/cybersecuritybeeld-nederland/cybersecuritybeeld-nederland-5/1/CSBN5.pdf
Norris, P. (2001). *Digital divide: Civic engagement, information poverty, and the Internet worldwide*. Cambridge: Cambridge University Press.

Oriwoh, E., & Conrad, M. (2015). 'Things' in the Internet of Things: Towards a definition. *International Journal of Internet of Things*, *4*(1), 1-5.
Pauli, D. *414,949 D-Link cameras, IoT devices can be hijacked over the net.* Geraadpleegd op 4 april 2017: www.theregister.co.uk/2016/07/08/414949_dlink_cameras_iot_devices_can_be_hijacked_over_the_net
Peppet, S.R. (2014). Regulating the internet of things: First steps toward managing discrimination, privacy, security and consent. *Texas Law Review, 93*, 85-176.
Pb7 Research (2017). Meldplicht datalekken in de praktijk. Geraadpleegd op 4 april 2017: http://newsroom.kaspersky.eu/fileadmin/user_upload/nl/Downloads/meldplichtdatalekken.pdf
Pereira, Â.G., Benessia, A., & Curvelo, P. (2013). *Agency in the Internet of Things*. Luxemburg: Publications Office of the European Union.
Platform Onderwijs 2032 (2016). *Ons onderwijs2032: Eindadvies*. Den Haag: Platform Onderwijs 2032.
PWC (2014). 6th annual Digital IQ survey: The five behaviors that accelerate from digital investments. Geraadpleegd op 4 april 2017: www.pwc.nl/nl/assets/documents/pwc-6th-annual-digital-iq.pdf
Remerie, M., & Brake, G. te (2017). *Verkenning van nut, noodzaak en haalbaarheid van een nationaal cybertestbed*. Den Haag: The Hague Security Delta.
Roberti, M. (2015). *The History of RFID Technology*. Geraadpleegd op 4 april 2017: www.rfidjournal.com/articles/view?1338
Roca, D., Nemirovsky, D., Nemirovsky, M., Milito, R., & Valero, M. (2016). Emergent behaviors in the Internet of Things: The ultimate ultra-large-scale sSystem. *IEEE Micro, 36*(6), 36-44.
Roose, K. (2014). *The sharing economy isn't about trust, it's about desperation*. Geraadpleegd op 4 april 2017: http://nymag.com/daily/intelligencer/2014/04/sharing-economy-is-about-desperation.html
Rose, K., Eldridge, S., & Chapin, L. (2015). *The Internet of Things: an overview: Understanding the issues and challenges of a more connected world*. Genève: Internet Society.
Russell, S.J., & Norvig, P. (2010). *Artificial intelligence: A modern approach*. New Jersey: Prentice Hall.
Santucci, G. (2010). The internet of things: between the revolution of the internet and the metamorphosis of objects. Geraadpleegd op 4 april 2017: http://cordis.europa.eu/fp7/ict/enet/documents/publications/iot-between-the-internet-revolution.pdf
Schneier, B. (2014). *The Internet of Things is wildly insecure: And often unpatchable*. Geraadpleegd op 4 april 2017: www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem
Schneier, B. (2016a). *Regulation of the Internet of Things*. [Blog post] Geraadpleegd op 4 april 2017: www.schneier.com/blog/archives/2016/11/regulation_of_t.html
Schneier, B. (2016b). Security economics of the Internet of Things. [Blog post] Geraadpleegd op 4 april 2017: www.schneier.com/blog/archives/2016/10/security_econom_1.html
Scuro, G. (z.j.). *Automotive industry: Innovation driven by electronics*. Geraadpleegd op 4 april 2017: http://embedded-computing.com/articles/automotive-industry-innovation-driven-electronics
Silver, E., Wallenstein, S., & Levy, A. (2012). Inward and outward: The role of patient self-monitoring and patient communities in IBD. *Inflammatory Bowel Diseases*, *18*, 45-46.

