Herijking van het ICT-Veiligheidsbeleid

Analyse van de lopende initiatieven van de ministeries van Economische Zaken, Binnenlandse Zaken en Koninkrijksrelaties en Justitie

September 2006

Michel van Eeten
Ruben van Wendel de Joode

Faculteit Techniek, Bestuur en Management
Technische Universiteit Delft

Michel van Eeten & Ruben van Wendel de Joode
Sectie Beleidskunde, Organisatie en Management
Faculteit Techniek, Bestuur en Management
Technische Universiteit Delft
Postbus 5015
2600GA Delft
m.j.g.vaneeten@tbm.tudelft.nl
+31 15 2787050 (t)
+31 15 2786233 (f)

Overzicht

- Opgave
- Vragenlijst
- Kenmerken van huidige initiatieven
- Een sluitende aanpak?
- Een efficiënte aanpak?
- Een effectieve aanpak?
- Herijking van ICT Veiligheidsbeleid
- Implicaties

TU Delft

Opgave

- Analyse van huidige initiatieven op het gebied van ICT-veiligheid
- Naar een "sluitende, efficiënte en effectieve aanpak"

3

TU Delft

Analyse van huidige initiatieven op het gebied van ICT-veiligheid

Doelstelling van het herijkingproject is om de bestaande projecten, organisaties en afdelingen op het gebied van ICT-veiligheid van de ministeries van EZ, BZK en Justitie met elkaar te confronteren en vast te stellen of er sprake is van een "sluitende, efficiënte en effectieve aanpak".

De uitdaging is om ondanks het grote aantal en de grote verscheidenheid aan activiteiten deze toch in samenhang te beschouwen.

Materiaal

- Initiatieven te pluriform voor vragenlijst: omvatten nieuwe taken, nieuwe programma's, nieuwe organisatievormen, maar ook bestaande taken in gevestigde organisaties
- Vragenlijst vooral bruikbaar voor het overzicht
- Antwoorden slechts indicatief, niet goed vergelijkbaar
- Ondanks deze beperkingen, toch aantal dominante beelden aangaande het huidige ICT Veiligheidsbeleid
- Aangevuld met relevante plannen, programma's en projectdocumentatie

TU Delft

Vragenlijst

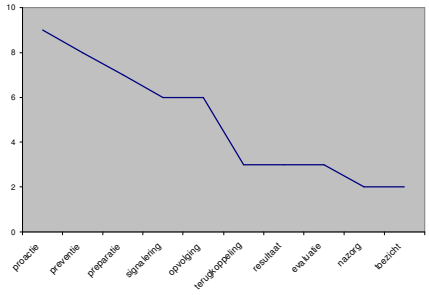
In de zomer van 2006 zijn er vragenlijsten verstuurd aan alle relevante organisatieonderdelen. De vragenlijst is ingevuld door vertegenwoordigers van de verschillende initiatieven op het gebied van ICT veiligheid. We gebruiken de term initiatieven hier als een koepelnaam voor organisaties, bestaande afdelingen, projecten en platformen.

Wat als eerste opvalt, is de grote diversiteit tussen de initiatieven. Deze diversiteit maakt dat de antwoorden op de vragen lastig vergelijkbaar zijn. Voor een project is het relatief eenvoudig om het aantal inzetbare fte aan te geven. Voor bestaande taken die opgaan in een breed beleidspakket van een staande directie is het veel moeilijker om de beschikbare capaciteit te schatten.

Ondanks deze beperkingen biedt de vragenlijst in combinatie met de documentatie van de diverse initiatieven wel degelijk voldoende basis om enkele dominante patronen te schetsen.

Kenmerken huidige initiatieven (1)

- Groot aantal initiatieven met relatief kleinschalige middelen
  - 9 van de 16 ondervraagde initiatieven = 4 fte
  - meeste middelen bij uitvoerings- en toezichtsorganisaties
- Nadruk op eerste stappen in veiligheidsproces



5

TU Delft

Kenmerken huidige initiatieven

We zullen hieronder een aantal kenmerken van de initiatieven benoemen. Hierbij moet gezegd dat het benoemen van deze kenmerken geen waardeoordeel impliceert. Het gaat primair om het vinden van patronen in de gevarieerde verzameling van lopende initiatieven. Die patronen zullen uiteindelijk helpen 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 geven de respondenten aan dat 9 van de 16 ondervraagde initiatieven minder dan 4 fte inzet voor de activiteiten. De uitzonderingen hierop zijn de uitvoerings- en toezichtsorganisaties. De OPTA, AIVD en AT geven aan dat ze meer fte hebben toegewezen aan deze activiteiten.

