

ICT en maatschappij, afhankelijk maar wel weerbaar

Verslag van de haardvuursessie van 20 november 2003

Deelnemers in de binnenkring:

- Mr. Marcel van Eck, projectleider Bescherming Vitale Infrastructuur (ministerie van Binnenlandse Zaken)
- Dr. Valerie Frissen, senior onderzoeker ICT en Sociale Verandering (TNO-STB) en bijzonder hoogleraar ICT en Sociale Verandering bij de Erasmus Universiteit Rotterdam, Faculteit der Wijsbegeerte
- Drs. Jan Nekkers, directeur FutureConsult bv, bureau voor scenariostudies en toekomstverkenningen
- Dhr. Willem Blanken, directeur Enterprise & Partnergroup, Microsoft Nederland

Moderator

- Dhr. Eric van der Want, partner f-fectis, management adviseurs

Verslag

Oude en nieuwe risico's van de informatiesamenleving

ICT raakt steeds verder ingebed in de Nederlandse samenleving. Het is doorgedrongen tot in de haarvaten van de samenleving die daarmee steeds afhankelijker wordt van een goed functionerende ICT. Maar wat gebeurt er als deze verstoord raakt of uitvalt? Is de Nederlandse samenleving door het ICT gebruik kwetsbaarder geworden?

Nee, zegt het Rathenau Instituut. Hoewel er zich regelmatig incidenten voordoen, zijn de gevolgen niet zo groot dat sprake is van maatschappelijke ontwrichting. Wel zorgen ze voor grote ongemakken en aanzienlijke schadeposten. Maar van een toegenomen maatschappelijke kwetsbaarheid door ICT is geen sprake.

Door de grote complexiteit van digitale systemen en de onderlinge verwevenheid is de kans echter alles behalve denkbeeldig dat zich op termijn wel ernstige verstoringen voordoen die een ontwrichtende werking hebben.

De eerste reactie op deze resultaten van Rathenau onderzoek komt van **Jan Nekkers**. Hij vindt het allemaal te somber. *"Ik wil graag een wat optimistischer visie uitdragen. ICT is niets anders dan de beheersing van de natuur door de mens. Het maakt het leven gemakkelijker en aangenamer. Maar omdat we de eisen hoger leggen, is de teleurstelling ook groter als het eens een keertje misgaat. Technologie conditioneert en beïnvloedt ons gedrag. Je moet daarom een voortdurend debat voeren over de grenzen die ICT aan ons stelt. Het gaat eigenlijk om de vraag of jij de techniek beheerst of dat de techniek jou beheerst."*

Valerie Frissen brengt in haar bijdrag aan het debat een nuancering aan bij het begrip 'Maatschappelijke ontwrichting'. Ook zij vindt de insteek van de discussie vaak te somber: *"Ontwrichting hoeft niet per definitie negatief te zijn. We moeten dat een beetje creatief zien. Als het veiligheidsbeleid niet in staat is om in te spelen op het gedrag van mensen - zoals bijvoorbeeld in de virtuele wereld - dan kunnen we dat ontwrichting noemen, maar we kunnen*

het ook als het vertrekpunt beschouwen voor nieuw beleid. Bovendien lijkt het teveel op een rampscenario terwijl veel ontwikkelingen sluipenderwijs gaan."

Volgens **Willem Blanken** kan technologie mensen ook weerbaarder maken. *"Je moet het in context zien: in welke omgeving wil je technologie probleemoplossend inzetten. Maar alle technologie kan falen en daarom is risicoanalyse zo belangrijk."*

Volgens **Marcel van Eck** moet de burger beseffen dat hij in een risicomaatschappij leeft. *"Hij moet er weer rekening mee houden dat de kachel uit kan vallen, en voor alle zekerheid een deken in huis hebben."*

Kortom, 'ontwrichting' is een te zware term. Waar het om gaat is dat mensen met technologie proberen structuur op te leggen aan de natuur. Daarmee leggen ze tegelijkertijd ook zichzelf grenzen op. Mensen creëren zo hun eigen afhankelijkheid. Door iemand uit de zaal wordt een bekend voorbeeld genoemd: als de trein niet rijdt, ervaren mensen dat als vervelend, als ongemakkelijk of zelfs als ontwrichtend. Veel mensen staan dan met de handen in het haar. Ze zijn afhankelijk geworden van de trein en hebben niet zo snel een alternatief ter beschikking, maar dat wil natuurlijk niet zeggen dat het er ook niet is.

