Centraal Planbureau

# Kaders voor code: beleid voor veilige digitale middelen

Verplichte testfases of veiligheidsstandaarden nodig om grote maatschappelijke schade te voorkomen:

- Digitale en niet-digitale producten hebben dezelfde regels
- Complexiteit en schaal is groter bij digitale producten
- Daarom is soms aanvullend beleid nodig
- De kosten van aanvullend beleid worden doorberekend aan de gebruiker

Drie redenen waarom de overheid soms moet ingrijpen:

- Externe effecten: anderen worden getroffen door digitaal falen
- Informatieproblemen: consument kan veiligheid niet goed beoordelen
- Marktmacht: aanbieder heeft weinig prikkels voor meer betrouwbaarheid

CPB Policy Brief

Bastiaan Overvest

april 2020

# Beleid voor digitale middelen

Producten en diensten digitaliseren. Dat heeft voordelen, maar digitale middelen kunnen ook onbetrouwbaar zijn.

Een digitaal product of dienst kan ondeugdelijk zijn, of niet goed beveiligd tegen aanvallen van buitenaf.
Dit kan processen verstoren, maar ook leiden tot schade aan goederen of gezondheid.

## Er zijn drie redenen waarom de overheid soms moet ingrijpen

Aanbieders en gebruikers kunnen niet altijd zelf zorgen voor adequate betrouwbaarheid

### Externe effecten

- Via identiteitsfraude slachtoffers in sociaal netwerk
- DDoS-aanvallen
- Ongevallen met zelfrijdende auto's

### Informatieproblemen

- Consument ziet betrouwbaarheid niet
- Levert de fabrikant ná verkoop goede updates?

### Marktmacht

- Fabrikanten met marktmacht stoppen te vroeg met productondersteuning
- Prijsdiscriminatie via lagere betrouwbaarheid

### Mogelijke maatregelen

**Aansprakelijkheid, veiligheidseisen, vooraf testen en zo nodig verbieden**

**Voorlichting, markt aanzetten tot transparantie en certificering**

**Toezicht bij fusies, markt prikkelen**

### Nadelen en risico's

- Financiële compensatie niet voldoende bij fysieke schade.
- Risico's soms moeilijk vooraf in te schatten

Overheid doorgaans niet in een betere positie om informatie-problemen op te lossen dan marktpartijen

Verplichte ondersteunings-periode kan innovatie ontmoedigen

# Samenvatting

**Producten en diensten digitaliseren.** Een product of dienst ('middel') is digitaal wanneer deze software bevat. Niet alleen traditionele ICT-producten zoals computers en communicatienetwerken gebruiken software, ook traditionele producten zoals auto's, vliegtuigen of thermostaten digitaliseren en relatief nieuwe producten en diensten zoals apps of clouddiensten zijn volledig digitaal. Voor consumenten levert digitalisering van producten een betere prijs-kwaliteitsverhouding op, of helemaal nieuwe producten: denk aan boeken (e-readers), muziek (streaming) en apparaten (van auto's tot wasmachines).

**Behalve voordelen brengt deze ontwikkeling ook risico's met zich mee.** Software bevat vaak onbekende fouten of softwarekwetsbaarheden die misbruikt kunnen worden door kwaadwillenden. Hierdoor kan een digitaal product onveilig zijn in gebruik of is het product, of de informatie die het product verwerkt, niet goed beveiligd tegen aanvallen van buitenaf. Op de markt voor digitale middelen kunnen verschillende problemen optreden ('marktfalen') zoals externe effecten, informatieasymmetrie of marktmacht. Een digitaal voorbeeld van een extern effect is een massale aanval op websites ('DDoS-aanval') via slecht beveiligde digitale middelen. Dergelijke problemen zijn bij digitale middelen groter, doordat ze grootschalig gebruikt worden, complex zijn en markten soms geneigd zijn tot monopolievorming. Volgens sommige experts levert de markt nu producten die onvoldoende betrouwbaar zijn en zijn strengere regels nodig voor digitale middelen.

**Deze policy brief onderzoekt de vraag of, vanuit een economisch perspectief, nieuw of aanvullend beleid nodig is.** Een product is betrouwbaarder naarmate de verwachte schade voor gebruikers of anderen door gebruik van het product lager is. Kunnen aanbieders en gebruikers zelf zorgen voor adequate betrouwbaarheid, of moet de overheid extra maatregelen nemen? De interventieladder in hoofdstuk 3 van deze policy brief geef houvast bij het beantwoorden van deze vragen.

**De basis voor beleid voor betrouwbare digitale middelen bestaat al.** De regels voor bijvoorbeeld productaansprakelijkheid en mededinging zijn technologieneutraal en geven daarom ook belangrijke randvoorwaarden aan de markt voor digitale middelen. Toch kan aanvullend beleid nodig zijn. Bijvoorbeeld wanneer geleden schade niet via het aansprakelijkheidsrecht vergoed kan worden en de maatschappelijke kosten groot zijn. In die situaties kan gedacht worden aan veiligheidsstandaarden of een verplichte testfase. In een uiterste situatie is een (voorlopig) verbod op gebruik optimaal, bijvoorbeeld bij gebruik van volledig autonome voertuigen in de bebouwde kom. De overheid kan nog meer doen om betrouwbaarheid van digitale middelen te vergroten. Een beleidsoptie is het verplichten van aanbieders om kopers te informeren over belangrijke aspecten, zoals de periode waarvoor de aanbieder het product ondersteunt. Of zelfs verplichten dat bedrijven voor een vastgesteld aantal jaren veiligheidsupdates leveren. Verder kunnen overheden de ontwikkeling van betrouwbare open source software stimuleren, zoals via *challenges* of inkoopbeleid.

