TNO Informatie- en Communicatietechnologie

TNO-rapport

035.31231

ICT-veiligheidsbeleid in Nederland – Analyse en overwegingen bij herijking

Datum	25 september 2006
Auteur(s)	Drs. Sandra Helmus Ir. André Smulders Dr. Ir. Frans van der Zee (red.)
Exemplaarnummer	Eindrapport deel II, project Herijking ICT Veiligheid in opdracht van het Ministerie van Economische Zaken.
Oplage	
Aantal pagina's	21
Aantal bijlagen	1
Opmerkingen	Van deel I, getiteld 'ICT-veiligheidbeleid in Nederland – een quickscan', verscheen begin september 2006 eveneens een eindrapport.

Inhoudsopgave

1 ICT-veiligheid – het nu 3
1.1 ICT-veiligheid en vertrouwen – over dynamiek, complexiteit en beleid 3
1.2 Huidig ICT-veiligheidsbeleid in Nederland - vorm en inhoud 6

2 ICT-veiligheid – de toekomst 11
2.1 De ‘rationale’ voor herijking van het ICT-veiligheidsbeleid 11
2.2 Naar een robuust ICT-veiligheidsbeleid 11

3 Samenvatting aanbevelingen ICT-veiligheid 17

Annex I. Marktfalen en systeemfalen 19

Referenties 21

1 ICT-veiligheid – het nu

1.1 ICT-veiligheid en vertrouwen – over dynamiek, complexiteit en beleid

Toenemende complexiteit van infrastructuur en diensten. De wereld van elektronische communicatie - en meer algemeen ICT - kenmerkt zich door een sterke dynamiek, waarin technologische verandering en innovatie de toon zetten, met een veelheid aan nieuwe producten en gebruiksmogelijkheden voor burgers, bedrijven en overheden. Het gebruik van informatiesystemen en netwerken en de context waarin informatietechnologie zijn weg vindt zijn sterk veranderd in de afgelopen jaren. Steeds krachtiger pc's, convergentie in technologieën en markten en wijdverspreid gebruik van open netwerken (het internet) bepalen tegenwoordig het speelveld, waar vroeger beperkte *stand-alone* systemen en gesloten netwerken meer de overhand hadden. Koppelingen en verwevenheid van informatiesystemen en netwerken maken dat de complexiteit rond ICT-infrastructuur belangrijk is toegenomen. Het is vaak niet evident en eenduidig welke afhankelijkheden binnen deze complexe infrastructuur bestaan en wie waarvoor verantwoordelijk is. Tegelijkertijd zien we een trend naar ontkoppeling van diensten en infrastructuur. Verliep vroeger de telefonie via het vaste net en televisie van de antenne of kabel, tegenwoordig zijn deze diensten leverbaar over verschillende infrastructuren. De aanbieder van de dienst is daarbij niet automatisch eigenaar van de infrastructuur waarover deze diensten worden aangeboden. Denk bijvoorbeeld aan VOIP operators die geen eigen infrastructuur hebben, maar alleen het opzetten van verbindingen faciliteren. Ook voor organisaties die zelf gebruik maken van de ICT-infrastructuur is het vaak niet meer inzichtelijk wie voor welk onderdeel van deze infrastructuur aangesproken kan worden.

Naarmate mogelijkheden, belang en impact van ICT op het economisch en maatschappelijk leven toenemen, wordt ook de roep om en het belang van veiligheid van informatiesystemen en netwerken, en breder ICT, steeds pregnanter. Als gevolg van de toenemende interconnectiviteit is de kwetsbaarheid van informatiesystemen en netwerken aanzienlijk toegenomen, zowel in aantal als in diversiteit van mogelijke bedreigingen. E-crime bijvoorbeeld, waaronder identiteitsdiefstal en online fraude (inclusief pogingen daartoe), en de verspreiding van malware zijn wereldwijd in omvang sterk gestegen (bijvoorbeeld http://research.pestpatrol.com). Dit geldt ook voor de rijke landen (OECD, 2005; Tanaka, 2005). Nederland gaat met Finland en Ierland in de EU aan kop waar het computervirusaanvallen op bedrijven betreft (Tanaka, 2005; Eurostat, 2005). Ook als het gaat om 'unauthorised access' bij bedrijven scoort Nederland hoog (d.w.z. negatief en potentieel gevaarlijk) in de vergelijkende statistieken. Veiligheid is onlosmakelijk verbonden met vertrouwen. Vertrouwen op zijn beurt is onontbeerlijk voor de verdere verspreiding en integratie van ICT, en daarmee gepaard gaande baten, in onze samenleving.

ICT-veiligheid - verschillende niveaus en verschillende onderliggende belangen. Het belang van veiligheid doet zich op verschillende niveaus gelden: zo is de individuele burger gediend bij een veilig gebruik van ICT waarin zijn privacy is gewaarborgd en waarin ongestoord en veilig communiceren en handelen met anderen centraal staat. Dit geldt niet alleen voor het gebruik van bijvoorbeeld e-mail en MSN-achtige diensten, maar ook voor zaken doen met de bank (eBanking), met bedrijven (B2C), en de overheid (G2C). Wat geldt voor burgers geldt evenzeer voor bedrijven en

overheden, zij het dat de intensiteit van interconnectiviteit daar hoger ligt en het belang van continuïteit en bescherming van communicatie- en informatiestromen nog pregnanter liggen. Voor de samenleving als geheel geldt eveneens dat continuïteit van informatie- en communicatiestromen en vitale systemen die mede op ICT berusten geborgd moet zijn. Onvoldoende borging kan in geval van incidenten en calamiteiten leiden tot aanmerkelijke economische en maatschappelijke schade, die zelfs zo ver kan gaan dat we spreken over maatschappijontwrichtende gebeurtenissen. Grootschalige uitval van ICT-infrastructuur of andere majeure *cyber incidents* zijn niet vergelijkbaar met de financiële, fysieke of psychisch-emotionele schade die een individuele gebruiker kan lijden door spam, phishing, virussen of andere vormen van gerichte *cyber attacks*. De mogelijke schaal, intensiteit en impact (financieel-materieel, psychisch-emotioneel dan wel fysiek) van ICT-onveiligheid doet er dan ook toe in het stellen van prioriteiten, voor individuen, bedrijven maar ook de overheid.

ICT-veiligheid: netwerkeffecten en positieve externe effecten. Het feit dat gebruikers van internet en open ICT-systemen met elkaar verbonden zijn (interconnectiviteit) heeft niet alleen als/tot gevolg dat de potentiële baten van gebruik toenemen naarmate meer gebruikers zijn aangesloten en zij meer gebruikmaken (vgl. 'always on') van internet. Dit geldt evenzeer voor beschermingsmaatregelen door individuele gebruikers. Naarmate meer gebruikers dergelijke acties treffen, zal het algehele effect door dezelfde netwerkeffecten navenant groter zijn, *ceteris paribus*. Deze redenering geldt echter ook de andere kant op. Naarmate downloaden en uploaden van informatie meer onbeschermd en willekeurig gebeurt, zullen de risico's van ICT-onveiligheid toenemen. In formele zin kan gesteld worden dat netwerkeffecten maken dat acties ter bevordering van ICT-veiligheid door individuele actoren zich vertalen in positieve externe effecten[1] voor andere gebruikers. Zie verder Annex 1 voor een nadere belichting van ICT-veiligheid vanuit het perspectief van markt- en systeemfalen.