Bescherming vitale infrastructuur

Door de overheid is in april 2002 het project Bescherming Vitale Infrastructuur gestart met als doel een samenhangend pakket beschermingsmaatregelen te ontwikkelen, dat de vitale infrastructuur veiliger maakt. Het bedrijfsleven speelt hierbij een belangrijke rol.

Projectleider **Marcel van Eck** over het project: *"De eerste stap was het in kaart brengen wat nu eigenlijk die vitale infrastructuren zijn. Daarbij kwamen elf sectoren naar voren, waaronder de energievoorziening maar ook transport en logistiek, voedselvoorziening enzovoort. Vervolgens werd onderzocht hoe deze sectoren met elkaar verweven en van elkaar afhankelijk zijn. Daarbij bleek dat ICT en elektriciteit als rode draden overal doorheen lopen. Een verstoring van ICT of energie kan dus een grote impact hebben op veel vitale sectoren in de samenleving."*

Het project zit inmiddels in de tweede fase bezig waarbij de kwetsbaarheid van de knooppunten in kaart worden gebracht. *"Daarbij houden we rekening met de impact die een verstoring heeft op zowel nationaal als internationaal niveau, of er veel slachtoffers te verwachten zijn en in hoeverre er alternatieven bestaan om op terug te vallen. Uiteindelijk moet dit de vraag helpen beantwoorden welke veiligheidsmaatregelen er moeten zijn. Een aantal terreinen is voor de overheid bovendien extra belangrijk: veiligheid, handhaving van de rechtsorde en de economie."*

De uiteenzetting van Van Eck wordt met goedkeuring ontvangen in de zaal. Er worden wel een aantal kanttekeningen bij geplaatst. Zo wordt opgemerkt dat het risico van een verstoring bestaat uit de kans op een verstoring maal het effect (risico = kans x effect). Maar de notie 'kans' uit dit rekensommetje leeft nog onvoldoende. Te gemakkelijk sussen mensen zichzelf in slaap door te zeggen dat iets niet kán gebeuren, omdat het nooit ís gebeurd.

Door de zaal wordt geopperd om meer aandacht te besteden aan onverwachte voorvallen en daarvan te leren. Net zoals luchtvaartautoriteiten een vliegtuigongeluk uitgebreid analyseren om een volgend ongeluk te voorkomen zou van de huidige ICT verstoringen geleerd kunnen worden om toekomstige kwetsbaarheden te voorkomen..

Als het over ontwrichting gaat is het bovendien belangrijk onderscheid te maken tussen de gepercipieerde ontwrichting en de werkelijke maatschappelijke ontwrichting. Deze kunnen nogal uiteen lopen. Neem een ziekte als SARS. Hoewel het reële gevaar mee viel, voelden veel mensen zich onveilig. De ziekten die de krantenpagina's vullen zijn lang niet altijd de meest ernstige. Maar de beleving van de burger is wel van invloed op zijn vertrouwen in de technologie.

Het gebruik van ICT

Valerie Frissen onderzoekt het vertrouwen dat mensen hebben in de technologie aan de hand van de manier waarop men dagelijks met ICT en internet omgaat. Nu veel mensen toegang hebben is het tijd te kijken wat ze er eigenlijk mee doen en welke risico's dat met zich meebrengt. Het is eenvoudig gezegd, maar zo'n onderzoek valt in de praktijk niet mee. Aan het gebruik van ICT zitten namelijk zowel goede als kwade kanten.

Als voorbeeld hiervan noemt **Valerie Frissen** het artikel dat een columnist van de treinkrant Metro had geschreven over Greta Duisenberg. Het blad moest van de rechter een rectificatie plaatsen en de columnist werd gesommeerd het artikel van zijn website te halen. Dat deed hij maar het effect was dat allerlei webloggers de column op hun eigen website plaatsten. *"Het is een onbeheersbaar proces. Juridisch is er niets tegen te doen. Er is zo veel maatschappelijke turbulentie waardoor normen en waarden steeds veranderen en het is maar de vraag of het recht dat allemaal wel kan bijbenen. Een effectief veiligheidsbeleid moet met die turbulentie kunnen omgaan."*

De ouderwetse hackersmentaliteit is volgens **Valerie Frissen** eveneens een mooi voorbeeld. *"Vroeger waren hackers min of meer aanspreekbaar op hun gedrag. Ze hackten dikwijls uit ideologische motieven en legden tegenover elkaar verantwoording af over wat ze deden. Maar door de democratisering van de technologie zijn de ouderwetse hackers vervangen door de 'script kiddies.' Zij hacken puur voor de lol en zijn nauwelijks aanspreekbaar op hun gedrag. Dat kan grote gevolgen hebben"*.

