WRR

WETENSCHAPPELIIKE RAAD VOOR HET REGERINGSBELEID

ICT EN INTERNET

CASESTUDIE TEN BEHOEVE VAN HET PROJECT VEILIGHEID

Mr. dr. F.J.P.M. Hoefnagel

WEBPUBLICATIE NR. 37

Den Haag, oktober 2007

De serie Webpublicaties omvat studies die in het kader van de werkzaamheden van de WRR tot stand zijn gekomen. De verantwoordelijkheid voor de inhoud en de ingenomen standpunten berust bij de auteurs. Een overzicht van alle webpublicaties is te vinden op de website van de WRR (www.wrr.nl).

INHOUDSOPGAVE

TEN GELEIDE

Deze studie is geschreven door mr. Dr. F.J.P.M. Hoefnagel, wetenschappelijk medewerker van de WRR en lid van de projectgroep veiligheid. Inhoudelijk is deze studie afgerond op 1 mei 2006. Ontwikkelingen die daarna hebben plaatsgevonden zijn derhalve niet in deze studie verwerkt.

In de voorbereiding van deze studie is door de auteur met diverse deskundigen gesproken en sommigen van hen hebben tussentijds inhoudelijk commentaar gegeven. De auteurs wil hiervoor graag de volgende personen bedanken:

ICT-deskundigen:

drs. Jan Wester, E.R. de Lange en J. van Bergenhenegouwen, ministerie van Economische zaken DG-TC EN POST.
prof. dr. C. Verhoef, hoogleraar informatica, Vrije Universiteit.
prof. dr. E. Michiels, hoogleraar veiligheid ICT Technische Universiteit Twente en deskundige Ernst and Young.
mr. W.H.M. Hafkamp, deskundige Rabobank.
ir. H.A.M. Luijf en dr. A.C.M. Smulders, respectievelijk senior en principal consultant security TNO.
drs. M. Leenaars, directeur Internet Society Nederland.

Deskundigen recht, bestuur en ICT:

prof. dr. N. Van Eijk en prof. mr. E. Dommering, beiden hoogleraar Universiteit van Amsterdam.
prof. dr. E.J. Koops en mw. dr. A. Lips, Universiteit van Tilburg.
dr. M.J.G. van Eeten, TU Delft.
prof dr. A.H.J. Schmidt, hoofd Centrum E-law, Universiteit Leiden.
drs. J.G.M. Timmermans en mr. J.J. Moelker, ministerie Binnenlandse zaken en koninkrijksrelaties, directie Innovatie en Informatiebeleid Openbare sector.
prof. dr. J. Grijpink, ministerie van Justitie, directie Algemene Justitiële Strategie.

1 INLEIDING

Deze studie beoogt de patronen van (on)veiligheid en van veiligheidszorg op het terrein van informatie- en communicatietechnologie (ICT) en internet, zoals zij zich nu en in de komende jaren manifesteren, zo goed mogelijk te diagnosticeren.

De vraagstelling bij deze casus valt in vier delen uiteen:

1. *Welke* risico's? Wat zijn nu en in de komende jaren de belangrijkste veiligheidsrisico's op dit terrein? Speciale aandacht gaat uit naar de *wicked problems* (gemene problemen), met als belangrijkste kenmerken: een hoge of onbekende waarschijnlijkheid, ernstige schade en slechte corrigeerbaarheid.

2. Wat zijn de *inhoudelijke* doelen en richting van de veiligheidszorg? Welk soort afwegingen tussen belangen en waarden zullen de komende jaren bij de veiligheidszorg centraal staan? Een subvraag betreft de al of niet juiste formulering van het afwegingsprobleem. Is het bijvoorbeeld wel juist te stellen dat men moet kiezen tussen veiligheid en innovatie? Is veiligheid niet eerder een belangrijke voorwaarde voor innovatie?

3. De veiligheid, *wie* een zorg? Twee vragen zijn hier te stellen. Allereerst is er de vraag van de (ver-)deling van verantwoordelijkheden tussen overheden, maatschappelijke en professionele instellingen, bedrijven en de burger. Vervolgens is de gewenste (ver-)deling van verantwoordelijkheden binnen de overheid aan de orde: welke overheid is op welk territoriaal niveau wanneer de meest gerede partij?

4. *Hoe* de veiligheidszorg hier organisatorisch en instrumenteel vorm te geven? Vooral is hier de vraag welk type beleidsregime waar en wanneer het meest effectief is, gezien het antwoord op de eerdere drie vragen en gelet op het eigen karakter van ICT en internet? Moet bijvoorbeeld voor online en offline zonder meer hetzelfde beleidsrégime gelden?

De opzet van de studie is als volgt. Allereerst worden in hoofdstuk twee het domein en de kernbegrippen nader bepaald. Daarna komen de ontwikkelingen in het veld zelf aan bod. In hoofdstuk vier wordt ingegaan op het bestuur en beleid, waarna de vier vragen van deze casestudie worden beantwoord.

2 DOMEINBEPALING EN DEFINIËRING KERNBEGRIPPEN

2.1 Ict en internet

Onder ICT valt in beginsel alle elektronische technologie voor opslag, bewerking, overdracht en presentatie van informatie, in de vorm van beeld, geluid of tekst. ICT vormt de meest algemene term. De term betreft niet alleen telecommunicatie, computers, kabels, maar ook rekenapparatuur, meet- en navigatie-instrumenten.

Bij internet moet onderscheid gemaakt worden tussen internet als systeem en internet als technologische methode.

Internet als systeem betreft een 'netwerk van netwerken', waarbinnen het gegevensverkeer een eenvormig specifiek protocol volgt. De belangrijkste karakteristieken van dit systeem van internet zijn de open architectuur (iedereen die de nodige apparatuur heeft, kan zich op het internet aansluiten), de decentralisatie, de afwezigheid van één *alomvattend* beheers- en bestuurscentrum, en het interactieve en multimediale karakter. De interactiviteit houdt in dat iedere toetreder potentieel producent en consument is. Het multimediale karakter betekent dat de communicatie in termen van beeld, geluid en woorden in technische zin gestalte krijgt op een éénvormige digitale wijze. De belangrijkste applicaties en communicatievormen die internet als systeem mogelijk maakt, zijn e-mail en het *World Wide Web* (WWW).

Nadere toelichting vraagt het decentrale karakter van het systeem. Internet als systeem heeft een beperkt aantal centrale elementen: het Internet Protocol (IP), het naam- en nummerbeheer (domeinnamen en IP-adressen), wereldwijde afspraken over technische standaarden, en de dertien root servers, die aan de top van de hiërarchie van domeinnamen staan en als centrale wegwijzer fungeren. Binnen dit beperkt gemeenschappelijke kader bestaat het systeem uit een groot aantal aan elkaar gekoppelde deelsystemen van verschillende serviceproviders. Deze richten zich op het transportdeel, of op de toegang tot het systeem van de eindgebruiker, of ze faciliteren, of ze richten zich op de inhoud, zoals bepaalde websites. Juist deze koppeling van zeer verschillende segmenten vormt de kern van het decentrale karakter. In termen van verschillende lagen kunnen de deelsystemen als volgt worden aangeduid:

a) de fysieke laag voor het vervoer van bits over de fysieke infrastructuur, zoals de kabels, de satellieten en de netwerkcomputers;

b) de netwerklaag die de inter-connectie van de verschillende fysieke netwerken verzorgt. Centraal staat hier het Internet Protocol dat de routering mogelijk maakt van de IP-pakketjes die over het internet gaan;
c) de transportlaag die verantwoordelijk is voor het transmissiebeheer, vooral door het *Transport Control Protocol* (TCP) dat nagaat of alle pakketjes ook op de plaats van bestemming aankomen en dat zonodig om een herhaling van de zending van pakketjes vraagt;
d) de applicatielaag. Dit is de laag die alle gebruikersgerelateerde applicaties verzorgt, zoals e-mail en webgebruik.

Voor ons wellicht nog belangrijker is internet als technologie, die alleen de netwerklaag en het daarbij behorend eenvormige Internet Protocol betreft en die ook buiten het WWW toegepast kan worden in afgeschermde netwerken en infrastructuren. Zo kennen veel organisaties en bedrijven eigen interne netwerken die wel gebaseerd zijn op de internettechnologie, maar niet gekoppeld zijn aan het internet als systeem. Juist dit gebruik van de internettechnologie buiten het eigenlijke systeem heeft een hoge vlucht genomen. De laatste jaren heeft deze netwerklaag van internet zich ontwikkeld tot een aparte, cruciale en universele tussenlaag voor transport van digitale informatie. Dit heeft geleid tot convergentie: alle typen diensten en inhouden kunnen via de netwerklaag van internet worden verspreid.

Internet als technologie biedt ongekende mogelijkheden tot vernieuwing, omdat nieuwe toepassingen mogelijk zijn zonder dat het transportsysteem als zodanig moet veranderen, zoals bij het klassieke telefoonnet. Bij internet als technologie is het netwerk uniform en zit de intelligentie in de randapparatuur. Bij het klassieke telefoonnetwerk is het precies omgekeerd.

Internet is kortom vooral een instrument dat op allerlei manieren kan worden ingezet. Het is een ‘domme’ transporteur van digitale informatie van en naar ieder punt van de wereld, die zich niet bekommert over het type informatie en type inhoud, of het soort netwerk waarbinnen de doorgifte van informatie plaatsvindt. Er is alle ruimte voor meer en minder intelligent en meer en minder geoorloofd gebruik, voor alles wat de deelnemers aan de randen van het systeem maar kunnen bedenken. In de vorm van een gemeenschappelijk transportkanaal schept internet als technologie tenslotte een nieuwe gemeenschappelijke ruimte van elektronische communicatie, variërend van computers die met elkaar communiceren tot en met de klassieke radio en televisie.

Ter wille van de duidelijkheid wordt in het verdere betoog bij gebruik van het woord internet het systeem bedoeld. Waar het gaat om internet als technologie zal worden gesproken van

ICT. Binnen het ICT-systeem is immers internet als technologie steeds meer de dominante manier van transporteren.

2.2 De term veiligheid

De nota Kwetsbaarheid en Internet (Kwint) van het ministerie van economische zaken en het ministerie van verkeer en waterstaat (2001) toont aan dat in ieder geval de navolgende aspecten van belang zijn: a) de vertrouwelijkheid, oftewel de exclusiviteit van de informatie; b) de authenticiteit en integriteit, oftewel de waarheidsgetrouwheid van de bron van de informatie en de informatie zelf; c) de algemene toegankelijkheid en de beschikbaarheid van de informatie. Veiligheid betekent hier derhalve waarborging van de beoogde kernfuncties van ICT-systemen en internet.

Bij de veiligheidsnorm in deze sector zijn derhalve waarden als privacy, waarheidsgetrouwheid en gelijkheid, in de zin van toegankelijkheid, in het geding. Veiligheid heeft hier derhalve een brede en ook sterk sectorspecifieke betekenis. Het gaat niet alleen om traditionele veiligheid, gerelateerd aan criminaliteit, terrorisme, nationale veiligheid en dergelijke.

3 ONTWIKKELINGEN BINNEN DE SECTOR

3.1 Algemene ontwikkelingen

De netwerklaag van internet wordt, zoals we zagen, steeds meer het dominante transportmiddel voor alle elektronische communicatie. Het internetverkeer groeit sterk. Er is sprake van een vertienvoudiging in de laatste drie jaar. Het internetgebruik in Nederland behoort tot de hoogste ter wereld. In 2004 had 74 procent van de Nederlanders thuis toegang tot internet en maakte 60 procent van de werkenden en 63 procent van de scholieren en studenten gebruik van een computer (Sociaal en Cultureel Planbureau 2004).

Op het brede terrein van ICT is sprake van een constante technologische verbetering van capaciteit en kwaliteit. Gewezen kan worden op de toenemende draadloze verbinding tussen delen van een ICT-systeem en het fenomeen van met elkaar verbonden computers die gebruik kunnen maken van elkaars capaciteit (de zogenaamde *grids*). Verder is de toenemende mobiliteit van ICT en internet een belangrijke robuuste ontwikkeling. Het is duidelijk dat deze versterkte 'de-lokalisering' het aantal gedragsalternatieven voor alle actoren enorm vergroot.

Er is een toenemend gebruik van ICT bij het bestuur en beheer van maatschappelijke kernvoorzieningen, in de publieke en in de private sfeer. ICT en internet zijn maatschappelijk geïntegreerd en 'ingebed'. Het romantisch-anarchistische idee van internet en cyberspace als aparte wereld, als het rijk van de absolute vrijheid en zelfregulering, zoals dat midden jaren negentig in intellectuele kringen overheerste, is echt *temps passé*. ICT en internet zijn in hoge mate een fenomeen van alledag aan het worden.

