Dr. M.H.A. Klaver, ir. H.A.M. Luijf *

Nieuwe technologische doorbraken zijn aan de orde van de dag. Ze worden snel door de commercie tot wasdom gebracht en door een breed publiek geaccepteerd. De sterke integratie van Informatie- en Communicatietechnologie (ICT) in de samenleving maakt het functioneren van de samenleving in toenemende mate afhankelijk van de technische betrouwbaarheid van de (tele-) communicatievoorzieningen. De whitepaper 'Bitbreuk', geschreven door TNO in opdracht van Infodrome, buigt zich over de kwetsbaarheden van de nieuwe technologie en de wijze van implementatie daarvan. Is Nederland er op voorbereid om een infrastructurele crisis beheerst het hoofd te bieden? Kan de Nederlandse samenleving überhaupt optredende grootschalige verstoringen in 'cyberspace' alleen oplossen?

Stevent ICT-Nederland af op een bitbreuk?

Verstoorde communicatieverbindingen, uitval van elektronische diensten en mogelijk verlies aan vertrouwen van de samenleving in de informatiemaatschappij. Het zijn allemaal aspecten die zich laten samenvatten onder de noemer 'Bitbreuk'. Betrouwbaarheid in de ICT is niet voor niets een duaal begrip. Het rapport 'Stroomloos', geschreven voor de introductie van GSM, spreekt zelfs van een kwetsbaarheidsparadox: 'Naarmate een land minder kwetsbaar is in haar voorzieningen, komt iedere verstoring van de productie, distributie en consumptie van die voorzieningen des te harder aan'. Tellen we daarbij nog de kwetsbaarheid van de integriteit en exclusiviteit op (bijvoorbeeld verstoringen in het publieksvertrouwen in financiële transacties via openbare netwerken), dan kan de kwetsbaarheid van kritische ICT-infrastructuren daarmee de achilleshiel van de Nederlandse samenleving worden. Betrouwbaarheid van de ICT-infrastructuur heeft nog een ander dualisme in zich. Is de infrastructuur onbetrouwbaar, dan komt de elektronische dienstverlening trager of in het geheel niet tot ontwikkeling. Is de betrouwbaarheid echter hoog, dan kan een ernstig incident leiden tot geschokt vertrouwen van consument, bedrijfsleven en overheid. Hierdoor kan een scheuring ontstaan in de ontwikkeling en het gebruik van ICT: een deel van de samenleving gaat door, het andere deel wijst de nieuwe technologie nadrukkelijk af.