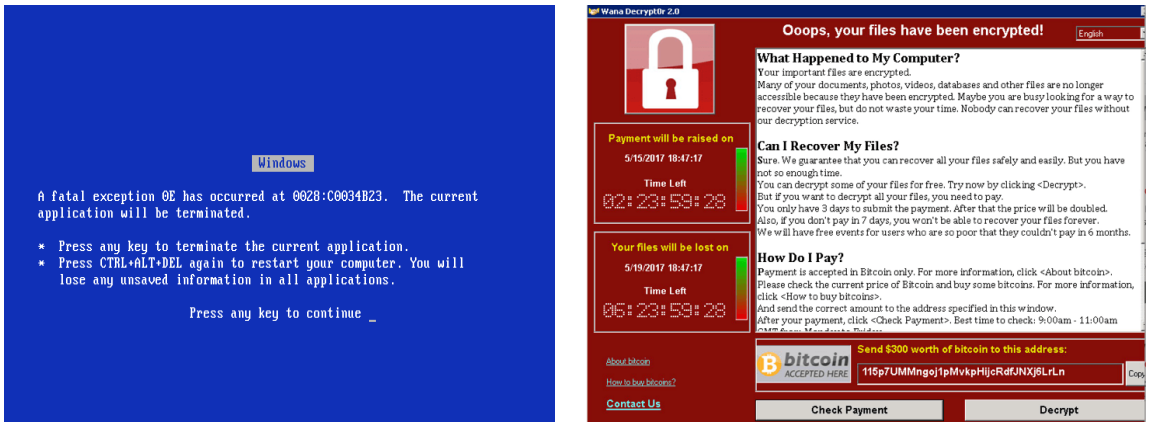
**De betrouwbaarheidsbaten van extra maatregelen moeten afgewogen worden tegen de maatschappelijke kosten.** Ook beleid voor digitale middelen moet doelmatig zijn. Aanvullende maatregelen, zoals extra certificaten of voorwaarden, leiden tot hogere kosten voor handhaving en naleving. Deze kosten worden uiteindelijk doorberekend aan de gebruiker. Ook kunnen ondoelmatige regels de introductie van nieuwe producten tegenhouden. Deze nadelen moeten opwegen tegen de voordelen van meer betrouwbaarheid.

# 1 Inleiding

**Onze samenleving digitaliseert.** Sociale levens spelen zich voor een groot deel online af en bedrijven zijn sterk afhankelijk van ICT. Zo heeft 98 procent van de Nederlanders thuis toegang tot internet en gebruikt dat voor bijvoorbeeld zoeken naar informatie (84 procent), internetbankieren (83 procent) of online winkelen (78 procent) (CBS, 2019). Het aantal ICT'ers in Nederland neemt sinds 2011 onafgebroken toe en 19 procent van de bedrijfsinvesteringen is bestemd voor ICT. Producten, van thermostaten tot televisies, worden ook steeds meer digitaal: ze maken meer gebruik van software, of zijn verbonden met internet. Naar schatting zijn wereldwijd in 2022 29 miljard apparaten gekoppeld aan het internet.[1]

**De betrouwbaarheid van digitale middelen is daarom steeds belangrijker.** Een digitaal product of dienst zien we als 'betrouwbaarder' naarmate de verwachte schade van storingen, aanvallen of andere incidenten lager is. ICT-storingen zijn allang niet meer alleen een bron van ergernis, maar kunnen belangrijke processen verstoren en tot schade leiden (zie figuur 1). Zo waren in 2018 sites van Nederlandse banken en de Belastingdienst tijdelijk slecht bereikbaar door DDoS-aanvallen, ontwrichtte het virus NonPetya de APM-terminals op de Rotterdamse haven en besmette het gijzelvirus WannaCry in 2017 meer dan 200.000 computers – waaronder honderden Engelse *National Health Service* zorginstellingen.[2] Gebrek aan betrouwbaarheid kan dus zelfs mensenlevens riskeren.[3]

**Figuur 1.1 Van de 'Blue screen of death' naar het rode WannaCry-scherm**




Noot: De 'Blue screen of death' verscheen als foutmelding bij het vastlopen van oude Windows-versies. WannaCry is een recent voorbeeld van een gijzelvirus dat gegevens soms voorgoed ontoegankelijk maakte en tot economische en maatschappelijke schade leidde.

**Desondanks zijn er weinig regels voor digitale middelen.** Voor veel niet-digitale producten, zoals voedsel, speelgoed of gastoestellen, zijn veiligheidseisen vastgelegd in Europese richtlijnen en verordeningen. Voor digitale middelen ontbreken dit soort product-specifieke kaders. Een uitzondering hierop vormen digitale middelen die van belang zijn voor de staatsveiligheid, daarvoor bestaan strengere veiligheidseisen.[4] De afwezigheid van product-specifieke regels voor de betrouwbaarheid van digitale middelen zien sommige experts als een lacune. Bruce Schneier, een computerbeveiligingsexpert, stelt bijvoorbeeld: "*Increasing the cybersecurity of these devices is paramount, and it's heartening to see both individual states and the European Union step in where*

[1] Bron: Ericsson. (link).
[2] https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.
[3] Anderzijds kan digitalisering ook veiligheid vergroten – algoritmes laten zich niet afleiden door ruiënde kinderen op de achterbank.
[4] De AIVD beoordeelt bijvoorbeeld staatsgevoelige software en hardware voor gebruik door overheidsorganisaties. Zie hier voor een overzicht van geëvalueerde producten.

*the US federal government is abdicating responsibility. But we need more, and soon."*[5] Verder roepen de computerwetenschappers Leverett, Clayton en Anderson (2017), in een rapport geschreven voor de Europese Commissie, de EU op om betrouwbaarheid van digitale producten strenger te reguleren: "*The EU is already the world's main privacy regulator, as Washington doesn't care and nobody else is big enough to matter; it should aim to become the main safety regulator too*".

