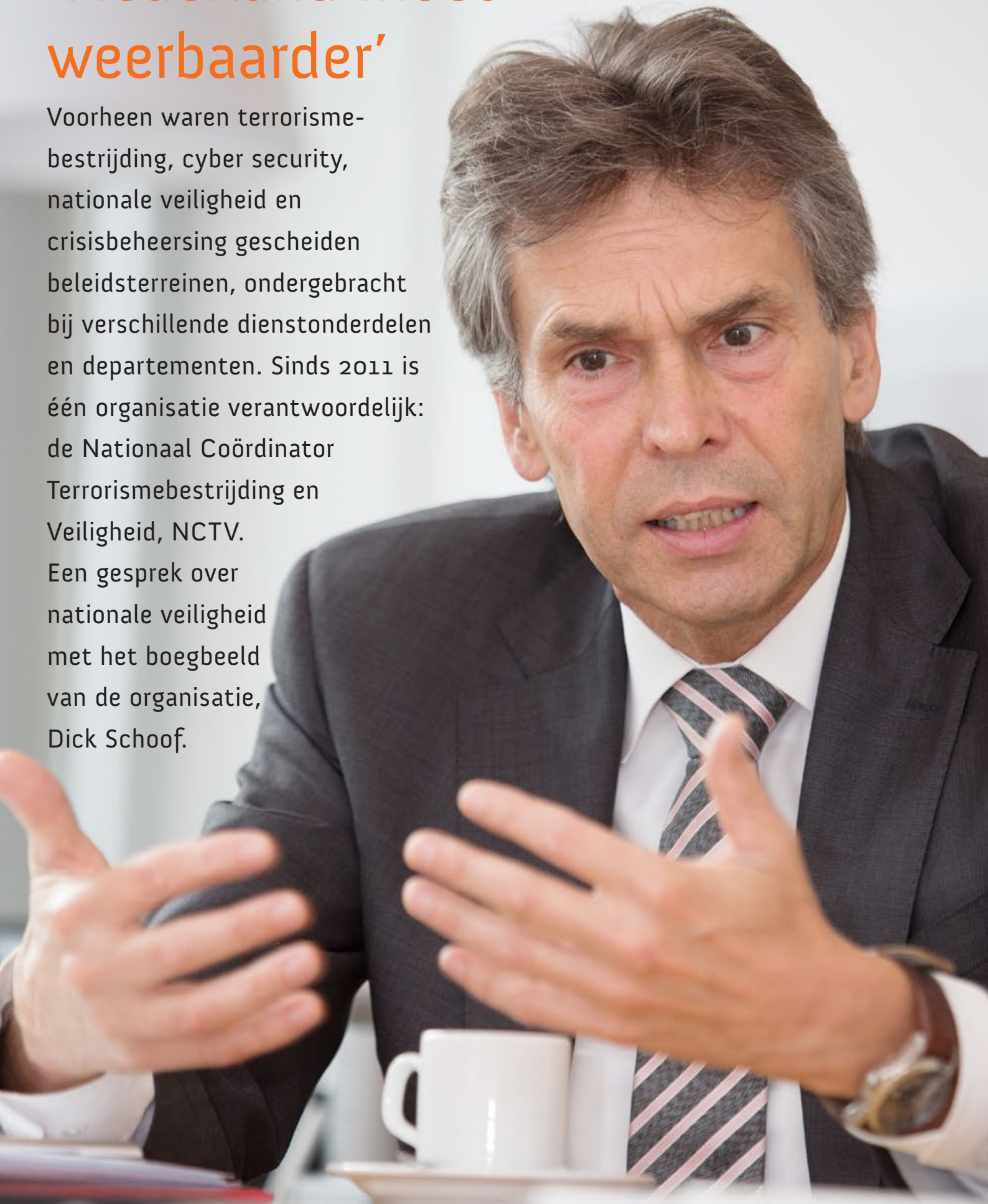
Dick Schoof, Nationaal Coördinator Terrorismebestrijding en Veiligheid:

‘Nederland moet weerbaarder’

Voorheen waren terrorisme-bestrijding, cyber security, nationale veiligheid en crisisbeheersing gescheiden beleidsterreinen, ondergebracht bij verschillende dienstonderdelen en departementen. Sinds 2011 is één organisatie verantwoordelijk: de Nationaal Coördinator Terrorismebestrijding en Veiligheid, NCTV. Een gesprek over nationale veiligheid met het boegbeeld van de organisatie, Dick Schoof.