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

Kenmerken huidige initiatieven (2)

- Nadruk op bewustwording
  - 10 van de 16 ondervraagde initiatieven noemt dit als een cruciaal onderdeel van het initiatief
- Nadruk op PPS-achtige constructies
  - 7 van de 16 ondervraagde initiatieven noemt dit als een cruciaal onderdeel van het initiatief
  - andere initiatieven richten zich meestal op overheid zelf
- Weinig nadruk op specifieke veiligheidsoplossingen
  - eigenlijk alleen wanneer het de overheid zelf betreft (bv. PKI-overheid, DigID, eNIK)

TU Delft

Een volgend kenmerk is de nadruk op activiteiten die zich richten op het stimuleren van bewustwording. Van de 16 ondervraagde initiatieven, noemen 10 dit als een cruciaal onderdeel van het initiatief. 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'.

Verder valt op dat veel initiatieven kiezen voor publiek-private samenwerkingsconstructies (PPS-constructies). Van de 16 ondervraagde initiatieven noemen 7 dit als een cruciaal onderdeel van het initiatief. Ook dit kent weer verschillende verschijningsvormen. Zo zijn er verschillende platforms rondom veiligheidskwesties, maar ook organisaties die zich richten op advies aan private partijen, zoals NAVI.

De 9 initiatieven die geen PPS-constructies kiezen, lijken zich vooral te richten op de overheid zelf. Denk hierbij aan ICT-veiligheid binnen de overheidsorganisatie en voorzieningen die primair op de overheid zijn gericht, zoals de PKI-overheid. Een belangrijke uitzondering is de uitvoering van toezichtstaken door OPTA en AT.

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 ook hier, om dezelfde redenen, de activiteiten die zich richten op de overheid zelf. Denk hierbij aan projecten als PKI-overheid, DigiD en eNIK.

Kenmerken huidige initiatieven (3)

- Doelen vaak geformuleerd op twee niveaus:
  - in termen van middelen (*outputs*); bijvoorbeeld 'opzetten van platform voor kennisuitwisseling'
  - in termen van strategische uitkomsten ten aanzien van veiligheid (*outcomes*); bijvoorbeeld 'het borgen van nationale veiligheid'
- Lastige koppeling tussen *outputs* en *outcomes*:
  - middelen steken vaak schraal af bij ernst van gesignaleerde probleem
  - middelen hebben causaal weinig invloed op veiligheid
  - doelbereiking wordt doorgaans 'gemeten' in termen van middelen, niet van veiligheid

7

TU Delft

Een volgend kenmerk dat opvalt, betreft de *doelen* die de initiatieven zich stellen. Vaak zien we twee typen doelen naast elkaar bestaan: Doelen in termen van de op te leveren middelen (zoals het organiseren van een publiek-privaat platform voor kennisuitwisseling of het uitvoeren van een pilotproject) en doelen in termen van de uiteindelijk beoogde effecten van die middelen (zoals het borgen van nationale veiligheid). We spreken dan respectievelijk van *outputs* en *outcomes*:

Veel initiatieven formuleren doelstellingen van beide typen. Dan 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 causaal weinig invloed op ICT-veiligheid. Tenslotte wordt doelbereiking doorgaans 'gemeten' en afgerekend in termen van middelen en niet in termen van veiligheid.

Kenmerken huidige initiatieven (4)

- Verantwoordelijkheid voor bereiken strategische doelen (*outcomes*) meestal toegewezen aan andere partijen dan initiatiefnemer
- Veel aandacht voor verdeling van rollen en verantwoordelijkheden over betrokkenen (m.n. publiek-privaat)
- Veel initiatieven geven aan een 'gebrekkig urgentiebesef' te constateren bij die andere – doorgaans private – partijen

