

# Gespreksnotitie rondetafelgesprek aangaande grote ICT-projecten bij de overheid

C. Verhoef

*VU Amsterdam, Department of Computer Science,  
De Boelelaan 1081a, 1081 HV Amsterdam, The Netherlands*

x@cs.vu.nl

7 februari 2011

## 1 Achtergrond en aanleiding

De vaste commissie voor Binnenlandse Zaken (BiZa) heeft besloten een rondetafelgesprek te organiseren, ter voorbereiding op het algemeen overleg op 17 februari 2011, waar diverse brieven over ICT bij de overheid worden besproken.

Het rondetafelgesprek vindt plaats ter voorbereiding van een algemeen overleg tussen de leden van de vaste commissie Binnenlandse Zaken met de minister van Binnenlandse Zaken en Koninkrijksrelaties over ICT-projecten bij de rijksoverheid.

Op de agenda van dat overleg staat een aantal brieven van de minister aan de Tweede Kamer die gaan over de volgende onderwerpen.

- DigiD
- Grote ICT-projecten bij de rijksoverheid
- Digitale werkomgeving Rijksdienst
- De rol die ICT kan spelen bij vermindering van de regeldruk

Tijdens het rondetafelgesprek willen de Kamerleden kennisnemen van mijn visie op ICT-projecten bij de rijksoverheid, zowel betrekking hebbend op hoe het nu gaat (Hoofdstuk 2) en hoe het beter zou kunnen (Hoofdstuk 3). Nadat de notitie verzonden was kwamen er nog nadere vragen, die komen kort aan bod in Hoofdstuk 4. Vervolgens heeft de bijeenkomst op 26 Januari 2011 plaatsgevonden en daar zijn tal van additionele vragen tijdens de discussie opgekomen bij de Kamerleden. In Hoofdstuk 5 geven we een neerslag van de vragen die tijdens de discussie zijn gesteld. We geven aanvullende antwoorden zodat ook die vragen waar de tijd antwoorden niet toeliet toch een antwoord krijgen. Dit document moet naast de feitelijke discussie gelezen worden. Die is beschikbaar op Internet<sup>1</sup>.

---

<sup>1</sup>Zie [www.cs.vu.nl/~x/knipsselkrant/rtg-cie-biza-26-jan-2011.mp4](http://www.cs.vu.nl/~x/knipsselkrant/rtg-cie-biza-26-jan-2011.mp4)

## 2 Hoe het nu gaat

Sinds de overheid zich meer stelselmatig bezighoudt met ICT projecten zie ik een aantal fundamentele veranderingen. Ik geef een drietal belangrijke weer. De huidige praktijk is als volgt te kenschetsen.

- Toegenomen transparantie door rapportages
- Zelfreinigend vermogen geïnstitutionaliseerd
- Afbreken Thorbeckehuis voor bedrijfsvoering

**rapportages** Door de rapportages zien we nu dat de ICT-praktijk bij de overheid niet goed genoeg is. In het verleden kwam dat af en toe aan de oppervlakte, nu weten we dat standaard. Een paar voorbeelden. Het centrale informatiesysteem van de politie. Daarvan kwamen meldingen binnen rond 2003 dat er 430 miljoen Euro was verspild. Recentelijk is daar nog eens 42 miljoen bijgekomen. Verder zagen we recent stopzetting van een IT project bij justitie met een schadepost van 18 miljoen Euro. De rapportages verbeteren de situatie niet, ze brengen deze beter, maar onvoldoend volledig en onvoldoend scherp, in kaart.

**zelfreinigend vermogen** De nu op vrijwillige basis ingestelde Gateway reviews zijn een goed initiatief. Elke review is beter dan geen review. De gateway reviews zijn een goed middel om de grootste blunders te identificeren. Soms komen die reviews aan de oppervlakte en dan zien we dat de toetsers van hun hart geen moordkuil maken. Dat is goed voor het elkaar scherp houden. Reviews voor en door ambtenaren. De gateway reviews verhogen de awareness and dragen bij aan kwaliteitsverbetering. We zijn er daarmee echter nog niet.

**Thorbecke en bedrijfsvoering** Onze vorm van lokale democratie is populair gezegd het Thorbeckehuis. In de tijd dat dat bedacht werd was reizen duur, en arbeid goedkoop. In termen van bedrijfsvoering is derhalve geen rekening gehouden met centralisatie. Door instelling van CIOs en een Rijks CIO ontstaat de natuurlijke concern discussie over werk dubbel doen of niet. Daarmee ontstaat afbraak van het Thorbeckehuis op het gebied van de bedrijfsvoering. Omdat dit niet expliciet in wet- en regelgeving vervat is, is deze afbraak wellicht nog te vrijblijvend.

## 3 Wat kan beter

In het voorafgaande kwamen drie belangrijke goede ontwikkelingen ter sprake die mede het gevolg zijn geweest van ingrijpen door de Tweede Kamer naar aanleiding van aanhoudende berichtgeving in de media over problemen bij de grote ICT projecten van de overheid.

Die goede ontwikkelingen kunnen nog wat versterking gebruiken en er zijn andere springende punten die voor verbetering vatbaar zijn waar ook de aandacht op gevestigd wordt in deze gespreksnotitie.

**rapportages** Wat beter kan bij de rapportages is dat niet naar projecten vanaf 20 miljoen wordt gekeken maar naar de top projecten. En dat er breder gekeken wordt, dus ook buiten de kerndepartementen. Vraag de top  $x$  op zodat voor  $x$  projecten je op zo'n 80% van het budget zit, en vraag vervolgens het totaal aantal projecten op plus de totale besteding. Daarmee kun je de inzichten sterk verhogen. De top  $x$  voorkomt perversie van je rapportages. Voorbeelden zijn om alle projecten op 19.7 miljoen te zetten zodat je niet hoeft te rapporten. Of projecten kunstmatig op te delen zodat elk deel onder de limiet komt. Nota bene: na de eerste rapportage met 73 projecten hadden we het jaar erop ineens 34 projecten, dus dit mechaniek is in werking.

**zelfreinigend vermogen** Een gateway review is in principe opvraagbaar wegens de wet openbaarheid bestuur. Omdat in gateway reviews concurrentiegevoelige zaken kunnen staan en omdat in dat soort reviews mensen vrijuit moeten kunnen spreken is het van belang na te denken over een vorm zodat het doel van de deze vorm van peer review niet aan effectiviteit verliest door de opvraagbaarheid van deze reviews. Indien transparantie om welke reden dan ook tijdens een project gewenst is, is dat uiteraard niet verboden.

**Externe audits** Aansluitend op Gateway reviews is de aanbeveling om externe audits uit te laten voeren. In het Besluit informatievoorziening in de rijksdienst 1990 (Besluit IVR 1990) is in artikel 12 al een contra-expertise geregeld:

#### **Contra-expertise**

##### **Artikel 12**

1. Voordat een geautomatiseerd informatiesysteem wordt ontwikkeld, ingevoerd of gewijzigd, waarbij aanzienlijke risico's bestaan, laat de minister wie het aangaat een onafhankelijke contra-expertise verrichten.
2. De minister van Binnenlandse Zaken kan in overeenstemming met het gevoelen van de ministerraad nadere aanbevelingen opstellen omtrent de inhoud en de uitvoering van contra-expertises.

