Project Herijking ICT Veiligheidsbeleid

Eindrapportage

December 2006

Interdepartementaal project van de ministeries van Economische Zaken,
Binnenlandse Zaken en Koninkrijksrelaties en Justitie

Inhoudsopgave

0 Samenvatting

Dit rapport beschrijft de resultaten van het door EZ, BZK en JUS uitgevoerde project 'Herijking ICT Veiligheidsbeleid'. De aanleiding voor het project was het grote aantal lopende ICT-veiligheidsactiviteiten van de overheid.

Het rapport heeft drie doelen:
- een overzicht te geven van de overheidsactiviteiten op ICT veiligheidsgebied;
- analyse van de samenhang van die activiteiten, meer in het bijzonder of de huidige aanpak sluitend, effectief en efficiënt is;
- een voorstel voor een agenda te doen waarmee de samenhang tussen deze activiteiten kan worden bevorderd.

De **analyse**, uitgevoerd door TUDelft en TNO, leidt tot de volgende conclusies.
Aanpak sluitend? Wel in de zin dat alle bekende risico's worden geadresseerd in een van de vele initiatieven. Niet qua gekozen beleidsinstrumenten. Er is een eenzijdigheid in het instrumentarium dat de overheid kiest. Veel is gericht op bewustwording en het via platforms opdoen en uitwisselen van informatie. In deze publiek-private samenwerkingsverbanden opereert de overheid meestal op basis van gelijkwaardigheid. Financiële en wetgevende instrumenten worden beduidend minder vaak ingezet. Verder ontbreekt een samenhangend beleidskader dat sturing kan geven aan de diverse activiteiten.
Aanpak effectief? De eenzijdigheid van het instrumentarium heeft zijn weerslag op de effectiviteit van het beleid. Het opzetten van platforms om de kennisbasis te versterken èn private partijen tot handelen te bewegen staat centaal in veel initiatieven. Dit is een rationele strategie: ICT is dynamisch en complex en daardoor moeilijk te vatten. Tegelijkertijd is doelbereiking kwetsbaar in die gevallen waar overheid en marktpartijen een afwijkende perceptie en divergerende belangen hebben t.a.v. de aanpak van risico's. De dominante inzet van instrumenten gebaseerd op informatieverstrekking en overtuiging is in zo'n situatie weinig effectief.
Aanpak efficiënt? Het valt op dat ondanks de beperkte personele middelen er veel activiteiten zijn. Tegelijkertijd raakt door verwarrende overlap tussen activiteiten schaarse deskundigheid (ambtelijke expertise en private partijen) versnipperd. Hier bestaat een reëel risico dat deze, voor het resultaat essentiële, deskundigen afhaken.

De implicaties van deze analyse zijn omgevormd tot een **agenda** waar EZ, BZK en JUS de komende tijd aan moeten werken. De agenda is opgebouwd rondom drie thema's: governance, professionalisering en internationaal. Punten die onder deze thema's naar voren komen zijn onder andere:
- de noodzaak voor een samenhangend en richtinggevend beleidskader. Dat kader moet tevens handvatten bieden voor diversificatie van het te gebruiken instrumentarium opdat het gewenste effect wordt bereikt;
- de versnippering van schaarse deskundigen en het risico van afhaken van partijen noopt tot ordening en afstemming van activiteiten.

Een aantal punten van de agenda kunnen direct worden toebedeeld aan of een departement of worden ondergebracht bij een bestaand project. Een aantal andere punten zullen in interdepartementaal verband verder moeten worden ontwikkeld.

1 Inleiding

Er zijn verschillende redenen te onderkennen waarom ICT veiligheid op de agenda van de overheid staat.

Allereerst is een goede benutting van ICT van belang voor een gezonde economische groei en voor het welslagen van de elektronische dienstverlening van de overheid. Voldoende vertrouwen in de veiligheid van ICT wordt gezien als een belangrijke randvoorwaarde om tot een goede benutting van ICT te komen.

Ten tweede is onze samenleving inmiddels zó afhankelijk geworden van ICT, dat een grootschalige verstoring van ICT zou kunnen leiden tot maatschappelijke ontwrichting ('digitale verlamming'). Het betalingsverkeer, het keren en beheren van water en energie zijn enkele voorbeelden van sectoren die sterk afhankelijk zijn van het goed functioneren van ICT.

Tegelijk zien we dat onze ICT-huishouding in toenemende mate wordt bedreigd door vormen van cybercriminaliteit. Of, zoals in de Europese beleidsnotitie inzake een veilige informatiemaatschappij wordt gesteld[1]: "while traditionally attacks have been predominantly motivated by curiosity and a desire to show off technical virtuosity, many current threats are motivated by profit and often attempt to perpetrate criminal acts, such as identity theft, extortion and fraud."

De ministeries van BZK, EZ en JUS hebben begin 2006 besloten om alle op ICT veiligheid gerichte de activiteiten van de overheid te 'herijken' via het project 'Herijking ICT Veiligheidsbeleid'. De aanleiding voor het project zijn de vele, 'als paddenstoelen uit de grond gekomen' overheidsinitiatieven ten aanzien van ICT-veiligheid. Dit is op zich verklaarbaar omdat ICT zich de afgelopen jaren heeft ontwikkeld tot een cruciaal onderdeel van onze maatschappij. De toename aan activiteiten werd nog eens versterkt door de groeiende aandacht binnen de overheid voor veiligheid in het algemeen. Op basis van de ervaringen die dit heeft opgeleverd is het nu een natuurlijk moment voor beleidsmatige reflectie op al die initiatieven en te bezien hoe de toekomstige ICT-veiligheidsagenda van de overheid er uit moet komen te zien.

Het voorliggende rapport beschrijft de resultaten van het interdepartementale project 'Herijking ICT Veiligheidsbeleid'.

Het rapport heeft drie **doelen**:

- Een overzicht te geven van de huidige nationale overheidsactiviteiten[2] op ICT veiligheidsgebied. Het betreft de activiteiten van de ministeries van BZK, EZ en JUS, en daaronder ressorterende organisaties.
- Uitspraken te doen over de samenhang van het geheel aan activiteiten, meer in het bijzonder of de huidige aanpak van de overheid sluitend, effectief en efficiënt is.
- Een voorstel voor een agenda te doen waarmee de samenhang tussen deze activiteiten kan worden bevorderd.

[1] EU (2006b)
[2] Hieronder worden zowel structurele activiteiten als projecten verstaan

De analyse richt zich primair op de *nationale* overheidsactiviteiten. Voor een aantal aspecten, zoals spam, kan een oplossing alleen gevonden worden in een internationale context. Hoewel de internationale samenwerking buiten de scope van dit project valt, wordt waar relevant deze internationale context wel aangestipt.

Aanpak
Om de overheidsinitiatieven te beschrijven is gebruik gemaakt van Kamerstukken, projectplannen en -rapportages, fact sheets en door dossierhouders[3] ingevulde vragenlijsten.
De analyse van de overheidsprojecten is uitgevoerd door TUDelft (faculteit Techniek, Bestuur en Management) en TNO Informatie en Communicatie Technologie. De analyse is uitgevoerd op sluitendheid, effectiviteit en efficiëntie en is gedaan op basis van hiervoor genoemde stukken.
Om de bevindingen te toetsen is 31 augustus 2006 een workshop gehouden met dossierhouders van binnen de overheid. Daarnaast zijn klankbordbijeenkomsten gehouden met onafhankelijke experts en met stakeholders uit de markt.

Opzet van de rapportage
Het rapport is als volgt opgezet. Allereerst komt in hoofdstuk 2 de reikwijdte van het rapport aan de orde. Aangegeven wordt wat onder ICT-veiligheid wordt verstaan en welk overheidsbeleid binnen de scope van analyse valt. Vervolgens schetst hoofdstuk 3 enkele voor het beleid relevante omgevingskenmerken[4] (in §6.3 wordt beschreven wat deze kenmerken betekenen voor het ICT veiligheidsbeleid).
Na deze inleidende hoofdstukken geeft hoofdstuk 4 een overzicht van de huidige overheidsactiviteiten op ICT-veiligheidsgebied. Hieronder vallen zowel structurele activiteiten als projecten van de ministeries van BZK, EZ en JUS, als de onder die ministeries ressorterende uitvoerings- en toezichtinstanties.
Hoofdstuk 5 bevat een analyse van deze activiteiten. De analyse doet uitspraken over de samenhang van het geheel aan activiteiten, meer in het bijzonder of de huidige aanpak van de overheid sluitend, effectief en efficiënt is. De analyse doet geen uitspraken over individuele activiteiten.
Tenslotte staat hoofdstuk 6 stil bij de implicaties van de analyse voor het overheidsbeleid en worden in hoofdstuk 7 deze implicaties omgevormd tot een agenda waar de overheid de komende jaren aan zou moeten werken.

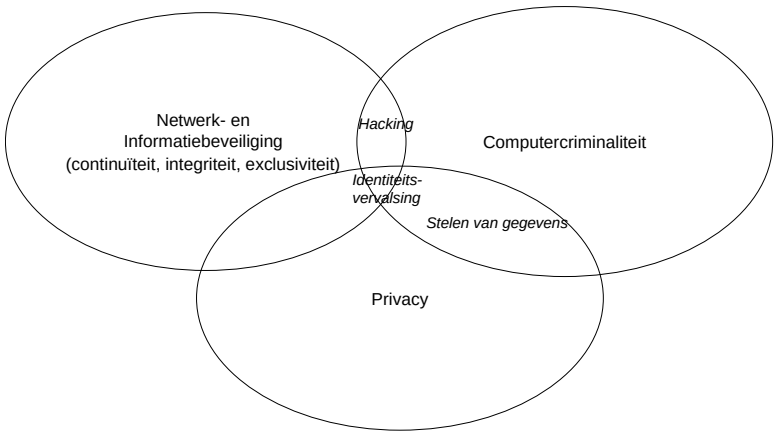
Tot slot van deze inleiding nog een opmerking. Omdat het onderwerp van dit document ICT-veiligheid betreft, heeft het in zich dat er een beeld ontstaat dat het gebruik van ICT alleen maar tot meer risico's leidt. Dit is echter geenszins de bedoeling. Toepassing van ICT leidt tot vele goede maatschappelijke oplossingen en mogelijkheden. De vraag die in dit rapport voorligt, is echter of de aandacht voor veiligheidszorg voldoende aansluit bij de ook aanwezige kwetsbaarheden die ICT met zich meebrengt.

[3] Beleidsmedewerkers van BZK (dgMOS en dgV), JUS (dg Directoraat-Generaal Rechtspleging & Rechtshandhaving), EZ (dg Energie en Telecom), daaronder vallende uitvoeringsorganisaties en de AIVD
[4] Hierbij zijn de relevante ontwikkelingen meegenomen zoals beschreven in de nota Toekomst van Elektronische Communicatie (EZ, 2005).

2 Reikwijdte

2.1 *Het begrip ICT veiligheid*

ICT veiligheid is onder te verdelen in drie samenhangende, elkaar deels overlappende, deeldomeinen (zie onderstaande figuur[5]).



Figuur 1 Deeldomeinen ICT-veiligheid

Netwerk- en informatiebeveiliging
Netwerk- en informatiebeveiliging omvat de maatregelen die genomen kunnen worden om een netwerk of informatiesysteem te beschermen tegen toevallige gebeurtenissen of opzettelijke handelingen die de beschikbaarheid, integriteit en exclusiviteit van opgeslagen of overgedragen gegevens en de diensten die door of via het netwerk worden aangeboden, in gevaar brengen.

- *exclusiviteit* betreft het beschermen van gevoelige informatie tegen onbevoegde kennisname;
- *integriteit* betreft het waarborgen van de correctheid (inclusief authenticiteit) en de volledigheid van informatie en systemen;
- *beschikbaarheid* betreft het zekerstellen dat informatie en essentiële diensten op de juiste momenten beschikbaar zijn voor gebruikers

Privacy
Privacy betreft de bescherming van persoonsgegevens en de persoonlijke levenssfeer. Bij de bescherming van persoonsgegevens kunnen een aantal aspecten worden onderscheiden:

- de vertrouwelijkheid van opgeslagen persoonsgegevens
- de vertrouwelijkheid van gecommuniceerde persoonsgegevens
- het verstrekken en gebruik van persoonsgegevens.

De eerste twee aspecten zijn in feite vormen van exclusiviteit; een goede netwerk- en informatiebeveiliging dienen er toe om dit te borgen.
Als onzorgvuldig wordt omgegaan met persoonsgegevens, kan dit leiden tot een ongevraagde inbreuk op de persoonlijke levenssfeer. Maar het kan ook zo zijn dat er een inbreuk wordt gemaakt op de persoonlijke levenssfeer zonder dat ooit

[5] EU (2001)

persoonsgegevens zijn verstrekt. Dit kan bijvoorbeeld optreden bij spam, als e-mailadressen op basis van proberen worden misbruikt.

Onder de reikwijdte van het project vallen alleen die privacy issues die leiden tot een afnemend vertrouwen in het gebruik van ICT. Spam is hier een voorbeeld van. Daarentegen vallen zaken als bijvoorbeeld misbruik van persoonsgegevens om geadresseerd reclamewerk per post te sturen buiten de scope van het project.

Computercriminaliteit
Voor het begrip computercriminaliteit wordt de definitie van het KLPD gehanteerd[6]: cybercrime omvat elke strafbare en strafwaardige gedraging, voor de uitvoering waarvan het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is. Onder strafwaardig moet tevens worden verstaan “gedrag waarvan verwacht wordt dat het binnen afzienbare tijd strafbaar wordt gesteld”.

Cybercrime valt verder onder te verdelen in twee verschijningsvormen.
- de traditionele criminaliteit in een nieuw jasje: hierbij wordt de computer als middel gebruikt, zoals het verspreiden van kinderporno;
- cybercrime in enge zin: bij deze verschijningsvorm is de computer naast middel ook doel van het strafbare of strafwaardige gedrag, zoals inbreuk op de integriteit van gegevensbeheer of beschadiging van het netwerk.

Dit project richt zich op cybercrime in enge zin.
N.B. *Aftappen* en *bewaren verkeersgegevens* vormen geen onderdeel van dit project.

2.2 *Het betreft het generieke ICT veiligheidsbeleid*

Het project richt zich op het overheidsbeleid t.a.v. het creëren van generieke en gemeenschappelijke randvoorwaarden (zoals standaarden waarmee kan worden aangetoond dat aan een bepaald veiligheidsniveau wordt voldaan, delen van dreigingsinformatie etc.) waardoor sectoren en individuele publieke en private organisaties in staat zijn hun eigen ICT veiligheid te kunnen borgen. Tevens richt het project zich op typische overheidstaken gericht op opsporing en vervolging.