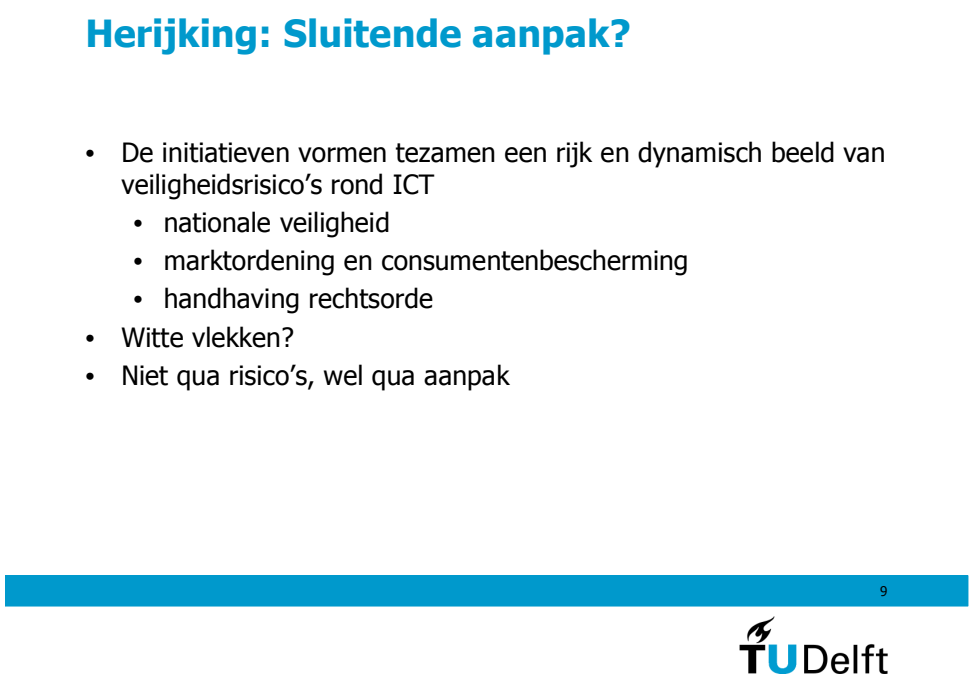
8

TU Delft

Een ander kenmerk dat opvalt, is dat de verantwoordelijkheid voor het bereiken van de strategische doelen (*outcomes*) meestal toegewezen aan andere partijen dan de initiatiefnemer – vaak aan private partijen. Het is dan ook niet verrassend dat initiatieven veel aandacht besteden aan de verdeling van rollen en verantwoordelijkheden over betrokkenen. Het toewijzen van die verantwoordelijkheid aan anderen is alles behalve vanzelfsprekend.

Hoeveel er ook gesproken wordt over de verdeling van rollen en de verantwoordelijkheden tussen publieke en private organisaties, echt handelingsgericht wordt het zelden. Dit komt met name doordat het de overheid is die dit vaststelt en dat de partijen die de verantwoordelijkheid toebedeeld krijgen hier zelf niet of nauwelijks een aandeel in hebben.

Dat leidt tot voorspelbare discrepanties tussen de gepercipieerde rollen en verantwoordelijkheden tussen de overheid en het bedrijfsleven. Er wordt vaak gezegd dat de bedrijven zelf hun verantwoordelijkheid onvoldoende invullen. In menig overheidsdocument treffen we dan ook zorgelijke uitspraken aan over een 'gebrekkig urgentiebesef' bij andere – doorgaans private – partijen. Dit is echter een rechtstreeks uitvloeisel van de rolopvatting van de overheid zelf: men 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.



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?
- Efficiënte aanpak?
- Effectieve aanpak?

Sluitende aanpak?

De initiatieven vormen samen een rijk en dynamisch beeld van de veiligheidsrisico's die bestaan over het onderwerp van ICT. We denken daarbij aan risico's rondom: a) nationale veiligheid, b) marktordening en consumentenbescherming en c) handhaving rechtsorde. Ook de risico's zoals die naar voren komen in de recente trendanalyses rond *cybersecurity* (zie bijvoorbeeld *IBM Security Threats and Attack Trends Report 2006*), komen op diverse plaatsen aan bod.

Op de vraag of er witte vlekken zijn, kunnen we dus stellen, dat het scala aan mogelijke risico's adequaat gedekt lijkt. Qua aanpak is het echter een ander verhaal, zoals blijkt uit de volgende dia.

Herijking: Sluitende aanpak?