Management-summary

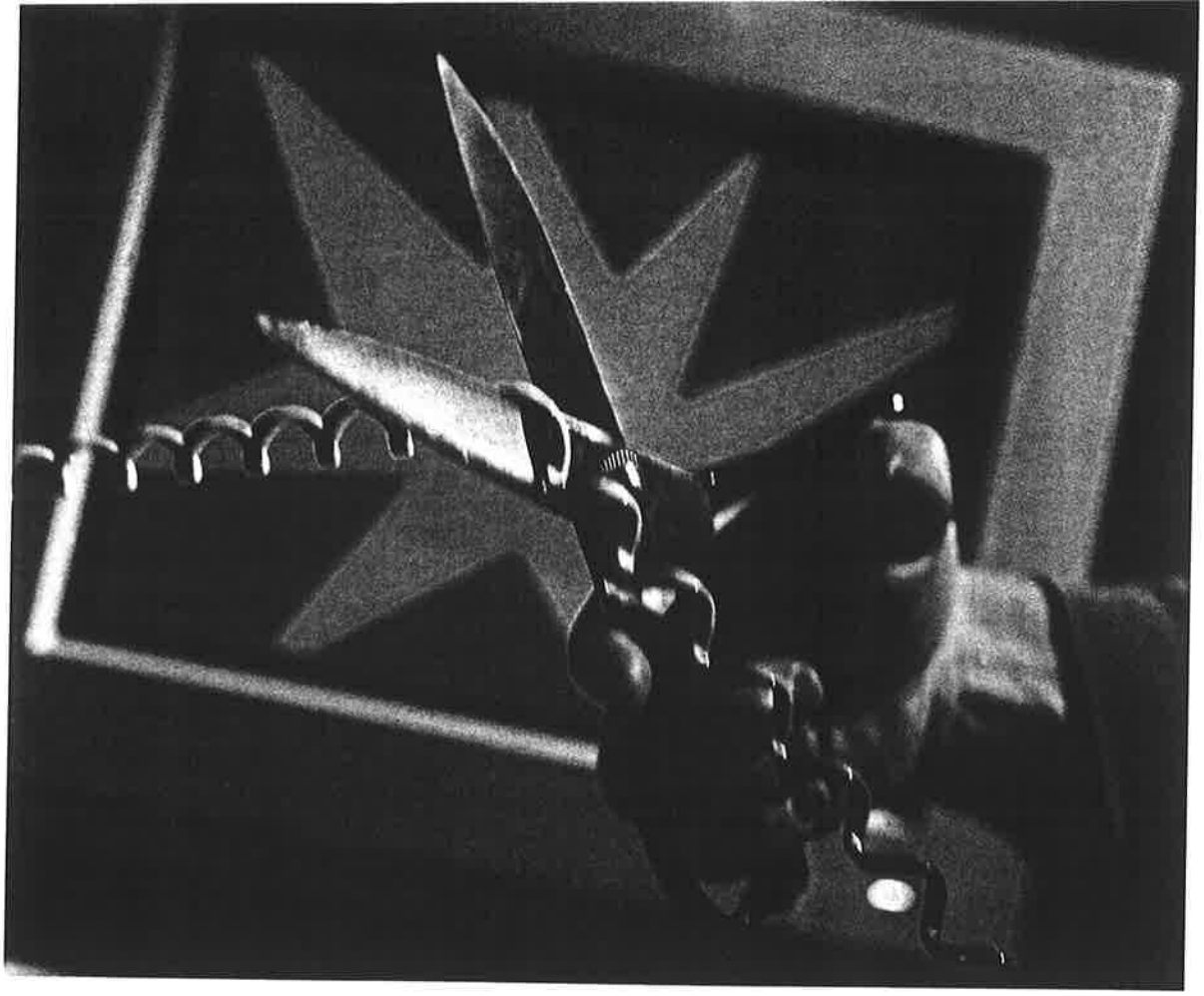
De samenleving verandert snel. Dat komt onder andere door het razend tempo van opeenvolgende ontwikkelingen van de informatie- en communicatietechnologie. Buitenlandse studies onderkennen de kwetsbaarheid van de samenleving bij verstoring van kritische infrastructuren en geven reden tot bezorgdheid en nieuw beleid. Ook in Nederland dringt het besef van kwetsbare ICT-infrastructuren langzamerhand door. Verstoring van (delen van) de kritische ICT-infrastructuur door opzettelijke of onopzettelijke oorzaak zou kunnen leiden tot ingrijpende consequenties voor het maatschappelijk systeem en de economie. De vraag is of Nederland voorbereid is om een dergelijke situatie beheerst het hoofd te bieden.

Infrastructuren

De sterke integratie van ICT in de samenleving maakt de samenleving steeds meer afhankelijk van de onderliggende infrastructuren. De recente problematiek rond de millenniumovergang heeft laten zien hoezeer de huidige maatschappij ICT nodig heeft in haar functioneren en hoe weinig inzicht er is in de onderliggende infrastructuurketens. (Figuur 1)

De basis van dit alles is elektriciteit. Zonder elektriciteit doen computers het immers niet. Boven de elektriciteitsinfrastructuur ligt de ICT-netwerkinfrastructuur, bestaande uit informatietransmissievoorzieningen als telecommunicatieapparatuur, glasvezels en kabels, radio- en TV-zenders, satellieten en lokale ICT. Deze voorzieningen zijn overi-

* werken beide bij TNO-FEL als principal consultant.



gens ook opgebouwd uit ICT-componenten en software voor de monitoring en besturing.