Uiteenlopende inschattingen van risico's en belang van ICT-veiligheid. Investeringen in ICT-veiligheid worden door actoren gemaakt op basis van kosten en mogelijke baten van ICT die deze investering oplevert in de toekomst[2]. Deze rationele afweging van kosten en baten is mede afhankelijk van de inschatting van bestaande en toekomstige risico's van ICT-onveiligheid. Het inschatten van dergelijke risico's is buitengewoon lastig, zeker voor individuele burgers / consumenten, en is bovendien afhankelijk van het type gebruik. Naarmate het belang van continuïteit en veiligheid van versturen en ontvangen van informatie en communicatie toeneemt, zal ook de neiging om meer veiligheidsmaatregelen te treffen toenemen. Dit is evenwel mede afhankelijk van de mate waarin actoren geïnformeerd zijn over de mogelijke risico's en daaraan zelfstandig en evenwichtig conclusies en beslissingen kunnen verbinden. In een professionele omgeving (bedrijf) is dit doorgaans in redelijke mate het geval. Voor individuele consumenten ligt deze kwestie lastiger. Los van de vraag naar bewustzijn en geïnformeerdheid over risico's bij individuele actoren, lijkt er een discrepantie te bestaan tussen de inschatting die individuele actoren (bedrijven, burgers) maken van risico's en van beslissingen om in ICT-veiligheid te investeren, en de perceptie en

[1] Formeel gedefinieerd: als de niet in marktprijzen of subsidies verrekende positieve invloed die van economische handelingen uitgaat op de productievoorwaarden waaronder goederen en diensten worden voortgebracht dan wel op het bevredigingspeil (nut) van andere huishoudingen. Externe effecten zijn een vorm van marktfalen die in principe overheidsingrijpen rechtvaardigen. In het bovenstaande geval is de toename van de ICT-veiligheid overigens juist een reden voor de overheid om niet in te grijpen.

[2] De term investeringen wordt in dit verband ruim gehanteerd. Investeringen behelzen zowel financiële uitgaven in ICT-veiligheid als aandacht, tijd en moeite die gemoeid is om het ICT-veiligheidsniveau te verhogen.

inschatting van de noodzaak en wenselijkheid van investeringen in ICT-veiligheid op maatschappelijk niveau. Als 'hoeder van het algemeen belang' is de overheid hier primair aan zet (zie ook Annex 1 over markt- en systeemfalen). Hoe is echter in een complexe, dynamische omgeving van *interconnectivity* op voorhand niet evident. In hoofdstuk 2 worden hiervoor handreikingen gegeven.

De rationaliteit van onderinvesteringen en afwentelingsgedrag. Het kan voor individuele actoren rationeel kan zijn om te onderinvesteren in ICT-veiligheid. Vertrouwen op ingrijpen door de overheid in geval van incidenten of calamiteiten kan daarbij een rol spelen (afwentelingsgedrag). Indien iedereen, of een significant deel van de populatie actoren, dergelijk gedrag vertoont kan dit op macroniveau, d.w.z. op het niveau van netwerken, leiden tot risico's inzake mogelijke impact/schade. Het dilemma waarin de overheid verkeert, is dat zij dit weliswaar kan signaleren, maar dat zij in veel gevallen niet eigenmachtig de ICT-veiligheid op een hoger niveau kan brengen. De mogelijkheden tot direct ingrijpen zijn beperkt.

Deze constatering staat overigens nog los van de vraag of dit vanuit meer ideologisch getinte optiek überhaupt wenselijk zou zijn, in een tijdperk waarin de politiek burgers en anderen aanspreekt eigen verantwoordelijkheden te nemen en te dragen en waarin de overheid meer en meer een pacificerende rol in onze maatschappij inneemt. Het adagium van het Kabinet Balkenende-II "van zorgen voor naar zorgen dat" is daarvan een duidelijke exponent. In het huidige ICT-veiligheidsbeleid wordt daarom niet alleen van de overheid maar ook van andere betrokken partijen een bijdrage verwacht in het garanderen, bewaken en beschermen van de ICT-veiligheid.

ICT-veiligheid als containerbegrip. ICT-veiligheid is een containerbegrip met vele dimensies en gedaanten op verschillende niveaus, geografisch (globaal, nationaal, regionaal), type actor (burger/consument, bedrijf, overheidsorganisatie) of anderszins (sector, value chain of netwerk, maatschappelijk domein). ICT-veiligheid kan worden beschouwd als een onderdeel van een vraagstuk dat wel wordt aangeduid als de 'new security economy' waarin nieuwe risico's, maatschappelijk zowel als privaat, centraal staan (OECD, 2004).

Dat ICT-veiligheid een containerbegrip is heeft belangrijke gevolgen voor het wie, waar en hoe van oplossingen en het streven naar een optimale 'ICT-veiligheid'. Technologische oplossingen zijn daarbij voor de hand liggend, maar niet noodzakelijkerwijs dekkend, noch *a priori* waterdicht. De onvoorspelbaarheid van menselijk handelen – zowel in goede als in kwade zin – en de feilbaarheid van menselijk handelen pleiten voor het zoeken naar oplossingen gericht op *resilience* (weerbaarheid) en bewustwording en -making.

Een cultuur van ICT-veiligheid en best practices. De door de OESO opgestelde richtlijnen voor de veiligheid van informatiesystemen en netwerken waarin het ontwikkelen van een cultuur van veiligheid ('Towards a Culture of Security') centraal wordt gesteld vormen een goede leidraad voor het vergroten van de ICT-veiligheid waaraan alle betrokkenen kunnen bijdragen. Daarbij zijn de volgende 10 kernprincipes in het geding: Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management, and Reassessment (OECD, 2003). Hoewel nuttig en nodig, geven de OESO richtlijnen geen blauwdruk hoe ICT-veiligheidsbeleid het beste georganiseerd kan worden, of hoe de 10 kernprincipes in onderlinge samenhang dienen te worden afgewogen. Best practices

kunnen een leidraad voor beleid vormen, maar zijn in een sterk dynamische omgeving bepaald geen garantie voor dekkendheid, effectiviteit of efficiëntie van beleid. Op het individuele niveau van burgers, bedrijven en overheden zelf kan overdracht van kennis waaronder best practices uiteraard wel effectief zijn. Ook van bad practices kan een leereffect uitgaan.

1.2 Huidig ICT-veiligheidsbeleid in Nederland - vorm en inhoud

In een speelveld waarin technologieën, producten en daarmee ook gebruiksmogelijkheden voor burgers, bedrijven en overheden zich snel ontwikkelen, is het vaststellen van een eenduidig en welomschreven ICT-veiligheidsbeleid voor nu en morgen een lastige zaak. Beleid dient flexibel te zijn en in te spelen op behoeften, knelpunten en kansen die ontstaan. Beleid in een snel veranderende complexe omgeving vraagt juist ook om wisselwerking met ontwikkelingen, in samenspraak met betrokken partijen, zonder dat beleid een onnodige rem zet op die ontwikkelingen. In een dergelijke dynamische innovatieve *technology*- en *market-driven* omgeving is geregelde aanpassing van staand beleid een natuurlijke en tevens noodzakelijke gang van zaken.

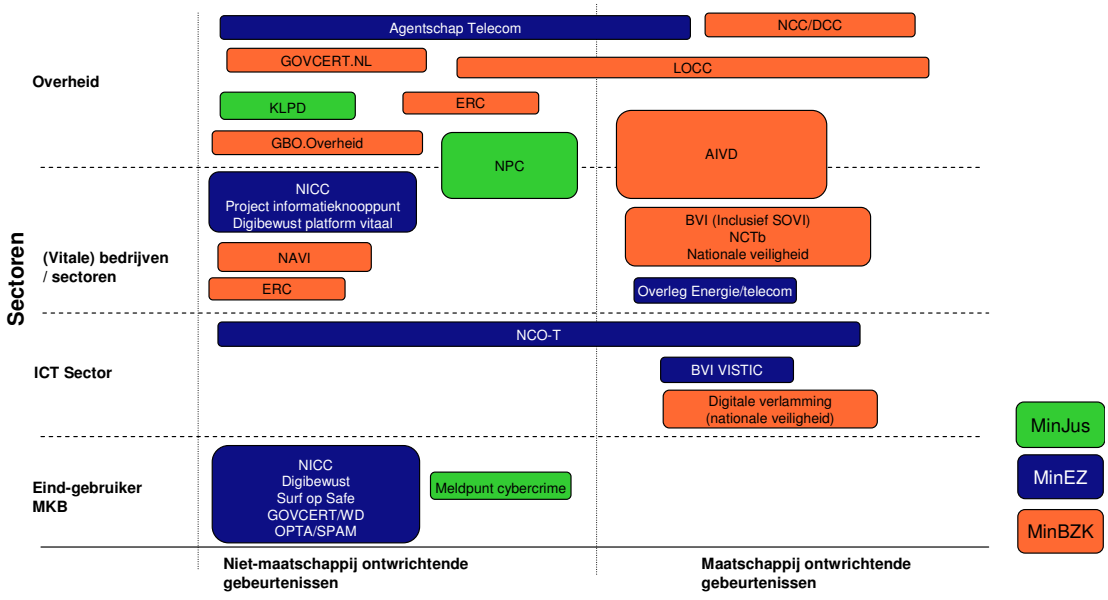
Collectieve èn private actie. In maatregelen ter verbetering en versterking van de ICT-veiligheid dient een duidelijk onderscheid gemaakt te worden tussen (overheids)beleid en collectieve actie enerzijds en individuele (private) actie anderzijds. Met de term ICT-veiligheidsbeleid in het navolgende worden zowel (overheids)beleid als vormen van collectieve actie bedoeld. Daarmee wordt een beleidsbegrip in brede zin gebezigd, waarin niet alleen wet- en regelgeving, maar ook bewustwording, informatievoorziening, coördinatie (inclusief vormen van zelfregulering en toezicht) en het gebruik van financiële en andere prikkels (*incentives*) in beschouwing worden genomen. Tevens worden in dit brede beleidsbegrip ook collectieve actie door anderen dan de overheid alleen begrepen, merendeels te vatten onder de brede noemer van publiek-private samenwerking (PPS). Naast beleid leveren ook individuele burgers en bedrijven zelf actief een bijdrage aan het vergroten van de ICT-veiligheid. Door intrinsieke netwerkeffecten kan actie door de één een positieve uitwerking hebben op de ICT-veiligheid van anderen. Bovendien kan de bereidheid tot individuele actie op haar beurt (en daarmee positieve externe effecten als gevolg) door beleid worden versterkt.