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

(Gebaseerd op WRR, *Bewijzen van maatschappelijke dienstverlening*, 2004)

TU Delft

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 maatschappelijke dienstverlening* (WRR, 2004).

De achterliggende vraag bij de coördinatiemechanismen is: op welke wijze wordt het gedrag van actoren 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 actoren 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 actoren.

Binnen elk institutioneel 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 te financieren of als *launching customer* op te treden, 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 Zweedse overheid de

kosten van bepaalde investeringen die ze gerealiseerd wil zien in de netwerken van telecommunicatie-operators. Denk ook aan het Noodnet, waar de overheid een bepaalde veiligheidsvoorziening zelf ontwerpt en financiert.

Enkele andere voorbeelden. DigiBewust combineert hiërarchie met informatievoorziening: De overheid draagt een bepaalde veiligheidsvisie uit en probeert de maatschappelijke partijen tot een bepaalde gedragsverandering te bewegen. Op het gebied van markt en informatievoorziening kunnen we bijvoorbeeld wijzen op het opstellen van de zogenaamde 'transparameters', waarmee klanten van ISP's kunnen vragen transparantie te verschaffen over de veiligheid en betrouwbaarheid van hun diensten. Op het gebied van regelgeving zijn er weinig voorbeelden. De spamwetgeving is het meest duidelijke voorbeeld van hiërarchie en regelgeving – en, voor zover het de regulering van bonafide commerciële uitingen betreft, van markt en regelgeving. Rond de andere initiatieven zien we alleen 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 van een bepaalde groep operators verplicht is gesteld (netwerk en wet- en regelgeving) en omdat in het procesontwerp van het NCO-T de mogelijkheid is opgenomen dat de overheid zelf maatregelen identificeert en oplegt, mochten deze niet op vrijwillige basis tot stand komen (hiërarchie en wet- en regelgeving).

Herijking: Sluitende aanpak?

- Twee beelden:
  - zwaartepunt bij informatieverstrekking, in mindere mate wet- en regelgeving, financiële sturing zo goed als afwezig
  - zwaartepunt bij netwerk-coördinatie, in mindere mate hiërarchische sturing, marktmechanismen zo goed als afwezig

11

TU Delft

We hebben de verzameling aan lopende initiatieven gepositioneerd op deze twee dimensies. 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.

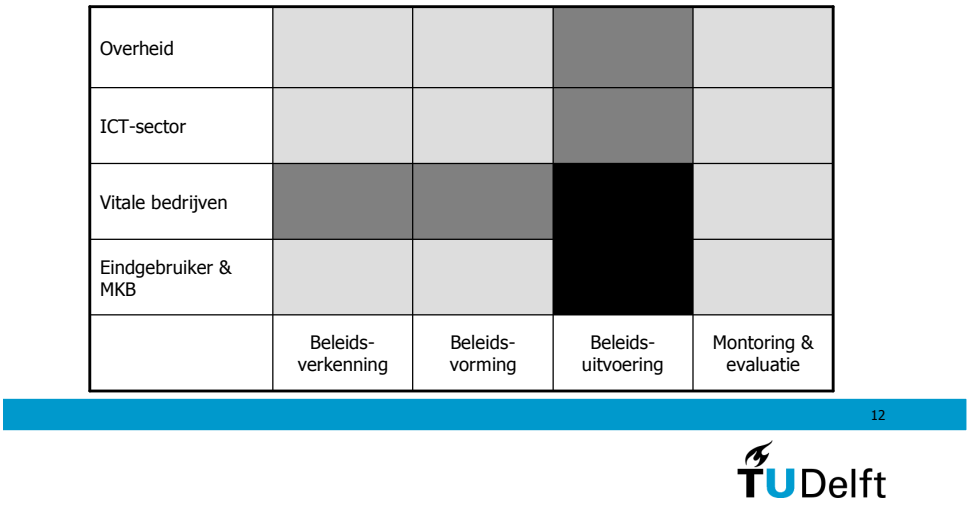
Hoe donkerder de cel, hoe meer initiatieven de betreffende aanpak volgen. Zo zien we dat de bulk van de initiatieven gebruik maakt van de instrumentfamilie informatievoorziening binnen netwerk-achtige coördinatie. Hier zien we de eerder gesignaleerde nadruk terug op PPS-achtige constructies en op bewustwording.