Een verbeterpunt is om dit besluit ten uitvoer te leggen en wat mij betreft ruim te interpreteren: grote ICT-projecten kennen sowieso een verhoogd risico en de ICT-projecten bij de overheid kennen een faalkans die tweemaal zo hoog is als in de private sector. Dit is uitgerekend op basis van de eerste rapportage, en is gevalideerd met de cijfers uit nieuwere rapportages<sup>2</sup>. Zwaardere externe toetsingen van grote ICT-projecten zijn een probaat middel om tijdig en krachtig te kunnen bijsturen om problemen of erger te voorkomen.

**Thorbecke en bedrijfsvoering** Omdat het Thorbeckehuis in zijn volle glorie in werking is, is alles wat naar centralisatie riekt, uiteindelijk vrijblijvend. Wat beter kan is betere borging voor de uitzonderingspositie die op bedrijfsvoering van kracht is op het Thorbeckehuis om daarmee de vrijblijvendheid in te korten ten faveure van effectieve en efficiënte bedrijfsvoering, waar ICT onder valt.

<sup>2</sup>Voor meer informatie zie *Benchmarking the expected loss of a federal IT portfolio*, opvraagbaar via [www.cs.vu.nl/~x/fed/fed.pdf](http://www.cs.vu.nl/~x/fed/fed.pdf)

**De Europese aanbestedingspraktijk** Een springend punt is het aanbestedingsbeleid. Het aanbesteden van ICT-projecten op kwaliteit is uiterst lastig en zorgt ervoor dat kwalitatief hoogwaardige partijen het onderspit delven ten opzichte van minder goede leveranciers. In de praktijk worden ICT projecten op prijs beslecht ook al is er sprake van een prijsmodel waarbij niet op laagste prijs wordt gegund (dat is de Economisch Meest Voordelige Inschrijving, of EMVI). Waarom dit uiterst lastig is valt na te lezen in twee stukken die ik erover publiceerde in binnenlands bestuur. In het kort, het is een combinatie van juristerij, wiskunde en onvoldoende kennisbasis<sup>3</sup>. Een mogelijkheid die voor ogen staat is gerelateerd aan het Thorbeckehuis: het centraliseren van inkoopkennis.

**Privacy, Security, en Safety** Gevolgen van slechte aanbestedingspraktijken zijn dat er op aspecteisen ingeboet wordt. Aspecteisen zijn zaken als Reliability, Availability, Maintainability, Safety, Security, Health, Environment, Economics, en Politics (RAMS SHEEP). Enkele voorbeelden. De HSL is sterk vertraagd door het veiligheidssysteem. De Roer en Swalmetunnel zijn sterk vertraagd door het veiligheidssysteem, en idem voor de overkappingsconstructie in Rijksweg A2 nabij Leidsche Rijn. Een voorbeeld uit de privacy en security. Door optimalisatie naar laagste prijs stromen IT-systemen naar verre landen (off-shoring) en daar kunnen ook systemen van de IND en andere diensten bij zitten. De security is daar op papier goed geregeld maar de praktijk wijst anders uit.

**Achilleshiel** Dan zijn er nog de projecten die niemand als ICT projecten kenschetst maar waar ICT wel de Achilleshiel is. Enkele voorbeelden. De Ketelbrug vertoonde onveilig gedrag: de slagboom kan open en dicht, het licht op groen en rood, de brug open en dicht, maar de combinatie is niet altijd betrouwbaar. Gevolg: een dode doordat de brug open stond terwijl het licht op groen stond. Wat te denken van de recente tunneldrama's: het is de ICT die voor sterke vertraging zorgt (Roertunnel, A2 Leidsche Rijn). Of de HSL: het is het veiligheidssysteem dat voor vertraging zorgt. Deze projecten zitten niet in de ICT rapportages, want worden niet zo gezien. Een vorm van rapportage voor projecten met ICT als Achilleshiel valt te overwegen.

## 4 Nagekomen bericht

Naar aanleiding van vragen van een aantal genodigden voor deze ronde tafel is in de procedurevergadering van de vaste commissie voor Binnenlandse Zaken—nadat deze gespreksnotitie was verzonden—het rondetafelgesprek kort aan de orde geweest. De leden is gevraagd wat zij in het rondetafelgesprek aan de orde willen stellen. Hieronder de weergave daarvan.

- De succes- en faalfactoren van grootschalige ICT-projecten bij de overheid.
- De voor- en nadelen van cloud computing.
- De mogelijkheden van open source standaarden.

<sup>3</sup>Zie *Aanbesteden zonder hoofdpijn?* opvraagbaar via [www.cs.vu.nl/~x/knipsselkrant/db-16.pdf](http://www.cs.vu.nl/~x/knipsselkrant/db-16.pdf)  
*Eerste hulp bij aanbesteden* [www.cs.vu.nl/~x/knipsselkrant/db-17.pdf](http://www.cs.vu.nl/~x/knipsselkrant/db-17.pdf)

- Beveiligingsaspecten, bijvoorbeeld hoe voorkom je dat informatie op straat komt te liggen?
- Ontwikkeling van de elektronische overheid: wat zijn de ontwikkelingen van de elektronische overheid en zijn de beschikbare instrumenten voldoende om de doelstellingen te realiseren?

Die zullen we ook kort behandelen voor zover nog niet aangestipt.

**succes- en faalfactoren** Zoals aangegeven is het faalrisico van de IT-portfolio van grote projecten bij de overheid minstens tweemaal zo hoog als in de private sector. De faalfactoren die vaak bij elkaar komen bij overheidsprojecten zijn als volgt:

- fantasy deadlines
- geen convergentie van het eisen- en wensenpakket
- revolutie in plaats van evolutie
- veel te grote projecten
- elke keer weer in zee gaan met de kneuzen uit de industrie

Deze faalfactoren zijn keurig uitgewerkt in een overzichtscollage dat ik schreef voor binnenlands bestuur<sup>4</sup>. Vervolgens is elke faalfactor per stuk nog eens verder uitgediept in een specifiek op dat risico toegesneden college in binnenlands bestuur.

Wat beter moet om uit deze impasse te geraken is om deadlines door experts uit te laten rekenen, politieke discipline te betrachten (niet elke week een ander idee), veel meer gebruik te maken van wat er al is en dat verbeteren, kleine stappen te zetten, en met echte vaklui in zee gaan.

**de cloud** Cloud computing is niets anders dan het mainframe model uit de 1960er jaren: een groot computercluster waar iedereen via een terminal op werkt. Nu is het computercluster gedistribueerd, de terminals zijn zelfstandige computers geworden en de lijnen ertussen is het Internet. Het gaat dus om een technisch verhaal. De vraag of je er iets mee moet wordt derhalve ingegeven of het bedrijfsprobleem dat je hebt zich het best laat oplossen met dit technische middel. Soms zal dat het geval zijn, maar vaker niet. Denk aan gevoelige informatie, of gevoelige communicatie. Moet dat ergens op deze wereld rondzwerven, of houden we dat binnenshuis? Je kunt daarmee niet spreken over voor- en nadelen van cloud computing.