De NCTV – onderdeel van het ministerie van Veiligheid en Justitie – is een samenvoeging van de voormalige directie Nationale Veiligheid, de NCTb en GovCERT. De organisatie kent ongeveer 260 medewerkers en bestaat, naast de Nationaal Coördinator Terrorismebestrijding en Veiligheid, uit vijf beleidsdirecties, het Nationaal CrisisCentrum en het Landelijk Operationeel Coördinatie Centrum.

'Samen met onze partners uit het veiligheidsdomein – overheden, semipublieke en private organisaties – maken we ons sterk voor een veilig en stabiel Nederland. De focus ligt op het voorkomen en beperken van maatschappelijke ontwrichting', aldus Dick Schoof, die de functie van Nationaal Coördinator Terrorismebestrijding en Veiligheid sinds 1 maart jl. vervult. 'De NCTV beschermt Nederland tegen bedreigingen die de maatschappij kunnen ontwrichten. Samen met de andere stakeholders zorgen we ervoor dat de Nederlandse vitale infrastructuur veilig is én blijft. Want zonder elektriciteit, drinkwater of voedsel kan onze samenleving niet meer veilig functioneren.'

De NCTV is er voor het identificeren en verminderen van dreigingen, voor een optimale cyber security en voor het bewaken en beveiligen van personen, objecten en de burgerluchtvaart. Ook versterkt de NCTV de weerbaarheid tegen dreigingen. En als het dan toch mis mocht gaan, dan is de NCTV verantwoordelijk voor optimale crisisbeheersing en crisiscommunicatie.

Schoof: 'Wij richten onze aandacht ruwweg op drie onderwerpen: contraterrorisme, cyber security, en rampen en crisisbeheersing. Wij zijn een relatief kleine netwerkorganisatie, die vooral streeft naar samenwerking met publieke en private partners. Vanuit onze centrale coördinerende positie verbinden we de drie domeinen met elkaar, binnen de driehoek van dreiging, weerbaarheidsverhoging en belangenbescherming.'

U legt sterke nadruk op samenwerking met de private sector; waarom is dat zo belangrijk?

Schoof: 'Twee redenen. Ten eerste is een groot deel van de vitale sectoren – water, gas, elektriciteit en telecom – privaat. Ten tweede: de bedrijven hebben een eigen verantwoordelijkheid om hun bedrijfsvoering te beveiligen. Wij willen daar als overheid bij helpen, maar ook inzicht hebben in de manier waarop bedrijven die verantwoordelijkheid nemen en invullen. Niet voor niets hebben we een tweekoppige leiding van onze Cyber Security Board: de CEO van KPN, Eelco Blok, is covoorzitter, om zo op het gebied van cyber security een goede aansluiting met de private sector te garanderen.'

Nationaal Cyber Security Centrum

Volgens de NCTV is één van de grootste uitdagingen de komende jaren het bewaken van de nationale digitale veiligheid. *Dat klinkt nogal breed; hoe gaat u dat aanpakken?*

Schoof: 'Onze samenleving en economie zijn kwetsbaar door de toenemende afhankelijkheid van ICT. Nederland is 'hyper-connectief' en wereldwijd koploper op het gebied van digitalisering en internetgebruik. Cybercriminaliteit en digitale spionage zijn dan ook grote bedreigingen voor overheid en bedrijfsleven, niet alleen vanuit criminele netwerken, maar steeds vaker ook vanuit landen. Dat betekent dat we twee dingen moeten doen: aan de voorkant zorgen dat we weerbaarder worden en aan de achterkant zorgen dat we adequaat kunnen reageren, mocht er iets misgaan. Dat is wat wij hebben samengebracht in het Nationaal Cyber Security Centrum.'

Het Nationaal Cyber Security Centrum (NCSC) vormt de verbindende schakel in de zorg voor digitale veiligheid. Het NCSC brengt kennis en expertise bij elkaar, helpt bij dreigingen en incidenten en is de spil in de operationele coördinatie bij een grote ICT-crisis. Het NCSC werkt hierbij nauw samen met vele andere nationale én internationale partijen uit de cyber security community. Het NCSC geeft de ingebrachte kennis en informatie terug in de vorm van inzichten en handelingsperspectieven.