Het ICT-veiligheidsbeleid in Nederland heeft sinds het einde van de jaren negentig een stormachtige opkomst gekend. Veel beleid is geformuleerd in de vorm van programma's en projecten; sommige daarvan zijn in de loop der jaren geëvolueerd tot zogenoemde structurele beleidsdossiers. Tegelijkertijd zijn er rondom ICT-veiligheid nieuwe instituties opgericht, soms op instigatie van ministeries, soms op basis van eigen initiatief van maatschappelijke geledingen en sectoren. Zelfregulering in de vorm van convenanten en publiek-private samenwerking (PPS) blijken ook op ICT-veiligheidsgebied populaire vormen van overleg, bestuur en besluitvorming te zijn. Nadeel van dergelijke *poldermodel*vormen van overleg- en besluitvorming zijn de beperkte democratische verantwoordings- en controlemogelijkheden.

Zoals uit het TNO-rapport 'ICT-veiligheidsbeleid in Nederland – een quickscan' blijkt, ressorteert ICT-veiligheidsbeleid in Nederland niet onder één ministerie. De ministeries BZK, Justitie en EZ hebben verschillende rollen, taken en verantwoordelijkheden in het ICT-veiligheidsbeleid, waarvan sommige coördinerend en andere uitvoerend, naast

beleidsconcipiëring en visievorming. Daarnaast zijn er tal van publiek-private samenwerkingsvormen, waarin overheid en private partijen gezamenlijk optrekken en die door de overheid geheel of gedeeltelijk gefinancierd worden. Deze PPS-constructies hebben veelal de vorm van platforms, projecten en campagnes en zijn merendeels gericht op bewustwording, kennisoverdracht en informatie-uitwisseling.

Ministeries blijken dikwijls samen te werken in gedeelde verantwoordelijkheden, soms onder algehele coördinatie van één ministerie, met uitvoerende bevoegdheden voor en door andere ministeries. Soms blijken uitvoerende taken en verantwoordelijkheden te zijn neergelegd bij non-gouvernementele organisaties of publiek-private samenwerkingsverbanden waar de overheid voor (een deel van) de financiering zorg draagt en de uitvoering aan marktpartijen wordt overgelaten. Deze verdeling is soms thematisch, soms ook op basis van het proces of de ICT-veiligheidsketen zelf. Zo is er waar ICT-veiligheid over grote en kleine *cybercrime* gaat een verdeling in verantwoordelijkheden tussen ministeries te maken naar preventie, algehele coördinatie en bestuur, uitvoering, als ook opsporing en vervolging. Als het gaat om *terrorismebestrijding* is een dergelijk onderscheid eveneens relevant. Bij (grootschalige) *incidenten* is het tevens van belang dat de continuïteit van communicatie- en informatiestromen en van vitale infrastructuur gegarandeerd is en dat voldoende *back-up capaciteit* beschikbaar is (het voorbereid zijn op). Het spreekt voor zich dat naast continuïteit op het ICT-veiligheidsdossier ook zaken als privacy, integriteit en exclusiviteit (diverse vormen en gradaties van *classified information*; staats- en/of bedrijfsgeheimen; het tegengaan van staats- en/of bedrijfsspionage) meespelen die de nodige terughoudendheid in de publieke arena met zich meebrengen. Publieke verantwoording in alle details en finesses is dan niet op zijn plaats. Dit geldt evenzeer voor bijvoorbeeld terrorisme en het grote-incidentenbeleid.



Figuur 1. Initiatieven naar type gebeurtenis en doelgroep[3]

[3] Deze indeling naar doelgroep is ontleend aan de door EZ uitgezette enquête in het kader van dit onderzoek. Hoewel nuttig in onderscheid, is er ook kritiek mogelijk op deze indeling. Een deel van deze kritiek betreft het feit dat verschillende van de genoemde doelgroepen (actoren) in verschillende rollen tegelijkertijd actief kunnen zijn: die van eigenaar, operator of gebruiker (owner, operator and user) van informatiesystemen- en netwerken.

Veelheid aan organisaties en initiatieven - topzware beleidskerstboom? Wat vooral opvalt is het grote aantal organisaties en initiatieven dat zich sinds de jaren negentig met ICT-veiligheidsbeleid bezig houdt (zie ook figuur 1). Verklaringen daarvan dienen ten eerste gezocht te worden in het dynamische en zich snel ontwikkelende ICT-domein zelf. Waar de impact van nieuwe technologieën, producten en markten zich sterker en nadrukkelijker doet voelen en de kwetsbaarheid van ICT-infrastructuur en ICT-gebruik door zijn 'networked' karakter (Internet, open systemen) eerder toe dan af lijkt te nemen, zal beleid een natuurlijke neiging tot expansie en stapeling hebben.

Deze neiging wordt nog versterkt door het dynamische en nieuwe karakter van het beleidsterrein waar sprake is van een continue ontwikkeling en verschuiving in de mogelijkheden van technologie en daarmee ook voor individuen– ook kwaadwillenden. Waar nieuwe markten en realiteiten zich openbaren – zoals de eerdergenoemde convergentie van markten en technologieën - is 'het beleid' soms nog niet zo ver. Stapeling van beleid is dan ook te zien als na-ijleffecten van reacties van beleid op dergelijke ontwikkelingen.