"Dergelijke ontwikkelingen moeten we goed in de gaten houden. In scenario's moeten we rekening houden met dit soort risicogedrag. Burgers zoeken de grenzen op en overschrijden ze. Voor je het weet hebben we te maken met onbereikbare burgers. Dat is een doemscenario. Maar het kan ook zo zijn dat burgers zich met behulp van de technologie afzonderen en veiligheid op zoeken, dat ze zich ontwikkelen tot beheersbare burgers. Het is heel moeilijk om op dit soort ontwikkelingen in te spelen, maar we moeten er wel degelijk op voorbereid zijn. Ook omdat de grens tussen de uitersten steeds dunner wordt."

Daarbij speelt opnieuw de beleving van mensen een grote rol. De mate waarin mensen zich afhankelijk voelen van de technologie is bepalend voor het vertrouwen dat ze er in hebben. Tegelijkertijd is het echter weer zo dat gebruikers die zeggen zich afhankelijk te voelen van de technologie, hun handen er niet voor omdraaien zelf aan die technologie te knutselen.

Willem Blanken stipt een ander dilemma aan: de afnemende meerwaarde van innovaties: *"Verdere ICT innovatie kan een deel van de bestaande kwetsbaarheden en onzekerheden wegnemen. Technologische systemen worden gaandeweg steeds beter. Maar er ontstaat een kloof tussen het toepassen van innovaties en de bestaande systemen. De industrie moet steeds meer moeite doen om innovaties te verkopen. De gebruiker wil graag de ontwikkelingen bijhouden, maar het gaat soms wel heel erg hard. De technologische ontwikkelingen gaan door, maar de maatschappelijke acceptatie van nieuwe technologieën loopt steeds meer*

achter. Als je niet oppast, kom je in een spiraal terecht waarin de meerwaarde van de innovatie steeds minder wordt."

Verwachtingen voor de toekomst

Om meer zicht te krijgen op de wijze waarop mensen omgaan met aan ICT gerelateerde risico's heeft het Rathenau Instituut een aantal scenarioworkshops georganiseerd waarbij mensen met verschillende achtergronden van gedachten wisselden over verwachte risico's van ICT en internet. Een van de casestudies die daarbij besproken werden ging over de digitalisering van de Gemeentelijke Basisadministratie voor Persoonsgegevens (GBA) en de digitale dienstverlening door de overheid.

In deze scenarioworkshop kwam naar voren dat persoonsidentificatie een kerntaak van de overheid is. Daarvoor moet je één gezaghebbende instantie hebben. Voor de documenten die je daarvan afleidt maakt het niet uit. Of je paspoort nou van de overheid komt of van Johan Enschedé, maakt geen verschil. Maar je ziet dat de rollen door elkaar gaan lopen. De Belastingdienst wil dat bedrijven digitaal aangifte gaan doen en daar is authenticatie voor nodig. De Belastingdienst controleert vervolgens deze gegevens aan de hand van informatie van de bank. Je ziet de rollen verwisselen: de functie van de overheid is aan het veranderen.

Jan Nekkers: *"Stel je voor dat het centrale systeem van de overheid gehackt wordt en alle gegevens komen op straat te liggen, dan is er geen alternatief systeem waarop je kan terugvallen. Het is niet als bij een creditcardmaatschappij, waar je altijd kunt terugvallen op je bankrekening of op cashgeld. Daarnaast bestaat ook het risico dat iemand die gelegitimeerd is om het systeem te gebruiken er misbruik van maakt.*

Valerie Frissen: *"Het is een trend binnen het beleid om door middel van grote gesloten systemen de illusie van beheersbaarheid te geven. Burgers zijn geneigd daarin een heel eind mee te gaan. Maar uiteindelijk zal het voor zowel de burger als de overheid het paard van Troje blijken te zijn. Het is namelijk niet beheersbaar.*

Een alternatief voor één centrale database met gegevens zijn de 'trusted communities'. Doordat binnen een gemeenschap mensen elkaar kennen, kunnen ze elkaar identificeren. Zo is bijvoorbeeld iemand een leraar, omdat hij in een schoolgebouw rondloopt en de leerlingen en de andere docenten hem kennen als leraar."