**open source en open standaarden** De vraag zoals gesteld is betekenisloos. Er is open source, en er zijn open standaarden. Open source is programmatuur die je kunt downloaden vanaf het Internet en dat mag je onder bepaalde licentie condities gebruiken. Die licenties kunnen viraal zijn. Dat betekent dat alles wat je ermee maakt daarmee ook open moet worden. Als je dat niet wilt moet je kosten betalen. Er zijn ook andere licenties overigens. Open source is vaak *open sores*: behoudens een paar veel en vaak gebruikte zaken is er een ongelooflijke hoeveelheid programmatuur die nauwelijks aan de praat te krijgen valt. Dat is voor en door ontwikkelaars, en daar kun je als overheid niets mee. Voor het grootste gedeelte is de code van de overheid niet

<sup>4</sup>[www.cs.vu.nl/~x/knipsselkrant/db-01.pdf](http://www.cs.vu.nl/~x/knipsselkrant/db-01.pdf)

geschikt om vervangen te worden door open source. Dat komt omdat niemand open source belasting aangifte software schrijft, omdat niemand de wet op de nabestaanden uitprogrammeert voor de lol, enzovoorts. De bulk van overheids software is gesloten omdat het specifieke wetten uitvoert, daar is geen mondiale markt voor.

Dan open standaarden. Het is immer goed om je te realiseren dat als je een email systeem bedenkt dat niet aan RFC 822 (standard for the format of arpa internet text messages) voldoet, je met hele volksstammen niet kunt communiceren. Daarom is het meestal een goed idee om bij interoperabiliteit tussen systemen te streven naar open standaarden. Met andere woorden standaarden die iedereen kan lezen en toepassen. Een open standaard is vaak geen code, maar tekst, zoals RFC 822 uit 1992, die nog steeds uitlegt hoe een email bericht er precies uit moet zien zodat elk email systeem het kan verwerken.

**beveiligingsaspecten** Zoals aangegeven delven aspecteisen waar beveiliging onder valt vaak het onderspit bij de overheid. Dit is debet aan de faalfactoren die we vaker zien. Een simpel voorbeeld. Een maand nadat de toenmalige minister van defensie had aangekondigd dat de lekken in zijn website waren gedicht waardoor gevoelige informatie van onder andere Eric O. op straat lag, heeft defensie de website van het commando diensten centrum plat laten leggen omdat de auteur dezes nog eens 3000 documenten aantrof die daar niet hoorden, en men kreeg dat niet snel gemaakt. Met die documenten plus informatie op Internet lukte het om binnen vijf minuten een chauffeur die hoge militairen rondreed te achterhalen: naam, adres, woonplaats en foto. Je moet er niet aan denken wat kwaadwilligen daarmee hadden kunnen aanrichten.

In de Verenigde Staten is identiteitsdiefstal een plaag die in 2003 al 50 miljard dollar kostte. Er is stringente wet- en regelgeving: er zijn torenhoge boetes en veroorzakers moeten jarenlang zorgen dat de gevolgschade zoveel mogelijk wordt beperkt via het zogeheten credit monitoring. Het is van groot belang om dergelijke sancties ook in Nederland op te leggen: daarmee wordt de business case voor security en privacy hard. Nu kan iedereen een identiteit kopen en misbruiken en staan websites wagenwijd open, ook die van de overheid zo blijkt<sup>5</sup>.

**e-overheid** Het leveren van producten en diensten via de elektronische snelweg vergt het uiterste van de professionaliteit van zowel opdrachtgever als opdrachtnemer. De huidige graad van professionaliteit bij de overheid en de opdrachtnemers waar ze mee te werken komt door het Europees aanbestedingsbeleid is onvoldoende voor een dergelijke operatie. Eerst moeten dit soort fundamentele zaken aangepakt worden alvorens met ambitieuze trajecten in te gaan.

## 5 De discussie

Tijdens de bijeenkomst zijn nadere vragen gesteld door de commissieleden. In dit hoofdstuk gaan we daar puntsgewijs op in zodat ook vragen die ten tijde van de ronde tafel door tijdgebrek onvoldoende aanbod kwamen alsnog invulling krijgen.

**Vraag** Als het zo simpel is als u zegt, waarom zijn er dan—ik meen een jaar of acht inmiddels, zo niet langer—bezig met een OV-chipkaart die gister bleek te falen.

<sup>5</sup>[www.cs.vu.nl/~x/knipsselkrant/nieuwe-revu.pdf](http://www.cs.vu.nl/~x/knipsselkrant/nieuwe-revu.pdf)

**antwoord** We delen dit op in twee gedeeltes. Allereerst is er het aspect van de falende beveiliging. Op zich belangrijk genoeg. En ten tweede is de vraag hoe het toch kan dat iets simpels toch niet gebeurt? Dat behandelen we iets later bij een andere vraag die dat expliciet maakt.

Twee jaar terug werd de OV-chipkaart gekraakt, en dan duurt het even voor een consumentenversie op de markt is. Dat is dus nu zo ver. Gek genoeg lezen we nooit dat de chipknip gekraakt is: daar zitten de banken echt bovenop omdat het inhibitief hoge risico's in zich bergt als je dat niet goed voor elkaar hebt.

Wat is er aan de hand? Bij het maken van de OV-chipkaart zijn de ontwerpprincipes van cryptografie met voeten getreden. In 1883 beschreef Auguste Kerckhoffs de basis voor een goed ontwerp van encryptie. Eén van die principes is dat als de vijand het cryptosysteem in handen krijgt maar zonder de sleutel, hij er niets aan heeft. Dit heet heden ten dage in de vakliteratuur nog altijd Kerckhoffs' principe.

De OV-chipkaart kent een geheim cryptosysteem. Daarmee schenden de ontwerpers van de OV-chipkaart Kerckhoffs' principe. Het is heel lastig om een systeem te bedenken dat van leesbare teksten 'random rommel' maakt waar je niets aan kunt zien. Alleen met een sleutel kun je de geheime boodschap weer terug toveren. Een voorbeeld: de FBI was vorig jaar 5 maanden bezig om disks van een Braziliaanse bankier te ontcijferen. Dat lukte niet. Men wist wel dat het met een AES-256 algoritme was versleuteld.

Het bedenken van encryptie systemen staat precies gelijk aan het bedenken van nieuwe ingenieuze wiskunde. De kans dat een bedrijf dat in isolatie voor elkaar krijgt is vrijwel nihil. Het zou betekenen dat de grote crypto-denkers daar allemaal moeten werken. En dat is bij de OV-chipkaart geenszins het geval.

Dan is er het geld: goede versleuteling kost rekenkracht. Rekenkracht kost computerruimte, en een chip met meer ruimte is duurder dan een chip met minder ruimte. Het is dus een centenkwesie.