Oppassen geblazen

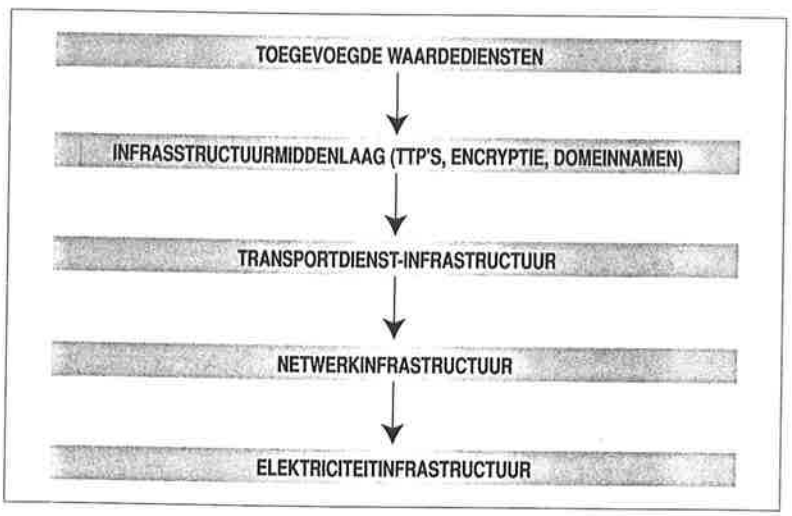
De ICT-netwerkinfrastructuur 'voedt' de volgende stap: transportdiensten als telefonie, fax, internettransmissie, televisie- en radiosignaaldistributie. Deze transportdiensten worden aangeboden door een grote verscheidenheid aan aanbieders, die al dan niet gebruik maken van dezelfde onderliggende infrastructuur.

De laag die weer boven de transportdienst-infrastructuur ligt, noemen we de infrastructuurmiddenlaag. Deze middenlaag faciliteert de toegevoegde waardediensten. Denk aan Trusted Third Party, domeinnaamdienst, messageservices (zoals voice mail en SMS) of internetservers.

Al deze stappen maken tenslotte de toegevoegde waardediensten mogelijk. Denk hierbij aan e-commerce, automatische belastingheffing, verwerking van transportvergunningen, positieafhankelijke internetinformatiediensten als GPS of een 24-uursloket van de overheid. Wel is het oppassen geblazen. Onderlinge ketenafhankelijkheid kan leiden tot onvoorziene domino-effecten, waarbij een verstoring van de ene infrastructuur naar andere infrastructuren overslaat. Het tegengaan van dergelijke domino-effecten is alleen mogelijk wanneer de onderlinge afhankelijkheid inzichtelijk is en er goed doordachte calamiteitenmaatregelen zijn genomen. Het feit dat het deels afhankelijkheden betreft die nationale grenzen overschrijden vormt hierbij een extra complicerende factor.