**Verschillende organisaties pleiten daarom voor extra regels en maatregelen.** De Nederlandse Cyber Security Raad (CSR) (2017) adviseert bijvoorbeeld beveiligingsstandaarden voor IoT-apparaten.[6] Hierbij denkt de CSR aan minimumstandaarden voor de duur dat producten worden onderhouden, de manier waarop veiligheidsupdates beschikbaar komen en de eis dat apparaten van het internet afgeschakeld kunnen worden met behoud van de reguliere functionaliteit. De Europese Commissie (EC) heeft een voorstel gedaan voor een Europees certificeringssysteem en het ministerie van EZK (2018) stelt, in lijn met het CSR-advies, onder meer een verplichting van veiligheidsupdates voor. Sinds 2018 zijn in Californië *default* wachtwoorden (zoals 'admin') verboden voor IoT-apparaten.[7]

**Zijn extra regels om de betrouwbaarheid van digitale middelen te vergroten wenselijk?** Deze *Brief* onderzoekt deze vraag vanuit een economisch perspectief, waarbij de betrouwbaarheid van digitale middelen – in termen van de verwachte schade van incidenten – centraal staat. Een discussie over maatschappelijke wenselijkheid van het gebruik van kunstmatige intelligentie of algoritmen, in bijvoorbeeld de rechtsspraak of opsporing, valt buiten de scope.[8] Deze *Brief* gaat daarmee over marktfalen dat speelt op de markt voor digitale middelen, de economische legitimatie van overheidsingrijpen en voor- en nadelen van verschillende beleidsopties.

**In deze *Brief* zien we digitale middelen als producten en diensten die computercode bevatten.** Software is zelf dus ook een digitaal middel, net als hardware waarop software is geïnstalleerd. Door digitalisering zijn steeds meer producten digitaal of deels digitaal: denk aan boeken (e-books), muziek (streaming) en apparaten met firmware (van auto's tot wasmachines).

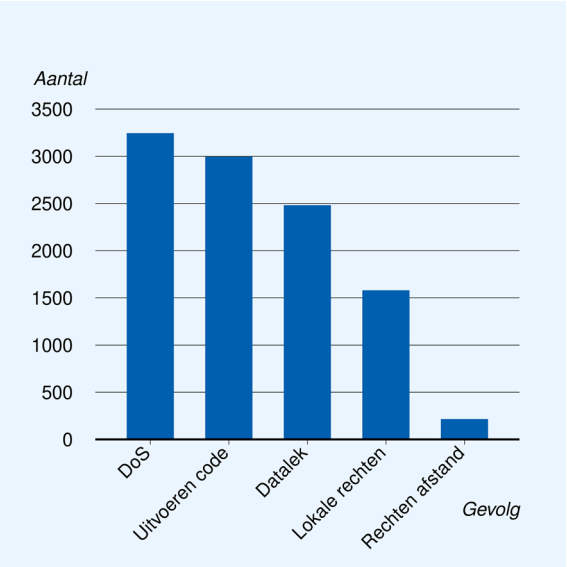
**De gevolgen van ICT-incidenten voor gebruikers en eventuele derden staan centraal, niet de ICT zelf.** In de computerwetenschappen wordt cyberveiligheid gedefinieerd vanuit het systeem, of het product. Software wordt als 'veilig' gezien als het Beschikbaar, Integer en Vertrouwelijk (BIV) is.[9] De definitie van cyberveiligheid is uitgebreider, maar stelt ook het ICT-systeem of de computer centraal: "Alle beveiligingsmaatregelen die men neemt om schade te voorkomen door een storing, uitval of misbruik van een informatiesysteem of computer. Ook worden maatregelen genomen om schade te beperken en/of herstellen als die toch is ontstaan".[10] Het economische perspectief in deze Policy Brief is risicogebaseerd: digitale middelen noemen we betrouwbaarder naarmate de verwachte schade voor gebruikers of anderen van ICT-incidenten lager is.

[5] Bron: blog van Bruce Schneier (link).
[6] Een IoT-apparaat is een digitaal middel dat data kan versturen en ontvangen via een netwerk. Voorbeelden van IoT-apparaten zijn smart speakers, beveiligingscamera's, of industriële controlesystemen.
[7] Bron: *The Economist*. (link).
[8] Fry (2018) is een recente bespreking van de mogelijke invloed van toepassingen van algoritmen op verschillende publieke belangen.
[9] De Engelse afkorting is CIA: Confidentiality, Integrity en Availability.
[10] Bron: Cybersecurity Woordenboek (link).

# 2 (Geen) markt voor betrouwbare digitale middelen

**In de praktijk zijn digitale middelen nooit volledig betrouwbaar.** Software bevat bijna altijd kwetsbaarheden, waardoor de kans bestaat op uitval, misbruik of een andere type verstoring. Alleen al voor software die gebruikt wordt in Nederlandse 'vitale' processen publiceert het Nederlands Cyber Security Centrum (NCSC) jaarlijks over honderden kwetsbaarheden. Deze kwetsbaarheden kunnen misbruikt worden in een aanval, of kunnen leiden tot een datalek (zie figuur 2.1). Bij sommige producten kunnen softwarekwetsbaarheden of ontwerpfouten leiden tot veiligheidsrisico's, zoals bij voertuigen of vitale waterwerken.[11]

**Figuur 2.1 Gevolgen van bekende softwarekwetsbaarheden**

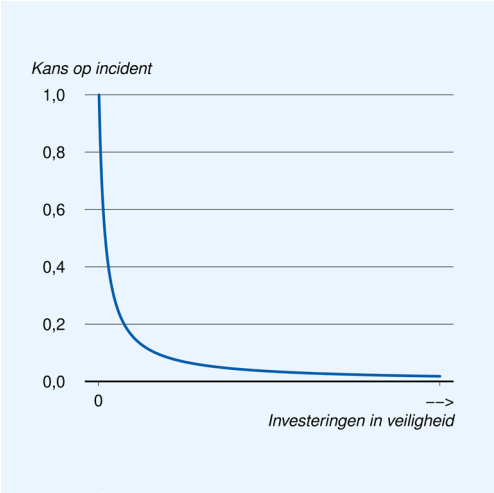



NB. Bovenstaande figuur geeft voor de NCSC-adviezen uit de periode 2012 t/m augustus 2018 het gevolg van kwetsbaarheden weer die zijn beschreven in die adviezen. Gevolgen kunnen bijvoorbeeld zijn dat een kwaadwillende code kan uitvoeren ('uitvoeren code') op een computer of dat een kwaadwillende met fysieke toegang tot het apparaat beheerdersrechten kan verkrijgen ('lokale rechte'). Bron: Ruesink en Windig (2019).