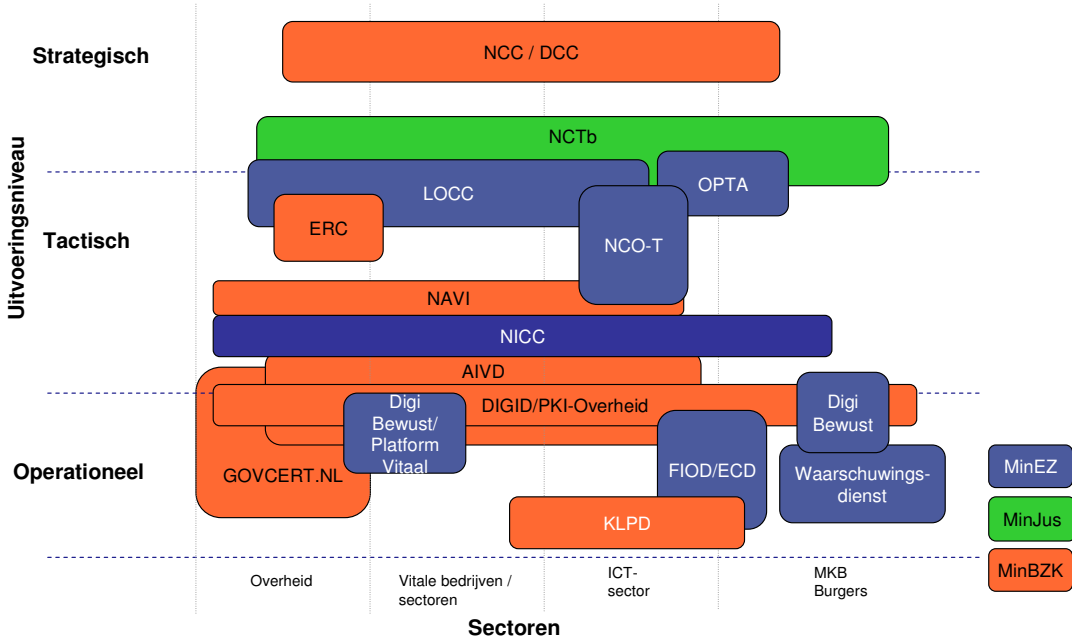
Public governance – populariteit van bottom-up processen en PPS. Niet onbelangrijk in de verklaring van het grote aantal partijen en initiatieven zijn de huidige populaire en dominante visies op overheidssturing (public governance) waarin 'bottom-up' processen, publiek-private samenwerking, het op afstand plaatsen van overheidsdiensten en decentralisatie de boventoon voeren. Dat de problematiek er een is die complex en multidimensionaal is en snel evolueert is daarbij te zien als extra prikkel om deelprobleemgericht en bottom-up naar oplossingen te zoeken. De multi-stakeholderbenadering is overigens niet alleen populair in Nederland maar ook in andere rijke, ontwikkelde landen (OECD, 2005a). Teveel bottom-up en publiek-private samenwerking kan echter leiden tot gebrek aan regie, en gebrek aan overzicht en inzicht in de hand werken.

Efficiëntie en effectiviteit op gespannen voet met veelheid aan organisaties en initiatieven. Het uitgedijde en nog uitdijende ICT-veiligheidsbeleid in Nederland roept het beeld op van een topzware beleidskerstboom, met daarin tal van instrumenten en actieve spelers, zonder dat duidelijk is wie waarvoor precies verantwoordelijkheid draagt, wie uitvoert en waarom. De grote spreiding van partijen en initiatieven staat op gespannen voet met logische samenhang en transparantie, en met een efficiënte en effectieve uitvoering van beleid. Bovendien, waar meerdere partijen en initiatieven zich bezighouden met min of meer dezelfde deelproblematieken zullen coördinatie- en transactiekosten oplopen. Een al te grote spreiding van rollen, taken en verantwoordelijkheden tussen partijen (d.i. platforms, organisaties, projecten) kan de efficiëntie en effectiviteit van beleid negatief beïnvloeden. Daarnaast is het de vraag of de partijen van elkaar nauwgezet en tot in detail weten wie wat te doen staat in tijden van daadwerkelijke crisis. Uit de interviewresultaten en overige beleidsdocumenten kon geen helder inzicht worden verkregen in deze materie. In meer algemene zin kan worden gesteld dat een (te) grote spreiding de handelingssnelheid negatief kan beïnvloeden. Naarmate beleid over meer schijven gaat, neemt bovendien de kans op fouten, d.w.z. het risico van menselijk en ander falen, navenant toe.

Public accountability minder dan optimaal. Bij de wenselijkheid van zelf-regulering en PPS-constructies kunnen in termen van *public accountability* vragen geplaatst worden. Beleidseffectiviteit is daarmee in zekere zin een zaak van goed vertrouwen geworden. Wie stuurt tijdens het traject bij, mocht blijken dat tussentijdse doelen niet of

onvoldoende gehaald worden? En is de overheid zelf nog bij machte voldoende richting te geven aan dergelijke processen? Behalve een groei in quasi-publieke organisaties lijkt ook sprake te zijn van een zekere wildgroei aan organisaties rond ICT-veiligheid, zonder dat soms duidelijk is hoe onderlinge verhoudingen geregeld zijn, hoe verantwoordelijkheden liggen en waar en hoe publieke verantwoording – daar waar nodig - geregeld is.

Overlap tussen initiatieven in rollen, taken en verantwoordelijkheden. Op een aantal gebieden lijkt/is sprake van overlap/dubbelingen in activiteiten (zie hoofdstuk 3 van de quickscan voor een nadere beschrijving; zie TNO, 2006). Overlap geldt bijvoorbeeld voor het NAVI, het NICC en Platform Vitaal in wijze van doelstelling (kennisoverdracht), invulling en aanpak (het Engelse Informatiemodel), sturingsvorm (PPS), doelgroep (vitale bedrijven/sectoren) en het niveau waarop activiteiten worden ontplooid (vooral tactisch, zie figuur 2)[4]. Ook Digibewust en NICC vertonen verrassend veel overlap. In andere gevallen heeft reeds een bundeling door bestaande initiatieven zelf plaatsgevonden, bijvoorbeeld op het gebied van bewustwordings- en voorlichtingscampagnes (zoals Digibewust en Surf op Safe).



Figuur 2. Huidige initiatieven naar uitvoeringsniveau en doelgroep

Dekkendheid van het huidige ICT-veiligheidsbeleid. Op de vraag of het huidige ICT-veiligheidsbeleid een 'witte vlekken'vertoont, werd door de bevraagde huidige initiatieven en organisaties ontkennend geantwoord. Daarmee is echter nog niet met zekerheid geconstateerd of het huidige ICT-veiligheid daarmee dekkend geacht kan

[4] Binnen het ICT veiligheidspallet van activiteiten, kunnen de activiteiten op het gebied van security grofweg onderverdeeld worden naar drie niveau's: operationeel, tactisch en strategisch (zie figuur 2). De strategische activiteiten hebben voornamelijk betrekking op het stellen van beleidskaders en stragische doelen, geredeneerd vanuit de overheid. Op strategisch niveau worden deze beleidskaders en strategische doelen vertaald naar de diverse doelgroepen en wordt (vaak in overleg organen/structuren) met deze doelgroepen een marsroute uitgezet. Uiteindelijk zullen op operationeel niveau de daadwerkelijke security maatregelen geïmplementeerd moeten worden.

worden. Gebrek aan samenhang, een zekere onbalans naar aard en type maatregel en een gesegmenteerde in plaats van integratieve benadering van het huidige ICT-veiligheidsbeleid kunnen ieder voor zich als 'witte vlekken'in het ICT-veiligheidsbeleid aangewezen worden.

Sterke bias in huidige beleidsmix. De balans in aard en type maatregelen is een niet onbelangrijk aspect in de uiteindelijke effectiviteit van beleid. De huidige beleidsmix blijkt nogal scheef verdeeld en vooral maatregelen te bevatten die zich richten op bewustwording, voorlichting en kennisoverdracht.

Overigens zijn bewustwording, voorlichting en kennisoverdracht bepaald nodig. In een analyse van ICT-veiligheid vanuit het perspectief van bedrijven maakt Ki Yoo (2005) een onderscheid naar vier fasen in de volwassenwording van bedrijven inzake ICT-veiligheid: deze loopt via 'blissful ignorance', via 'awareness' naar 'correction' en uiteindelijk 'operations excellence'. Veel bedrijven – in de VS bijvoorbeeld de helft van de bedrijven - blijken nog in de 'awareness' fase te verkeren. Een niet onaanzienlijk deel (30% in 2004) blijkt zelfs nog in een staat van 'blissful ignorance' te verkeren. In dit perspectief zijn acties gericht op bewustwording, voorlichting en kennisoverdracht nuttig en noodzakelijk. Hoewel concrete cijfers over burgers / consumenten ontbreken, lijkt ook hier de nadruk op bewustwording, voorlichting en kennisoverdracht nuttig en nodig. De vraag rijst echter of hiermee voldoende wordt gedaan om de ICT-veiligheid te borgen.

Financiële instrumenten, vraagaggregatie en innovatief procurement onderbelicht. Financiële instrumenten als sturingsinstrument, in de vorm van subsidies of fiscale maatregelen aan burgers of bedrijven, om ICT-veiligheid op een hoger plan te brengen door bijvoorbeeld het gebruik van bepaalde veiligheidssoftware te stimuleren, blijken nauwelijks gebruikt te worden. Slechts in de financiering van publiek-private samenwerking (PPS) wordt dit beleidsinstrument actief maar indirect gebruikt. De meeste PPS richten zich juist weer op informatie- en kennisoverdracht. Er worden ook in wetgevende en handhavende sturende zin activiteiten ontplooid. Deze liggen vooral in de preventieve en corrigerende sfeer (handhavingsbeleid, bestraffing) bij het ministerie van Justitie (door non-response onderbelicht in de quickscan-rapportage). Naast de categorie 'financiële instrumenten' zijn ook vraagaggregatie en 'innovatief' procurement' (waaronder begrepen de rol door de overheid van 'launching customer') sterk onderbelicht (zie verder paragraaf 2.2).