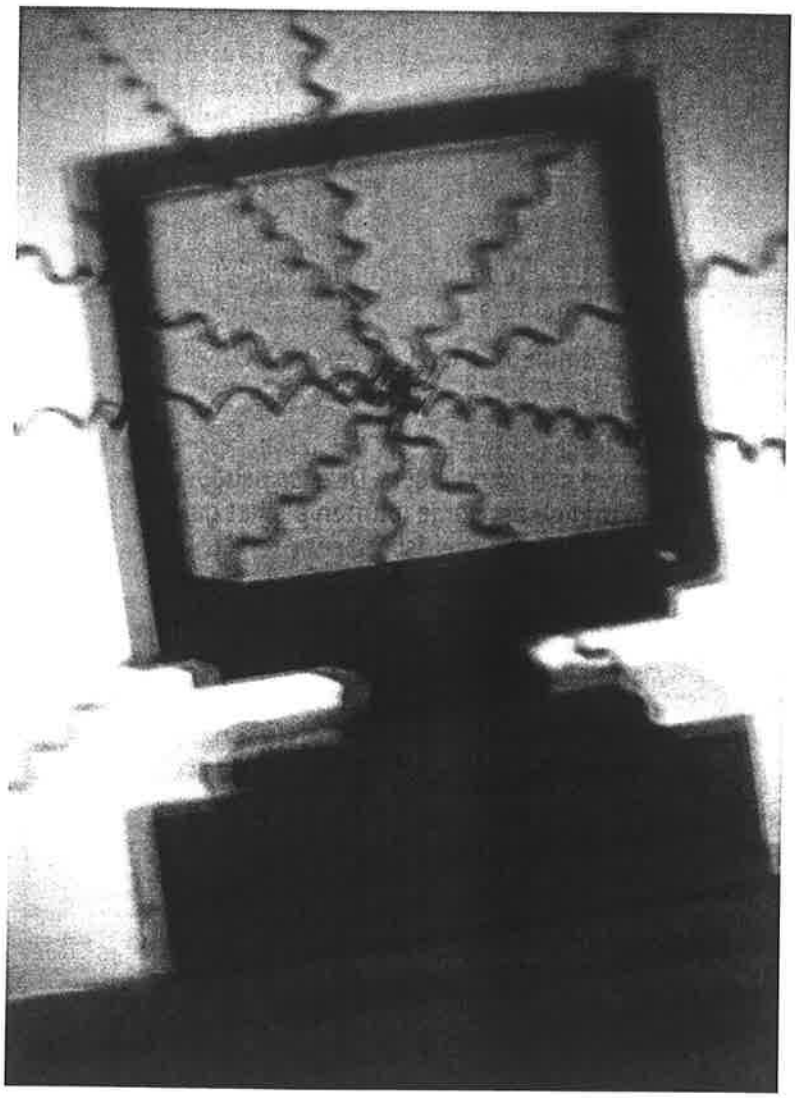
Kwetsbaarheden

Niet goed functioneren van de toegevoegde waardediensten kan vele oorzaken hebben. Zoals gezegd is er zonder elektriciteit geen ICT en dus ook geen toegevoegde waardedien-



Figuur 1. Model van verticaal gestapelde infrastructuren

sten. De kwetsbaarheid van ICT-infrastructuren is dan ook in grote mate afhankelijk van de kwetsbaarheid van de elektriciteitsinfrastructuur. Met uitzondering van het Nationaal Noodnet en het grootste deel van de vaste telefonie-infrastructuur zijn de openbare ICT-infrastructuren in het algemeen niet voorzien van noodstroomvoorzieningen.
Zit het met de elektriciteit wel goed, dan moeten we ons bekommeren om de bovenliggende laag, de netwerkinfrastructuurlaag. Deze verzorgt het 'bittransport' voor de transportdiensten. De kwetsbaarheid betreft hier met name de beschikbaarheid. Fysieke verstoringen door het al dan niet opzettelijk in ongerede raken van kabels is de grootste kwetsbaarheid. Het risico van opzettelijke manipulatie of sabotage van knooppuntapparatuur is alleen in te schatten door veiligheidsdiensten en kan aanzienlijk verkleind worden door het treffen van preventieve (veelal fysieke) beveiligingsmaatregelen. Feit is dat verstoring van deze laag grote gevolgen kan hebben in het maatschappelijke en economische leven.



Bron van zorg

De kwetsbaarheid van de volgende laag, de transportdiensten-infrastructuur, kent velerlei oorzaken. We beschouwen hier de kwetsbaarheden van de systemen die deze diensten moeten leveren zélf niet, al is dit wel een bron van zorg. De grootste kwetsbaarheid ligt in het moedwillig buiten gebruik stellen van deze diensten. Voorbeelden hiervan zijn fysieke of elektromagnetische aanvallen (HPM); spoofing en 'denial-of-service' aanvallen - het 'platleggen' van internetsites door ze zó vaak aan te roepen dat de server op hol slaat. Daarnaast bestaat het risico dat door de snelle groei van de infrastructuur onvoldoende rekening gehouden wordt met bedienfouten en technische storingen.