**Honderd procent betrouwbaarheid is voor digitale middelen doorgaans niet haalbaar**. Om de kans op een incident te verkleinen, kan een aanbieder extra kwetsbaarheden opsporen en proberen deze te verhelpen. Dit is een arbeidsintensief en daarom kostbaar proces. Hierbij speelt ook dat software vaak complex is, met soms miljoenen regels code. Ook een gebruiker van een digitaal product of dienst kan de kans op schade verkleinen door voorzorgsmaatregelen te nemen, zoals het regelmatig maken van back-ups van data, het controleren van hyperlinks, of het tijdig updaten van software. Deze voorzorgsmaatregelen brengen kosten met zich mee, vooral in de vorm van tijd en moeite. Het gevolg van dit alles is dat de kans op ICT-incidenten afneemt naarmate aanbieders en gebruikers meer investeren in (of meer moeite doen voor) veiligheid, maar dat de kans op een incident waarschijnlijk niet naar nul gaat. Figuur 2.2 laat dit zien.

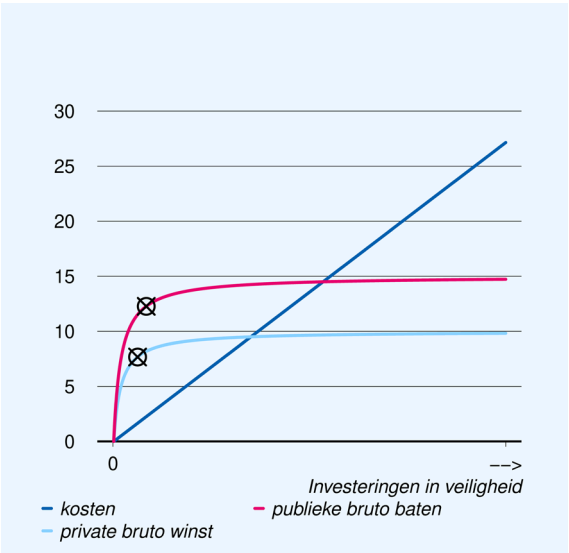
[11] Zie dit bericht van de Algemene Rekenkamer.

**Figuur 2.2 Kans op schade daalt als investeringen in veiligheid stijgen**




**Een aanbieder of gebruiker zal de baten van extra betrouwbaarheid afwegen tegen de kosten.** Voor een aanbieder kunnen de baten bestaan uit extra winst door eerder op de markt te zijn dan een concurrent, een prijsopslag vanwege een betere reputatie, of een intrinsieke motivatie om een betrouwbaar product aan te bieden. De baten voor een gebruiker kunnen zijn het ongestoord blijven gebruiken van ICT, het niet hoeven betalen van losgeld (zoals bij gijzelsoftware of 'ransomware' geëist wordt), het voorkomen van het verlies van waardevolle gegevens, of het voorkomen van fysieke schade. In principe, als aanbieders rationeel zijn en goed geïnformeerd over de kosten en effecten van investeringen, zal de betrouwbaarheid van een product zodanig zijn dat het verschil tussen de baten en de kosten maximaal zijn. In dat geval is de betrouwbaarheid van een digitaal product optimaal, vanuit het perspectief van de aanbieder. Vanuit het maatschappelijke perspectief is dit niet noodzakelijk optimaal. Figuur 2.3 illustreert dit. De lichtblauwe lijn laat zien hoe de brutobaten afhangen van investeringen in veiligheid. Aanvankelijk stijgen de brutobaten snel naarmate de investeringen toenemen, maar geleidelijk aan zwakt deze toename af. Op het punt waar het verschil tussen de private baten en de kosten maximaal is (aangegeven met het icoontje), is het investeringsniveau privaat optimaal.

**Figuur 2.3 Maatschappelijk optimaal investeringsniveau ligt hoger dan privaat optimaal niveau**



**Vanuit maatschappelijk perspectief kan het investeringsniveau op een vrije markt te laag zijn.** Aanbieders en gebruikers hebben weliswaar een prikkel om te investeren in betrouwbaarheid, want een aanbieder kan een hogere prijs vragen voor een betrouwbaar product en een gebruiker heeft meer plezier van een product als de kans op een schadelijk incident kleiner is. Het 'probleem' is echter dat de baten van een betrouwbaarder product ook terecht kunnen komen bij anderen, die niet betrokken zijn bij de transactie. De baten van investeringen in betrouwbaarheid voor deze derden worden op een ongereguleerde markt niet of maar ten dele meegewogen door de aanbieder en de koper. Dit probleem staat bekend als het probleem van externe effecten. Het gevolg van deze externe effecten is dat het investeringsniveau op een ongereguleerde markt lager is dan wat maatschappelijk optimaal is; zie figuur 2.3 voor een illustratie. Het maatschappelijk optimale investeringsniveau (weergegeven als het icoontje op de roze lijn) ligt rechts van het private optimum.

**Externe effecten komen in verschillende varianten voor bij digitale middelen.** Externe effecten doen zich bijvoorbeeld voor wanneer door onvoldoende betrouwbaarheidsinvesteringen een crimineel persoonsgegevens kan bemachtigen en daarmee, via identiteitsfraude, familieleden, vrienden of collega's oplicht. Een ander voorbeeld zijn IoT-apparaten die, als ze onvoldoende beveiligd zijn, gebruikt kunnen worden bij een DDoS-aanval op belangrijke websites, zoals die van banken. De derden zijn in dat geval de getroffen banken en hun klanten, die zijn namelijk niet betrokken bij de productie en koop van IoT-apparaten. De externe effecten kunnen ook van fysieke aard zijn. Haperingen in de betrouwbaarheid van digitale middelen kunnen tot ongelukken leiden met transportmiddelen, zoals auto's[12] of vliegtuigen.[13]

**Bij digitale middelen is het probleem van externe effecten vaak relevanter dan bij niet-digitale middelen.** Zodra een kwaadwillende weet dat de software van een digitaal product een kwetsbaarheid bevat, kan hij via internet deze misbruiken bij alle apparaten die deze software bevatten. Daarom kan een extern effect in potentie snel een groot aantal slachtoffers maken.[14] Bij niet-digitale producten beschikken criminelen minder snel over dit 'schaalvoordeel'.