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 de aanpak van de overheid twee eenzijdigheden kent: een sterke nadruk op netwerkcoördinatie en op informatieverstrekking. Zo zou de overheid 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. Via wet- en regelgeving zou de overheid aansprakelijkheden kunnen definiëren of effectiever anders kunnen arrangeren. Dat heeft vervolgens weer gevolgen voor de (financiële) *incentives* van marktpartijen.

Herijking: Sluitende aanpak?

- Doelgroep - beleidsactiviteit



We hebben de verzameling initiatieven ook nog doorsneden naar doelgroep en beleids-fase. Daarbij blijkt de meeste activiteit plaats te vinden in en rond beleidsuitvoerende en toezichthoudende taken. Ook ligt er een sterke nadruk en overlap tussen de initiatieven qau doelgroep van de vitale bedrijven.

Herijking: Sluitende aanpak?

- Twee beelden:
  - zwaartepunt in initiatieven ligt rondom beleidsuitvoering, in relatief beleidsarme context
  - zwaartepunt ligt bij doelgroep vitale bedrijven
- Zwaartepunt bij toezichthouders en uitvoerende instanties kan ook deels eenzijdigheid in instrumenten en sturingsarrangementen verklaren: netwerksturing en informatieverstrekking passen binnen bestaande bevoegdheden, vereisen geen nieuwe beleidskaders

13

TU Delft

Uit de tabel kunnen we twee dominante beelden destilleren. 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. Het tweede beeld is dat het zwaartepunt ligt bij de doelgroep van vitale bedrijven. Een groot deel van de initiatieven richt zich hierop, zij het niet allemaal in exclusieve zin. Dit kon verwacht worden, gezien het belang van vitale infrastructuren en de initiatieven op dit terrein sinds de millenniumwisseling en de aanslagen van 11 september 2001.

De nadruk op beleidsuitvoering kan ook een verklaring zijn voor de eerder gesignaleerde eenzijdigheid in het instrumentarium – namelijk de nadruk op netwerksturing en informatieverstrekking. Deze instrumenten vereisen geen wettelijke kaders of beleidsmatige wijzigingen. De uitvoerende en toezichthoudende instanties kunnen niet op eigen kracht nieuw beleid of wettelijke kaders introduceren. In het licht van de lichtbeleidsarme context waarin ze opereren resulteert dat in een eenzijdig instrumentarium. Met andere woorden, ze ontvangen weinig rugdekking vanuit het beleid. Andersom geldt dat hun activiteiten weinig sturing en visie kennen vanuit een samenhangend beleidskader.

Herijking: Efficiënte aanpak?

- Ondanks beperkte middelen, toch veel initiatieven
- Maar twee problemen:
  - Verwarrende overlap
  - Schaarse middelen raken versnipperd: inbreng ambtelijke expertise en private partijen

TU Delft

Herijking: Efficiënte aanpak?

Het tweede criterium is efficiëntie. Hier valt op dat ondanks de beperkte middelen er toch veel activiteiten en initiatieven zijn. In die zin wordt er gewoekerd met middelen.

Toch is er ook een aantal problemen. Zo is er veel en verwarrende overlap tussen de initiatieven, bijvoorbeeld wat de beoogde deelnemende partijen betreft. Daarnaast raken schaarse middelen versnipperd doordat er zoveel initiatieven lopen.

Herijking: Efficiënte aanpak?

- Veel overlap tussen initiatieven
  - overlap in beoogde deelnemende partijen
  - overlap in problematiek
- Enige overlap is functioneel voor complexe en dynamische problemen: ICT-veiligheid laat zich (nog) onvoldoende in deelproblemen opsplitsen
- Strategische doelen (*outcomes*) bieden te weinig richting om de fora ten opzichte van elkaar af te bakenen, omdat 'alles met alles samenhangt'
- Daardoor kunnen veel veiligheidsissues in meerdere fora ter sprake komen (bv. grootschalige uitval telecom in NAVI, NICC, NCO-T, Digitale Verlamming)
- Zelfs insiders hebben geen 'begrijpelijk verhaal' over samenhang

