Netcentrisch toezicht: het toezicht van de toekomst

Falend toezicht is de reden tot vernieuwing waarbij de informatiepositie moet verbeteren. Een netcentrische werkwijze en digitale trends maken dit mogelijk.

Highlights

Het toezicht van de toekomst gaat uit van:

- Digitale dienstverlening en ketenprocessen, ofwel 'digitaal tenzij'.
- Netcentrische (netwerkgerichte) werkprocessen.
- Samenwerking door de overheid met burgers en bedrijven rond een actuele en gedeelde informatiepositie.
- Slim (her)gebruik van het goede bestaande, voorbeelden van innovatie en succesvolle voorzieningen uit verschillende overheidsdomeinen.

Digitale dienstverlening en het toezicht van nu

Hoe kan het dat, na het verlenen van een vergunning, alsnog een raffinaderij ontploft? Of een monstertruck het publiek in rijdt? In de media zijn talloze voorbeelden te vinden van incidenten of evenementen die verkeerd aflopen of toeslagen en uitkeringen die onterecht zijn verleend, terwijl op papier alles in orde lijkt. Dit leidt tot vragen van burgers, politiek en journalisten, zoals:

- Waarom had het bedrijf of persoon deze vergunning?
- Waarom wisten we niet van deze gevaarlijke stoffen in deze hoeveelheden en combinaties?
- Hoe kan het dat dezelfde persoon toeslagen/uitkeringen aanvraagt met verschillende digitale identiteiten?
- Hoe heeft deze persoon of dit bedrijf zolang zijn gang kunnen gaan?
- Is onze privacy wel gewaarborgd?

Dit soort voorbeelden onderstrepen de noodzaak van modernisering van het huidige toezicht van de overheid. Het blijkt niet effectief om als overheid sec te vertrouwen op de juiste aangifte van een burger of op een rapport over de veiligheid van een bedrijf. Als in het administratieve proces alle seinen op groen staan, betekent dat nog niet dat de veiligheid of rechtmatigheid gegarandeerd is. De overheid handelt te vaak op basis van een papieren (of digitale) schijnwerkelijkheid.

We zien een parallel met fraudebestrijding. Er ontstaan steeds geraffineerdere fraudevormen waarbij het voor de toezichthouder administratief lijkt dat elke transactie of gebeurtenis op zichzelf rechtmatig is. Pas bij controles of inspecties achteraf, waarbij meer data worden vergeleken en contra-informatie wordt geraadpleegd, blijkt dat

“Real-time informatie over de locatie, hoeveelheden en samenstelling van stoffen in het geval van een brand in een opslag voor gevaarlijke stoffen is cruciaal voor het aanvalsplan van brandweer en andere hulpdiensten maar ook voor een risicobeoordeling over de risico’s en gevolgen binnen het effectgebied en daarmee voor besluitvorming over mitigerende responsmaatregelen en crisiscommunicatie. Ik herken vanuit mijn huidige rol maar ook als voormalig inspecteur, de trend van toenemende digitalisering van bijvoorbeeld voorraadbeheer, vrachtbrieven en andere begeleidende documenten, maar ook in de modellering van effecten, risicobeoordeling en alarmering. Dit proces is te herkennen door de gehele keten. Het zou ideaal zijn om bij een calamiteit al deze broninformatie bij elkaar te brengen en te koppelen zodat het proces van crisisbesluitvorming sneller kan worden doorlopen. Er zijn ongetwijfeld wetten en overig praktische bezwaren die de uitvoering in de weg staan, maar het zou wat zijn; op het moment van een incident bij op- en overslag of vervoer op weg, spoor, water, buisleidingen en door de lucht direct en digitaal geïnformeerd te worden over de actuele hoeveelheid en samenstelling van gevaarlijke stoffen betrokken bij het incident.”

Peter Westerbeek, Adviseur crisisbeheersing, ministerie van Infrastructuur en Milieu

er sprake was van een samenstel van handelingen (samenspanning) in een keten die tot doel hadden de overheid te benadelen.