**Ook door informatieproblemen levert de markt onvoldoende betrouwbaarheid.** De betrouwbaarheid van een digitaal product is afhankelijk van (ten minste) twee factoren. Ten eerste de tijd en moeite die een fabrikant vóór verkoop in veiligheid en beveiliging heeft gestoken, zoals testen en controles. Gebruikers zien dat niet en hebben zo een informatieachterstand op de fabrikant. Deze informatieachterstand is moeilijk op te lossen; als de broncode van software al inzichtelijk is, dan nog is het vanwege de omvang en complexiteit van de code praktisch onmogelijk om deze zelf te controleren. De tweede factor is de tijd en moeite ná de verkoop, zoals het monitoren en updaten van software. Dit gaat over toekomstig gedrag van de aanbieder, dat deels ook niet zichtbaar zal zijn voor de gebruiker. Hierdoor is het voor een fabrikant moeilijk om hierover bij de transactie geloofwaardige informatie te verstrekken. Bovenstaande problemen staan bekend als problemen van asymmetrische informatie. Het informatieprobleem kan versterkt worden door beperkte rationaliteit: voor gebruikers die zich niet bewust zijn van risico's is de betrouwbaarheid van een product minder relevant. Ze wegen betrouwbaarheid dan onvoldoende mee in hun koopbeslissingen.

**Marktmacht kan betrouwbaarheid zowel positief als negatief beïnvloeden.** Voor verschillende digitale middelen hebben aanbieders vaak een zeer hoog marktaandeel; het klassieke – maar zeker niet enige – voorbeeld is Microsoft dat met Windows langdurig een dominante positie had. Deze neiging tot concentratie wordt veroorzaakt door schaalvoordelen en netwerkeffecten, want de marginale kosten van een softwareprogramma zijn nihil en een product met veel gebruikers is aantrekkelijk voor andere gebruikers en aanbieders van complementaire software. Ook bij meer 'fysieke' digitale middelen, zoals smartphones, kunnen de marginale productiekosten relatief laag zijn. Een aanbieder met marktmacht kan een prikkel

[12] Zoals dit filmpje demonstreert.
[13] Dat betoogt een beveiligingsonderzoeker in dit artikel.
[14] Een voorbeeld is het eerder genoemde virus *Wannacry* dat in korte tijd ruim 200.000 slachtoffers maakte.

hebben om software voor een maatschappelijk gezien te korte periode te ondersteunen. Dit beperkt de economische levensduur van een product (Bulow, 1986). Om een praktisch voorbeeld te geven: een fabrikant van een telefoon kan besluiten om te stoppen met softwareondersteuning, zodat hij minder concurrentie ondervindt van eerder verkochte telefoons (denk aan 'refurbished' telefoons). Daarnaast kan een monopolist de betrouwbaarheid van producten differentiëren: een betrouwbaar product voor gebruikers met een hoge betalingsbereidheid en een minder betrouwbaar product voor gebruikers met een lagere betalingsbereidheid (Mussa en Rosen, 1978). Een praktisch voorbeeld hiervan is de Boeing 737 MAX, waarbij bepaalde waarschuwingslampjes alleen beschikbaar waren als duurdere optie.[15] Hier staat tegenover dat bedrijven met marktmacht ook een positieve prikkel hebben om te investeren in cyberveiligheid; de reputatie en het marktaandeel staan immers op het spel.[16]

# 3 Beleid voor digitale middelen

## Uitgangspunten

**Aanvullend beleid voor betrouwbare digitale middelen is nodig als externe effecten of andere verstoringen zorgen voor onwenselijke marktuitkomsten.** In rapporten over computerveiligheid worden hiervoor verschillende oplossingen geadviseerd, zoals certificaten, transparantieverplichtingen, veiligheidsnormen, of software-updateverplichtingen. Welke oplossing is optimaal? Bij goed beleid sluit het gekozen instrument aan op het specifieke probleem, en doet dat met zo min mogelijk kosten en negatieve bijwerkingen. Een instrument dat niet past bij het probleem is ineffectief – een APK is bijvoorbeeld geen oplossing voor autodiefstal. Overheidsingrijpen gaat meestal gepaard met kosten. Denk aan een software-updateverplichting, waarbij aanbieders extra moeten investeren om de regel na te leven en de overheid kosten maakt vanwege handhaving. Vanuit een economisch perspectief bezien moeten de verwachte maatschappelijke baten van zo'n regel opwegen tegen die kosten. Een instrument kan ook negatieve bijwerkingen hebben. Een veiligheidscertificaat kan bijvoorbeeld marktmacht versterken als alleen de dominante aanbieder aan de voorwaarden van een certificaat kan voldoen. En een veiligheidsstandaard kan na verloop van tijd technologisch achterhaald zijn waardoor het innovatie belemmert.

## Externe effecten

**Externe effecten kunnen 'geïnternaliseerd' worden**. Het klassieke antwoord op externe effecten is beprijzing. Door het beprijzen van het externe effect geeft de overheid financiële prikkels aan aanbieders en kopers om de effecten op anderen mee te wegen. Dit kan via een boetesysteem, waarbij partijen door een toezichthouder een boete krijgen als blijkt dat ze onvoldoende zorgvuldig hebben gehandeld. Het toezicht op beveiliging van persoonsgegevens is bijvoorbeeld (onder andere) op deze gedachte gebaseerd. Een andere route om hetzelfde doel te bereiken is het aansprakelijkheidsrecht. Door aanbieders aansprakelijk te stellen voor geleden schade van gebruikers of derden, nemen aanbieders de maatschappelijke waarde van meer betrouwbaarheid mee in hun afwegingen. Een kenmerk van aansprakelijkheid is dat het technologieneutraal[17] is – het geldt net zozeer voor donuts als voor drones. Dat maakt aansprakelijkheid in principe een geschikt instrument voor digitale middelen, waarvan de mate van technologische onzekerheid hoog is. In de praktijk wordt het aansprakelijkheidsrecht ook benut bij digitale middelen: zie de zaak van de Consumentenbond