De rapportage gaat niet in op veiligheidsissues die spelen binnen een specifieke sector of organisatie (zoals de vraag of de ziekenhuizen hun beveiliging wel op orde hebben). Daarvoor zijn de sectoren zelf immers primair verantwoordelijk.

[6] Mooij, J. en J. van der Werf (2002)

3 Verkenning van de beleidsomgeving

In dit hoofdstuk worden omgevingskenmerken beschreven die van belang zijn voor de agenda van de overheid. Achtereenvolgens komen aan bod:

- toenemende afhankelijkheid van ICT;
- geldelijk gewin steeds meer een drijfveer voor cybercriminelen;
- gefragmenteerde omgeving;
- complexe en dynamische technologische omgeving.

3.1 *Toenemende afhankelijkheid van ICT*

Voor het besturen en beheren van maatschappelijke kernvoorzieningen maken zowel publieke als private partijen steeds meer gebruik van ICT. Hier zijn goede redenen voor, zoals betere dienstverlening en productiviteitsgroei. De tijd dat Internet een aparte wereld was naast de fysieke wereld is voorbij. Het economisch en maatschappelijk verkeer betreft steeds meer 'immateriële' kennis en informatie.
Naast de vele positieve kanten van benutting van ICT, betekent dit tegelijkertijd dat eventuele kwetsbaarheden van ICT steeds grotere gevolgen krijgen voor het functioneren van de samenleving en het dagelijks leven. Het betreft de toegankelijkheid en manipuleerbaarheid van deze kennis en informatie. Hierdoor neemt behoefte aan beleid en bestuur (governance) t.a.v. ICT veiligheid toe.

Ten gevolge van de toenemende afhankelijkheid van ICT zijn er grofweg 2 soorten risico's te onderkennen:

- *risico's waar we als ICT gebruikers dagelijks mee geconfronteerd worden, maar die een beperkte schade hebben (zoals bepaalde virussen).*
  Dit zijn risico's die we goed kennen doordat we er vaak mee worden geconfronteerd. Hierbij kan een nader onderscheid worden gemaakt in directe en indirecte risico's. Directe risico's betreffen diefstal van gevoelige gegevens of productiviteitsverlies als gevolg van ICT problemen en de kosten die zijn gemoeid met het herstellen daarvan. Indirecte risico's zijn risico's die te maken hebben met reputatieschade en afnemend vertrouwen van gebruikers, resulterend in verlies van klanten en minder benutting van ICT.
- *maatschappij ontwrichtende risico's met een slecht kenbare kans maar met mogelijk ernstige schade.*
  Dit type risico heeft te maken met de afhankelijkheid van maatschappelijke kernvoorzieningen van ICT[7]. Uitval van ICT leidt in dit soort situaties tot uitval van andere maatschappelijk vitale functies, bijvoorbeeld het elektronische betalingsverkeer. Over de waarschijnlijkheid van dit soort vergaande ontwrichtingen zijn deskundigen het vaak niet eens. Redenen voor de ongekendheid van dit soort risico's zijn dat weinig historische data voorhanden zijn en huidige risicoanalyse methoden eigenlijk niet geschikt zijn voor analyses op macro (maatschappelijk) niveau (te complexe materie). Ondanks het feit dat er sprake is van een grote maatschappelijke afhankelijkheid van het goed functioneren van ICT, zijn er in Nederland nog geen ICT gerelateerde incidenten geweest die hebben geleid tot grootschalige maatschappelijke

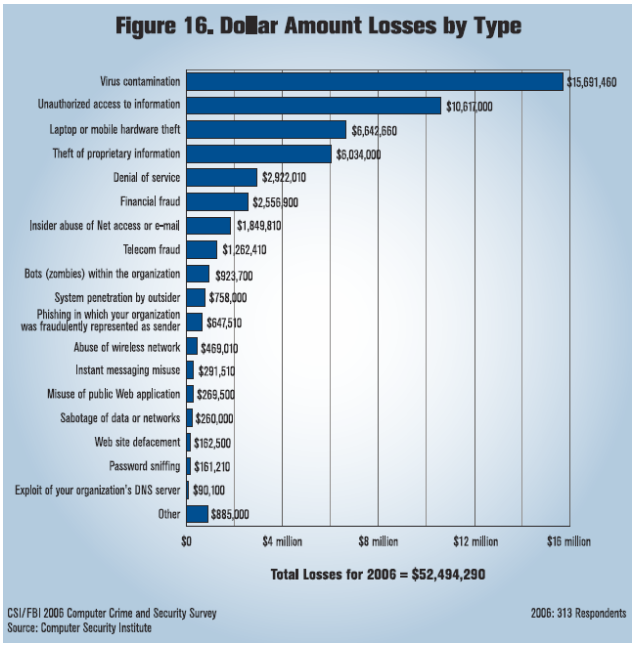
[7] BZK (2003)

ontwrichting. Op basis van wetenschappelijk onderzoek[8] lijkt het echter reëel te veronderstellen dat een risico met ernstige schade ooit zal optreden: een combinatie van kleine factoren, welke combinatie vooraf niet werd vermoed, kan bij complexe systemen met veel koppelingen tussen verschillende deelsystemen tot grootschalige uitval van vitale functies leiden.

3.1.1 Intermezzo: schade; is het nu zo erg?

Het kwantificeren van risico's is lastig vanwege het simpele feit dat er weinig data voorhanden zijn. Veel van wat we weten is gebaseerd op onderzoek van individuele incidenten dat nauwelijks is te generaliseren. Daarnaast zijn er met name voor maatschappijontwrichtende risico's lastig te verifiëren anekdotes. Maar los van het feit dat we het probleem moeilijk kunnen kwantificeren kan wel worden vastgesteld dat er regelmatig wordt ingebroken bij organisaties en dat criminaliteit toeneemt op het internet. Beleidsmatig moet het dus serieus worden genomen.

Het weinig beschikbare onderzoek waarin wel geprobeerd wordt de risico's te kwantificeren heeft veelal betrekking op risico's waar we dagelijks mee geconfronteerd worden, en dan met name de directe schade die daarvan het gevolg is. Het Amerikaanse Computer Security Institute (CSI)[9] doet in samenwerking met de FBI al jaren onderzoek onder Amerikaanse bedrijven en overheden naar de schade door 'cybersecurity breaches'. CSI berekent voor 2005 voor de 313 respondenten een totale schadepost van 52 miljoen dollar[10] (figuur 2). Het CSI/FBI onderzoek is gebaseerd op vrijwillige responses en bevat alleen incidenten waarvan bedrijven weten en die ze bekend willen stellen.



Figuur 2 Schade in de VS als gevolg van 'Cybersecurity breaches'

[8] Perrow (1984) en TUDelft (2004)
[9] www.gocsi.com
[10] CSI/FBI (2006)

Ook in het Verenigd Koninkrijk wordt al sinds 1991 regelmatig een 'information security breaches survey' uitgevoerd, gesponsord door de Britse overheid. Waar de Britse onderzoekers op wijzen is dat het bedrijfsleven over het algemeen terughoudend is met het bekend maken van veiligheidsincidenten daar dat reputatieschade kan opleveren. De negatieve effecten met betrekking tot reputatieschade (indirecte schade) kunnen daarbij veel aanzienlijker zijn dan de directe schade van het veiligheidsincident.

Naast de constatering dat er weinig kwantitatieve data voorhanden zijn, is de vraag echter wat voor conclusies je kan trekken uit de wel beschikbare data. Vaak zie je dat het tot de conclusie leidt dat partijen onderinvesteren in beveiliging. De logische beleidsactie die overheden daar vervolgens aan koppelen is het starten van bewustwordingscampagnes.
In een persbericht over de Europese beleidsnotitie inzake een veilige informatie-maatschappij[11] staat: "Businesses, individuals and public administrations in Europe still underestimate the risks of insufficiently protecting networks and information. Security presently represents only around 5-13% of IT expenditure, which is alarmingly low. The Commission is therefore promoting greater awareness, in a policy document adopted today"

De vraag is echter of de door de overheid getrokken conclusie van onderinvesteren wel altijd klopt, of dat partijen de kosten/baten van extra beveiligingsmaatregelen wel goed afwegen. Niet elk veiligheidsrisico is namelijk per definitie slecht en vergt dus niet altijd een overheidsrol. De creditcard is hier een goed voorbeeld van: blijkbaar zijn de kosten voor banken om dit systeem veiliger te maken hoger dan de kosten die zij moeten maken om klanten te compenseren voor geleden schade t.g.v. fraude. Hoewel dit systeem dus niet veilig is, maken de banken op bedrijfseconomische gronden de afweging om niet te investeren in een veiliger systeem zonder dat de klanten hier de dupe van worden. Er is hier in beginsel dus geen noodzaak voor bemoeienis van de overheid.

Dit intermezzo leidt tot twee conclusies.
Allereerst dat we door het ontbreken van kwantitatieve gegevens vaak geen goed beeld hebben van wat precies het probleem is en hoe groot het is.
Ten tweede dat wanneer wel schadegetallen voorhanden zijn, deze getallen alleen een onvoldoende basis vormen voor de overheid om over te gaan tot actie. Als deze schade namelijk beperkt blijft tot de partij die zelf ook de maatregelen moet treffen, gaat het om een bedrijfseconomische kosten/batenafweging van die partij en is er geen reden voor de overheid om beveiligingsmaatregelen af te dwingen. Mochten echter ook anderen schade ondervinden van de afweging van die partij, en men is niet in staat om deze schade onderling te verhalen, dan kan er wel reden zijn voor de overheid om een partij te dwingen deze 'baten voor anderen' mee te wegen in haar investeringsbeslissing. Paragraaf 6.3 gaat verder in op dit type governance vraagstukken.

3.2 *Geldelijk gewin drijfveer voor cybercriminelen*

Doordat de samenleving steeds meer gebruik gaat maken van ICT, wordt dit ook voor criminelen een steeds interessanter werkterrein. Slecht beveiligde PC's, aangesloten via 'always on' verbindingen, worden als botnets (een verzameling

[11] EU (2006a)

van gekraakte computers) steeds meer ingezet voor georganiseerde aanvallen. Partijen die deze botnets controleren worden door criminele organisaties ingehuurd om criminele activiteiten te faciliteren, zoals afpersing en diefstal. Van 'hacking for fun' naar 'hacking for money'.
Veel criminologe factoren zijn af te leiden uit het karakter van Internet als systeem: de *tools* voor crimineel gedrag zijn eenvoudig beschikbaar op Internet, het internationale, deterritoriale karakter en de vergrote mogelijkheid om de identiteit te vervalsen of anoniem te blijven.

In de annex[12] bij de Europese beleidsnotitie inzake een veilige informatie-maatschappij wordt gesteld:
"Network and information security should be understood as one of the crucial elements of the Information Society enabling smooth development and deployment of new systems, applications and on-line services. Its economic significance to the European economy cannot be understated. At the same time, security problems persist, as illustrated daily by reports of new incidents (whether technical failures, accidents or intentional attacks). In addition, an interesting change in the "threat landscape" is currently taking place: while traditionally attacks have been predominantly motivated by curiosity and a desire to show off technical virtuosity, many current threats are motivated by profit and often attempt to perpetrate criminal acts, such as identity theft, extortion and fraud."

3.3 *Gefragmenteerde omgeving*

De gefragmenteerdheid van de beleidsomgeving wordt aan de hand van 3 punten beschreven:

- Veelheid aan partijen
- Causaal verband tussen oorzaak en gevolg van incidenten niet eenduidig
- Internationale dimensie van het veiligheidsvraagstuk

Veelheid aan partijen
Kenmerkend voor het terrein van ICT zijn dat diensten worden geleverd door een keten van samenwerkende partijen, die steeds in samenstelling kan variëren. Deze keten bestaat uit afnemers en aanbieders van diensten op verschillende functionele lagen[13]: toegang, routering, toepassingen, content en gebruik. De partijen kunnen verschillende belangen en afwegingen t.a.v. veiligheid hebben, hetgeen kan leiden tot collectieve actieproblemen en het naar elkaar afschuiven van verantwoordelijkheden. *Wie voelt zich verantwoordelijk en is tevens in staat om risicoreducerende maatregelen te treffen?* Naarmate er meer partijen zijn betrokken en minder duidelijk is wie waarvoor verantwoordelijk kan worden gehouden, zijn de stimulansen om iets aan veiligheidszorg te doen minder aanwezig.

Causaal verband tussen oorzaak en gevolg niet eenduidig
In veel sectoren is een helder causaal verband te leggen tussen een beslissing van een partij en het gevolg van die beslissing. Een bedrijf kan bijvoorbeeld ertoe besluiten een goedkoop productieproces te hanteren dat het milieu ongewenst belast. Regulering kan in zo'n geval een bedrijf dwingen een schoner productieproces te gebruiken, conform het principe "de vervuiler betaalt". Bij

[12] EU (2006b)
[13] TEC (EZ,2005), blz.12

ICT is dit principe minder makkelijk toepasbaar door de veelheid aan betrokken partijen. Bijvoorbeeld, is het misbruiken van een botnet de schuld van de gebruikers die hun PC beter hadden moeten beveiligen, of is het de schuld van de softwareleveranciers die software met beveiligingslekken leveren? We kunnen de oorzaak ook zoeken bij de ISP's die klanten met ondeugdelijke PC's hadden moeten afsluiten of bij de criminelen die deze botnets misbruiken. Of is het toch zo dat degenen die slachtoffer worden van het misbruik van deze botnets maar beter op moeten letten? Zeg het maar...

Wat wel gesteld kan worden is dat al deze partijen in de keten door de beslissingen die ze nemen een risico kunnen verminderen of verergeren. De vraag die hier voorligt is: *hebben betrokken partijen de juiste incentives om aan veiligheidszorg te doen bij aanschaf, gebruik, beheer of levering van ICT-systemen en/of hebben mensen die deze systemen willen misbruiken voldoende incentives om hiervan af te zien?* Nemen partijen bij het nemen van een beslissing voldoende de eventuele externe effecten op anderen mee bij hun afweging?