Veel belangrijker is het ontwerpprincipe van de OV-chipkaart zelf: het is een onding en totaal verkeerd bedacht. Zo is in Duitsland een veel pragmatischer oplossing bedacht. Daar heeft men het ontwerp compleet omgekeerd. De chip die in Nederland elke reiziger bij zich draagt, zit in Duitsland in de muur.

De kaartlezer is de mobiele telefoon die vrijwel elke reiziger heeft. Dus geen poortjes, geen netwerk, geen stroomvoorziening en geen Trans Link Systems. Een bijkomend voordeel: die chip hoeft niet beveiligd te worden. Alles is verder geregeld: de klantrelatie die je toch al had en het plaatsgebonden draadloos in- en uitchecken: op de mobiel zit namelijk een chiplezer. Alles geregeld met een chip van een cent in de muur, en een mobieltje met een lezer.

**Vraag** Had een ICT-instituut, waar de andere inleider ook over spreekt, een debacle als met de OV-chipkaart kunnen voorkomen?

**antwoord** Zonder doorzettingsmacht kun je nooit voorkomen dat projecten van start gaan die te duur zijn, die ondoordacht zijn, die niet pragmatisch zijn, die niet te handhaven zijn, etc. Dus dit soort zaken valt of staat met een autoriteit die onafhankelijk kan oordelen over de business case van een investering, een grote IT-investering inclusief.

Een voorbeeld van hoe dat elders is geregeld is wellicht instructief. In de Verenigde Staten is sinds 1996 een Wet van kracht: de Clinger Cohen Act. Dat is een wet op de besteding van publiek geld aan ICT. Deze wet is gekomen nadat de Senaat in een Congressional hearing had vastgesteld:

poor planning and program management and an overburdened acquisition process have resulted in the American taxpayers not getting their money's worth from the expenditure of \$200,000,000,000 on information systems during the decade preceding the enactment of this Act

In die wet staan een paar heel simpele zaken die debacles zoals met de OV-chipkaart voor hadden kunnen zijn. We geven daar simpel inzicht in via een memo van het Office of Management and Budget van de President van de Verenigde Staten. We citeren het relevante gedeelte:

Investments in major information systems proposed for funding in the President's budget should support work processes that have been simplified or otherwise redesigned to reduce costs, improve effectiveness, and make maximum use of commercial, off-the-shelf technology.

Hier staat in principe dat je voordat je aan de haal gaat met iets als de OV-chipkaart voor miljarden Euro's je eerst het werkproces moet versimpelen of op de één of andere manier moet herontwerpen. Dat is een cruciale eis die in de VS ligt op toestemming voor dit soort investeringen vanuit de federale overheid. Per deze eis, plus één of ander onafhankelijk orgaan die dit soort eisen toetst was zowel de encryptie als ook het verbatim omzetten van een papieren treinkaart en strippenkaart naar een chipkaart tegen het licht gehouden. Dan was wellicht ook aan het licht gekomen dat dit concept weliswaar in Hong Kong geslaagd was maar dat het in Australië niet goed verliep. Sterker, daar is de stekker uit het project getrokken ondanks het feit dat de chipkaart beter beveiligd was.

Kortom: met extra regelgeving rond grote (ICT)-investeringen en een onafhankelijke autoriteit die daaraan toetst kun je dit soort grote debacles voorkomen.

**Vraag** En hoe hadden we dat dan moeten inrichten?

**antwoord** Onafhankelijkheid, 100% toegang tot alle bronnen zowel op papier als mensen, wet- en regelgeving die een kader stelt, zijn ingrediënten waar je aan moet denken bij het inrichten van een dergelijke autoriteit.

**Vraag** Is door aanvulling, meer bevoegdheden, toevoeging van deskundigheid, het College Bescherming Persoonsgegevens tot deze ICT-autoriteit op te waarden of moet dat afzonderlijk?

**antwoord** De specifieke deskundigheid die nodig is voor allerlei uiteenlopende investeringen noopt tot een kleine kern van vaste mensen die gepokt en gemazeld is in het toetsvak. Dit moet worden aangevuld met ad hoc deskundigheid op specifieke deelgebieden. Verder is het nodig om ingewikkelde harde techniek soepel te kunnen vertalen naar voor bestuurders begrijpelijk niveau. Voorbeelden van dit soort gremia met andere taken/doelen zijn de Wetenschappelijke Raad voor het Regeringsbeleid of de Onderzoeksraad voor Veiligheid. De voorziene taken overstijgen die van het CBP, maar het CBP zou afnemer kunnen zijn van en deskundigen op privacy gebied kunnen leveren aan een dergelijke ICT autoriteit.

**Vraag** En als je dat afzonderlijk doet is het dan niet een toezichthouder op het bredere terrein van de bedrijfsvoering waar ICT een geïntegreerd onderdeel van is? En waar hebben we het dan precies over, dan wordt het wel heel erg ruim.

**antwoord** ICT-investeringen kennen een hoog afbreukrisico, hoger dan andersoortige investeringen. Een civiel-technische installatie wordt zelden afgeschreven omdat deze achteraf niet gerealiseerd blijkt te kunnen worden. ICT-systemen in wording, worden meer dan eens afgeschreven. Uitbreiding die voorstelbaar is, is kijken naar grote investeringen in het algemeen, maar liefst te beginnen bij die investeringen die keer op keer in hoofdpijndossiers veranderen. Helaas is dat maar al te vaak als ICT in het spel is.

**Vraag** Wij hoeven de ICT systemen niet te bouwen, wij controleren de bouwers. We werken wel aan wetgeving mee op dat punt. Dat is een onderdeel dat weinig beschreven is in de notities. Kan daar verder op ingegaan worden?

**antwoord** De eerste opmerking is, dat door het maken en evolueren van wet- en regelgeving dat direkt impact heeft op het bouwen en evolueren van de ICT ondersteuning die daarbij hoort. Voor het idee, je hebt zo meer dan duizend mensen nodig om de systemen van de Belastingdienst in de lucht te houden, laat staan als er wijzigingen komen. Een boodschap aan de politiek is dan ook: vraag je bij elke wet af of dat niet (enorme) repercussies heeft op de ICT-landschap van de overheid.

Dan is de volgende opmerking: het controleren van de bouwers gebeurt kennelijk onvoldoende, gegeven het systematisch falen. De middelen zijn wel ter beschikking, zie het Besluit IVR 1990 waar een contra-expertise in geregeld is.

Dan het maken van wetgeving omtrent ICT. De trend is minder wet- en regelgeving, de regeldruk moet omlaag. De constatering die je moet maken door het aanhoudend falen van ICT-projecten bij de overheid noopt toch tot een andere houding. De VS ging ons voor in 1996 met de Clinger Cohen Act. Het valt te overwegen om de kern van die wet tegen het licht te houden. Dat zijn Raine's Rules waar 8 simpele stelregels in staan die allen moeten gelden voor een ICT investering. We zagen er al een over herontwerpen van het werk proces voordat je gaat automatiseren. Een ander voorbeeld is deze:

Investments in major information systems proposed for funding in the President's budget should be undertaken by the requesting agency because no alternative private sector or governmental source can efficiently support the function.