[15] Aldus dit nieuwsbericht van Reuters.
[16] Zo rapporteert Microsoft dat hun investeringen in de cybersecurity van zijn producten jaarlijks 1 miljard dollar bedragen. (link).
[17] Technologieneutrale regels schrijven geen bindende technische specificatie voor, maar wel welk doel gehaald moet worden, of aan welke gedragsnorm voldaan moet worden. Zie Bijlsma et al. (2016).

tegen Samsung[18], de claim van de Estse politie tegen Gemalto[19] en nabestaanden van vliegtuigrampen tegen Boeing.[20]

**Aansprakelijkheid van schade bij ICT-incidenten heeft ook nadelen.** Ten eerste kan schade niet altijd vergoed worden. Dit kan gebeuren als de financiële schade na een incident zodanig hoog is dat de aanbieder failliet gaat. Ook is een financiële compensatie nooit een werkelijke compensatie bij ernstige fysieke schade. Compensatie is ook problematisch wanneer de schade verspreid is over een groot aantal partijen. Een tweede nadeel is dat, zeker bij digitale middelen, risico's moeilijk voorspelbaar zijn.[21] Het gevolg van deze beperkingen is dat een aanbieder niet de volle maatschappelijke baten van investeringen in betrouwbaarheid mee kán wegen en dat het investeringsniveau suboptimaal blijft. Voor die gevallen is aanvullend beleid nodig – al zal het niet eenvoudig zijn om in de praktijk in te schatten wanneer dat zo is.

**De zelfrijdende auto is een voorbeeld van een case waarbij mogelijk aanvullend beleid nodig is.** Als auto's volledig zelfrijdend worden, zitten mensen niet meer zelf aan het stuur. Een systeem waarbij autobestuurders aansprakelijk zijn voor de schade bij derden na een ongeluk is dan ook zinloos in zo'n wereld. Welk systeem daarvoor in de plaats moet komen is echter nog onduidelijk. Een gevolg kan zijn dat de aansprakelijkheid voor schade bij een auto-ongeluk verschuift van de bestuurder naar de fabrikant, maar andere regels zijn ook mogelijk. Als het bepalen van de schuld bij autonome voertuigen technisch complexer (en dus duurder) is dan bij menselijke bestuurders, dan is een verschuiving van aansprakelijkheid naar fabrikanten niet efficiënt. De fabrikanten zullen elkaar dan wederzijds compenseren en niet de volledige maatschappelijke schade voelen.[22] Een systeem dat dan betere prikkels geeft voor investeringen is om autofabrikanten ieder de *volledige* schade te laten betalen aan de overheid. Dergelijke implicaties suggereren dat ook voor andere producten een herziening van het aansprakelijkheidsrecht noodzakelijk is.

**De optimale interventie om te corrigeren voor externe effecten hangt af van de omvang van het probleem.** Figuur 3.1 illustreert dit. Als externe effecten beperkt zijn, in de eerste trede van de interventieladder, dan is aansprakelijkheidsrecht in principe voldoende. Als achteraf een schadelijk incident optreedt, dan kan die aanbieder via aansprakelijkheidsrecht de schade vergoeden. Dit prikkelt de aanbieder om externe effecten te internaliseren.

[18] In deze zaak wees de rechtbank de klacht van de Consumentenbond af, omdat niet aangetoond kon worden dat Samsung zich onvoldoende inspant (link).
[19] Zie bijvoorbeeld dit nieuwbericht van Reuters.
[20] Volgens dit bericht in de Washington Post.
[21] Naast andere, al genoemde incidenten in dit stuk, is Heartbleed ook een voorbeeld van een kwetsbaarheid met onverwacht grote gevolgen. Hierbij konden voor veel populaire websites wachtwoorden gehackt worden via een lek in open source proramma OpenSS.
[22] Dit wordt beargumenteerd in een recent paper van Shavell (2019).

**Figuur 3.1 Interventieladder voor externe effecten**


**Veiligheidsmaatregelen vóór de verkoop zijn nodig als aansprakelijkheid achteraf tekortschiet.** Dit is de tweede trede van de interventieladder. Overheden kunnen eisen opleggen aan de veiligheid van producten en diensten, en zo corrigeren voor externe effecten. Dit kan via het voorschrijven van technische specificaties, of gedragsnormen. Voorbeelden zijn de verplichting voor airbags in nieuwe auto's, of het dragen van autogordels. Dit soort standaarden kunnen effectief zijn om betrouwbaarheid te vergroten. De kans op een dodelijke afloop bij een auto-ongeval is bijvoorbeeld met meer dan tachtig procent verminderd na de verplichtstelling van airbags en autogordels (Crandall, Olson en Sklar, 2001). Technische specificaties of gedragsnormen zijn minder geschikt als een product complex of uniek is, of als het product door innovatie snel verandert en de technologische onzekerheid dus hoog is. Een mogelijkheid om in die gevallen de betrouwbaarheid te vergroten, is door het product vooraf te toetsen onder verschillende omstandigheden, zoals bij auto's en vliegtuigen gebeurt. 100% zekerheid kan ook bij toetsing vooraf niet gegarandeerd worden (Murdoch, Bond en Anderson, 2012).

