Management van vernetwerkte risico's

Naar een agenda voor de auditor

Rotterdam, december 2013

Mark van Twist
Ernst ten Heuvelhof
Martijn van der Steen

ESAA Erasmus School of Accounting & Assurance

Management van vernetwerkte risico's

Naar een agenda voor de auditor

Rotterdam, december 2013

Mark van Twist
Ernst ten Heuvelhof
Martijn van der Steen

ESAA Erasmus School of Accounting & Assurance

Inhoudsopgave

1 Inleiding

1.1 Achtergrond

De soliditeit van landen, de continuïteit van organisaties en het succes van projecten mogen op het eerste gezicht weinig of niets met elkaar van doen hebben, bij nader inzien zijn er wel degelijk overeenkomsten. Eén is dat er bij alle drie risico's in het geding zijn: ze hebben allemaal te kampen met risico's die zo dominant zijn, dat veel aandacht uitgaat naar het managen ervan. Risico's kunnen de soliditeit van landen aantasten, de continuïteit van organisaties bedreigen en het succes van projecten in de weg staan. Risicomanagement is daarom van belang en krijgt inmiddels vanzelfsprekend de aandacht die het verdient.

Risicomanagement is op de golven van aandacht voor beeldbepalende incidenten en affaires een steeds belangrijker professie binnen organisaties geworden, uitgevoerd door een speciaal daarvoor opgeleide beroepsgroep, de risicomanagers. Nog nooit was er zoveel aandacht voor als in de afgelopen twintig jaar.[1] Het behoort volgens commissarissen en bestuursvoorzitters tot de top drie van belangrijke onderwerpen bij het vorm geven aan de governance van organisaties.[2] Risicomanagers zijn professionals, met de daarbij horende professionele codes, instrumenten, certificering en een door onderling debat aangroeiende professionele standaard. Hun adviezen zijn van cruciaal belang en hebben op de allerhoogste niveaus *impact*. Hun manier van werken is onderworpen aan hoge standaarden. **Organisaties erkennen alom het belang van het adequaat omgaan met risico's en het belang van risicomanagement als kernproces in de organisatie. Het goed omgaan met risico's kan de organisatie niet *maken*, maar voorkomt wel het *breken* er van.**

Vanuit het belang voor de continuïteit voor de organisatie is risicomanagement ook steeds meer een onderwerp van internal auditing geworden. Om de kwaliteit van het risicomanagement te borgen en te vergroten voeren organisaties interne audits uit. Dat is ook nodig, want de aandacht voor risicomanagement vertaalt zich niet vanzelf naar een adequate invulling ervan in organisaties. Niet zelden worden rapportages over risicomanagement als nietszeggend ervaren. Bovendien is er de klacht dat veel vragen onbeantwoord blijven en dat rapportages wel veel tekst bevatten maar eigenlijk nogal nietszeggend zijn, ook al omdat ze zich vaak concentreren op de bekende kansen op fouten: op de operationele risico's in bedrijfsprocessen, op de naleving van regels en financiële parameters die ook nogal voorspelbaar zijn. Dat terwijl de reputatierisico's die voor de governance van een organisatie vaak minstens zo belangrijk zijn en te maken hebben met onzekerheden die de grenzen van de eigen organisatie overstijgen buiten beeld bleven en toekomstige ontwikkelingen al helemaal onbenoemd blijven. Risicomanagementsystemen blijven vaak nog teveel gericht op operationele problemen terwijl bij de leiding van de organisatie, en bij bestuurders en toezichthouders juist behoefte bestaat aan strategische risicoinformatie die niet terugkijkt maar toekomstgericht is en die zich niet slechts

[1] In lijn met COSO verstaan wij hier onder risicomanagement: een continu beheersproces dat erop gericht is mogelijke gebeurtenissen te inventariseren die van invloed kunnen zijn op de onderneming en probeet de nadelige effecten ervan te beheersen.
[2] F. van Eenenaam (2006), Dynamics of Strategy, The Games of Competitiveness and Corporate Governance.

richt op interne beheersmaatregelen maar juist ook op de veelheid aan ontwikkelingen op het grensvlak tussen organisatie en omgeving.[3]

De auditing van het risicomanagement is in het algemeen belegd op het niveau van de organisatie. Daarbij wordt gekeken naar de risico's die in beeld zijn en naar de beheersmaatregelen die daartoe zijn ingezet. Voor veel organisaties geldt dat die processen relatief goed op orde zijn. Veel risico's zijn in beeld en de belangrijkste incidenten die kunnen voorvallen zijn doordacht. De organisatie heeft geleerd hiermee te leven en maatregelen te treffen om de risico's te beheersen, zowel preventief als in het omgaan met eventuele calamiteiten. Denk hierbij aan risico's als een planning die niet gehaald wordt, een reorganisatie die uit de begroting loopt, een ambitie die weerstand wekt bij andere partijen, of een calamiteit die zich rond het productieproces voordoet. Deze voorbeelden zijn voor elke organisatie herkenbaar en komen overal – zij het in andere gedaante – voor. Het zijn voorbeelden van 'gewone' risico's: risico's die ons op het netvlies staan, vaak omdat we ze heel concreet eerder al eens hebben meegemaakt.

Naast 'gewone' risico's zijn er echter ook andere risico's: de buitencategorie, de risico's waar vooraf niet aan is gedacht, eenvoudig omdat ze (tot het moment dat ze zich manifesteren) zo ongeveer ondenkbaar worden geacht. Ze zijn het resultaat van een vooraf onwaarschijnlijk geachte, onvoorstelbare samenloop van omstandigheden. Denk aan de val van Oost-Europese regimes, de Arabische lente, BSE et cetera. Het zijn de risico's die er wel zijn, ook al kunnen we ze nog amper bedenken. Niet omdat ze zo extreem moeilijk te verzinnen zijn, maar "gewoon" omdat we de historische referentie missen om te voorzien wat achteraf vaak zo logisch lijkt. Zo lopen organisaties – net als individuen – gevaar vanuit de risico's die ze zien, maar ook – en misschien wel meer – vanuit de risico's die ze niet voorzien, niet verwachten en waar ze niet op anticiperen. Belangrijk daarbij is dat deze bijzondere en niet voorstelbare risico's eigenlijk heel alledaags zijn. Het gaat niet om extreme natuurrampen of een aanval van buitenaardse wezens, maar om iets veel eenvoudigers: **de samenloop van omstandigheden, waarin op zichzelf overzichtelijke risico's of gebeurtenissen interacteren met andere risico's of ontwikkelingen – en vervolgens samen leiden tot nieuwe, grotere, andere en onvoorziene risico's.** Het risico dat we niet voorzien komt niet zozeer voort uit nieuwe spelers of nooit vertoonde gebeurtenissen, maar uit het intensieve samenspel van op zich heel gewone, bekende en nu al alom aanwezige factoren. Deze categorie risico's manifesteert zich overal waar gewone risico's samenlopen, zich met elkaar vervlechten en elkaar versterken. En dat gebeurt op steeds meer plekken, zo is onze stelling in dit essay. Dat vraagt om aandacht voor deze categorie risico's, doe wij hier aanduiden als **vernetwerkte risico's**. Dit essay handelt over deze categorie risico's. Wij bespreken vernetwerkte risico's en vragen ons af wat hun betekenis is voor individuele organisaties die er (al dan niet) mee geconfronteerd worden.

1.2 Zwarte zwanen

Een risico laat zich kort maar krachtig via de volgende formule weergeven: *risico = kans maal effect*. Hoe groter de kans, hoe groter het risico. En ook: hoe groter het effect, hoe groter het risico. Risico's hebben vaak een negatieve connotatie, maar dat is vanuit de gepresenteerde formule niet vanzelf terecht. Effecten kunnen positief zijn en dan is het risico dus ook positief. Niet voor niets zeggen we wel dat ondernemen een kwestie is van kansen benutten, en dus ook van risico nemen. Maar dit is

[3] Zie Publieke Managementletter van de NBA: Risico's managen is mensenwerk, risocomanagement en –verslaggeving bij grote ondernemingen, november 2013.

niet de gebruikelijke betekenisgeving in het dagelijks spraakgebruik. In het gesprek over risico's gaat het doorgaans om de kans op een *negatief* effect: schade, last of verlies. Dat effect kan financieel zijn ('geld verliezen'), maar ook fysiek ('geblesseerd raken') of sociaal ('verlies van reputatie en status').

Er zijn maar weinig risico's waarvan de effecten voor iedereen negatief zijn. Integendeel, vaak is het hetzelfde risico voor de één positief, maar voor de ander negatief. Of het is niet voor iedereen even negatief, bijvoorbeeld omdat in het geval van een faillissement de één een meer achtergestelde positie heeft dan de ander. De kans is dan voor iedereen even groot, maar het effect is anders. En daarmee is het totale risico ook verschillend. De waardering van risico's hangt ook af van het niveau waarop de waardering plaatsvindt. Zo kan oud worden voor mensen een zegen zijn, zeker als dat in betrekkelijk gezonde toestand gebeurt. Maar een pensioenfonds kwalificeert het feit dat mensen gemiddeld ouder worden als een risico dat beheersing behoeft.