2 ICT-veiligheid – de toekomst

2.1 De ‘rationale’ voor herijking van het ICT-veiligheidsbeleid

Naarmate nieuwe technologieën en producten verder uitkristalliseren en ‘volwassen’ worden, en naarmate er tevens - zoals in het ICT-domein - sprake is van toenemende convergentie van technologieën en markten, kan er een duidelijke aanleiding en *rationale* zijn voor het opnieuw evalueren van bestaand beleid en instituties die zich met beleid bezighouden. Voldoet het beleid en kan het wellicht beter (doelmatiger, sneller, doeltreffender, dekkender)? Een dergelijk proces van evaluatie kan vervolgens leiden tot aanpassing van de beleidsmix en waar nodig ‘opschoning’ van bepaalde beleidsinstrumenten, maar dit is niet vanzelfsprekend. Ingesleten gewoonten en eenmaal gevestigde belangen (bureaupolitiek!) laten zich niet altijd even gemakkelijk herdefiniëren. Bovendien kunnen bepaalde beleidsinstrumenten naar behoren functioneren zodat een meer radicale herformulering en herschikking niet behoeft plaats te vinden. Overlap van activiteiten alleen lijkt voor dat laatste onvoldoende grond. Juist op ICT-veiligheidsgebied hoeft het bestaan van overlap niet per definitie ‘slecht’ te zijn en aanleiding voor correctie. In een op *resilience* (veerkracht en weerbaarheid) gericht beleid kan overlap - een zekere dubbeling - van rollen, taken en verantwoordelijkheden ook functioneel zijn, mits goed op elkaar afgestemd.

De resultaten van de quickscan ondersteunen de gedachte om tot herijking van het ICT-veiligheidsbeleid te komen. Hoe een dergelijke herijking eruit zou moeten zien is een kwestie van politieke besluitvorming. Er is ook niet één maar er zijn meerdere ‘blauwdrukken’ van herijking mogelijk. Een gedetailleerde beschrijving daarvan ligt echter buiten het bestek van deze notitie. Wat deze notitie wel beoogt is het aanreiken van een aantal aandachtspunten en overwegingen in het denken over herijking en oplossingen.

2.2 Naar een robuust ICT-veiligheidsbeleid

In het interdepartementale project *Herijking ICT Veiligheidsbeleid* worden bevordering van samenhang en een sluitende, effectieve en efficiënte aanpak benoemd als kerndoelen voor herijking. De onderliggende premisse daarbij is dat het huidige veiligheidsbeleid beter kan. Samenhang vraagt om een passende institutionele vormgeving van beleid waarin rollen, taken en verantwoordelijkheden van sleutelactoren zo duidelijk en transparant mogelijk gedefinieerd te zijn in onderlinge samenhang en om een adequate beleidsmix (gebalanceerde combinatie en inzet van beleidsinstrumenten). Waar ICT-veiligheid een grensoverschrijdende dimensie heeft – en dit is door het gebruik van het internet en open systemen doorgaans het geval - vraagt dekkend veiligheidsbeleid tevens om afstemming en samenwerking op internationaal, supranationaal (EU) dan wel bilateraal (andere landen) niveau. Geconstateerd wordt dat juist dit internationale aspect zou moeten worden meegenomen in de herijking van ICT-veiligheidsbeleid.

Publiek en privaat belang en de vormgeving van ICT-veiligheid. Met ICT-veiligheid is zowel een publiek als een privaat belang gemoeid. Aan de vervolgvraag hoe dit belang, en vooral het publieke belang, het beste te borgen is, gaat feitelijk nog een

belangrijke vraag vooraf, namelijk wat ICT-veiligheid feitelijk is. ICT-veiligheid kent immers vele aspecten en dimensies (zie paragraaf 1.2). Deze zijn in belangrijke mate bepalend voor de vraag waar private partijen aan zet zijn en waar de overheid. Interconnectiviteit en het '*networked*' karakter van de problematiek maken dat 'de' oplossing niet door één partij – de overheid, ISP, veiligheidssoftwareontwikkelaar of anderszins – kan worden voorzien. Meerdere partijen – overheid, bedrijven en burgers – dienen ieder voor zich maatregelen te treffen. Dit gebeurt reeds. De vraag is of het beter kan en hoe. ICT-veiligheid is een containerbegrip. Slechts in het duidelijk onderscheiden en helder benoemen van onderdelen van veiligheid kan de basis worden gelegd voor een efficiënter en effectiever beleid.

Definieer helder en concreet wat ICT-veiligheid op onderdelen inhoudt en streef een integrale benadering na. Het huidige ICT-veiligheidsbeleid is meer een verzameling, een samenraapsel, van dossiers op deelonderwerpen dan een integraal beleidsdossier, hoezeer de term ook anders doet vermoeden. Dit is gezien het karakter van het containerbegrip ICT-veiligheid niet verbazingwekkend en begrijpelijk gezien de veelkoppigheid van de problematiek. Wel kan worden geconstateerd dat hierdoor een meer integrale benadering van ICT-veiligheidsbeleid op de achtergrond geraakt is. Herijking zou zich op deze meer integrale benadering moeten richten, door heldere koppelingen tussen de deeldossiers te maken. Dit vraagt evenwel ook om het zo concreet mogelijk benoemen van die deelproblemen, met voldoende aandacht voor en een toets op onderlinge samenhang.

De huidige versnippering leidt tot onduidelijkheid over wat ICT-veiligheidsbeleid 'overall' zou moeten zijn, en waar de accenten van overheidsaandacht moeten liggen. De huidige bottom-up en deels budget-gedreven allocatie van middelen in het ICT-veiligheidsdomein leidt ertoe dat vragen rijzen over wie de regie nu eigenlijk heeft en waar een rol voor de overheid is weggelegd en waar niet. Deze rol kan er een zijn van actieve sturing, van financiering maar kan ook liggen in preventief toezicht en handhaving. Het moge duidelijk zijn dat deze integraliteit doorgaans niet op het bord ligt van degenen die geacht worden een van de deelproblemen op te lossen. Op integraliteit staat voor hen immers geen directe premie in welke zin dan ook. Men zou zelfs kunnen stellen dat *bureaupolitieke* incentives en de eigen 'dynamiek' en levenscyclus van organisaties er juist toe kunnen leiden dat de balans in het samenstel van maatregelen (en daarmee ook integratie) teloor gaat of dat reeds is. Organisaties en initiatieven hebben de neiging een eigen leven te gaan leiden, en hun voortbestaan te stellen boven het hogere integrale beleidsdoel – 'overall' ICT-veiligheid.

Vergroot transparantie, streef naar eenvoud in sturingsarrangementen en schuif huidige initiatieven waar mogelijk in elkaar. De huidige initiatieven op ICT-veiligheidsbeleid reflecteren sterk het dynamische karakter van ICT waarin technologische vooruitgang, nieuwe producten en mensen en organisaties die in toenemende mate 'connected' en 'networked' zijn. Het merendeel van de initiatieven richt zich op *deelproblemen* in het ICT-veiligheidsdomein. Daarbij is ook voor de trekkers van initiatieven zelf veelal het algehele overzicht – het grotere geheel - gaandeweg uit zicht geraakt of op z'n minst vertroebeld. Meer is niet per definitie beter. Transparantie kan mede vergroot worden door het bij elkaar voegen en in elkaar schuiven van bestaande initiatieven. De verdeling van rollen, taken en verantwoordelijkheden dient zo eenvoudig mogelijk institutioneel / organisatorisch te worden vormgegeven. Een ministerie van veiligheid – met daaronder ressorterend alles wat met ICT-veiligheid te maken heeft - is daarbij een uiterste variant. Transparantie en

eenvoud ('simplicity') in sturingsarrangementen kan niet alleen de doelmatigheid maar ook de snelheid en doeltreffendheid van ICT-veiligheidsbeleid vergroten.