In de praktijk zien we dat de controles aan de poort niet effectief genoeg werken. Toenemende digitalisering van overheidsprocessen heeft als voordeel dat besluiten over toekenning snel genomen worden. Het gevolg hiervan is dat het systeem op basis van vooraf gestelde regels de lichten automatisch op groen zet en er geen tussenkomst meer is van ‘het geoefende oog’. Ditzelfde zien we in de veiligheidssector waar aanvragers van een vergunning precies weten wat ze moeten doen om administratieve goedkeuring te krijgen, echter zonder dat de fysieke veiligheid werkelijk is gegarandeerd.

Trends voor het toezicht in het digitale tijdperk

Dit moet en kan anders. We zien drie trends die belangrijk zijn voor het toekomstig toezicht van de overheid

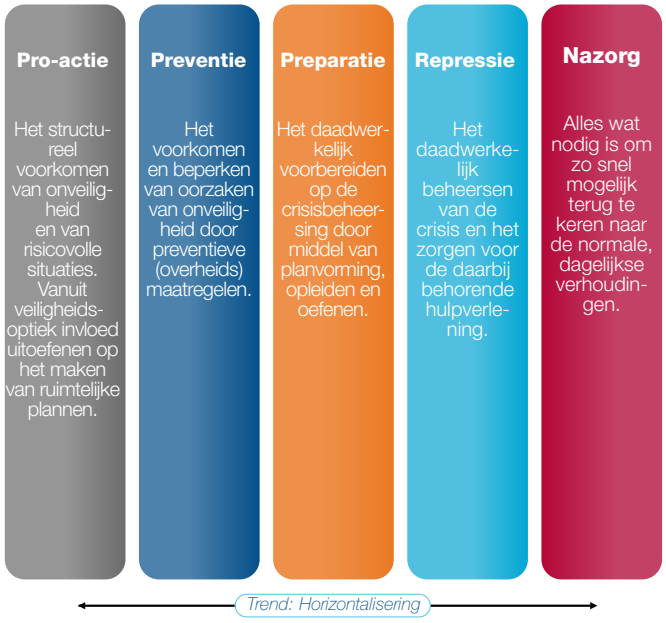
1. Administratieve lastenverlichting en meer doen met minder

Toezichthouders en inspectiediensten werken continu aan de stroomlijning en digitalisering van administratieve verplichtingen. Het uitgangspunt is 'digitaal, tenzij'. Door de trend van digitalisering voelen overheidsinstellingen zich (terecht) gedwongen om enerzijds te blijven voldoen aan de hogere eisen voor dienstverlening in termen van snelheid en anderzijds te blijven voldoen aan eisen van rechtszekerheid.

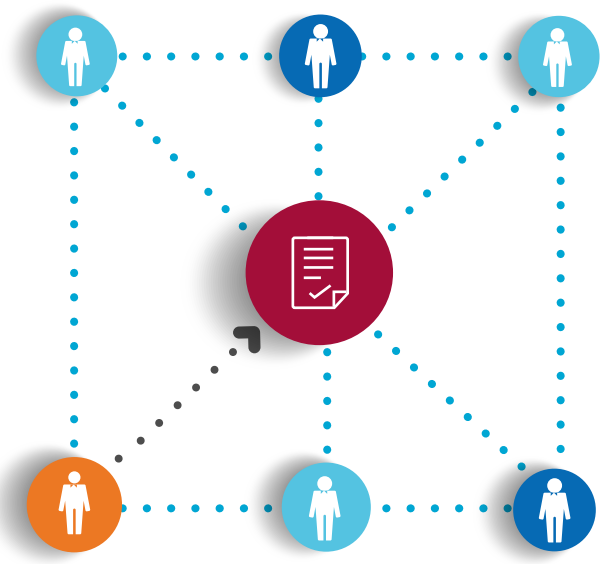
2. Horizontaal toezicht

Het klassieke werkveld van toezicht en handhaving is gericht op de preventieve taken in de veiligheidsketen (zie figuur 1), ofwel het voorkomen dat het mis gaat. De actuele trend is de uitoefening van 'horizontaal toezicht': het toezicht wordt gericht op de effectiviteit en werking van de gehele veiligheidsketen. Daarmee komt het toezicht in dienst te staan van de werking van het gehele netwerk van samenwerkende overheden, burgers en bedrijven. We spreken van netcentrisch werken.