Risico als kans maal effect is een rekensom, en niet meer dan dat. Het is niet tastbaar en ook niet zichtbaar. **Risico is een abstractie, een constructie. Dat neemt niet weg dat we er ondertussen heel concrete berekeningen over kunnen maken, met harde consequenties. Risico's zijn in het dagelijks leven misschien niet meteen zichtbaar, ze zijn zeker niet slechts 'bedacht'.** Het zijn geen bedenksels van verzekeringsagenten die producten willen verkopen, maar eerder pogingen om tastbaar en zichtbaar – en ook verhandelbaar – te maken wat nog niet gebeurd is en wat mogelijk ook helemaal niet zal gebeuren, maar wel kan gebeuren. Verzekeringsmaatschappijen berekenen brandrisico's en de harde conclusie is een premie die moet worden betaald en voorwaarden die voor de verzekerde in geval van brand vervelend kunnen uitpakken. De verzekering maakt een inschatting van de kans op brand, op het negatieve effect ervan (schade en kosten), en biedt in ruil daarvoor een betaalde voorziening. Niets meer en niets minder.

Met het voorbeeld van de brandverzekering komen wij bij een cruciaal element van het denken over risico's. **Risico's gaan om kansen, om dingen die niet gebeurd zijn en waarvan inherent onzeker is of ze zich ooit ook echt zullen manifesteren.** Die cirkel wordt pas rond op het moment dat de potentiële gebeurtenis werkelijkheid wordt: als het risico uitmondt in een incident. Een risico van arbeidsongeschiktheid kan zich materialiseren in échte arbeidsongeschiktheid. Het risico op zich is geen schade, het is de materialisatie ervan die schade veroorzaakt. Zo onzichtbaar als het risico is, zo zichtbaar, tastbaar en voelbaar is het incident dat hieruit kan voortvloeien. Risico wordt via een incident ook echt in een concrete schade omgezet. De kans is dan werkelijkheid geworden en er is schade die kan worden vastgesteld. Wat eerst een potentieel probleem was, is er nu ook echt.

Risico-inschattingen gaan over de toekomst, maar ze worden in de regel gebaseerd op ervaringsgegevens. Op incidenten die zich werkelijk hebben voltrokken, zoals ook de levensverwachting van mensen een ingewikkelde cocktail is van extrapolaties van historische gegevens. De kans op brand in huis of van arbeidsongeschikt worden en de schade daarvan wordt gebaseerd op eerdere ervaringen in het verleden. Zo krijgt het risico vorm door een analyse van het verleden. **Het inschatten van risico's is een vorm van vooruitzien, maar gebeurt in de regel door middel van scherp achteruitkijken.**

Dat geeft onze inschatting van risico's een bijzondere dimensie: de inschatting wordt ingeperkt door eerdere ervaringen uit het verleden en ons voorstellingsvermogen als het gaat om de toekomst. Sommige risico's worden voor onwaarschijnlijk of zelfs onmogelijk gehouden. De kans dat een gebeurtenis zich voordoet wordt op nihil geschat – het berekenen van een kans impliceert al

een concrete gedachte over iets dat zou kunnen gebeuren. Terugkijkend blijken evenwel sommige van deze voor onmogelijk gehouden risico's toch in een incident uit te monden en werkelijkheid te worden. Dat soort 'onmogelijke risico's' is uitgebreid beschreven en geanalyseerd door Taleb. Taleb noemt risico's die voor onmogelijk worden gehouden '*black swans'.*[4]

> Tot het eind van de 17e eeuw was een '*black swan'* een staande uitdrukking. Iemand die een fenomeen typeerde als een *black swan* gaf daarmee te kennen dat het fenomeen niet bestond. Een *black swan* was een onmogelijke gebeurtenis. Totdat in 1697 in Australië een *black swan* werd waargenomen. Daarna is de betekenis van het concept *black swan* veranderd. Vanaf die tijd wordt een fenomeen dat onmogelijk zou zijn, maar tot ieders verrassing toch blijkt te bestaan aangeduid als een *black swan.*

De essentie van een *black swan* is dat het een fenomeen betreft dat op zich bekend is maar tegelijk als 'niet mogelijk' werd verondersteld. Een zwaan die zwart is, een witte tijger, het breken van een bepaald record. Of het instorten van het financiële systeem: dat leek niet mogelijk, maar bleek dat bij nader inzien wel. Volgens Taleb staan *black swans* aan de basis van bijna alle grote veranderingen in de wereld. Onze wereld wordt pas echt op zijn kop gezet door incidenten die *niet* in onze modellen en verwachtingen waren opgenomen. Met alle systemen en mechanismen om de risico's die we kennen af te dekken zijn het uiteindelijk de niet gedachte incidenten die zorgen voor de échte grote veranderingen. **We worden het meest geraakt door datgene dat we niet bedenken en waarvoor we dus ook geen risico-inschatting hebben gemaakt. Laat staan dat we een voorziening voor getroffen hebben.**

Of deze claim nu wel of niet stand houdt, het is duidelijk dat *black swans* een grote impact hebben op onze wereld. Ze komen niet dagelijks voor, maar als ze er zijn dan zijn ze een aankondiging van iets groots en ingrijpends, dat diep doordringt in al onze systemen en zekerheden. De *black swans* zijn ook niet zozeer een signaal dat er iets bijzonders staat te gebeuren, maar een vroege verschijning van iets dat een 'nieuw normaal' wordt.[5] Er *zijn* nu witte en zwarte zwanen, zoals het financiële systeem nu ook wordt ingericht met de kans op totale instorting als reële optie. We houden er in die zin rekening mee. Maar, dat is de paradox die bij de notie van *black swans* hoort, we houden rekening met de zwarte zwanen van gisteren.

Dit essay handelt over een deelverzameling van de *black* swans. **We kijken naar voor onmogelijk gehouden risico's, die het resultaat zijn van een verrassende, soms zelfs volkomen ondenkbaar geachte samenloop van omstandigheden, of beter van risico's. Dit zijn *vernetwerkte risico's*.**[6] Risico's die niet voorzienbaar zijn, of in ieder geval niet voorzien werden en die primair het product zijn van de interactie-effecten binnen netwerken. ***Vernetwerkte risico's*** **zijn risico's die het resultaat zijn van verrassende, onverwachte interferenties van 'gewone' risico's. De mogelijkheid van interferentie was eenvoudigweg niet aan de orde of de interferentie zelf werd onmogelijk geacht.** De 'samenloop van omstandigheden' was onvoorzien.

1.3 Opbouw van dit essay

[4] Taleb, N.N. (2010), The Black Swan. The impact of the highly improbable, New York
[5] REF 'the new normal'
[6] World Economic Forum (2008), Global Risks 2008. A Global Risk Network Report

Om te beginnen schetsen we in hoofdstuk 2 een aantal inzichten die relevant zijn voor ons denken over risico's, aan de hand van theoretische concepten als de netwerksamenleving, de risicomaatschappij en de audit society. In hoofdstuk 3 gaan wij in op de kwesties die hiermee verbonden zijn, waarbij we inzoomen op de verklaringen voor en dimensies van *vernetwerkte risico's.* In hoofdstuk 4 stippen we enkele mogelijkheden aan om deze risico's te managen, waarna tot slot in hoofdstuk 5 ook aangeven wat dit voor de auditor kan betekenen.

2 Een veranderende context

2.1 De netwerksamenleving

Het is tegenwoordig een gemeenplaats om te spreken over radicale verandering of accelererende vernieuwing in de wereld. Met gemak spreken we over de samenleving en de geglobaliseerde wereld als *netwerk*. Reizen over de wereld, productieprocessen die letterlijk alle uithoeken van de wereld met elkaar verbinden en kapitaal dat over de grenzen via virtuele beurshandel over de wereld vliegt.[7] Steeds gaat het om de idee dat de wereld *kleiner* is geworden door technische manieren om beweging en nabijheid te faciliteren, waardoor verbindingen ontstaan tussen partijen, plaatsen en domeinen die eerder om praktische redenen moeilijk mogelijk waren. Daarnaast gaat het om de idee dat verbinding niet alleen oppervlakkig is, om het met elkaar in contact brengen van gescheiden entiteiten, maar dat de verbinding steeds meer het karakter heeft van versmelting, van bundeling en clustering. Nike, Dell en Apple verknopen niet de verschillende partijen over de wereld samen tot één productieproces, ze *zijn* een globaal producerend netwerk. **Netwerken gaan in dat opzicht niet alleen over partijen die meer dingen samen doen, maar om partijen die in elkaar opgaan, vervlechten en in dat opzicht ook een deel van zichzelf in de ander verliezen.**

Netwerken worden vaak gezien als 'gewoon' gecompliceerde ketens, waarbij partijen meer dan eerst met elkaar te maken hebben. Relaties zijn er meer *gecompliceerd* – er zijn er meer, en meer onderling verbonden, met meer interferenties. Maar dat zijn zaken die grotendeels binnen bestaande beelden van systemen kunnen worden ingevuld. Als een organisatie meer verbindingen moet onderhouden, dan kan de oplossing eenvoudigweg zijn om meer mensen aan te stellen om die verbindingen te onderhouden. Als het resultaat meer buiten de organisatie behaald wordt, bijvoorbeeld door participatie in netwerken van belanghebbenden, kan het voldoende zijn om daar met meer inzet en overtuiging in te participeren – en de eigen interne organisatie daar wat op aan te passen. Bijvoorbeeld door interne agenda's en processen aan te passen aan de ritmiek en agendering van buiten.

