Eindrapport

Beleidsdoorlichting van de operationele doelstellingen 2 en 3 (van art. 10 van de begroting van het Ministerie van EL&I)

16 juni 2011

Voor meer informatie
Kwink Groep BV
Hartogstraat 11
Postbus 93063
2509 AB DEN HAAG
+31 (0)70 359 6955
www.kwinkgroep.nl

Ir. B.P.A. (Bill) van Mil
Projectleider
+31 (0)6 3449 2008
bvanmil@kwinkgroep.nl

INHOUDSOPGAVE

1 INLEIDING

1.1 DOELSTELLING, SCOPE EN AANPAK

Elektronische communicatienetwerken en -diensten leveren een belangrijke bijdrage in het streven van het Ministerie van Economische Zaken, Landbouw en Innovatie (EL&I) om in een open wereldeconomie de condities voor een welvarend, duurzaam en ondernemend Nederland te realiseren. De algemene doelstelling van artikel 10 van de EL&I-begroting (2010) luidt: 'Een hoogwaardig en adequaat aanbod van netwerken en diensten voor elektronische communicatie en post.' Deze doelstelling richt zich op het bevorderen van de positieve effecten van elektronische communicatienetwerken en -diensten en het beperken van de risico's die aan het gebruik ervan kleven.

De algemene doelstelling van artikel 10 is opgesplitst in drie operationele doelstellingen, waarvan er twee in deze beleidsdoorlichting zijn onderzocht:

- Operationele Doelstelling 2 (OD 2): 'Een veilig en betrouwbaar elektronisch en postnetwerk'
- Operationele Doelstelling 3 (OD 3): 'Ontwikkeling van innovatieve voorzieningen, digitalisering van omroeptoepassingen, faciliteren van producten en diensten voor elektronische communicatie en benutting ervan door de consument, het bedrijfsleven en de (semi-)publieke sector'

Het doel van deze beleidsdoorlichting is het gevoerde beleid ten aanzien van OD 2 en OD 3 te beoordelen op *legitimiteit*, *doeltreffendheid* (en samenhang) en *doelmatigheid*.

De periode waarop de beleidsdoorlichting van OD 2 terugkijkt is 2001-2010. De periode over welke de beleidsdoorlichting van OD 3 plaatsvindt is 2004-2010. Van de volgende onderwerpen heeft de opdrachtgever bepaald dat ze buiten de scope van deze beleidsdoorlichting vallen: aftappen en dataretentie, de postmarkt en de uitgifte van vergunningen voor frequenties voor nieuwe technieken, toepassingen en diensten.[1]

De onderzoeksstrategie was erop gericht om zo veel mogelijk 'evidence-based' uitspraken te kunnen doen. Daartoe is bijvoorbeeld gezocht naar zo veel mogelijk kwantitatieve gegevens en indicatoren die een beeld geven van het doelbereik en de bijdrage van de door het Ministerie van EL&I ingezette instrumenten daarbij. In hoofdstuk 4 zijn deze kwantitatieve indicaties weergegeven.

De uitvoering van deze beleidsdoorlichting is begeleid door een begeleidingscommissie met zowel vertegenwoordigers van het Ministerie van EL&I als een tweetal externe vertegenwoordigers (zie Bijlage 1). Het onderzoek is primair gebaseerd op documentenanalyse. In aanvulling daarop is een relatief beperkt aantal interviews gehouden (zie Bijlage 2).

1.2 LEESWIJZER

In de hoofdstukken 2, 3 en 4 wordt telkens onderscheid gemaakt tussen 'beschrijving' en 'beoordeling'.

[1] Voor 'aftappen en dataretentie' geldt dat het EL&I-beleid faciliterend is voor het Ministerie V&J dat eerstverantwoordelijke is en haar beleid ten aanzien van aftappen en dataretentie inzet om criminaliteit in algemene zin te bestrijden. Aftappen en dataretentie hebben zodoende dus niet primair het doel om bij te dragen aan een veilig en betrouwbaar elektronisch en postnetwerk. De postmarkt valt volgens het Ministerie van EL&I buiten de scope van het onderzoek omdat Nederland in internationaal perspectief zeer goed presteert. Gedurende de evaluatieperiode zijn er daarom geen specifieke beleidsdoelstellingen ten aanzien van een veilig en betrouwbaar postnetwerk opgesteld. Voor de uitgifte van vergunningen voor frequenties voor nieuwe technieken, toepassingen en diensten geldt dat hierover in de beleidsdoorlichting van OD 1 reeds een evaluatie heeft plaatsgevonden.

In hoofdstuk 2 gaan we in op de legitimiteit van de rol van de overheid en de gekozen doelstellingen. Hiertoe worden allereerst de operationele doelstellingen OD 2 en OD 3 en de bijbehorende subdoelen beschreven. Daarna wordt aangegeven waarom de overheid het tot haar verantwoordelijkheid rekende om een rol te nemen. Tot slot wordt in de paragraaf 'beoordeling' ons oordeel hierover weergegeven.

In hoofdstuk 3 worden alle instrumenten van OD2 en OD3 beschreven alsmede de ingezette middelen. Daarna wordt ingegaan op de vraag of de juiste instrumenten zijn gekozen en of de instrumenten kostenbewust zijn ingezet: doeltreffendheid en doelmatigheid.

In hoofdstuk 4 wordt ten slotte beschreven wat is bereikt en waar nog verbeterruimte zit voor de toekomst.

In bijlage 1 en 2 wordt achtereenvolgens een overzicht gegeven van de leden van de begeleidingscommissie en een overzicht van de geïnterviewde externe stakeholders. In bijlage 3 van dit rapport is een afkortingenlijst opgenomen.

2 LEGITIMITEIT VAN DE ROL VAN DE OVERHEID EN GEKOZEN DOELSTELLINGEN

2.1 BESCHRIJVING

2.1.1 BESCHRIJVING DOELEN

In het schema hierna is de uitwerking van de beleidsdoelstelling van OD 2 in sub-beleidsdoelstellingen opgenomen.

OD 2: "Veilig en betrouwbaar elektronisch- en postnetwerk"
De achterliggende gedachte van OD 2 is dat de elektronische communicatie zich ontwikkelt tot alomtegenwoordige en kritische infrastructuur zonder welke de meeste economische en maatschappelijke functies niet meer zouden functioneren. Vertrouwen in en veiligheid van elektronische communicatie en post zijn van steeds groter belang, maar ook het vermogen van de gebruikers om met de onveiligheid daarvan om te gaan.
Sub-beleidsdoelstellingen
1. Publieke belangen (veiligheid, betrouwbaarheid, toegankelijkheid en transparantie) waarborgen. *In werkplannen uitgelegd als "Continuïteit en betrouwbaarheid vitale elektronische telecommunicatienetwerken en -diensten zijn gewaarborgd"* i. Sector optimaal voorbereid laten zijn op verstoringen van elektronische communicatienetwerken en -diensten ii. Inzicht verkrijgen in kwetsbaarheden en afhankelijkheden van de vitale elektronische telecommunicatienetwerken en -diensten iii. Werkbare afspraken maken over respons en informatievoorziening
2. Vertrouwen in elektronische netwerkdiensten en -toepassing bevorderen. *In werkplannen uitgelegd als "Gebruik van internet is veilig en betrouwbaar"* i. Beperking economische schade en overlast door cybercrime ii. Bescherming persoonlijke levenssfeer / privacy op internet iii. Vergroten vertrouwen in ICT-gebruik bij burgers en bedrijven (door voorlichting)

In het schema hierna zijn de sub-beleidsdoelstellingen en instrumenten met betrekking tot het OD 3-beleid weergegeven.

OD 3: "ontwikkeling van innovatieve voorzieningen, digitalisering van omroeptoepassingen, faciliteren van producten en diensten voor elektronische communicatie en benutting ervan door de consument, het bedrijfsleven en de (semi-) publieke sector"
De gedachte achter OD 3 is dat met ICT meer economisch en maatschappelijk rendement kan worden behaald en dat de overheid, waar nodig, het gebruik van ICT faciliteert of stimuleert.
Sub-beleidsdoelstellingen
1. Bevorderen dat bedrijven ICT inzetten waardoor productiviteit en efficiëntie toenemen
2. ICT toepassen in de overheidsdienstverlening aan bedrijven waardoor de dienstverlening van de overheid verbetert en er verlaging van administratieve lasten plaatsvindt
3. Stimuleren dat in met publieke middelen gefinancierde sectoren ICT wordt toegepast waardoor maatschappelijke problemen worden opgelost
4. Ervoor zorgen dat burgers actief kunnen deelnemen aan de informatiemaatschappij en daarvoor een goede toegang hebben tot infrastructuren en een divers dienstenaanbod

2.1.2 WAT WAS HET PROBLEEM EN WAAROM REKENDE DE OVERHEID HET TOT HAAR VERANTWOORDELIJKHEID?

Voor OD 2 geldt dat er een duidelijk te definiëren probleem is. De potentiële uitval van telecommunicatie is een groot probleem, omdat veel burgers en bedrijven daarvan zeer afhankelijk zijn. Bij grootschalige uitval

ontstaat er maatschappelijke ontwrichting en ondervindt de economie grote schade. Uitval van openbare telecommunicatie moet dus worden voorkomen en staat daarom al lange tijd op de agenda.

Als het gaat om internetveiligheid, dan geldt dat de omvang van de internethandel groot is geworden, maar dat tegelijkertijd cybercrime als probleem ook omvangrijker is geworden. In de Kwint-nota - waarin het beleid voor een belangrijk deel is vervat - zijn vele verschillende vormen van kwetsbaarheden die de internetveiligheid ondermijnen benoemd.[2] Dat vormde aanleiding om te concluderen dat ingrijpen door overheid (en door marktpartijen) noodzakelijk is.

De probleemoriëntatie van OD3 richt zich op een betere benutting van ICT(-toepassingen). Want hoewel Nederland al een aantal jaren lang koploper is binnen Europa als het gaat om de ICT-basis, werd er vooral in de beginperiode van deze beleidsevaluatie nog onvoldoende rendement gegeneerd uit ICT-toepassingen in termen van productiviteitsgroei, vermindering administratieve lasten en maatschappelijk nut[3]. Om internationaal tot de voorhoede te kunnen (blijven) behoren, is het daarom van belang om te zorgen dat de Nederlandse bevolking kan omgaan met digitale diensten, deze vertrouwt, waardeert en gebruikt om eigen welvaart en welzijn te bevorderen en daardoor bijdraagt aan duurzame economische groei. De maatschappelijke meerwaarde van ICT-gebruik is daarnaast gelegen in de verbetering van dienstverlening (van overheden), de verhoging van de arbeidsproductiviteit en het vergroten van het innovatieve vermogen van de publieke en private sectoren.[4]

Waarom rekende de Rijksoverheid het tot haar verantwoordelijkheid?

Beleid is legitiem en noodzakelijk wanneer er sprake is van een publiek belang waarbij (wordt verwacht dat) bestaande marktprocessen, sociale processen en innovatieprocessen niet 'vanzelf' zullen leiden tot borging van dit publieke belang. Overheidsingrijpen kan derhalve worden gelegitimeerd zodra marktpartijen tekort schieten in het bereiken van (specifiek geformuleerde) maatschappelijke doelstellingen.

De Rijksoverheid rekent het tot haar verantwoordelijkheid om het probleem te helpen oplossen omdat er sprake is van een publiek belang en omdat er sprake is van marktfalen en systeemfalen, waardoor dat publieke belang niet als vanzelfsprekend wordt geborgd.[5] Hierna worden de vormen van marktfalen en systeemfalen genoemd waarbij een directe relatie wordt gelegd met de instrumenten die in het kader van OD 2 en OD 3 zijn gehanteerd. Daarmee wordt duidelijk wat de legitimering van het beleid is.

Marktfalen

Er kan een viertal vormen van marktfalen worden onderscheiden die aanleiding hebben gegeven voor overheidsingrijpen.[6]

Ten eerste: externaliteiten (waaronder spillovers). Er is sprake van externaliteiten als de kosten en baten van een investering niet bij dezelfde organisatie belanden. Dat is onder andere aanleiding geweest voor het **spamverbod** en de handhaving ervan door OPTA. Immers, zodra één ISP zich voorneemt spam te bestrijden door spamverstuurders actief aan te pakken draagt deze ISP de kosten en verslechtert zijn concurrentiepositie ten opzichte van de andere ISP's die geen spamverstuurders aanpakken en die dus niet die kosten maken.

---

[2] Tweede Kamer, vergaderjaar 2000-2001, 26 643, nr. 30.

[3] Beter Presteren met ICT; Vervolg Rijksbrede ICT-Agenda 2005 - 2006, Tweede Kamer, vergaderjaar , 2004-2005, 26 643, nr. 63

[4] ICT-Agenda 2008-2011 De Gebruiker Centraal in de Digitale Dienstenmaatschappij, Tweede Kamer, vergaderjaar 2007-2008, 26 643, nr. 125.

[5] WRR (2000). *Borging publieke belangen*. Den Haag. In recentere studies voegt de WRR toe dat ook systeemfalen kan leiden tot overheidsingrijpen teneinde publieke belangen te borgen. Zie: WRR (2008). *Innovatie vernieuwd: opening in viervoud*. Den Haag. Naast marktfalen en systeemfalen kan overheidsingrijpen ook worden gelegitimeerd op grond van het argument van inkomensherverdeling. Een markt kan Pareto-efficiënt zijn, maar tegelijkertijd leiden tot ongewenste inkomensongelijkheid. De overheid kan in dit geval ingrijpen middels het heffen van inkomstenbelasting.

[6] Zie bijvoorbeeld Poel, M. en L. Kool (2008). *The policy mix for ICT innovation in the Netherlands: in search of new instruments, policy coherence and impact*. Delft: TNO. Zie ook: Stiglitz, J.E. (2000). *Economics of the public sector*. Third Edition. W.W. Norton & Company: New York.

Andere ISP's profiteren daar in beginsel van, omdat hun klanten minder spam ontvangen van de verstuurders (en daardoor het netwerk minder wordt belast). Het is ook de aanleiding voor een **Platform Internetveiligheid** waar wordt gewerkt aan de aanpak van internetproblemen als botnets. Voor dergelijke problemen geldt dat de aanpak ervan geld kan kosten voor providers, maar dat opbrengsten niet noodzakelijkerwijs ook bij deze providers belanden. Ook gelden externaliteiten als één van de aanleidingen voor het **programma NDiV**; MKB-ers willen enerzijds de boot niet missen, maar anderzijds wil geen van hen als eerste 'de boot in' als het gaat om het initiëren van ketensamenwerking. Het **NCO-T** kan hier ook als voorbeeld worden genoemd: het NCO-T is bij wet ingesteld om overleg met de sector te hebben over continuïteitsmanagement aangezien de overheid geen eigenaar meer was van netwerken. Externaliteiten spelen een belangrijke rol bij het continuïteitsmanagement. Daarnaast vormen externaliteiten de aanleiding voor het **platform ECP-EPN**. ECP-EPN stelt zelf dat sectoroverschrijdende publiek-private samenwerking op het gebied van ICT onmogelijk door één partij kan worden gerealiseerd.[7] Bovendien is er sprake van spill-over effecten omdat de inzet of deelname van de ene marktpartij ten goede kan komen aan de andere marktpartij.

Ten tweede kan sprake zijn van collectieve goederen. Dat zijn goederen die onmogelijk aan slechts één individu zijn te leveren (bijvoorbeeld een dijk ter bescherming van overstromingen of het leger), waardoor geen partij zich verantwoordelijk voelt om hiervoor te betalen. Dit argument speelt op het gebied van OD 2 en OD 3 geen belangrijke rol: gebruikers kunnen worden uitgesloten van telecommunicatie en internet, bijvoorbeeld wanneer zij geen abonnement hebben.