… met als baten vermindering van transactiekosten- en 'schijven'problematiek. Het kritisch en nauwgezet doorlichten van de huidige initiatieven en organisaties door een externe commissie of evaluator verdient aanbeveling. Dit zou moeten uitmonden in concrete aanbevelingen inzake het bij elkaar voegen en in elkaar schuiven van bestaande initiatieven en organisaties. Een dergelijke stroomlijning werkt transactiekostenverlagend (minder coördinatiekosten – lees afstemmings- en vergaderkosten), maar bevordert, mits in een slim ontwerp gepresenteerd en geïmplementeerd, tevens de trefzekerheid, handelingssnelheid en doeltreffendheid van noodzakelijke acties in geval van ICT-incidenten en calamiteiten. Functionele eenvoud loont.

Vergroot de *public accountability* van ICT-veiligheidsbeleid. De bovengenoemde stroomlijning en opschoning van initiatieven en organisaties kan *ceteris paribus* een positieve impact hebben op de *public accountability* van ICT-veiligheidsbeleid. Zelfregulering en publiek-private samenwerking – hoe wenselijk wellicht ook vanuit het perspectief van het creëren van een 'cultuur van veiligheid' (vgl. OECD, 2002) – heeft doorgaans een negatieve uitwerking op het vlak van *public accountability*. In de herijkingsoperatie verdient het aanbeveling om kritisch te kijken naar nut en noodzaak van de bestaande zelf- en co-reguleringsarrangementen. Duidelijker definiëring van onderdelen van ICT-veiligheidsbeleid (zie eerder deze paragraaf) biedt ook de mogelijkheid een duidelijke keuze te maken in de beschikbare sturingsarrangementen (publiek, publiek-privaat, privaat; ofwel respectievelijk, *hierarchies, networks or markets*). Monitoring en periodieke toetsing (evaluatie) van beleidsactiviteiten dienen ingebracht te worden in het democratische debat (Tweede en Eerste Kamer), tenzij met deze democratische toetsing de ICT-veiligheid zelf gehinderd wordt of in gevaar wordt gebracht.

ICT-veiligheid - mogelijke indelingen op onderdelen. Door het interdepartementale project *Herijking ICT-veiligheidsbeleid* en in navolging van de Europese Commissie (2001) worden drie deeldomeinen gedefinieerd: netwerk- en informatiebeveiliging, computercriminaliteit en privacy. Hoewel beveiliging, criminaliteit en privacy een sterke samenhang kennen, met daarboven - als het ware overkoepelend - het woord 'trust' (vertrouwen), is deze invalshoek analytisch niet de meest gelukkige. Netwerk- en informatiebeveiliging en (het bestrijden van) computercriminaliteit en haar effecten vragen om acties die gericht zijn op ICT-veiligheid – en kunnen – hoewel niet volledig dekkend – gezien worden als twee kanten van eenzelfde medaille. Privacy daarentegen is te zien als een aspect en een afgeleide van ICT-veiligheid. ICT-veiligheid is een noodzakelijke maar niet bepaald een voldoende voorwaarde om privacy te garanderen.

In het zoeken naar een indeling op onderdelen is het zinnig een onderscheid te maken naar acties gericht op het vergroten van de veiligheid van informatiesystemen, netwerken en informatie-overdracht aan de ene kant – gericht op detectie en repressie van ongewenste elementen die deze veiligheid in gevaar kunnen brengen -, en het opsporen en 'onschadelijk maken' van menselijke actoren die hiervoor verantwoordelijk geacht kunnen worden aan de andere kant. In functionele zin vraagt dit onderscheid om een aanpak gericht op het in stand houden en verbeteren van de veiligheid van het systeem als zodanig – door overheid en betrokken actoren – in

technisch-operationele termen, en tevens het effectief opsporen en berechten van kwaadwillenden (criminelen en terroristen).

Schaal, intensiteit en impact van *cyber*incidenten als richtsnoer. Een in operationele zin bruikbaar tweede onderscheid is dat tussen maatschappij-ontwrichtende gebeurtenissen en niet-maatschappij-ontwrichtende gebeurtenissen (zie ook figuur 1). Daarmee wordt een onderscheid bedoeld tussen majeure cyberincidenten met omvangrijke impact, d.i. maatschappelijke schade op financieel-materieel, psychisch-emotioneel dan wel fysiek-humanitair niveau enerzijds, en beperkte, 'alledaagse' en veelal individuele *cyber*incidenten anderzijds. Schaal, intensiteit en impact van *cyber*incidenten geven een eerste duiding voor de mate van actief overheidsingrijpen en overheidsbetrokkenheid, vooraf (ex ante), tijdens, zowel als achteraf (ex post). Tegelijkertijd dient men ervan bewust te zijn dat de term majeur incident (d.w.z. grootschalig, ingrijpend en met grote impact) op verschillende incidenten van toepassing kan zijn, van de 9/11 aanslag op de Twin Towers in New York, langdurige en grootschalige stroomuitval tot een regionale ramp op de schaal van de vuurwerpramp in Enschede. De indeling maatschappij-ontwrichtend en niet-maatschappij ontwrichtend is overigens, zoals uit deze voorbeelden blijkt, niet zwart-wit, maar meer een continuüm. Wel kan in dit continuüm een staffeling of gradatie worden aangebracht die het mogelijk maakt op objectiveerbare gronden tot overheidsactie te komen.

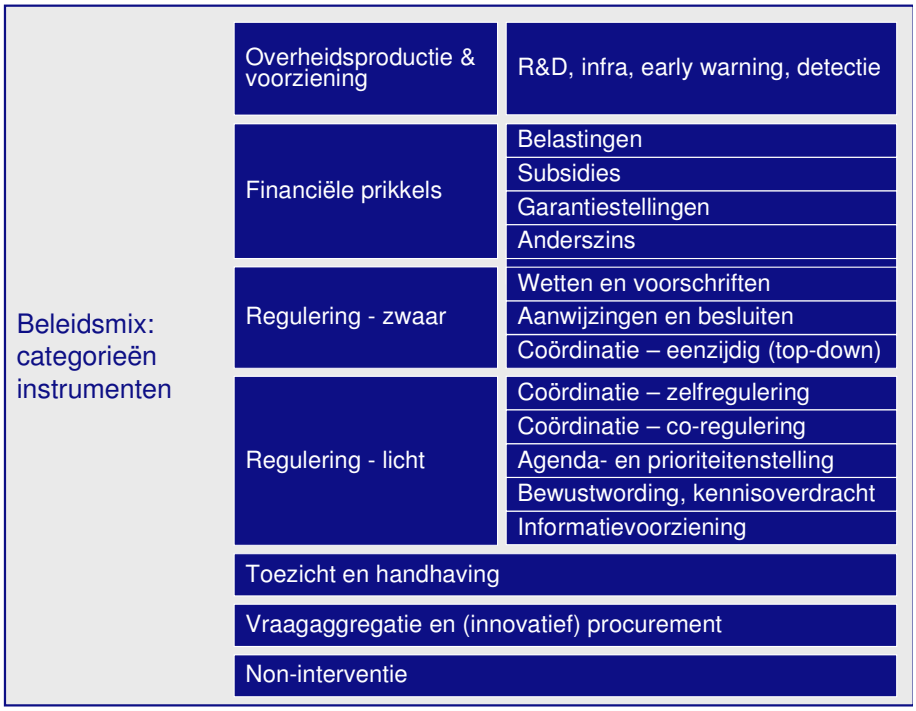
Vergelijkingen met beleid en best practices in bestaande sectoren of domeinen met een langere bestaanshistorie kan zinvol zijn. Zo zal de oplossing van een langdurige en grootschalige stroomuitval in eerste instantie bij het betreffende elektriciteitsbedrijf (publiek dan wel privaat) gezocht worden, of bij een breder collectief van elektriciteitsbedrijven. Voor de overheid ligt hier een rol van informatieverspreiding en mogelijk bemiddeling. Bij rampen en aanslagen ligt deze rolverdeling veelal anders en meer direct op het bord van de overheid. De rol van de overheid bij ICT-incidenten en calamiteiten wordt dan ook grotendeels bepaald door de gebeurtenis of omstandigheid die zich voordoet. De eerdergenoemde intrinsieke netwerkeffecten maken dat de vergelijking van ICT-incidenten met de bovengenoemde andersoortige incidenten overigens maar gedeeltelijk opgaat (vgl. de eerdere externe effectendiscussie). Overigens daar waar aanslagen op en molest van fysieke ICT-infrastructuur (bekabeling, tussenstations, etc.) aan de orde is gaat deze vergelijking overigens wel degelijk op.