De idee van ingewikkelde ketens van partijen volstaat voor een aantal samenwerkingsvormen, maar het is alles behalve het eindpunt van de ontwikkeling. Netwerkvorming gaat veel verder dan dat, omdat zo uiteindelijk een gecompliceerd web aan verbindingen en interacties tussen partijen ontstaat. Dat web is niet alleen op zich ingewikkeld of 'gewoon' gecompliceerd, maar produceert ook zelf *complexiteit*: onvoorspelbaarheid, ondoorgrondelijkheid en emergentie. Het netwerk is meer dan de optelling van de samenstellende delen en heeft een eigen leven. Partijen gaan koppelingen aan, vermengen, nieuwe verbindingen ontstaan en er is afwezigheid van centrale regie. Het één reageert op het ander, onbedoelde effecten treden op, met onverwachte reacties van partijen. Verbanden komen op en verdwijnen weer; groeien door, of maken plaats voor andere verbanden. Niet als onderdeel van een centraal aangestuurd plan of een bestaande traditie, maar als uitkomst van ondoorzichtige en ongestuurde ontwikkelingen. Of beter gezegd, sturing en coördinatie vindt *decentraal* plaats, vanuit de randen van het netwerk in plaats van vanuit een centrale kern (die is in netwerken afwezig). Er spelen allerlei praktijken van coördinatie en sturing naast elkaar, die onvoorspelbare en onvoorzienbare resultaten produceren.

[7] Castells, Manuel (1996, second edition, 2000). The Rise of the Network Society, The Information Age: Economy, Society and Culture Vol. I. Cambridge, MA; Oxford, UK: Blackwell.

Een andere consequentie van deze meer radicale versie van het netwerkbeeld is dat bestaande patronen en structuren van ordening niet langer passend zijn, of op een andere manier functioneren. Netwerken bewegen over grenzen heen, bijvoorbeeld omdat ze expansief zijn en op nieuwe terreinen actief willen zijn, of omdat ze bestaande regels binnen grenzen willen vermijden. Domeinen vermengen. Tot voorheen niet specifiek verbonden deelterreinen raken via netwerken geïntegreerd. Castells duidt dit in zijn veel geciteerde werk over de netwerksamenleving als het verlies van relevantie van het begrip van *territoir* en fysieke plaats als primaire ordening.[8] In plaats van 'plaats' als dominante context van activiteit gaat het om wat Castells de *space of flows* noemt: processen, verbindingen, die er weliswaar zijn maar niet aan een bepaalde locatie te binden zijn of daardoor ingeperkt worden. Het meest bekende voorbeeld van dit verschijnsel zijn – of waren – de door Castells al vroeg aangeduide stromen 'flitskapitaal', die op zoek naar extreem korte termijn rendement in virtuele transacties over de wereld gaan in transacties die nergens tot fysieke landing in concrete assets leiden. Het netwerk is dan niet een verzameling lokale partijen, maar ontstijgt die lokale plaats van de partijen; de lokale plaats van deelnemende partijen is een vindplaats van het netwerk, maar het netwerk is meer dan die vindplaatsen. Eén van de eerste en meest evidente vragen is dan natuurlijk onder welke regels het netwerk dan valt?

Let wel, het werk van Castells waarin deze gedachte voor het eerst krachtig werd uitgewerkt kwam uit rond 1996. Het web stond in de kinderschoenen, smartphones bestonden niet, social media waren nog niet eens een idee en de BRIC-economieën stonden aan het begin van hun stormachtige ontwikkeling. De wereld was vanuit het heden bezien voor nog geen fractie geïntegreerd. Inmiddels is het model van fysiek en geografisch onthechtte stromen veel meer gebruikelijk geworden. Het is bijna gewoon geworden dat bedrijven – groot en klein – zich over de wereld begeven, net zoals particulieren selectief zijn in waar ze hun producten online kopen en waar ze verbindingen aangaan. Multinationale bedrijven, financiële instellingen, kapitaalstromen, maar ook de productie van consumptiegoederen zijn op grote schaal onthecht geraakt van fysieke plaats – of landt veel meer tijdelijk dan eerst. Net zoals productieprocessen opgeknipt zijn in delen die niet over enkele, maar soms honderden locaties en meerdere continenten verspreid zijn. Of, zoals Friedman het noemt, 'de wereld is plat geworden'.[9] **Er zijn grenzen en hiërarchie bestaat onverminderd, maar deze zijn gecontextualiseerd in netwerken – in plaats van dat ze zelf de dwingende context vormen waarbinnen netwerken zich kunnen organiseren**. Bedrijven opereerden ooit 'over de grenzen', nu zijn ze letterlijk verspreid over vele landen en zijn ze alleen nog administratief tot een bepaalde vestigingsplaats te reduceren. Waarbij die plaats weinig verband hoeft te houden met traditie, geschiedenis of de werkelijke plaats van productie, meer met onthechtte afwegingen als lokaal belastingklimaat, regeldichtheid en imago (*Apple: "made in…, designed in California"*). En ook voor Friedman geldt dat zijn werk stamt uit 2001; voordat Skype bestond, Twitter er nog niet was en Facebook alleen bestond in het hoofd van twee studenten. De concepten die we voor de netwerksamenleving gebruiken voldoen, maar tegelijkertijd onderschatten we gemakkelijk de radicale betekenis er van: **de wereld opereert niet als een netwerk, maar *is* in velerlei opzicht een netwerk geworden. Het is de vraag of die radicale (constituerende/vormende) in plaats van instrumentele betekenis netwerken voldoende heeft gevonden in ons denken over sturing, controle, toezicht en beheersing (van risico's en bedreigingen).**

[8] Castells, Manuel (1996, second edition, 2000). The Rise of the Network Society, The Information Age: Economy, Society and Culture Vol. I. Cambridge, MA; Oxford, UK: Blackwell.
[9] Friedman, The World is Flat, 2005.

Ondertussen is er een organisatiepraktijk gegroeid die de netwerkprincipes juist optimaal weet te benutten als hefboom voor productie. Zo zijn op alle niveaus van de samenleving de afhankelijkheden in de loop van decennia sterk gegroeid. Iedereen en alles is intensief verbonden met de buitenwereld: selectieve en gekanaliseerde communicatie is veranderd in communicatie van *any to any.* Informatie ligt niet 'op straat', het is nog meer direct: informatie wordt vanuit elke huiskamer en elke plaats op de wereld met elke andere plek gedeeld. Iedereen staat met iedereen in contact en kan samen tot 'iets' van productie komen. Een idee delen, een werkproces afstemmen, een taak overdragen, een opdracht verwerven, of een transactie sluiten. Communicatie en interactie is daarmee plaatsonafhankelijk geworden. Geografie, tijd en ruimte hebben daarmee een andere betekenis gekregen.

En zo zijn ook de klassieke randen en kaders van organisaties veranderd. Vroeger kenden we ambachtelijke bedrijven die alle activiteiten benodigd om tot hun product te komen zelf deden: van ontwerp tot verkoop, van opleiding tot productie, financiering in eigen hand. Tegenwoordig domineren de hyper-gespecialiseerde bedrijven die precies datgene doen waar ze goed in zijn en niet meer dan dat. Taken zijn als proces nog wel gebundeld, maar in organisatietermen volledig ontkoppeld: een product bestaat uit een lange lijst componenten, die op verschillende plaatsen, door verschillende bedrijven worden geproduceerd en pas heel dicht bij de klant uiteindelijk bij elkaar komen. In dat proces is ook de veranderende betekenis van afstand relevant. Diensten zijn *ge-outsourced*: soms naar een ander gebouw op hetzelfde bedrijventerrein, maar evengoed naar een ander continent.

Daarnaast zijn ook de financieringsconstructies wezenlijk veranderd. Bedrijven zijn strak gefinancierd om een maximale hefboom te bewerkstelligen. Ze lopen de risico's die daarmee samen vallen weliswaar zelf maar niet alleen. Deze bedrijven werken intensief samen met andere bedrijven, *upstream* en *downstream* in de keten, en ook deze samenwerking is strak georganiseerd, met *just-in-time* leveranties, kort *getimede* betalingen en op maximale hefboom gerichte financiering. Daarmee is een enorme stijging van productie – en van welvaart – mogelijk geworden, die pas in de kredietcrisis en de daarop volgende economische crisis tot een correctie is gekomen. Daarmee zijn een aantal zaken veranderd, maar is het onderliggende principe van verder gaande vernetwerking op geen enkele manier veranderd.

Meer dan ooit geldt dat alles en iedereen (individuele bedrijven *en* de keten als geheel) *lean and mean* georganiseerd is en iedereen afhankelijk is van elkaar. Afhankelijkheid is de prijs van de enorme hefbomen die door de vernetwerking ontstaan: partijen kunnen letterlijk meer aan door zich te verbinden aan andere partijen – veraf of dichtbij – en hoe meer verbindingen hoe groter de mogelijkheden. Maar tegenover die mogelijkheden staan afhankelijkheden en dus ook kwetsbaarheid. Een probleem op één plaats in het netwerk kan overslaan naar elders in het netwerk. Deels kan het netwerk dat ondervangen met andere verbindingen en ingebouwde reserves, maar soms ook niet. Dan kan een crisis op één plaats in het netwerk het hele netwerk of vitale delen er van platleggen. **Dat is de paradoxale dimensie van netwerken: enerzijds vergroten ze onze effectiviteit en weerbaarheid enorm, maar anderzijds omvatten ze ook vaak *onzichtbare* en *ongrijpbare* bronnen van potentiële problemen**.

SARS: een vernetwerkt virus

In 2003 werd de wereld opgeschrikt door een tot dan toe onbekend virus. Mensen ontwikkelden van het ene op het andere moment hoge koorts, ontstekingen aan vitale organen en een aantal van hen

overleed. Het virus ontkiemde in Azië en nam direct de wereld in zijn greep. Overal leek besmetting op te treden, wat de vraag opriep hoe het virus zich verspreidde. Al snel kwam op die vraag het dramatische antwoord: het virus gebruikte het geglobaliseerde netwerk om zich over de wereld te verspreiden. Een besmet persoon in een vliegtuig stak via de airconditioning aan boord een aantal anderen aan. Die stapten op de luchthaven over op andere vliegtuigen en verspreiden zich over de wereld. Zo reisde het virus via de internationale hubs van het vliegverkeer naar alle uithoeken van de wereld. Het legde hele steden en staten – zoals Singapore – volledig plat. Er werd een vaccin gevonden en virologen spraken achteraf over het geluk dat het virus zich relatief snel manifesteerde. Daardoor was besmetting tijdig zichtbaar, zodat quarantaine mogelijk was en de verspreiding in ieder geval vertraagd kon worden. Tegelijkertijd toonde SARS de ultieme kwetsbaarheid van de vernetwerkte wereld. In Singapore heeft het er toe geleid dat men over de hele wereld monitort welke virussen en epidemieën dreigen, zodat men in noodgevallen de stekker uit het mondiale vliegverkeer kan trekken en Singapore zich letterlijk van het netwerk kan afkoppelen.