De belangrijkste, in de komende jaren te verwachten nieuwe ontwikkeling betreft vooral nieuwe vormen van toepassing van internettechnologie, die niet noodzakelijk aan het systeem van internet gekoppeld zijn: de komst van 'ingebedde processoren en sensoren', chips die in allerlei goederen, apparaten of in het menselijk lichaam kunnen worden ingebracht. Deze chips communiceren met elkaar en met de buitenwereld. Voorbeelden hiervan zijn: elektronische volgsystemen voor patiënten of criminelen, de ontwikkeling van domotica: het elektronisch beheer van allerlei processen in en rond het huis. Ten dele is die ontwikkeling al realiteit; denk aan de talloze, onderling communicerende processoren in auto's.

De productiviteitsgroei die met behulp van ICT en internet technologisch mogelijk is, wordt zeker in veel publieke sectoren bij lange na niet gehaald; dit geldt bij voorbeeld voor de zorg. Culturele, bedrijfsorganisatorische en economische condities voor een effectieve inschakeling

van ICT zijn meestal niet vervuld, vooral omdat de gewenste veranderingen bestaande machtsposities en belangen aantasten. Het gaat niet alleen om machtsposities en belangen die onterecht zijn en maar beter kunnen verdwijnen, maar ook om belangen die we algemeen als waarde hoog achten, zoals privacy en, in beperktere mate, de nationale bestuurlijke soevereiniteit.

Andere stagnerende factoren zijn van algemene bestuurlijke en juridische aard. Een concreet voorbeeld vormt de huidige onzekerheid over de gewenstheid van patenten op software, een vraag die vooral in het Europese informatiebeleid speelt. In meer algemene zin is er de beperkte manier waarop de *governance* van internet en ICT thans zijn vorm gegeven. Eind 2005 is op een conferentie in Tunis een begin gemaakt, maar ook niet meer. Dit onderwerp komt verderop uitvoeriger ter sprake.

Een andere stagnerende juridische factor betreft de aansprakelijkheid. Op zich is het al moeilijk bij complexe vormen van interactie, die kenmerkend zijn voor internet en ICT, de aansprakelijkheid goed vast te stellen. Er is immers sprake van meerdere ketens met ook weer per keten verschillende actoren. Dit geldt a fortiori bij een vrij nieuw terrein, waar bovendien verschillende nationale rechtstelsels een rol spelen en waar ook niet altijd duidelijk is welk recht waar en wanneer van toepassing is en welke rechter bevoegd is. Naarmate minder duidelijk is welke régime van aansprakelijkheid geldt, is de kans groter dat ook de hiermee verbonden stimulansen om aan veiligheidszorg te doen minder effectief zijn.

3.2 Negatieve ontwikkelingen

3.2.1 Algemene factoren onveiligheid

Het gaat hier om negatieve ontwikkelingen die essentiële karakteristieken en normatieve waarden binnen het ICT systeem zelf aantasten, zoals vertrouwelijkheid, authenticiteit, integriteit en de beschikbaarheid van gegevens. Welke algemene factoren maken ICT-systemen en internet onveilig?

Koops et al. (2005) noemen de volgende factoren. Allereerst is er de voortdurende vernieuwing van ICT en de toenemende complexiteit van ICT-systemen. Er ontstaan meer potentiële gaten, omdat de ontwerpers bij de toename van het aantal technologische opties en combinaties steeds minder het geheel en alle mogelijke eventualiteiten kunnen overzien. Algemeen geldt dat slechts 20 procent van de softwareprojecten slaagt, 30 procent eindigt in een totale mislukking en de rest voldoet niet aan de verwachting. Wereldwijd gaat 290 miljard per jaar op aan falende softwareprojecten (Automatiseringsgids 3 maart 2006, blz. 6).

De inherente instabiliteit van verschillende, op zich al complexe, aan elkaar gekoppelde systemen is volgens veel deskundigen een cruciale factor, die onveiligheid veroorzaakt. Er is bovendien een toenemende verwevenheid van niet alleen ICT-netwerken onderling, maar ook van verwevenheid van deze netwerken met sociaalorganisatorische en fysieke netwerken in de 'echte' niet-virtuele wereld. ICT-netwerken raken immers in toenemende mate maatschappelijk ingebed. Burgers, bedrijven en overheid zijn, deels onbewust, al zo afhankelijk geworden van ICT, dat een kleine kink in de kabel al snel grote maatschappelijke gevolgen heeft. Deze toenemende penetratie van ICT in het dagelijks leven leidt, in combinatie met de technologische convergentie en digitalisering, tot nieuwe en complexe geïntegreerde systemen, die zelf ook weer extra kwetsbaar zijn. Deze technologische integratie bevordert dat het economische en maatschappelijke verkeer in de huidige en komende tijd vooral 'immateriële' kennis en informatie betreft, met alle nieuwe kwetsbaarheden van dien, zoals manipuleerbaarheid van deze kennis en informatie.

In economisch opzicht zijn de kosten van beveiliging wel en de baten niet direct zichtbaar. Het is zeer de vraag of alle grote bedrijven en instellingen als overheden wel de goede stimulansen hebben om aan veiligheidszorg te doen en of zij bij de aanschaf en beheer van ICT -systemen een goede afweging maken tussen veiligheids- en andere aspecten. Waarschijnlijk zijn hier grote verschillen per sector. Zo is in de financiële sector het belang van een veilig betalingssysteem zo evident, dat er een goede stimulans is voor investeringen in veiligheidsmaatregelen. Wanneer de banken bovendien aansprakelijk zijn voor schade in het betalingsverkeer (zoals in het Verenigd Koninkrijk, maar niet in Nederland) worden ze bovendien geprikkeld tot *kosteneffectieve* investeringen in veiligheid. In 2001 kwam in een onderzoek van het Amerikaanse Congres (House of Representatives of the United States 2001) naar voren dat van de groep van grootste bedrijven in de Verenigde Staten veertig procent geen gebruik maakte van veiligheidsexperts op ICT-terrein! Verder hebben diegenen die betrokken zijn bij een ICT-ongeval, er meestal geen belang bij om dit aan de openbaarheid prijs te geven. Men wil immers imagobeschadiging vermijden.

Tenslotte is er een groot aantal contextuele ontwikkelingen die de kwaliteit van de besluitvorming over ICT-investeringen nog verder ten nadele van de veiligheid kan verslechteren. Allereerst is de besluitvorming hier een zaak van meerdere actoren en ook van meerdere disciplines. Er spelen immers niet alleen technologische en vakinhoudelijke, maar zeker ook economische en juridische aspecten. Lang niet altijd is gegarandeerd dat de verschillende disciplines goed weten wat men van elkaar reëel kan verwachten. Er is het risico van een 'dialoog der doven' tussen alpha- en bètadeskundigen. Bovendien vindt de besluitvorming hier bijna nooit plaats in een machts- en belangenvrije sfeer. ICT kan immers door de creatie van nieuwe informatiepatronen direct invloed uitoefenen op deze machts- en

belangenconstellatie. Denk bijvoorbeeld aan de ontwikkeling van elektronische patiëntensystemen in de zorg. Op het niveau van het bestuur en het management is er het risico dat vragen van beslissingsmacht over eigendom, gebruik en beheer van ICT-systemen veel meer aandacht krijgen dan vragen van veiligheid. Ook veranderingen in systemen van besturing van maatschappelijke kernvoorzieningen kunnen hier grote invloed hebben. Liberalisering, vermarkting en commercialisering van voorheen publieke diensten scheppen een geheel nieuwe *incentive*-structuur; men moet immers concurreren. Dit kan ten nadele gaan van een langetermijnbelang als ICT-veiligheid. Ook kunnen bedrijfseconomisch gewenste reducties van personeelskosten of door de overheid opgelegde bezuinigingen leiden tot lichtvaardige besluitvorming over ICT-investeringen.

Men kan tenslotte nog wijzen op de sociaalculturele context, waarbinnen op dit terrein risico's worden gedefinieerd en geselecteerd. Zeker in de jaren negentig was men zo gefascineerd van de geweldig nieuwe mogelijkheden van ICT, dat de schaduwzijden buiten beeld bleven. De euforie is over zijn hoogtepunt heen, maar toch is het waarschijnlijk dat deze historische factor op een of andere manier doorwerkt.

3.2.2 Specifieke toekomstige factoren

De laatste jaren is er een toenemende concentratie op één specifieke fysieke infrastructuur, namelijk de kabel. Wanneer die concentratie zich doorzet en aanbieders bij het toegankelijk maken van hun dienstverlening via het internet bijvoorbeeld steeds meer gebruik maken van een en dezelfde glasvezelkabel, heeft het niet beschikbaar zijn van deze glasvezel vergaande gevolgen. De afhankelijkheid en kwetsbaarheid worden groter.

Een tweede probleem dat in de toekomst extra aandacht vraagt is *time to patch*. Veel virussen maken in de vorm van een kwaadaardig programma misbruik van een bekende kwetsbaarheid in een applicatie- of computersysteem. In het jargon heet een dergelijk programma een 'exploit': het programma exploiteert immers de kwetsbaarheid. De gemiddelde tijdsduur tussen het bekend worden van een kwetsbaarheid en het beschikbaar komen van een 'exploit' is de laatste jaren dramatisch gedaald. De tijdsfactor wordt steeds nijpender. Leveranciers hebben immers tijd nodig om herstelsoftware (*patches*) te ontwikkelen. Hetzelfde geldt voor eindgebruikers die deze herstelsoftware in hun systemen moeten aanpassen.

3.2.3 Duiding van oorzaken en gevolgen van onveiligheid

Zowel de oorzaken als de gevolgen zijn zeer divers. De oorzaken kunnen liggen bij menselijke opzet, nalatigheid en onzorgvuldigheid, bij natuurlijke factoren als een blikseminslag, maar

ook bij gedrag van dieren (bijv. kabels die worden doorgeknaagd). Ook is lang niet altijd sprake van een externe oorzaak. Veel beveiligingsincidenten zijn het gevolg van gedrag van medewerkers binnen een bedrijf.

Het type schade is eveneens zeer divers. De schade is soms wel en soms niet goed te lokaliseren en binnen een bepaald tijdsvak te plaatsen. Bovendien is sprake van diversiteit van schade omdat het niet alleen gaat om schade binnen het ICT-systeem. Bij de toenemende vervlechting van ICT-netwerken met externe, sociaalorganisatorische en fysieke netwerken is vaak de externe schade veel groter. Bijvoorbeeld zodra maatschappelijke kernvoorzieningen als de zorg of de elektriciteitsvoorziening niet meer functioneren door uitval van systemen. Geconcludeerd kan worden dat bij ICT, gegeven de complexe interactie van talloze actoren en deelsystemen, oorzaak en gevolg van ongelukken vaak niet eenduidig te bepalen zijn, hetgeen de vraag van de aansprakelijkheid moeilijk beantwoordbaar maakt. Dit betekent dat het analytische element in het beveiligingsbeleid hier extra aandacht vraagt. Oorzaak en gevolg zijn hier minder een evident gegeven, dan bij bijvoorbeeld de verkeersveiligheid.

3.2.4 Mogelijke grootte van de schade

Uit een in 2004 uitgebracht rapport van de *Royal Academy of Engineering* en de *British Computer Society* (www.raeng.org.uk en www.bcs.org.uk) over de problemen bij complexe ICT-projecten, kwam naar voren dat in het Verenigd Koninkrijk slechts rond de zestien procent van dit soort ontwikkelingsprojecten een succes is. Een schatting van de jaarlijkse kosten van falende ICT-projecten kwam in de Verenigde Staten uit op 150 en voor Europa op 140 miljard dollar. Hoewel deze cijfers niet specifiek over Nederland gaan, is van belang dat Nederland op Europees niveau al sinds jaren een van de grootste gebruikers is van ICT, met name door de aanwezigheid van veel multinationals. De volgende oorzaken van dit falen worden genoemd: een algemene afwezigheid van collectief professionalisme in de bedrijfstak van ICT; tekorten in de opleiding en training van professionals bij aanbieders en gebruikers; een eindverantwoordelijkheid van slecht gekwalificeerde managers; weinig aandacht voor risicomanagement; en onderwaardering van de vitale rol van de systeemarchitect. Ook worden de operationele kosten op lange termijn van grootschalige ICT -investeringen vaak onderschat. Voorgesteld wordt dat overheid en bedrijfsleven een *Software Engineering Institute* oprichten voor onderzoek, advies, training en het verspreiden van *best practices*. Het werkterrein moet breed worden opgevat: software *engineering* en het managen van complexe ICT-projecten.