Een illustratie van een situatie waar de incentives om te doen aan veiligheidszorg verkeerd lagen, maar door ontwikkelingen in de tijd vanzelf goed kwamen te liggen, betreft centrale virusscanning door ISP's. Tegenwoordig scannen ISP's uit eigen beweging virussen op hun centrale mailservers, iets wat zij tot enkele jaren terug niet tot hun taak rekenden. In die tijd lagen de baten van het centraal scannen bij de klanten van een ISP en de kosten bij de ISP zelf. Doordat ISP's recent zelf erg veel last kregen van de hoeveelheid mailverkeer die door virussen wordt gegenereerd, en dientengevolge extra servercapaciteit moesten plaatsen, ontstond de prikkel om er wat aan te doen. Kosten en baten van het treffen van een veiligheidsmaatregel kwamen bij dezelfde partij (ISP) te liggen.

Daarnaast is het zeer de vraag of grote bedrijven en overheden bij aanschaf en uitrol van ICT systemen wel altijd de juiste incentives hebben om een goede afweging te (kunnen) maken tussen veiligheids- en andere aspecten. Vaak zijn de kosten van (extra) beveiliging namelijk wel direct zichtbaar, maar de baten niet (doordat het bijvoorbeeld een compleet nieuw systeem betreft waarvan de kwetsbaarheden pas in exploitatie aan het licht komen).

Samenvattend, bij veel ICT beveiligingsrisico's is het lastig om eenduidig vast te stellen welke partij verantwoordelijk is voor het ontstaan van problemen. Omdat verschillende partijen in de keten beslissingen nemen die van invloed zijn op de grootte van een risico, is de vraag relevant hoe de incentives voor elk van die partijen liggen om beveiligingsmaatregelen te treffen. De zojuist gegeven voorbeelden geven aan dat deze incentives verkeerd kunnen liggen omdat de kosten en baten van een beveiligingsmaatregel bij verschillende partijen kunnen liggen (1e voorbeeld) of omdat op grond van onvoldoende (onjuiste?) informatie omtrent risico's besluiten worden genomen (2e voorbeeld). Deze beslissingen beïnvloeden echter wel de uiteindelijke veiligheid van de keten.

Internationale dimensie
Hoewel het project zich primair richt op het nationale overheidsbeleid, draagt het feit dat sommige veiligheidsproblemen alleen effectief in internationale samenwerking kunnen worden opgelost bij aan de gefragmenteerde omgeving.

Internationale samenwerking in bijvoorbeeld harmonisering van wetgeving, data uitwisseling en in opsporing en vervolging blijft noodzaak.

Concluderend betekent een gefragmenteerde omgeving:
- dat de veelheid aan partijen die betrokken is bij het aanbieden en afnemen van ICT diensten het lastig maakt eenduidig te bepalen wie verantwoordelijk is voor het voorkomen en oplossen van problemen;
- dit extra wordt bemoeilijkt doordat bij problemen vaak niet eenduidig het causaal verband tussen oorzaak en gevolg is vast te stellen. Ofwel, het principe 'de vervuiler betaalt' is lastig toepasbaar;
- dat beslissingen van individuele partijen (mede) bepalen in hoeverre zich problemen zullen voordoen;
- dat een beslissing van een individuele partij om al dan niet te investeren in veiligheidszorg afhangt van de incentives die hij daartoe ervaart;
- dat de uitkomst van zo'n beslissing niet altijd de maatschappelijk gewenste uitkomst hoeft te zijn (vanwege verkeerde incentives);
- dat internationale samenwerking vereist is om (bepaalde) problemen effectief aan te kunnen pakken.

3.4 *Een complexe en dynamische omgeving*

Mede door de snelle innovatie die de ICT sector en dienstverlening kenmerkt, wordt het moeilijker om de kwetsbaarheden ervan te kennen en te ondervangen. Of het nu gaat om terroristische aanvallen, niet voorziene interacties tussen delen van het netwerk, onbedoelde effecten van overhaast operationeel gemaakte software of onverwacht gedrag van gebruikers, ze hebben één ding gemeen: het kan leiden tot verrassingen.

De conventionele beheersmodellen voor betrouwbaarheid zijn gebaseerd op het gegeven dat de meeste risico's vooraf kunnen worden ingeschat en in het ontwerp worden verdisconteerd. Voor de laatste paar procent heeft men dan real time bewaking. Die verhouding is aan het schuiven[14]. Steeds meer van de betrouwbaarheid van netwerken wordt gerealiseerd in *real time*. Dat is waar verrassingen zich manifesteren en om een response vragen. In dit soort omstandigheden is een strategie van veerkracht (*resilience*) effectiever dan een van vooraf afdekken (*anticiperen*).

3.5 *Betekenis voor beleid*

Ter afsluiting, de in dit hoofdstuk genoemde omgevingskenmerken zijn een gegeven. De vraag is vervolgens wat dit betekent voor het beleid. Leveren deze kenmerken aangrijpingspunten voor wanneer de overheid wat moet doen? En wat zij dan het beste kan doen? In de analyse (hoofdstuk 5) wordt teruggegrepen op enkele van de hier beschreven kenmerken. In hoofdstuk 6 komt aan bod wat deze kenmerken betekenen voor het ICT veiligheidsbeleid.

[14] Schulman, Van Eeten (2002)

4 Overheidsinitiatieven

Het verleden: cyberspace als aparte wereld
In de jaren ’90 werd Internet algemeen gezien als een aparte wereld, waar slechts de ‘early adopters’ voor hun dagelijks functioneren min of meer afhankelijk van waren. De ontwikkeling van Internet is vooral een product van vrijwillige samenwerking van private partijen. Het was een rijk van absolute vrijheid en zelfregulering. Het overheidsbeleid is vooral faciliterend, en bestaat uit het bieden van ruimte om innovatie te bevorderen. Dit was ook de filosofie in de door EZ en V&W in 2001 uitgebrachte beleidsnota KWINT (Kwetsbaarheid Internet). De enige andere overheidsspeler die op dat moment echt in beeld is voor ICT veiligheid is BZK. De overheid gebruikt immers zelf ook ICT systemen en deze moeten veilig en betrouwbaar zijn.

Het heden: ICT als vitale infrastructuur
Inmiddels is de maatschappij sterker afhankelijk geworden van op Internet technologie gebaseerde ICT. De verwachting is dat dit in de nabije jaren alleen maar zal toenemen. Deze ontwikkelingen hebben er toe geleid dat de overheid actiever is geworden op het gebied van ICT-veiligheid. Dit blijkt ook uit het feit dat meerdere overheidspartijen bezig zijn beleid te formuleren op ICT-veiligheidsgebied.

Maar vanuit welke achtergrond houdt de overheid zich eigenlijk met ICT veiligheid bezig? Dit hangt vaak samen met de departementale invalshoek.

Achtergronden overheidsbemoeienis
Nationale veiligheid
Nationale veiligheid heeft betrekking op de bescherming van de Nederlandse staat en samenleving en de kernwaarden die wij delen. De nationale veiligheid is in het geding als vitale belangen van onze staat en/of samenleving zodanig bedreigd worden dat sprake is van (potentiële) maatschappelijke ontwrichting. De vitale belangen zijn: territoriale veiligheid (het ongestoord functioneren van Nederland als onafhankelijke staat in brede zin, dan wel de territoriale integriteit in enge zin), economische veiligheid (het ongestoord functioneren van Nederland als een effectieve en efficiënte economie), ecologische veiligheid (het beschikken over voldoende zelfherstellend vermogen van de leefomgeving bij aantasting), de fysieke veiligheid (het ongestoord functioneren van de mens in Nederland en zijn omgeving) en de sociale en politieke stabiliteit (het ongestoord voortbestaan van een maatschappelijk klimaat waarin groepen mensen met elkaar kunnen samenleven binnen de democratische rechtsstaat en gedeelde waarden).
Omdat onze samenleving inmiddels zó afhankelijk is geworden van ICT, kan uitval van ICT zulke verstrekkende gevolgen hebben dat bovengenoemde vitale belangen aangetast kunnen worden. BZK (DGV) is belanghebbende in het voorkomen van zo’n scenario en opereert als beleidsmaker (zij stelt een strategie op t.a.v. Nationale Veiligheid die betrekking heeft op het voorkomen van en reageren op maatschappelijke ontwrichting, waaronder dus een grootschalige digitale verlamming) en aanjager van andere partijen die hierin een rol hebben. Verder geeft BZK (nationale) veiligheidsadviezen aan publieke en private sector.

Bescherming persoonlijke levenssfeer
Dit betreft de bescherming van persoonsgegevens en de persoonlijke levenssfeer. Bij de bescherming van de persoonsgegevens kunnen een aantal aspecten worden onderscheiden: de vertrouwelijkheid van opgeslagen en gecommuniceerde persoonsgegevens en het verstrekken en gebruik van persoonsgegevens. Het toenemend gebruik van ICT betekent dat ook steeds meer persoonlijke data in ICT systemen is opgeslagen en via deze systemen wordt verzonden. Verschillende departementen zijn actief in de bescherming van de persoonlijke levenssfeer. BZK v.w.b. de bescherming van persoonsgegevens voor zover opgeslagen binnen en behandeld door de overheid, JUS aangaande wetten die in algemene zin het gebruik van persoonsgegevens regelen en EZ specifiek aangaande het gebruik van persoonsgegevens door communicatie aanbieders.

Duurzame economische groei
Een goede benutting van ICT is belangrijk voor de economische groei. Een voorwaarde voor een goede benutting is dat gebruikers vertrouwen hebben in ICT en dat ze het veilig gebruiken. Vanuit deze achtergrond geeft EZ bijvoorbeeld voorlichting aan eindgebruikers.
Voor een goede benutting is het daarnaast van belang dat de ICT diensten die worden aangeboden een zekere betrouwbaarheid kennen. EZ heeft hiertoe een rol in de ordening van de communicatiemarkt (Telecommunicatiewet). Vanuit deze marktordenende rol beziet EZ met aanbieders van ICT diensten wat zij kunnen doen aan het vergroten van de veiligheid.

Opsporing en vervolging
De overheid heeft hier een monopolie op in de samenleving. Als dit soort zaken aan de orde zijn op ICT (veiligheid) gebied, zoals de opsporing en vervolging van cybercriminelen, dan staat de overheid (JUS) hier dus voor aan de lat.

Goed huisvaderschap eigen systemen (BZK/DIIOS als beleidscoördinator binnen overheid)
De overheid heeft zelf veel ICT systemen in gebruik en levert ook ICT diensten aan de samenleving. Deze systemen en diensten moeten uiteraard veilig en betrouwbaar zijn. In dat kader bestaan bijvoorbeeld de Voorschriften Informatiebeveiliging Rijksoverheid (VIR) en - Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIR-BI) en worden periodieke audits gehouden.

Vanuit deze verschillende achtergronden onderneemt de overheid dus activiteiten op ICT-veiligheidsgebied. Voor een beschrijving van deze activiteiten wordt hier verwezen naar het rapport van **TNO*, ICT-Veiligheidsbeleid in Nederland – een quick scan*, september 2006**.

De volgende initiatieven (bestaande uit zowel structurele activiteiten van staande organisaties als projecten) komen in dat rapport aan bod.

Initiatieven	karakter		departement		PPS-vorm
	beleid	uitvoerend	trekker	overig	
Nationaal Crisiscentrum (NCC) / Departementaal Crisiscentrum (DCC)		uitvoerend	BZK_NCC	alle_DCC	nee
Nationaal Coördinator Terrorismebestrijding (NCTb)	beleid	uitvoerend	Jus/BZK	diverse	nee
Algemene Inlichtingen en Veiligheidsdienst (AIVD)	beleid	uitvoerend	BZK		nee
Agentschap Telecom (AT)		uitvoerend	EZ		nee
Bescherming Vitale Infrastructuur (BVI)	beleid		BZK	diverse	gezamenlijke risicoanalyse
BVI (VISTIC)	beleid		EZ		gezamenlijke risicoanalyse
Strategisch Overleg Vitale Infrastructuur (SOVI)	beleid		BZK	diverse	overlegplatform
Nationaal Continuïteitsoverleg Telecom (NCO-T)	beleid	uitvoerend	EZ		platform voor kennisdeling en gezamenlijk uitvoeren activiteiten
Nationale veiligheid (Digitale verlamming)	beleid		BZK/EZ	Def, Jus	gezamenlijke analyse
GBO.Overheid		uitvoerend	BZK	EZ, FIN, SZW	nee
GOVCERT		uitvoerend	BZK	EZ	informatieuitwisseling en samenwerking bij aanpak incidenten
Waarschuwingsdienst		uitvoerend	EZ	BZK	nee
OPTA		uitvoerend	EZ		nee
Korps Landelijke Politiedienst (KLPD)		uitvoerend	Jus/BZK		nee
High Tech Crime Team		uitvoerend	Jus/BZK		nee
Nationaal Platform Criminaliteitsbeheersing (NPC)	beleid		EZ	BZK, Jus	overlegplatform
NICC		uitvoerend	EZ	BZK, Jus	samenwerking in projecten
NICC – Project Informatieknooppunt		uitvoerend	EZ	BZK, Jus	knooppunt voor informatieuitwisseling
Nationaal Adviescentrum Vitale Infrastructuren (NAVI)	beleid		BZK	diverse	informatieuitwisseling / advisering
Digibewust, Nationaal Platform Continuïteit Vitale ICT (Platform Vitaal)		uitvoerend	EZ		platform voor informatieuitwisseling
Programma Digibewust (door ECP.nl)		uitvoerend	EZ	BZK, Jus, OCW	diverse vormen
Surf op Safe (door ECP.nl)		uitvoerend	EZ		partners lichten eigen doelgroepen voor
Nationaal Authenticatie Platform (NAP door ECP.nl)		uitvoerend	EZ	BZK	platform voor kennisdeling
PKIoverheid, DigiD en eNIK		uitvoerend	BZK	EZ	nee

N.B. De kolom ‘PPS-vorm’ geeft de diverse verschijningsvormen aan van min of meer geïnstitutionaliseerde publiek-private samenwerkingsverbanden

5 Analyse

Dit hoofdstuk bevat de resultaten van een externe analyse uitgevoerd door TUDelft (2006)en TNO (2006a en 2006b).