De netwerksamenleving is geen 'technologische innovatie'. Het is een sociale ontwikkeling in die zin dat het gaat om menselijke interactie. Technologie is daarin echter wel een cruciale drijvende kracht. De interactie gaat sneller, makkelijker en inmiddels op veel plaatsen automatischer dan anders mogelijk was geweest. ICT is daarin een cruciale factor, omdat het mogelijk maakt dat partijen over de hele wereld verspreid toch in *real time* – zonder vertraging als gevolg van afstand – met elkaar kunnen interacteren.[10] Transportmiddelen en de daaromheen gegroeide logistieke systemen zijn een tweede cruciale factor. Door technische innovaties en verder groeiende economies of scale is het steeds beter en makkelijker mogelijk om fysieke goederen en personen te transporteren. Ook hier is sprake van versnelling, naast een forse reductie van kosten. Het maakt dat nabijheid niet alleen een virtueel begrip is, maar ook werkelijk fysiek dichterbij zijn betekent. Partijen kunnen elkaar ontmoeten als ze willen, elkaar spullen sturen en handen schudden als het nodig is. **De netwerksamenleving is niet alleen een digitaal en virtueel fenomeen, maar is evenzeer een fysiek, tastbaar en voelbaar.**

Zoals bij alle nieuwe technologie duurt het een generatie alvorens de mogelijkheden ervan ten volle benut worden. In de eerste fase wordt de nieuwe technologie vooral gebruikt om de bestaande processen te stroomlijnen of te vergemakkelijken. In de volgende fase kruipt de technologie meer naar het hart van de processen en ontstaat een zekere vervanging en verplaatsing. Bepaalde beroepen bestaan simpelweg niet meer, omdat ze zijn vervangen door geautomatiseerde systemen en sommige apparaten zijn uit de handel genomen als gevolg van nieuwe technologie. Pas in een volgende fase, en vaak met de generatie die technologie niet heeft 'aangeleerd' maar er in is opgegroeid, ontstaat de meer radicale inzet van innovaties. Dan ontstaan geheel nieuwe toepassingen die niet het bestaande vergemakkelijken maar iets heel nieuws doen. Zo is het ook met netwerktechnologie gegaan. Eerst was het een middel voor bedrijven om makkelijker over grenzen zaken te doen, vervolgens werd de interactie zelf de kern van het bedrijfsproces. Zo is netwerktechnologie ook in bijvoorbeeld de financiële wereld de basis geworden van nieuwe financiële producten. De markt werkt principieel nog op dezelfde manier als vroeger – vraag en aanbod komen bij elkaar – maar ICT heeft het mogelijk gemaakt om tot oneindig meer complexe producten te komen. Bijvoorbeeld het opknippen, waarderen en verhandelen van risico's – die bovendien niet lokaal, maar over de hele wereld verhan-

[10] Castells, Manuel (1996, second edition, 2000). The Rise of the Network Society, The Information Age: Economy, Society and Culture Vol. I. Cambridge, MA; Oxford, UK: Blackwell.

deld worden. Zo heeft de technologische innovatie geleid tot majeure sociale innovatie, met heel andere manieren van werken, handelen, organiseren en nieuwe omgang met risico's met zich mee gebracht. Nieuwe technologie vormt de basis van de vernetwerkte samenleving, maar de netwerken beperken zich niet tot technologie. **Daarom spreken wij hier van de *netwerksamenleving*: de samenleving gaat niet soms een netwerkachtige verbinding aan, maar *is* een netwerk geworden.**

2.2 De risicomaatschappij

Zoals aangegeven zorgt het vernetwerkte karakter van de moderne samenleving voor grote hefbomen die de effectiviteit en mogelijkheden van partijen enorm vergroten. Tegelijkertijd zorgt precies diezelfde vernetwerking ook voor een veel bredere en minder goed voorspelbare verdeling van risico's. Gevaren en kosten als gevolg van zaken die mislopen verspreiden zich dankzij dezelfde structuren die de grotere productiviteit mogelijk maken door het netwerk. De schuldencrisis is daar het meest recente en dramatische voorbeeld van. In september 2008 beweerde Minister van Financiën Bos nog dat de val van Lehman Brothers niet meer dan een Amerikaanse gelegenheid was. Een Amerikaanse bank, in de problemen door een crisis die een sterk lokaal karakter had: een crisis op de lokale Amerikaanse huizenmarkt en problemen met hypotheken. Maar dat was denken in de termen van de oude wereld, waar niet het netwerk maar de lokale verankering centraal stond: de val zette dezelfde keten in als de opkomst van het SARS-virus jaren eerder, maar nu zonder de fysieke belemmeringen die er daar nog waren en het vaccin dat toen relatief snel te ontwikkelen was. Lehman was niet de lokale bank die de minister bedoelde, maar dé *hub* in een volstrekt internationaal opererend financieel systeem. Voor de minister was het één stukje van een zeer groot systeem met allerlei partijen. Vanuit het netwerk geredeneerd was Lehman een *verdeelpunt* van waaruit op slag het gehele netwerk aan het risico was blootgesteld. Vervolgens gebeurde een tweede voor netwerken cruciaal fenomeen: de schade *verdeelde* zich niet alleen door het netwerk, maar werd door allerlei onderlinge interacties steeds *groter*. Lehman was niet één steen in een bouwwerk, maar bleek een dominosteen die een lange rij andere stenen omgooide. Zo verspreide het risico zich door het gehele mondiale financiële systeem, waarbij elke aangetaste bank weer zorgde voor de verspreiding van nieuwe en grotere risico's door het systeem. **Uiteindelijk was er niet één rij vallende dominostenen, maar waren er allerlei tegelijk vallende rijen stenen, waarbij uiteindelijk geen enkele steen zich aan de val kan onttrekken – ook niet de gezond geachte banken.**

Zo werd een volgend kenmerkend fenomeen van de vernetwerkte samenleving zichtbaar: de kosten verspreidden zich niet alleen over het financiële systeem, maar sprongen van daaruit over naar andere systemen en domeinen, die niets te maken hadden met Lehman Brothers of zelfs maar met de financiële markten. De kosten en risico's beperken zich in een vernetwerkte wereld niet tot één systeem, maar omdat systemen onderling verbonden zijn is ook daar sprake van snel overslaande besmetting. De problemen bij banken zorgden er voor dat kredietverlening opdroogde, maar ook dat voor veel banken het voortbestaan in gevaar kwam. Zo sloeg de crisis over van het financiële systeem naar de reële economie – en dus ook direct naar de dagelijkse levens van mensen. De overheid moest garant staan voor financiële instellingen – waarmee het systeem tijdelijk gered leek. Vervolgens sloeg de crisis echter over naar de overheden zelf, die om het eigen vege lijf te redden over gingen op grote besparingsprogramma's en alleen konden overleven door nieuwe garantstellingen van centrale banken.

En zo werd Lehman voor iedereen heel concreet en had de val van Lehman uiteindelijk een veel grotere impact op het leven van gewone mensen in heel de wereld dan de val van de Twin Towers enkele jaren eerder en enkele honderden meters verderop in Manhattan. De beelden van de brandende torens staan op ons netwerk gebrand en 9/11 herinneren we als een historische datum. Niemand weet hoe het gebouw van Lehman er precies uit ziet, wanneer de bank definitief instortte of hoe de baas van de bank toen heette. Maar de impact ervan is enorm, als voorbeeld van hoe netwerken ons veiliger en sterker maken, maar tegelijkertijd zorgen voor ongekende en bijna onbegrensde kwetsbaarheid. **Netwerken maken dat het ons goed gaat; totdat het mis gaat.**

De financiële crisis biedt zo zicht op een aantal inherente eigenschappen van het netwerk. Zoals gezegd, dat gaat niet om uit te bannen of te voorkomen 'ontwerpkwesties' of kinderziekten. Risico's en kosten verspreiden zich over dezelfde kanalen en structuren die we gebruiken voor de nuttige, productieve en prettige opbrengsten van het netwerk. Zoals SARS zich via de vliegverbindingen verspreidde die we gebruiken voor vakanties en internationaal zakendoen, en zoals de kredietcrisis over de wereld golfde via het hetzelfde financiële systeem dat jarenlang voor het goedkope krediet zorgde dat consumptie en economische groei mogelijk maakte. **Het netwerk kan welvaart vergroten en brengt waarde op plekken waar het anders niet zou komen, maar datzelfde gebeurt met risico's, schade en kosten.**

Zo heeft de moderne samenleving zich ontwikkeld van een schuld- tot een risicomaatschappij. **Waar lokaliteit vroeger centraal stond waren schade en last direct verbonden met een ergens door een aanwijsbaar iemand genomen risico. Schade stond dichtbij de schuldige, die met zijn eigen handelen een probleem had veroorzaakt.** De schade beperkte zich vaak niet tot de schuldige alleen, zoals angstaanjagend zichtbaar werd bij de vuurwerkramp in Enschede of bij ongelukken met treinen of vliegtuigen. In dat perspectief van schade en schuld is het risico steeds sterk verbonden met een lokale en aanwijsbare handelende actor, die iets nalaat of een risicovolle handeling onderneemt. Bijvoorbeeld het met minimaal onderhoud laten vliegen van een vliegtuig of het naast elkaar opslaan van in combinatie explosieve chemicaliën. Last en schade zijn dan herleidbaar naar schuld en naar een schuldige. Systemen van toezicht en controle proberen dat risico in te dammen, voor de direct betrokkenen maar vooral ook voor de omstanders of gebruikers die weliswaar in de nabijheid van het risico verkeren maar er verder zelf geen invloed op kunnen uitoefenen. De inspectie controleert het vliegtuig, zodat de inzittenden zich daarover geen zorgen hoeven te maken. Mocht er ergens iets mis gaan, dan is dat iemands schuld – waarbij de praktijk ook is dat ook gekeken wordt naar de rol van de toezichthouder die mogelijke medeschuldig gehouden wordt.