Vertrouwen

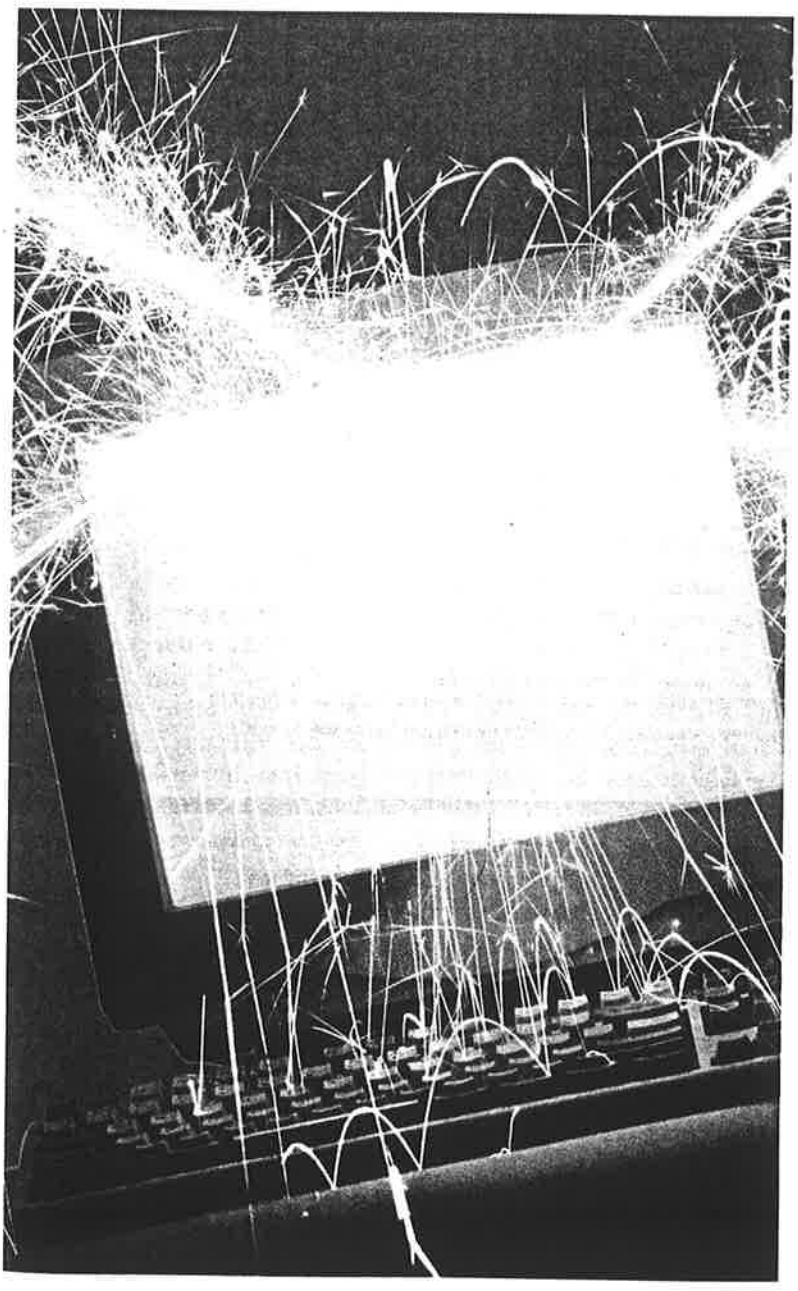
De betrouwbaarheid van ICT-diensten is van cruciaal belang voor het kunnen gebruiken van de toplaag: de toegevoegde waardediensten en niet te vergeten voor het vertrouwen van het publiek en de overheid in vergaande integratie van ICT in onze Nederlandse samenleving. De kwetsbaarheid van deze ICT-diensten betreft de kwetsbaarheid van het systeem dat de dienst aanbiedt en de kwetsbaarheid van de infrastructuur waarover de dienst aangeboden wordt. Het recent op straat raken van alle gegevens van 300.000 creditcards door een computerinbraak is een voorbeeld van een dergelijke kwetsbaarheid.
Ook basisdiensten van internet service providers (ISP's) zijn kwetsbaar. Betreft het één ISP dan kan men dat als bedrijfsrisico aanmerken. Als echter gelijktijdig dergelijke diensten bij het gros van de ISP's langdurig onbereikbaar gemaakt worden, kan dat het vertrouwen in