**Beveiligingsstandaarden voor IoT-apparaten hebben voor- en nadelen.** Verschillende experts pleiten voor beveiligingsstandaarden voor IoT-apparaten. Vanuit de economische beleidstheorie kunnen beveiligingsstandaarden zinvol zijn als aansprakelijkheid achteraf tekortschiet. Bij misbruik door een hacker van slecht beveiligde IoT-apparaten is dat waarschijnlijk het geval, want aanbieders kunnen eventuele schade moeilijk voorzien en worden bovendien beschermd door beperkte aansprakelijkheid. Of een beveiligingsstandaard welvaartsverhogend is, hangt af van de omstandigheden. Er zijn veel verschillende typen IoT-apparaten[23], waardoor het vaststellen van een standaard-standaard niet eenvoudig is. Met name wanneer de externe effecten beperkt zijn, is niets doen ook een optie. Andere marktpartijen zullen dan proberen om de impact van externe effecten te mitigeren. Zo hebben internet service providers bijvoorbeeld een prikkel om de impact van DDoS-aanvallen, bijvoorbeeld via gehackte IoT-apparaten, te beperken.[24]

**In extreme gevallen is een verbod optimaal.** Dit is de derde trede van de interventieladder. Als de negatieve externe effecten van een digitaal product of dienst erg groot zijn en de andere overheidsinstrumenten onvoldoende effectief, dat kunnen de netto maatschappelijke baten uiteindelijk negatief zijn. In die situaties is een verbod, al dan niet tijdelijk, de beste maatregel. Verboden niet-digitale producten in Nederland zijn

[23] Denk aan digitale assistenten, energiemeters, smartphones, thermostaten, lampen, deursloten, deurbellen, camera's, etc.
[24] In Nederland doen ISP's dit onder andere via de 'Nationale Wasstraat' (link).

bijvoorbeeld gevaarlijk vuurwerk, de meeste wapens of medicijnen zonder marktvergunning. Ook bij digitale producten is een verbod een mogelijkheid. De internationale discussie[25] over wel of niet toelaten van Huawei bij de aanleg van 5G-netwerken draait om de mogelijke negatieve externe (geopolitieke) effecten op de samenleving.

## Informatieproblemen

**Informatieproblemen zijn moeilijk op te lossen door de overheid.** Deze problemen kunnen soms beter opgelost worden door aanbieders dan door de overheid, omdat aanbieders niet alleen op kopers een informatievoorsprong hebben, maar ook op de overheid. Als de betrouwbaarheid van een product voor consumenten belangrijke informatie is, dan heeft een aanbieder een prikkel om die informatie te geven. Dit kan door een onafhankelijke partij te laten controleren welke maatregelen genomen zijn en dit via een certificaat of keurmerk[26] bekend te maken. Een aanbieder kan ook een garantie geven op (onderdelen van) het product of een reputatie opbouwen.

**Voor consumenten helpt het conformiteitsbeginsel om informatieproblemen te beperken.** Dit beginsel[27] is de wettelijke (en 'technologieneutrale') voorwaarde dat consumenten ervan uit mogen gaan dat een product naar behoren functioneert en veilig is. Dus ook consumenten die zich nauwelijks verdiepen in de beveiligingsaspecten mogen verwachten dat een digitaal product beveiligd is tegen hacken. Een nadeel van het conformiteitsbeginsel is rechtsonzekerheid; met name bij producten die zich snel ontwikkelen kan het onduidelijk zijn waar een consument van uit had mogen gaan.

**De overheid kan betrouwbaarheid van digitale middelen verder vergroten via informatievoorziening.** In sommige gevallen kan beleid over informatie toch wenselijk zijn. Eén mogelijkheid is dat consumenten zich onvoldoende bewust ('beperkt rationeel') zijn van de impact van een ICT-incident en bij de aankoop of gebruik te weinig letten op betrouwbaarheid. Beleid kan hierop inspelen met voorlichtingscampagnes, of het afdwingen van gestandaardiseerd belangrijke productinformatie. Bij o.a. financiële producten (de financiële bijsluiter) of voedsel (over ingrediënten en voedingswaarde) bestaan dergelijke verplichtingen al. Bij een digitaal product kan gedacht worden aan informatie over de periode waarvoor de aanbieder garandeert dat beveiligingsupdates worden verstrekt. Een tweede mogelijkheid is dat het aanbieders niet lukt om samen afspraken over te maken over een certificaat ('coördinatiefalen'). De overheid kan hierbij een intermediaire rol spelen. Een certificaat heeft vooral meerwaarde als een onafhankelijke partij het product of dienst objectief kan toetsen en de resultaten relevant zijn voor consumenten.

**Europese certificaten kunnen coördinatieproblemen helpen oplossen.** De Europese Cybersecurity Act uit 2019 stelt voor om voor de betrouwbaarheid van digitale middelen Europese certificaten in te stellen en nationale systemen te harmoniseren.[28] Als aanbieders of consumentenorganisaties niet in staat zijn om te coördineren op een werkbaar systeem, dan kan een Europees systeem een oplossing bieden. Een ander doel van een Europees systeem is om de bestaande nationale systemen te harmoniseren. Als de nationale systemen bestaan vanwege een gebrek aan vertrouwen tussen landen, dan zijn Europese certificaten waarschijnlijk niet het juiste antwoord, omdat het achterliggende probleem van gebrek aan wederzijds vertrouwen niet wordt opgelost.

[25] Zie bijvoorbeeld dit artikel in *The Economist*.
[26] Een keurmerk is een zichtbaar bewijs (beeldmerk of logo) voor afnemers dat een product aan bepaalde standaarden voldoet. Een certificaat is een schriftelijke verklaring dat een product of dienst aan bepaalde eisen voldoet. Een certificaat geeft zo informatie over aspecten van de betrouwbaarheid van een digitaal product en kan consumenten helpen om beter geïnformeerde keuzes te maken.
[27] Dit uitgangspunt staat bijvoorbeeld in artikel 7:17 BW.
[28] Zie hier de toelichting van de EC.