Ook elders in de samenleving werkt dit principe. Een handtekening wordt geaccepteerd, hoewel ze nergens geregistreerd is; in bepaalde gevallen wordt geaccepteerd dat iemand de persoon is die hij beweert te zijn, omdat hij een bankpasje kan laten zien waarop dat staat. Zo gaat het ook in de elektronische omgeving gaan. Het principe blijft hetzelfde, alleen de vormgeving wordt anders. De overheid zou dan als taak hebben het proces te controleren. Uiteindelijk is het bankpasje ook ooit afgeleid van een centrale administratie. Als vanzelf komt de discussie hiermee terecht bij de vraag wie nu eigenlijk waarvoor verantwoordelijk is.

Doemscenario

Iemand uit de zaal houdt de leden van de binnenkring een doemscenario voor, waarin het internet volledig dichtslibt. Het aantal megabytes dat verzonden wordt, groeit namelijk zo snel dat de infrastructuur het niet meer aan kan. Het gevolg is dat de hele boel vastloopt, tenzij nu als een razende nieuwe kabels worden neergelegd. Als dat geen maatschappelijke ontwrichting is! En de kans dat het gebeurt is reëel, dus wat te doen?

Willem Blanken: *"Dat is inderdaad wel behoorlijk doemdenken. Als het zou gebeuren is het zeker ontwrichtend, maar ik geloof er niet zo in. Iets dergelijks is ook al eens gezegd over*

zoekmachines, dat die het allemaal niet meer aan zouden kunnen. En juist op het moment dat het dan echt zou mislopen, kwam Google met een nieuwe zoekmethode. Elk nieuw probleem leidt vanzelf tot een technische oplossing.”

Valerie Frissen: *“Uit het rapport van het Rathenau Instituut trek ik de conclusie dat een dergelijk scenario niet voor de hand ligt. Er zal natuurlijk een enorme chaos ontstaan als het internet vastloopt, maar er zal ook een nieuwe oplossing gevonden worden. Het zal trouwens niet zo’n vaart lopen met het dichtslippen van het internet. In Amerika heb je nu een trend dat steeds meer oude, ervaren gebruikers zich van internet afkeren, vanwege de congestie en de spam.”*

Willem Blanken signaleert het probleem dat mensen onvoldoende vertrouwen hebben in het functioneren van ICT en internet en stelt dat de overheid daarbij een belangrijke vertrouwenwekkende rol heeft te vervullen. *“De overheid moet op de een of andere manier vertrouwen en veiligheid van ICT en internet kunnen garanderen. Dat is van groot belang voor de verdere ontwikkeling ervan.”* Willem Blanken maakt daarbij de vergelijking met de ontwikkeling van de nutsvoorzieningen waarbij de betrouwbaarheid van gas, water en licht door de overheid werden gegarandeerd en er standaardisatie kon optreden in deze voorzieningen.

Aanbevelingen

Tot slot van de discussie werd aan de aanwezigen gevraagd welke aanbevelingen zij zouden willen doen.

- Pas op voor het Piggelmee-effect: als je een aantal wensen mag doen, vraag je altijd om het verkeerde, omdat je niet weet wat je wensen moet. Wees daarom voorzichtig en overdenk de kern.
- Eigenlijk snappen we er nog steeds niets van. Er moet meer in onderzoek geïnvesteerd worden. Misschien moet er zelfs wel een innovatie-instituut komen. Het wordt zo langzamerhand tijd meer hierover te leren.
- Kijk ook eens naar waar de burger nu eigenlijk behoefte aan heeft.
- De discussie te eenzijdig economisch. Er moet meer aandacht komen voor de achtergronden.
- We moeten een beter zicht krijgen op de problemen en daar beter over leren communiceren. Het besef moet ontstaan dat honderd procent veiligheid niet.
- We moeten meer de dialoog opzoeken en de partijen rond de tafel brengen.
- Het is een fascinerende tijd: er is veel onzekerheid, maar alles ligt ook open!