Daarmee was rekeningrijden afgeschoten door een ICT autoriteit ten faveure van het verder uitbuiten van trajectcontrole. We weten namelijk al wie, waar en wanneer rijdt: dat heet trajectcontrole. We sturen nu alleen een rekening als men te hard rijdt, maar je kunt natuurlijk ook altijd een rekening sturen. De infrastructuur staat er al, de klantrelatie is er al via de Belastingdienst, en in Londen werkt het ook al zo.

**Vraag** Dit structureel toezicht, wie zou dat moeten doen en hoe zou je dat moeten regelen zodat het effect heeft?

**antwoord** Zie eerdere antwoorden.

**Vraag** Kennis en kunde omtrent aanbestedingen ontbreekt. Op welke wijze is dat te verbeteren?

**antwoord** Aanbesteden op kwaliteit is een hoofdpijn dossier. Het is niet toegestaan om aan te besteden op past performance. Terwijl je dat privé juist wel doet. Een alle-daags voorbeeld. Je hebt een ruitje stuk en weet niet wie dit kan maken. De buurman had dit laatst ook aan de hand. Je vraagt of dat naar wens is verlopen, zo ja, ben je snel klaar zo nee, neem je een ander. Dit nu mag niet. Bedrijven die aantoonbaar zaken goed of beter kunnen en een lager faalrisico hebben zijn uiteindelijk goedkoper dan bedrijven die stunten met lage uurlonen en die uiteindelijk geen werkend systeem opleveren. Nadenken over hoe past performance op een eerlijke manier kan worden ingebed in het Europees aanbestedingsrecht is een optie.

Naast het ontberen van zaken als past performance, wat innovatie en kwaliteitsverhoging stimuleert is er ook een verbetering mogelijk in het huidige stelsel. Inkopen van ICT vergt tegenwoordig investment management, niet de laagste prijs. Dat vergt ander inkoopgedrag en dito rollen voor probleemeigenaren, inkopers, economen en juristen. Hier is dus een systemische verandering noodzakelijk.

**Vraag** Als er iets heel simpel kan, hoe kan dat dan? Hoe functioneren blijkbaar mechanismen dat simpele dingen niet kunnen?

**antwoord** We zagen al als voorbeelden de OV-chipkaart die je ook omgekeerd kunt implementeren: chip in de muur en kaartlezer in de pocket. We zagen ook voorbij komen het rekeningrijden: geen kastjes in de auto en infrastructuur langs de weg maar de bestaande middelen gebruiken van de trajectcontrole en niet alleen een rekening sturen als men te hard rijdt, maar altijd. Zo is er ook het Elektronische kinddossier. Dat faalde tegen 9.6 miljoen na rechtszaken over de aanbesteding. Waar was het om begonnen? Nooit meer een maasmeisje. De politie te Assen heeft daar iets op gevonden: zij vinken elke keer als een kind met de politie in aanraking komt en als dat te vaak gebeurt in korte tijd dan gaat het dossier naar de jeugdzorg. Die krijgt daardoor deze kinderen in risicogezinnen veel eerder in beeld. Dat vinklijstje kost een fractie van een dossier voor alle kinderen. We zoeken naar die paar procent met een verhoogd risico, maar we registeren iedereen en de functionaliteit dijt uit tot megalomane proporties. Of het Elektronisch Patiënten Dossier. Waarom was het begonnen? Contra-indicaties bij het voorschrijven van medicijnen om onnodige slachtoffers van medische missers voor te zijn. Wat heb je hiervoor nodig? Recente gegevens over wat een patiënt voorgeschreven heeft gekregen. Daar is een bestaand systeem voor waar momenteel 89.7% van de huisartsen op is aangesloten, waar 83.4% van de apothekers op is aangesloten, en 83.8% van de ziekenhuizen op is aangesloten<sup>6</sup>. Dit systeem is bedoeld voor het verhogen van de effectiviteit en efficiëntie van de administratieve stromen tussen zorgverleners en zorgverzekeraars. Aanhaken op die ontwikkeling lijkt toch een beter idee dan een systeem ernaast bedenken. En zo zijn er vele voorbeelden.

Niets staat het uitvoeren van projecten onder een minder optimaal gesternte in de weg zo lijkt het. Niemand is kennelijk bij machte om dit soort projecten een halt toe te roepen. Het begin van een antwoord is toch om dit soort plannen te toetsen met de doorzettingsmacht om zeer krachtig te kunnen bijsturen. Dat toetsen zou via een ICT-autoriteit kunnen. De vraag is echter waar de doorzettingsmacht zit die de budgetten

<sup>6</sup>Cijfers actueel per 4 november 2010: [http://www.vecozo.nl/web/download.aspx?bin=aansluitingen\\_vecozo](http://www.vecozo.nl/web/download.aspx?bin=aansluitingen_vecozo)

alloceert of bevriest. Er zijn draconische methodes met de huidige wet- en regelgeving: een project kan onder financieel toezicht worden gesteld maar daar is de regeling niet voor bedoeld.

Kortom, één of andere vorm van niet vrijblijvende afspraken lijkt hier toch op zijn plaats. Hoe dat precies moet: wet- en regelgeving, of iets anders laat ik graag aan anderen.

**Vraag** Zou dit komen doordat we als overheid meer redeneren vanuit de elektronische overheid in plaats van uitgaan van de elektronische burger? Dus kijken vanuit de vraag van de burger.

**antwoord** De problemen ontstaan niet zozeer door vraag gestuurd of aanbod gestuurde ICT-investeringen. De problemen ontstaan doordat er weinig tot geen tegengas kan worden gegeven bij n'importe welke investering dan ook.

Daarnaast is het zeer onverstandig om investeringen te doen waar de gebruikers onvoldoende bij betrokken zijn. De kans is dan groot dat de innovatie niet wordt geaccepteerd. Dat zien we ook wel eens, bijvoorbeeld met het hoger beroep strafrechtstelsel dat faalde tegen 28 miljoen gulden. De vragen die destijds in een algemeen overleg naar voren kwamen, komen ook nu weer naar voren, we citeren uit het verslag van 2002:

Het opzetten van een HBS (hoger beroep strafrechtstelsel) is mislukt. 28 mln gulden is over de balk gegooid. Hoe is het mogelijk dat zo'n groot project zo jammerlijk mislukt? Welke instantie is verantwoordelijk voor de architectuur van dit stelsel, voor de kennis en de gekozen techniek, die niet aansluit bij de werkprocessen en de overige systemen van de gerechtshoven? De hoven moeten nu handmatig de werklastgegevens bijhouden. Hoeveel extra geld moet worden besteed aan de aanpassing van de bestaande systemen in de hoven en wat kost de introductie van een nieuw stelsel bij het hof in Den Haag? Uit publicaties blijkt dat dit laatste te wensen overlaat. Dat gaat ten koste van de rechtspleging. Wat gebeurt er met de appèllen die van de rechtbanken naar de hoven gaan? De minister heeft bij de begrotingsbehandeling al aangegeven dat op geen enkele post nog iets te halen valt. Welk geld zal de minister vrijmaken om de gevolgen van dit echeec tegen te gaan? Het uurtarief van de sociale advocatuur kon niet worden verhoogd en het sobere regime in de cellen kon niet worden opgeheven omdat er te weinig geld was, maar die 28 mln kan niet meer worden gebruikt. Blijkbaar moeten deze wrange vruchten geplukt worden. Kan de minister hierop een overtuigende reactie geven?