3.2.5 Specifieke vormen van onveiligheid

De volgende vijf vormen van onveiligheid bij internet en ICT-systemen worden algemeen onderkend (De Bruijn et al. 2004):

Onrechtmatige ondervanging van elektronische informatie
De schade is vaak maar niet altijd beperkt. Ondervanging van informatie van de politie of bedrijfsspionage kunnen bijvoorbeeld verstrekkende gevolgen hebben. De waarschijnlijkheid hiervan is hoog, gezien ervaringen uit het verleden. Een sterke terugkoppeling en correctie bij incidenten is in beginsel mogelijk. Er is sprake van convergente toedeling van kosten en baten, hetgeen betekent dat er een goede *incentive*-structuur is 'om er wat aan te doen'. Wanneer evenwel ook derden, bij wijze van neveneffect, in hun belangen worden getroffen, zal die *incentive*-structuur minder goed werken.

Onrechtmatige toegang tot computers en netwerken
Ook hier is de schade vaak maar lang niet altijd beperkt. Er is sprake van hoge waarschijnlijkheid dat er via spyware en niet-geautoriseerde technieken inzage ontstaat in informatiebestanden. Er is de mogelijkheid van sterke terugkoppeling bij incidenten. In het algemeen is er een convergente toedeling van kosten en baten, maar ook hier geldt weer de uitzondering, in het geval ook derden worden benadeeld die er weinig aan kunnen doen. Denk bijvoorbeeld aan patiënten bij gevoelige medische informatie.

Ontwrichting van het netwerk
Er wordt een onderscheid tussen ontwrichting op *beperkte* schaal (wormen, kleinschalige *Distributed Denial of Service* (DDoS)-aanvallen, dat wil zeggen het vanuit meerdere punten overbelasten en onbereikbaar maken van services en netwerken) en *grootschalige* vernietiging en onbruikbaar maken van netwerken en gegevens, zoals opzettelijke (bijvoorbeeld terroristische) aanvallen op centrale *root*services. Ook elektromagnetische verstoring en stroomuitval kunnen tot grootschalige ontwrichting leiden. De ontwrichting op beperkte schaal komt vrij veel voor, maar is tot nu toe beheersbaar gebleven. Grootschalige ontwrichting heeft geheel andere kenmerken dan de hiervoor genoemde negatieve ontwikkelingen, zoals zeer grote schade, lage maar onbekende waarschijnlijkheid, zwakke terugkoppeling en correctie. Er is immers sprake van divergente toedeling van kosten en baten. Er is geen goede *incentive*-structuur die leidt tot noodzakelijke collectieve actie. Er is vooral het gevaar van het zogenaamde 'cascade-effect': bij complexe systemen kan een niet verwachte combinatie van kleine voorvallen juist grote rampen veroorzaken. Overigens moet ook hier rekening worden gehouden met het eigen technologisch karakter van internet. Internet is oorspronkelijk opgebouwd om onder alle omstandigheden te functioneren. Bijvoorbeeld terroristische acties die een algehele destructie van het netwerk beogen, zullen

weinig kans van slagen hebben. Goed doordachte zeer precieze aanvallen, die zich richten op kernonderdelen als *root*-servers, zijn wellicht gevaarlijker.

Malware (virussen en wormen)
Het gaat bij *malware* om boosaardige software die informatie wijzigt en/of vernietigt. Een toenemend probleem zijn in dit verband de zombies: zwaar geïnfecteerde computers die slecht beveiligd zijn en vervolgens andere computers infecteren. Eigenaren van zombiecomputers hebben zelf vaak geen weet van de infecties en vaak ook geen belang bij correctie. Zij hebben immers zelf nergens last van. Zombies worden alom gezien als een van de toekomstige *wicked problems* (De Bruijn et al. 2004). Er is sprake van een grote kans, met in toenemende mate grote schade. Er is een beperkte *incentive*-structuur die leidt tot actie en correctie. In dit verband wordt vaak ook spam genoemd. Dit punt vraagt om een aantekening. De aard van de schade is bij spam immers verschillend. Bij spam wordt er geen informatie gewijzigd of vernietigd. Het probleem is hier vooral dat de kosten voor de veroorzaker van spam relatief gering zijn, maar voor het ICT-systeem en de ontvangers van spam de (im-) materiële kosten zeer hoog kunnen oplopen. Denk aan het gebruik van de bandbreedte, de kosten voor de consument bij het ophalen van al die e-mail en de irritatie die dit verschijnsel opwekt.

Boosaardige identiteitsverwisseling
Een recente ontwikkeling is het fenomeen van *phishing*. Een voorbeeld hiervan is een e-mail van een vervalste website die de schijn wekt een echte bank te zijn en klanten oproept om hen vertrouwelijke gegevens te verschaffen, zoals nummers van creditcards. Evenals bij spam zullen de kosten voor de veroorzakers meestal gering zijn, maar kan de schade voor de ontvangers in zijn totaliteit zeer hoog oplopen, ook wanneer slechts een beperkt aantal geadresseerden op het aanbod ingaat en 'erin tuint'. De vraag of goede terugkoppeling en correctie bij incidenten mogelijk zijn, valt in zijn algemeenheid nu nog niet goed te beantwoorden.

3.3 Externe negatieve ontwikkelingen

Bij externe negatieve ontwikkelingen gaat het om bredere negatieve ontwikkelingen, waarbij ICT en internet een instrument of bepalende omgevingsfactor zijn. Er is natuurlijk een zekere vorm van overlap met enkele in de vorige paragraag beschreven vormen van interne onveiligheid. Zo kan *phishing* ook onder de categorie worden ondergebracht van externe negatieve ontwikkelingen, die hier aan de orde is. Het is immers ook een vorm van ordinaire oplichting. Belangrijk in dit verband is de constatering dat veiligheid bij ICT en internet niet alleen interne technische verstoringen betreft, zoals bij de klassieke vormen van

telecommunicatie, maar ook nieuwe vormen van boosaardig, crimineel gebruik van de techniek mogelijk maken.

Bij deze externe ontwikkelingen wordt de volgende *hoofdonderscheiding* gemaakt: a) cybercriminaliteit in bredere zin, zoals elektronische vermogensdelicten, inhoudgerelateerde delicten (kinderporno), aanbieding van illegale diensten en producten, inbreuk op intellectuele eigendom en privacy ('digitale schandpaal') en b) de aantasting van vitale infrastructuren die door ICT worden beheerd en gestuurd (Luijf 2004).

3.3.1 Cybercriminaliteit

Wereldwijd neemt de misdaad met behulp van internet met sprongen toe (Kaspersen 2004). Dit geldt met name voor de internationaal georganiseerde misdaad, die door middel van verstoring van ICT-systemen bedrijven en organisaties kan chanteren en afpersen. Het gaat niet alleen meer om jonge roekeloze eenlingen die, op zoek naar avontuur, ICT-systemen binnendringen of virussen verspreiden en onbedoeld veel schade aanrichten. Voor de georganiseerde misdaad is verstoring van ICT-systemen ook een lucratieve vorm van 'zaken doen'. Het feit dat territoriale beperkingen er weinig toe doen, vormt een begunstigende factor.

Veel criminogene factoren zijn direct af te leiden uit de aard van internet als systeem: de programma's voor crimineel gedrag die internet zelf biedt, het internationale, deterritoriale karakter, het gegeven dat de dader veelal niet direct geconfronteerd wordt met de negatieve gevolgen van zijn handelen, en de vergrote mogelijkheid om de identiteit te vervalsen of om anoniem te blijven.

Normstelling, opsporing, bewijsvergaring en handhaving vergen een vergaande internationale samenwerking tussen overheden, die wordt belemmerd door culturele en juridische verschillen tussen landen en door de wens van staten om hun soevereiniteit te handhaven. De nog te bespreken *Convention on Cybercrime* van de Raad van Europa een is een grote stap vooruit. Vooral van de politie vraagt cybercrime extra middelen en de opbouw van kennis en expertise. Het gebrek aan kennis is voor de Nederlandse justitie en politie de grootste hindernis (Stol 2004). Prioriteiten in het huidige politiebeleid betreffen vooral kinderporno en internetfraude. Daarnaast doet het nationale kennis- en expertisecentrum *National High Tech Crime Center* (NHTCC) veel onderzoek naar nieuwe vormen van al of niet georganiseerde elektronische criminaliteit.

Belangrijk is in dit verband tenslotte ook dat de juridische aansprakelijkheid van de serviceprovider voor onrechtmatige handelingen van zijn contractanten bewust is beperkt

(Alberdingk Thijm 2004). Wel is er een recent arrest van de Hoge Raad (HR, 25 november 2005), waarin beslist is dat providers en andere internetaanbieders in bepaalde gevallen de identiteit moeten onthullen van anonieme spelers op internet die van hun diensten gebruik maken, wanneer gedupeerde derden aannemelijk maken dat de uitingen van deze anonieme spelers onrechtmatig, bijvoorbeeld beledigend, *kunnen* zijn.

3.3.2 Aantasting van bestuur en beheer van vitale infrastructuren

Aantasting kan geschieden met een criminele opzet of gewoon door een ongeluk. Risicoversterkende factoren zijn het toenemende gebruik van ICT bij de sturing en beheer van infrastructuren, de convergentie van netwerken, en toepassingen van IP-technologie in systemen voor procescontrole op de terreinen van elektriciteit, gas, waterbeheersing drinkwatervoorziening en de procesindustrie. Ook de internationale koppeling van netwerken voor elektriciteit, gas en telecommunicatie verhoogt het risico. Bovendien kan een de historisch sterke traditie van betrouwbare vitale voorzieningen, bij voorbeeld bij elektriciteit, soms tot te lichtvaardige invoering van sturing en beheer met behulp van ICT zonder dat men nadenkt over mogelijke alternatieven.

Tenslotte moet hier in het verlengde van wat eerder is gezegd, gewezen worden op de nieuwe bestuurlijk-economische context van het beheer van infrastructuren. De vraag is of de in gang gezette liberalisering en commercialisering van het beheer van infrastructuren aan het management wel de juiste *incentives* geven voor een evenwichtige afweging van commerciële continuïteit en (ICT-)veiligheid. Dit geldt temeer waar de kosten van veiligheidszorg vooraf wel duidelijk zijn, maar de baten zich niet direct manifesteren. Is in het nu overheersende marktconforme besturingsmodel met de veiligheidszorg voldoende rekening gehouden?

3.4 Mogelijke remedies

Wij beperken ons in dit hoofdstuk tot die remedies die in principe los staan van het overheidsbeleid, zoals technische, organisatorische en juridische maatregelen (Koops et al. 2005).

Technische, organisatorische en juridische maatregelen
Onder technische maatregelen vallen allereerst vormen van cryptografie, waarbij gegevens versleuteld worden. Deze technische maatregelen worden vaak gecombineerd met organisatorische arrangementen, zoals het inschakelen van een vertrouwde derde persoon (*Trusted Third Party* (TTP), die als sleutelbeheerder fungeert of die garandeert dat versleutelde gegevens toegankelijk blijven voor bevoegden, ook wanneer de ontcijfersleutel

onverhoopt niet meer beschikbaar is. De export van cryptografische technieken is aan internationale regels gebonden.

Ten tweede valt onder deze technische categorie de digitale handtekening, als middel om de authenticiteit en integriteit van elektronische gegevens te garanderen. Hierbij is vaak sprake van een combinatie met organisatorische en juridische voorzieningen. De organisatorische maatregelen betreffen vooral de verschillende vormen van certificatie, zoals de *Public Key Infrastructure* (PKI), die verderop worden besproken. Met het oog op de gelijkstelling van de handmatige en elektronische handtekening is er vrij veel, vooral Europese, overheidsregelgeving.

Tenslotte zijn er de biometrische methoden voor beveiliging van gegevens en de herkenning van personen. De combinatie met organisatorische en juridische maatregelen is ook hier aanwezig: de ontwikkeling van herkenningssystemen enerzijds, regels met het oog op grondrechten als privacybescherming en lichamelijke integriteit anderzijds.