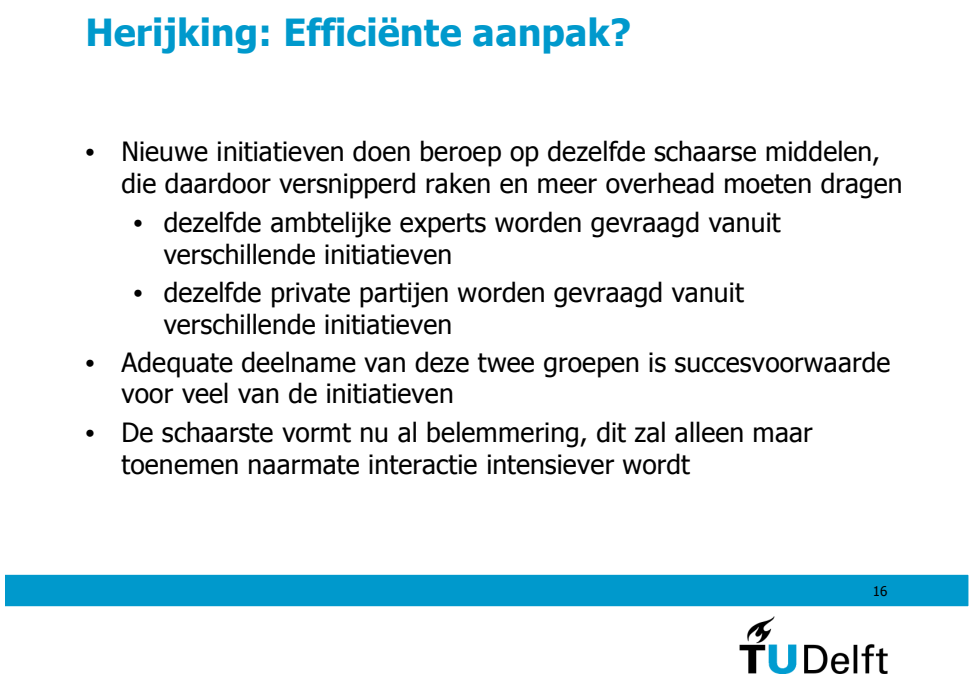
15

TU Delft

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 zelfs 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.

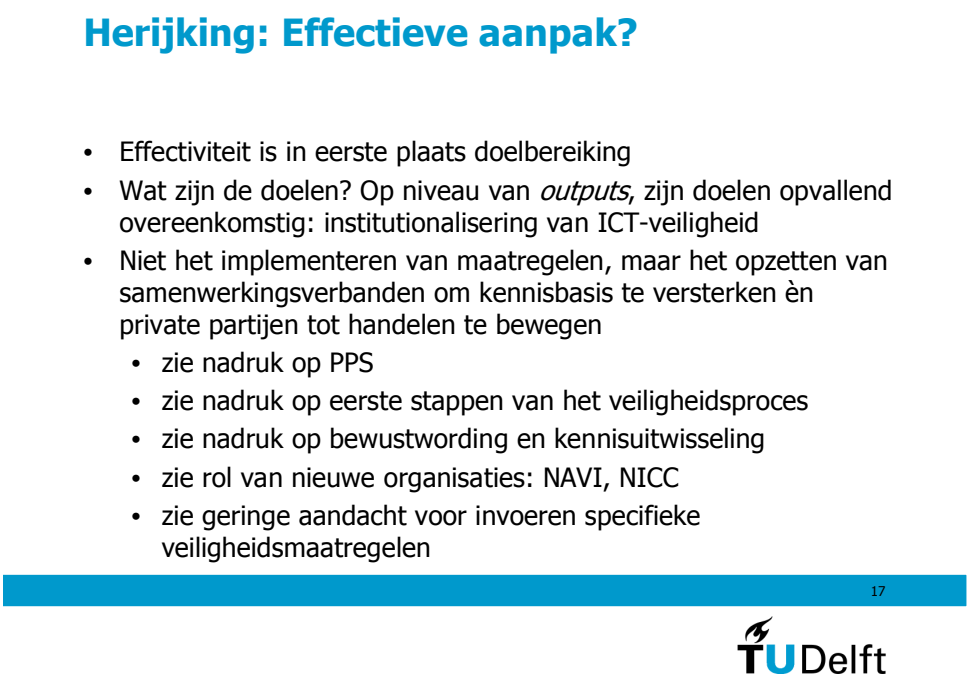
In het algemeen geldt dat niemand, zelfs de *insiders* niet, een 'begrijpelijk verhaal' hebben over de samenhang. Sommige initiatieven claimen een kader te scheppen waarbinnen de andere initiatieven een plek krijgen, maar hun claims stemmen onderling niet overeen. De verschillende initiatieven hebben uiteenlopende opvattingen 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. ICT-veiligheid laat zich (nog) onvoldoende in deelproblemen opsplitsen voor een scherpere afbakening van onderwerpen en taken.