De vraag die in 2011 voorliggend is, is gaan we over tot het instellen van die instantie die verantwoordelijk wordt voor het voorkomen van dit soort debacles? In principe is er nu geen instantie die de plannen toetst, die de architectuur toetst, die de methode van ontwikkelen toetst, etc. Een ICT autoriteit met tanden en gezaghebbende deskundigheid kan zonder twijfel dit soort dwalingen voorkomen, opsporen, of een halt toeroepen in een vroeg stadium.

**Vraag** Een aanvullende vraag over de OV-chipkaart. Is de groep die in aanmerking komt voor aanbesteding wellicht te gesloten zodat nieuwe technologie minder snel gebruikt wordt omdat men minder thuis is in de nieuwe technologie?

**antwoord** Je laat de aannemer je huis niet ontwerpen en de architect het niet bouwen. Wat meer en meer gebeurt is dat ontwerp, bouw, onderhoud en beheer, plus soms financiering in één hand komt te liggen. De overheid neemt dan het product af voor pay-per-use of via een fixed rate. Dat mag voor sommige investeringen werken, als ICT in het spel komt zitten er blijkbaar haken en ogen. Door een knip aan te brengen tussen ontwerp en bouw kan voortgang geboekt worden. Als alles in één hand komt krijg je het ontwerp dat het goedkoopst te bouwen is. Wat je wilt is het ontwerp dat de eisen het best gestand doet. Te overwegen valt om eerst een ontwerp aan te besteden (op kwaliteit en niet op prijs) met als uitkomst een uitvoeringsontwerp (zeg een bestek) dat gevalideerd de eisen het beste heeft verwerkt. Dat bestek moet vervolgens gebouwd worden. En dat kun je dan meer op prijs aanbesteden omdat al vast ligt wat precies moet worden gemaakt.

De OV-chipkaart—het woord zegt het al—leidt aan ontwerp myopie: er is meteen een tunnelvisie ontstaan over een kaart met een chip erin die de strippenkaart en de treinkaart moest gaan vervangen. Andere opties waren daarmee uitgesloten. Let wel: dit is een heel dure optie en wie heft er belang bij om te vertellen dat het veel goedkoper kan? Een ontwerp wedstrijd voor het beste idee om draadloos plaatsgebonden te betalen had zeker geleid tot andere en goedkopere opties dan degene die men gebouwd heeft.

Kortom, de partijen, de manier van uitvragen, het gebrek aan toetsingsmomenten, en commerciële belangen zijn allen debet aan de keus zoals die naar voren is gekomen.

**Vraag** De aanbestedingswet heeft minder goede effecten. Dat is al jaren bekend. Er zijn ook initiatieven genomen bijvoorbeeld de pre-competitie fase. Hoe denkt u daarover?

**antwoord** Deze pre-concurrentiële dialoog neemt het probleem niet weg dat ontwerp en bouw van ICT vaak in één hand wordt aanbesteed met alle gevolgen van dien. Het vergt meer creativiteit om ervoor te zorgen dat degenen die het kunnen het werk ook gaan doen, en degenen die het niet kunnen te weren. Dat is een lastig spel waar de pre-concurrentiële dialoog niet bij helpt.

**Vraag** Hoe ga je met elkaar verenigen dat enerzijds de burger maar één keer zijn gegevens vastlegt maar anderzijds dit juist zoveel mogelijk beperkt per wet in verband met privacy.

**antwoord** Het adagium dat de burger de gegevens maar één keer hoeft vast te leggen heeft enorme repercussies op het ICT-landschap, de daarmee gepaard gaande kosten en de sterk toegenomen complexiteit. Bijvoorbeeld, het UWV en de Belastingdienst werden daardoor onderdeel van een keten. Dus we spreken tegenwoordig al heel snel over ketenautomatisering vanwege die ene simpel klinkende eis. Vragen die voorliggend zijn: wat is de toegevoegde waarde van het slechts één keer hoeven vertellen wie je bent, en waar je woont? Is dat het op de schop nemen en het overhoop halen van de overheidsautomatisering waard? Brengt dat meer op dan het kost in termen van geld en risico's?

Dan het volgende punt van de privacy: juist door het centraliseren van privacy gevoelige gegevens ontstaan risico's. Via hacken, social engineering (babbeltrucs om aan informatie te geraken), omkoping, chantage en onoordeelkundig gebruik komen gegevens ongewenst in handen van kwaadwilligen.

De eis van privacy en de eis van één bronadministratie staan op gespannen voet met elkaar.

Laten lekken van gegevens heeft in de VS behoorlijk pittige gevolgen. Per gelekt gegeven kost het je minimaal een bedrag (100 dollar of daaromtrent). En voor de potentiële slachtoffers van identiteitsfraude moet je credit monitoring betalen. Dat kost je handen vol met geld als er ook maar één laptop zoekraakt. Een voorbeeld: er werd een bedrijfslaptop uit een huis gestolen met daarop informatie van miljoenen veteranen. De credit monitoring voor een jaar kostte 160.5 miljoen dollar. Totale kosten van dit debacle liggen met boetes erbij in de honderden miljoenen dollars. Daarmee wordt de business case om scherp op procedures te zijn, om laptops met hoogwaardige encryptie uit te voeren en om gegevensbanken zeer goed te beveiligen een no-brainer. In Nederland roept er iemand: sorry, zal niet meer gebeuren. En dan is het wachten op het volgende lek.

Te overwegen valt om stringente regelgeving in te voeren die fikse boetes zet op dit soort zaken, plus de daarbij behorende credit monitoring. Dat maakt de business case voor privacy hard. Daarmee wordt het ook een echt issue bij systemen waar dit soort gegevens een rol spelen.

**Vraag** Waarom is er op dit moment geen toezicht op de ontwerpen van ICT om privacy te borgen?

**antwoord** Dit haakt aan op de vraag hiervoor. De business case voor privacy is er momenteel niet tot nauwelijks. Dus waarom zou je die privacy dan borgen? Verder zal een ICT-autoriteit moeten toetsen of de privacy in voldoende mate is geborgd.

**Vraag** Zit het probleem niet meer in de domeinkennis dan ICT-kennis? De overheid werkt anders als het bedrijfsleven.

**antwoord** Het probleem zit hem in een gebrek aan kennis en kunde op elk vlak. Een citaat uit het Verenigd Koninkrijk waar men dit ook op grote schaal heeft onderzocht.

A striking proportion of project difficulties stem from people in both customer and supplier organisations failing to implement known best practice. This can be ascribed to the general absence of collective professionalism in the IT industry, as well as inadequacies in the education and training of customer and supplier staff at all levels. Moreover, there is a broad reluctance to accept that complex IT projects have many similarities with major engineering projects and would benefit from greater application of well established engineering and project management procedures. For example, the importance of risk management is poorly understood and the significance of systems architecture is not appreciated.