Bij organisatorische maatregelen moet onderscheid worden gemaakt tussen interne en externe maatregelen. Bij interne maatregelen gaat het om interne beveiligings- en autorisatieprocedures (in de vorm van zowel fysieke als elektronische toegangscontrole), het opzetten van een brandmuur (*firewall*) die tegen externe indringers beschermt en de verschillende vormen van viruscontrole. Ook bewustwording van eindgebruikers via voorlichting en educatie, die ervoor moet zorgen dat zij het belang ervan inzien om de beveiligingsprocedures na te leven, valt onder deze categorie. Tenslotte moet in dit verband nog het laten uitvoeren van *Electronic Data Processing* (EDP)-audits worden genoemd, waarbij externe deskundigen ICT-systemen testen op punten als veiligheid en betrouwbaarheid.

Onder de externe maatregelen vallen allereerst de verschillende vormen van certificatie, zowel van sleutels, als van documenten als van programmatuur. Bij de certificatie van sleutels en documenten is er bovendien een overkoepelende *Public Key Infrastructure* (PKI), waarbij *Certification Authorities* (CA) elkaar certificeren, hetgeen extra vertrouwen moet geven in het systeem van certificatie. Ten tweede moet de constructie van *Trusted Third Party* (TTP) worden genoemd, waarbij een vertrouwde derde door beide partijen wordt ingeschakeld, bij voorbeeld voor de certificatie van publieke sleutels voor ondertekening. Tenslotte vallen onder deze categorie algemene preventieve maatregelen voor een bepaalde regio of sector, zoals de oprichting van een *Computer Emergency Response Team* (CERT), dat waarschuwt bij dreigingen en ondersteunt bij de afwikkeling van veiligheidsincidenten. Zo kent ons land een CERT voor de overheid, de burger en het kleinbedrijf. Door de

onderlinge verbinding en samenwerking tussen de verschillende CERT's in Europa wordt de effectiviteit van dit type instellingen flink vergroot (Koops et al. 2005).

Hieronder vallen vormen van overheids- en zelfregulering, contracten, richtlijnen, algemene voorwaarden en rechterlijke uitspraken. Dit punt komt met name bij paragraaf 4.7 en 4.8.3 aan de orde.

3.5 Conclusie

Zoals iedere technologie biedt ICT een veelvoud aan nieuwe problemen en oplossingen. Het probleem is dan ook niet dat de verdere ontwikkeling en toepassing van ICT alleen maar leidt tot een kwantitatieve en kwalitatieve vergroting van bedreigingen. Centraal moet de vraag staan of er voldoende aansluiting is tussen de bedreigingen en de veiligheidszorg in termen van preventie en repressie (herstel).

De aansluitingsvraag heeft meerdere kanten. Allereerst is er een aansluitingsprobleem in termen van tijd: omdat kwetsbaarheden van het internet tegenwoordig zo snel bekend worden, is het steeds moeilijker om tijdig herstelsoftware te ontwikkelen en toe te passen. Ten tweede zijn er vrij grote verschillen tussen de verschillende actoren in de capaciteit om de verantwoordelijkheid voor de veiligheidszorg te effectueren. De capaciteit wordt zeker niet alleen bepaald door geld. Zeker op dit terrein zijn kennis, expertise, maar ook de cultuur van een organisatie even cruciaal. Ten derde is problematisch dat de *incentive*-structuur om veiligheidszorg in de besluitvorming over ICT de plaats te geven die het verdient, door een groot aantal factoren niet adequaat is. Hierdoor dreigt veiligheid een 'ondergeschoven kindje' te worden. In algemene zin bestaat bij besluitvorming over investeringen al een risico dat veiligheid niet de verdiende aandacht krijgt, omdat de relatie tussen kosten en baten van veiligheidszorg vooraf niet helemaal helder is. Bij ICT is er bovendien een aantal, in paragraaf 3.4 beschreven, aanvullende factoren die het risico extra kunnen verhogen op een onevenwichtige besluitvorming ten nadele van de veiligheid. Deskundigen komen, als gezegd, tot de voorzichtige conclusie dat de kosten van lichtvaardige besluitvorming in de Verenigde Staten en Europa afzonderlijk op jaarbasis ver boven de 100 miljard liggen.

4 BESTUURLIJKE EN BELEIDSONTWIKKELINGEN

4.1 Algemeen

Een aantal factoren is hier van belang. Internet is weliswaar van oorsprong een overheidsinitiatief, van het Amerikaanse agentschap voor defensie onderzoek (ARPA), maar de expansie van internet is vooral een product van vrijwillige samenwerking van private partijen. Vanouds is dit private karakter ook gezien als een van de sterke punten van internet. In tegenstelling tot andere infrastructuren heeft internet zich niet ontwikkeld binnen een centrale overheidsregie die het geheel als probleemeigenaar bewaakt. Bovendien is internet tot bloei gekomen binnen de Amerikaanse culturele en juridische traditie met de daarbij behorende, terughoudende visie op de overheidsrol. Verder is in de beginfase het overheidsbeleid vooral ruimte biedend en vrijmakend geweest, om innovatie te bevorderen, zie onder andere de nota Kwint (Ministerie van economische zaken en Ministerie van verkeer en waterstaat 2001). Beperkend beleid omwille van de veiligheid had in deze nota geen prioriteit.

Tenslotte, men kan zeker niet zeggen dat bij afwezigheid van een overheid, internet ‘dus’ een gewone markt is met de instrumenten voor sturing en correctie die daarbij horen. Op dit punt zijn twee visies mogelijk. Enerzijds kan men internet als een slecht georganiseerde markt aanmerken. In veel opzichten is sprake van marktfalen: er zijn veel private monopolies (Microsoft, Google) en er is vaak sprake van een informatieasymmetrie tussen de aanbieder en de eindgebruikers, hetgeen de concurrentie belemmert. Anderzijds kan men vaststellen dat Internet eerst en vooral een speciale markt is, waarin steeds nieuwe spelers de dan overheersende actoren uitdagen, de dominantie van hen willen overnemen en zelf de algemeen geldende standaarden willen bepalen. De ontwikkelingen zijn nog niet uitgekristalliseerd tot een eenduidig concept van de markt. De regels inzake intellectuele eigendom zijn evenmin eenduidig. Enerzijds zijn internationaal met name de auteursrechten op de inhoud (*content*) verscherpt, hetgeen de concurrentie kan verkleinen. Anderzijds zijn er ook bedrijven zoals Cisco die bewust hun intellectuele eigendomsrechten op bijvoorbeeld protocollen vrijgeven om daardoor dominantie te krijgen, de standaarden te zetten en deze aan anderen op te leggen.

4.2 Het conceptuele aspect: visies op het bestuur van ICT-systemen en internet

In de discussie spelen volgens De Bruijn et al. (2004) de volgende visies een rol:

a) Internet is een nieuw decentraal fenomeen. Op de enkele punten waar centrale regels nodig zijn kunnen de huidige particuliere instanties volstaan; dit is de huidige situatie.
b) Breng internet onder bij het internationale en nationale overheidsregime voor de klassieke telecommunicatie.
c) Niet internet, maar het gehele gebied van de elektronische communicatie, mogelijk gemaakt door internet als technologie, vormt het nieuwe fenomeen. Herdenk, los van de geschiedenis van internet, nut en noodzaak van *governance* en *government* in termen van nieuwe concepten.

4.3 Typologie van instrumenten

Allereerst is er het reeds aan de orde gestelde onderscheid tussen technische, organisatorische en juridische instrumenten. De Bruijn et al. (2004) onderscheiden binnen de derde, juridische groep nog een subcategorie: het via aansprakelijkheidsregelingen een zodanige *incentive*-structuur scheppen dat preventie en reparatie gestimuleerd worden door het juridisch conditioneren van decentrale transacties. In deze laatste visie hoeft alleen een beperkt aantal zaken, zoals een grootschalige ontwrichting van internet, een directe, operationele overheidsverantwoordelijkheid te zijn.

4.4 Bestuur en beleid op mondiaal niveau

4.4.1 Particuliere organisaties

Oorspronkelijk was de Amerikaanse overheid de belangrijkste 'eigenaar' van internet. Overwegingen van privatisering en internationalisering hebben er in de jaren negentig toe geleid dat er een veelvoud van particuliere en professionele internationale organisaties is ontstaan, die vooral actief zijn op het terrein van de technische ontwikkeling en het beheer van Internet en het uitgeven van namen en nummers.

De belangrijkste organisatie op het terrein van de technische ontwikkeling is het *World Wide Web Consortium*. Bij het technische beheer zijn de belangrijkste instellingen voor de technische standaarden de volgende organisaties: *Internet Society* (ISOC), *Internet Engineering Taskforce* (IETF), *Internet Engineering Steering Group* (IESG) en *Internet Architecture Board* (IAB) en *Internet Research Taskforce* (IRTF). Voor de namen en nummers is *Internet Corporation for Assigned Names and Numbers* (ICANN) de

belangrijkste beleidsbepaler. Met name bij ICANN behoudt de Amerikaanse federale overheid een belangrijke eindverantwoordelijkheid. Beide partijen hebben een overeenkomst gesloten naar Amerikaans recht, warbij de federale overheid invloed kan houden op deze particuliere organisatie. In dit contract zijn met name enkele beleidsprincipes vastgelegd (www.icann.org). Voor de andere particuliere organisaties geldt dit niet of in mindere mate.

De belangrijkste kenmerken van de mondiale particuliere organisaties zijn: hun internationale non-profit karakter, hun in beginsel sterke onafhankelijkheid van overheden (zij het in een aantal gevallen met uitzondering van de Amerikaanse federale overheid), zelfregulering als organisatieprincipe, hun onderlinge verwevenheid, de dominantie van de professionele technische producenten en de ontwikkeling van technische vooruitgang via openbare standaardisatieprocessen (Koops en Lips 2003). Het gaat meer om pluricentrische netwerken dan om vormen van monocratisch leiderschap. Er is geen sprake van één machtscentrum. Wel lijkt het erop dat feitelijk de onevenredig grote betrokkenheid van niet alleen de Amerikaanse overheid, maar ook vooral van Amerikaanse bedrijven en instellingen ertoe leidt dat de juridische, bestuurlijke en bedrijfscultuur van dat land bij al deze organisaties sterk domineert.

In toenemende mate is er de laatste jaren vanuit Europa en niet westerse landen kritiek op instituten als het ICANN, omdat zij steeds meer politieknormatieve afwegingen moeten maken zonder adequate democratische legitimatie en verantwoording. Het politieknormatieve karakter van sommige besluiten van deze organisaties komt op verschillende manieren naar voren. Allereerst bij wijze van neveneffect. Zo zijn het gehanteerde systeem van domeinnamen en vooral de keuze voor generieke domeinnamen juridisch en maatschappelijk niet neutraal en kan het systeem bepaalde taalgroepen bevoordelen. Meer expliciet komt dit naar voren, wanneer in de technische architectuur normen worden ingebouwd die direct gerelateerd zijn aan waarden als privacy en de vrijheid om informatie te geven en te ontvangen. Denk aan filtersystemen.

In meer algemene zin wordt het idee van internet als een volledige soevereine ruimte, die door niet-overheidsorganisaties kan worden bestuurd, als achterhaald beschouwd, mede gezien de toenemende verwevenheid van de fysieke en virtuele wereld. Internet is ingebed in het dagelijkse leven. Deze gehele problematiek kwam najaar 2005 op een conferentie van de Verenigde Naties in Tunis aan de orde. Zie hierover de volgende subparagraaf.

4.4.2 Overheidsorganisaties

De *International Telecommunication Union* (ITU) is een gespecialiseerde organisatie van de Verenigde Naties (VN) voor telecommunicatie, de *World Intellectual Property Organization* (WIPO) een voor auteursrechten. Mondiaal is met name de vraag of taken van ICANN niet

over moeten gaan naar de ITU, omdat de verstrekking van telefoonnummers wel onder de ITU valt. Vooral de Amerikaanse overheid verzet zich hiertegen. De VN en de ITU organiseren periodiek een *World Summit on the Information Society* (WSIS), binnen welk kader een aantal globale uitgangspunten voor informatiebeleid, waaronder veiligheid, zijn geformuleerd. Uiteraard zijn deze uitgangspunten vrij algemeen, gezien de grote culturele en juridische verschillen tussen de westerse en niet-westerse landen. In de verklaring van Genève van 12 december 2003 worden bijvoorbeeld de volgende uitgangspunten genoemd: de internationaal erkende politieke -, sociale en culturele vrijheids- en gelijkheidsrechten, waaronder met name de feitelijke toegankelijkheid van Internet voor mensen uit de armere landen en voor marginale groepen, culturele pluriformiteit, rechtsstatelijke principes als multilateraliteit, democratie en transparantie, internationale samenwerking, goede marktwerking en *last but not least*, het opbouwen van voldoende vertrouwen in stabiele en veilige ICT-systemen (www.itu.int/wsis/does/geneva).