Smit, W., Peters, S., Kemps, D., Vos, R., & Sterk, W. (2016). Industrial Internet of Things: Noodzaak voor industrie, kans voor IT-sector. Geraadpleegd op 4 april 2017: https://insights.abnamro.nl/2016/02/industrial-internet-of-things
SER (Sociaal-Economische Raad) (2016). Verkenning en werkagenda digitalisering: Mens en technologie: samen aan het werk. Den Haag: SER.
Soest, T. van (2015). Proef met elektrische auto als batterij voor zonne-energie. *de Volkskrant*. Geraadpleegd op 4 april 2017: www.volkskrant.nl/economie/proef-met-elektrische-auto-als-batterij-voor-zonne-energie~a4065297
Stratix (2015). *Internet of Things in the Netherlands: Applications, trends and potential impact on radio spectrum*. Hilversum: Stratix.
Swan, M. (2013). The quantified self: Fundamental disruption in big data science and biological discovery. *Big Data*, *1*(2), 85-99.
Talbot, E.B., Frincke, D., & Bishop, M. (2010). Demythifying Cybersecurity. *IEEE Security & Privacy, 8*(3), 56-59.
Thierer, A. (2015). The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation. *Richmond Journal of Law & Technology*, *21*(2.
Thomas, A. (2007). *Youth online: Identity and literacy in the digital age*. New York: Peter Lang Publishing.
Thomson, I. (2016). *If you use 'smart' Bluetooth locks, you're asking to be burgled*. Geraadpleegd op 4 april 2017: www.theregister.co.uk/2016/08/08/using_a_smart_bluetooth_lock_to_protect_your_valuables_youre_an_idiot
Tjong Tjin Tai, T.F.E. (2006). *Zorgplichten en zorgethiek*. Deventer: Wolters Kluwer.
Tjong Tjin Tai, T.F.E., Koops, E.J., Heij, D.O., Silva, K.E., & Skorvánek, I. (2015). *Duties of care and diligence against cybercrime*. Tilburg: Tilburg University.
Velde, R. te, Veldkamp, J., & Janswhitmaasen, M. (2014). *De softwaresector in Nederland: Survey 2014.* Utrecht: Dialogic.
Verbeek, P.P. (2011). *De grens van de mens: Over techniek, ethiek en de menselijke natuur.* Rotterdam: Lemniscaat.
Vermeulen, P. (2016). *Internet of Things Survey: Nederland 2016*. Pb7 Research. Geraadpleegd op 4 april 2017: www.sogeti.nl/download-onderzoekspaper-van-internet-things-survey-2016
Voorst, S. van (2016). *Datalekken, botnets en encryptie: Oude thema's werpen nieuwe vragen op*. Geraadpleegd op 4 april 2017: https://tweakers.net/reviews/5107/4/datalekken-botnets-en-encryptie-internet-of-insecure-things.html
Wan, J., Chen, M., & Leung, V.C.M. (2015). M2M Communications in the cyber-physical world: case studies and research challenges. In V. Mišic & J. Mišic (red.), *Machine-to-machine communications: Architectures, technology, standards, and applications* (pp. 1-30). Boca Raton: CRC Press.
Wang, Y.F., Lin, W.M., Zhang, T., & Ma, Y.Y. (2012). Research on application and security protection of internet of things in smart grid*. IET International Conference on Information Science and Control Engineering 2012 (ICISCE 2012)*, 1-5.
Weinberg, B.D., Milne, G.R., Andonova, Y. G., & Hajjat, F. M. (2015). Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons, 58*(6), 615-624.
Welle, M. ter, Peters, S., & Sterk, W. (2015). *Internet of Things: Kansen in software en maatschappelijke groeimarkten*. Geraadpleegd op 4 april 2017: https://insights.abnamro.nl/2015/09/internet-of-things-kansen-in-software-en-maatschappelijke-groeimarkten
Went, R., & Kremer, M. (2015). Hoe we robotisering de baas kunnen blijven: Inzetten op complementariteit. In Wetenschappelijke Raad voor het Regeringsbeleid (WRR), *De Robot de baas: De toekomst van werk in het tweede machinetijdperk* (pp. 23-46). Amsterdam: Amsterdam University Press.

WRR (Wetenschappelijke Raad voor het Regeringsbeleid) (2013). *Toezien op publieke belangen: Naar een verruimd perspectief op rijkstoezicht*. Geraadpleegd op 4 april 2017: www.wrr.nl/onderwerpen/toekomst-van-toezicht/documenten/rapporten/2013/09/09/toezien-op-publieke-belangen-naar-een-verruimd-perspectief-op-rijkstoezicht

WRR (Wetenschappelijke Raad voor het Regeringsbeleid) (2015). *De publieke kern van het internet: Naar een buitenlands internetbeleid*. Geraadpleegd op 4 april 2017: www.wrr.nl/publicaties/rapporten/2015/03/31/de-publieke-kern-van-het-internet

WRR (Wetenschappelijke Raad voor het Regeringsbeleid) (2016). *Big Data in een vrije en veilige samenleving*. Geraadpleegd op 4 april 2017: www.wrr.nl/publicaties/rapporten/2016/04/28/big-data-in-een-vrije-en-veilige-samenleving

Whitman, M.E., & Mattord, H.J. (2014). *Principles of information security*. Boston: Cengage Learning.