De risicomaatschappij, als eerste met diepte omschreven door Ulrich Beck[11], wijst op een ander soort risico's. **In de risicomaatschappij worden mensen het meest bedreigd door risico's die *niet* vanuit hun directe nabijheid komen en die hun voorstellingsvermogen soms te boven gaan.** Dat type risico's is moeilijk zichtbaar, laat staan voor individuen beïnvloedbaar. Het gaat dan om risico's die weliswaar heel klein zijn maar waarvan de gevolgen enorm zijn, zoals nucleaire crisis, de gevolgen van massaal gebruik van antibiotica in vlees, genetische mutaties in de voedselketen of het gebruik van nog niet uitontwikkelde DNA-technologie in de gezondheidszorg. Daarin nemen mensen risico's die tot mogelijk majeure gevolgen kunnen leiden waarvan het – als het ooit zover is – onvoorstelbaar

[11] Beck, Ulrich (1992) Risk Society: Towards a New Modernity. London: Sage.

is dat we ze hebben genomen. De waarde van goedkope kernenergie verbleekt bij de eerste grootschalige nucleaire ramp, zoals in Fukushima bijna het geval was. Om over genetische manipulatie of manipulatie in voedselketen nog te zwijgen. De mens loopt, zo stelt Beck, allerlei risico's die ver boven en buiten het eigen voorstellingsvermogen liggen en nergens echt geadresseerd worden. Ze worden 'gemanaged' in beheersmaatregelen die weliswaar strikt zijn, maar nooit de garantie bieden dat het goed gaat. Of ze zijn verzekerd in arrangementen die in het geval van een optreden van het risico waardeloos zijn. Wat is de waarde van een verzekering bij een nucleaire ramp? Wat heeft iemand aan een levensverzekering als genetische mutaties van voedsel tot een globale epidemie leiden? Schade en schuld zijn zo in zekere zin ontkoppeld geraakt. **Risico's worden niet meer bewust genomen, maar iedereen loopt ze wel.** Mensen nemen een paraplu mee voor als het regent en dekken daarmee hun risico op regen af. Wie geen paraplu meeneemt wordt nat, eigen schuld. Maar wat de risicomaatschappij daar aan toevoegt is dat diezelfde mensen – met of zonder paraplu – tegelijkertijd ook het risico lopen dat ze in een nucleaire ramp belanden of in aanraking komen met giftige deeltjes uit een chemisch proces ver weg. **Schade en schuld zijn dan moeilijk meer te verbinden.** Met of zonder paraplu, niemand overleeft de nucleaire storm.

Het vernetwerkte karakter van de samenleving voegt hier een extra dimensie aan toe. De risico's hangen niet alleen als een onzichtbare vlek boven de markt, ze zijn letterlijk onzichtbaar en ongrijpbaar omdat ze pas in onvoorspelbare interacties ontstaan en zich over het netwerk verspreiden. Risico's komen niet voort uit causaliteit waar we ons niet van bewust zijn, maar uit circulaire patronen waarbij de interactie van gebeurtenissen leiden tot risico's die er eerst écht niet waren. Risico's zitten als onbedoelde en onverwachte gevolgen verpakt in allerlei relaties die we aangaan en producten die verhandeld worden. Derivaten zijn bijvoorbeeld in essentie financiële producten om risico's te beheersen, maar door grootschalige handel werden ze een mechanisme dat op zichzelf voor grote nieuwe risico's zorgde. Net zoals banken op zichzelf een manier zijn om risico's te mitigeren en de kapitaalvoorziening in de samenleving te verzekeren, maar in de financiële crisis juist zorgden voor de verspreiding van problemen over de wereld en voor de sprong van het financiële systeem naar de reële economie. **Dat zorgt voor een extra dimensie in het denken over risico: het gaat niet alleen om de risico's die onzichtbaar zijn of te groot om er mee rekening te houden, maar ook om risico's die letterlijk nog ongekend of onvoorstelbaar zijn omdat ze zich pas in onvoorspelbare interacties van een complex systeem manifesteren**. Dat maakt het systeem van risicobeheersing door het uitvoeren van een stresstest ook zo wankel: de stresstest test het systeem op het vermogen om een volgende keer met de vorige crisis om te gaan, niet op het vermogen om op een nog onbekende nieuwe crisis te reageren.

Interessant aan de hiervoor geschetste ontwikkelingen is dat bijna parallel aan het toenemen van de risico's de we lopen de acceptatie van risico's in ons denken sterk is veranderd. Kort gezegd is er een breed gevoelde acceptatie van het nemen van risico ontstaan, maar die gaat tegelijk wel gepaard met een sterk verminderde verdraagzaamheid als het gaat om pech.

Risico wordt in algemene zin gezien als een noodzakelijk kwaad om verder te komen. Het hoort bij het leven en wordt geassocieerd met positieve waarden als ondernemerschap, innovatie, creativiteit, groei en ontplooiing. In de risicomaatschappij wordt vooruitgang geboekt door risico's te nemen. Het dominante paradigma in de risicomaatschappij is dat onze huidige samenleven zo succesvol is , omdat we bereid zijn risico's aan te gaan en deze betrekkelijk goed weten te managen. Onze bedrijven kunnen hun activiteiten strak financieren. In het algemeen, maar niet altijd, gaat dat goed. Wie er

goed in is overleeft, wie de risico's minder goed doorziet en beheerst gaat failliet. Dat wordt benoemd als de tucht van de markt. Risico is daarmee niet een soort lot dat ongeacht het eigen handelen boven ons hoofd hangt, maar is een toestand waarop we zelf in belangrijke mate controle uitoefenen. Tot op zekere hoogte is het zelfs een utiliteit geworden, een 'ding': we praten er over in termen die het bijna tastbaar maken, tot iets dat je in de koffer meeneemt, dat je kunt wegnemen of uitsluiten als je het maar goed aanpakt. Dat is een productieve manier van omgaan met risico gebleken. We calculeren risico's, gaan de risico's aan en managen ze.

Toch heeft die opbrengst een keerzijde, die ook door Beck naar voren wordt gebracht. Beck stelt dat wij steeds meer bezig zijn de risico's en de bijbehorende incidenten te bestrijden, te mitigeren en te verdelen.[12] Hij doelt hier met name op grote technologische risico's. Deze risico's zijn veelal onzichtbaar, onomkeerbaar en zo groot dat ze niet te verzekeren zijn. In dit perspectief is onze welvaart gebouwd op risico's; we zijn rijk omdat we risico's nemen en een bepaalde categorie risico's stelselmatig besluiten te vergeten. Alleen door risico's te nemen, weten wij onze welvaart te verhogen – en alleen door bepaalde risico's niet in de afweging mee te nemen kunnen we op die weg doorgaan. Dat proces versterkt zichzelf; eenmaal op het pad van nucleaire stroom of in een economie gebaseerd op koolstof is het bijna onmogelijk om het risico van nucleaire catastrofes of opwarming van de aarde helemaal op waarde te schatten. Dat zou leiden tot passiviteit: vooruit kan niet, maar terug kan ook niet meer. Beck waarschuwt voor de gevolgen van deze omgang met risico's. Ooit worden de nu nog onzichtbare risico's concrete en tastbare incidenten die ons dan zo veel kosten dat de eerder opgebouwde welvaart verdwijnt. In die zin is al het risicomanagement dat we plegen een illusie en is de groei die er uit voortkomt eerder een lening; uiteindelijk betalen we terug, maar dan later en mogelijk elders. De utilisatie van het risicobegrip vergroot het gevoel van grip op risico, maar het vertroebelt het zich op de categorie risico's die te groot of te complex zijn voor het management ervan. Het maakt het dagelijks leven makkelijker en prettiger – én het dekt een kleinere categorie risico's ook echt af – maar dat gebeurt tegen de prijs van andere en grotere risico's die er door kunnen voortgroeien.

De risicomaatschappij heeft als paradoxale opbrengst dat juist door het nemen van risico's we het optreden van pech niet meer verdragen. Mensen streven naar volledige controle over risico's, ook als die ver buiten ons vermogen van beheersing liggen. En daarbij komt dat het voorkomen van risico's en mislukking onmogelijk is, omdat de welvaart er juist op is gebaseerd. Dat sentiment steekt vooral op als een risico tot een daadwerkelijk incident wordt. Er bestaat dan steeds minder bereidheid om de kosten van het incident te dragen. Deze op risico gebaseerde *risk averse* samenleving is ook wel samengevat in het motto 'pech moet weg'.[13] We leven gevaarlijk, maar accepteren geen ongeluk. We nemen elke dag grote risico's, maar accepteren niet de gevolgen van de onveiligheid die dat mogelijk oplevert.