Nationaal Detectie en Response Netwerk

De afgelopen jaren is gebleken dat Nederland kwetsbaar is voor rampen, aanslagen en andere incidenten. Denk aan de hack bij DigiNotar, en de recente DDoS-aanvallen op de banken. Het blijft belangrijk om altijd alert te zijn op nieuwe dreigingen en om klaar te staan als het onverhoopt misgaat. Mede in dat kader wordt nu een Nationaal Detectie en Response Netwerk opgebouwd, binnen het NCSC. *Wat gaat dat inhouden en welke rol ziet u daarin voor de vitale sectoren, zoals de drinkwatervoorziening?*

Schoof: 'In onze Cyber Security Board is het idee ontstaan voor een Nationaal Detectie en Response Netwerk, om aan de voorkant van de problemen te komen. Een veiligheidsprobleem op het internet willen we vroegtijdig signaleren en melden aan de relevante betrokken partijen. Zij kunnen dan hun maatregelen nemen. Daar hoort bij dat private en publieke partijen, die te maken krijgen met security breaches, dat ook onmiddellijk aan het NCSC en elkaar doorgeven. In de praktijk merken we dat partijen daar soms terughoudend in zijn, vanwege privacy of om commerciële redenen. We proberen alle partners ervan te overtuigen dat ze informatie echt moeten delen. Transparantie is niet eng, integendeel: onderzoek toont keer op keer aan dat de burger heel goed kan omgaan met de waarheid, als je maar handelingsperspectieven aangeeft en uitlegt wat je als overheid of als bedrijf doet om problemen aan te pakken. Kwetsbaarheden communiceren kan dus best, als je het maar goed insteekt.'

Wat verwacht u van de drinkwatersector op het gebied van cyber security en wat mag de sector van de overheid verwachten?

Schoof: 'Ik verwacht dat de drinkwaterbedrijven zich op boardroom-niveau realiseren welke risico's de toegenomen digitalisering met zich meebrengt. Het is van essentieel belang dat ze adequate risicoanalyses uitvoeren en beschikken over reele beveiligingsplannen, omdat ook kleine digitale verstoringen er uiteindelijk voor zouden kunnen zorgen dat er geen drinkwater meer uit de kraan komt. Veiligheid moet een integraal onderdeel vormen van de bedrijfsstrategie.'

'In dat kader is een initiatief zoals de regelmatige SCADA-benchmarks van de drinkwaterbedrijven al een goede stap. Ik ben sowieso een voorstander van peer reviews en zelfregulering; het is niet altijd nodig dat wij als overheid overal regels voor opstellen. Andersom mag de sector van de overheid verwachten dat wij ons uiterste best doen om het nationale belang – en daarmee de vitale sectoren – te beschermen.'

Wettelijke meldplicht security breaches

In reactie op de DigiNotar-affaire heeft de Tweede Kamer gevraagd om een wettelijke meldplicht security breaches. Deze gaat ook gelden voor de drinkwatersector. *Bent u niet bang dat dit leidt tot een hoop administratieve lasten bij het NCSC én de vitale sectoren?*

Schoof: ‘De NCTV is niet geïnteresseerd in élke security breach, maar wel wanneer een incident maatschappelijk ontwrichtend kan werken. Dat onderscheid is trouwens moeilijk te maken: iets kan klein beginnen, maar uitmonden in een majeure crisis. Het wetsontwerp voor de meldplicht gaat een dezer weken ter consultatie. We zijn al in gesprek met de sectoren en ook bij de verdere uitwerking zullen we hen uiteraard betrekken. Maar ik benadruk nogmaals: er zijn reële dreigingen en het kan zomaar zijn dat een beetje administratieve lastendruk een heel redelijke prijs is voor de extra veiligheid die dat oplevert.’

‘De recente DDoS-aanvallen op de banken geven aan wat de risico’s zijn, daar kan niemand de ogen voor sluiten. Zeker als je beseft dat de bankensector van oudsher vooroploopt op het gebied van digitale beveiliging. Daarnaast hebben deze aanvallen duidelijk gemaakt dat er bijeffecten kunnen optreden in sectoren die niet primair worden aangevallen. Internet is één geheel, en je zult maatregelen dus met z’n allen moeten nemen. Ook hier geldt: de keten is zo sterk als de zwakste schakel.’