Echter, te veel overlap heeft als nadeel dat de schaarse middelen versnipperd raken. Twee schaarse middelen zijn cruciaal: ambtelijke expertise en de deelname van private partijen. Beide worden vanuit een veelheid aan initiatieven benaderd, hetgeen al snel tot een dalend *commitment* en gebrekkige participatie zal leiden. De ambtelijke experts zijn de facto coördinatoren geworden tussen de diverse fora. Hetzelfde geldt voor de private partijen die worden gevraagd vanuit verschillende initiatieven. Dit geldt wederom vooral voor vitale bedrijven. Men gaat "forum shoppen".

Het is duidelijke dat adequate deelname van ambtenaren en private partijen een succesvoorwaarde is voor veel van de initiatieven. De schaarste vormt nu al een belemmering en dit zal alleen maar toenemen naarmate interactie intensiever wordt.



Herijking: 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 om kennisbasis te versterken èn private partijen tot handelen te bewegen. Dit is reeds op verschillende plekken in de argumentatie duidelijk geworden. Zie bijvoorbeeld de nadruk op PPS-achtige constructies, de nadruk op de eerste stappen van het veiligheidsproces, de nadruk op bewustwording en kennisuitwisseling en de geringe aandacht voor implementeren van specifieke veiligheidsmaatregelen.

Herijking: Effectieve aanpak?

- Inzet op institutionalisering is rationele strategie, ook omdat vraagstuk vrij recent op agenda is gekomen
  - veiligheidsproblemen rond ICT te complex en dynamisch om op oplossingen te sturen
  - mobiliseren van kennis en kunde, maar ook *problem sharing*
  - andere partijen mede verantwoordelijk maken door aanspreekpunten te institutionaliseren
  - andere partijen stimuleren tot nemen van veiligheidsmaatregelen

TU Delft

Deze institutionalisering is, zeker in de fase van het beleidsproces, een rationele strategie. ICT is immers dynamisch en complex en daardoor moeilijk te vatten. Er wordt daarom allereerst getracht om de problemen te agenderen bij de juiste partijen en fora te organiseren die tot actie moeten leiden. De overheid probeert de private partijen mede verantwoordelijk te maken door aanspreekpunten te institutionaliseren. Tenslotte probeert de overheid andere partijen te stimuleren tot het nemen van veiligheidsmaatregelen.

Herijking: Effectieve aanpak?

- Maar effectiviteit van samenwerkingsvormen is erg kwetsbaar
- Bereiken *outcomes* is primair in handen van private partijen
- Die delen vaak niet de probleemperceptie van de initiatiefnemende overheidspartij
- Afwijkende probleempercepties worden soms ten onrechte geduid als 'geringe urgentiebeleving' (bv. NICC Programmaplan)
- Partijen kennen uiteenlopende prikkelstructuren en belangen
- Voorgestelde samenwerkingsvormen (informatieverstrekking/netwerkcoördinatie) zijn hier niet op ingericht: overtuiging is niet genoeg
- Er ontbreken governance-arrangementen voor samenwerkingsverbanden die gegeven de uiteenlopende prikkelstructuren tot wenselijke uitkomsten leiden

19

TU Delft

Maar de effectiviteit van samenwerkingsvormen die gebaseerd zijn op netwerkcoördinatie en informatieverstrekking is erg kwetsbaar. Het bereiken van de *outcomes* is namelijk primair in de handen van private partijen. 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.