Need I say more?

**Vraag** Gaat het nu om de toepassing van de regels van het Europees aanbestedingsrecht maar niet de regels zelf?

**antwoord** Zie eerdere antwoorden.

**Vraag** Hoe kijkt Verhoef aan tegen het uitbesteden van grote ICT-projecten zoals in Engeland met de belasting?

**antwoord** Het uitbesteden van grote ICT projecten in het algemeen hoeft geen probleem te zijn. Er zijn voorbeelden bekend van goed lopende uitbesteding. Evenzo zijn er voorbeelden bekend, ook bij de Nederlandse overheid, waar het minder florissant is verlopen. In het geval van de belastingdienst in Engeland was er eerst een contract met EDS waar men kennelijk minder tevreden over was. Daarna is er een contract met Capgemini gesloten met daarin meerdere partijen verenigd.

Het verhaal van de Engelse belastingdienst waar de Kamerleden naar verwijzen is opgesteld in opdracht van een deelvertegenwoordiging van de leveranciers. Meer precies de onderzoeksopdracht was om twee *vooraf geselecteerde succesvolle trajecten* te beschrijven. Op basis van dit onderzoek komt men tot aanbevelingen over uitbesteding in Nederland. Dit onderzoek geeft *geen inzicht in de algehele praktijk van ICT uitbesteding* laat staan inzicht in hun faal- en slaagkans. De aanbevelingen moeten dan ook in dat licht worden gezien.

Results	Percent of Outsource Arrangements
Both parties generally satisfied	70%
Some dissatisfaction by client or vendor	15%
Dissolution of agreement planned	10%
Litigation between client and contractor probable	4%
Litigation between client and contractor in progress	1%

Tabel 1: Verdeling van uitbestedingsresultaten na 24 maanden in de VS.

Ter vergelijking wat onderzoek uit de Verenigde Staten over (on)tevredenheid met ICT uitbesteding. Tabel 1 is overgenomen uit [2, Table 1]. Het toont de kans op geschillen na 24 maanden bij outsourcing in de Verenigde Staten. We zien dat na 24 maanden al 10% het plan heeft om de overeenkomst te ontbinden, 4% acht het waarschijnlijk dat geschillen gaan optreden en in 1% van de gevallen is dit reeds aan de hand.

project outcome	project size expressed in function points			
	< 100	100–1000	1000–5000	> 5000
canceled	3%	7%	13%	24%
late by > 12 months	1%	10%	12%	18%
late by > 6 months	9%	24%	35%	37%
approximately on-time	72%	53%	37%	20%
earlier than expected	15%	6%	3%	1%

Tabel 2: Resultaten van software projecten waar uitbesteding een rol speelde opgedeeld naar omvang.

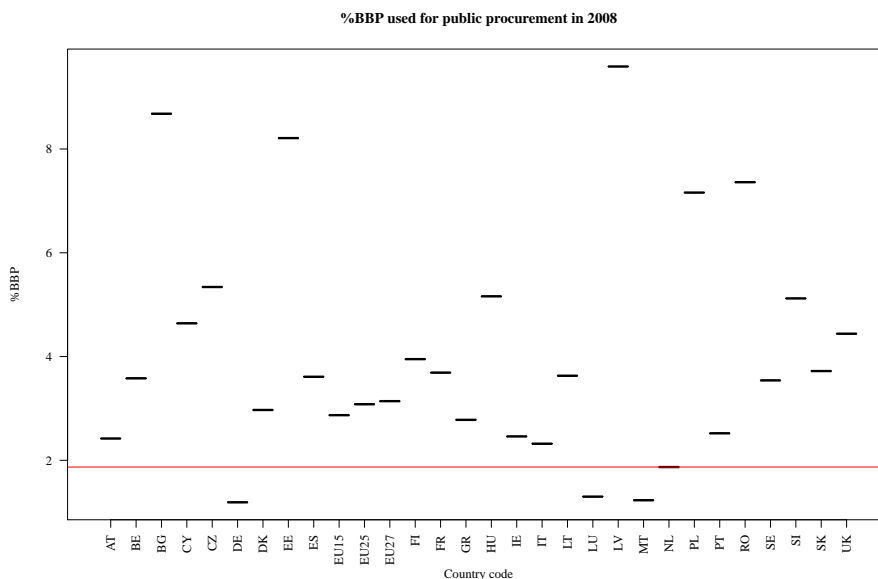
Dan zijn er ook verschillen tussen kleinere en grotere uitbestedingstrajecten. Ook daar is al onderzoek naar gedaan. We geven dat weer in Tabel 2 (overgenomen uit [1, Table 1]). De tabel laat duidelijk zien dat als systemen groter worden (dit wordt uitge-

drukt in zogeheten functiepunten<sup>7)</sup> dat adequate oplevering slechts plaatsvindt in 21% van de gevallen. De faalkans is 24% en het risico op flinke tijdoverschrijdingen is significant: 55% kans op zes maanden vertraging of meer.

De les die we hieruit trekken is dat je prima na kunt denken over ICT uitbesteding maar dat het niet de oplossing is voor de problemen die de overheid momenteel heeft met ICT.

**Vraag** Hoe is de uitbesteding van ICT in andere landen georganiseerd?

**antwoord** Tijdens deze discussie kwam het cijfer 46% naar voren dat steller dezes recentelijk had vernomen van een topambtenaar. Het zou zo zijn dat van alle gelden die in geheel Europa publiek werden aanbesteed, Nederland 46% voor haar rekening neemt. Kamerlid Heijnen had dit cijfer ook gehoord. Na de bijeenkomst heb ik dat cijfer gecontroleerd omdat een journalist naar de bron vroeg.



Figuur 1: Value of public procurement which is openly advertised, as a percentage of GDP (2008).

Het is één van de structurele indicatoren die letterlijk van Eurostat te halen is, dus er was geen vermoeden dat het cijfer kon rammelen. Toch bleek dat het cijfer niet klopt. In Figuur 1 zijn de Eurostat gegevens samengevat. Horizontaal staan de landcodes, en verzamelscodes zoals de 15 EU lidstaten. Verticaal staat het percentage BBP dat voor openbare aanbestedingen geadverteerd is. Nergens komt de lijn uit op 46%. De rode lijn is Nederland met 1.87% van het BBP, waarmee Nederland in de laagste regionen zit (nog niet eens in het eerste kwartiel). De topambtenaar is ingelicht over de discrepantie tussen het genoemde cijfer en de gegevens op Eurostat. Wie weet horen we nog wat de 46% precies behelst.

<sup>7)</sup>Een functiepunt is de kubieke meter van de IT-bouw.

Dan een antwoord op de vraag over hoe uitbesteding in andere landen is georganiseerd. Er is mij niets bekend over significant andere praktijken rond uitbesteding van ICT in andere landen waarbij er andere slaag- en faalkansen optreden dan wat we in Nederland zien. Het onderzoek met de twee vooraf gekozen succesverhalen is pertinent geen voorbeeld van dergelijk onderzoek.