De sterke integratie van ICT in de samenleving maakt de samenleving steeds afhankelijker van de onderliggende infrastructuren.

de beheersing van de ICT-technologie schaden. Voor de volledigheid noemen we het risico voor het vertrouwen in de financiële infrastructuur voor elektronische handel. Dat vertrouwen kan verdwijnen als bekend wordt dat een niet snel te dichten gat in de beveiliging van elektronische transacties is geconstateerd.

Dreiging en incidenten

Als we de oorzaken van (ver)storingen beschouwen, kunnen we die in drie groepen indelen. De eerste groep betreft natuurlijke oorzaken, technische storingen en onopzettelijke menselijke fouten. Deze risico's en de maatregelen daartegen zijn in redelijke mate voor iedere infrastructuurlaag op zich in te schatten. De overheid gebruikt hiervoor de afhankelijkheids- en kwetsbaarheidsanalyses conform het VIR (VIR 1994). Ook marktpartijen gebruiken vergelijkbare methodieken, waarbij de geleverde diensten van anderen worden geschat. De risico's in deze groep vallen in het normale bedrijfsrisicoprofiel en zouden bij 'goed ouderschap' in voldoende mate voorzien en ondervangen moeten zijn.



De tweede groep betreft ketenafhankelijkheden en -kwetsbaarheden. De ketenbetrouwbaarheid is door de convergentie en verwevenheid alleen maar ondoorzichtiger worden. Afhankelijkheids- en kwetsbaarheidsanalyses vereisen inzicht in de infrastructuurketens en medewerking van alle (markt)partijen. Dergelijke analyses komen overeen met de complexe analyses zoals die op dit gebied zijn uitgevoerd in het kader van de millenniumproblematiek. De validiteit van zo'n analyse kan snel achterhaald zijn door de snelle, dynamische ontwikkelingen in de markt en snelle wisseling van onderliggende marktpartijen en technologieën.

De derde groep betreft opzettelijke menselijke verstoringen door insiders of externe hackers en terroristen, al dan niet uit vijandelijke staten. Uit onderzoek van onder meer de Britse NCC, de Amerikaanse CSI en KPMG blijkt dat veel bedrijven het risico van 'insiders' onderkennen. Insiders zouden echter verantwoordelijk zijn voor 40 procent tot 80 procent(!) van de beveiligingsincidenten. De externe dreiging (ernstige verstoringen, aanslagen en sabotage) is hoofdzakelijk in te schatten door veiligheidsdiensten. Let wel, nieuwe dreigingen kunnen onvoorzien snel ontstaan, zoals de snelle aanloop naar de Kosovo-crisis liet zien. Het is daarom belangrijk de dreigingstrends tijdig te onderkennen en tijdig de juiste preventieve, detectie-, reducerende en herstelmaatregelen te treffen.

Trends en factoren

E-commerce rukt op in onze Nederlandse samenleving. De economische kosten van verstoring van de ICT-infrastructuur zijn door de dynamische en explosieve veranderingen in ICT-gebruik en bandbreedte nu nog niet meetbaar te