Whitmore, A., Agarwal, A., & Xu, L.D. (2015). The Internet of Things: A survey of topics and trends. *Information Systems Frontiers, 17*(2), 261-274.

Williams, C. (2016). *Thermostat ransomware*. Geraadpleegd op 4 april 2017: www.theregister.co.uk/2016/08/08/smart_thermostat_ransomware

Witten, I.H., & Frank, E. (2005). *Data Mining: Practical machine learning tools and techniques* (2nd ed.). San Francisco: Morgan Kaufmann Publishers.

Wolff, J. (2016). Perverse effects in defense of computer systems: When more is less. *Journal of Management Information Systems, 33*(2), 597-620.

Wolters, P.T.J., & Verbruggen, P.W.J. (2016). De verplichting tot het bijwerken van onveilige software. *Weekblad voor Privaatrecht, Notariaat en Registratie*, (7123), 832-839.

WEF (World Economic Forum) (2015) *Deep shift: Technology tipping points and societal impact*. Genève: WEF.

WP29 (Working Party 29) (2014). *Opinion 8/2014 on the on Recent Developments on the Internet of Things*. Geraadpleegd op 4 april 2017: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

Wurman, R.S. (1989). *Information Anxiety*. New York: DoubleDay

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2013). A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE communications surveys & tutorials, 15*(1), 5-20.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal, 1*(1), 22-32.

Zarsky, T.Z. (2014). Understanding discrimination in the scored society. *Washington Law Review, 89*, 1375-1412.

Zarsky, T.Z. (2016). The trouble with algorithmic decisions. An analytic road map to examine efficiency and fairness in automated and opaque decision making. *Science, Technology & Human Values, 41*(1), 118-132.

Zeemeijer, I. (2016). Spin-offs zijn aangewezen op diepe zakken universitaire holding. *Het Financieele Dagblad*, 26 februari 2016, p. 7. Geraadpleegd op 4 april 2017: https://fd.nl/economie-politiek/1141026/spin-offs-zijn-aangewezen-op-diepe-zakken-universitaire-holding

Ziegler, C., & Patel, N. (2016). *Meet the new Ford, a Silicon Valley software company*. Geraadpleegd op 4 april 2017: www.theverge.com/2016/4/7/11333288/ford-ceo-mark-fields-interview-electric-self-driving-car-software

Zwenne, G.J., & Mommers, L. (2010). Eigenzinnig en afwijkend Nederlands voorstel verstoord internationale concurrentieverhoudingen, *Het Financieele Dagblad,* 11 juni 2010, p. 7. Geraadpleegd op 4 april 2017: https://openaccess.leidenuniv.nl/bitstream/handle/1887/15687/pdf20100611_7064.pdf?sequence=1%3E

Zwenne, G.J. (2015). De onbestaanbare olifant: gedachten over Big Data en de Privacywet. *Tijdschrift voor Internetrecht, 4*, 142-147.

Bijlage 1 Samenstelling begeleidingscommissie

Voorzitter

Dr. P.W.M. Rutten	Creating010, Hogeschool Rotterdam

Leden

Dr. B. van den Berg	Universiteit van Leiden
Prof. dr. B. van Lier	Centric
Drs. M.H.G van Leeuwen	Ministerie van Veiligheid en Justitie
Drs. S. van der Weide	Ministerie van Economische Zaken
Drs. E. van den Heuvel	Cyber Security Raad (aanvrager)

Bijlage 2 Lijst geïnterviewde personen

Geïnterviewde personen

Ben van Lier	Centric
Joeri Kamp	Eneco
Willemieke Hornis	Ministerie van Infrastructuur en Milieu
Piet Bel	Philips
Mieke van Heeswijk	SIDN (fonds)
Wienke Giezeman	The Things Network

Deelnemers rondetafelgesprek Smart Cities

Marijn Fraanje	Gemeente Den Haag
Frank Vieveen	Gemeente Rotterdam
Peter van Waart	Hogeschool Rotterdam
Remco Muijs	Philips Lighting Research

Deelnemers rondetafelgesprek Smart Industries

Andrei Robachevsky	Internet Society
Maarten Botterman	NLNET Foundation en GNKS Consult
Berry van Halderen	Stichting NLnet Labs
Ruben van den Brink	Surfnet
Rob van Kranenburg	Waag Society en European Research Cluster on the Internet of Thing