In de praktijk zien we overigens al dat beleid zich door dergelijke noties – bijvoorbeeld in de oprichting van organisaties of initiatieven – richt. Wel lopen in opsommingen instrumenten en doelen nogal eens door elkaar heen. Het is zinnig om issues als digitale crisis, digitale verlamming en het begrip vitale sectoren samen te nemen in een beleidscluster, en opvoeding, bewustwording, informatie- en kennisoverdracht en het creëren van een cultuur van veiligheid van burgers en bedrijven in een ander beleidscluster samen te nemen. Criminaliteit en kwaadwillendheid lopen dwars door beide clusters heen. Maar ook daar ligt het voor de hand om onderscheid te maken tussen cyberterrorisme en 'normale', meer alledaagse vormen van cybercrime en fraude.

Typen van beleid en beleidsinstrumenten

De mogelijkheden voor de overheid om zelf en eenzijdig de vormgeving van ICT-veiligheid ter hand te nemen zijn beperkt. Toch kan de overheid bepaalde

beleidsinstrumenten in te zetten om actoren aan te zetten tot gewenst gedrag, meer dan zij tot nu toe heeft gedaan. Figuur 3 geeft een overzicht van instrumenten die door de overheid zijn in te zetten bij beleid. Hoewel betrekkelijk universeel van aard, is de bovenstaande figuur toegespitst op de ICT-veiligheidsproblematiek. Wat feitelijk geconstateerd is in paragraaf 1.2 is dat momenteel een sterke en eenzijdige nadruk ligt op de beleidscategorieën 'regulering - licht' en in mindere mate op 'regulering - zwaar', 'toezicht en handhaving' (inclusief justitie, d.w.z. de opsporings- en vervolgingsketen) en 'overheidsproductie en voorziening'. De categorieën 'financiële instrumenten' en 'vraagaggregatie en 'innovatief' procurement' (waaronder begrepen de rol door de overheid van 'launching customer') zijn sterk onderbelicht.[5]



Figuur 3. De beleidsmix: mogelijke categorieën van beleidsinstrumenten

Ex ante of ex postbeleid? De eerder gememoreerde driedeling in (1) ex ante beleid bestaande uit preventieve en op detectie gerichte maatregelen, (2) proactief en mitigerend beleid in geval van daadwerkelijk optreden van incidenten en calamiteiten (repressie, ofwel directe damage control, restoration and re-activation, en (3) ex post beleid gericht op structureel en volledig herstel, compensatie en slachtofferhulp in de meest brede zin is daarbij een nuttig onderscheid. Overigens kunnen bepaalde beleidsinstrumenten - bijvoorbeeld bewustwording, informatie- en kennisoverdracht - in alle drie typen beleid zinvol worden ingezet.

Richt het beleid meer op resilience en op adequaat anticiperen op complexiteit. Preventieve maatregelen zijn vooral daar effectief als bekend is waar kwetsbaarheden op kunnen treden en wat daarvan mogelijke gevolgen zijn. Door de toenemende complexiteit wordt het echter steeds moeilijker om effectieve preventieve maatregelen

[5] De categorie non-interventie is opgenomen ter completering van de keuzemogelijkheden maar is in de praktijk in het ICT-veiligheidsbeleid aan te duiden als een niet-adequate keuze.

op te zetten. Een alternatief is het inzetten van meer detectieve, repressieve en correctieve maatregelen. Preventief beleid is nuttig, maar niet alles is te voorkomen. Om veiligheid effectief en efficiënt in te richten is een evenwichtiger maatregelen pakket noodzakelijk. Zo zijn met detectieve maatregelen problemen in een vroeg stadium waarneembaar. Vervolgens zijn repressieve maatregelen erop gericht om eventuele schade zo beperkt mogelijk te houden. Tenslotte zijn correctieve maatregelen erop gericht om de geleden schade te herstellen.

Veel activiteiten in het huidige beleid zijn evaluerend van aard. In verschillende overlegorganen wordt nagegaan wat er allemaal mis kan gaan of gaat. Dit soort evaluatietrajecten is een belangrijke bron voor het vaststellen welk type maatregelen het meest effectief en efficiënt zijn.

Van bewustwording en informatie-overdracht naar 'operations excellence'. De fase van awareness waarin kennis- en informatie-overdracht een cruciale rol speelt dient te worden gecompleteerd met maatregelen die gericht zijn op 'correction' en 'operations excellence' (zie Ki Yoo, 2005). Wat geldt voor bedrijven geldt evenzeer voor de overheid, zeker waar het de interne bedrijfsvoering betreft. Vanuit het publieke belang van 'operations excellence' op het hoogste niveau – de maatschappij als geheel – geldt dat de overheid zich meer dan tot nu toe zich zou dienen te richten op actieve detectie, repressie en correctie.

…met uitbreiding 'sensor'-netwerk en middellange termijn detectie als voorbeeld. Wat betreft detectie wordt nu reeds breed ingezet op korte termijn trendanalyse (early warning) door partijen als GOVCERT.NL, AIVD (waar het gaat om hun bemoeienis in vitale bedrijven) en CERT's van andere sectoren (bijvoorbeeld banken). Het NICC heeft momenteel een rol op meer strategisch-coördinerend niveau en richt zich op middellange termijn trendanalyse en opvolging daarvan. Er ligt een uitdaging om tot een sterkere structuur te komen zodanig dat operationele (early warning) informatie gebruikt gaat worden voor het vaststellen en bijstellen van middellange termijn informatie, die gebruikt kan worden als 'sensor'-netwerk voor mogelijke crisissituaties. Nu vervullen noch het NICC, noch andere partijen deze rol; aan invulling bestaat echter dringend behoefte.

Benoem concreter en explicieter gewenste veiligheidsniveaus en doelstellingen. Daarnaast is het van belang dat gewenste veiligheidsniveaus en doelstellingen concreter en explicieter benoemd worden door de betrokkenen. Dit is niet alleen voor trendwatchers van belang maar ook degenen die door (preventieve of andere) maatregelen getroffen (kunnen) worden. Momenteel lopen doelstellingen per deeldomein zodanig uiteen dat tegenstrijdige acties/ maatregelen niet ondenkbaar zijn. Een sterk gesimplificeerd voorbeeld dient als illustratie. Bij een computerinbraak bij een onderneming is het primaire belang voor de ondernemer dat er kan worden doorgewerkt. Vanuit een opsporingsperspectief (politie en justitie) zou men het liefst de bedrijfsvoering willen stilleggen tot bekend is wat de oorzaak is en wie de dader is. Tevens missen de partijen die bezig zijn met early warning (detectie) vaak de aansluiting met partijen die de repressie/herstel uit moeten voeren in geval er waargenomen wordt dat er iets misgaat.

3 Samenvatting aanbevelingen ICT-veiligheid

- Definieer helder en concreet wat ICT-veiligheid op onderdelen inhoudt, benoem zo concreet mogelijk de deelproblemen en streef een integrale benadering na door heldere koppelingen te maken tussen de deeldossiers en een transparante eenduidige uitvoerings- en verantwoordingsstructuur.

- Maak helder(der) wie de regie heeft over onderdelen van het ICT-veiligheidsbeleid en waar de overheid primair aan zet is.

- Streef naar eenvoud in sturingsarrangementen en schuif huidige initiatieven waar mogelijk in elkaar, ofwel consolideer op een intelligente manier de veelheid aan bottom-up en budget-gedreven initiatieven op ICT-veiligheidsgebied. Een intelligent herontwerp kan aldus transactiekostenverlagend (lees minder coördinatie-, afstemmings- en vergaderkosten) werken en de trefzekerheid, handelingssnelheid en doeltreffendheid van noodzakelijke acties in geval van ICT-incidenten bevorderen.