Figuur 2: Horizontalisering



Figuur 1: Netcentrisch werken domein



Werkwijze: Netcentrisch
Houding: Ik deel "alles" met iedereen
Resultaat: Ik weet alles en ik weet het sneller

3. Toenemende behoefte aan actuele en integrale informatiepositie van de overheid

Driekwart van de Nederlanders is ervan overtuigd dat met de toename van informatie de opsporingskansen voor de overheid toenemen op voorwaarde dat 'slim' met Big Data wordt omgegaan (bron: het Capgemini Trends in Veiligheid onderzoek 2015, uitgevoerd door TNS Nipo). Dit uit zich enerzijds in het op orde brengen van de basisinformatie, bijvoorbeeld door middel van de invoering van het stelsel van (basis)registraties. Anderzijds stijgt de behoefte aan actuele en gerichte informatieuitwisseling tussen samenwerkende organisaties.

Een plek waar deze drie trends samenkomen is de veiligheidsketen. Daar wordt de netcentrische werkwijze al succesvol toegepast bij het bestrijden (de repressie) van calamiteiten. Overheden en bedrijven werken daar effectief, snel, betrouwbaar, verantwoordbaar en transparant samen om van een calamiteit weer terug te gaan naar een normale situatie. Dit gebeurt op basis van real-time informatieuitwisseling (via digitale kanalen) op basis van afspraken over informatieverplichtingen die vooraf binnen het netwerk van organisaties zijn gemaakt. De sleutel binnen een netcentrische werkwijze is de samenwerking rondom een actueel gedeeld (informatie) beeld en de directe beschikbaarstelling van relevante informatie voor partners binnen het gedeelde netwerk (zie figuur 2).

Ontwerp van het toezicht van de toekomst

Als deze (netcentrische) werkwijze de veiligheidsketen aantoonbaar effectiever maakt dan is het logisch om te veronderstellen dat dit ook toepasbaar is op processen van handhaving en toezicht.

Voor effectiever toezicht ligt de toegevoegde waarde in het opzetten van geïntegreerd toezicht, geïntegreerde controles en (digitale) samenwerkingsverbanden tussen burgers, bedrijven en overheid. Daarbij horen duidelijke afspraken over onderlinge informatieverplichtingen en -uitwisseling. Er ontstaat zo een samenhangend vangnet om onrechtmatig gedrag of onveilige situaties vroegtijdig te detecteren of zelfs te voorspellen.

Door slimme en geautomatiseerde systemen zijn de lasten voor de aanvragers minimaal. Je hoeft niet meer álle aanvragen te controleren om de onjuiste of frauduleuze eruit te filteren. Bovendien stellen deze systemen, gecombineerd met geavanceerde analyse-technieken, de toezichthouders en handhavers beter in staat om op basis van een integraal inzicht en actuele informatie beslissingen te nemen. De overheid is beter in staat om bij afwijkingen op basis van de juiste informatie in te grijpen. Toezicht staat in dienst van het totale netwerk. We spreken dan van netwerkgericht ofwel netcentrisch toezicht.

Ter illustratie van het positieve effect op de totale keten, zie de casus (kader) die de impact van netcentrisch werken op het toezicht van de overheid op een BRZO-bedrijf illustreert. Het gaat hierbij om bedrijven die werken met grote hoeveelheden gevaarlijke stoffen en/of deze in opslag hebben. Deze bedrijven vallen onder de werking van het Besluit risico's zware ongevallen (BRZO).