De beperkte tolerantie voor mislukking, gekoppeld aan de risico's die overal zijn, leidt tot wat de voorzorgcultuur wordt genoemd.[14] In deze voorzorgcultuur is steeds minder plaats voor *risico als afweging*, maar wordt er alles aan gedaan om risico te ontlopen. Risico is er niet om te nemen, maar

[12] Beck, Ulrich (1992) Risk Society: Towards a New Modernity. London: Sage.
[13] Stutterheim, R.H. (1991), Pech moet weg. Risicoaansprakelijkheden bij onrechtmatige daden en zorgvuldigheidsnormen. In: Rechtshulp 1991/12 2-7
[14] Pieterman, R. (2008), De Voorzorgcultuur. Streven naar veiligheid in een wereld vol risico's en onzekerheid, Boom Juridische Uitgevers

om te ontlopen. Op alles wordt geanticipeerd en er worden (dure) voorzorgsmaatregelen genomen, die het leven evenwel uiteindelijk lang niet altijd veiliger maken. Dit is zichtbaar in de gezondheidszorg (het langdurig door-testen van nieuwe geneesmiddelen), jeugdzorg (interventies achter-de-deur en onder-het-bed) en het financiële toezicht (extra hoge buffers, steeds strengere protocollen). Zo wordt geprobeerd om alle bekende risico's in te dammen en vooraf uit te sluiten. Dat leidt tot allerlei kosten. De voorbereidingstijd neemt bijvoorbeeld toe, omdat het lang duurt voordat alle risico's in beeld zijn en er voldoende maatregelen getroffen zijn. Ondertussen vallen er slachtoffers, want mensen die ernstig ziek zijn hebben beperkte wachttijd tot het medicijn gereed is. Daar komen de kosten in het primaire proces bij, omdat alle voorzorgsmaatregelen in zekere zin het proces frustreren. Het vliegtuig wordt bij wijze van spreken zo veilig gemaakt dat het amper nog vliegt. De regels voor kredietverlening van banken worden zo zwaar dat banken nauwelijks meer krediet verlenen. **Zo gaat voorzorg ten koste van de productiviteit, terwijl het bedoeld is om de schade aan de productie te voorkomen en dus te minimaliseren. Er gaat minder mis, maar er komt ook minder tot stand.**

Daar komt bij dat een cruciaal element van voorzorg is dat de risico's bekend zijn. **Voorzorg vereist voorkennis**. De WRR benadrukt echter in een studie naar de risicomaatschappij dat veel risico's niet bekend maar juist *onkenbaar* zijn.[15] In dit soort situaties is er sprake van onzekerheid. Organisaties worden alleen deels bedreigd door risico's die ze kennen. Die zijn er wel, maar er is meer. Veel belangrijker zijn de onbekende risico's, of – zoals de WRR ze noemt – de *onzekere risico's.* Met name deze onzekere risico's vragen volgens velen om een voorzorgbenadering. Juist omdat ze niet precies bekend zijn moeten we er voorzichtig mee omspringen. Deze benadering is heel expliciet in het volgende citaat uit de Rio Declaratie: '*where there are threats of serious or reversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation.'*[16] De idee hier is dat het niet kennen van het risico – of het ontbreken van sluitende bewijslast ervoor – in gevallen van serieuze consequenties van een risico geen argument mogen zijn om niet te handelen. **Met andere woorden, risico's die met enige overtuigingskracht als ernstig kunnen worden neergezet verdienen voorzorg.** Dit idee vormt de basis van het denken over duurzaamheid en milieubeleid.

Daar waar risico samenleving en voorzorgcultuur in elkaar overlopen, kunnen grote misverstanden ontstaan.

> Overheden stuiten bij de realisatie van risicovolle projecten nogal eens op weerstand van burgers. Deze burgers lijken niet bereid te zijn het risico te dragen van een leven in de nabijheid van een risicovolle infrastructuur of van een bedrijf waarbinnen zich risicovolle processen afspelen. Overheden reageren hierop door aan te tonen dat aan deze activiteit niet of nauwelijks risico's kleven (de 'intrinsiek veilige kernenergiecentrale'). Overheden bestempelen dit gedrag, ietwat minachtend, al gauw als NIMBY gedrag. Aan de andere kant: burgers blijken wel degelijk bereid om risico's aan te gaan, als ze er ook maar de vruchten van kunnen plukken of als de risico's redelijk gespreid worden. De overheid die steeds meer kiest voor het voorzorg principe ('er zijn geen risico's) verwijt hier burgers alle risico's uit te sluiten, terwijl juist burgers nogal eens het principe van de risicomaatschappij toegepast willen

[15] WRR (2008), Onzekere Veiligheid. Verantwoordelijkheid rond fysieke veiligheid, Amsterdam
[16] Rio Declaration on Environment and Development (1992)

zien, d.w.z. dat degene die risico loopt ook de vruchten moet plukken van die risico's.[17] De oplossing zou dan kunnen zijn dat gezocht wordt naar mogelijkheden om burgers die het risico lopen, ook te laten meedelen in het profijt van de risicovolle activiteit. Overheden zouden meer energie moeten steken in het ontwikkelen van op profijtverdeling gerichte arrangementen dan in het wegwerken resp. ontkennen van risico's waarvan iedereen aanvoelt dat er minimaal een rest-risico, zo niet meer, blijft bestaan.

Wildavsky is een belangrijke en klassieke criticaster van het voorzorg-denken.[18] Hij beschouwt risico aanvaarding als een voorwaarde voor dynamiek en ontwikkeling en in deze zin is hij een adept van de risicomaatschappij. Hij is van mening dat we niet te veel moeten inzetten op de anticipatie op risico's, maar dat het beter is om te vertrouwen op veerkracht of *resilience* en op het nemen van risico's volgens het principe van *trial and error*. Wildavsky wijst en passant op het feit dat, ondanks dat onze welvaart is gebouwd op risico's, de veiligheid in rijke landen is toegenomen. Anders gezegd: het mag dan zo zijn dat onze welvaart is gebouwd op risico's, maar dat is geen probleem zolang de risico's zich maar niet manifesteren en kennelijk slagen wij daar goed in. Een belangrijk punt in de redenering van Wildavsky is dat voorzorg op de korte termijn dan wellicht veiliger maakt, maar dat de gevolgen er van op langere termijn dramatisch kunnen zijn. Hij gebruikt het voorbeeld van antibiotica-gebruik. Door nu op grote schaal antibiotica in te zetten kunnen we tijdelijk virussen de baas blijven, maar het versnelt eveneens de resistentie van de virussen. Door antibiotica in te zetten helpen we de virussen op weg naar resistentie voor de bekende antibiotica en het aantal varianten daarop is beperkt. Op langere termijn snijden we ons daarmee in de vingers. Een ander voorbeeld is het zo sterk verhogen van de veiligheidsregels voor handelen, dat het handelen nauwelijks meer opbrengsten genereert. Er gebeuren dan geen ongelukken, maar doordat de productie zelf ook uit blijft gaat welvaart verloren. En die welvaart is op de langere termijn juist weer nodig om veilig te blijven en voldoende vermogen te hebben om de dan opkomende nieuwe risico's te lijf te gaan. De bankencrisis is daarvan een interessant voorbeeld. Enerzijds is het goed dat banken hun buffers moeten versterken en scherper kijken naar kredietaanvragen. Dat voorkomt schade aan de economie door 'omvallende banken'. Anderzijds veroorzaakt het stilvallen van de kredietverlening die hier een direct gevolg van is eveneens grote en misschien wel veel grotere schade aan de economie. De banken vallen dan weliswaar niet om, maar daar staat tegenover dat kleine en grote bedrijven niet kunnen investeren of in financieringsproblemen. De rem op de economische ontwikkeling leidt tot minder vertrouwen in de economie, tot uitval van de vraag en tot economische malaise. De banken zijn veilig, maar daardoor loopt iedereen op andere vlakken grote risico's.

2.3 De audit society

Toegenomen risicobesef, nadruk op voorzorg en de wens om gevaar te beheersen – in een vernetwerkte wereld waarin gevaar alom is en we steeds meer risico lopen – heeft geleid tot een vlucht naar voren, in systemen van controle en beheersing. Michael Power is één van de auteurs die wijst op de vaak paradoxale gevolgen van onze pogingen om risico's te beheersen en gevaar te ontlopen.