Op de top van de WSIS, die in november 2005 onder de vlag van de VN in Tunis werd gehouden, manifesteerde zich een scherp verschil van inzicht tussen een groot aantal niet-westerse landen zoals China, India, Brazilië en Iran enerzijds en de Verenigde Staten anderzijds. Europa had hier een tussenpositie. Eerstgenoemde landen wilden meer invloed van de wereldwijde opererende overheidsorganisaties op het bestuur en beheer van internet, bijvoorbeeld door het beheer van domeinnamen onder te brengen bij een orgaan van de VN. Zij vonden het onjuist dat alleen de Verenigde Staten, door hun band met het ICANN, wijzigingen in het adresboek kunnen doorvoeren. De Amerikanen wensten de bestaande situatie te handhaven. Zij wezen op de gevaren van een sterker overheidsbeheer op mondiaal niveau, die ook in de sector zelf worden gezien: een grotere dreiging van meer overheidscensuur op het web en vertraging bij belangrijke technische beslissingen. Europa bepleitte vooral een verbetering èn internationalisering van het toezicht op deze professioneel-technische organisaties door ook andere overheden dan de Amerikaanse.

Karrenberg, een van de Europese pioniers van internet, plaatste aan de vooravond van de conferentie hierbij enige kritische kanttekeningen (NRC 12 november 2005). Hij vindt dat het huidige beheer van internet juist een uitdrukking is van het subsidiariteitsbeginsel van zo veel mogelijk decentralisatie en dat juist het niet centrale karakter van internet voorwaarde is voor verdere ontwikkeling. Bovendien wordt de bestuurlijke coördinatierol van het ICANN volgens hem zwaar overschat. Zij beperkt zich tot één aspect van het beheer, namelijk de domeinnamen. Onderbrenging van deze taak bij een VN-orgaan zoals het ITU zou alleen maar tot zware politisering leiden.

Het is zijns inziens inderdaad nodig op langere termijn te bekijken hoe publieke belangen beter kunnen worden behartigd en wat de rol van overheden moet zijn, maar op de korte termijn vragen volgens hem niet bestuurlijke zaken van vormgeving voorrang om aandacht, maar meer inhoudelijke zaken zoals het tegengaan van spam, het bestrijden van computerspecifieke criminaliteit en een betere toegang tot internet in de arme landen.

Uiteindelijk is in Tunis afgesproken dat de VN zal onderzoeken hoe ook andere landen en overheden buiten de Verenigde Staten beter kunnen worden betrokken bij het beheer door deze technische professionele organisaties. Ook krijgen individuele staten een grotere stem over eigen domeinen, zoals het Nederlandse 'nl', de aanduiding aan het einde van het internetadres.

Belangrijker zijn de besluiten die in Tunis zijn genomen op het terrein van het algemene bestuur van internet. De verklaring van Tunis (www.itu.int/wsis/doc2/tunis) omschrijft het bestuur van internet, internet *governance*, als volgt: "the development and application by governments, the private sector and civil society, in their respected roles of shared principles, norms, rules, decision making procedures, and programmes that shape the evolution and the use of the Internet". Uitdrukkelijk wordt gesteld dat bestuur over internet meer omvat dan het uitdelen van namen en adressen, een taak van het ICANN. Het gaat ook om het borgen van tot nog toe verwaarloosde publieke belangen zoals veiligheid.

Er komt er een nieuw wereldwijd overlegorgaan, het *Internet Governance Forum* (IGF), waarin internationale en nationale overheden, bedrijven, professioneel-technische organisaties en non-gouvermentele organisaties praten over de vele publieke en andere belangen die bij internet in het geding zijn, waaronder de veiligheid en de gewenste vorm van internet *governance*. Dit IGF heeft geen algemene toezichtsfunctie op reeds bestaande organisaties. Met het dagelijkse beleid en met technologische operaties van deze organisaties mag het IGF zich niet bemoeien. Het IGF is vooral opgezet als een gespreksforum: een neutraal, niet-duplicerend en niet-bindend beleidsproces en eerder gebruik maken van bestaande regels en instituten, zoals het ICANN, dan trachten die te vervangen. Op het continentale en op het nationale niveau moeten met het IGF vergelijkbare instellingen gestimuleerd worden. Minister Brinkhorst zei na afloop: "de trein is op de rails gezet, de weg naar internationalisering van het bestuur van internet is ingezet" (NRC 24 november 2005). Over het internationale bestuur van internet wordt in de slotverklaring van Tunis meer specifiek het volgende gezegd. Het internationale bestuur moet gebaseerd zijn op de eerder genoemde in Genève overeengekomen principes en op de volledige betrokkenheid van nationale overheden, de private bedrijfssector, de *civil society* en internationale professioneel-technische en ook de internationale publieke overheidsorganisaties.

Staten hebben, aldus de slotverklaring, rechten en verantwoordelijkheden voor internationale *public policy issues* die samenhangen met internet. De private sector heeft een belangrijke rol te spelen bij de technologische en economische ontwikkeling van internet, de *civil society* heeft vooral een taak op het niveau van de ontwikkeling van gemeenschappen, internationale publieke overheidsorganisaties dienen een bijdrage te leveren aan de coördinatie van *public policy issues* en internationale private en professionele organisaties hebben een taak op het punt van technologische standaarden en daarmee samenhangend beleid. Kortom, uitdrukkelijk wordt gekozen voor een *multi-stakeholders*-benadering. Speciale aandacht krijgt het ontwikkelen van een globale cultuur van cyber-*security*. Staten hebben de primaire taak om samen te werken en tot goede internationale wetgeving en handhaving te komen bij het bestrijden van cybercriminaliteit. Op het niveau van de middelen worden zowel publieke als private, juridische en andere feitelijke en informatieve instrumenten genoemd: overheidswetgeving, zelfregulering, technologische maatregelen, educatie en voorlichting, met name over *best practices*. Daarbij moeten de internationale regels inzake privacy en de vrijheid van meningsuiting worden gerespecteerd. Samenwerkende nationale staten hebben verder een belangrijke verantwoordelijkheid bij het waarborgen van het recht van toegang tot internet, de veiligheid en regels voor consumentenbescherming bij *e-commerce*.

4.5 Beleid op Europees niveau

De *Organisation for Economic Cooperation and Development* (OECD 2002) heeft een aantal richtlijnen voor veiligheid op internet geformuleerd die een zekere bindende waarde hebben. Binnen de Raad van Europa is, zoals gezegd, een verdrag over *cybercrime* opgesteld, waarbij ook andere Westerse landen zich hebben aangesloten. Aandacht voor veiligheid op internet is bij de Europese Unie (EU) relatief laat op gang gekomen; men gaf lange tijd voorrang aan andere aspecten van ICT-beleid, zoals innovatie.

In het nieuwe beleidskader van de Europese Commissie voor het algehele informatiebeleid vanaf midden 2005, geheten 'i2010', formuleerde de Europese Commissie een drietal doelen: de ontwikkeling van een afzonderlijke Europese informatieruimte, versterking van innovatie van en investeringen in ICT en de bevordering van een inclusieve Europese informatiemaatschappij. In dat kader zijn bevordering van vertrouwen en veiligheid van internet en van andere infrastructuren en communicatienetwerken, dé uitdagingen van de toekomst. Onderkend wordt dat het hier om een lastig probleem gaat, omdat geografische grenzen hier grotendeels irrelevant zijn en klassieke, met name juridische instrumenten voor regulering- en handhaving hier niet goed werken (Europese Commissie 2005). Bij toename van breedband en draadloos internet worden het veiligheids- en vertrouwensprobleem urgenter. Veiligheid is een wezenlijke conditie in het genereren van consumentenvertrouwen in de nieuwe generatie technieken en voor het waarborgen van privacy. Samen met de

lidstaten moet de EU komen met een alomvattende coördinerende aanpak, die alle aspecten van ICT en alle mogelijke instrumenten betreft: regulering, technologische maatregelen, onderwijs en onderzoek, voorlichting en bewustwording. In het door Ecotec verrichte voorbereidend onderzoek (Ecotec 2005: 68) wordt vooral gewezen op het gebrek aan samenhang tussen onderzoek, beleidsvorming, wetgeving en uitvoering.

Inmiddels heeft de EU een vrij omvattend juridisch raamwerk opgesteld:een richtlijn inzake de wederzijdse erkenning van elektronische handtekeningen (authentificatie en integriteit van documenten), een regeling ter liberalisering van de handel in encryptieproducten (vertrouwelijkheid en integriteit van informatie) en een richtlijn ter beveiliging van persoonsgegevens en bescherming van de persoonlijke levenssfeer bij de elektronische communicatie en *e-commerce*. In navolging van de Raad van Europa heeft ook de EU een verordening *cybercrime* vastgesteld. De nieuwe richtlijnen voor aanbieders op het terrein van de telecommunicatie geeft hen een specifieke taak op het terrein van de veiligheid.

Voor advisering, signalering, alarmering en voorlichting is in 2004 een apart Europees agentschap opgericht, het *European Network and Information Security Agency* (ENISA). ENISA werkt nauw samen met de zusterinstellingen van de lidstaten. Dit expertisecentrum heeft geen uitvoerende bevoegdheden. Een adviescommissie uit het Europese bedrijfsleven staat ENISA bij. Voor ontwikkeling van nieuwe veiligheidstechnieken en educatie kent de EU een aantal fondsen, zoals *The Safer Internet plus programme*. Eind 2006 zal de Europese Commissie komen met een specifieke strategie voor een veilige informatiemaatschappij met speciale nadruk op zelfbescherming, waakzaamheid en toezicht en voor snelle, tijdige reacties op systeemstoringen. Onderwerpen als ontwerpintrinsieke beveiliging en identiteitsbeheer zullen speciale aandacht krijgen.

4.6 Beleid op nationaal niveau

Onderscheid moet worden gemaakt tussen de nationale overheid, als een van de gebruikers van ICT en de bredere verantwoordelijkheid van de overheid voor veiligheid op ICT-terreinen. Voor de eerste functie is met name het Voorschrift informatiebeveiliging rijksoverheid 1995 van belang. In het vervolg komt vooral de bredere verantwoordelijkheid aan de orde, uitgewerkt in een aantal nota's.

De nota Kwint van 2001
Specifiek voor internet is er het zogenaamde Kwint-programma, dat gebaseerd is op de nota Kwint (Ministerie van economische zaken en Ministerie van verkeer en waterstaat 2001). Uitgangspunt is de primaire verantwoordelijkheid van internetgebruikers en aanbieders. Dit geldt natuurlijk ook voor de overheid zelf als beheerder van ICT-systemen. Voor het geheel

heeft de overheid vooral een monitorende en faciliterende rol. Specifieke *nationale* regelgeving is, aldus deze nota, voorshands niet aan de orde. Maatregelen van de overheid mogen immers niet ten koste gaan van innovatie. (Inter) nationale publiekprivate samenwerking is noodzakelijk en het beheersbaar maken van de kwetsbaarheid van internet is thans het hoogst haalbare. Maatregelen betreffen voorlichting, bewustwording en alarmering, bevordering van onderzoek, stimuleren van intern- organisatorisch beleid door bedrijven en instellingen en het meer transparant maken van de markt van beveiligingsproducten. Daarnaast worden internationale regels op dit terrein in de nationale wetgeving verwerkt en uitgevoerd. Dit gebeurt soms in het algemene civiel- of strafrecht, maar meestal in de nieuwe Wet op de Telecommunicatie (TC-wet). Het gaat om de volgende onderwerpen: de regeling van de elektronische handtekening in het privaatrecht, de verwerking van het verdrag inzake cybercrime in de wetboeken voor strafrecht en strafrechtsvordering, regels in de TC-wet inzake het bevoegd aftappen, afluisteren en aflezen van vormen van elektronisch verkeer, zoals e-mail, en tenslotte om regels in genoemde wet die de privacy beperken, zoals regels inzake de opslag door onder anderen providers van verkeers-, locatie- en persoonsgegevens. Tenslotte is er het verbod op spam dat op natuurlijke personen is gericht. Handhaving en uitvoering van de spamregels zijn een zaak van de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA).

De nota Nederland in verbinding van 2006

In het verlengde van de afspraken die in Tunis zijn gemaakt, zal ook op nationaal niveau getracht worden te komen tot een betere (ver-)deling van verantwoordelijkheid tussen overheid en andere actoren. Voor de bestrijding van cybercrime zal een nationale structuur worden ontwikkeld. Het beleid gericht op bewustwording, voorlichting en dienstverlening voor eindgebruikers binnen en buiten de overheid zal worden geïntensiveerd (Ministerie van economische zaken 2006).