**Vraag** Als de overheid met een beperkt aantal bedrijven zaken doet, dan kunnen daar bepaalde effecten optreden. Bijvoorbeeld geen gebruik maken van de nieuwste en innovatieve technologie. Wat is de mening van Verhoef, is dit een probleem of niet?

**antwoord** Bij een aanbesteding door de overheid is de vraag die je je moet stellen waarom bepaalde partijen niet hebben geboden in plaats van welke wel hebben geboden. Omdat in de praktijk aanbesteding van ICT-intensieve projecten of diensten op prijs uitgevochten worden, en omdat het in meerjarige mantelovereenkomsten om significante bedragen gaat, gaan leveranciers wel eens te ver in hun toezeggingen. Bedrijven die het diepst gaan hebben het geld het hardst nodig. Dat is niet altijd de beste leverancier (the winner's curse).

Het uurtarief van de ICT'er kan daardoor in een vrije val geraken. Tarieven van 20-40 Euro per uur komen al voor. Voor dat geld gooit elke loodgieter schaterend de hoorn op de haak, maar de overheid denkt daarmee kenniswerkers in de ICT te kunnen krijgen. Dat is een misvatting en daardoor krijgen we kromme constructies waar uren in lage lonen landen worden gemaakt met alle risico's van dien. Een voorbeeld. Specificaties worden van het Nederlands naar het Engels vertaald (zonder inhoudelijke controle want dat kost teveel), systemen worden verkeerd geïnterpreteerd maar toch gebouwd. En er wordt dan weer van het Engels terugvertaald naar het Nederlands (eveneens zonder controle op inhoudelijkheden). Communicatie verloopt zeer traag, kennisborging is een probleem omdat iedere programmeur in dergelijke landen meteen overstapt als er een dollar meer te verdienen is bij de concurrent (geen secundaire arbeidsvoorwaarden), en de kwaliteit is vaak ondermaats. Uiteindelijk is de prijs die de klant betaald flink hoger dan je zou denken op grond van de voorgespiegelde uurtarieven. Het is kennelijk heel verleidelijk maar tevens ook heel kortzichtig om op basis van uurtarieven te gunnen.

Men kan veel beter op andere indicatoren zoals productiviteit gunnen. Een civiel voorbeeld. Een aannemer die mensen heeft die voor 20 Euro per uur komen werken klinkt aantrekkelijk. Als nu blijkt dat men bouwt tegen 500 uur per kuub, dan ligt de kubieke meter prijs op 10000 Euro. Het uurtarief is zeer laag maar de productiviteit is onacceptabel. Een aannemer die 75 Euro per uur rekt, maar die tegen 20 uur per kuub werkt, heeft een prijs per kuub van 1500 Euro. In de bouw weten we dat je niet naar uurtarieven maar naar de prijs per kuub moet kijken. Dat kun je ook overwegen in de IT bouw. Uiteraard is kwaliteit in de civiele bouw gebonden aan wet- en regelgeving. Dat kun je ook overwegen in de IT-bouw: prijs per functiepunt bijvoorbeeld. Daarnaast moet je net als in de civiele bouw een normenkader opleggen dat reeds bestaat maar niet vaak wordt opgenomen in contracten (kennisgebrek).

**Vraag** Er is te weinig geld voor onderwijs. Wij geven jaarlijks zoveel geld uit aan ICT en alleen al van de faalkosten moeten heel veel mensen op te leiden zijn. Waarom gebeurt dit niet? Waarom is die kennis en kunde er niet? Krijgen we wel waar voor ons geld bij inhuur van dure consultants?

**antwoord** Dit dilemma is ooit door Derek Bok, decaan van Harvard University, eloquent samengevat:

**If you think education is expensive, try ignorance.**

Kamerlid Koopman heeft volkomen gelijk dat van de ICT-faalkosten alleen heel veel vakmensen in de ICT op te leiden zijn. Dat zal inderdaad geld kosten, maar het kennisgebrek kost een veelvoud. Evengoed kun je meer blauw op straat regelen van dat geld, of meer verpleegzorg.

De vraag die je je moet stellen is wat je zoal moet doen om deze verspilling tegen te gaan. Dat zal investeringen kosten, en niet voor de korte termijn. Daar zijn we wel wat laat mee. Een voorbeeld uit de Verenigde Staten. Daar stelde men in 1999 al vast dat de VS door niet genoeg in ICT onderwijs en onderzoek te investeren in grote problemen zou geraken. Dit werd geconcludeerd door het PITAC (President's Information Technology Advisory Committee). Op zich ziet men hier al dat er een hoog adviesorgaan is dat de politiek op het hoogste niveau adviseert over ICT. Iets dergelijks zou in Nederland ook niet misstaan. We citeren twee alinea's uit hun rapport van 1999.

After careful review of the Federal programs this Committee has concluded that Federal support for research in information technology is seriously inadequate. Research programs intended to maintain the flow of new ideas in information technology and to train the next generation of researchers are funding only a small fraction of the research that is needed, turning away large numbers of excellent proposals. Compounding this problem, Federal agency managers are faced with insufficient resources to meet all research needs and have naturally favored research supporting the short-term goals of their missions over long-term high-risk investigations. While this is undoubtedly the correct local decision for each agency, the sum of such decisions threatens the long-term welfare of the nation.

The Nation needs significant new research on computing and communication systems. This research will help sustain the economic boom in information technology, address important societal problems such as education and crisis management, and protect us from catastrophic failures of the complex systems that now underpin our transportation, defense, business, finance, and healthcare infrastructures. If the results are to be available when needed, we must act now to reinvigorate the long-term IT research endeavor and to revitalize the computing infrastructure at university campuses and other civilian research facilities, which are rapidly falling behind the state of the art. If we do not take these steps, the flow of ideas that have fueled the information revolution over the past decades may slow to a trickle in the next.

Hier geeft men duidelijk aan dat de maatschappij essentieel afhankelijk is geworden van ICT, dat de toenmalige investeringen "seriously inadequate" waren, en dat het daarmee van groot belang is om de kennis en kunde weer op het peil te krijgen dat nodig is voor de uitdagingen waar het land voor staat. Dit is in Nederland niet veel anders. Ook in ons land is software de onzichtbare motor van de economie. Zet essentiële computers uit, en het land komt knarsend tot stilstand.

Het geld dat gemoeid is met falende ICT, het geld dat je betaald aan dure consultants wordt door die leveranciers niet geïnvesteerd in onderwijs en onderzoek naar

ICT. Te overwegen valt om een pakket van maatregelen te nemen zoals dat is opgesteld in het PITAC rapport. De rode draad zou moeten zijn om duurzaam te investeren in ICT onderwijs en ICT onderzoek. Hoe precies zal apart onderzoek vergen.

## **Referenties**

- [1] C. Jones. Conflict and Litigation Between Software Clients and Developers, 1996. Version 1 – March 4. Technical note.
- [2] C. Jones. Conflict and Litigation Between Software Clients and Developers, 2001. Version 10 – April 13. Technical note.