Ten derde kan informatieasymmetrie een reden zijn voor overheidsingrijpen, omdat er sprake is van beperkte rationaliteit van consumenten (als gevolg van de transactiekosten die gepaard gaan met het zoeken en vergelijken van producten en diensten). De overheid onderneemt dan initiatieven om de eindgebruiker (consumenten maar ook bedrijven) van betere informatie te voorzien dan wel hun positie te verbeteren zodat ze zelf betere informatie kunnen vragen aan aanbieders. De **projecten ICT-verstoring** en **CAET** zouden hier als voorbeeld kunnen worden genoemd.

Ten vierde kan er sprake zijn van onvoldoende marktwerking. Als gevolg hiervan kan marktmacht ontstaan waardoor bijvoorbeeld monopolie- of oligopolievorming kan optreden. De overheid houdt toezicht op de marktwerking via de mededingingsautoriteiten. Deze vorm van marktfalen is expliciet onderdeel van het beleid op het gebied van Operationele Doelstelling 1, en heeft in mindere mate betrekking op de instrumenten onder OD 2 en OD 3. Een voorbeeld van onvoldoende marktwerking is onduidelijkheid over standaarden en het gebrek aan level playing field op de softwaremarkt. Dit vormde onder meer aanleiding voor de oprichting van het **College en Forum Standaardisatie** (open standaarden en interoperabiliteit) en **het actieplan NOiV** voor het stimuleren van het gebruik van Open Source Software (OSS).

Systeemfalen

Voorts kan een vijftal vormen van systeemfalen worden onderscheiden die aanleiding kunnen zijn voor overheidsingrijpen.[8]

Ten eerste kunnen er belemmeringen in infrastructuren bestaan. Belemmeringen in infrastructuren dienen zich aan als er een ontoereikend aanbod is van bijvoorbeeld fysieke infrastructuur.[9] Deze belemmering is bijvoorbeeld reden geweest te investeren in breedband, met het **Actieprogramma Breedband**. Ook is deze belemmering een achterliggende reden geweest om beleid te maken in het licht van **spambestrijding**. Immers, spam doet een beroep op de netwerkcapaciteit waardoor congestie op netwerken kan ontstaan.

Ten tweede kan sprake zijn van 'lock-in' effecten en padafhankelijkheid. Het 'lock-in' effect houdt in dat organisaties niet in staat zijn om zich aan te passen aan nieuwe technologie, nieuwe 'business models' of

[7] ECP-EPN (2010). Van beschikbaarheid naar toepassing, p21

[8] WRR (2008). *Innovatie vernieuwd: opening in viervoud*. Den Haag.

[9] Smith, K. (2000). Innovation as a systemic phenomenon: rethinking the role of policy, *Enterprise & Innovation Management Studies 1*(1), 73-102.

nieuwe manieren om een productieproces in te richten. Bij padafhankelijkheid is er sprake van een beperking met betrekking tot toekomstige keuzemogelijkheden door eerder gemaakte keuzes.[10] Als het gaat om het **gebruik van OSS** geldt dat het voor organisaties veelal onaantrekkelijk is om over te stappen op andere software omdat software veelal onderdeel is van geïntegreerde softwarepakketten en de compatibiliteit met software van andere organisaties in het geding komt. En ook is sprake van padafhankelijkheid door bestaande contracten met leveranciers, technische afhankelijkheid van bestaande systemen en maatwerk-software. Het programma **NOiV** richt zich op deze problematiek. Ook in de digitalisering van overheidsdienstverlening (**eOverheid voor Bedrijven**) is sprake van lock-in-effecten bij overheidsorganisaties (onvoldoende kennis van en prikkel voor digitalisering dienstverlening).

Ten derde kunnen er institutionele belemmeringen zijn. Instituties zijn gewoonten, gebruiken, routines, afspraken en regels die de relaties en interacties tussen individuen, groepen en organisaties in een markt reguleren.[11] Zo zijn de informatieknooppunten van het **NICC** te beschouwen als een programma dat voortkomt uit institutionele belemmeringen. Immers, marktpartijen (uit de vitale sectoren) waren voorheen niet gewend om elkaar te informeren over cybersecurity dreigingen. Het heeft in het NICC overigens ook bijna twee jaar geduurd voordat een vertrouwensband was opgebouwd. Ook trajecten als het **Project ICT-Verstoring** en **Bescherming Vitale Infrastructuur** zijn hier te noemen. Ook binnen de **eOverheid voor Bedrijven** spelen institutionele belemmeringen een rol, bijvoorbeeld als het gaat om (privacy)regels ten aanzien van de (digitale) overheidsdienstverlening. Het **Bel me niet-register** is een ander voorbeeld hiervan: voorheen was de gebruikelijke routine dat ondernemingen via telemarketing burgers konden benaderen ongeacht het gegeven of de onderneming een klantrelatie heeft met de burger.

Ten vierde kunnen falende interacties reden zijn voor overheidsingrijpen. Er kan sprake zijn van bijvoorbeeld falende interactie tussen organisaties als de telefoonnetwerken van verschillende aanbieders niet op elkaar aansluiten.[12] Of als aanbieders zelf verschillende vormen van authenticatie zouden ontwikkelen, waardoor voor de gebruiker minder duidelijk wordt welke vormen van authenticatie het meest betrouwbaar zijn. Dat is bijvoorbeeld één van de redenen geweest voor het **TTP-beleid**. Ook vormen falende interacties (gebrek aan interoperabiliteit) aanleiding voor het erkennen en herkennen van **Open Standaarden**, en voor het stimuleren van ketenoptimalisatie in het programma **SGGV**. Uitgangspunt van SGGV is dat overheidsorganisaties onvoldoende op de hoogte zijn van de gegevens die ondernemers toch al verzamelen en aanleveren. Bovendien maken falende interacties tussen overheden en bedrijven dat er onvoldoende gebruik wordt gemaakt van de mogelijkheden om anders en beter met overheidsregulering om te gaan.[13]

Ten vijfde kan sprake zijn van onvoldoende kennis en vaardigheden. Een gebrek aan technische kennis en opleiding kan een oorzaak van systeemfalen zijn waardoor innovatie niet tot stand komt of waardoor gebruik van voorzieningen achterblijft bij de mogelijkheden en verwachtingen ervan. Dit argument speelt bij **DigiVaardig & Digibewust**, waarbij is geconstateerd dat gebruikers enerzijds over onvoldoende vaardigheden beschikken om de mogelijkheden van ICT en internet ten volle te benutten (met name ouderen) of zich onvoldoende bewust zijn van de risico's die daarmee gepaard gaan. Via DigiVaardig & Digibewust worden zij voorgelicht en opgeleid. Dit argument speelde bijvoorbeeld ook bij de **Waarschuwingsdienst** (die burgers en kleinbedrijf informeert over virussen en dergelijke en hen oplossingen biedt om zich er tegen te weren) en ook bij de inspanningen van de centrale overheid in het licht van het **Noodnet**. Gebruikers van het Noodnet werden voorgelicht en werden gestimuleerd om te oefenen met het gebruik van het Noodnet.

---

[10] WRR (2000). *Borging publieke belangen*. Den Haag.

[11] Edquist, C. & Johnson , B. (1997). Institutions and organizations in systems of innovation. In C. Edquist (Eds.). *Systems of innovation-Technologies, institutions and organizations*. Pinter: London, pp. 41-63. Zie ook: Martin, S. & Scott, J.T. (2000). The nature of innovation market failure and the design of public support for private innovation, *Research Policy 29*(4-5), 437-447.

[12] Edquist & Johnson (1997). Institutions and organizations in systems of innovation. In C. Edquist (Eds.), *Systems of innovation-Technologies, institutions and organizations*. Pinter: London, pp. 41-63.

[13] Ministerie van EL&I (2008). Programmaplan SGGV, p.8-9

Tenslotte gaat het **programma M&ICT** uit van alle hiervoor genoemde vormen van systeemfalen, als mogelijke reden waarom opschaling van ICT-toepassingen in maatschappelijke sectoren niet of beperkt van de grond komt.

Uit het voorgaande blijkt dat alle ingezette instrumenten op het gebied van OD 2 en OD 3 hun legitimering vinden in een geconstateerd marktfalen dan wel systeemfalen. Daarbij past de opmerking dat de hiervoor gevolgde redenering met betrekking tot legitimiteit vooral is ingegeven door de economische rationaliteit. Tegelijkertijd speelt er ook een politiek-bestuurlijke rationaliteit die het legitiem en noodzakelijk maakt om beleid te ontwikkelen, bijvoorbeeld als Tweede Kamer en Regering speerpunten hebben benoemd die een beleidsmatige uitwerking vragen. Dat laatste is bijvoorbeeld aan de orde waar het gaat om de beleidsinspanningen die gericht zijn op het bevorderen van innovatie: het stimuleren van bedrijven om ICT in te zetten en het stimuleren dat in de met publieke middelen gefinancierde sectoren (zorg, onderwijs, et cetera) ICT wordt toegepast. Hier gaat het veelal om stimuleringsbeleid en innovatiebeleid, dat erop gericht is om bepaalde innovaties te versnellen waardoor er eerder van de voordelen kan worden geprofiteerd. Die vervroegde (ICT-)innovatie brengt dan voordelen met zich mee als snellere en goedkopere dienstverlening door bedrijven/ketens, productiviteitsgroei in sectoren en vermindering van administratieve lasten (en daarmee kostenvoordelen). Dat is goed voor de Nederlandse economie en daarmee goed voor de werkgelegenheid en de Staat.

2.2 Beoordeling van de legitimiteit van de rol van de overheid en de gekozen doelstellingen

Beleid is legitiem en noodzakelijk wanneer er sprake is van een publiek belang waarbij (wordt verwacht dat) bestaande marktprocessen, sociale processen en innovatieprocessen niet 'vanzelf' zullen leiden tot borging van dat publieke belang. Overheidsingrijpen kan derhalve worden gelegitimeerd zodra marktpartijen tekort schieten in het bereiken van (specifiek geformuleerde) maatschappelijke doelstellingen. Ook kan een politiek-bestuurlijke rationaliteit (zoals speerpunten van de Regering) de ontwikkeling van beleid legitimeren.

We constateren dat de Rijksoverheid beleid op het gebied van OD 2 en OD 3 terecht tot haar verantwoordelijkheid rekent om het probleem te helpen oplossen, omdat er sprake is van een publiek belang en omdat er sprake is van (vormen van) marktfalen en systeemfalen, waardoor dat publieke belang niet als vanzelfsprekend wordt geborgd.[14]

De beschikbaarheid en continuïteit van veilige en betrouwbare ICT- en telecommunicatievoorzieningen (OD 2) wordt beschouwd als een publiek belang, omdat steeds meer maatschappelijke processen afhankelijk zijn van ICT en telecommunicatie. Bij uitval hiervan - bijvoorbeeld door problemen als cybercriminaliteit, spam, botnets - ontstaat maatschappelijke ontwrichting. De ontwikkeling van innovatieve voorzieningen voor elektronische communicatie en de benutting ervan door de maatschappij (OD 3) wordt beschouwd als een publiek belang, omdat zowel de toepassing van ICT in (keten)samenwerking in het bedrijfsleven als de digitalisering van overheidsdienstverlening van bedrijfsprocessen leidt tot kostenreductie, kwaliteitsverbetering en vermindering van administratieve lasten. De toepassing van ICT in maatschappelijke sectoren draagt bij aan het oplossen van maatschappelijke problemen en het stimuleren van e-vaardigheden van consumenten. Tenslotte resulteert het zowel in een toename van participatiemogelijkheden en sociale cohesie als loontoename en consumptieve voordelen.

Als het gaat om de vertaling van de rol van de overheid naar de operationele doelstellingen OD 2 en OD 3, dan constateren wij dat deze logisch voortvloeien uit de geïdentificeerde vormen van markt- en systeemfalen. Met andere woorden: de doelen passen bij het probleem en beslaan de volledige reikwijdte van het probleem.

[14] WRR (2000). *Borging publieke belangen*. Den Haag. In recentere studies voegt de WRR toe dat ook systeemfalen kan leiden tot overheidsingrijpen teneinde publieke belangen te borgen. Zie: WRR (2008). *Innovatie vernieuwd: opening in viervoud*. Den Haag. Naast marktfalen en systeemfalen kan overheidsingrijpen ook worden gelegitimeerd op grond van het argument van inkomensherverdeling. Een markt kan Pareto-efficiënt zijn, maar tegelijkertijd leiden tot ongewenste inkomensongelijkheid. De overheid kan in dit geval ingrijpen middels het heffen van inkomstenbelasting.

3 DOELTREFFENDHEID EN DOELMATIGHEID: ZIJN DE JUISTE INSTRUMENTEN GEKOZEN EN ZIJN DEZE KOSTENBEWUST INGEZET?

3.1 BESCHRIJVING

3.1.1 WELKE INSTRUMENTEN ZIJN GEKOZEN?

Instrumenten OD2

In de tabel hierna is in de rechterkolom voor OD 2 aangegeven welke instrumenten door het Ministerie van EL&I zijn ingezet en aan welk deel van de doelstelling(en) de instrumenten bijdragen. Onder de tabel is per instrument een korte beschrijving van het instrument opgenomen.

OD 2: "Veilig en betrouwbaar elektronisch- en postnetwerk"	
De achterliggende gedachte van OD 2 is dat de elektronische communicatie zich ontwikkelt tot alomtegenwoordige en kritische infrastructuur zonder welke de meeste economische en maatschappelijke functies niet meer zouden functioneren. Vertrouwen in en veiligheid van elektronische communicatie en post zijn van steeds groter belang, maar ook het vermogen van de gebruikers om met de onveiligheid daarvan om te gaan.	
Sub-beleidsdoelstellingen	**Instrumenten**
Publieke belangen (veiligheid, betrouwbaarheid, toegankelijkheid en transparantie) waarborgen. *In werkplannen uitgelegd als "Continuïteit en betrouwbaarheid vitale elektronische telecommunicatienetwerken en -diensten is gewaarborgd"* i. Sector optimaal voorbereid laten zijn op verstoringen van elektronische communicatienetwerken en -diensten ii. Inzicht verkrijgen in kwetsbaarheden en afhankelijkheden van de vitale elektronische telecommunicatienetwerken en -diensten iii. Werkbare afspraken maken over respons en informatievoorziening	• NACOTEL / NCO-T (Tw H14, Buitengewone omstandigheden) • Noodnet • Project Bescherming Vitale Infrastructuur, VISTIC • Project ICT-verstoring binnen programma Nationale Veiligheid (CAET, IRB) • Internationale beleidskaders • Toezicht (OPTA en AT)
Vertrouwen in elektronische netwerkdiensten en -toepassing bevorderen. *In werkplannen uitgelegd als "Gebruik van internet is veilig en betrouwbaar"* i. Beperking economische schade en overlast door cybercrime ii. Bescherming persoonlijke levenssfeer / privacy op internet iii. Vergroten vertrouwen in ICT-gebruik bij burgers en bedrijven (door voorlichting)	• Tw H11: bescherming persoonlijke levenssfeer (TTP- en spambeleid, Bel me niet-register) • Programma NPC / NICC (ook IKC) • Waarschuwingsdienst • Platform Internetveiligheid • Voorlichtingsprogramma Surf op Safe en diens opvolger (DigiVaardig en) DigiBewust • Internationale beleidskaders • Toezicht (OPTA en AT)

Het **NCO-T (Nationaal Continuïteitsoverleg Telecommunicatie)** - looptijd vanaf 2006 - heeft tot doel maatregelen te treffen ter voorbereiding van het verzorgen van elektronisch transport van gegevens in buitengewone omstandigheden als bedoeld in artikel 14.2 van de Telecommunicatiewet.[15] Op grond van artikel 14.6 van de Telecommunicatiewet heeft de Minister telecommunicatieaanbieders aangewezen die verplicht zijn deel te nemen aan het NCO-T. Deze aanbieders moeten onder meer jaarlijks voor 1 april rapporteren over de bedoelde voorbereiding in het afgelopen kalenderjaar. **NACOTEL** (looptijd 2001-2006) was de voorloper van

[15] Voorts kan de Minister op grond van artikel 14.4 van de Telecommunicatiewet in geval van buitengewone omstandigheden (beperkte of algehele noodtoestand) bindende aanwijzingen geven aan alle aanbieders van openbare telecommunicatienetwerken, openbare telecommunicatiediensten, huurlijnen en aan gebruikers van de frequentieruimte. Die aanwijzingen van de Minister kunnen betrekking hebben op het verzorgen van telecommunicatie in buitengewone omstandigheden door alle aanbieders. Dit is ongeacht of deze aanbieders van tevoren zijn aangewezen door de Minister op grond van artikel 14.6 van de Telecommunicatiewet.

het NCO-T. Dit was een publiek-private samenwerkingsconstructie tussen telecommunicatieaanbieders en het ministerie op basis van een convenant uit 2001.