Crisissituaties

Het bredere beleid van de rijksoverheid betreft meer specifiek de noodsituaties. Sinds 1990 functioneert een Nationaal Noodnet, dat volledig gescheiden is van de openbare netten. Overheidsorganisaties en vitale bedrijven zoals leveranciers van energie zijn verzekerd van een communicatiemiddel, wanneer het reguliere openbare telecommunicatienetwerk uitvalt. Daarnaast heeft de overheid samen met particuliere aanbieders het Nationaal Continuïteitsplan Telecommunicatie (Nacotel) opgericht. De overheid is hier primair *regisseur*. Partijen hebben afspraken gemaakt over het ongestoord blijven functioneren van diensten op het terrein van telecommunicatie (TC) en het snel verhelpen van storingen. Doel van het publiekprivate samenwerkingsmodel is de aansluiting van de maatschappelijke belangen, waar de overheid voor staat, op de commerciële belangen van de aanbieders. Alle partijen hebben zich verplicht te zorgen voor een eigen continuïteitsplan, voor het inrichten

van een eigen organisatie gericht op crisismanagement en voor het regelmatig verslagleggen. Op termijn zal de samenwerking worden uitgebreid met aanbieders op het bredere terrein van ICT. Nu ligt nog te veel nadruk op de telefonie. Ook zal de samenwerking een minder vrijblijvend karakter krijgen. De meest vitale aanbieders zullen worden verplicht deel te nemen aan het overleg en het maken van afspraken.

Verder bevat de nieuwe TC-wet van 2004 regelingen die bijzondere bevoegdheden aan de centrale overheid geeft in crisissituaties. De minister kan alsdan aanwijzingen geven aan aanbieders van openbare TC-netwerken en -diensten. Bovendien geldt een op genoemde TC-wet gebaseerde ministeriële regeling Voorbereiding buitengewone omstandigheden. Het plan Nacotel is geen uitwerking van deze wetgeving en dient juist te voorkomen dat deze regels van toepassing worden.

Voorlichting, educatie, overleg en onderzoek

Er is een nationale door de overheid opgerichte waarschuwingsdienst voor bedreigingen van ICT-systemen (CERT). Het ministerie van economische zaken stimuleert daarnaast in het basisonderwijs het Diploma Veilig Internet, dat kinderen informatie geeft over risico's op internet en hen leert hiermee om te gaan. Tenslotte moet nog het Platform Criminaliteitsbeheersing worden genoemd, waarin publieke en private partners sinds 2004 samenwerken in het Project Aanpak Cybercrime. Het gaat daarbij zowel om specifieke, digitale vormen van criminaliteit als om klassieke vormen van criminaliteit in een modern ICT-jasje. Hoofdpunten van dit plan zijn: de vermindering van de kwetsbaarheid van overheid en bedrijfsleven voor cybercriminaliteit, verhogen van het bewustzijn van de bevolking voor cybercriminaliteit, preventieve maatregelen en verbetering van het collectieve reactievermogen. Binnen dit kader functioneert het *National High Tech Crime Center*, een samenwerkingsverband van de politie en enkele departementen, dat gericht is op een proactieve aanpak van met ICT verband houdende criminaliteit. De overheid bevordert onderzoek door onder andere de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO) en *Rand Europe*. Safe.nl is het forum voor onderzoekers, waar de wetenschappelijke wereld, overheid en bedrijfsleven informatie uitwisselen.

Wenselijk beleid

De consumentenbond heeft aan de Tweede Kamer in april 2006 een petitie aangeboden, waarin zij pleit voor wetgeving, krachtens welke computerleveranciers, internetproviders, en de aanbieders van andere internetdiensten de veiligheid voor consumenten moeten waarborgen. Veiligheid moet een vast onderdeel worden van het ICT-product, net zoals autogordels standaard worden geleverd bij auto's. Het installeren van een beveiligingspakket is immers te ingewikkeld voor de meeste consumenten.

4.7 Vergelijking beleid Verenigde Staten en Europa

De sector kent geen (internationale) regels over licensies voor het beroep van informatietechnoloog (het is in alle opzichten een vrij beroep) en geen algemene regels over kwaliteitscertificaten van ICT-systemen, -apparatuur en -producten. Dit in tegenstelling tot de telecommunicatie. Evenmin zijn er nationale regels voor de privé-sector betreffende de transparantie bij besluitvorming over grote ICT-investeringen en over de accuraatheid en betrouwbaarheid van deze investeringen. Mede gezien het belang dat aandeelhouders en andere stakeholders hierbij hebben, kent de Verenigde Staten wel een dergelijke regeling, de zogenaamde *Sarbanes-Oxley Act* van 2002 (Publ. No. 107-204).

Deze regeling eist dat de financiële verslaglegging aan drie eisen voldoet: ze moet volledig, correct en traceerbaar zijn. Dit betekent dat bedrijven moeten verantwoorden, waarom ze besloten hebben om (in ICT) te investeren en dat de rechter deze verantwoording ook aan genoemde eisen kan toetsen. Aan de procedurele eis van traceerbaarheid is wellicht het gemakkelijkste te voldoen. Vooral met het oog op de belangen van de aandeelhouders geeft de wet de ondernemers de nodige stimulansen om duidelijk te maken dat investeringen in ICT winstgevend zijn. Zij zullen, volgens Verhoef (2005), er alle belang bij krijgen hun investeringen goed te motiveren, ze vooraf te specificeren in termen van kosten, wijze van financiering, tijdsperiode, risico's en verwachte winstgevendheid. Ook zullen zij er belang bij krijgen aan te geven hoe een bepaalde ICT-investering bijdraagt aan de winstgevendheid van het geheel van uitgaven voor ICT. Verhoef (2002) noemt dit de 'portfolio-benadering'.

De *Clinger-Cohen Act* van 1996 (Publ. No. 104-106) legt overheden al een dergelijke benadering op. Voor de publieke sector verplicht deze wet overheden tot portfoliomanagement op het terrein van ICT. Overheden moeten een integraal beleid voor al hun ICT-investeringen voeren, dienen vooraf kosten-baten-, haalbaarheids- en risicoanalyses te maken, en vooraf aandacht te besteden aan de interoperabiliteit met andere ICT-systemen en aan gemeenschappelijke ICT standaarden binnen de overheid. Ook moet bekeken worden of voor een bepaald doel geheel nieuwe systemen echt wel nodig zijn of dat bestaande systemen kunnen worden aangepast. Doordat overheden zich primair moeten richten op die producten die zich reeds op de markt bewezen hebben, kunnen onnodige risico's worden vermeden.

Veel overheden zijn bovendien verplicht hun ICT-investeringen op een speciale website te verantwoorden. Dit soort regels is in de Verenigde Staten ingevoerd na talloze onderzoeken, waaruit bleek dat grote ICT-investeringen van overheden vaak werden gekenmerkt door irreële inschattingen van kosten, doorlooptijd en risico's en dat overheden weinig gebruik maakten van het systeem van *best practices* (House of Representatives 2001*)*.

In ons land heeft een dergelijk onderzoek nooit plaats gevonden. De politieke discussie heeft zich altijd op onderdelen gericht, met name op de ICT-investeringen in de zorg, zoals het elektronisch medicatiedossier. De problemen betroffen vooral de slecht ingeschatte tijdsduur van totstandkoming, de te beperkte risicoanalyse voor informatiebeveiliging en kostenberekening (Tweede Kamer 2004-2005, 27529 met name nr. 14). Juist omdat het in de ICT-sector erg moeilijk is om vooraf realistische inschattingen te maken van kosten, doorlooptijden en van verwacht rendement, stellen dergelijke stimulansen hoge eisen aan de professionals en het management. In die situatie krijgt de afwezigheid van iedere vorm van licensering van ICT-professionals extra reliëf. De vroegere adviseur van het Witte Huis Harold Schmitt pleitte onlangs op een congres ervoor om de verantwoordelijkheidsregels nog meer te verscherpen en opstellers van software zelf verantwoordelijk en aansprakelijk te stellen voor gebreken, kwetsbaarheden en vormen van onveiligheid in de door hen ontwikkelde software. Hij verwees naar een recent onderzoek van Microsoft, waaruit bleek dat bijna tweederde van de ontwikkelaars meende niet in staat te zijn compleet veilige software te ontwikkelen. Op dit congres werd algemeen onderkend dat de juiste vragen van verantwoordelijkheid terecht werden gesteld. Wel was het de vraag of niet eerder het bedrijf, waar deze ontwikkelaars in dienst zijn, aangesproken moest worden en of ook de gebruiker niet een zekere eigen verantwoordelijkheid heeft. Een systeem van accreditering van ontwikkelaars van software kan de gebruiker hiertoe meer informatie geven (news.zdnet.co.uk 12 oktober 2005).

4.8 Conclusie

4.8.1 Algemeen: de conceptuele achterstand

Een van de belangrijkste conclusies luidt dat er een duidelijke conceptuele discrepantie is tussen de behoeften aan beleid en bestuur die ICT en internet oproepen en de traditionele bestuurlijke taal en concepten. ICT en internet grijpen diep in op bestuurlijke aannames als territoriale gebondenheid en een vanzelfsprekend gezag van de overheid over een bepaald territoir. Een ander aanname die ICT op de tocht zet, betreft het concept van regelgeving. Regels die in de fysieke wereld door overheden worden vastgesteld, zijn bij ICT en internet vaak een zaak van softwareproducenten (code as code), die een professionele en zeker geen democratische legitimatie hebben. Ook veiligheidsproblemen van ICT en internet zouden eigenlijk binnen geheel nieuwe bestuurlijke paradigmata aan de orde moeten komen, maar deze zijn er nog niet.

In de toekomst vraagt deze conceptuele herdenking van belangrijke bestuurlijke uitgangspunten en waarden als democratie en overheidsgezag binnen de nieuwe context van ICT en internet zeker veel aandacht.

4.8.2 Wie bestuurt? De rol van de overheid

Een van de belangrijkste punten hierbij is de herformulering van de overheidsrol. Deskundigen zijn het er in ieder geval over eens dat de relatie tussen bestuur door particuliere of overheidsorganisaties niet als of-of keuze moet worden opgevat, maar voor de toekomst meer moet worden gezien in termen van wederzijdse aanvulling. Deze complementariteit kan op verschillende manieren haar beslag krijgen.

Koops et al. (2005) noemen de volgende mogelijkheden. Op basis van het uit het volkenrecht bekende 'comitasbeginsel' erkennen niet-statale en particuliere internetorganisaties enerzijds en overheden anderzijds elkaars jurisdictie. Veel kan in deze visie worden overgelaten aan particuliere organisaties, maar bij specifieke, gelokaliseerde vitale publieke belangen moeten (samenwerkende) staten kunnen ingrijpen. Ook kan mogelijkerwijs een verbreed ITU-verdrag, waarbij naast de klassieke TC ook ICT en internet een expliciet werkterrein van deze organisatie kunnen zijn, het legitimerende kader bieden voor overheidsinterventie, wanneer rechtswaarden waarvoor de overheid een eindverantwoordelijkheid draagt in het geding zijn. In feite is in Tunis een derde weg gekozen, waarbij sterke nadruk ligt op de vraag, waarvoor de verschillende actoren verantwoordelijk zijn.

Met name het hier gemaakte onderscheid tussen politiekbestuurlijke vragen die publieke belangen betreffen en meer technologische vragen van beheer, die primair de private professionele organisaties regarderen, biedt een goed perspectief om deze wederzijdse aanvulling vorm te geven.

4.8.3 Het probleem toegespitst op de regelgeving

Internet heeft een lange traditie van zelfregulering ('netiquêtte'), die versterkt is doordat providers deze in hun contracten overnamen. Het is dan ook de stelling van de 'klassieke' internetjuristen (onder andere Alberdingk Thijm 2004) dat online technologische maatregelen, spontane zelfregulering en contracten de voorkeur verdienen, terwijl pas in de laatste plaats gedacht moet worden aan wetgeving van de overheid; dit is derhalve een duidelijke andere koers van wat offline geldt. De vraag is of deze redenering ook voor de toekomst kan worden doorgetrokken, waarbij on- en offline nog veel meer met elkaar verweven zullen zijn en internet nog veel meer maatschappelijk zal zijn ingebed.