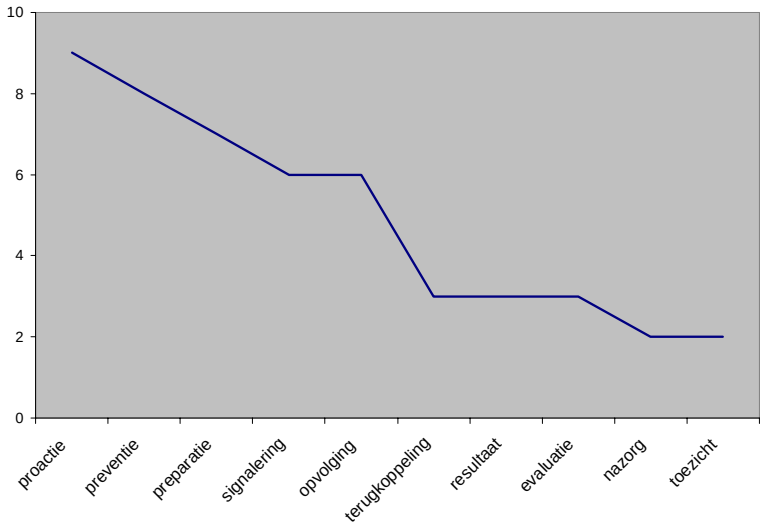
De analyse is gebaseerd op Kamerstukken, projectplannen en -rapportages, fact sheets en ingevulde vragenlijsten. Deze documentatie vormt voldoende basis om enkele dominante bevindingen te schetsen. De hier gepresenteerde resultaten zijn tijdens een terugkoppelsessie gepresenteerd aan betrokken dossierhouders. Tijdens die bijeenkomst bleek instemming met de in dit hoofdstuk gepresenteerde bevindingen.

5.1 *Kenmerken huidige initiatieven*

Eerst worden een aantal kenmerken van de initiatieven benoemd. Nadrukkelijk wordt opgemerkt dat het benoemen van deze kenmerken geen waardeoordeel impliceert. Het gaat primair om het vinden van patronen in de gevarieerde verzameling van lopende initiatieven. Deze patronen helpen vervolgens bij het beantwoorden van de vraag of er sprake is van een “sluitende, effectieve en efficiënte aanpak”.

Er is een groot aantal initiatieven met relatief kleinschalige middelen. Zo geeft het merendeel van de bekeken initiatieven aan minder dan 4 fte in te zetten voor de activiteiten. De uitzonderingen hierop zijn vooral de uitvoerings- en toezichtsorganisaties.

Een tweede kenmerk is dat de bulk van de initiatieven hun bijdragen positioneert aan het begin van de veiligheidsketen (proactie, preventie, preparatie – de linkerkant van de x-as in de onderstaande figuur). Naarmate we verder in het veiligheidsproces komen, dunt het aantal initiatieven snel uit.



Figuur 3: Nadruk op eerste stappen in veiligheidsproces (TUDelft 2006)

Een kenmerk dat in lijn ligt met het voorgaande is de nadruk op activiteiten die zich richten op het stimuleren van bewustwording. Het stimuleren van

bewustwording neemt allerlei vormen aan, zoals voorlichting aan eindgebruikers en het MKB via DigiBewust of het instrueren van overheidsmedewerkers aangaande het zorgvuldig omgaan met vertrouwelijke gegevens.
Verder valt op dat veel van de initiatieven die zich bezig houden met bewustwording aangeven dat er een veiligheidsprobleem is, maar dat het probleem door anderen nog onvoldoende erkend wordt. In dat verband wordt wel gesproken over een 'geringe urgentiebeleving'.

Veel initiatieven kiezen voor publiek-private samenwerkingsconstructies (PPS-constructies). Veel initiatieven noemen dit als een cruciaal onderdeel van het initiatief. Ook dit kent weer verschillende verschijningsvormen (zie hoofdstuk 4). Zo zijn er verschillende platforms rondom veiligheidskwesties, maar ook organisaties, die zich richten op advies aan private partijen (zoals NAVI).

Er is over het algemeen weinig nadruk op specifieke veiligheidsoplossingen. De projecten richten zich vooral op het agenderen van onderwerpen en het verzamelen van kennis. Uitzonderingen zijn de activiteiten die zich richten op de overheid zelf. Denk hierbij aan projecten als PKI-overheid, DigiD en eNIK.

Een volgend kenmerk dat opvalt, betreft de doelen die de initiatieven zich stellen. Vaak zien we twee typen doelen naast elkaar bestaan Het eerste type noemen we ***outputs***: doelen in termen van de op te leveren middelen. Denk hierbij aan het organiseren van een publiek-privaat platform voor kennisuitwisseling of het uitvoeren van een pilotproject. Het tweede type noemen we ***outcomes***: doelen in termen van de uiteindelijk beoogde effecten van die middelen (zoals het borgen van nationale veiligheid). Veel initiatieven formuleren doelstellingen van beide typen. **Het valt op dat er een grote kloof bestaat tussen de outputs en de outcomes – met andere woorden, tussen de gekozen middelen en de beoogde maatschappelijke effecten.** De koppeling tussen outputs en outcomes is lastig, zeker als het om ICT-veiligheid gaat. Zo steken de middelen, zoals het stimuleren van kennisuitwisseling, vaak schraal af bij de omschreven ernst van de gesignaleerde problemen. De middelen hebben daar causaal weinig invloed op ICT-veiligheid. **Tenslotte wordt doelbereiking vaak 'gemeten' en afgerekend in termen van outputs en minder in termen van outcomes.**

Een ander kenmerk dat opvalt, is dat de verantwoordelijkheid voor het bereiken van de strategische doelen (outcomes) meestal wordt toegewezen aan andere partijen dan de initiatiefnemer zelf – vaak aan private partijen. Het toewijzen van die verantwoordelijkheid aan anderen is alles behalve vanzelfsprekend. Hoeveel er ook gesproken wordt over de verdeling van rollen en verantwoordelijkheden tussen publieke en private organisaties, echt handelingsgericht wordt het zelden. Dit komt met name doordat het de overheid is die deze verdeling vaststelt en dat de partijen die de verantwoordelijkheid toebedeeld krijgen hier zelf niet of nauwelijks een stem in hebben. Dat leidt tot voorspelbare discrepanties tussen de gepercipieerde rollen en verantwoordelijkheden tussen overheid en private partijen[15].

[15] Zo kan de overheid bijvoorbeeld private partijen oproepen om uitval van ICT systemen t.g.v. een EMP bom (bom die een elektromagnetische puls veroorzaakt) te voorkomen. Zo'n oproep zal weinig gehoor vinden. De investeringen zijn dusdanig dat dit niet past binnen het business model van private partijen.

De overheid agendeert tamelijk eenzijdig het probleem alsmede de ernst er van, terwijl men tegelijkertijd voor wat betreft de probleemoplossing een faciliterende rol kiest en de verantwoordelijkheid elders legt. Die twee zaken staan op gespannen voet met elkaar, zoals nader zal blijken in §5.2.2 “effectieve aanpak?”.

5.2 *Beoordeling*

Na deze inventarisatie van enkele opvallende kenmerken van de huidige overheidsinitiatieven, beoordelen we de initiatieven aan de hand van de drie criteria zoals die door het project zijn geformuleerd. Is er sprake van een:

- Sluitende aanpak?
- Effectieve aanpak?
- Efficiënte aanpak?

5.2.1 **Sluitende aanpak?**

Het gehele scala aan bekende risico’s wordt wel ergens in een activiteit van de overheid geadresseerd. We denken daarbij aan: a) grootschalige risico’s die leiden tot maatschappelijke ontwrichting en b) alledaagse risico’s met beperkte schade.

Op de vraag of er witte vlekken zijn, is het antwoord dat het scala aan bekende risico’s gedekt lijkt. Qua aanpak is het echter een ander verhaal, zoals blijkt uit de volgende figuur (hoe donkerder een cel, hoe meer initiatieven de betreffende aanpak volgen).

		Interventie-instrumenten		
		Financiële sturing	Informatie-verstrekking	Wet- en regelgeving
Coördinatiemechanismen	Markt			
	Netwerk			
	Hiërarchie			

Figuur 4 beoordelingstabel sluitendheid aanpak (TUDelft 2006)

De getoonde tabel inventariseert het gehanteerde instrumentarium vanuit twee dimensies: de drie klassieke institutionele coördinatiemechanismen uit de economie (markt, netwerk en hiërarchie) afgezet tegen de drie klassieke instrumentenfamilies uit de bestuurskunde (economische, communicatieve en regulerende instrumenten). We hanteren hier de benamingen van de WRR voor deze categorieën, zoals benoemd in het rapport ‘Bewijzen van goede dienstverlening’ (WRR, 2004).

De achterliggende vraag bij de *coördinatiemechanismen* is: op welke wijze wordt het gedrag van partijen op elkaar afgestemd en welke positie heeft de overheid hierbij. In een markt zorgt prijsvorming voor coördinatie. De overheid zou zich wat veiligheid betreft dan vooral dienen te richten op marktordening, het internaliseren van marktexternaliteiten en andere maatregelen die het functioneren van markten verbeteren, zoals het vergroten van de transparantie van het aanbod.

In het geval van een netwerk gaat het ruwweg gezegd om coördinatie tussen publieke en private partijen op basis van vrijwilligheid, wederzijds voordeel en vertrouwen. De overheid opereert hierbij op basis van gelijkwaardigheid.
In het geval van hiërarchie, tenslotte, is het de overheid die aanstuurt hoe er met veiligheid omgegaan dient te worden en welk gedrag gewenst is van private partijen.

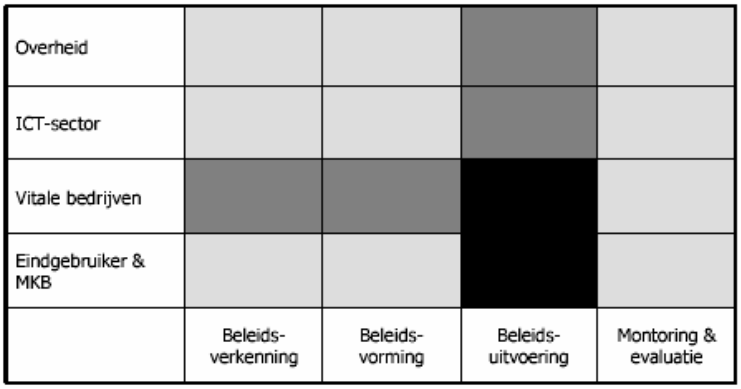
Binnen elk coördinatiemechanisme kan elke instrumentfamilie worden ingezet, zij het met andere doeleinden. *Interventie-instrumenten* zijn dus conceptueel anders dan coördinatiemechanismen. Het is dus niet zo dat financiële prikkels alleen maar toegepast worden binnen het mechanisme van een markt. Zo kan de overheid besluiten bepaalde pilot-projecten (mede) te financieren, waarbij ze hoopt dat het project een vrijwillige verandering in het gedrag van andere partijen teweeg brengt (netwerk-coördinatie). Ook kan een financieel instrument ingezet wordt als de overheid besluit hiërarchisch op te treden. Zo vergoedt de Noorse overheid de kosten van bepaalde investeringen die ze gerealiseerd wil zien in de netwerken van telecommunicatieoperators. Denk ook aan het Noodnet, waar de overheid een bepaalde veiligheidsvoorziening zelf mede financiert.

Om meer gevoel te geven voor de WRR terminologie, nog enkele voorbeelden van hoe enkele huidige veiligheidsinitiatieven passen in figuur 4.
De onder Digibewust uitgevoerde voorlichtingscampagne combineert hiërarchie met informatieverstrekking: zij draagt een bepaalde veiligheidsvisie uit en probeert eindgebruikers tot een gedragsverandering te bewegen.
Op het gebied van markt en informatieverstrekking kunnen we bijvoorbeeld wijzen op het opstellen van de zogenaamde ‘transparameters’ (in project KWINT/Digibewust). Middels deze indicatoren kunnen klanten aan ISP’s vragen transparantie te verschaffen over de betrouwbaarheid van hun dienstverlening.
Op het gebied van regelgeving zijn ook voorbeelden. De spamwetgeving is een voorbeeld van hiërarchie en regelgeving. Rond andere initiatieven zien we ook lichte regulerende elementen. Zo is het NCO-T een typisch voorbeeld van netwerk-coördinatie en informatieverstrekking, maar speelt regulering op de achtergrond een rol omdat de deelname aan het NCO-T voor een bepaalde groep operators verplicht is gesteld (netwerk en wet- en regelgeving). Tevens zitten in NCO-T hiërarchie en wet- en regelgeving opgesloten: in het procesontwerp van het NCO-T is de mogelijkheid opgenomen dat de overheid zelf maatregelen identificeert en oplegt, mochten deze niet op vrijwillige basis tot stand komen.

Gegeven figuur 4, wat zijn onze bevindingen? We hebben de verzameling aan lopende initiatieven gepositioneerd op de tabel van figuur 4. Zonder in lastige en detaillistische discussies te vervallen over de positionering van elk afzonderlijk initiatief, valt toch op dat de verdeling allesbehalve sluitend te noemen is. Zo zien we dat de bulk van de initiatieven gebruik maakt van de instrumentfamilie informatieverstrekking binnen netwerk-achtige coördinatie. Hier zien we de eerder gesignaleerde nadruk terug op PPS-achtige constructies en op bewustwording. Financiële instrumenten en wet- en regelgeving worden beduidend minder vaak ingezet. Ook de mechanismen markt en hiërarchie worden minder vaak gebruikt en ingezet. De meeste initiatieven brengen partijen bij elkaar en hopen op basis van kennisuitwisseling en advisering tot een verbetering van de veiligheid te komen.

Alles overziend, kan gesteld worden dat de aanpak van de overheid twee eenzijdigheden kent: een sterke nadruk op netwerkcoördinatie en op informatieverstrekking. Zo zou de overheid bijvoorbeeld meer kunnen doen aan marktordening en aan wet- en regelgeving. Hierbij valt te denken aan het analyseren van de incentive-structuur die beïnvloedt welke afwegingen marktpartijen maken (zie ook §3.3). Via wet- en regelgeving zou de overheid aansprakelijkheden kunnen definiëren of effectiever anders kunnen arrangeren. Dat heeft direct gevolgen voor de (financiële) incentives van marktpartijen.

We hebben de verzameling initiatieven ook nog doorsneden naar doelgroep en beleidsfase.



Figuur 5 Initiatieven ingedeeld naar doelgroep – beleidsfase (TUDelft 2006)

Als eerste valt op dat veel initiatieven zich bevinden rondom beleidsuitvoering in een relatief beleidsarme context. Bij de uitvoerende en toezichthoudende instanties vinden we de meeste fte's, dus begrijpelijkerwijs ook veel activiteit – in verhouding tot de kleine en gefragmenteerde inzet van fte's bij de beleidsdirecties. Als tweede valt op dat het zwaartepunt ligt bij de doelgroep van vitale bedrijven.