Het doel van het **Noodnet** is ervoor te zorgen dat communicatie en coördinatie kunnen blijven plaatsvinden wanneer door rampen of calamiteiten het normale telecommunicatienetwerk niet meer functioneert. Het Nationaal Noodnet (NN) vindt zijn wettelijke basis in de Tw (H14). Van oudsher rust op KPN een wettelijke verplichting om het (gesloten) Nationale Noodnet in stand te houden, zodat telecommunicatiediensten in buitengewone en crisisomstandigheden beschikbaar blijven voor partijen die een functie hebben om die omstandigheden te managen (waaronder bestuurders en hulpdiensten). De beleidsverantwoordelijkheid voor het Nationaal Noodnet is per 1 januari 2009 van het voormalige Ministerie van EZ overgedragen aan het voormalige Ministerie van BZK.

Het project **Bescherming Vitale Infrastructuur (BVI)** is in 2002 gestart en had als doel (1) een samenhangend pakket van maatregelen te ontwikkelen ter bescherming van de vitale infrastructuur, waaronder ICT en (2) deze maatregelen binnen de bedrijfsvoering van overheid en bedrijfsleven te verankeren.[16] Het ministerie van EL&I was verantwoordelijk voor de kwetsbaarheidsanalyse voor de ICT- en telecomsector en de implementatie van de daaruit voortvloeiende maatregelen. In het project VISTIC (Vitale Infrastructuur, Telecommunicatie en ICT) is daar vanaf 2003 uitvoering aan gegeven. Na 2005 zijn deze analyses gecontinueerd onder regie van het Ministerie van BZK als onderdeel van het programma Strategie Nationale Veiligheid.

In 2008 zijn binnen het Programma Nationale Veiligheid[17] dreigingsscenario's rondom het thema ICT-verstoring nader uitgewerkt: het **Project ICT-verstoring**.[18] Het doel van dit project was zicht te krijgen op mogelijke bedreigingen rondom het thema ICT-verstoring, om vervolgens te komen tot aanvullende maatregelen of afspraken om deze dreigingen te voorkomen dan wel de gevolgen ervan te beperken.

Het Nederlandse **spamverbod** is vastgelegd in artikel 11.7 van de Telecommunicatiewet.[19] Deze wetgeving is in 2004 in werking getreden en heeft als doel om spam gericht aan natuurlijke personen te voorkomen door te verbieden dat internetgebruikers zonder toestemming mogen worden benaderd via e-mail en fax. Op 1 oktober 2009 is de Telecommunicatiewet zodanig uitgebreid dat (1) spam gericht aan rechtspersonen eveneens is verboden en (2) alle organisaties die aan telefonische verkoop doen (telemarketing) verplicht zijn om het **Bel me niet-register** te raadplegen (en consumenten die staan ingeschreven niet telefonisch te benaderen tenzij er sprake is van bijvoorbeeld een bestaande klantrelatie). Via www.consuwijzer.nl kunnen consumenten hun klachten over telemarketing bij OPTA indienen.[20] OPTA is verantwoordelijk voor het toezicht op het spamverbod en houdt actief toezicht op de naleving van regels inzake telemarketing en kan onder meer boetes en lasten onder dwangsom opleggen.

Het doel van het **TTP-beleid**, dat eind jaren '90 is ontwikkeld, was een betrouwbaar systeem voor elektronische handtekeningen te ontwikkelen, met als doel om elektronische handel te bevorderen.[21] Een goed ontwikkelde openbare Nederlandse infrastructuur van Trusted Third Parties (TTP's) werd daarbij als voorwaarde gezien. OPTA is belast met het toezicht op de certificatiedienstverleners die in Nederland gekwalificeerde certificaten

[16] Het voormalige Ministerie van BZK verzorgde de rijksbrede interdepartementale coördinatie, monitoring en toetsing.

[17] Het Programma Nationale Veiligheid (PNV) is een rijksbreed programma, dat een nieuwe werkwijze introduceert om dreigingen van de nationale veiligheid te kunnen bepalen en hierop te kunnen anticiperen.[17] Het programma is gebaseerd op de in april 2007 door het kabinet goedgekeurde Strategie Nationale Veiligheid.[17] De dreigingen worden in een Nationale Risicobeoordeling (NRB) beoordeeld. Zie: Tweede Kamer, vergaderjaar 2006-2007, 30821, nr 3.

[18] In 2007 zijn reeds de dreigingsscenario's betreffende energieuitval, grieppandemie en overstroming nader uitgewerkt.

[19] Eerste lid tot en met het vierde lid.

[20] Zie: www.opta.nl.

[21] Tweede Kamer, vergaderjaar 2004-2005, 26 581, nr. 3.

aan bedrijven aanbieden of afgeven. Deze dienstverleners moeten aan de Wet elektronische handtekeningen en de bijbehorende regelgeving voldoen.

Het programma **NICC** (Nationale Infrastructuur tegen Cybercrime) heeft als doel betrokken partijen vertrouwelijke informatie te laten delen over cybercrime en ICT-security ten einde de weerbaarheid van deze betrokken partijen te versterken en uitval te voorkomen.[22] Het Informatieknooppunt (**IKC**) maakt deel uit van het NICC. In het Informatieknooppunt overlegt een selecte groep overheidsdiensten (AIVD, KLPD en Govcert) met partijen uit vitale sectoren over de risico's van cybercrime en het nemen van maatregelen daartegen. Het programma kwam in 2006 tot stand vanuit de behoefte aan een integrale aanpak van enerzijds de versterking van de bestrijding van ICT-criminaliteit door de National Hightech Crime Center (NHTCC) en anderzijds de informatie-uitwisseling, samenwerking en coördinatie tussen publieke en private partijen in het NPC-project Aanpak Cybercrime, NPAC.[23]

De **Waarschuwingsdienst** is een voor gebruikers gratis en onafhankelijke overheidsdienst die sinds 2003 bestaat en als doel heeft burgers en kleinbedrijf te attenderen op dreigingen ten aanzien van de ICT-veiligheid. Deze Waarschuwingsdienst is ondergebracht bij de organisatie Govcert. Die dienst is gelanceerd als een website met als doel om 1) waarschuwingen te geven ten aanzien van computervirussen, wormen en beveiligingslekken in software, en 2) achtergrondinformatie te geven in de vorm van voorlichting en adviezen over computerbeveiliging. In urgente gevallen waarschuwt de dienst burgers en kleinbedrijf tevens via sms en mail.[24]

Het **Platform Internetveiligheid** is eind 2009 van start gegaan en heeft als doel om een structurele bijdrage te leveren aan het verbeteren van de internetveiligheid voor de internetgebruiker. Dat vergt samenwerking door de gehele (internet-)keten, bestaande uit onder andere ISP's, softwareleveranciers, bedrijven en overheid.[25] Het platform streeft naar efficiency in de bestaande overlegstructuren en heeft als doel om maatschappelijke trends te signaleren en te vertalen naar concrete initiatieven die in werkgroepen worden uitgewerkt.[26]

Via verschillende **internationale overlegorganen** wordt door het ministerie van EL&I via ambtelijke vertegenwoordiging samengewerkt op het terrein van netwerk- en informatiebeveiliging en internetveiligheid. Een drietal belangrijke fora zijn: de Europese Unie, de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) en de VN.

Instrumenten OD3

In de tabel hierna is in de rechterkolom voor OD 3 aangegeven welke instrumenten door het Ministerie van EL&I zijn ingezet en aan welk deel van de doelstelling(en) de instrumenten bijdragen. Onder de tabel is - net als bij OD 2 - per instrument een korte beschrijving van het instrument opgenomen.

OD 3: "ontwikkeling van innovatieve voorzieningen, digitalisering van omroeptoepassingen, faciliteren van producten en diensten voor elektronische communicatie en benutting ervan door de consument, het bedrijfsleven en de (semi-) publieke sector"	
De gedachte achter OD 3 is dat met ICT meer economisch en maatschappelijk rendement kan worden behaald en dat de overheid, waar nodig, het gebruik van ICT faciliteert of stimuleert.	
Sub-beleidsdoelstellingen	**Instrumenten**
1. Bevorderen dat bedrijven ICT inzetten waardoor productiviteit en	• Programma Nederland Digitaal in Verbinding

[22] PWC (2009). Evaluatierapport Informatieknooppunt Cybercrime.
[23] Tweede Kamer, vergaderjaar 2005-2006, 26 671, nr. 24.
[24] http://www.logius.nl.
[25] Terms of Reference Platform Internetveiligheid, 2009.
[26] Terms of Reference Platform Internetveiligheid, 2009.

efficiëntie toenemen	
2. ICT toepassen in de overheidsdienstverlening aan bedrijven waardoor de dienstverlening van de overheid verbetert en er verlaging van administratieve lasten plaatsvindt	• eOverheid voor bedrijven • Programma Nederland Open in Verbinding • Bijdrage aan College en Forum Standaardisatie • Programma Slim Geregeld Goed Verbonden
3. Stimuleren dat in met publieke middelen gefinancierde sectoren ICT wordt toegepast waardoor maatschappelijke problemen worden opgelost	• Programma breedband (waaronder Kenniswijk) • Actieprogramma Maatschappelijke Sectoren en ICT
4. Ervoor zorgen dat burgers actief kunnen deelnemen aan de informatiemaatschappij en daarvoor een goede toegang hebben tot infrastructuren en een divers dienstenaanbod	• Programma Digivaardig & Digibewust
5. Algemeen	• Programma Implementatie ICT-agenda (PRIMA) • ECP-EPN

NDiV (Nederland Digitaal in Verbinding): Het Ministerie van EL&I stelde zich met het programma NDiV (looptijd 2007-2010) ten doel om de ketendigitalisering in het MKB te bevorderen, om zo Nederland in de Europese top te krijgen en te houden voor wat betreft het gebruik van ICT door het MKB. Voor NDiV werd een programmatische aanpak gekozen met meerdere uitvoerders onder regie van een programmabureau dat was belegd bij SenterNovem. De uitvoerders van het programma waren Syntens, Media Plaza en Nederland Breedband Land (NBL).

Het College en Forum Standaardisatie (sinds 2006) hebben als doel om interoperabiliteit tussen overheden onderling en tussen overheid, bedrijven en burgers te bevorderen door het gebruik van open standaarden. O.a. door de ontwikkeling van een lijst met open standaarden waarop een pas-toe-of-leg-uit-regime van toepassing is.

Het **NOiV (Nederland Open in Verbinding)** - gestart vanaf 2008 - ondersteunt overheidsorganisaties bij het gebruik en de implementatie van open standaarden en open source software (OS/OSS). Voor wat betreft het gebruik van OS beoogt het actieplan om de voorwaarden te scheppen die bijdragen aan inbedding van OS in overheidsorganisaties zodat het 'business as usual' wordt. Met andere woorden: organisaties kiezen voor open standaarden tenzij er specifieke redenen zijn waarom dat niet mogelijk is ('ja, mits...'). Voor OSS geldt dat het doel is om OSS een eerlijke kans te geven in aanbestedingen. Daarmee wordt bedoeld dat OSS als optie worden meegenomen bij de aanschaf van nieuwe software en bij gelijke geschiktheid met software onder licentie de voorkeur krijgt.

Het **programma SGGV (Slim Geregeld, Goed Verbonden)** - gestart in 2009 - heeft als doel om informatieketens tussen overheden en bedrijven te optimaliseren met behulp van proces- en gegevensstandaardisatie en ondersteund door ICT. SGGV beoogt hiermee een substantiële bijdrage te leveren aan de vermindering van de regeldruk voor bedrijven en de hiermee samenhangende verbetering van de uitvoering door de overheid.[27] In het Programmaplan wordt een indicatieve schatting gegeven van een regeldrukvermindering van 10% tot 35% bij betrokken bedrijven.[28]

eOverheid voor bedrijven (2006-2009) is een bundeling van projecten ter verbetering van de elektronische overheidsdienstverlening aan bedrijven, met als gezamenlijk doel om het voor bedrijven zo gemakkelijk mogelijk te maken om zaken te doen met de overheid. Belangrijke projecten die binnen eOverheid voor bedrijven zijn uitgevoerd, zijn: Antwoord voor Bedrijven, eHerkenning voor Bedrijven en eFormulieren.

[27] Dit is de doelstelling conform het Programmaplan SGGV (2008), p.4

[28] Ministerie van EL&I (2008) Programmaplan SGGV, p.24-25. Overigens wordt bij deze doelstelling geen termijn genoemd.

Het Actieprogramma Breedband (2004-2008) is een verzameling van 14 beleidsacties met als doel om bij te dragen aan het realiseren van Nederland Breedbandland. De ambitie is Nederland tot de internationale top van ICT-gebaseerde kenniseconomieën te late behoren.[29]

Het Actieprogramma M&ICT (Maatschappelijke sectoren & ICT) heeft als doel opschaling van ICT-toepassingen te stimuleren in maatschappelijke sectoren, door belemmeringen als gevolg van systeemfalen[30] weg te nemen. Het programma loopt sinds 2005 en is formeel beëindigd per 1 januari 2010. Op dat moment waren 25 van de 63 projecten afgerond. Door een maximale projectduur van 2,5 jaar, duurt het tot en met 2012 voordat alle projecten zijn afgerond. M&ICT is een programma van de ministeries van EL&I, BZK, Justitie en Veiligheid, OCW, VWS en I&M. De sectoren waar M&ICT zich op richt zijn mobiliteit, onderwijs, veiligheid, energie en zorg.

Digivaardig & Digibewust heeft als doel om het aantal Nederlandse digibeten sterk terug te dringen, de digivaardigheden van de Nederlandse bevolking verder te versterken en de benutting van ICT-mogelijkheden te bevorderen. Daarnaast wil het programma bewustwording creëren ten aanzien van de mogelijke risico's die samenhangen met het gebruik van internet en verstandige manieren aanreiken over hoe met deze risico's om te gaan. Tot de specifieke doelgroepen van het programma Digivaardig & Digibewust behoren digibeten, jongeren en opvoeders, senioren, overheidsprofessionals en het MKB.

Bijdrage ECP-EPN aan doelbereik OD3. ECP-EPN is een onafhankelijk platform waar overheden, bedrijfsleven en maatschappelijke organisaties samenwerken en kennis uitwisselen met het oog op de toepassing van informatie- en communicatietechnologie in de Nederlandse samenleving. Verder draagt ECP-EPN bij aan het creëren van maatschappelijk draagvlak door stakeholders te organiseren en terugkoppeling te vragen. ECP-EPN doet dit door een neutraal platform te bieden voor debat met alle maatschappelijke actoren en door in gezamenlijkheid met uiteenlopende stakeholders (overheid, gebruikers, leveranciers, belangenorganisaties) concurrentieoverstijgende projecten te faciliteren. Een dergelijk platform kan niet door de markt of de overheid alleen worden geboden. Daarom hebben overheid en markt besloten tot deze publiek-private samenwerking.[31]

Programma Implementatie ICT-Agenda (PRIMA). Met het Programma Implementatie ICT-agenda (PRIMA) stelt het Kabinet jaarlijks € 20 mln. beschikbaar voor de realisatie van de prioriteiten uit de (interdepartementale) ICT-agenda.[32] Het Ministerie van EL&I coördineert het programma. Naast de prioriteiten uit de ICT-agenda voor de periode 2008-2011 komen in tweede instantie ook projecten voor een PRIMA-bijdrage in aanmerking die betrekking hebben op één of meer aspecten van de ICT-basis.[33] Voorstellen voor projecten kunnen uitsluitend door departementen worden ingediend.