Er zijn ook andere tendensen. In vooral de rechtsspraak wordt bijvoorbeeld vaak de voorrang gegeven aan het beginsel dat voor off- en online dezelfde (overheids-)regels moeten gelden. Ook bij deze stelling kunnen vragen worden gesteld. Moet niet onderscheid gemaakt worden tussen de zuiver normatieve vragen op het niveau van de waarden en normen, die in principe

off- en online op dezelfde manier moeten worden beantwoord en de uitwerking van dit normatieve antwoord in concrete regels? Op het niveau van concrete regels kunnen verschillen tussen of- en online best gerechtvaardig zijn, omdat beide sferen feitelijk niet gelijk zijn. Op enkele onderdelen is er bovendien al veel voor internet en ICT specifieke overheidsregeling van de EU of de Raad van Europa: denk aan het verbod op spam (bestuursrecht) en kinderporno (strafrecht). Ook bij bescherming van auteurs- en merkenrecht neemt de internationale overheidsregulering juist toe. Wellicht interessanter is de ontwikkeling in de Verenigde Staten, waar men federale wetgeving kent voor de particuliere en publieke sector, die directe eisen stelt aan de kwaliteit van (onder andere) ICT-investeringen, ook op het punt van veiligheid.

In meer algemene zin vragen wetenschappers zich af of geen overheidsregulering nodig is die, met goede controlemechanismen gewaarborgde, kwaliteitseisen stelt aan beroepsbeoefenaren, apparatuur en producten op ICT-terrein (zie bijv. Verhoef 2002). Waarom geen licentiesysteem voor beroepsbeoefenaren en een stelsel van certificatie voor apparatuur en producten? Waarom wel wettelijke eisen inzake autogordels die standaard moeten worden geleverd bij auto's maar geen wettelijke veiligheidsregels voor aanbieders van apparatuur, producten en diensten op ICT-terrein? Waarom gelden deze veiligheidseisen wel voor een andere maatschappelijk cruciale sector als de gezondheidszorg? Ook kan men zich afvragen waarom de overheid hier wel regels stelt voor de telecommunicatie (TC), maar niet voor de ICT-sector? Zo worden bij TC wel regels gesteld inzake de maximale duur van uitval. Falende ICT-technologie leidt jaarlijks in de Verenigde Staten en Europa tot meer dan honderd miljard schade. Onvoldoende wordt vooraf geanticipeerd op gegevensbescherming, fraudegevoeligheid en mogelijke aanvallen van binnenuit. Ook de in de Verenigde Staten gevoerde discussie over een mogelijk sterkere aansprakelijkheid voor producenten van software is voor ons land relevant. Dit instrument wordt extra interessant, wanneer de aansprakelijkheid wordt gelegd op het niveau van de onderneming en het management, waar de echte afwegingen inzake het belang van veiligheid worden gemaakt. Ook regels die de aansprakelijkheid uitbreiden tot de indirect veroorzaakte schade, kunnen het management en de onderneming stimuleren om het veiligheidsbelang naar waarde te schatten.

Uiteraard speelt ook hier het probleem van de deterritorialisering en de beperkte werking van nationale wetgeving, maar dit geldt minder voor vormen van publieke dienstverlening die zich op Nederland richten. Bij particuliere dienstverlening, die zich specifiek op ons land richt, blijven er weldegelijk aanknopingspunten voor Nederlandse regels en beleid. Ook kan gedacht worden aan een combinatie van nationale en Europese regelgeving, zoals op mediaterrein. Kortom deterritorialisering moet je niet zonder meer zien als een algehele hindernis voor handhaving van vooral nationale regels.

5 DE KERNVRAGEN VAN HOOFDSTUK ÉÉN BEANTWOORD

Eerst twee opmerkingen vooraf. Als publiek probleem is veiligheid bij internet en ICT pas vanaf 2001 een echt erkend vraagstuk en dan vooral bij een beperkte groep van specialisten. Een breed politiek en maatschappelijk debat is afwezig. In die zin verkeert het onderwerp nog in de fase van bewustwording. Hierbij komt een tweede aspect. In iedere sector hebben actoren er belang bij om slechte prestaties op het gebied van veiligheid te verzwijgen. Specifiek voor de onderhavige sector is dat men beter dan elders mislukkingen hier ook goed geheim *kan* houden. De gebrekkige ordening op dit terrein leidt tot weinig of geen regels op het terrein van de openbaarheid. Bovendien is het voor niet deskundigen heel moeilijk om vast te stellen of sprake is van tekorten in de veiligheidszorg. Om deze reden kan in dit stuk hier niet met dezelfde precisie worden geconcludeerd als bij andere casussen.

1)Wat is de aard van het veiligheidsprobleem? Zijn er 'wicked problems in termen van hoge of onkenbare waarschijnlijkheid, mogelijk ernstige schade en slechte corrigeerbaarheid?

Een cynicus zal de volgende vragen stellen: is er wel zoveel nieuws onder de zon? Is bij de introductie van nieuwe complexe netwerken en infrastructuren niet altijd de maatschappelijke afhankelijkheid van zo'n voorziening als heel groot en bedreigend gezien? Is niet sprake van een angst die vanzelf wel zal overgaan?

Allereerst moet worden geconstateerd dat de geschiedenis zich juist niet herhaalt. De introductie van internet ging in de jaren negentig niet gepaard met doemdenken en irrationele angsten, zoals bij de komst van de stoomtrein, maar juist met een grote euforie over de fantastische mogelijkheden van het medium. De verhalen over een nieuwe virtuele wereld en een nieuwe economische orde domineerden wereldwijd het debat. Zorg om veiligheid is pas in de eenentwintigste eeuw op de agenda gekomen. Belangrijker is het antwoord op de eerste vraag zelf. Het antwoord luidt dat er wel degelijk *wicked problems* zijn die specifiek voor internet en ICT zijn, in termen van hoge of in ieder geval onbekende waarschijnlijkheid, ernstige schade en beperkte corrigeerbaarheid. Het is niet de bedoeling alle genoemde factoren die onveiligheid bevorderen (paragraven 3.2 en 3.3) , hier nog eens de revue te laten passeren, maar enkele moeten nog maar eens worden genoemd. Allereerst de inherente instabiliteit van op zich al complexe, aan elkaar gekoppelde systemen. Juist een combinatie van kleine factoren, welke vooraf niet kon worden vermoed, kan bij veel koppelingen tussen op zich al complexe systemen tot grote schade leiden. Dit is het zogenoemde cascade-effect.

Ten tweede is er de afwezigheid van een adequate orde die alle actoren ertoe stimuleert om vooraf een goede afweging te maken tussen veiligheids- en overige aspecten. Specifiek voor internet is bovendien dat deze orde niet meer op de klassieke manier kan worden

vormgegeven, omdat internet een aantal aannames, die aan de klassieke ordening ten grondslag liggen, onderuit haalt: de aanname van territoriaal gebonden overheidsordening en de aanname dat natuurlijke en rechtspersonen kunnen worden geïdentificeerd. Er is wel een zekere zelfordening, maar die is in hoge mate bepaald door de Amerikaanse bestuurlijke en rechtscultuur, met een grote nadruk op de *civil society*.

In meerdere opzichten is zeker het Europese bestuurlijk en juridisch denkrégime niet adequaat om deze nieuwe problemen te lijf te gaan. In Tunis 2005 is wel een begin met deze ordening gemaakt, maar niet meer. De nieuwe concepten die nodig zijn, verkeren nog in het begin van hun ontwikkeling. Juist die gebrekkige orde versterkt een derde specifieke karakteristiek van het veiligheidsrisico op internet, namelijk onvoldoende transparantie en het geringe belang dat actoren als overheden en bedrijven hebben om opening van zaken te geven en incidenten en systeemfouten openbaar te maken, teneinde het vertrouwen van de eindgebruiker niet te schaden. Het veiligheidsrisico is vaak slechts voor een beperkte groep van belanghebbenden en professionals kenbaar. Ook deze factor versterkt de 'gemeenheid' van het probleem. Omtrent de ernst van de schade zijn de eerder genoemde schattingen ten gevolge van verkeerde ICT-beslissingen in zowel de Verenigde Staten als Europa voldoende indicatief, waarbij nog geen rekening is gehouden met de immateriële schade in termen van aantasting van privacy, de authenticiteit van de informatie en de toegankelijkheid. De beperkte corrigeerbaarheid komt vooral naar voren in de te geringe tijd om op kwaadaardig misbruik van kwetsbaarheden met herstelsoftware te reageren.

2) Welke inhoudelijke afwegingen zullen in de toekomst centraal moeten staan?

Algemeen

De Geneefse verklaring van de WSIS inzake de ordenende beginselen voor de informatiemaatschappij van 2003 stelt, dat veiligheid in de zin van waarborging van privacy, de authenticiteit van de gegevens en bescherming van consumenten een *randvoorwaarde* is voor de ontwikkeling van internet op basis van beginselen als vrijheid, gelijkheid, pluriformiteit, ontplooiing, toerusting en intellectuele eigendomsrechten. In die zin is geen afweging nodig tussen veiligheid en andere belangrijke waarden doelen van ICT en internetbeleid. Bij internet en andere ICT systemen die zo lek zijn als een mandje, komen immers ook de andere beginselen niet tot hun recht. In abstracto is er derhalve geen botsing tussen de eis van veiligheid en andere beginselen. In concreto zullen zich wel afwegingsvragen manifesteren tussen veiligheid en andere beginselen, vooral wanneer juridische instrumenten voor de veiligheid worden ingezet.

Aan de producentenkant kan gedacht worden aan inperking van de vrijheid door een systeem van licensies voor producenten van software, of door kwaliteitsregels voor ICT-producten. Aan de consumentenkant kan gedacht worden aan mogelijke diploma's die verplicht worden gesteld. Bedacht moet worden dat dit soort afwegingsvragen ook in talloze andere sectoren zoals de zorg spelen en dat beperking van de vrijheid hier wel is geaccepteerd. Bij de toenemende maatschappelijke inbedding van internet, zullen dit soort afwegingen derhalve hierbij ook een rol gaan spelen. De beleidsredenering bij de afweging is bij zorg en internet in principe gelijk: mag de vrijheid van de producent worden ingeperkt om de vrijheid van de consument te bevorderen en moeten ook consumenten geen eisen worden gesteld, omdat zij anders een mogelijk gevaar zijn voor anderen? Het verschil tussen traditionele sectoren als zorg en Internet betreft de instrumentatie, gegeven de verschillende context. Hierover gaat de slotvraag die verderop zal worden behandeld.

Twee meer specifieke afwegingsproblemen

Deze betreffen de relatie tussen veiligheid en het voorzorgsbeginsel en de uitwerking van het veiligheidsbeleid op bovennationaal niveau. In de eerste ontwikkelingsfase van internet is uitdrukkelijk voorrang gegeven aan de baten die ICT en internet opleverden in termen van economische en sociale vernieuwing boven het vermijden van mogelijke slecht inschatbare risico's. In deze onzekere situatie had strikte toepassing van het voorzorgsbeginsel – bij twijfel niet doen - een flinke rem betekend op de verdere uitbouw van internet en ICT. Het is, achteraf bezien, twijfelachtig of zo'n strikte toepassing een goede zaak zou zijn geweest. Aan de andere kant zijn bepaalde elementen van dit beginsel voor ook deze sector functioneel, zoals de noodzaak om bij het ontwerpen van nieuwe software de mogelijke risico's zo goed mogelijk *ex ante* te evalueren, af te wegen en zo nodig een bepaald risico te accepteren, omdat men de kosten beheersbaar acht. Een dergelijke procedure is gevolgd bij het ontwerp van het internationale systeem van creditcards. Ook de Amerikaanse regel dat overheden ICT en internetproducten moeten aanschaffen die op de markt hun waarde hebben bewezen, is een goed voorbeeld. Onnodige risico's waarbij iedere overheidsinstantie zelf het wiel gaat uitvinden en gaat experimenteren, worden aldus vermeden. De onderhavige casus laat zien dat het voorzorgsbeginsel vraagt om nadere differentiatie, waarbij soms lichtere en soms zwaardere gradaties functioneel zijn. Men kan zeggen dat noch een zware uitwerking, noch een negeren van het voorzorgsbeginsel in deze sector past.

Een tweede afwegingsprobleem dat in de toekomst belangrijker wordt ligt op het terrein van mondiaal recht. De verschillen in waardehiërarchieën en bestuurlijke praktijken tussen westerse, rechtstatelijke democratieën enerzijds en opkomende landen als China anderzijds. kunnen moeilijke keuzevragen oproepen. De uitgebreide Chinese internetpolitie heeft geheel andere taken dan die in westerse landen.