maken in bijvoorbeeld het aantal euro per bandbreedte-eenheid per uur storing. Om dit wel te kunnen is nader onderzoek naar de effecten van opgetreden verstoringen nodig. De aanpak zoals geschetst in het rapport 'Stroomloos' kan hierbij een uitgangspunt zijn. De samenleving beweegt zich sterk naar een 24-uurs economie en een 24-uurs bereikbaarheid en de grenzen aan de groei in mobiele communicatie en internetgebruik zijn nog niet in zicht. E-commerce over deze mobiele en snelle media zal leiden tot een nieuwe impuls.
Ook iets om rekening mee te houden is de groeiende telecommunicatiemarkt. Tot enkele jaren geleden was de overheid exclusief verantwoordelijk voor de aanleg, instandhouding, vernieuwing en functionering van de ICT-infrastructuren in Nederland, zowel in normale als in bijzondere omstandigheden. In verband met de liberalisering van de telecommunicatiemarkt zijn de overheidsinfrastructuren overgedragen aan marktpartijen en is concurrentie gestimuleerd. Resultaat is dat de infrastructuurontwikkeling, de capaciteitsontwikkeling en investeringen nu marktgedreven zijn. Hierbij kan de benodigde redundantie in verbindingen in het geding komen, evenals de reservecapaciteit om congestie bij calamiteiten te voorkomen. In bepaalde gevallen kan de dagelijks benodigde capaciteit niet blokkeringvrij geleverd worden.

Naarmate een land minder kwetsbaar is in haar voorzieningen, komt iedere verstoring van de productie, distributie en consumptie van die voorzieningen des te harder aan.

Cruciaal belang

Iets dat samenhangt met de groeiende telecommunicatiemarkt is de elektronische dienstverlening. Deze wordt met de dag complexer vanwege de vele nieuwe toepassingen die er bijna dagelijks bijkomen. Door deze supersnelle ontwikkelingen is het van cruciaal belang dat de verticale en horizontale infrastructuren betrouwbaar functioneren. Is een marktpartij naar oordeel van de e-consument niet snel genoeg of lijkt die niet betrouwbaar, dan verschuift koopgedrag snel naar een concurrent. Of deze concurrent nu in Nederland of elders gevestigd is, is nauwelijks meer van belang. E-dienstverlening is wereldwijd.
De 'rechts- en zwaardmacht van de overheid' berust als vanouds op een territoriale afbakening die door informatie- en communicatietechnologie aan betekenis verliest. De revolutie van internet en andere internationale computernetwerken is gelegen in het feit dat de ICT-diensten zich niets van de nationale territoria aantrekken en dat 'actor, actie en gevolg van de actie' niet meer aan één plaats gebonden zijn. De negatieve aspecten van technologische ontwikkelingen, zoals 'cyber graffiti', 'cyber vandalisme', 'gewone' criminaliteit die gebruik maakt van ICT als middel, 'cyber hacktivisme' en 'cyber terrorisme' zijn sterk in opkomst. Deze trends werpen hun schaduw vooruit en moeten meegewogen worden in de beschouwingen over de kwetsbaarheid van ICT-infrastructuren in de voorziene planperiode van Infodrome.

Beheerst proces

De paper 'Bitbreuk' stelt dat het essentieel is dat de beschikbaarheid en betrouwbaarheid van de ICT-infrastructuren hoog is, indien Nederland tot de voorhoede van de informatiesamenlevingen wil gaan behoren. Het oplossen van ernstige storingen in en verstoringen van Nederlandse ICT-infrastructuren is een beheerst proces. De huidige situatie qua kwetsbaarheid van de Nederlandse ICT-infrastructuren baart volgens de auteurs de nodige zorgen. 'Bitbreuk' geeft hierbij de aanzet voor de discussie binnen Infodrome. ■

Informatie:
TNO-FEL
Postbus 96864
2509 JG 's-Gravenhage
☎ 070 - 374 00 00

Literatuur:

'Bitbreuk: De kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de informatiemaatschappij', ir. H.A.M. Luijf, mw. dr. M.H.A. Klaver, TNO Fysisch en Elektronisch Laboratorium, in opdracht van Infodrome, 2000.

'Stroomloos, kwetsbaarheid van de samenleving: gevolgen van verstoringen van de elektriciteitsvoorziening', I. Steetskamp en A. van Wijk, Rathenau Instituut, Den Haag, 1994.