3.1.2 Welke middelen zijn ingezet?

Als het gaat om de middelen die door het Ministerie van EL&I zijn ingezet, kan onderscheid worden gemaakt tussen de inzet de mensen (fte's) en de inzet van financiële middelen.

---

[29] Daarmee bouwde het voort op eerder beleid dat primair tot doel had de vaste en draadloze infrastructuur te ontwikkelen (1998-2003), in: PWC (2010). *De draad opgepakt*, p. 9.

[30] TNO (2010), *Opschaling van maatschappelijk relevante ICT-toepassingen. Lessen uit de praktijk.*), van Lieshout, Kool, Huveneers, Poel, Delft: Vormen van systeemfalen: onvoldoende zicht op samenwerkingsvormen, onevenwichtige verdeling kosten en baten, onvoldoende bestuurlijke regie, onvoldoende transparantie, onvoldoende vraagmacht, randvoorwaarden onvoldoende op orde.

[31] ECP-EPN (2010). Van beschikbaarheid naar toepassing, p. 21.

[32] Dit was voorheen het Nationaal Actieprogramma Elektronische Snelwegen (NAP).

[33] Zie voor de prioriteiten en de onderdelen van de ICT-basis: Beschrijving gevoerde beleid OD3.

Fte's

Op basis van de werkplannen is het aantal fte's in kaart gebracht dat specifiek is ingezet ten behoeve van OD 2 en OD 3. Voor wat betreft OD 2 kan worden gesteld dat er gemiddeld ongeveer 10 fte is ingezet. Daarbij past de relativering dat de inzet in de laatste jaren van de te evalueren periode (2008-2010) relatief minder groot was: gemiddeld ongeveer 8 fte. Voor wat betreft OD 3 zijn er jaarlijks gemiddeld ongeveer 24 fte ingezet.

Financiële middelen

Hierna worden de financiële middelen weergegeven die per instrument zijn ingezet ten behoeve van OD 2 dan wel OD 3.

De instrumenten met betrekking tot OD 2 en OD 3 zijn in één overzicht opgenomen, omdat sommige instrumenten in de praktijk aan beide doelen bijdragen. Zo draagt DigiVaardig en DigiBewust bij aan zowel OD 2 als OD 3, terwijl dit programma in het overzicht is opgenomen als onderdeel van OD 3. Verder geldt voor (bijna) alle projecten onder OD 2 dat ze ook in enige mate bijdragen aan OD 3. Immers, veilig gebruik van internet (onderdeel van OD 2) leidt in algemene zin tot meer gebruik van ICT door bedrijven, burgers, overheid en maatschappelijke sectoren.

Tabel: Ingezette budgetten per instrument. De cijfers zijn aangeleverd door het Ministerie van EL&I.

Instrument in € mln.	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**
Cybercrime: Programma NICC	-	-	-	1,4	1,5	1,6	0,9	1,8[34]
Onderzoeken, in het licht van onder meer NACOTEL/NCO-T, Project ICT-verstoring (CAET/IRB), Platform Internetveiligheid en VISTIC	0,2	0,2	0,4	0,3	0,2	0,2	0,4	0,4
Programma Nederland Digitaal in Verbinding	n.v.t	-	-	-	1,0	1,3	2,0	1,2
eOverheid voor bedrijven	n.v.t	-	6,2	3,9	4,6	7,0	17,4	3,7
Programma Nederland Open in Verbinding	n.v.t	-	-	-	-	1,6	3,3	2,7
Bijdrage aan College en Forum Standaardisatie	n.v.t			2,2	2,2	2,2	2,2	2,2
Programma Slim Geregeld Goed Verbonden	n.v.t	-	-	-	2,5	2,3	3,8	5,8
Kenniswijk	n.v.t	4,1	11,2	6,2	2,6	0,4	-	-
Actieprogramma Maatschappelijke Sectoren en ICT	n.v.t	-	7,5	7,5	7,5	7,5	7,5	-
Programma Digivaardig & Digibewust	n.v.t	-	-	-	-	-	1,5	2,0

[34] Dit verplichte bedrag leidt tot betalingen in 2011 en 2012.

Uitvoering geven aan de ICT-Agenda	n.v.t	-	-	-	-	-	-	-
Programma Implementatie ICT-Agenda (PRIMA)[35]	n.v.t	15,0	11,5	24,5	26,6	15,1	24,7	17,4
Jaarprogramma ECP-EPN	n.v.t	0,3	0,4	0,6	0,5	0,5	0,6	0,6
Totaal	**0,2**	**19,6**	**37,2**	**46,6**	**49,2**	**39,7**	**64,3**	**37,8**

Bij deze tabel hoort een aantal kanttekeningen.

- Ten eerste: In deze tabel zijn middelen weergegeven die eenduidig zijn toegerekend aan de onderzochte instrumenten. Dat neemt niet weg dat er ook middelen zijn ingezet op beleidsinitiatieven die weliswaar raken aan deze instrumenten dan wel OD's, maar er niet aan zijn toegerekend.

- Ten tweede: De evaluatie van het OD 3-beleid betreft de periode vanaf 2004. Daarom is in de kolom 2003 telkens 'n.v.t.' vermeld waar het gaat om de ingezette budgetten voor de instrumenten die OD 3 betreffen.

3.2 Beoordeling doeltreffendheid en doelmatigheid

3.2.1 Doeltreffendheid: Zijn de juiste instrumenten gekozen (is de instrumentkeuze plausibel)?

Conclusie:

De instrumenten zijn goed gekozen en afgewogen.

Het gekozen instrumentenpalet is compleet en heeft zich gericht op zowel aanbieders (van telecommunicatie, internet en ICT-voorzieningen) als op gebruikers. Er worden geen instrumenten gemist.

Er is een goede instrumentenmix gekozen van faciliteren en aanjagen, van voorlichting geven, van financieel stimuleren en van wettelijke verplichtingen opleggen en handhaven. De instrumenten versterken elkaar.

De primaire verantwoordelijkheid is - waar dat kon en opportuun was - bij aanbieders en gebruikers neergelegd. Zelfregulering heeft een reële kans gekregen alvorens andere meer verplichtende instrumenten zijn ingezet.

Hier staat de vraag centraal of de instrumenten goed zijn gekozen in relatie tot het op te lossen probleem en de geformuleerde doelstellingen. Hierna wordt de hiervoor weergegeven conclusie onderbouwd, waarbij wordt ingegaan op OD 2 (enerzijds het borgen van de continuïteit en betrouwbaarheid van de telecommunicatie en anderzijds het borgen van de veiligheid en betrouwbaarheid van het internet) en OD 3 (de ontwikkeling van innovatieve voorzieningen, faciliteren van producten en diensten voor elektronische communicatie en benutting ervan door de consument, het bedrijfsleven en de (semi-) publieke sector

Instrument en rol overheid zorgvuldig gekozen

Ten eerste is de instrumentkeuze en de rol van de overheid zorgvuldig gekozen in het licht van het samenspel met de rollen van anderen. De primaire verantwoordelijkheid is - waar dat mogelijk was - gelegd bij aanbieders en gebruikers. Hen is de ruimte gegeven om via zelfregulering met oplossingen te komen, alvorens is gekozen voor dwingender instrumentarium (zoals wetgeving).

Bij OD 2 is bijvoorbeeld aan enerzijds aanbieders van internet en telecommunicatie en anderzijds de gebruikers daarvan (waaronder grote bedrijven, MKB-ers en individuele consumenten) de ruimte gegeven om zelf met

[35] In 2004 tot en met 2007 hebben de middelen betrekking op het programma Nationaal Actieplan Elektronische Snelwegen, de voorloper van PRIMA.

oplossingen te komen. Dat is bijvoorbeeld het geval bij de aanpak van internetveiligheid (via het Platform Internetveiligheid), bij het borgen van de continuïteit en beschikbaarheid van de telecommunicatie (via het PPS-verband NACOTEL, de voorloper van het verplichte NCO-T), bij het aanpakken van spam en bij het opzetten van het Bel me niet-register (aanvankelijk via Infofilter).

Ook bij OD 3 kan worden geconstateerd dat het Ministerie van EL&I aanbieders van ICT(-toepassingen) en de gebruikers daarvan (overheidsorganisaties, MKB-ers en burgers) aanspreekt op hun verantwoordelijkheid en een duidelijke rol voor hen laat bij het oplossen van problemen. Zo wordt uitgegaan van de autonomie van (decentrale) overheidsorganisaties bij de bevordering van digitalisering van overheidsdienstverlening. Daarnaast stimuleert het ministerie van EL&I ketensamenwerking onder MKB-ers (met advies, voorlichting en communicatie) zonder deze samenwerking zelf te organiseren. Hiervoor blijven MKB-ers zelf verantwoordelijk. Ook met ECP-EPN - en de publiek-private samenwerking die daarbij is gekozen - laat de overheid zien geen verantwoordelijkheden van marktpartijen of overheidsorganisaties over te nemen, maar een platform te bieden waar partijen zelf met ideeën kunnen komen. Tenslotte hanteren ook het College en Forum Standaardisatie een werkwijze waarbij standaarden niet zomaar worden aangewezen of opgelegd, maar in een open proces met stakeholders worden geïdentificeerd en erkend.

Gebalanceerde instrumentenmix

Ten tweede heeft het Ministerie gekozen voor een gebalanceerde instrumentenmix. Een instrumentenmix die zich zowel richt op de aanbieders als op de gebruikers, en die aansluit bij de ontwikkelingen die sectoren doormaken, maar ook aansluit bij wat eerder uitgevoerd beleid al wel en nog niet heeft bereikt. Daarbij is telkens gekozen voor een combinatie van instrumenten die elkaar onderling versterken: op onderdelen is gefaciliteerd en aangejaagd, op onderdelen is voorlichting gegeven, op onderdelen is financieel gestimuleerd en op onderdelen zijn wettelijke verplichtingen opgelegd die worden gehandhaafd (door onder meer OPTA).

- Zo zijn in het licht van de *borging van de betrouwbaarheid en continuïteit van de telecommunicatie* (als onderdeel van OD 2) door de Minister *telecommunicatieaanbieders* aangewezen die verplicht zijn deel te nemen in het NCO-T en ook verplicht zijn jaarlijks aan de Minister te rapporteren over hun continuïteitsplanning en crisismanagement. In het NCO-T treffen de aanbieders voorbereidingen om uitval van telecommunicatie te voorkomen. Voorts heeft het Ministerie van EL&I een faciliterende rol gekozen in projecten als Bescherming Vitale Infrastructuur en het Project ICT-Verstoring. Daarin is via risicoanalyses en scenarioanalyses de afhankelijkheid van de telecommunicatievoorziening van andere vitale producten en diensten onderzocht.
  Richting gebruikers van telecommunicatie is gekozen voor enerzijds het creëren van bewustwording ten aanzien van hun afhankelijkheid van telecommunicatie en anderzijds het geven van voorlichting en handreikingen voor het treffen van aanvullende maatregelen. Bewustwording van vitale gebruikers is gecreëerd via onder meer de analyses in de projecten Bescherming Vitale Infrastructuur en het Project ICT-Verstoring.
  Voorts is hier relevant op te merken dat het Ministerie van EL&I met haar instrumentenmix niet alleen heeft gekozen voor borging van de openbare telecommunicatie, maar ook voor borging van de noodcommunicatie (voor het geval de openbare telecommunicatie is uitgevallen). Immers, op één van de aanbieders - KPN - rustte gedurende de evaluatieperiode een wettelijke verplichting tot het in stand houden van een Noodnet voor noodcommunicatie door onder meer bestuurlijke partijen, hulpdiensten en vitale bedrijven. Als het reguliere telecommunicatienetwerk uitvalt, dan kan via het noodnet door de aangesloten partijen nog worden gecommuniceerd. Door de breedte van de aanpak wordt de continuïteit vanuit verschillende invalshoeken geborgd.

- In het licht van de *borging van de veiligheid en betrouwbaarheid van het gebruik van internet* (als onderdeel van OD 2) heeft het Ministerie van EL&I richting internetaanbieders gekozen voor faciliteren, voor financieel stimuleren en voor het opleggen van wettelijke verplichtingen (waar

zelfregulering niet tot stand kwam) die worden gehandhaafd door OPTA. Zo is gekozen voor het geven van financiële ondersteuning aan het NICC dat via zogenaamde informatieknooppunten kennisuitwisseling tussen aanbieders en andere instanties (zoals politie, AIVD, Justitie) faciliteerde ten einde cybercrime te bestrijden. In het Platform Internetveiligheid - dat door het ministerie van EL&I wordt gefaciliteerd - werken overheid en marktpartijen samen om op niet-verplichte basis internetveiligheidsvraagstukken op te lossen. Voorts is er gekozen voor het opstellen van wetgeving: het spamverbod, het TTP-beleid en de verplichting om het Bel me niet-register te raadplegen. Deze wetgeving wordt gehandhaafd door OPTA, die op dat vlak ook boetes en waarschuwingen heeft gegeven.
Richting gebruikers van internet is vooral gekozen voor het geven van voorlichting. Via programma's als Digivaardig & Digibewust en via de Waarschuwingsdienst zijn met name consumenten en MKB-ers bewust gemaakt van de risico's van het gebruik van het internet en hebben ze handreikingen gekregen voor de bescherming tegen die risico's.
Ook hier geldt dat de verschillende gekozen rollen en instrumenten elkaar versterken. Door te kiezen voor de verschillende rollen en perspectieven om het probleem op te lossen, wordt de volle breedte van het instrumentarium benut.

- In het licht van het gebruik van ICT (OD 3) is ten eerste te zien dat de instrumentkeuze van de overheid een duidelijke fasering kent, die afhankelijk is geweest van de ontwikkeling van het probleem en de mate waarin het probleem met eerder beleid al dan niet is opgelost. De beleidsontwikkeling en de rolkeuze hebben zich aangepast aan de fase waarin Nederland zich bevindt bij het invoeren en benutten van ICT. In de eerste fase (circa 1998 – 2002) hadden de beleidsinstrumenten voornamelijk als doel om kaders te stellen voor een snelle introductie en uitrol van vaste en draadloze infrastructuur en van computers. Het Actieprogramma Breedband is hier een voorbeeld van. Daarnaast is ingezet op het bevorderen van een goede marktwerking. Dit beleid heeft er mede toe bijgedragen dat Nederland internationaal tot de voorhoede behoort voor wat betreft computerbezit en internetaansluitingen. Vervolgens is in de periode tussen circa 2003 en 2008 de aandacht verschoven richting instrumenten die het gebruik van ICT bevorderen, door het stimuleren van het gebruik van diensten en toepassingen. Hiertoe werden bijvoorbeeld subsidies verleend voor projecten gericht op het gebruik van ICT in de zorg of in het onderwijs, werd elektronische dienstverlening door de overheid op gang gebracht en werd voorlichting gegeven over veilig gebruik van internet. Het programma M&ICT, eOverheid voor bedrijven en Digivaardig & Digibewust zijn hier voorbeelden van. De meest recent opgestarte instrumenten laten zien dat het beleid inmiddels vooral gericht is op het faciliteren van 'verbindingen'. ICT geeft de mogelijkheid ketens, netwerken, maar ook toepassingen en diensten met elkaar te verbinden en daaruit (maatschappelijke) winst te halen. Het ministerie van EL&I faciliteert deze totstandkoming van verbindingen met programma's als SGGV en NDiV.