De nadruk op beleidsuitvoering kan mogelijk een verklaring zijn voor de eerder gesignaleerde eenzijdigheid in het instrumentarium – de nadruk op netwerksturing en informatieverstrekking. Deze instrumenten vereisen namelijk geen wettelijke kaders of beleidsmatige wijzigingen, iets dat de uitvoerende en toezichthoudende instanties niet op eigen kracht kunnen introduceren[16]. Zeker is wel dat hun activiteiten weinig sturing kennen vanuit een samenhangend beleidskader.

Samenvattend, een sluitende aanpak? Op de vraag of er witte vlekken zijn, kunnen we stellen dat het scala aan bekende risico's wel ergens door de overheid in een activiteit wordt geadresseerd. Qua aanpak is er wel een eenzijdigheid in ingezet instrumentarium: een sterke nadruk op overtuiging en op informatieverstrekking. Deze eenzijdigheid heeft invloed op de mate waarin beleidsdoelstellingen kunnen worden gehaald. In §5.2.2, dat als onderwerp de effectiviteit van beleid heeft, wordt hier nader op ingegaan.
Verder wordt geconstateerd dat een samenhangend beleidskader ontbreekt dat sturing kan geven aan de diverse activiteiten.

[16] N.B. Dit moet niet geïnterpreteerd worden als dat beleid alle problemen van uitvoering op haar agenda moet (laten) zetten. Zaken die binnen bestaande kaders in de uitvoering geregeld kunnen worden, moeten daar ook worden opgepakt

5.2.2 **Effectieve aanpak?**

Effectiviteit gaat in de eerste plaats over doelbereiking. De vraag is dus, wat zijn de doelen? Op het niveau van de outputs zijn de doelen opvallend overeenkomstig. Veel richten zich op de institutionalisering van ICT-veiligheid. Niet het implementeren van maatregelen staat centraal, maar het opzetten van samenwerkingsverbanden of fora om de kennisbasis te versterken èn private partijen tot handelen te bewegen. Dit is reeds op verschillende plekken in de analyse duidelijk geworden. Zie bijvoorbeeld de nadruk op PPS achtige constructies, de nadruk op bewustwording en kennisuitwisseling en de geringe aandacht voor het implementeren van specifieke beveiligingsmaatregelen.

Deze institutionalisering is een rationele strategie. ICT is immers dynamisch en complex en daardoor moeilijk te vatten. Er wordt daarom allereerst getracht om kennis te vergaren en de problemen te agenderen bij de juiste partijen via het opzetten van fora. De overheid probeert de private partijen via deelname aan deze fora mede verantwoordelijk te maken. Het in publiek-private samenwerking “bottom-up” zoeken naar oplossingen is overigens niet alleen populair in Nederland, maar ook in andere rijke, ontwikkelde landen[17].

Maar de effectiviteit van samenwerkingsvormen die hoofdzakelijk gebaseerd zijn op netwerkcoördinatie en informatieverstrekking is erg kwetsbaar. Het bereiken van de outcomes is vaak primair in de handen van private partijen[18]. Dat is precair in een netwerkcontext, omdat vrijwilligheid betekent dat elke oplossing in beginsel wederzijds voordelig dient te zijn. Dit laatste is niet altijd het geval. Private partijen delen vaak niet de probleemperceptie van de initiatiefnemende overheidspartij. Dat is wellicht nu nog niet zo scherp zichtbaar,
maar het wordt wel duidelijk bij de klachten die veel initiatieven hebben over een ‘gebrekkig urgentiebesef’ bij de private partijen. De reactie daarop is veelal: het probleem is zeer ernstig, jullie zijn medeslachtoffer en daar gaan we wat aan doen. Echter, de partij die de schade draagt, ervaart die urgentie niet omdat men de schade in een ander kader beoordeelt (zie ook §3.1.1).

Neem bijvoorbeeld de 2006 CSI/FBI Computer Crime and Security Survey. Die signaleerde dat bedrijven gemiddeld zo’n 170 duizend dollar schade per jaar hebben door veiligheidsproblemen. Dit klinkt wellicht als een stevige schadepost, maar de maatregelen die nodig zijn om deze problemen te voorkomen zijn al snel kostbaarder dan de schade. Met andere woorden, de Return on Investement is te laag om het bedrijfseconomisch rationeel te maken deze schade sterk terug te dringen.

Dat laat onverlet dat de overheid redenen kan hebben om deze schade toch maatschappelijk onacceptabel te vinden. Maar haar perceptie zal dan afwijken van die van de marktpartijen. In die situatie zijn instrumenten gebaseerd op informatieverstrekking en overtuiging weinig effectief. Daarvoor zijn meer robuuste governance-arrangementen nodig, bijvoorbeeld gebaseerd op marktordening en op wet- en regelgeving.

[17] OECD (2005)
[18] Zij zijn in veel gevallen namelijk leverancier, eigenaar, beheerder of gebruiker van systemen

Samenvattend, effectieve aanpak? Het opzetten van platforms om de kennisbasis te versterken èn private partijen tot handelen te bewegen staat centaal in veel initiatieven. Deze institutionalisering is een rationele strategie: ICT is immers dynamisch en complex en daardoor moeilijk te vatten. Gegeven de logica voor institutionalisering is doelbereiking tegelijkertijd kwetsbaar in die gevallen waar overheid en marktpartijen een afwijkende perceptie en divergerende belangen hebben t.a.v. de aanpak van risico's. De dominante inzet van instrumenten gebaseerd op informatieverstrekking en overtuiging (figuur 4) is in zo'n situatie weinig effectief. Daarvoor zijn meer robuuste governance-arrangementen nodig. Nieuwe spelregels en instrumenten die de samenwerking met private partijen tot gewenste uitkomsten doen leiden en die dus moeten kunnen omgaan met uiteenlopende percepties en belangen.

5.2.3 **Efficiënte aanpak?**

Het derde criterium waarop is geanalyseerd, betreft efficiëntie. Hier valt op dat ondanks de beperkte personele middelen er toch veel activiteiten en initiatieven zijn. In die zin wordt er gewoekerd met de beperkte personele capaciteit van met name ambtelijke ICT veiligheidsdeskundigen en private partijen. Toch is er ook een aantal problemen. Zo is er **veel en verwarrende overlap tussen de initiatieven**. **Daarnaast raken schaarse personele middelen versnipperd doordat er zoveel initiatieven lopen**. De verantwoordelijkheden zoals ze nu binnen de overheid zijn belegd, bieden ook ruimte voor deze overlap.

Eerder werd al duidelijk dat veel verschillende initiatieven zich richten op vitale bedrijven. Daarnaast is er een duidelijke overlap in problematiek. Neem bijvoorbeeld een scenario waarin een aanslag leidt tot grootschalige uitval van telecommunicatievoorzieningen. Dat scenario is relevant voor een reeks aan initiatieven: NAVI, NICC, NCO-T, Digitale Verlamming, NCTB, AIVD en het NCC. De strategische doelen (outcomes) van deze initiatieven zijn vaak wel anders, maar deze zijn te abstract en te ver verwijderd van de middelen (outputs) om richting te geven aan wat in welk forum besproken wordt en met welke consequenties. Daardoor lopen veel initiatieven in elkaar over. In het algemeen geldt dat niemand, zelfs de insiders niet, een 'begrijpelijk verhaal' hebben over de samenhang. Sommige initiatieven claimen een kader te zijn waarbinnen de andere initiatieven een plek krijgen, maar hun claims stemmen onderling niet overeen. Bovendien hebben de andere initiatieven waarschijnlijk een andere opvatting over de onderlinge samenhang.

Enige vorm van overlap is functioneel, zeker bij complexe en dynamische problemen. Partijen brengen informatie in uit verschillende bronnen en vanuit verschillende doelstellingen. Dat leidt tot correctie van foute of eenzijdige beelden en zorgt er voor dat niet snel iets over het hoofd wordt gezien. Echter, te veel overlap heeft als nadeel dat de schaarse deskundigen versnipperd raken. De schaarse deskundigheid bestaat uit de deelname van ambtelijke experts en private partijen. Beide worden vanuit een veelheid aan initiatieven benaderd, hetgeen al snel tot een dalend commitment en gebrekkige participatie zal leiden[19]. De ambtelijke experts zijn de facto coördinatoren geworden tussen de diverse fora. Hetzelfde geldt voor de private partijen die worden gevraagd vanuit verschillende

[19] Het bedrijfsleven heeft al van verschillende kanten laten doorschemeren dat zij dreigen af te haken als de "overheid zich niet beter organiseert".

initiatieven. Dit geldt wederom vooral voor vitale bedrijven. Men gaat “forum shoppen”.

Samenvattend, een efficiënte aanpak? Het valt op dat ondanks de beperkte personele middelen er veel activiteiten en initiatieven zijn. Dit heeft tegelijkertijd een schaduwzijde. Zo is er veel en verwarrende overlap tussen de initiatieven en raakt dientengevolge schaarse deskundigheid (ambtelijke expertise en private partijen) versnipperd. Hier bestaat een reëel risico dat deze, voor het resultaat essentiële, deskundigen afhaken. Vanuit het bedrijfsleven zijn al serieuze signalen in deze richting ontvangen met de oproep richting overheid zich beter te organiseren.

5.3 *Conclusie*

Deze analyse beantwoordt de vraag of de overheid een “sluitende, effectieve en efficiënte aanpak” hanteert t.a.v. ICT-veiligheid. Het is nu een logisch moment om deze analyse te doen. Immers, de overgang enkele jaren geleden van ‘cyberspace als aparte wereld’ naar de situatie waarin ICT een vitale infrastructuur binnen onze maatschappij is geworden, heeft de afgelopen jaren vanzelfsprekend geleid tot vele overheidsinitiatieven t.a.v. ICT-veiligheid. Dit werd versterkt door de toenemende aandacht binnen de overheid voor veiligheid in het algemeen. Op basis van de ervaringen die dit heeft opgeleverd, is het nu een natuurlijk moment voor beleidsmatige reflectie op al die initiatieven en te bezien hoe de toekomstige ICT-veiligheidsagenda van de overheid er uit moet komen te zien.

Is het beleid sluitend? Op de vraag of er witte vlekken zijn, is het antwoord dat de bekende risico’s allemaal wel ergens geadresseerd worden. Echter, qua door de overheid gehanteerde aanpak is het een ander verhaal. Er bestaat een eenzijdigheid in gebruikt instrumentarium: er is een sterke nadruk op informatieverstrekking en het overtuigen van partijen om maatregelen te nemen (figuur 4). Verder wordt geconstateerd dat een samenhangend beleidskader ontbreekt dat sturing geeft aan activiteiten.

Is het beleid effectief? De eenzijdigheid in gebruikt instrumentarium heeft invloed op de mate waarin beleidsdoelstellingen kunnen worden gehaald. Er wordt veelal getracht via platforms informatie uit te wisselen en problemen te agenderen bij de juiste partijen. Hoe logisch deze werkwijze ook is bij deze complexe problematiek, de effectiviteit van instrumenten als informatievoorziening en overtuiging is beperkt in die gevallen waar overheid en marktpartijen een afwijkende perceptie en divergerende belangen hebben t.a.v. de aanpak van risico’s. Daarvoor zijn meer robuuste governance-arrangementen nodig, bijvoorbeeld gebaseerd op marktordening en op wet- en regelgeving.

Verder valt op dat er veel en verwarrende overlap bestaat tussen de initiatieven. Schaarse capaciteit (ambtelijke expertise en private partijen) raakt versnipperd. Hier bestaat een reëel risico dat deze, voor het resultaat essentiële, schaarse mensen afhaken. Vanuit het bedrijfsleven zijn al serieuze signalen in deze richting ontvangen onder de oproep richting overheid zich beter te organiseren.

6 Implicaties analyse

Wat zijn de implicaties van de analyse zoals beschreven in het voorgaande hoofdstuk?

- de noodzaak voor een samenhangend en richtinggevend beleidskader. Dat kader moet tevens handvatten bieden voor diversificatie van het te gebruiken instrumentarium opdat het gewenste effect wordt bereikt;
- de versnippering van schaarse deskundigen en het risico van afhaken van partijen noopt tot ordening en afstemming van activiteiten.

Dit hoofdstuk gaat op deze punten nader in, waarbij in §6.3 al een aanzet tot een beleidskader wordt gegeven.

6.1 *Noodzaak voor een samenhangend beleidskader*

Een door de drie departementen gedeeld en richtinggevend beleidskader biedt een mogelijkheid om synergie tussen diverse overheidsactiviteiten te verbeteren. In dit opzicht constateerde de analyse al dat het goed zou zijn als de vele initiatieven meer sturing vanuit een samenhangend beleidskader zouden krijgen. Tevens moet zo'n kader richting geven aan de keuze van instrumenten die effectief zijn voor een gegeven situatie. Dit moet tegemoet komen aan het bezwaar van de huidige te eenzijdige keuze voor instrumenten.

Ook uit discussies in de praktijk over ICT-beveiliging blijkt dat er behoefte is aan een conceptueel denkkader. Deze discussies verlopen vaak chaotisch omdat er vele probleempercepties mogelijk zijn, en vanuit die percepties vervolgens een diversiteit aan oplossingsrichtingen wordt aangedragen. Een beleidskader kan besluitvorming binnen de overheid ondersteunen.

Meerdere partijen onderstrepen de behoefte aan een conceptueel denkkader. Naast dat de TUDelft en TNO constateren dat een samenhangend beleidskader ontbreekt, is ook Europese Commissie zoekende naar zo'n kader. Zij stelt in een mededeling (EU 2005) dat Veiligheid, ICT en Internet voor de overheid een lastig vraagstuk betreft daar geografische grenzen grotendeels irrelevant zijn en klassieke instrumenten voor regulering en handhaving hier niet goed werken. Onderkend wordt dat er een conceptuele discrepantie is tussen de behoefte aan beleid en bestuur, dat het toenemend belang van ICT oproept, en de huidige bestuurlijke concepten. De conclusie die in hoofdstuk 5 wordt getrokken t.a.v. de beperkte effectiviteit van het veelal ingezette instrumentarium is evenzeer toepasbaar op de Europese context. Kortom, er is een conceptuele herdenking van beleid en bestuur nodig, waaronder de herformulering van de overheidsrol en robuuste governance-arrangementen. Een uitdaging hierbij is het ontbreken van een historisch gezien vanzelfsprekend overheidsgezag over Internet.

6.2 *Zorg voor ordening en afstemming*

Een goede ordening en afstemming van activiteiten kan voorkomen dat schaarse capaciteit (ambtelijke expertise en private partijen) te zeer versnipperd raakt en afhaakt. Een optimale inzet van deze capaciteit is een belangrijke succesfactor voor goede en gedragen resultaten.