### Marktmacht

**Er is meer dan alleen het mededingingstoezicht om te voorkomen dat bedrijven te veel marktmacht krijgen.** Bij een fusie of overname van aanbieders van digitale middelen zal de toezichthouder (Autoriteit Consument & Markt in Nederland en DG Competition van de Europese Commissie) niet alleen kijken naar de prijseffecten, maar ook naar de verwachte effecten van de fusie op kwaliteit en betrouwbaarheid. Daarnaast kan de overheid de concurrentie vergroten via slim inkopen, 'launching customership' of prikkelen van betrouwbare opensourcesoftware (OSS). Het bestaan van OSS geeft commerciële aanbieders een prikkel om betaalbare en betrouwbare producten te ontwikkelen. OSS is een voorbeeld van een publiek goed dat door de markt wordt ontwikkeld; per definitie kan niemand worden uitgesloten van gebruik van OSS en het gebruik van OSS gaat niet ten koste van andere gebruikers (OSS is 'niet-rivaal' in economisch jargon). Niet alleen OSS is een publiek goed, maar ook de *betrouwbaarheid* van OSS is dat. Overheidsorganisaties kunnen de betrouwbaarheid van OSS vergroten door onderzoeksbeurzen of prijzen voor betrouwbaarheidsoplossingen voor OSS.[29]

**Een verplichte ondersteuningsperiode kan leiden tot onbedoelde neveneffecten.** Aanbieders van digitale middelen die beschikken over marktmacht ondersteunen software mogelijk voor een te korte periode. Een oplossing hiervoor die soms genoemd wordt, is een verplichting om software voor een vastgestelde periode te ondersteunen.[30] Een uitdaging bij een dergelijke verplichting is dat de mate van marktmacht varieert tussen markten én over de tijd. Dit betekent dat de optimale wettelijke ondersteuningsperiode verschilt tussen producten en na verloop van tijd kan veranderen. Risico's van een te korte of te lange wettelijke ondersteuningsperiode zijn dat toetreding door nieuwe bedrijven wordt ontmoedigd, of dat bedrijven minder snel innoveren. Als een ondersteuningsperiode te lang is zal een bedrijf minder snel een nieuw product aanbieden, omdat de ondersteuningskosten niet opwegen tegen de onzekere opbrengsten. Tenslotte brengt een verplichting handhavingskosten met zich mee. Voor ieder type product moet een periode worden vastgesteld (een smartphone gaat minder lang mee dan een auto). Ook is toezicht nodig op de snelheid en kwaliteit van updates. Een risico is dat bedrijven zich formeel houden aan de verplichting, maar te late of te onvolledige updates versturen.

# 4 Ten slotte

**Beleid is nodig voor de betrouwbaarheid van digitale middelen.** In deze *Policy Brief* hebben we de vraag onderzocht of, vanuit een algemeen economisch perspectief, overheidsingrijpen gericht op betrouwbaarheid op de markt voor digitale middelen wenselijk is. Vanwege verschillende vormen van marktfalen is ingrijpen inderdaad legitiem. De manier waarop de overheid kan ingrijpen wordt bemoeilijkt door de grote diversiteit van digitale middelen en de technologische onzekerheid. Een eerste pijler voor beleid is het aansprakelijkheidsrecht. De schade die is ontstaan door een foutief digitaal product kan achteraf verhaald worden op de aanbieder, die daarmee vooraf geprikkeld wordt om aandacht te hebben voor de betrouwbaarheid. Een tweede pijler is het conformiteitsbeginsel. Dit is de wettelijke voorwaarde dat consumenten ervan uit mogen gaan dat een product naar behoren functioneert en veilig is. Deze regel geldt net zo goed voor digitale middelen en is daarom technologieneutraal. Aansprakelijkheid en het conformiteitsbeginsel leveren soms, vanuit maatschappelijk perspectief, een te laag niveau van betrouwbaarheid op. Die gevallen vergen aanvullende maatregelen zoals certificaten, informatievoorziening

[29] SPIN is een voorbeeld van OSS voor betrouwbare IoT-netwerken. Zie deze site van SIDN voor meer informatie.
[30] Bij een verplichte ondersteuningsperiode is de aanbieder verplicht om veiligheidsupdates te leveren, zie EZK (2018).

of veiligheidsnormen. De interventieladder van figuur 3.1 helpt bij het bepalen welke type maatregelen dat zijn.

**Verder verhogen van betrouwbaarheid kan op verschillende manieren.** Deze *Policy Brief* noemt de mogelijkheid om beveiligingsstandaarden in te stellen, of producten vooraf te toetsen. De resultaten van deze toetsen kunnen kenbaar gemaakt worden aan potentiële kopers via certificaten. Daarnaast kan de overheid transparantie over betrouwbaarheid vergroten door aanbieders te verplichten om kopers te informeren over belangrijke aspecten, zoals de periode waarvoor de aanbieder het product ondersteunt. Overheden kunnen de ontwikkeling van betrouwbare open source software stimuleren, zoals via *challenges* of inkoopbeleid.

**Beleid voor digitale middelen kan doorschieten.** Een maatregel kan leiden tot hogere kosten voor handhaving en naleving, of de introductie van nieuwe producten tegenhouden. Deze nadelen moeten opwegen tegen de voordelen van meer betrouwbaarheid.

# Literatuurlijst


Bijlsma, M., B. Overvest en S. Straathof, 2016, Marktordening bij nieuwe ICT-toepassingen, CPB Policy Brief.

Bulow, J., 1986, An Economic Theory of Planned Obsolescence, *The Quarterly Journal of Economics*, vol. 10: 729-749.

CBS, 2019, ICT, Kennis en Economie (link).

Crandall, C.S., L.M. Olson en D.P. Sklar, 2001, Mortality Reduction with Air Bag and Seat Beld Use in Head-on Passenger Car Collisions, *American Journal of Epidemiology*, vol. 153: 219-224.

CSR, 2017, Naar een veilig verbonden digitale samenleving: advies inzake de cybersecurity van het Internet of Things (IoT).

EZK, 2018, Roadmap Digitaal Veilige Hard- en Software.

Fry, H., 2018, *Hello World. Being Human in the Age of Algorithms*, Transworld Publishers Ltd.

Leverett, E., R. Clayton en R. Anderson, 2017, Standardisation and Certification of the 'Internet of Things', Proceedings of WEIS.

Murdoch, S., M. Bond en R. Anderson, 2012, How Certification Systems Fail: Lessons from the Ware Report, University of Cambridge.

Ruesink, F. en R. Windig, 2019, Een blik op de NCSC-beveiligingsadviezen, CPB Notitie.

Shavell, S., 2019, On the redesign of accident liability for the world of autonomous vehicles, NBER Working Paper, nr. 26220.