  Verder constateren wij dat er sprake is van samenhang tussen de verschillende parallel uitgevoerde beleidsinstrumenten binnen OD3. Hierdoor versterken de instrumenten elkaar. Dit laat zich bijvoorbeeld illustreren aan de hand van de projecten en programma's waarin aan standaarden en de toepassing ervan wordt gewerkt. Zo wordt via het College en Forum Standaardisatie gewerkt aan het herkennen en erkennen van maatschappelijk relevante open standaarden. In het programma NOiV wordt vervolgens ondersteuning geboden bij het gebruik van open standaarden aan overheden. In diverse andere programma's (eOverheid voor bedrijven, SGGV, M&ICT) wordt het gebruik van standaarden als voorwaarde gesteld. Daarmee versterken de instrumenten elkaar. Tenslotte is synergie gezocht en geborgd doordat sommige projecten vanwege hun samenhang zijn gecombineerd. Dat geldt bijvoorbeeld voor het samengaan van Digibewust en eVaardigheden in Digivaardig & Digibewust. Ook is er samenhang aangebracht door de uitvoering (of ondersteuning) van - weliswaar verschillende - programma's te clusteren door ze onder te brengen bij een beperkt aantal

'uitvoeringsorganisaties' waaronder ECP-EPN. In 2009 zijn verschillende overlegplatforms samengegaan in ECP-EPN. Bovendien participeert ECP-EPN op haar beurt weer in andere platforms (bijvoorbeeld het Platform Internetveiligheid en het Expertisecentrum Mediawijsheid). Dat zorgt voor samenhang.

3.2.2 *Doelmatigheid: Zijn de instrumenten kostenbewust ingezet?*

Conclusie:

De instrumenten zijn kostenbewust ingezet. Er zijn voorzieningen getroffen die waarborgen dat beschikbare budgetten doelmatig zijn toegewezen aan de verschillende instrumenten. Daarnaast zijn voorzieningen getroffen die waarborgen dat de toegewezen budgetten doelmatig zijn besteed.

Doelmatigheid heeft betrekking op de verhouding tussen de input (gedane investeringen) en de daaruit voortvloeiende resultaten en effecten. Ondanks dat de input relatief inzichtelijk is, constateren we dat het buitengewoon lastig is om uitspraken te doen over de doelmatigheid. Daar is een aantal redenen voor te geven.

- Ten eerste zijn de resultaten en met name de effecten van het beleid op (te) veel fronten onbekend. Dat maakt dat het bepalen van de verhouding tussen enerzijds input en anderzijds de daaruit voortvloeiende resultaten en effecten niet exact mogelijk is.
- Ten tweede is in veel gevallen het Ministerie van EL&I slechts één van de partijen die financiert, naast andere partijen. Dat betekent dat de vraag naar doelmatigheid ook moet worden bezien in het licht van de bijdragen van anderen.
- Ten derde hebben veel van de ingezette middelen als doel om ontwikkelingen die in de maatschappij plaatsvinden te versnellen. Daarbij is het ingewikkeld om te bepalen welk deel van het effect autonoom al zou zijn opgetreden zonder overheidsinterventie, en wat de aanvullende versnelling is die op het conto van het overheidsbeleid te schrijven is.
- Ten vierde zit er een tijdsverschil tussen enerzijds het moment van de beleidsinspanning en de financiering ervan en anderzijds het optreden van effecten als gevolg van die beleidsinspanning en financiering. Dat maakt de toerekening van effecten aan de ingezette middelen buitengewoon lastig.
- Tot slot is relevant te constateren dat sommige beleidsinstrumenten financieel georiënteerd zijn en dus (veel) inzet van financiële middelen vergen (een subsidie, een stimuleringsregeling), terwijl andere beleidsinstrumenten dat niet of veel minder vergen (zoals wetgeving). Die instrumenten kunnen in een beschouwing over doelmatigheid niet zomaar met elkaar worden vergeleken op grond van hun verhouding tussen ingezette middelen en resultaten.

De doelmatigheid van het beleid als het gaat om OD 2 en OD 3 is dus in deze beleidsdoorlichting niet in kaart te brengen op basis van de verhouding tussen enerzijds de input en anderzijds de resultaten en effecten. Daarom is als alternatief hiervoor een analyse gemaakt van de kostenbewuste inzet van de instrumenten. Daarbij is onderzoek gedaan naar de voorzieningen die door het ministerie van EL&I worden gehanteerd om middelen doelmatig toe te wijzen aan instrumenten en om middelen vervolgens doelmatig te besteden.

Voorzieningen voor doelmatige toewijzing van middelen

Er zijn verschillende voorzieningen die bijdragen aan kostenbeheersing (zodanig dat binnen het budgettair kader wordt gebleven) en aan het doelmatig verdelen van de middelen over projecten. Zo wordt bijvoorbeeld bij de toewijzing van middelen aan projectvoorstellen bezien of projecten kunnen worden gecombineerd, of projecten in omvang kunnen worden beperkt, of er wellicht alternatieve aanpakken voor handen zijn, of de markt meer kan worden ingeschakeld en of (alsnog) cofinanciers kunnen worden gevonden. Dat de meerjarenreeks voor OD 3 afnemend is als gevolg van de taakstelling (en er ook nog een nieuwe taakstelling

aankomt) vormt een extra aanleiding om goed te sturen op beheersing van de kosten. Op deze wijze wordt gestuurd op kostenreductie en optimalisering van beleidseffecten binnen de bestaande budgetten.

Voorzieningen voor doelmatige besteding

Hier wordt een toelichting gegeven op de getroffen voorzieningen die een doelmatige *besteding* van de middelen borgen.

Doelmatige besteding wordt bevorderd door afwijkingen van de begroting altijd onderwerp van gesprek te maken. Zo worden afwijkingen besproken in het MT van de betrokken directies en wordt bijgestuurd op basis van doeltreffendheid en de doelmatigheid.[36] Voor de niet-bestede middelen geldt dat opnieuw wordt afgewogen hoe deze middelen in het daarop volgende jaar worden ingezet. De middelen moeten via de werkplannen opnieuw worden aangevraagd en er ontstaat opnieuw een afweging waarbij doelmatigheid wordt gewogen.

Doelmatige besteding wordt ook bevorderd door een duidelijke verantwoordingssystematiek te hanteren. Allereerst zijn er verantwoordingsmomenten die zijn gekoppeld aan de begrotingscyclus van de rijksoverheid. Ten tweede zijn er verantwoordingsmomenten binnen de instrumenten, bijvoorbeeld maand- of kwartaalrapportages. Zo wordt in het programma eOverheid een monitor uitgevoerd en maakt het programma NOiV gebruik van monitoringsrapportages. Een derde te noemen voorziening betreft de governance rondom projecten en programma's, waarin wordt gestuurd op doeltreffendheid en doelmatigheid. Hier wordt gedoeld op een structuur met stuurgroepen of klankbordgroepen die een rol spelen bij het selecteren en prioriteren (van deelprojecten) en bij het sturen op de inzet van middelen en op de samenhang. Partijen zoals VNO-NCW, ICT-Office en het CIO-platform vervullen rollen in dergelijke stuurgroepen of klankbordgroepen van één of meer projecten of programma's.

Doelmatigheid van de bestedingen wordt daarnaast bevorderd doordat bij aanvang van projecten een zorgvuldige selectie en prioritering van cases plaatsvindt. Zo zijn de cases in het programma SGGV op basis van de adviezen van de Commissie Wientjes zorgvuldig geselecteerd en geprioriteerd. Bovendien is hierbij expliciet om het commitment - in de vorm van een handtekening - van de ketenpartners gevraagd alvorens de projectwerkzaamheden in gang te zetten.

Doelmatigheid van de bestedingen wordt voorts bevorderd doordat projecten tijdig worden stopgezet als blijkt dat de resultaten tegenvallen en de verwachtingen over toekomstige resultaten onvoldoende bemoedigend zijn. Een voorbeeld van een voorziening om te voorkomen dat projecten onnodig lang voortduren, is het hebben van een go-/no-go-procedure zoals die wordt toegepast in het programma SGGV. De mogelijkheid om projecten voortijdig te stoppen en ervan te leren is met name bij OD 3 van cruciaal belang omdat het gaat om het vormgeven van complexe, innovatieve oplossingen die zich niet gemakkelijk vanaf de tekentafel laten schetsen. In dat kader is ook het project eFormulieren een voorbeeld van een project dat tussentijds is beëindigd: gemeenten maakten er in de praktijk onvoldoende gebruik van. Na de stopzetting is ervoor gekozen om standaarden af te spreken via het College Standaardisatie.[37] Van dit project is geleerd dat alleen nog initiatieven worden ontwikkeld als er ook *launching customers* zijn. Dat is bijvoorbeeld het geval bij het meer

[36] Er is een zekere flexibiliteit in de begroting omdat aanspraak kan worden gemaakt op middelen uit de post 'Algemene beleidsuitgaven'. Voor OD 2, waarvoor in de Rijksbegroting geen specifieke middelen zijn gereserveerd onder de noemer OD 2, is daar bijvoorbeeld voor gekozen. Daarnaast is er flexibiliteit omdat - zonder afstemming met het Ministerie van Financiën - tot een bepaald percentage binnen de begroting mag worden geschoven, de zogenaamde eindejaarsmarge. Voorts heeft het Ministerie van EL&I de ruimte om binnen een begrotingsartikel 1 procent van het begrotingstotaal van het ene naar het andere jaar te schuiven. Via deze voorzieningen kan ten behoeve van een doelmatige besteding worden bijgestuurd.

[37] Overigens kan op grond van de beschikbare informatie geen uitspraak worden gedaan over de tijdigheid van het stopzetten.

recente project eHerkenning waarbij al in vroegtijdig stadium duidelijk was dat de Belastingdienst en Agenstchap NL –als launching customer- van eHerkenning gebruik zouden gaan maken.

Doelmatigheid van de bestedingen wordt tot slot bevorderd doordat de uitvoering bij partijen wordt belegd die op grond van hun belang, kennis en ervaring zorg kunnen dragen voor de meest doeltreffende en doelmatige uitvoering. Daar wordt ten eerste invulling aan gegeven, bijvoorbeeld door prijsvragen op een specifiek thema uit te schrijven (M&ICT). Daar wordt ten tweede invulling aan gegeven door de platforms als ECP-EPN een rol te geven. Ten derde wordt er invulling aan gegeven door de uitvoering te beleggen bij uitvoeringsorganisaties van de overheid die daarvoor het best zijn geëquipeerd (zoals Logius, Syntens of ICTU) of door - indien meerdere uitvoerders voor uitvoering in aanmerking komen - potentiële uitvoerders om de uitvoering te laten concurreren op grond van prijs-kwaliteit-verhouding. Zo is voor uitvoering van het programma M&ICT zowel door SenterNovem als door ICTU een voorstel gemaakt.

Op grond van het voorgaande blijkt dat diverse voorzieningen zijn getroffen die bijdragen aan een doelmatige toewijzing van middelen aan instrumenten en die bijdragen aan een doelmatige besteding van de middelen. Tegelijkertijd past bij deze conclusie wel de kanttekening dat kostenbeheersing wat anders is dan doelmatigheid (verhouding kosten en opbrengsten).

4 Is er nog verbeterruimte en waar moet die worden gezocht?

4.1 Beoordeling

4.1.1 Wat is bereikt?

> ***Conclusie:***
>
> ***Het beleid en de ingezette instrumenten hebben de doelen dichterbij gebracht. De door het Ministerie van EL&I ingezette instrumenten hebben een substantiële bijdrage geleverd aan het doelbereik en zijn overwegend doeltreffend gebleken.***

Doelbereik OD2

OD 2 betreft een 'veilig en betrouwbaar elektronisch netwerk'. Die doelstelling is uitgesplitst in enerzijds de continuïteit en betrouwbaarheid van de telecommunicatienetwerken en anderzijds de veiligheid en betrouwbaarheid van het internet (en het vertrouwen van gebruikers daarvan). Hierna wordt aangegeven wat is bereikt op deze twee doelstellingen.

Mate van borging van de continuïteit en betrouwbaarheid van de telecommunicatienetwerken en -diensten

Als het gaat om de borging van de continuïteit en betrouwbaarheid van telecommunicatie, dan moet ten eerste worden geconstateerd dat uitval niet altijd te voorkomen is. Honderd procent continuïteit bestaat niet, dan wel is economisch niet rendabel.

Dat geconstateerd hebbende, kan worden opgemerkt dat de crisisorganisaties van telecommunicatiebedrijven relatief goed voorbereid zijn op potentiële grotere verstoringen doordat zij reeds goed om kunnen gaan met kleine en middelgrote verstoringen die veelvuldig voorkomen. Ook kan worden opgemerkt dat de sector beter voorbereid is op verstoring dan een aantal jaren geleden.

Ten eerste heeft er institutionalisering plaatsgevonden in een platform waarin wordt gesproken over continuïteitsmanagement en over het voorkomen van uitval: het NCO-T. Door deelname aan dat platform kennen de contactpersonen van de grootste telecombedrijven elkaar waardoor ze elkaar ook gemakkelijker kunnen vinden als dat nodig is (bij buitengewone omstandigheden).

Ten tweede rapporteren de NCO-T-leden jaarlijks (voor 1 april) aan de Minister van EL&I inzake de door hen getroffen voorbereidingen op een verstoring. Daarin is beschreven hoe de continuïteitsplanning en het crisismanagement in het bedrijf zijn vormgegeven. Het format voor de rapportage dwingt de aanbieders transparant te zijn over de voorbereidingen die ze hebben getroffen en de zwaarte van de genomen maatregelen (bijvoorbeeld: de hoeveelheid noodaggregaten op vitale locaties als backup voor het geval de elektriciteit uitvalt). Uitvoering van deze exercitie - het maken van de rapportage an sich - lijkt op grond van de door ons gevoerde gesprekken met enkele telecomoperators te hebben bijgedragen aan het (nog beter) op de agenda krijgen van continuïteitsplanning en crisismanagement bij deze individuele aanbieders. Bovendien is er volgens het ministerie van EL&I op grond van de jaarlijkse rapportages een stijgende lijn te ontdekken in het niveau van de door aanbieders getroffen voorbereidingen.

Ten derde: de sector is betrokken geweest bij verschillende risicoanalyses en scenario-analyses. In 2008/2009 zijn twee scenario's geanalyseerd in het kader van het Project ICT-Verstoring. In het project Bescherming Vitale Infrastructuur en VISTIC zijn risicoanalyses uitgevoerd. Door deze analyses is meer inzicht ontstaan in mogelijke

oorzaken en gevolgen van uitval en in de voorbereidingen die kunnen worden getroffen om uitval te voorkomen. Dat inzicht heeft ertoe geleid dat telecombedrijven maar ook eindgebruikers maatregelen hebben getroffen om weerbaarder te zijn tegen uitval. Daarbij past wel de kanttekening dat onze verwachting is dat alleen maatregelen zijn genomen waarvan de kosten voor bijvoorbeeld een individueel telecommunicatiebedrijf opwegen tegen de opbrengsten van datzelfde bedrijf. In dat licht is ook relevant te noemen dat in opdracht van het ministerie van EL&I en onder regie van het NCO-T in 2009 een onderzoek heeft plaatsgevonden naar de mogelijke aanwijzingen die de Minister zou kunnen geven aan aanbieders in het geval van buitengewone omstandigheden. Voor elk van die aanwijzingen is de uitvoerbaarheid onderzocht en is in kaart gebracht welke voorbereidingen aanbieders vooraf al kunnen treffen zodat ze - in het geval van buitengewone omstandigheden - adequaat kunnen reageren.[38]

Ten vierde: De sector heeft zich voorbereid door deel te nemen aan oefeningen. Er vinden regelmatig crisisoefeningen plaats op zowel bestuurlijk als op technisch-operationeel niveau waaraan de sector deelneemt. Met de oefening Shift-Control in 2007 is voor het eerst in Nederland grootschalig geoefend met een ICT-uitval scenario. In september 2010 vond oefening Cyberstorm III plaats, waarin is geoefend met de plannen en procedures bij grootschalige uitval van ICT-systemen.[39] In 2011 zal een volgende oefening plaatsvinden. Overigens is in dit licht ook relevant te constateren dat de sector zeer regelmatig te maken met heeft met kleine verstoringen. Door dat gegeven is aannemelijk dat de crisisorganisaties van aanbieders regelmatig worden getest in hun vermogen deze verstoringen op te lossen, wat ook bijdraagt aan hun voorbereiding op de grotere verstoringen.