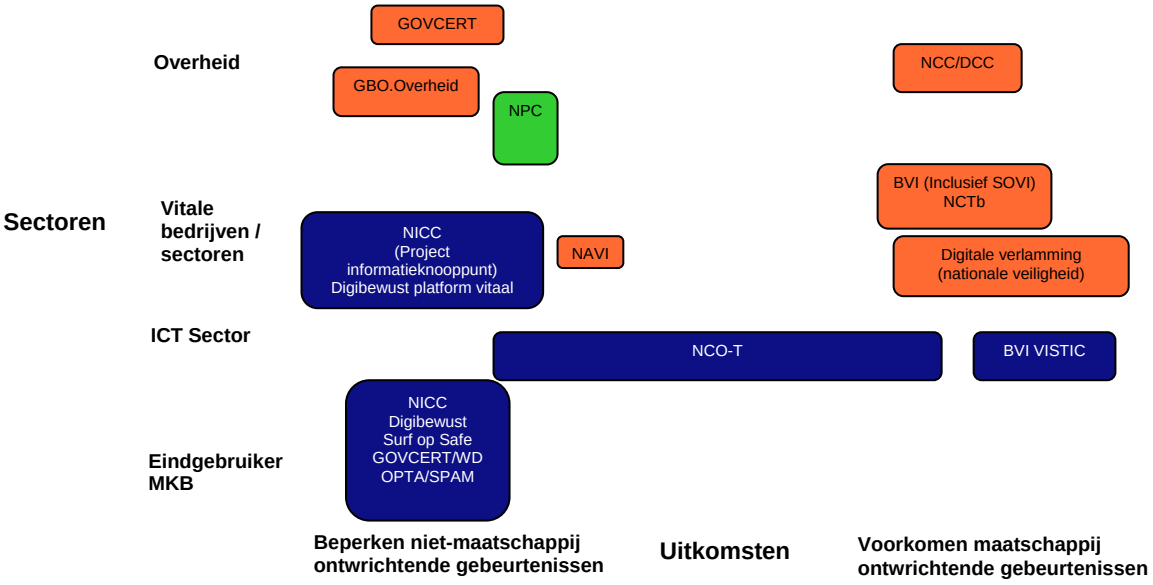
6.2.1 **Ordening**

Uit de analyse blijkt dat er de noodzaak is te komen tot governance-arrangementen die *outputs* en *outcomes* dichter bijeen brengen. Anders gezegd, zorg dat de rol die je als overheid kiest en de instrumenten die je daarbij inzet, passen bij de uitkomsten die je wilt bereiken. Een ordening van de activiteiten rond de uitkomsten die je wilt bereiken is aldus een eerste aangrijpingspunt.

Een onderverdeling naar uitkomsten kan resulteren in de drie volgende arena's:

- *Voorkomen van maatschappij ontwrichtende gebeurtenissen*: hier worden vraagstukken omtrent maatschappij-ontwrichtende risico's en nationale veiligheid behandeld. Het betreft gebeurtenissen die we bijna ten koste van alles willen voorkomen. Daar treed je als overheid sturend op, opdat de overheid zeker weet dat partijen doen wat je vanuit publiek belang wilt. BZK (DGV) is in deze arena de belangrijkste portefeuillehouder.
- *Beperken van niet maatschappij ontwrichtende gebeurtenissen*: vraagstukken omtrent risico's waar we last van hebben, maar die niet maatschappij-ontwrichtend zijn. De overheid tracht hier d.m.v. interventies organisaties te beïnvloeden het gewenste gedrag te vertonen. Vanuit haar marktordenende rol is EZ hier een belangrijke portefeuillehouder. Waar het goed huisvaderschap van de eigen overheidssystemen betreft, is dit BZK (DIOS) als beleidscoördinator binnen de overheid.
- *Opsporen en vervolgen cybercriminelen*: vraagstukken die te maken hebben met opsporing en vervolging van cybercriminelen. Het betreft hier reguliere overheidstaken van het OM, politie en opsporingsdiensten; JUS is in deze arena de belangrijkste portefeuillehouder.

Om een beeld te schetsen wat dat betekent voor de ordening van de huidige activiteiten (hoofdstuk 4), is in onderstaande figuur een poging gedaan een aantal van deze activiteiten conform het bovenstaande te ordenen.



Figuur 6 Ordening van activiteiten naar uitkomsten (TNO 2006)

Het verdient aanbeveling om bestaande en geplande activiteiten te ordenen naar de drie zojuist genoemde arena's en kenbaar te maken wie binnen de overheid eerste aanspreekpunt is voor zo'n arena.

Verder blijkt uit de analyse (efficiënte aanpak?) dat de schaarse personele middelen versnipperd worden ingezet. Tegelijkertijd vormt de deelname van ambtelijke en private experts voor veel van de activiteiten een succesvoorwaarde. Een ordening van de activiteiten rond de schaarse middelen is aldus een tweede aangrijpingspunt. Daarbij zou je kunnen denken aan het bijeenbrengen van activiteiten waar dezelfde schaarse mensen aan deel nemen. Hierbij bestaan vergaande opties als het samenvoegen van activiteiten (bijvoorbeeld binnen de hiervoor onderkende arena's) en minder vergaande, zoals het achter elkaar plannen van bijeenkomsten.

6.2.2 **Afstemming**

Ordening is een eerste vereiste. Daarnaast is afstemming een belangrijk issue. Er zijn minimaal twee zaken te onderkennen die bijdragen aan een betere afstemming: een institutionele en een conceptuele. De mogelijkheid om via een gedeelde conceptuele bril synergie tussen diverse overheidsactiviteiten te verbeteren is al in §6.1 aangegeven.

Hoe kan je daarnaast via institutionele of organisatorische verbanden c.q. afspraken zorgen dat er betere afstemming tussen verwante activiteiten komt? Een eerste vraag die daarbij naar boven komt is wat de verwante activiteiten zijn? De hiervoor beschreven ordening helpt hierbij en maakt afstemming eenvoudiger omdat de hoeveelheid aan projecten waar intensief mee moet worden afgestemd is verminderd: de meest verwante activiteiten zitten immers in dezelfde arena. Het is van belang dat projectleiders van deze activiteiten elkaar kennen opdat zij in direct contact met elkaar kunnen afstemmen; hieronder valt ook de afstemming van de Nederlandse inbreng in de internationale arena. Dit kan bijvoorbeeld worden ondersteund door het geregeld houden van (informele) bijeenkomsten. Naast deze directe afstemming tussen trekkers van activiteiten lijkt er ook behoefte te bestaan aan een meer formeel, interdepartementaal orgaan van leidinggevenden van BZK, EZ en JUS. Zo'n orgaan kan een goede rol vervullen in passende interdepartementale besluitvorming ten aanzien van het gezamenlijk beleid en in het beheren van de gezamenlijke beleidsagenda.

6.3 ***Invulling van een beleidskader***

Het hier geschetste beleidskader bouwt voort op inzichten uit eerdere studies van TUDelft (2002), TUDelft en Stratix (2004), Centraal Plan Bureau (2004) en het interdepartementale Kenniscentrum voor Ordeningsvraagstukken (2005). De strategie sluit aan op de in de vorige paragraaf beschreven arena's en op de in hoofdstuk 3 genoemde omgevingskenmerken en geeft hier een beleidsmatig antwoord op.

In het beleidskader zal aandacht moeten zijn wat deze arena's betekenen voor de rol van de overheid en het instrumentarium dat de overheid in zet. Dit zal per arena verschillen. Lering trekkend uit de analyse ('effectieve aanpak?'), moet in de strategie bekeken worden in hoeverre aanvulling van het huidige eenzijdige instrumentarium zinvol kan zijn. Of, zoals TUDelft en TNO in hun analyse stellen "in overkoepelende zin zijn er robuustere governance-arrangementen nodig: nieuwe spelregels, institutionele vormen en instrumenten die de samenwerking met private partijen tot gewenste uitkomsten doen leiden en die dus moeten kunnen omgaan met uiteenlopende prikkelstructuren, percepties en belangen".

Het beleidskader wordt aan de hand van twee thema's beschreven:

- governance en de rol van de overheid
- professionalisering

6.3.1 Governance en rol overheid

Als het aankomt op ICT, dan wordt er 'gestuurd' door veel partijen, zoals leveranciers, beheerders, gebruikers en diverse overheidspartijen. Al deze partijen nemen beslissingen die de beveiliging van ICT beïnvloeden. De optelsom van al deze beslissingen bepaalt de uiteindelijke veiligheid. In het kader van dit document wordt governance gedefinieerd als het zetten van de condities waaronder beslissingen door partijen worden genomen.

Twee regimes

In hoofdstuk 4 zijn redenen aangegeven waarom de overheid (als beleidsmaker) zich met ICT veiligheid bemoeit. Maar met welke risico's bemoei je als beleidsmaker wel, en hoe intensief dan, en met welke niet? Deze paragraaf geeft daar richting aan.
De complexe en dynamische omgeving pleit voor decentrale oplossingen; ofwel het uitgangspunt is dat partijen (hieronder worden zowel marktpartijen verstaan als uitvoerende organisaties binnen de overheid) hun eigen keuzes maken in het omgaan met risico's zonder dat de overheid (als beleidsmaker) zich hiermee bemoeit. In principe zijn partijen zelf immers het beste in staat een kosten/baten afweging te maken omtrent het omgaan met veiligheidsrisico's. Zij hebben het beste zicht op hun specifieke omstandigheden en wensen en maken ieder hun eigen afweging. Die afweging kan ook wel eens betekenen dat dingen misgaan, maar dat is niet per definitie erg.

Schade betekent niet per definitie dat er onvoldoende is geïnvesteerd in beveiliging (uit: OECD, 2006). "There have been numerous attempts to quantify the damage of cyber attacks. Some of the estimates circulating in official documentation are extremely high, bordering on the ridiculous. It is important to note that many of these number are provided by organizations with an incentive to overestimate the damage – such as security consulting firms. The yearly CSI/FBI estimates are also problematic, but nevertheless widely regarded as the best data current available.
Often, these numbers are used to create a (political) sense of urgency. Security experts argue that cybersecurity is not taken seriously enough and that there is underinvestment in security measures, because actors are not aware of the damages – or only after it is too late. Typically, the argument then continues to call for some form of governmental action.
The problem with all these estimates – no matter how reliable – is that they remove the damage assessments from the context in which they matter most: decentralized cost/benefit tradeoffs by actors, corporate or otherwise. One can put a monetary value on a security failure, but that number really is not very informative, unless one also estimates what it would cost to prevent that damage. In other words, if we really want to now if the private sector is under-investing in cybersecurity, we need to asses the Return of Security Investment (ROSI) levels."

Creditcards Een voorbeeld van de notie dat niet elk veiligheidsrisico slecht is, betreft de creditcard: blijkbaar zijn de kosten voor banken om dit systeem veiliger

te maken hoger dan de kosten die zij moeten maken om klanten te compenseren voor geleden schade t.g.v. fraude. Hoewel dit systeem dus niet veilig is, zijn alle partijen tevreden met deze situatie: klant leidt geen financiële schade en bank heeft een efficiënt systeem. Er is dus geen noodzaak voor overheidsbemoeienis.
De overheid (als beleidsmaker) komt pas in beeld als die afwegingen leiden tot maatschappelijk ongewenste consequenties. Afhankelijk van de grootte van de eventuele maatschappelijke effecten van de keuzes (en dus de mogelijkheid van een verkeerde keuze), zal de overheid partijen meer of minder vrij laten in het maken van hun beslissingen. De overheid kan kiezen voor een faciliterende of sturende (borgende) rol. De twee betrouwbaarheidsregimes die hierbij horen zijn[20]:

- Regime van 'uit te sluiten gebeurtenissen': bij maatschappij ontwrichtende risico's en als de incentives verkeerd liggen om aan veiligheidszorg te doen;
- Regime van 'uitruilbare betrouwbaarheid': bij beperkte risico's en als de incentives verkeerd liggen om aan veiligheidszorg te doen.

Uit te sluiten gebeurtenissen
Uit te sluiten gebeurtenissen zijn gebeurtenissen die we bijna ten koste van alles willen voorkomen, hier is sprake van een publiek belang. Daar treed je als overheid sturend op, opdat de overheid zeker weet dat organisaties de door de overheid gewenste afweging maken en doen wat je vanuit publiek belang wilt. Waar we in de dagelijkse beleidspraktijk vaak worstelen met het veel gebruikte begrip 'vitale diensten', en steeds opnieuw proberen te definiëren wat we daar onder verstaan, kunnen we naar verwachting veel preciezer zijn over wat we ten koste van heel veel proberen te voorkomen. Bijvoorbeeld het onbeheerd achterblijven van het vaste net na een faillissement van KPN. Dit type gebeurtenissen heeft zulke schrikwekkende maatschappelijke consequenties dat ze nooit mogen gebeuren. Er is daardoor altijd vergaande overheidsbetrokkenheid. Die betrokkenheid is zeer specifiek: het uitsluiten van bepaalde gebeurtenissen.

Uitruilbare betrouwbaarheid
Het merendeel van de beleidskwesties zit echter in het regime van uitruilbare betrouwbaarheid. Het woord "uitruilbaar" wordt hier gebruikt in de economische betekenis, in de zin dat veiligheid inwisselbaar is tegen andere aspecten en organisatorische prioriteiten. De mate van veiligheid wordt door de meeste organisaties bepaald in relatie tot prijs, flexibiliteit en andere aspecten. Daarbij geldt dus per definitie niet veiligheid tegen elke prijs, maar juist tegen *welke* prijs. Hier maken organisaties hun afwegingen.
In het regime van uitruilbare betrouwbaarheid is de overheid faciliterend, maar in deze faciliterende rol kan de overheid meer of minder invloed uitoefenen op de uitkomst van die afwegingen door organisaties, het is een glijdende schaal. Een voorbeeld van een lichte invulling van de overheidsrol is een voorlichtingscampagne waarmee de overheid probeert gebruikers te bewegen tot het beveiligen van hun PC's. Een voorbeeld van een zwaardere invulling van de overheidsrol, maar nog steeds in het regime van uitruilbare betrouwbaarheid, is te vinden in de energiesector. Daar wordt de continuïteit van energielevering niet voor 100% gegarandeerd, maar wordt op basis van economische afwegingen geaccepteerd dat energie tijdelijk weg kan vallen. Tegelijkertijd heeft de overheid echter een regeling getroffen dat klanten financieel gecompenseerd worden door

[20] De werkelijkheid is minder dichotoom dan hier geschetst; hier wordt zo op terug gekomen

energieleveranciers als een blackout langer dan twee uur duurt. Dit levert weer een prikkel op voor de energieleverancier om uitval zoveel mogelijk te voorkomen.