Casus: horizontaler toezicht op een BRZO-bedrijf

Incidentbestrijding bij BRZO-bedrijven werkt op basis van papieren bestrijdingsplannen en het ter beschikking stellen van informatie aan bijvoorbeeld de veiligheidsregio via een cd-rom in een brievenbus. Deze manier van werken voldoet niet meer in het licht van netcentrisch toezicht. De brandweer om hulp vragen als het misgaat, zonder bekende actuele informatie mee te geven, kan dan ook niet meer, want dat wordt gedetecteerd als non-compliancy. Het gevolg van houding en gedrag (we delen 'alles' met iedereen) is dat als vanzelfsprekend de informatiesystemen van bedrijf en overheid slim en beveiligd gekoppeld worden, zodat informatie kan stromen als het misgaat, of dreigt mis te gaan. Telefoontjes naar diverse meldkamers met summiere informatieoverdracht behoren tot het verleden, deze zijn vervangen door digitale meldingen. Deze meldingen zijn dan rijkelijk voorzien van zowel de voorgeschiedenis als de actuele informatie (welke stof zat in welke hoeveelheid en combinaties op tijdstip x in welke installatie, leiding etc.). Als het dan toch misgaat, zijn de hulpverleningsdiensten en overheden in staat veiliger en effectiever op te treden. Zij nemen bijvoorbeeld niet onnodig zware maatregelen omdat ze geen actueel of een onvolledig situationeel beeld hebben, zoals het langdurig stilleggen van bedrijf, verkeer, luchtruim of een gehele binnenstad. Maatregelen die ineffectief en schadelijk zijn voor het betrokken BRZO-bedrijf en de lokale economie.

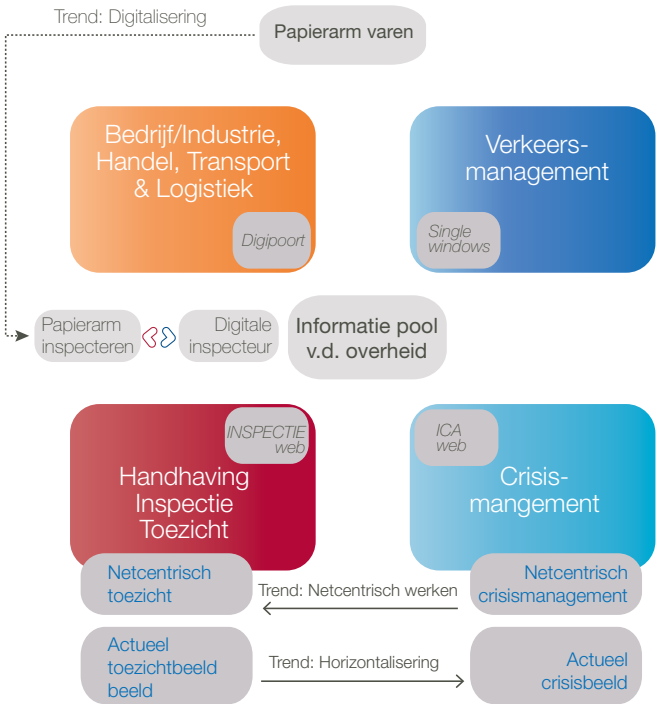
Bouwstenen voor het toezicht van de toekomst

Er zijn vele technologieën en concepten die elders al succesvol zijn toegepast en in onze ogen bouwstenen vormen waarmee het toezicht van de toekomst kan worden gerealiseerd. Voorbeelden zijn de digitale ambtenaar (inspecteur) die werkzaam is binnen de toeslagen- en studiefinancieringprocessen, de overheidstransactiepoort (digipoort), diverse single windows (binnenvaart, maritiem, handel&transport), multimodaliteit, gebeurtenisgedreven ketens en digitale netwerkanalyse ten behoeve van vroegtijdige fraudedetectie. Zie ook figuur 3 waarbij wij zowel enige trends als te 'transporteren' oplossingen hebben gevisualiseerd.

Enkele voorbeelden worden hieronder toegelicht vanwege de hoge mate van toepasbaarheid:

- Het concept 'Papierarm Varen' voor het digitaal delen van informatie op basis van het douaneproces. In dit project is naar voren is gekomen dat naast douane en inspectiediensten ook de veiligheidsregio de benodigde informatie met de papiervervangende hulpmiddelen sneller beschikbaar heeft zelfs zonder het schip te betreden. 'Papierarm inspecteren' waarbij routinematig werk wordt gedaan door een digitale inspecteur zien wij dan ook als waardevolle toevoegingen aan het inspectiedomein.