Ten vijfde zijn er werkbare afspraken gemaakt die bijdragen aan een goede respons. Zo zijn er verplichtingen om in de responsfase aanwijzingen van de Minister van EL&I uit te voeren in het geval van buitengewone omstandigheden (BO).

Mate waarin gebruik van internet veilig en betrouwbaar is
Een belangrijke graadmeter voor de veiligheid en betrouwbaarheid van het internet is de grootte van de schade en overlast door cybercrime. Echter, met betrekking tot de omvang van die schade zijn weinig gezaghebbende cijfers beschikbaar. Dat komt omdat niet alle incidenten worden gemeld en geregistreerd, omdat de diversiteit van de verschillende vormen van cybercrime lastig eenduidig te registreren is (bijvoorbeeld in de systemen van politie en justitie) en omdat de schade per geval varieert en dus niet eenvoudig te veralgemeniseren is.[40] Wel is bekend dat in 2010 ruim 70% van de internetgebruikers in Nederland te maken heeft gehad met virussen en/of spam.[41]

Het Ministerie levert aan de bestrijding van cybercrime een significante beleidsinspanning middels een variëteit aan instrumenten. In dat licht is ook relevant te constateren dat Nederland in Europa een voortrekkersrol vervult als het gaat om het bestrijden van cybercrime en internet onveiligheden. De aanpak van

[38] Zie: Kwink Groep, Herijking methodiek voor het aanwijzen van aanbieders, 2010.
[39] Hierin is ook het functioneren geoefend van de nieuwe ICT Response Board (IRB, in oprichting) waarin bedrijven uit de ICT-, de telecom- en de energiesector en de financiële wereld samenwerken met de crisisorganisaties van de Rijksoverheid om de effecten van een grote ICT-verstoring zo veel mogelijk te beperken.
[40] Ondanks dat de omvang van de schade niet precies bekend is, kan worden geconstateerd dat de toename van het internetgebruik en het aantal online markttransacties in ieder geval een stuwende factor is gebleken voor het aantal incidenten. Op dat punt nemen we ook een aantal verontrustende trends waar. De totale kosten door malware nemen wereldwijd toe en malware wordt tegenwoordig niet alleen via pc's maar ook via mobiele telefoons verspreid. Momenteel wordt het dagelijks aantal verstuurde spamberichten op 100 tot 200 miljard geschat. Ook in Nederland bij de OPTA stijgt het aantal binnengekomen klachten over spam nog steeds. Nederland komt dan ook structureel voor in de top 10 van meest gespamde landen en is vanwege haar sterk ontwikkelde breedbandnetwerk een aantrekkelijk doelwit voor cybercriminelen.
[41] CBS, 2010 (www.cbs.nl).

spambestrijding en de rollen die OPTA (handhaving) en het NICC (kennisdeling via informatieknooppunten) vervullen worden in het buitenland als best practices gezien en op onderdelen overgenomen.

Daarnaast worden waarschuwingen gegeven door de Waarschuwingsdienst (met ongeveer 70.000 leden), wordt voorlichting gegeven via programma's als DigiVaardig & DigiBewust en is publiek-private samenwerking opgestart binnen het Platform Internetveiligheid. In 2007, 2008 en 2009 werden door de Waarschuwingsdienst achtereenvolgens 107, 102 en 65 waarschuwingen gegeven. Omdat burgers en bedrijven via de Waarschuwingsdienst worden voorgelicht over de op dat moment actuele risico's op internet en advies krijgen hoe daarmee om te gaan, wordt een positieve bijdrage geleverd aan het beperken van economische schade en overlast van cybercrime. Het blijft uiteraard wel de primaire verantwoordelijkheid van burgers en bedrijven om naar aanleiding van deze waarschuwingen actie te ondernemen ten aanzien van de bescherming van de eigen ICT-voorzieningen. In dat licht is interessant dat uit onderzoek van Eurostat in 2011 naar voren is gekomen dat Nederlanders zich relatief goed wapenen tegen onder andere malware en virussen. Van alle inwoners van de EU maken Nederlanders het meest gebruik van beveiligingssoftware.[42]

Via het instellen van het Platform Internetveiligheid is een overlegstructuur gerealiseerd waarin publieke en private partijen afspraken met elkaar maken, bijvoorbeeld over het verwijderen van illegale of onrechtmatige content van websites, de zogenaamde 'Notice-and-Take-Down' gedragscode. De procedure heeft ervoor gezorgd dat online dienstverleners nu duidelijk weten hoe zij dienen om te gaan met een melding van mogelijk illegale of onrechtmatige informatie: conform de NTD-code kunnen zij die zo spoedig mogelijk verwijderen van de website. Het platform heeft ook een Werkgroep botnets opgezet die beoogt om een structurele bijdrage te leveren aan de bestrijding van botnets en het tegengaan van de negatieve gevolgen ervan. Daarnaast heeft het platform in aanvulling op de voortdurende inspanningen van politie, justitie en het Meldpunt Kinderporno een Werkgroep filteren/ blokkeren Kinderporno opgezet die samenwerking tot stand brengt ten aanzien van de inrichting van een blokkade voor kinderporno.

Voor wat betreft de stand van zaken in Nederland ten aanzien van de bescherming van de privacy op internet is een tweetal constateringen van belang. Ten eerste staat volgens Govcert de privacy van burgers onder druk omdat zowel de overheid als het bedrijfsleven steeds meer persoonsgegevens registreren maar die 'niet altijd adequaat beschermen.' Persoonsgegevens van Nederlanders komen gemiddeld in 250 tot 500 verschillende databestanden voor.[43] Ten tweede delen eindgebruikers vrijwillig veel persoonlijke informatie via elektronische netwerken zoals sociale netwerken 'zonder daarvan in alle gevallen de consequenties te overzien.' Dit betekent dat computergebruikers, zowel burgers als bedrijven, zich niet altijd bewust zijn van de risico's van internet en andere ICT-voorzieningen en best practices voor informatiebeveiliging ook niet altijd toepassen.

Als het gaat om de bescherming van de persoonlijke levenssfeer in het licht van telemarketing (art. 11.7 Tw), dan is het beleid rondom het wettelijke Bel-me-niet Register van belang. Op 1 oktober 2009 is dat register wettelijk verankerd in de Telecommunicatiewet en ingesteld. In het register kunnen natuurlijke personen zich inschrijven als zij geen ongevraagde (verkoop)telefoontjes meer willen ontvangen. Bedrijven die gebruik maken van telemarketing (zoals adverteerders of call centers) moeten het Bel-me-niet Register raadplegen als ze natuurlijke personen waar zij nog geen bestaande (klant)relatie mee hebben, willen bellen voor (verkoop)acties. Bij aanvang van het register waren er circa 2,6 miljoen telefoonnummers geregistreerd, een jaar later waren dat er ruim 5,5 miljoen en nam het aantal inschrijvingen nog gestaag toe.[44] Dat toont aan dat de bekendheid van het register relatief groot is geworden in vergelijking met de periode voor 1 oktober 2009 waarin het register onder de naam Infofilter nog een zelfreguleringsinitiatief was. OPTA houdt toezicht op de naleving van de regels inzake ongevraagde elektronische communicatie met menselijke tussenkomst

[42] Eurostat rapport 'Safer Internet Day' (2011) via: http://europa.eu.
[43] Govcert (2010). *Nationaal trendrapport cybercrime en digitale veiligheid 2010.* Den Haag.
[44] Zie: Tweede Kamer, vergaderjaar 2010-2011, 27 879, nr. 36, p. 1.

(telemarketing). Gedurende het eerste jaar van het register heeft OPTA via ConsuWijzer ruim 9500 klachten over telemarketing van consumenten ontvangen.[45] Op basis daarvan heeft OPTA handhavend opgetreden, meestal door informele waarschuwingen uit te delen op grond waarvan een groot deel van de bedrijven en organisaties haar telemarketingactiviteiten overeenkomstig de wet heeft aangepast. Indien de informele waarschuwingen niet het gewenste effect hebben, worden door OPTA formele handhavingsinstrumenten ingezet die kunnen leiden tot het uitdelen van boetes of lasten onder dwangsom. Op grond van het voorgaande is door het Ministerie van EL&I geconstateerd dat OPTA voldoende toezicht houdt op de telemarketingbranche en interventies pleegt wanneer blijkt dat er veel signalen binnenkomen over een bepaalde organisatie.[46]

Uit trendrapportages blijkt dat burgers en bedrijven voldoende vertrouwen hebben in de veiligheid van ICT om er gebruik van te maken. Zo heeft 81% van de internetgebruikers aangegeven voldoende vertrouwen in de beveiliging van de eigen computer te hebben. Van de 35.000 MKB'ers die zijn ondervraagd in het kader van de Digibarometer vanuit het voorlichtingsprogramma Digivaardig & Digibewust is 80% van mening dat de digitale veiligheid van de eigen organisatie op orde is. Slechts 7% van de mensen die online aankopen doen zijn van mening dat elektronische handel niet veilig is. Als gevolg van het vertrouwen groeit het aantal internetactiviteiten. In 2009 was Nederland op Denemarken en het Verenigd Koninkrijk na koploper van de West-Europese landen als het gaat om het online doen van aankopen.[47] Het aantal e-shoppers in Nederland is sterk gegroeid: uit onderzoek is gebleken dat ruim 70% van de Nederlandse internetgebruikers wel eens aankopen doet via internet.[48] Ook elektronisch bankieren is sterk toegenomen: in 2005 maakte 58% van de internetgebruikers hiervan gebruik, in 2009 is dit aantal gestegen naar 78% van de internetgebruikers.[49]

De overheid heeft bijgedragen aan het vergroten van het vertrouwen van burgers en bedrijven in ICT-gebruik door het bestrijden van cybercrime middels instrumenten als het spambeleid en door het geven van voorlichting over een veilig gebruik.[50] Daarbij moet worden opgemerkt dat juist ook de markt zelf in belangrijke mate bijdraagt aan het vertrouwen van consumenten in online diensten, bijvoorbeeld doordat die markt de financiële schade als gevolg van veiligheidsincidenten in veel gevallen voor eigen rekening neemt (bijvoorbeeld inzake creditcardfraude).

Het voorgaande neemt niet weg dat cybercrime een hardnekkig probleem is en waarschijnlijk zal blijven, omdat cybercriminelen steeds geavanceerder methoden ontwikkelen. De middelen om het probleem aan te pakken zijn daarbij niet oneindig en het succes van de aanpak van cybercrime is sterk afhankelijk van autonome ontwikkelingen en van de inspanningen van andere (internationale) organisaties dan het ministerie van EL&I.

Doelbereik OD3

OD3 luidt: 'Ontwikkeling van innovatieve voorzieningen, digitalisering van omroeptoepassingen, faciliteren van producten en diensten voor elektronische communicatie en benutting ervan door de consument, het bedrijfsleven en de (semi-) publieke sector'. Kort gezegd gaat het om het ontwikkelen en faciliteren van innovatieve voorzieningen en het stimuleren van de toepassing ervan door consumenten, bedrijven en de (semi-) publieke sector. Hierna wordt aangegeven wat is bereikt, door de resultaten te beschrijven ten aanzien van de ICT-basis en vervolgens het ICT-gebruik van achtereenvolgens bedrijven, overheidsorganisaties, maatschappelijke sectoren en burgers.

---

[45] Zie: Tweede Kamer, vergaderjaar 2010-2011, 27 879, nr. 36, p. 2.
[46] Zie: Tweede Kamer, vergaderjaar 2010-2011, 27 879, nr. 36, p. 3.
[47] Eurostat (2009). Via : http://epp.eurostat.ec.europa.eu.
[48] Govcert (2010). *Nationaal trendrapport cybercrime en digitale veiligheid 2010*. Den Haag.
[49] CBS (2009). *De digitale economie 2009*. Den Haag.
[50] Een kanttekening hierbij is dat de bijdrage van het TTP-beleid aan het vergroten van het vertrouwen van consumenten minder groot is dan er van tevoren van werd verwacht.

ICT-basis

Als het gaat om de ontwikkeling van ICT-voorzieningen, is met het Actieprogramma Breedband vooral in de beginperiode van deze beleidsevaluatie geïnvesteerd in de ontwikkeling van een solide ICT-basis. Nederland doet het goed op dit punt. Het aantal huishoudens met toegang tot een PC is van 85% in 2005 gestegen naar 91% in 2009.[51] Het percentage huishoudens met toegang tot internet is gestegen van 78% in 2005 naar 90% in 2009.[52] De precieze bijdrage van het Actieprogramma Breedband aan de doelstelling is lastig vast te stellen omdat resultaten van het programma beperkt zijn vastgelegd: van de 14 beleidsacties binnen het Programma Breedband is -behalve voor Kenniswijk en Nederland BreedbandLand (NBL) - geen tot weinig informatie beschikbaar over de uitvoering van de acties dan wel over de resultaten.

ICT-gebruik door bedrijven

Als het gaat om de stimulering van het gebruik van ICT door bedrijven, heeft het Ministerie van EL&I een bijdrage geleverd met het programma NDiV.

Alle gesprekspartners geven aan dat het programma NDiV een waardevolle bijdrage heeft geleverd aan het stimuleren van het gebruik van ICT en het zoeken van samenwerkingsverbanden in het MKB. Enerzijds geldt voor veel ondernemers dat er nog ICT-vraagstukken spelen die voorafgaan aan het verkennen van ketenmogelijkheden, waardoor het starten van ketenprojecten voor een deel van de MKB-ers nog een brug te ver is. Tegelijkertijd geven betrokkenen aan dat het NDiV voor die MKB-ers heeft bijgedragen aan het inzicht in de meerwaarde van het opzoeken van (digitale) samenwerking. Daarnaast heeft het programma gestimuleerd dat ICT-behoeften zijn geïdentificeerd. Het programma wordt daarmee door betrokkenen beschouwd als 'smeerolie'. Op termijn zouden MKB-ers ook zelfstandig tot deze ontwikkeling zijn gekomen, maar het programma NDiV heeft dit proces versneld.

Verder kan worden vastgesteld dat Nederland in Europa voorop loopt voor wat betreft de 'ICT-use' door bedrijven; in de European e-business Readiness Index is Nederland gestegen van de vijfde plek in 2005 naar de tweede plek in 2008.[53] Wij kunnen echter niet vaststellen in hoeverre deze ontwikkeling is toe te schrijven aan NDiV. Afgezet tegen de totale omvang van ICT-uitgaven per jaar door het bedrijfsleven vormde NDiV een zeer klein programma.[54] Daar komt bij dat de impact van NDiV grotendeels pas op termijn zichtbaar zal worden.

ICT-gebruik door overheidsorganisaties

Als het gaat om de stimulering van het gebruik van ICT door overheidsorganisaties, heeft het Ministerie van EL&I een bijdrage geleverd met programma's als eOverheid voor bedrijven, SGGV, het College en Forum Standaardisatie en NOiV.

Het College en Forum Standaardisatie hebben een lijst met ruim 40 gangbare open standaarden ontwikkeld en gepubliceerd en 17 relevante open standaarden opgenomen in een lijst waarop het zogeheten pas-toe-of-leg-uit-principe van toepassing is.[55] Deze lijst is groeiende. Ook is de Nederlandse Overheids Referentie Architectuur (NORA) 3.0 voor de inrichting van ICT-systemen van overheden overheidsbreed erkend. Verder

[51] CBS, Digitale Economie, 2009.

[52] Eurostat, tabel 4.4.

[53] World Economic Forum, Networked Readiness Index, 2009.

[54] In 2007 bedroegen de totale investeringen in ICT-kapitaal in Nederland circa 15,3 miljard euro (bron: Digitale Economie 2009).

[55] Dit beginsel is voor de rijksoverheid vastgelegd in de in november 2008 gepubliceerde "Instructie rijksdienst bij aanschaf ICT-diensten of ICTproducten".

heeft NOiV geleid tot concrete resultaten. Voorbeelden daarvan op het terrein van OS zijn het toepassen van open standaarden bij eFacturen, en de administratieve lastenverlichting door de open standaard XBRL[56].