Cyber security en security breaches

Bij cyber security gaat het om de bescherming van het functioneren van ICT en van informatie. Wanneer ICT niet naar behoren functioneert, of de vertrouwelijkheid en integriteit van informatie in het geding zijn, kunnen belangen in onze samenleving worden geschaad.

Een security breach is een ‘inbreuk op de veiligheid of een verlies van integriteit van informatiesystemen, waardoor de beschikbaarheid of betrouwbaarheid van een product of dienst in belangrijke mate wordt of kan worden onderbroken.’

Veiligheidsregio’s

Eind mei heeft de Inspectie Veiligheid en Justitie de Staat van de Rampenbestrijding 2013 uitgebracht. Eén van de aanbevelingen is dat er meer overkoepelende en actieve sturing moet komen op de Veiligheidsregio’s met betrekking tot samenwerkingsafspraken met vitale partners. *Onderschrijft u dit en bij wie zou die sturing volgens u moeten liggen?*

Schoof: ‘Vooropgesteld, de Staat van de Rampenbestrijding onderschrijven wij volledig. Er is veel bestuurlijke discussie rondom de Veiligheidsregio’s, maar laat dat niemand weerhouden van de harde conclusie dat het beter moet en kan. Eén van de doelstellingen die de NCTV aan de Veiligheidsregio’s heeft meegegeven, is: ‘Zorg dat je met de vitale sectoren goede samenwerkingsafspraken maakt, zowel individueel als gezamenlijk. Als de Veiligheidsregio’s adequaat willen kunnen reageren op diverse typen rampen en crises, heb je een goede samenwerking met de vitale sectoren nodig, zowel een-op-een, als breder: regionaal of zelfs nationaal. Veel van de partijen uit de vitale sector opereren nu eenmaal nationaal en kunnen bezwaarlijk met 25 Veiligheidsregio’s separate afspraken maken. In die zin kan het dus geen kwaad dat er een meer overkoepelende en actieve sturing komt, maar dat is een zaak van de Veiligheidsregio’s zelf. Wij zouden daar wel een intermediaire rol in kunnen spelen. Overigens zullen er ook altijd enkele specifieke afspraken tussen afzonderlijke partijen nodig zijn, door de regionale verschillen in risico’s en dreigingen.’

Uitbreiding ATb

De drinkwatersector is sinds 2005 aangesloten op het ATb, het Alerteringssysteem Terrorismebestrijding. De NCTV is voornemens om het ATb uit te breiden naar nationale veiligheid. *Wat houdt dit in en wat zou dit voor de drinkwatersector betekenen?*

Schoof: ‘Het idee voor uitbreiding van het ATb is een logisch gevolg van de verbreding van ons werkveld: niet alleen meer terrorisme, maar ook andere dreigingen. We hebben nog geen concrete plannen, maar willen bij de vitale sectoren peilen of zij behoefte hebben aan uitbreiding van alertering bij andere dreigingen. We zouden bijvoorbeeld eenzelfde waarschuwingsmodel als bij het ATb kunnen hanteren bij cyberaanvallen of rampen zoals overstromingen of grote branden. Wordt vervolgd dus.’

Update Cybersecuritybeeld

Begin juli publiceerde het NCSC het jaarlijkse Cybersecuritybeeld Nederland. Topics dit jaar zijn:
- digitale spionage;
- criminele activiteiten op internet door het overnemen van netwerken;
- ontwikkeling van criminele industrie rondom internetcriminaliteit.

‘Concluderend kunnen we stellen dat
a) de afhankelijkheid van ICT voor individuen, organisaties, ketens en de maatschappij is gegroeid;
b) een aantal dreigingen is toegenomen en uitgaat van vooral staten en beroepscriminelen tegen overwegend overheden en private organisaties;
c) de weerbaarheid ongeveer gelijk is gebleven, omdat er meer initiatieven en maatregelen worden genomen die niet altijd gelijke tred houden met de kwetsbaarheden, en basismaatregelen niet altijd zijn getroffen.’

Meer informatie: www.ncsc.nl/actueel