- Maak institutionele arrangementen zoveel mogelijk immuun voor bureaupolitieke incentives en eigen 'dynamiek' van betrokken organisaties en initiatieven opdat budget en inspanning zoveel mogelijk gericht zijn op bedoelde beleidsuitkomsten (meer ICT-veiligheid).

- Vergroot de *public accountability* van ICT-veiligheidsbeleid en kijk ook in dat licht kritisch naar nut en noodzaak van de bestaande zelf- en co-reguleringsarrangementen en PPS-constructies.

- Neem schaal, intensiteit en impact van cyberincidenten als richtsnoer bij de formulering van beleid en overheidsoptreden.

- Heroverweeg de inzet van beleidsinstrumenten en de beleidsmix als zodanig, en heb daarbij oog voor momenteel veronachtzaamde instrumenten waaronder financiële instrumenten, 'vraagaggregatie en 'innovatief' procurement' (inclusief de overheid als 'launching customer').

- Ga uit van een onderscheid in ex ante, proactief en mitigerend en ex postbeleid. Ex ante beleid richt zich op preventieve en op detectie gerichte actie. Proactief en mitigerend beleid richt zich op adequaat optreden bij incidenten en calamiteiten, ook wel aangeduid met de term repressie (directe damage control, restoration and re-activation). Ex post beleid richt zich op structureel en volledig herstel, compensatie en slachtofferhulp.

- Bewerkstellig een fase-overstap in beleid waarbij naast bewustwording en informatie-overdracht ook correctie (detectie en repressie) en 'operations excellence' op zowel individueel als maatschappelijk niveau leidraad worden. Laat ook concreter en explicieter gewenste veiligheidsniveaus en doelstellingen door betrokkenen benoemen, zowel binnen als buiten de overheid (burgers/consumenten, bedrijven en maatschappelijke organisaties) en maak als overheid daarin uiteindelijk de afwegingen daar waar ICT-veiligheid op maatschappelijke niveau aan de orde is.

- Het verdient aanbeveling de huidige initiatieven en organisaties op ICT-veiligheidsgebied integraal, kritisch en nauwgezet te laten doorlichten door een

externe commissie of evaluator waarin met name ook de efficiëntie en effectiviteit (inclusief dekkendheid, handelingssnelheid en adequaatheid) onder de loep dienen te worden genomen. De evaluatie zou moeten uitmonden in concrete aanbevelingen inzake het bij elkaar voegen en in elkaar schuiven van bestaande initiatieven en organisaties, en een onafhankelijk oordeel over te nemen maatregelen en oplossingen om te komen tot een beter ICT-veiligheidsbeleid.

Annex I. Marktfalen en systeemfalen

Het optreden van marktfalen kan een belangrijke 'rationale' zijn voor overheidsoptreden. Marktfalen is daarvoor een noodzakelijke, maar overigens geen voldoende voorwaarde. Uiteindelijk is de vraag of overheidsoptreden gewenst is een politieke beslissing/afweging. Bovendien dient in deze afweging betrokken te worden de overweging dat ook overheidsoptreden (bijvoorbeeld het inzetten van een aanvullend beleidsinstrument) kan falen. Als dit overheidsfalen de aanleiding – het marktfalen – niet oplost maar in zijn effecten juist verder verergert, is de remedie erger dan de kwaal zelf. Overheidsfalen zou men tegenwoordig kunnen benoemen als een van de vormen van systeemfalen. In relatie tot ICT-(on)veiligheid zijn twee vormen van systeemfalen relevant. Het eerste wordt gerangschikt als 'transitiefalen' (transition failures), d.w.z. het niet adequaat in staat zijn van actoren zich aan te passen aan nieuwe technologische ontwikkelingen. Het tweede type wordt wel aangeduid met de term '*hard institutional failure'*. Hieronder wordt verstaan het falen van bestaande instituties waaronder zowel de organisatiestructuur en de samenhang tussen organisaties als het beleid zelf.[6] Theorieën van systeemfalen zijn in de jaren negentig opgekomen en wordt vooral aangehaald in relatie tot innovatiebeleid. De laatste jaren wordt getracht de afzonderlijke theorieën in een logisch en onderling coherente en consistente samenhang te brengen (zie bijvoorbeeld Woolthuis et al., 2005).

De theorie van marktfalen, die voortkomt uit de algemene economische theorie, is reeds in de jaren '60 van de vorige eeuw uitgekristalliseerd en geldt sindsdien als een gezaghebbend toetsingskader voor het al dan niet bestaan dan wel adequaat functioneren van markten. Tevens geeft de theorie van marktfalen een aantal argumenten aan waarom overheidsingrijpen in de economie gelegitimeerd en zinvol kan zijn.

Men spreekt van marktfalen als er sprake is van: publieke goederen en externe effecten; imperfecte mededinging (d.i. verschillende vormen en gradaties in marktmacht); incomplete informatie; onzekerheid. De samenhang tussen ICT-veiligheid en externe effecten is reeds beschreven in paragraaf 2.2. Doordat een individuele actor ICT-veiligheidsmaatregelen – bijvoorbeeld het installeren van een antivirusprogramma – neemt, plukken anderen daarvan de vruchten, zonder dat iemand van deze verbetering kan worden uitgesloten. Bepaalde aspecten van ICT-veiligheid laten zich ook typeren met wat economen non-rivaliteit in consumptie noemen. Dit houdt in dat consumptie van een goed door de een niet ten koste gaat van de consumptie van de ander (men denke aan de consumptie van het publieke 'goed' dijk). Non-rivaliteit is aan de orde als we het hebben over de *beschikbaarheid* van telecommunicatie- en ICT-netwerken, en daarmee de *continuïteit* van beschikbaarheid van informatie- en communicatiestromen. Dit onderdeel van ICT-veiligheid heeft daarmee karakteristieken van een *public good* (collectief of publiek goed). Aan een ander belangrijk criterium – de mogelijkheid van uitsluitbaarheid (ook wel aangeduid met de term exclusiviteit) van gebruik(ers) is echter wel voldaan. ICT-veiligheid in termen van (continue) beschikbaarheid van gebruik is daarmee te typeren als een quasi-collectief goed. In relatie tot veiligheid wordt wel

[6] Een onderdeel van deze 'hard institutional failure' is overheidsfalen (government failure), die als apart paradigma een uitgebreide literatuur achter zich weet (vgl public choicetheorie en de new political economy).

gerefereerd aan het begrip ‘weakest link public good’ (Hirshleifer, 1983): de bescherming van een dijk is zo goed als zijn zwakste schakel (dijkdeel); men vergelijke de analogie met ICT-veiligheid en individuele beschermingsinspanningen.

Onzekerheid en incomplete informatie (informatie-asymmetrie) bij actoren – burgers, bedrijven dan wel de overheid - kunnen beide leiden tot onderinvesteringen in ICT-veiligheidsmaatregelen. Eén van de rollen die de overheid hier kan spelen is die van ‘opvoeder’, door het creëren van bewustzijn (awareness) over mogelijke gevolgen en het geven van informatie.

Referenties

Brück, T. (2004) *Assessing the economic trade-offs of the Security Economy*. In: OECD (2004)

Eurostat (2005) Community Survey on ICT Usage in Enterprises. February 2005

Hirshleifer, J. (2003) From Weakest-Link to Best-Shot: The Voluntary Provision of Public Goods. *Public Choice* 41: 371-386

Ki Yoo, J. (2005) *Industry Perspective: What are the risks to be faced by organisations.* APEC-OECD Workshop on Security of Information Systems and Networks, 5-6 September 2005

Klein Woolthuis, R., M. Lankhuizen en V. Gilsing (2005) A system failure framework for innovation policy design. *Technovation* 25: 609-619

OECD (2002) OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

OECD (2003) Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

OECD (2004) The Security Economy

OECD (2005) OECD STI Scoreboard 2005

OECD (2005a) The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries

Tanaka, N. (2005) Trust & Security as Key Challenges to Promoting ICT and Economic Growth. Presentation by Tanaka, Director for Science, Technology and Industry OECD at the APEC-OECD Workshop on Security of Information Systems and Networks, 5-6 September 2005

TNO (2006) ICT-Veiligheidsbeleid in Nederland – een Quickscan.