De bijdrage van SGGV aan het doelbereik is nog beperkt. In SGGV zijn twee cases voltooid van de 15 tot 20 beoogde cases.[57] Begin 2011 zijn overigens nog eens vier cases afgerond en overgedragen aan de ketenpartners. Deze cases laten overigens wel zien dat het optimaliseren van informatieketens tussen overheden en met behulp van ICT leidt tot daadwerkelijke kostenbesparingen.

Via Antwoord voor Bedrijven en de onderliggende 'Berichtenbox' is het sinds 16 december 2009 mogelijk om bij 600 centrale en decentrale overheden digitaal informatie op te vragen. Bovendien zijn overheden verplicht digitaal te reageren. Hiermee wordt invulling gegeven aan de EU-Dienstenrichtlijn (2006/123/EC). Het aantal bezoekers van Antwoord voor Bedrijven is gestegen van circa 40.000 bezoeken per maand begin 2008 naar circa 140.000 bezoeken per maand in 2009.[58] De streefwaarden met betrekking tot bezoekersaantallen zijn daarmee ruimschoots gehaald.[59] Tenslotte is eHerkenning vanaf mei 2010 beschikbaar gemaakt. Vanaf dat moment is een aantal pilots met eHerkenning uitgevoerd. Vervolgens is in september 2010 de versie 1.0 beschikbaar gekomen en is eHerkenning in gebruik genomen door zeven verschillende overheidsorganisaties. Op dit moment bereiden acht organisaties, waaronder de Belastingsdienst, implementatie van eHerkenning voor.[60]

Allereerst stellen we vast dat in 2007 reeds 68% van alle overheidsdiensten gedigitaliseerd was (er zijn geen cijfers beschikbaar over de daarop volgende jaren). Tegelijkertijd wijst de internationale Networked Readiness Index[61] uit dat Nederland relatief laag scoort op ICT-gebruik en ICT-Readiness (22^{e} en 23^{e} plaats) in de overheidsdienstverlening. Ook uit onderzoek van CapGemini blijkt dat Nederland waar het gaat om de kwaliteit van eOverheid voor Bedrijven onder het Europese gemiddelde scoort.[62] Uit onderzoek van Ernst&Young blijkt dat - met name waar het gaat om het digitaal afhandelen van aanvragen (bij gemeenten) - de mogelijkheden voor burgers groter zijn dan voor ondernemers.[63] Echter, als het gaat om de bijdrage van instrumenten die het Ministerie van EL&I heeft ingezet, dient te worden opgemerkt dat het grootste deel van de programma's (College en Forum Standaardisatie, NOiV, SGGV) relatief kort bestaat, terwijl de effecten zich pas op de langere termijn zullen manifesteren.

Tegenover de relatief lage scores op de Networked Readiness Index (die door het ministerie van EL&I als belangrijke maatstaf wordt gebruikt in de Voortgangsrapportage ICT-agenda) staat echter een aantal positieve scores op basis van een recente Benchmark 'Digitizing Public Services in Europe'. Zo scoort de Nederlandse overheid (met 95%) ruim boven het EU-gemiddelde (82%) als het gaat om de 'full online availability'[64] van overheidsdienstverlening. Nederland staat daarmee op de 11^{e} positie in Europa. Als het gaat om de 'online sophistication[65] op public services' scoort Nederland tevens boven het Europese gemiddelde (met een score van 97% voor de overheidsdienstverlening aan bedrijven (ten opzichte van het EU-gemiddelde van 94%) en 99% voor de overheidsdienstverlening (ten opzichte van het EU-gemiddelde van 87%).

---

[56] XBRL (eXtensible Business Reporting) is een op XML gebaseerde open standaard voor het samenstellen en elektronisch uitwisselen van financiële rapportages. De XBRL-standaard staat sinds maart 2010 op de lijst van open standaarden voor 'pas toe of leg uit'.
[57] Ministerie van Economische Zaken (2008) Programmaplan SGGV, p.6.
[58] Voortgangsrapportage eOverheid, voorjaar 2010, p.9, via www.e-overheid.nl.
[59] Antwoord voor Bedrijven, jaarverslag 2010, via www.antwoordvoorbedrijven.nl.
[60] www.eherkenning.nl.
[61] World Economic Forum, Networked Readiness Index, 2009. Het gaat hierbij om factoren als ICT-bevordering door de overheid, beschikbaarheid van e-government diensten en ICT-gebruik en overheidsefficiëntie spelen daarbij een rol.
[62] CapGemini (2009). Smarter, faster, better eGovernment, p137.
[63] Ernst & Young (2009). Benchmark Digitale Dienstverlening 2009, p9.
[64] De mate waarin er sprake is van volledige geautomatiseerde en proactieve aanbod van overheidsdiensten.
[65] De mate waarin overheidsdienstverlening interactie en transacties mogelijk maakt tussen de overheid enerzijds en bedrijfsleven en burgers anderzijds. Hierbij zijn verschillende onderdelen van overheidsdienstverlening beoordeeld; belastingen, vergunningen, etc.

Tenslotte is het van belang om op te merken dat het Ministerie van EL&I slechts beperkte invloed heeft op de adoptie van OS, OSS en ICT-toepassingen in de overheidsdienstverlening door overheidsorganisaties, omdat het ministerie hierbij geen doorzettingsmacht heeft. Gelet op de autonomie van overheden, is de invloed op de uiteindelijke benutting van ICT-toepassingen door overheden dus beperkt, maar kan worden vastgesteld dat het Ministerie van EL&I een uitgebreide en brede bijdrage heeft geleverd aan het faciliteren van de adoptie van ICT-toepassingen door overheden, met inachtneming van de eigen verantwoordelijkheid van overheden.

ICT-gebruik in maatschappelijke sectoren
Met het programma M&ICT heeft het Ministerie van EL&I de opschaling van ICT-toepassingen in maatschappelijke sectoren gestimuleerd.

Over het Actieprogramma M&ICT concludeert TNO in 2010 dat het Actieprogramma een duidelijke bijdrage heeft geleverd aan het doorbreken van belemmeringen in het opschalen van maatschappelijk relevante ICT-toepassingen. Op directe wijze zijn 63 projecten materieel en immaterieel ondersteund; op indirecte wijze zijn afgewezen consortia soms doorgegaan en hebben voor eigen rekening opschaling gerealiseerd.[66]

Er zijn inmiddels 25 projecten van M&ICT afgerond. Voor alle afgeronde projecten geldt dat er een duidelijk inzicht is ontstaan in de belemmeringen die zich voor doen bij opschaling van ICT-toepassingen. Voorbeelden van afgeronde projecten zijn[67]: het ontwikkelen van business games in het onderwijs, het verbinden van open digitaal leermateriaal voor het voortgezet onderwijs met erfgoedbronnen van zes musea en archieven, het verbinden van drie kankercentra met 24 ziekenhuizen via videoconferentie en de aanpak schooluitval via een innovatieve ICT-toepassing.

ICT-gebruik door burgers
Als het gaat om de stimulering van het gebruik van ICT door burgers, heeft het Ministerie van EL&I een belangrijke bijdrage geleverd met het programma Digivaardig & Digibewust.

De bijdrage van Digivaardig & Digibewust aan het doelbereik kan aan de hand van een aantal kwalitatieve indicaties worden geïllustreerd.[68] Zo zijn er in totaal 400 vrijwilligers opgeleid in het kader van de 'Kennismakingscursus voor Senioren' en hebben zogenoemde I-coaches MKB-ers bezocht om advies te geven over de mogelijkheden van ICT-gebruik. Verder hebben meer dan 74.000 bezoekers gebruik gemaakt van de website Internetbootcamp en waren er meer dan 14.000 aanmeldingen voor de internettraining die door Digivaardig & Digibewust werd georganiseerd.

De PPS-constructie vormt een waarborg voor doeltreffendheid. Marktpartijen dragen financieel bij, hebben een signalerende rol en borgen daarmee dat juist die activiteiten worden ontplooid waar vraag naar is in de maatschappij.

Wij stellen vast dat het aantal huishoudens met toegang tot een PC van 85% in 2005 is gestegen naar 91% in 2009.[69] Het percentage huishoudens met toegang tot internet is in diezelfde periode gestegen van 78% naar

[66] TNO (2010) Oschaling van maatschappelijk *relevante ICT-toepassingen. Lessen uit de praktijk*. Delft, p. 13.
[67] Het betreft hier een aantal voorbeelden van de 25 afgeronde M&ICT-projecten, op basis van een aantal door het Ministerie van EL&I beschikbaar gestelde factsheets van projecten. Een integraal overzicht van alle afgeronde projecten en bijbehorende resultaten is niet beschikbaar (gesteld).
[68] Op basis van de Jaarverslagen over 2008 en 2009 van ECP-EPN. In de jaarverslagen van ECP-EPN wordt sinds 2008 op kwalitatieve wijze gerapporteerd over de (voorgenomen) activiteiten binnen Digivaardig & Digibewust. Er is echter geen overzicht van concrete resultaten en effecten van de activiteiten uit het programma op de e-vaardigheden in Nederland (beschikbaar). Dit geldt ook voor de voorlopers van Digivaardig & Digibewust.
[69] CBS, Digitale Economie, 2009

90%.[70] Nederland is in Europa koploper voor wat betreft individueel ICT-gebruik en de benutting van de mogelijkheden. Dat geldt ook voor internetactiviteiten zoals internetbankieren en online shoppen. Van de Nederlanders gebruikt 82% het internet bijna dagelijks.

Bijdrage ECP EPN aan doelbereik OD3

Als het gaat om de mate waarin ECP-EPN als neutraal PPS-platform heeft bijgedragen aan Operationele Doelstelling 3, dan zijn de volgende indicaties relevant.[71]

ECP-EPN heeft als platform een grote bekendheid. De meerwaarde wordt onderkend door gesprekspartners uit het bedrijfsleven en van de overheid. Een belangrijke ontwikkeling waaraan ECP-EPN heeft bijgedragen is eFactureren. ECP-EPN heeft zich de afgelopen jaren ingezet voor een grootschaliger adoptie van eFactureren. Zo is een convenant eFactureren opgesteld tussen het Ministerie van EL&I en het bedrijfsleven (in april 2009) en heeft ECP-EPN een informatieve website gerealiseerd.

Door de PPS-constructie die is gekozen voor ECP-EPN worden in samenwerking (en cofinanciering) met het bedrijfsleven resultaten geboekt met een relatief beperkte financiële bijdrage door het Ministerie van EL&I. Voor bijna elk project binnen ECP-EPN geldt dat zowel het ministerie als het bedrijfsleven er een financiële bijdrage aan levert.

4.1.2 WAAR ZIT NOG RUIMTE VOOR POTENTIËLE VERBETERING?

In deze paragraaf wordt aangegeven waar nog ruimte is voor potentiële verbetering.

Conclusie:

Op een aantal onderdelen van het beleid kan de doeltreffendheid in de toekomst nog worden vergroot.

Hierna volgt eerst een uiteenzetting over de potentiële verbeterruimte in het licht van OD 2. Vervolgens wordt de verbeterruimte in het licht van OD 3 beschreven, gevolgd door een overkoepelende opmerking over verbeterruimte (die zowel OD 2 als OD 3 betreft).

De potentiële verbeterruimte in het licht van OD 2 wordt gezien op vier gebieden. De vier punten worden hierna toegelicht.

Verbeterruimte door:
(1) Structureel (laten) uitvoeren van audits van de voorbereidingen die telecommunicatiebedrijven treffen ten einde de betrouwbaarheid en continuïteit van de telecommunicatie te borgen en uitval te voorkomen

Op dit moment zijn de telecommunicatieaanbieders reeds verplicht om jaarlijks voor 1 april te rapporteren over de getroffen voorbereidingen inzake hun continuïteitsplanning en crisismanagement. Volgens het ministerie is er op grond van de rapportages van de aanbieders een positieve ontwikkeling (stijgende lijn) te constateren in het niveau van de door aanbieders getroffen voorbereidingen.

Echter, het frequenter en grondiger (extern laten) auditen van die rapportages kan de doeltreffendheid van het beleid nog verder vergroten. De ingeleverde rapportages van telecommunicatiebedrijven zijn alleen in 2003 en 2008 extern beoordeeld. Daardoor wordt naar onze mening de sturende werking van de rapportageplicht nog niet in zijn volle omvang benut.

[70] Eurostat, tabel 4.4

[71] De bijdrage van verschillende individuele instrumenten die binnen ECP-EPN worden ondersteund (of uitgevoerd zoals in het geval van Digivaardig & Digibewust) aan Operationele Doestelling 3 wordt in paragraaf 4.4 beschreven.

Overigens constateren we bovendien dat het voor de NCO-T-leden - de huidige acht grootste netwerkaanbieders in de telecommunicatiesector - onvoldoende duidelijk is of de overheid van hen verwacht dat zij zich ook voorbereiden op omstandigheden waarop zij zich vanuit een commercieel belang niet uit zichzelf zullen voorbereiden (omdat de kosten voor hen zelf hoger zijn dat de baten). Op dat punt is nodig dat duidelijker wordt gemaakt vanuit de overheid wat van telecommunicatieaanbieders wordt verwacht. Dit speelde overigens ook in de projecten Bescherming Vitale Infrastructuur en Project ICT-verstoring. Daar zijn tal van maatregelen bedacht en belegd, waarbij voorbij lijkt te worden gegaan aan het gegeven dat een deel van de maatregelen niet tot implementatie leidt omdat het niet in het commercieel belang van marktpartijen is (terwijl wel impliciet wordt verondersteld dat marktpartijen de maatregelen uitvoeren) en er tegelijkertijd geen borgingsmechanisme aanwezig is dat implementatie kan verzekeren.

Verbeterruimte door:
(2) Verder versterken van de kennisuitwisseling tussen telecommunicatieaanbieders over continuïteitsplanning en crisismanagement

Het NCO-T beoogt een besloten omgeving van vertrouwen te bieden waarin telecommunicatiebedrijven - in aanwezigheid van het ministerie van EL&I – met elkaar kunnen spreken over te treffen maatregelen om de continuïteit beter te borgen. Het gremium wordt daarnaast gebruikt om kennis uit te kunnen wisselen. Zo heeft één van de bedrijven bijvoorbeeld haar kennis gedeeld over de mogelijkheden van brandbestrijding in vitale locaties (waar blussen met water geen optie is omdat daardoor apparatuur beschadigd kan raken met nadelige consequenties voor de continuïteitsborging).

Echter, telecommunicatiebedrijven geven ook aan dat de aanwezigheid van het ministerie volgens hen als consequentie heeft dat bedrijven soms enige terughoudendheid betrachten als het gaat om het delen van kwetsbaarheden en te treffen maatregelen. Hoewel wij vinden dat de verantwoordelijkheid voor kennisuitwisseling in beginsel bij de bedrijven zelf ligt en hoewel we ons bovendien realiseren dat ook de onderlinge concurrentieverhoudingen tussen bedrijven uitwisseling van kennis in de weg kunnen staan, geven we het ministerie toch in overweging mee een actieve aanjaagrol te vervullen ten einde de kennisdeling te stimuleren.

Verbeterruimte door:

(3) Monitoren van de resultaten van de aanpak van de botnetproblematiek die is gestoeld op zelfregulering, zodat tijdig kan worden overgegaan op andere instrumenten (zoals regulering) indien niet de gewenste resultaten worden bereikt

De botnetproblematiek is een actueel en vooralsnog hardnekkig probleem. Cybercriminelen verbeteren continu hun aanvalsmethoden en zijn in staat om steeds minder zichtbaar en steeds gerichter te werk te gaan door het inzetten van botnets. In het Platform Internetveiligheid is daarom een werkgroep opgericht die als doel heeft een bijdrage te leveren aan het oplossen van dat probleem. Echter, de vraag die zich hierbij voordoet is of zelfregulering zonder overheidsinterventie het meest geëigende instrument is en of ISP's zich voldoende geprikkeld voelen om effectieve maatregelen te nemen als die voor de individuele provider mogelijk meer kosten met zich mee brengen dan opbrengsten. Recent onderzoek liet zien dat providers hun inspanningen op dit terrein hebben geïntensiveerd, maar dat tegelijkertijd een substantieel deel van de problematiek nog niet wordt aangepakt. In dat licht vraagt de rolkeuze van het ministerie van EL&I bij dit vraagstuk aandacht en is het van belang om de effectiviteit van de zelfregulering continu te blijven toetsen, zodat andere beleidsinstrumenten als wetgeving kunnen worden ingezet als de resultaten onvoldoende zijn. Overigens speelt dit niet alleen bij de aanpak van botnets, maar ook breder. De vraag die zich altijd voordoet is

of de poging tot zelfregulering niet leidt tot onnodige en ongewenste vertraging van de oplossing van het probleem. Dat vergt blijvende alertheid van de overheid.