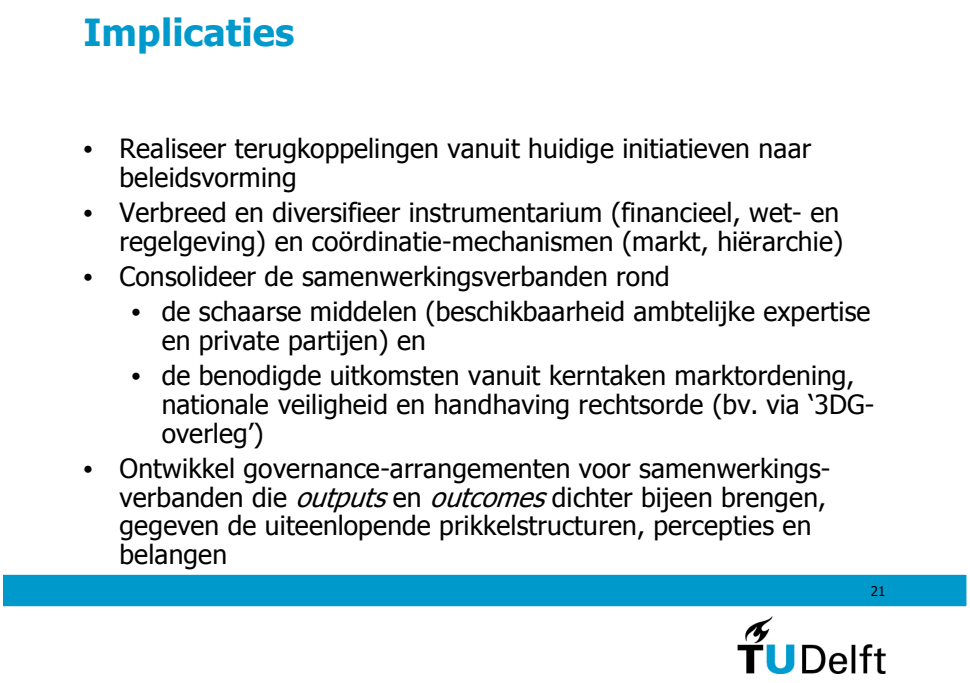
Neem bijvoorbeeld de *2006 CSI/FBI Computer Crime and Security Survey*. Die signaleerde dat bedrijven gemiddeld zo'n 170 duizend dollar schade per jaar hebben door veiligheidsproblemen. Dit klinkt wellicht als een stevige schadepost, maar de maatregelen die nodig zijn om deze problemen te voorkomen zijn 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 informatievoorziening en overtuiging weinig effectief. Daarvoor zijn meer robuuste *governance*-arrangementen nodig, bijvoorbeeld gebaseerd op marktordening en op wet- en regelgeving.

Samenvattend: Herijking van ICT-veiligheidsbeleid

- Naar een "sluitende, efficiënte en effectieve aanpak"
- Sluitende aanpak?
  - rijk en dynamisch beeld van risico's, maar eenzijdigheid in coördinatie-mechanismen en interventie-instrumenten
- Efficiënte aanpak?
  - veel initiatieven, maar ook verwarrende overlap en versnipperde inzet van schaarse middelen
- Effectieve aanpak?
  - doelbereiking is kwetsbaar, want vaak in handen van private partijen en robuust governance-arrangement ontbreekt

TU Delft



Implicaties

We benoemen tot slot kort de implicaties van de voorafgaande analyse. Allereerst is het van belang om terugkoppelingen te realiseren vanuit de huidige initiatieven naar de beleidsvorming. Er is relatieve beleidsschaarste. Veel van de uitvoerende partijen drukken tegen de grenzen aan van het instrumentarium. Zij zouden gebaat zijn bij meer rugdekking vanuit het beleid. Andersom zou het goed zijn als de vele initiatieven die nu rond uitvoeringstaken worden geïnitieerd meer sturing vanuit een samenhangende beleidsvisie zouden krijgen.

Daarnaast lijkt het van cruciaal belang om het instrumentarium te verbreden (met name de inzet van financiële instrumenten en wet- en regelgeving) en de samenwerkingsvormen te diversifiëren. Niet slechts netwerk-coördinatie, maar ook arrangementen die via markt en hiërarchie werken.

Ten derde toont het voorafgaande de noodzaak om de samenwerkingsverbanden te consolideren, langs twee aspecten: a) de schaarse middelen van ambtelijke expertise en deelname van private partijen; b) de verschillende uitkomsten die nodig zijn gegeven dat de ministeries andere kerntaken hebben een eigen positie impliceren ten opzichte van ICT-veiligheidsvraagstukken.

Tot slot, 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.