Het is relatief gemakkelijk mondiaal een aantal uitgangspunten te formuleren. Juist bij de uitwerking komen de verschillen weer in volle hevigheid terug.

3) De vraag van verantwoordelijkheidsdeling

Algemeen
De toedeling van verantwoordelijkheid vraagt hier een doorvertaling naar aansprakelijkheid, die vervolgens zijn uitwerking kan krijgen in stimulansen voor effectieve veiligheidszorg. Zowel de ICT-sector als geheel, als het systeem van internet, missen een algemeen geldende regeling van toedeling van verantwoordelijkheid. Dit kan als een lacune worden aangemerkt omdat bij zulke complexe technologisch nieuwe systemen met zeer verschillende interacties tussen meerdere actoren de verantwoordelijkheidsdeling niet zonder meer vanzelfsprekend is. Er is een discrepantie tussen het toenemend maatschappelijk belang van ICT en internet enerzijds en de afwezigheid van adequate systemen van deling van verantwoordelijkheid en van toedeling van aansprakelijkheid anderzijds.

Mondiaal niveau
Hier is vooral frappant dat particuliere professionele instellingen zoals ICANN een beheers- en ten dele bestuursverantwoordelijkheid hebben, die bij andere infrastructuren bij de overheden liggen. De taak van een particuliere organisatie als het ICANN overstijgt allang het technische beheer. ICANN maakt ook beleidskeuzes (Alberdingk Thijm 2004: 110). Najaar 2005 zijn, als gezegd, in Tunis wel enkele duidelijke stappen in de goede richting gezet. Gekozen is voor een systeem van multi-actoren, een gedeelde verantwoordelijkheid van overheden, professioneel-technische organisaties, het bedrijfsleven en non-gouvermentele organisaties. Een aantal inhoudelijke basisprincipes voor beleid waren al eerder in Genève geformuleerd en zijn in Tunis bevestigd. Bovendien is erkend dat publieke belangen, samenhangend met Internet een zaak zijn van (samenwerkende) overheden. Het begrip ‘publiek belang’ is niet ingevuld, maar kennelijk wordt gedoeld op klassieke staatstaken als grondrechten en veiligheid. Organisaties als het ICANN moeten zich beperken tot technische zaken van beheer en ook standaardisering. Natuurlijk is de scheiding niet sluitend, maar het op te richten Gemeenschappelijk Forum maakt wederzijdse afstemming mogelijk. In ieder geval is een inhoudelijk en institutioneel kader uitgezet.

Enkele zaken vallen in deze verklaring van Tunis op. Over de eigen verantwoordelijkheid van de eindgebruiker wordt niet gerept, terwijl er goede redenen zijn om die te versterken, zo kwam in het voorafgaande meerdere malen naar voren. De belangrijkste overweging luidt dat de nieuwe technologie de mogelijkheid biedt van interactiviteit, hetgeen voor de capaciteit van de eindgebruiker om verantwoordelijkheid te dragen versterkt (zie ook Van Eijk et al. 2005). Wel is de eigen verantwoordelijkheid van nationale overheden in Tunis erkend.

Zij kunnen eigen rechtsmacht uitoefenen, wanneer er sprake is van duidelijk te lokaliseren vitale nationale belangen.

Europees niveau
Kenmerkend op dit niveau is dat de overheid hier duidelijk aanwezig is als regelsteller en de professioneel technische organisaties hier minder sterk domineren. Vaak is sprake van gedeelde verantwoordelijkheid: een combinatie van kaderstellende overheidsregulering en zelfregulering. De regelgeving is wel partieel en algemene regels inzake aansprakelijkheid ontbreken. Daarnaast faciliteert de overheid in termen van onderzoek, voorlichting, met name in de vorm van een waarschuwingsdienst, en educatie. De concentratie van regelgeving op Europees niveau heeft een duidelijke ratio: er is immers sprake van grootschaligheid en er zijn geen fundamentele normatieve verschillen tussen de betrokken landen, zoals op mondiaal VN-niveau.

Nationaal niveau
De faciliterende rol van de overheid is hier ook prominent aanwezig. Autonome Nederlandse regelgeving ontbreekt. De overheid is hier wel aanwezig als regisseur, in het kader van het project Nacotel: de overheid organiseert het gesprek tussen alle relevante partijen en bevordert dat afspraken worden gemaakt, voor het geval er zich calamiteiten voordoen op het terrein van telecommunicatie, ICT en internet. Daarnaast is de overheid zelf grootgebruiker van ICT en van internet en dus ook een gewone marktpartij.

De rol van professionals
Toekomstige vragen van verantwoordelijkheid zullen zeker de rol van de professionals betreffen. Daarbij kan in eerste instantie gedacht worden aan de provider. Moet hij de klant niet faciliteren, hem informatie geven en een pakket van veiligheidsmaatregelen aanbieden? Mag van de provider niet verwacht worden dat hij maatregelen neemt, wanneer een van zijn klanten gebruik maakt van een evidente zombiecomputer? Natuurlijk, zeker nationale regelingen en zorgplichten voor providers hebben hun beperkingen: veel ICT-bestanden vallen buiten de klassieke serviceprovider en het zombieprobleem is in hoge mate een mondiaal probleem. Daartegenover staat dat nationale en zeker Europese regels in ieder geval een beperkt nut kunnen hebben en dat de operationele problemen van de beperkte effectiviteit van regels, op zich geen reden zijn om de principiële vraag van verantwoordelijkheid en aansprakelijkheid van de provider niet aan de orde te stellen.

Ten tweede is er de vraag van de verantwoordelijkheid en aansprakelijkheid van de softwareproducent. In het algemeen wordt in contracten van producenten met gebruikers de aansprakelijkheid van de softwareproducent minder goed of niet geregeld (mededeling geraadpleegde deskundige). Waar statistisch de kans groot is dat bij ontwikkeling van

software fouten worden gemaakt, is er extra reden om de vraag van aansprakelijkheid van de producent van software aan de orde te stellen. Dit stimuleert de producent om te investeren in nieuwe technieken om de complexiteit te reduceren en om een evaluatie, analyse vooraf van mogelijke risico's te maken. Zoals eerder is gesteld, ligt het meer voor de hand de aansprakelijkheid op het niveau van de onderneming te situeren en niet op dat van de professional, van de individuele werknemer.

4) Wijze van organisatie en instrumenten

Maatschappeljke mechanismen voor ordening
Dit terrein kent enerzijds veel vormen van marktfalen, met veel particuliere monopolie- en machtsposities aan de aanbodkant. Anderzijds versterkt internet bepaalde maatschappelijke correctiemechanismen, zoals het reputatiemechanisme. Het beeld is derhalve gemengd.

Technologische instrumenten
ICT en internet kennen vanouds een belangrijke negatieve sanctie, te weten uitsluiting. Daarnaast vindt veel ordening plaats in het kader van de productie van software; waar elders de overheid regels stelt, bepaalt in deze sector de professional bij de inrichting van de software vaak wat wel en niet kan, met alle reeds genoemde problemen van legitimatie van dien.

Informatieve instrumenten
Veel van dit soort instrumenten worden ingezet: anticiperend onderzoek in kennis en expertisecentra, voorlichting, educatie, centra voor waarschuwing en dergelijke. Toch vallen enkele lacunes op. Veel mislukkingen in deze sector blijven buiten de openbaarheid. In de private sector zijn er in Europa op dit punt geen regels. Er is evenmin een ICT-ongevallenraad, te vergelijken met de Transportongevallenraad, die onafhankelijk onderzoek doet naar die ICT-calamiteiten, waarmee overduidelijk publiek belangen zijn gemoeid. Zo'n raad kan het maatschappelijke leervermogen versterken.

Regelgeving
Op dit punt is het beeld gemengd. Toch zijn enkele tendensen duidelijk. De dogmatische voorkeur voor alleen zelfregulering verdwijnt. In Europa wordt de voorkeur gegeven aan co-regulering. Het internationale strafrecht breidt zich op dit terrein uit. Nationaal kent de nieuwe TC-wet regels voor calamiteiten. In de Verenigde Staten zijn privaatrechtelijke en publiekrechtelijke regels inzake ICT-investeringen in opmars, die respectievelijk de aandeelhouders en de belastingbetaler moeten beschermen tegen slechte besluitvorming op dit punt. Het voordeel van privaatrechtelijke openbaarheids- en aansprakelijkheidsregeling is vooral dat zij een betere evaluatie vooraf van mogelijke veiligheidsrisico's bevorderen,

maatschappelijk mechanismen als reputatie versterken, en in hoge mate *self-executing* zijn, en geen zwaar uitvoerend ambtelijk apparaat vergen.

Overige instrumenten

De nationale overheid is in bepaalde opzichten regisseur en brengt partijen bij elkaar bij de voorbereiding op crisisbeheersing (plan Nacotel). Verder biedt de belangrijke positie van de overheid als grootgebruiker van ICT de mogelijkheid om ten opzichte van andere gebruikers van ICT het goede voorbeeld te geven.

Conclusie

Juist bij een gedifferentieerd verschijnsel als ICT en internet past eerder een breed arsenaal van verschillende typen instrumenten die elkaar kunnen versterken.

LITERATUUR

Alberdingk Thijm, Ch. (2004) *Het nieuwe informatierecht*, Den Haag: Academic Services.

Bruijn, H. de, M. van Eeten, M. Kars, J. van Till, en H. Voort (2004) *The governance of E-security. A framework for policy*, Advies aan het ministerie van economische zaken, Delft: Stratix Consulting.

Ecotec (2005) *Preliminary analysis of the contribution of EU Information Society policies and programmes to the Lisbon and sustainable development strategies*, Birmingham.

Eijk, N. van, L. Asscher, M. Helberger en J. Kabel (2005) *Regulering van de media in internationaal perspectief*, webpublicatie WRR nr. 6, Amsterdam: Amsterdam University Press.

Europese Commissie (2005) *i2010 – Een Europese informatiemaatschappij voor groei en werkgelegenheid, http://www.europanu.nl/9353000/1/j9vvh6nf08temv0/vhivhg33vqq0*.

House of Representatives of the United States (2001) *Hearing before the Subcommittee on commerce, trade and consumer protection regarding Cyber security*, serial no. 107 -04, Washington: United States government printing office.

Kaspersen, H.W.K. (2004) 'Bestrijding van cybercrime en de noodzaak van internationale regelingen', *Justitiële Verkenningen*, nr.8, blz. 58-75.

Koops, E.J. en A.B.M. Lips (2003) 'Wie reguleert het internet? Horizontalisering en rechtsmacht bij de technische regulering van het internet', blz. 261-314 in H. Franken (red.) *Zeven essays over informatietechnologie en recht*, Den Haag: Sdu Uitgevers.

Koops E.J., F. van der Hof en V. Bekkers (2005) 'Risico's in de netwerksamenleving : over vervlochten netwerken en kwetsbare overheden', blz. 671-706 in V.J.J.M. Bekkers, A.M.B. Lips en A. Zuurmond (red.) *ICT en openbaar bestuur*, Utrecht: Lemma 2005.

Luijf, H.A.M. (2004) 'De kwetsbaarheid van de ICT samenleving', *Justitiële Verkenningen*, nr. 8, blz. 22-33.

Ministerie van economische zaken en Ministerie van verkeer en waterstaat (2001) *Nota Kwetsbaarheid op internet. Samenwerken aan meer veiligheid en betrouwbaarheid*, Den Haag.

Ministerie van economische zaken (2005) *De toekomst van de elektronische communicatie*, Den Haag.

Ministerie van economische zaken (2006) *Nota Nederland in verbinding. Beleidskader voor de elektronische communicatie*, Den Haag.

Organisation for Economic Cooperation and Development (2002) *Guidelines for the security of information systems and networks*.

Rand Europe (2003) *Cyber security in an era of technological change. Report on a conference held at The Hague*, 9 april 2001.

Sociaal en Cultureel planbureau (2004) *In het zicht van de toekomst,* Den Haag: Sdu.

Stol, W.Ph. (2004) 'Trends in cybercrime', *Justitiële Verkenningen*, nr. 8, blz. 76-94.

Verhoef, Ch. (2002) 'Quantative IT portfolio management', *Science of Computer Programming* 45, 2002: blz. 1-96.

Verhoef, Ch. (2005) 'Tijd rijp voor IT-portfoliomanagement', 19 -09-2005, www.cs.vu.nl/-x/knipselkrant/inzake.html.

World Summit on the Information society, Geneva 2003 –Tunis 2005; website: www.itu.int/wsis/wgig.index.html.