	Uitruilbare betrouwbaarheid	**Uit te sluiten gebeurtenissen**
Overheidsrol	Faciliterend (gericht op verbeteren keuze)	Sturend (gericht op afdwingen keuze)
Risico's	Beperkte risico's én verkeerde incentives	Maatschappij ontwrichtende risico's én verkeerde incentives
Keuzevrijheid organisaties	Ruimte voor afweging tussen veiligheids- en andere aspecten	Veiligheid niet-inwisselbaar tegen andere (organisatie)doelen
Maatstaf	Gemiddeld prestatieniveau over vele gevallen	Prestatie in elk geval

Figuur 7 Twee typen risico's en bijbehorende governance (TUDelft 2002)

Overheidsinterventies

In de vorige paragraaf is aangegeven dat er een overheidsrol is als de incentives om iets aan veiligheid te doen verkeerd liggen en dat de rol afhankelijk is van de grootte van het risico. Wat kan de overheid vervolgens doen?

De overheid kan kiezen tussen combinaties van verschillende interventie-instrumenten en coördinatiemechanismen (zie figuur 8). N.B. Voor de uitleg van deze figuur wordt verwezen naar §5.2.1.

		Interventie-instrumenten		
		Financiële Sturing	Informatie-verstrekking	Wet- en regelgeving
Coördinatiemechanismen	Markt			
	Netwerk			
	Hiërarchie			

Figuur 8 Diverse interventiemogelijkheden (naar: WRR (2004))

Ter illustratie, moet de overheid wat doen, en zo ja wat, om te bevorderen dat eindgebruikers hun PC beveiligen? Er kan beredeneerd worden dat hier de

incentives verkeerd liggen omdat gebruikers bij hun afweging tot het treffen van maatregelen niet de schade meenemen die anderen lijden als hun PC wordt misbruikt om systemen van anderen aan te vallen (extern effect). Er is dus een overheidsrol om te interveniëren. Welke opties[21] zijn er om deze rol in te vullen? Een eerste optie is om met ISP's in overleg te treden en hun te overtuigen dat zij maatregelen moeten treffen (netwerk / informatieverstrekking). Een tweede optie is het vanuit de overheid voorlichten van eindgebruikers dat het treffen van beveiligingsmaatregelen zeer belangrijk is (hiërarchie / informatieverstrekking). Een derde optie is het door de overheid niet meer afnemen van diensten van serviceproviders die bepaalde beginselen niet in acht nemen (markt / financiële sturing). Een vierde optie is ISP's aansprakelijk te stellen voor schade die ontstaat t.g.v. slecht beveiligde PC's van hun klanten (markt / wet- en regelgeving). Eventueel kan er ook voor worden gekozen om de interventies elkaar in de tijd te laten opvolgen, afhankelijk van het succes van een interventie (of als stok achter de deur).

Bij het plegen van een interventie moet de overheid er ook goed over nadenken tot wie de interventie het beste gericht kan zijn. Er zijn vele internationale experts die op het volgende eenvoudige principe wijzen: *de interventie moet er op gericht zijn om de incentives goed te leggen voor de partij(en) die het beste in staat is om het risico af te dekken*.

Ter illustratie (!) een aantal voorbeelden waarop het voorgaande is toegepast.

Phishing
(http://www.wired.com/news/politics/0,69076-1.html?tw=wn_story_page_next1)
"Push the responsibility -- all of it -- for identity theft onto the financial institutions, and phishing will go away. This fraud will go away not because people will suddenly get smart and quit responding to phishing e-mails, because California has new criminal penalties for phishing, or because ISPs will recognize and delete the e-mails. It will go away because the information a criminal can get from a phishing attack won't be enough for him to commit fraud -- because the companies won't stand for all those losses.
If there's one general precept of security policy that is universally true, it is that security works best when the entity that is in the best position to mitigate the risk is responsible for that risk. Making financial institutions responsible for losses due to phishing and identity theft is the only way to deal with the problem. And not just the direct financial losses -- they need to make it less painful to resolve identity theft issues, enabling people to truly clear their names and credit histories. Money to reimburse losses is cheap compared with the expense of redesigning their systems, but anything less won't work."

Software security
(http://www.ranum.com/security/computer_security/editorials/lawyers/Testimony_Schneier0603.pdf). "Software vendors do some security testing on their products, but it's minimal because most of the risk isn't their problem. When a vulnerability is discovered in a software product, the vendor fixes the problem and issues a patch. This costs some money, and there's some bad publicity. The real risk is shouldered by the companies and individuals who purchased and used the product, and that risk doesn't affect the vendor nearly as much. When the SQL

[21] Zijn hier niet uitputtend beschreven, slechts enkele ter illustratie

Slammer worm spread across the Internet in January 2003, worldwide losses were calculated in the tens of billions of dollars. But the losses to Microsoft, whose software contained the vulnerability that the Slammer used in the first place, were much, much less. Because most of the risks to Microsoft are ancillary, security isn't nearly as high a priority for them as it should be."

Botnets (uit: OECD, 2006)
"Of special interests are those cases where incentives are diverging – i.e., where the costs of security measures are borne by other actors than those reaping the benefits of improved security. An oft-cited example is the case of botnets. The compromised PCs of end-users are used for criminal purposes against other parties than the owners of the compromised PC. The latter may not even be aware of the presence of the malignant software that has turned his or her PC into a so-called 'zombie.' The costs of this security failure are borne by others, such as an online merchant suffering from Distributed Denial of Service Attacks."

Virusfiltering
Een illustratie dat incentives voor partijen tot het treffen van maatregelen door ontwikkelingen in de tijd ook vanzelf goed kunnen komen te liggen, betreft centrale virusscanning door ISP's. Tegenwoordig scannen ISP's uit eigen beweging virussen op hun centrale mailservers, iets wat zij tot enkele jaren terug niet tot hun taak rekenden. In die tijd lagen de baten van het scannen bij de klanten van een ISP, en de kosten bij de ISP zelf. Doordat ISP's recent zelf erg veel last kregen van de hoeveelheid mailverkeer die door virussen wordt gegeneerd, en dientengevolge extra servercapaciteit moesten plaatsen, ontstond de prikkel om er wat aan te doen. Kosten en baten werden convergent, zij kwamen bij dezelfde partij (ISP) te liggen

Je ziet ook internationaal[22] een verschuiving van doelgroep van beleid: wie is het beste in staat om het risico af te dekken? Waar tot nu toe veel activiteiten gericht zijn op het bewustmaken en voorlichten van eindgebruikers, zou meer moeten worden bezien of leveranciers niet aangespoord kunnen worden meer te doen. Enerzijds zal dit alleen effectief kunnen worden opgepakt in internationaal verband, met name waar het internationale leveranciers betreft en wanneer het wetgevende instrumenten betreft (*level playing field*). Anderzijds kunnen leveranciers ook nationaal worden aangespoord meer te doen.

6.3.2 **Professionalisering**

Professionalisering preventie, opsporing en vervolging
Omdat met cybercrime steeds meer geld te verdienen valt, zullen criminele organisaties zich hiertoe aangetrokken voelen. Cybercrime verdient daardoor een serieuze aanpak qua preventie, opsporing en vervolging. Een verdere professionalisering hierin verdient de aandacht, waarbij rekening moet worden gehouden met de verschillen in ICT skills. Dit betekent maatwerk voor diverse doelgroepen van het beleid, zij het de politie of de eindgebruikers.

[22] EU (2006a)

Vergroot domeinkennis en deel deze

In veel gevallen moeten we onderkennen dat we geen goed beeld hebben van wat precies het probleem is en hoe groot het is. Er bestaat geen eenduidig beeld over de risico's en gevolgen; er ontbreekt vaak ook een gedeelde probleemperceptie. Dit wordt mede veroorzaakt doordat analyses complex zijn en omdat feitelijkheden slechts beperkt voorhanden zijn, zie de eerdere analyse in §3.1.1. De vraag hierbij is: wie heeft behoefte aan welke kennis en hoe komen we daar aan? De gewenste kennis verschilt per departement: zo wil bijvoorbeeld EZ weten hoe de incentives liggen tot het treffen van beveiligingsmaatregelen, wil JUS weten hoe de incentives voor cybercriminelen liggen voor het plegen van misdaden en wil BZK weten wat de bedreiging voor identiteitsfraude is. Echter, er is ook een gedeelde kennisbehoefte. Dit betreft bijvoorbeeld het tijdig beschikbaar hebben van informatie over nieuwe technologische ontwikkelingen en de daarmee samenhangende ICT-veiligheidsvraagstukken en kennis omtrent geschikte risicoanalysemethodieken.

Afhankelijk van het kennisniveau omtrent specifieke risico's en hetgeen we willen weten, zijn verschillende methoden voorhanden, zie onderstaande figuur.

	Threat known	Scale of potential damage known	Probability of damage known
Problem hunting	Yes	Yes	Yes
Iceberg analysis	Yes	No	No
Analyzing the unimaginable	No	No	No

Figuur 9 Verschillende analyse methoden (TUDelft, Stratix, 2004)

Bij *problem hunting* gaat het om op zich bekende dreigingen, maar die zich in steeds nieuwe varianten kunnen voordoen. De focus is hier op één bepaalde dreiging. Vaak zie je dat aanvallers reageren op tegenmaatregelen en hun aanvallen daarop aanpassen. Op basis van analyse van bestaande ervaringen met deze dreiging, wordt geanalyseerd wat nieuwe kwetsbaarheden zouden kunnen zijn.
Bij *iceberg analysis* kunnen we de potentiële bedreiging bedenken, maar de mogelijke schade en kans van optreden zijn onbekend. Is de bedreiging het topje van de ijsberg, of is het de ijsberg zelf? Het risico van deze situatie is dat het kan leiden tot over optimisme of over pessimisme: wordt er te weinig of teveel geïnvesteerd in beveiligingsmaatregelen? De analyse zou zich in eerste instantie moeten richten op die bedreigingen waar een hoop discussie is over de ernst van die bedreigingen. Vervolgens kan door onder gecontroleerde omstandigheden te testen of door gaming meer zicht worden gekregen op de ernst van de kwetsbaarheid.
Tenslotte *analyzing the unimaginable*. Dit richt zich op het achterhalen van het onvoorstelbare, of wel die mogelijke scenario's die grote gevolgen hebben. Zo hadden weinigen voor 9/11 voor ogen dat passagiersvliegtuigen zouden kunnen worden ingezet als vliegende bommen. Vervolgens kan bekeken worden hoe de beveiliging is tegen dit soort scenario's.

Om de domeinkennis te vergroten zou een eerste actie moeten zijn om in interdepartementaal verband te bezien wie aan welke informatie behoefte heeft en

waarom, hoe die informatie verkregen kan worden en welke informatie met wie gedeeld kan worden. Bij dit laatste zal niet alle informatie zomaar gedeeld kunnen worden. Mocht dit echter wel wenselijk zijn, dan is het goed te bezien onder welke voorwaarden dit eventueel wel mogelijk is.

Vergroot veerkracht

Eerder is in §3.1 gesteld dat het reëel is te veronderstellen dat een risico met ernstige schade ooit zal optreden: een combinatie van kleine factoren, welke combinatie vooraf niet werd vermoed, kan bij complexe systemen met veel koppelingen tussen verschillende deelsystemen tot grootschalige uitval van vitale functies leiden. **In dit soort omstandigheden is een strategie van veerkracht (*resilience*) effectiever dan een van vooraf afdekken (*anticiperen*)**. Het belang van deze strategie werd in §3.4 nog eens benadrukt: de conventionele beheersmodellen voor betrouwbaarheid zijn gebaseerd op het gegeven dat de meeste risico's vooraf kunnen worden ingeschat en in het ontwerp worden verdisconteerd. Voor de laatste paar procent heeft men dan real time bewaking. Die verhouding is aan het schuiven. Steeds meer van de betrouwbaarheid van netwerken wordt gerealiseerd in *real time*. Dat is waar verrassingen zich manifesteren en om een response vragen. *Hoe deze gewenste real time early warning & responsecapaciteit vorm te geven?* Dit zou een belangrijke vraag op de overheidsagenda moeten zijn.

Er kunnen al een aantal richtingen voor een antwoord op deze vraag worden onderkend. Het blijkt dat veerkracht sterk samenhangt met informele, vertrouwde sociale netwerken tussen operationele controlecentra (TUDelft, 2002). Een voorbeeld van zo'n netwerk op ICT gebied bestaat al: het early warning (& response) netwerk waarin Computer Emergency Response Teams (CERT) wereldwijd opereren. Als je in Nederland kijkt zijn er een aantal CERT's operationeel die echter maar een beperkt aantal vitale sectoren dekken. Het lijkt raadzaam te bezien in hoeverre een dekking van alle vitale sectoren in Nederland wenselijk en haalbaar is, en wat de rol van GOVCERT daarin kan zijn.

Daarnaast lijkt het raadzaam om te bezien in hoeverre een link tussen dit CERT-netwerk en de bestaande crisisstructuur wenselijk is en hoe dit kan worden vormgegeven. De crisisstructuur binnen de overheid bestaat uit het Nationaal Coördinatiecentrum (NCC) bij BZK en de departementale DCC's. Deze DCC's houden bij crisis contact met (private) partijen binnen hun sector. Deze partijen hebben veelal intern ook een crisisorganisatie opgericht. Het mooie is dat deze crisisstructuur alle vitale infrastructuren in Nederland dekt. De vraag is echter of deze structuur specifieke ICT gerelateerde problemen het hoofd kan (en wil) bieden, of dat hier een aanvullende rol ligt voor CERT-achtige structuren. Dit zou nader bekeken moeten worden opdat Nederland een grootschalig ICT-incident dat meerdere sectoren treft het hoofd kan bieden.

Tenslotte dragen oefeningen ook bij aan het vergroten van de veerkracht.

7 Dit leidt tot de volgende agenda

De agenda die in dit hoofdstuk wordt voorgesteld, volgt uit de analyse en het voorgestelde beleidskader zoals beschreven in hoofdstuk 5 en 6. Deze agenda beschrijft een aantal stappen die genomen kunnen worden om het ICT veiligheidsbeleid van de overheid sluitend, efficiënt en effectiever te maken. Een aantal punten van deze agenda kunnen direct worden toebedeeld aan of een departement of worden ondergebracht bij project. Een aantal andere zullen in interdepartementaal verband verder moeten worden ontwikkeld.
De agenda is opgebouwd rondom drie thema's: governance, professionalisering en internationaal.