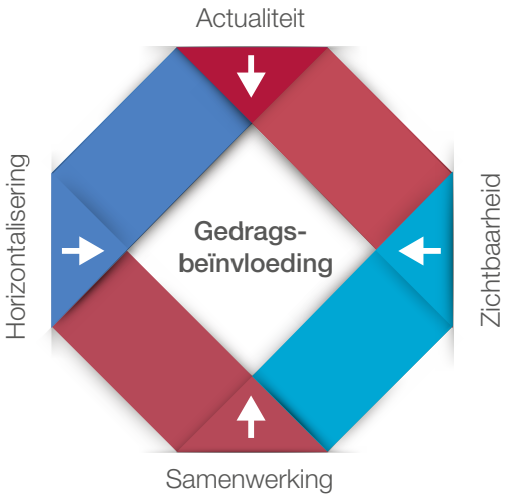
Figuur 3: Voorbeelden van toepasbare trends en oplossingen 'getransporteerd' naar het HI&T-domein.



- Een ander voorbeeld van een toepasbaar concept is de crisismanagementoplossing ICAWEB. Het ICAWEB laat meer dan 30 overheidsdiensten op een netcentrische basis samenwerken tijdens een calamiteit of crisis. Een variant van deze voorziening kan bijvoorbeeld de Douane versneld netcentrisch laten samenwerken rond een 'gedeeld toezichtbeeld' met organisaties uit het domein Handel en Transport.

Er komen met kansen ook bedreigingen mee in het toezicht van de toekomst: een hogere kans op (digitale) fraude en fouten maar ook op een mogelijke onbalans tussen dienstverlening en handhaving. Er zijn echter moderne methoden en technieken beschikbaar om niet-naleving (fraude en fouten) vroegtijdig te detecteren zonder dat de goedwillende ondernemer, belastingbetaler of anderszins daaronder lijdt. Voor fraudebestrijding zijn oplossingen beschikbaar die in staat zijn om netwerken en patronen in kaart te brengen en te monitoren. Daarbij worden transacties tussen (rechts)personen en bedrijven niet meer afzonderlijk, maar in samenhang bekeken. Dit stelt de toezichthouder in staat om op basis van zijn actuele en integrale informatiepositie vroegtijdig onrechtmatigheden te detecteren, te onderzoeken of direct in te grijpen.

Figuur 4: Factoren die bijdragen aan gedragsbeïnvloeding ten bate van netcentrisch toezicht.



Conclusie

Het is een illusie te denken dat - met enkel het naleven van de regelgeving - er niet meer gefraudeerd wordt of dat er nooit meer een raffinaderij ontploft. Om dergelijke incidenten of fraudevormen vroegtijdig te detecteren en het veiligheidsbewustzijn te verhogen, moet per inspectiedomein worden bepaald of en wanneer het netcentrisch toezicht toegepast kan worden. Om de veranderingen in werkwijze te bewerkstelligen, zal de toezichthouder zich continu bewust moeten zijn van houding en gedrag (zie figuur 4) van alle spelers in het netwerk en hoe dit positief te beïnvloeden.

Over de auteurs

Drs. Evert Voorn is organisatieadviseur voor overheden en hij is Capgemini's wereldwijde expert op het gebied van compliance-vraagstukken van uitvoeringsorganisaties in het werk- en inkomensdomein. Drs. ing. Erik van den Berg en drs. Stijn de Keijzer zijn de wereldwijde experts van Capgemini als het gaat om het ontwikkelen en implementeren van netcentrische informatiesystemen in het crisismanagementdomein.

Voor meer informatie kunt u contact met de auteurs opnemen via
evert.voorn@capgemini.com
erik.e.vandenberg@capgemini.com
stijn.de.keijzer@capgemini.com