[17] Eeten, M. van, Noordegraaf-Eelens, L, Ferket, J., Februari, M. (2012) Waarom burgers risico's accepteren en waarom bestuurders dat niet zien, Den Haag
[18] Wildavsky, A. (1988), Searching for Safety, New York

Hij beschrijft in een publicatie over de *Audit Society* hoe het omgaan met risico's problematische gevolgen produceert.[19] Het in beeld brengen en houden van de risico's van een activiteit – door Power benoemd als het doen van een 'audit' – is volgens Power van zodanig belang geworden dat dit langzamerhand het 'echte werk' overneemt. En omdat organisaties dit op grote schaal doen is er volgens hem sprake van een *Audit Society* – een samenleving die wordt overgenomen door systemen gericht op het meetbaar maken en kennen van risico's. En die poging, zo betoogt Power, kent geen grenzen. **Er is op zichzelf niets mis met het in beeld brengen van risico's, maar kenmerkend voor de audit society is dat de wens daartoe de onderliggende praktijk overneemt.** De praktijk is dat risico's niet goed eenduidig in beeld te brengen zijn en dat productieprocessen meer zijn dan risico's alleen, terwijl de drang naar inzicht in risico's ze daar wel toe reduceert. In die zin zijn begrippen als risico en control *performatieve* begrippen, begrippen die zichzelf door ze af te spreken meer werkelijk maken, doordat de sociale werkelijkheid zich er naar vormt. Het zijn geen onschuldige lenzen om mee naar een object of proces te kijken, maar concepten die er voor zorgen dat de wereld zich meer overeenkomstig daarmee gaat gedragen. Ze beschouwen de wereld niet, maar maken die mede. Doordat we vanuit een lens van risico en control kijken naar organisaties en daar systemen van beloning, bestraffing en waardering aan gekoppeld zijn, gaan organisaties zich steeds meer naar die lens gedragen. Ze brengen steeds explicieter de risico's in beeld en bouwen steeds grotere en nog meer zichtbare systemen van controle. En als dat proces eenmaal begint is er geen rem meer op. Niemand kan in een door risicomanagement gedomineerde organisatie nog pleiten voor de afbouw van controle. Let wel, daarmee is niet gezegd dat er ook daadwerkelijk geen risico's meer genomen worden. Dat is misschien wel het belangrijkste punt van Power. Het bouwen van omvangrijke risicosystemen is niet hetzelfde als het zorgvuldig omgaan met risico. Integendeel, het verwerkelijken van de audit society gaat over een samenleving en over organisaties die weliswaar heel veel controlesystemen hebben maar die daar uiteindelijk maar weinig gebruik van maken. Ze werken er omheen en nemen misschien zelfs meer risico omdat men zich veilig waant achter de hoog opgetrokken bescherming van de controlesystematiek.

Eén van de belangrijke paradoxen die de audit society met zich mee brengt is volgens Power dat de nadruk op het auditen van risico en control leidt tot wat hij de *rhetoric of accountability* noemt.[20] Er komt steeds meer nadruk te liggen op het proces van verantwoording en op de vermeende noodzaak om inzicht te verwerven via een onafhankelijke auditor in plaats van in de directe lijn tussen management en organisatie. Bedoeld of onbedoeld wordt daarmee de suggestie geïnstitutionaliseerd dat management en organisatie elkaar niet vertrouwen – en niet te vertrouwen zijn. Alleen door interventie van een onafhankelijke auditor, met een geobjectiveerde systematiek, komt de werkelijke informatie over risico en control boven tafel. Dat is eveneens een performatieve interventie. Juist omdat er op audit-infomatie gestuurd wordt en de parameters ervan relatief inzichtelijk zijn gaan auditees zich naar die informatie gedragen. **Ze poetsen hun prestaties, risico's en control-systematiek zodanig op dat deze goed scoort in het meetsysteem. Daarmee gaan ze zich onbedoeld gedragen op de manier die het systeem impliceert: niet te vertrouwen, gericht op ontduiking van de norm in plaats van op spontane naleving en misschien wel sublimering er van.** Voor het management geldt

[19] Power, M. (1996). The Audit Explosion. London, UK: Demos. First published in 1994, London. UK: Demos. Zie ook: Power (1997), in: The Audit Society - Second Thoughts, International Journal of Auditing, Int. J. Audit. 4: 111-119 (2000).

[20] Power, M. (1996). The Audit Explosion. London, UK: Demos. First published in 1994, London. UK: Demos. Zie ook: Power (1997), in: The Audit Society - Second Thoughts, International Journal of Auditing, Int. J. Audit. 4: 111-119 (2000).

hetzelfde. Zij hebben geen direct eigen zicht op de werkprocessen en gaan in plaats daarvan steeds meer sturen op de informatie die de audit-systemen hen leveren. Daarmee verandert de organisatie in hun beeld in de audit-systematiek en ontnemen ze zichzelf de mogelijkheid om zelf meer direct te gaan waarnemen. Ze creëren zelf afstand tot het primaire proces door letterlijk achter de audits plaats te nemen en op basis daarvan te gaan sturen. Daarmee transformeren audits van een gestileerde uitsnede van de werkelijkheid voor het management op de waarheid op basis waarvan gestuurd wordt. Daarmee doen ook zij wat de audit impliceert: ze nemen afstand van de werkvloer en verlaten zich in hun oordeelsvorming op de meting van de aanwezigheid van systemen om risico's te beheersen – niet op de aanwezigheid van de risico's of de rijke werkelijke activiteiten die op de werkvloer worden ondernomen om daar mee om te gaan. Het management komt op afstand te staan, wat het beeld op de werkvloer en de speelruimte aldaar voor het voeden van de audit-systematiek met onjuiste informatie vergroot. **Zo wordt de organisatie langzaam, als gevolg van de uitgerolde systematiek, tot datgene dat de systematiek er van maakt: een spel tussen principaal en agent, die elkaar niet vertrouwen én die niet te vertrouwen zijn.** Audit moet te midden van veel onzekerheid assurance bieden, doet dat in zekere mate ook, maar dat leidt niet tot toenemend vertrouwen. Integendeel, het vertrouwen wordt kleiner, wat vervolgens weer leidt tot verder geïntensiveerde systemen van toezicht en control.

Een andere belangrijke paradox die de audit society produceert is wat Power het *'auditable object'* noemt.[21] De audits waren ooit bedoeld om inzicht te verkrijgen in hoe de processen in de organisatie werken, maar die processen zijn meer heel beperkt in audits weer te geven. In plaats van de audits verder te ontwikkelen tot rijkere vormen is het tegenovergestelde volgens Power gebeurt: de processen zijn zich steeds meer geen voegen naar de gesimplificeerde eenduidige en vaak papieren werkelijkheid van de auditsystematiek. Dat is natuurlijk maar beperkt mogelijk, omdat de werkelijkheid in organisaties zo eenduidig niet is. Als tussenoplossing is op veel plaatsen daarom gekozen voor het steeds belangrijker maken van de interne procedures voor de beheersing en control van risico's. In plaats van de risico's in een proces zijn de systemen voor de controle het onderwerp van de audit – en de sturing – geworden. Dergelijke systemen zijn veel geschikter voor de audit zelf en maken het voor de organisatie makkelijker om te voldoen aan de gestelde eisen. Dat is voor de auditor en de manager die gebruik maakt van de systemen eveneens prettig, want het wekt de suggestie van control. De organisatie is op orde, want de systemen die orde brengen zijn aanwezig. Tegelijkertijd is dat natuurlijk ook een illusie. De systemen zijn niet de orde, ze kunnen er mogelijk aan bijdragen. Maar het hebben van een systeem zegt op zich niet veel over de werking daarvan, laat staan over het werkelijke gebruik. **De organisatie wordt steeds meer een meetbaar object, waarin alles dat niet tot meetbare eenheden terug te brengen is niet als waardevol wordt geaccepteerd. Daarmee komt de logica van de audit te liggen over de logica van het organiseren.** Terwijl organisaties uiteindelijk floreren, groeien en leren door goed organiseren, niet door zichzelf tot een audit-systematiek te simplificeren.

[21] Power, M. (1996). The Audit Explosion. London, UK: Demos. First published in 1994, London. UK: Demos. Zie ook: Power (1997), in: The Audit Society - Second Thoughts, International Journal of Auditing, Int. J. Audit. 4: 111-119 (2000).

Dat alles zou misschien nog waarde hebben als de organisaties er ook échte veiliger of beter van zouden worden. Maar dat is zeer de vraag. **De tragiek die Power suggereert – en er is behoorlijk wat reden om aan te nemen dat zijn stelling juist is – is dat er weliswaar veel *aan* controle gedaan wordt, maar dat er uiteindelijk door de mensen die de risico's nemen niet veel zinnigs *mee* gedaan wordt.** De audit society is geen samenleving die door een "abundance" van audit en controle heel veilig is geworden, maar is meer wereld waarin achter opgetrokken schermen van audit en contol het gedrag door heel andere principes en motieven wordt geleid. De organisaties worden er niet veiliger van en lopen geen kleinere risico's. De gevaren zijn ook niet meer in beeld, omdat wat gecontroleerd wordt een versimpelde variant is van de werkelijkheid – niet per ongeluk, maar bewust, omdat het de enige manier is om de complexiteit van de organisatie in een controlemechanisme te vatten. En in zekere zin gaan organisaties en omstanders zich gevaarlijker gedragen. Ze denken dat er 'ergens wel' op de veiligheid gelet zal worden, alles is immers wel ergens gecontroleerd. En zo ligt de Audit Society van Power in zijn werking dicht tegen wat Wildavsky al beschreef in zijn *Searching for Safety*: **de systemen die ons veiliger moeten maken dragen bij aan verhoogd risico en toenemende onveiligheid. In een wereld die gedomineerd wordt door systemen die moeten beschermen lopen mensen risico's die groter dan ooit zijn.**[22] De risico's zijn anders dan eerst, maar daarmee zeker niet minder, kleiner, of met afgenomen waarschijnlijkheid.

[22] Wildavsky, Searching for Safety, Transaction Publishers, 1988.

3 Vernetwerkte risico's

3.1 Gevaarlijk gevoel van veiligheid

We zijn in een paradoxale tijd aanbeland. De netwerksamenleving maakt ons welvarender dan ooit en biedt ongekende kansen. Tegelijkertijd zorgen netwerken voor risico's en gevaren die komen uit plekken waar we vroeger niet mee in contact stonden en groeien ogenschijnlijk kleine lokale gevaren uit tot wereldbedreigende problemen. Het bouwen van dijken helpt alleen als het probleem bekend en gelokaliseerd is – de zee of de rivier – maar netwerken gooien juist die logica van risico en beheersing in de war. **De risico's in onze moderne risicomaatschappij zijn niet meer zichtbaar, kenbaar en lokaliseerbaar, maar ontstaan in emergente processen, langs onvoorspelbare ketens, die ook nog eens dwars door maatschappelijke en geografische verbanden gaan. Zo heeft wat ons sterk maakt ons ook kwetsbaar gemaakt**. De nieuwe welvaart en grote intelligentie van systemen zou ons voor risico's kunnen en moeten behoeden, maar produceert zelf mede de risico's. Netwerken zijn geen instrumenten die we inzetten, de wereld en de systemen waarin we functioneren zijn zelf netwerken geworden. En dat zorgt voor heel andere, grotere en onvoorspelbare risico's.