1. Governance
Activiteiten onder dit thema beogen de *overheid zelf* beter te organiseren en meer synergie tussen diverse overheidsactiviteiten te bereiken. Daarnaast wordt beoogd de *overheidsrol* en het daarbij in te zetten instrumentarium zodanig in te richten dat de gewenste effecten ook daadwerkelijk worden gerealiseerd. De agenda van dit thema komt tegemoet aan de in §5.3 geconstateerde knelpunten. Een slimme invulling werkt kostenverlagend (minder afstemmings- en vergaderkosten) en vergroot de doeltreffendheid.

- Vervolmaking, 'formalisering' en actieve disseminatie van het in §6.3 geschetste gemeenschappelijke beleidskader voor ICT veiligheid. Waar het project Nationale Veiligheid een strategie voor veiligheidsbeleid in de breedte ontwikkelt, betreft dit actiepunt een uitwerking in de diepte voor veiligheid van ICT. Beide moeten uiteraard goed op elkaar aansluiten. Het beleidskader vormt een belangrijke bijdrage om helder te maken waar de overheid primair aan zet is en moet handvatten bieden voor diversificatie van het te gebruiken instrumentarium. Verder moet het een toetsingskader bieden voor lopende en geplande activiteiten. De uitdaging is om het echt een gezamenlijk, gezaghebbend kader te laten worden.
- Overweging of, en waar, de inzet van momenteel veronachtzaamde instrumenten (figuur 4) zinvol kan zijn. Voor met name wat verdergaande instrumenten als wet- en regelgeving is het van belang dat dit in een internationale context gebeurd. Ten eerste omdat veel wetgeving op dit gebied Europees rechtelijke kaders kent. Ten tweede om internationaal een *level playing field* te behouden.
  Om die reden is door EZ onlangs een onderzoeksvoorstel voor 2007 bij de OESO ingestoken. Doel daarvan is inzicht te verwerven in hoe de incentives voor partijen liggen om al dan niet wat aan beveiliging te doen en te bepalen wat dit betekent voor het te kiezen beleidsinstrumentarium. In dezelfde lijn lijkt voor JUS en BZK een onderzoek naar hoe de economische prikkels van cybercriminelen liggen, en via welke instrumenten hun business modellen kunnen worden beïnvloed, ook waardevol.
- Ordening van projecten/vraagstukken naar gewenste uitkomsten (voorkomen maatschappij ontwrichtende risico's; verminderen risico's waar we dagelijks last van hebben maar die niet maatschappij ontwrichtend zijn; opsporing en vervolging van cybercriminelen). Vervolgens het zorgen dat de noodzakelijke inbreng van schaarse capaciteit (ambtelijke expertise en private partijen) geborgd blijft door het meer bijeenbrengen van activiteiten. Het pleit er voor

dit zo vorm te geven dat bureaupolitieke belangen en eigen 'dynamiek' van betrokken organisaties weinig ruimte krijgen en de inspanningen zoveel mogelijk gericht zijn op bedoelde beleidsuitkomsten. Opties moeten worden geïnventariseerd hoe dit te bereiken, waarna een keuze kan worden gemaakt. In aanvulling op ordening, zorgen door een goed agendabeheer dat activiteiten afgestemd zijn en blijven en dat transparant is hoe de verschillende activiteiten zich tot elkaar verhouden.

2. Professionalisering

In veel gevallen moeten we onderkennen dat we geen goed beeld hebben van wat precies het probleem is en hoe groot het is. Er bestaat geen eenduidig beeld over de risico's en gevolgen; er ontbreekt vaak ook een gedeelde probleemperceptie. De vraag hierbij is: wie heeft behoefte aan welke kennis en hoe komen we daar aan? En hoe zorgen we ervoor dat we gezamenlijk wijzer worden?

- Stroomlijning en verbetering van structurele analyse en kennisdeling. In verschillende projecten (o.a. Nationale Veiligheid, NAVI, NICC, Digibewust) is reeds onderkend dat er behoefte is aan betere analyse, informatie uitwisseling, risicobeoordeling etc. Die projecten zijn ieder voor zich druk doende invulling te geven aan die behoefte. I.h.k.v. de gewenste professionalisering bepleit dit agendapunt dat dit meer in afstemming gebeurd opdat de uitkomst meer is dan de som der delen. Van belang daarbij is dat door BZK, EZ en JUS wordt geïnventariseerd wie aan welke kennis behoefte heeft en waarom, hoe die kennis kan worden verkregen en hoe die kan worden gedeeld (en onder welke voorwaarden). Enerzijds vergroot dit het inzicht in de problematiek, anderzijds blijkt dat door andere 'brillen' medewerkers verschillende informatiebehoeften hebben en daar andere conclusies aan verbinden. Dit kan in het slechtste geval leiden tot divergerend beleid.
- Ontwikkel een gezamenlijk onderzoeksagenda voor die onderwerpen waar gemeenschappelijke interesses liggen. Onderwerpen die hierin onder andere aan bod kunnen komen, zijn de beveiliging van de publieke dienstverlening (om ons scherp te houden) en de voorbereiding op nieuwe ontwikkelingen (om te anticiperen).

Twee ander punten die professionalisering behoeven, betreffen het versterken van de veerkracht en de opsporing en vervolging van cybercrime. In een complexe, dynamische omgeving is een strategie van veerkracht (*resilience*) effectiever dan een van vooraf afdekken (*anticiperen*). Steeds meer van de betrouwbaarheid wordt gerealiseerd in *real time*. Dit is waar verrassingen zich manifesteren en om een professionele response vragen.

- Hoe de gewenste real time early warning & responsecapaciteit vorm te geven? Welke functies zijn daarvoor nodig? Is een nationale CERT functie nodig en wat zou de relatie kunnen zijn tussen de CERT-functie en de al langer bestaande crisisinfrastructuur (NCC/DCC's/crisiscentra binnen sectoren)?
- Omdat met cybercrime steeds meer geld te verdienen valt, zullen steeds meer criminele organisaties zich hiertoe aangetrokken voelen. Cybercrime verdient daardoor een serieuze aanpak qua opsporing en vervolging.

3. Internationale samenwerking

Hoewel enigszins buiten de scope van dit project, mag internationale samenwerking niet ontbreken op de beleidsagenda. Het ICT-veiligheidsvraagstuk is de afgelopen jaren sterk naar boven gekomen op de internationale agenda.

Medio 2006 heeft de Europese Commissie een beleidsvoornemen gepubliceerd met betrekking tot ICT-veiligheid (EU, 2006a en 2006b). In het kader van R&D-stimulering is veiligheid een van de speerpunten geworden in de vorm van het European Security Research Program (ESRP). Ook het Europese Agentschap ENISA wordt na de energieverslindende opstartfase actiever.
In wereldwijd verband heeft de OESO structureel aandacht voor ICT-veiligheid. Zij heeft onder andere *guidelines* geschreven hoe diverse partijen, waaronder overheden, om moeten gaan met ICT-veiligheid. Voorts heeft OESO recent een anti-spam toolkit uitgebracht.

Om de effectiviteit van haar beleid te vergroten, moet Nederland zich steeds actief afvragen welke internationale inspanningen daartoe zijn benodigd. Dit heeft zowel betrekking op de internationale beleidsvoorbereiding als op het oppakken van internationale afspraken. Twee voorbeelden.
Qua beleidsvoorbereiding is onder governance al gesteld dat voor met name verdergaande instrumenten als wet- en regelgeving internationale samenwerking een vereiste is. De Europese Commissie lijkt op dit vlak actiever te worden, afgaande op haar laatste mededeling. De uitkomsten van de onder governance genoemde OESO studie moet Nederland inbrengen in de verdere gedachtevorming over dit type instrumenten binnen Europa.
Qua het invulling geven aan internationale afspraken is politiële en justitiële samenwerking en informatie-uitwisseling bij opsporing en vervolging een belangrijk agendapunt voor de komende jaren.

Hoe verder?
In dit hoofdstuk is een agenda voor de komende 2 à 3 jaar voorgesteld. Hoe daar aan te gaan werken? Dat is een lastig vraagstuk.
Zonder exact aan te geven hoe verder te gaan, zijn ons inziens twee criteria van belang om verbetering in de huidige situatie te brengen:

- nauwe betrokkenheid van belangrijkste dossierhouders. Er lijkt minder kans van slagen om veranderingen er door te krijgen als een projectgroep min of meer zelfstandig opereert, los van lopende grote projecten (zoals nu grotendeels het geval is);
- steun vanuit verantwoordelijk management van de drie betrokken departementen.

Dit laatste punt is de reden om de uitkomsten van dit project in januari 2007 onder de aandacht te brengen van DG's van BZK, EZ en JUS. Zij zijn tenslotte degenen die over een gezamenlijke agenda gaan en opdracht kunnen geven hier aan te gaan werken.

Een aantal punten van deze agenda kunnen direct worden toebedeeld aan of een departement of worden ondergebracht bij een bestaand project[23]. Een aantal andere punten zullen in interdepartementaal verband verder moeten worden ontwikkeld, met nauwe betrokkenheid van de belangrijkste dossierhouders.

[23] Een voorbeeld is de vraag hoe veerkracht kan worden vormgegeven; dit lijkt typisch iets dat in het project Nationale Veiligheid kan worden opgepakt. Een ander voorbeeld is de professionalisering van de opsporing en vervolging van cybercriminelen; dit lijkt typisch iets voor Justitie. Qua onderzoeksagenda kan mogelijk worden aangesloten bij het programma Technologie en Veiligheid van BZK

Afkortingen

AIVD — Algemene Inspectie en Veiligheid Dienst
AT — Agentschap Telecom, agentschap van het ministerie van EZ
BVI — Project Bescherming Vitale Infrastructuren
BZK — Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CERT — Computer Emergency Response Team
CSI — Amerikaanse Computer Security Institute
DCC — Departementaal Coördinatie Centrum
ECP.nl — Electronic Commerce Platform Nederland
EZ — Ministerie van Economische Zaken
ISP — Internet Service Provider
JUS — Ministerie van Justitie
KLPD — Korps Landelijke Politiediensten
MKB — Midden en Klein Bedrijf
NAVI — Nationaal Adviescentrum Vitale Infrastructuren
NCC — Nationaal Coördinatie Centrum
NCO-T — Nationaal Continuïteitsoverleg Telecom
NCTb — Nationaal Coördinator Terrorismebestrijding
NICC — Nationale Infrastructuur bescherming Cyber Crime
NPC — Nationaal Platform Cybercrime
OECD — Organisation for Economic Co-operation and Development
OM — Openbaar Ministerie
OPTA — Onafhankelijke Post en Telecommunicatie Autoriteit
PKI — Public Key Infrastructure
PPS — Publiek Private Samenwerking
SOVI — Strategisch Overleg Vitale Infrastructuren
VenW — Ministerie van Verkeer en Waterstaat
WD — Waarschuwingsdienst
WRR — Wetenschappelijke Raad voor het Regeringsbeleid

Literatuur

BZK (2003), *Critical Infrastructure Protection in the Netherlands*, publicatie i.h.k.v. het project BVI

CPB (2004), *Better safe than sorry? Reliability in network industries*

CSI/FBI (2006), *Computer crime & security Survey: 11th annual survey*, Computer Security Institute (CSI) in samenwerking met de FBI, www.gocsi.com

EU (2001), *Netwerk- en informatieveiligheid: voorstel voor een Europese beleidsaanpak*, COM(2001)298 definitief, Brussel, 6.6.2001

EU (2005), *2010-A European Information Society for growth and development*, COM(2005), Brussels

EU (2006a), *Een strategie voor een veilige informatiemaatschappij — "Dialoog, partnerschip en empowerment"*, COM(2006)251 definitief, Brussel, 31.5.2006

EU (2006b), *Annex to: A strategy for a secure information society – dialogue, partnership and empowerment*, Commission staff working document SEC(2006)656, Brussels, 31.5.2006

EZ (2005), *De toekomst van elektronische communicatie*, publicatie ministerie van EZ, publicatienummer. 05TP12

Kenniscentrum voor Ordeningsvraagstukken (2005), *Betrouwbaarheid in netwerksectoren. Reflectie op de rol van de overheid,* interdepartementale publicatie n.a.v. studie CPB (2004)

Mooij, J. en J. van der Werf (2002) Cybercrime. Zoetermeer: KLPD (NRI 22/2002)

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

OECD (2006), *Proposal for a study on the economics of cybersecuriy*, OECD Room document B, 21th meeting of the WPISP

Perrow, C. (1984), *Normal Accidents*, Princeton

Schulman, P en Van Eeten, M.J.G. (2002), *Reliablity in Real Time: Reliablity Theory and Management of Complex Systems*, paper in Administrative Science Quarterly

TNO (2006a), *ICT-Veiligheidsbeleid in Nederland – een quick scan*, in opdracht van het interdepartementale project 'Herijking ICT-veiligheidsbeleid'

TNO (2006b), *ICT-veiligheidsbeleid in Nederland – Analyse en overwegingen bij herijking*, in opdracht van het interdepartementale project 'Herijking ICT-veiligheidsbeleid'

TUDelft (2002), *Kwetsbaarheid, betrouwbaarheid en verantwoordelijkheid. Vormgeven aan overheidsbetrokkenheid bij een dynamische sector*, essay geschreven voor V&W

TUDelft, Stratix (2004), *Governance of e-security: a framework for policy*, paper geschreven voor EZ i.h.k.v. het EU-voorzitterschap

TUDelft (2006), *Herijking van het ICT-Veiligheidsbeleid, Analyse van de lopende initiatieven van de ministeries van Economische Zaken, Binnenlandse Zaken en Koninkrijksrelaties en Justitie*, in opdracht van het interdepartementale project 'Herijking ICT-veiligheidsbeleid'

PriceWaterhouseCooper (2006), *Information security breaches survey 2006*, in opdracht het het Britse DTI, URN 06/803

VenW (2001), *Kwetsbaarheid op internet: samenwerken aan meer veiligheid en betrouwbaarheid*, publicatie ministeries van VenW en EZ

Wetenschappelijke Raad voor het Regeringsbeleid (2004), *Bewijzen van goede dienstverlening*

Samenstelling Stuurgroep en Projectgroep

Stuurgroep

Simon van de Geer, JUS
Jan Moelker, BZK
Afke van Rijn, EZ, voorzitter
Michel Verhagen, EZ

Projectgroep

Koos Bossers, EZ
Ronald van der Luit, EZ, projectleider
Hin Oey, SenterNovem
John Stienen, BZK