Verbeterruimte door:

(4) Samenhang voldoende (blijven) borgen tussen enerzijds projecten binnen OD2 die worden geïnitieerd/geregisseerd vanuit het ministerie van EL&I en anderzijds projecten die door andere departementen worden geïnitieerd/geregisseerd. Dit geldt met name voor de projecten waarin er overlap is in de deelnemende partijen.

Vitale bedrijven en met name telecommunicatieaanbieders hebben te maken met meerdere (nationale en Europese) overheidsprojecten waaraan ze worden gevraagd of geacht deel te nemen.[72] We constateren dat sommige bedrijven daarbij vanuit hun perspectief niet altijd goed de samenhang tussen de verschillende projecten zien en dat die samenhang op onderdelen door de overheid kan worden versterkt. Een voorbeeld: de definitie voor een 'vitale' organisatie in het project Bescherming Vitale Infrastructuur / Strategie Nationale Veiligheid is een andere definitie dan de definitie die de Minister van EL&I gebruikt om een 'vitaal' telecommunicatiebedrijf aan te wijzen dat verplicht is deel te nemen in het NCO-T.

Het verschil in definities is wel te verklaren en is op zich ook niet onbegrijpelijk: BVI is een interdepartementaal project onder regie van het voormalige ministerie van BZK met een generieke definitie van vitaal die samenhangt met maatschappelijke ontwrichting, terwijl ten behoeve van het NCO-T een 'tailor-made'-definitie is ontwikkeld voor de telecommunicatiesector. Het voorgaande neemt echter niet weg dat op dit soort onderdelen de samenhang nog verder kan worden versterkt. Dat vergt dus ook de komende jaren onverminderde aandacht van het ministerie van EL&I, en ook strakke (inter)departementale afstemming.

Hierna volgt een uiteenzetting over de potentiële verbeterruimte in het licht van OD 3:

Verbeterruimte door:
(5) Zoeken van een optimale combinatie van enerzijds een specifieke, casusgerichte aanpak (waarbij de doelgroep relatief beperkt is) en anderzijds een generieke aanpak gericht op een grotere doelgroep (bijvoorbeeld MKB als geheel)

In programma's als NDiV en M&ICT is een bewuste keuze gemaakt voor een sectorspecifieke aanpak, gericht op het realiseren van een (relatief klein) aantal concrete projecten, in plaats van een meer generieke aanpak gericht op het creëren van bewustzijn bij de doelgroepen (maatschappelijke organisaties, MKB) in het algemeen[73]. Deze keuze is vooraf goed onderbouwd[74] en biedt meer kans op concrete resultaten dan een meer generieke aanpak.

Tegelijkertijd betwijfelen zowel het ministerie van EL&I als de gesprekspartners of succesvolle cases binnen NDiV ook leiden tot navolging in andere sectoren ('spill over'). Er bestaan nog steeds belemmeringen voor bedrijven om zelf het initiatief te nemen om met ketendigitalisering aan de slag gaan. Hetzelfde geldt voor het bereiken van opschaling van ICT-tools in maatschappelijke sectoren. Gesprekspartners betwijfelen of MKB-ers en maatschappelijke organisaties na afloop van de (stimulerings)programma's van het ministerie van EL&I uit zichzelf tot het initiëren van respectievelijk ketensamenwerking en opschaling van ICT zullen komen.

[72] Een deel van deze projecten dient vooral het belang van de sector zelf (bijvoorbeeld de kennisuitwisseling), maar een ander deel van de projecten dient daarnaast ook een breder belang: het publieke, maatschappelijke belang.
[73] Zoals het grootste aantal instrumenten binnen OD3 als doel heeft
[74] Zo werd de keuze in het programma NDiV onderstreept door een vergelijkbare succesvolle aanpak door HBD (Hoofdbedrijfschap Detailhandel) en door een studie van Dialogic uit 2008 in opdracht van het Ministerie van EL&I.

Dus hoewel stimuleringsprogramma's gedurende de looptijd in grote mate een smeerolie-functie hebben vervuld, verdient het de aanbeveling om in de toekomst bij de totstandkoming (en later in de monitoring) van programma's nadrukkelijk op zoek te gaan naar een optimale combinatie van een specifieke en een generieke aanpak. Bijvoorbeeld door een programma in eerste instantie te beginnen met een kleinschalige, specifieke aanpak met een korte termijn smeerolie-functie, om later over te gaan op een meer generieke aanpak waarbij de kennis en succesverhalen uit de specifieke cases worden verspreid, en er wordt ingezet op een structurele gedragsverandering en bewustwording bij een bredere doelgroep. Met als doel om zoveel mogelijk bij te dragen aan het doelbereik op lange termijn.

Verbeterruimte door:
(6) Bij het bevorderen van de inzet van ICT in overheidsdienstverlening nog meer rekening te houden met de behoeften en condities van de gebruikers (overheden), met inachtneming van hun autonomie.

We constateren dat het ministerie van EL&I veel inzet heeft gepleegd als het gaat om het stimuleren van ICT-gebruik door overheden in hun dienstverlening aan bedrijven. Met ondersteunende programma's als NOiV en speciale 'e-teams' zet het ministerie van EL&I daarbij in op het zoveel mogelijk faciliteren van de implementatie van ICT-toepassingen door overheden. De invloed van het ministerie van EL&I op de daadwerkelijke adoptie van ICT-toepassingen door overheden is daarbij maar zeer beperkt. Immers, het ministerie schept de kaders en geeft het goede voorbeeld, maar kan andere overheden niet dwingen hetzelfde te doen.

Toch zou het de doeltreffendheid van het toekomstig beleid ten goede kunnen komen als het ministerie nader zou bezien of er meer mogelijkheden kunnen worden benut om overheden te begeleiden richting de implementatie van bijvoorbeeld OS, OSS en andere e-overheidsdienstverlening (zonder verantwoordelijkheden van overheden over te nemen). Gesprekspartners geven namelijk aan dat overheidsinstanties meer behoefte hebben aan ondersteuning bij het daadwerkelijk toepassen van OS, OSS en ICT-toepassingen in de overheidsdienstverlening (een 'helpende hand'). De nadruk lijkt volgens hen momenteel nog teveel te liggen op het bevorderen van de *aanschaf* (het 'in huis halen') van de ICT-toepassing, en in minder mate op de ondersteuning bij het daadwerkelijke *gebruik* van de toepassing.

Verbeterruimte door:
(7) De focus te bewaken op het op te lossen probleem, door de vraagkant van het probleem centraal te stellen dan wel scherp te houden.

In een aantal instrumenten binnen OD3 (bijvoorbeeld M&ICT en Digivaardig & Digibewust) constateren wij het risico op een nadruk op de aanbodzijde in plaats van de vraagkant van het op te lossen probleem. Gesprekspartners onderstrepen dit.

Zo heeft het programma M&ICT als doel om maatschappelijke problemen op te lossen door het opschalen van ICT-toepassingen. TNO concludeert in 2010 weliswaar dat er voor alle 25 afgeronde projecten geldt dat er een duidelijk inzicht is ontstaan in de belemmeringen die zich voordoen bij opschaling van ICT-toepassingen. Tegelijkertijd stelt TNO ook vast dat in projecten vaak de koppeling ontbreekt tussen enerzijds de ICT-toepassing en anderzijds de onderliggende belemmeringen (waarom lukt opschaling niet?). Volgens TNO was niet altijd scherp in beeld of met de gekozen projectaanpak de aanwezige belemmeringen inderdaad kunnen worden overwonnen. Gesprekspartners bevestigen dit beeld en geven aan dat in de praktijk bleek dat vooral ICT-leveranciers geïnteresseerd waren in het indienen van projecten, en daarbij veel moeite moesten doen om de maatschappelijke organisaties (bijvoorbeeld scholen) mee te krijgen. Omdat opschaling van ICT-toepassingen bevorderen in maatschappelijke sectoren het doel van het programma is, bestaat het gevaar dat het gebruik van ICT een belangrijker doel wordt dan het oplossen van een maatschappelijk probleem (de ICT-toepassing wordt een doel op zich in plaats van een middel). Eenzelfde neiging tot aanbodsturing valt te constateren bij Digivaardig & Digibewust. Er is veel aanbod in termen van voorlichting, trainingen en bijeenkomsten, maar tegelijkertijd is niet voldoende duidelijk of dit aanbod goed aansluit bij de

tekortkomingen (en de specifieke behoeften en vragen) van de doelgroepen op het gebied van e-vaardigheden. Door middel van de Programmaraad worden de perspectieven van aanbieders van ICT(-diensten), overheden, vakbond en werkgeversorganisaties weliswaar betrokken, maar de behoefte/input van de doelgroep lijkt niet actief te worden betrokken.

Met de ICT-barometer voor het MKB (binnen Digivaardig & Digibewust) wordt hier overigens al invulling aan gegeven. Ook richt het meest recente gestarte instrument van OD3, SGGV, zich op zowel het creëren van het aanbod van innovatieve diensten als het stimuleren van de vraag (door belemmeringen op ketenniveau aan te pakken). Een ander voorbeeld is het betrekken van gebruikers in 'gebruikerspanels' zoals bij Antwoord voor Bedrijven wordt gedaan.

De hiervoor genoemde voorbeelden laten zien dat het ministerie van EL&I op verschillende thema's reeds de 'gebruiker centraal' stelt. Toch verdient het –op basis van onze observaties aangaande het programma M&ICT en Digivaardig & Digibewust- de aanbeveling om in de toekomst bij de totstandkoming en tijdens de uitvoering van programma's nog meer zicht te hebben op de vraagkant: wat is het probleem, wat zijn de behoeften van de doelgroep (de maatschappelijke organisatie of de burger) en hoe kan de ICT-toepassing daarbij helpen?

Verbeterruimte (voor zowel OD2 als OD3) door:
(8) Meer inzicht in resultaten en effecten van beleid in de maatschappij, kan bijdragen aan een meer evidence based inzet van het instrumentarium en goede bijsturing. Dat vergt ook dat doelen SMART worden geformuleerd en dat wordt gezocht naar prestatie- en effectindicatoren die een beeld geven van de bereikte resultaten en effecten en dat die indicatoren ook meerjarig worden gemonitord.

We constateren dat op sommige onderdelen van het beleid weinig bekend is over de concrete resultaten en de effecten ervan. Voor sommige instrumenten geldt dat weliswaar de verrichte activiteiten bekend zijn (alsmede de voortgang ervan), maar dat tegelijkertijd minder bekend is waartoe die activiteiten nu precies hebben geleid in termen van doelbereik. Dit geldt zowel voor instrumenten van OD2 als van OD3. Dat zicht op de effecten van het beleid is echter wel nodig om de gekozen overheidsrol goed te kunnen beoordelen, en ook om te kunnen bepalen of de rol zou moeten worden geëxtensiveerd, geïntensiveerd of op andere wijze dient te worden bijgestuurd.

Bovendien worden door beperkte monitoring en evaluatie van de individuele beleidsinstrumenten, de kansen nog onvoldoende benut om over de verschillende instrumenten van OD2 en OD3 heen van elkaar te leren. Wij constateren dat extra inspanningen in de toekomst met betrekking tot het inzichtelijk maken van de effecten, kunnen leiden tot een betere en meer *evidence based*-afweging van rol- en instrumentinzet.

BIJLAGE 1: SAMENSTELLING BEGELEIDINGSCOMMISSIE

Mw. Esther-Mirjam Sent (voorzitter)	Hoogleraar Economische Theorie en Economisch Beleid, Radboud Universiteit Nijmegen
Dhr. Kees Buis	CIO-platform
Dhr. Klaas Bouma	Ministerie van EL&I, MT-lid Directie Telecommunicatiemarkt
Dhr. Delroy Blokland	Ministerie van EL&I, MT-lid Directie Financieel Economische Zaken

BIJLAGE 2: OVERZICHT GEÏNTERVIEWDE EXTERNE STAKEHOLDERS

Marktpartijen en brancheorganisaties:

- UPC
- KPN
- ICT-Office
- IBM
- Hoofdbedrijfschap Detailhandel (HBD)
- CIO-Platform (twee Chief Information Officers van grote ondernemingen)
- VNO-NCW / MKB Nederland

Andere overheidsorganisaties en -vertegenwoordigers:

- Ministerie van BZK
- Ministerie van Veiligheid & Justitie
- Ministerie van OCW
- Ministerie van VWS
- IPO
- VNG

Overige stakeholders (waaronder uitvoeringsorganisaties en toezichthouders):

- NICC
- OPTA
- Govcert
- Antwoord voor Bedrijven
- ICTU
- Syntens
- ECP-EPN
- Forum Standaardisatie

Overig:

- Mediawijsheid Expertisecentrum

BIJLAGE 3: LIJST VAN AFKORTINGEN

AIVD – Algemene Inlichtingen en Veiligheidsdienst
AT – Agentschap Telecom
ATb – Alerteringssysteem Terrorismebestrijding
BVI – Bescherming Vitale Infrastructuur
BZK – Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CBS – Centraal Bureau voor de Statistiek
CIC Uitstraling - Concurreren met ICT-Competenties Uitstraling
CPNI – Center for the Protection of National Infrastructure
CSP - Certificatiedienstverlener van elektronische handtekeningen
ECP.nl – Electronic Commerce Platform
ECP-EPN – Electronic Commerce Platform-Electronic Highway Platform Nederland
EL&I – Ministerie van Economische Zaken, Landbouw & Innovatie
ENISA - European Network and Information Security Agency
EU – Europese Unie
EZ – Ministerie van Economische Zaken
FES – Fonds Economische Structuurversterking
FEZ – Financieel Economische Zaken
Govcert - Computer Emergency Response Team van de Nederlandse overheid
ICCP - Committee for Information, Computer and Communications Policy
ICTU – ICT uitvoeringsorganisatie
IKC – Informatieknooppunt Cybercrime
ISAC - Information Sharing and Analysis Centre
ISP - Internet Service Providers
KLPD – Korps Landelijke Politiediensten
KWINT – nota Kwetsbaarheid internet
M&ICT – Maatschappelijke sectoren & ICT
MT – Managementteam
NACOTEL - Nationaal Continuïteitsplan Telecommunicatie
NAP – Nationaal Actieplan Elektronische Snelwegen
NBL – Nederland Breedband Land
NCO-T – Nationaal Continuïteitsoverleg Telecommunicatie
NCV – Noodcommunicatievoorziening
NDiV – Nederland Digitaal in Verbinding
NGD – programma Nederland Gaat Digitaal
NICC – Nationale Infrastructuur Cyber Crime
NOiV – Nederland Open in Verbinding
NPC – Nationaal Platform Criminaliteitspreventie
NRF - New Regulatory Framework
OD – Operationele Doelstelling
OESO – Organisatie voor Economische Samenwerking en Ontwikkeling
OPTA – Onafhankelijke Post en Telecommunicatieautoriteit
OS – Open Standaarden
OSS – Open Source Software

PPS - Publiek Private Samenwerking
PRIMA – Programma Implementatie ICT-Beleid
R&D – Research & Development
RFID - Radio Frequency Identification
SGGV – Slim Geregeld Goed Verbonden
TTP – Trusted Third Party
VISTIC – Vitale Infrastructuur, Telecommunicatie en ICT
VN – Verenigde Naties
WPISP - Working party for Privacy and Information Security
XBRL - eXtensible Business Reporting
ZBO – zelfstandig bestuursorgaan