Wat die paradox nog wat vreemder maakt is dat te midden van die toenemende gevaren onze tolerantie voor risico en gevaar op het eerste gezicht is afgelopen. Mensen willen het risico ontlopen en treffen daarvoor allerlei maatregelen. Ze verzekeren zich, kopen veiligheidssystemen, betalen belastingen en hoge premies aan instituties die hen zeggen te beschermen en ze tolereren onder het motto van beveiliging en preventie van gevaar een ongekende inbreuk in hun privésfeer. En toch neemt de veiligheid door al die systemen, al die aandacht en al dat bewustzijn van gevaar niet per se toe. Integendeel, de schil van beveiliging lijkt het nemen van een risico zelfs gemakkelijker te maken. Denk aan de gordelparadox: het dragen van een gordel maakt dat mensen gevaarlijker rijden. De veiligheid van de gordel zorgt voor gevaarlijker gedrag, wat het effect deels wegneemt. Zo zijn organisaties zich ook niet veiliger gaan gedragen de afgelopen decennia. Integendeel, om hun productie te vergroten zijn ze de mogelijkheden van het netwerk steeds meer gaan benutten om via risico's de hefboom te vergroten. Ze gaan ondanks toegenomen aversie van gevaar de risico's tegemoet, zoeken ze op, deels onder de vermeende dekking van grotere bescherming.

De ontwikkeling richting wat Micheal Power de audit society noemt draagt nog verder aan dit geheel bij. De systemen voor beveiliging en controle, de manier waarop wij risico's proberen te beheersen, sluiten slecht aan bij de werkelijkheid waarin ze opereren. Risicosystemen zijn vanuit de ambitie om auditing mogelijk te maken zo gebouwd dat ze maar heel beperkt kunnen omgaan met complexiteit. Ze hebben, simpel gezegd, een versimpeling van de werkelijkheid nodig om te kunnen werken. En daarmee werken ze dus niet goed of zelfs averechts, omdat ze zicht houden op maar een beperkt deel van het geheel. Waarbij juist in het deel dat ze overslaan, de complexiteit, vaak de belangrijkste gevaren schuilen. Dat zou nog niet eens zo heel erg zijn als dat ook de basis voor het gebruik zou zijn: als bij elk risicosysteem de bijsluiter zou zitten dat op de grote beperkingen er van zou wijzen. Zoals ook de TomTom de bestuurder waarschuwt dat hij ondanks de aanwijzingen wel zelf zijn ogen open moet houden. Het interessante, en zorgwekkende, aan de controlesystemen is dat het tegenovergestelde lijkt te zijn gebeurd. De beperkte controlesystemen zijn in de grote wens tot beheersing van

risico's geworden tot een werkelijkheid op zichzelf.[23] Ze worden niet meer gezien als een versimpelde versie van de werkelijkheid, maar als de werkelijke of anders gewenste versie van hoe het zit. Het systeem wordt niet meer gezien als een afwijking van de werkelijkheid, maar het systeem wordt gezien als de werkelijkheid. Dat heeft twee perverse effecten. Het eerste effect is dat het systeem de werkelijkheid gaat overnemen. Niet echt, dat kan helemaal niet, maar wel als ambitie. De complexiteit uit het systeem moet weg en het management gaat op zoek naar de versimpeling van het controle systeem. De organisatie wordt dan omgebouwd tot een 'auditable object', waar de kern van die organisatie juist is dat de complexiteit ervan veel groter is dan wat de toezichtsystemen aankunnen. Zo gaat er veel energie in het ombouwen van de organisatie tot iets wat ze onmogelijk kan zijn. Daar gaat niet alleen veel tijd, geld en aandacht in verloren, het leidt ook tot meer gevaarlijk gedrag. Dat is de tweede perverse werking van dit mechanisme. Het maakt de organisatie niet veiliger. Het beeld van wat er in de organisatie gebeurt, wat de risico's zijn en of en hoe die beheerst worden, raakt overgenomen door het toezichtsysteem. Het bestuur of het management ziet de organisatie niet meer zoals hij is, maar krijgt alleen nog de versimpelde en gestileerde beelden van het toezichtsysteem te zien. De organisatie was immers verbouwd om te passen bij de systematiek, dus nu zal het systeem ook wel laten zien wat er in de organisatie gebeurt. Die behoefte is heel begrijpelijk, omdat het management het goed wil doen en daarom wil sturen op informatie. Controlesystemen bieden die informatie en dat is belangrijk voor managers die gerustgesteld willen worden over de risico's die ze lopen. Het controlesysteem geeft die geruststelling en waar men onzeker is biedt het systeem de optie tot verdere uitbouw van de controlesystematiek. Zo bouwen organisaties steeds ingewikkeldere systemen, die nog steeds de complexiteit van de organisatie niet afdekken, maar wel zorgen voor een gevoel van beheersing en controle van risico's. Achter die hoog opgetrokken dijken zoeken organisaties verder naar hefbomen voor productie en lopen ze steeds meer nieuwe risico's. Ze zijn bang voor gevaar, maar voelen zich veilig, beschermd door systematiek voor controle en beheersing van risico's. Op dat fenomeen richten wij ons in het vervolg van onze beschouwing.

3.2 De dynamiek van multiple failures

Hoe zijn de vernetwerkte risico's die organisaties lopen te duiden en welk repertoire past daar bij? Wat kunnen organisaties doen om hun manieren van omgaan met dit type risico's te verbeteren en beter passend bij de nieuwe realiteit van de netwerksamenleving te laten passen. We doen dat door de kennis over netwerken, vernetwerkte risico's en de kennis over toezicht en controlesystematiek samen te brengen. Zo ontstaat een nieuw perspectief op toezicht en controle van vernetwerkte risico's. Dat vereist allereerst meer conceptuele scherpte over wat deze risico's zijn, welke fenomenen het ontstaan ervan kunnen verklaren en de dimensies die er ten aanzien van dit type risico's te onderscheiden zijn.

Perrow heeft in zijn klassieker *Normal Accidents* het verschijnsel *vernetwerkte risico's,* weliswaar in andere woorden, mooi beschreven. [24] Perrow spreekt van zogenaamde "multiple failures": iets gaat niet alleen mis, maar zet een keten in werking van problemen die elkaar snel opvolgen. Multiple failures kunnen zich verspreiden en leiden tot een *cascade* van ongelukken. Bij de vraag of incidenten

[23] Van der Pijl, Afscheidsrede, 2013
[24] Perrow, C. (1999), Normal Accidents, living with high-risk technologies, Princeton, NJ

zich wel of niet verspreiden gaat het volgens Perrow om de aanwezigheid van twee fenomenen: *interactive complexity* en *tight coupling*. Samen bieden deze begrippen naar ons idee een sleutel tot het beter begrijpen van vernetwerkte risico's.

A. Interactive complexity

Bij interactive complexity gaat het om het vermogen van delen van een systeem om op een verrassende manier te interacteren met andere delen van het systeem. De verassing ligt in het verband zelf – de koppeling was niet verwacht – of in de uitkomst er van: de interactie veroorzaakt een uitkomst waar geen rekening mee gehouden was. Dergelijke verbanden kunnen lange tijd onzichtbaar blijven door non-lineaire verbanden tussen systeemdelen. **Indien twee systeemdelen op non-lineaire wijze met elkaar verbonden zijn, heeft een verandering in het ene deel van het systeem lange tijd geen zichtbare impact op het andere deel. Totdat een kritische drempelwaarde is overschreden en de interactie in alle hevigheid begint.** Het bekende voorbeeld hierbij is het verband tussen sneeuwval en het ontstaan van lawines. Gedurende lange tijd kan er sneeuw vallen zonder dat dit tot een lawine leidt. Er is dan eigenlijk geen enkel gevaar. Sneeuwval op zich leidt niet tot lawinegevaar. Maar op enig moment is één sneeuwvlok voldoende om een kritische drempel te overschrijden. Er gaat sneeuw schuiven die in *no time* aangroeit tot een lawine. De sneeuwval veroorzaakt uiteindelijk de lawine, maar voordat dat gebeurt is er al heel veel sneeuw gevallen zonder dat daar enig gevaar voor lawinevorming van uit gaat. Maar als de relatie er eenmaal is treedt een keten van effecten in werking, die bovendien amper meer te stoppen is.

De *interactive complexity* in de netwerksamenleving als geheel is onmiskenbaar toegenomen. De belangrijkste reden is de voortschrijdende arbeidsdeling. De achterliggende motor hiervoor is het profijt dat iedereen heeft van arbeidsdeling. Uiteindelijk wordt iederee er beter van wordt als iedereen datgene doet waar hij goed in is. Een belangrijke voorwaarde die dan wel vervuld moet zijn, is dat de gespecialiseerde actoren de mogelijkheden hebben hun producten en diensten te ruilen en te verhandelen. Zo komt iedereen toch weer aan alles wat hij nodig heeft ondanks het feit dat hijzelf slechts heel gespecialiseerde diensten of producten maakt. Aldus ontstaat interactie tussen delen van de samenleving die in vroegere tijden wellicht betrekkelijk onafhankelijk van elkaar opereerden. Die specialisatie, die dus tegelijkertijd gepaard gaat met toenemende afhankelijkheid, is de afgelopen decennia zeer sterk toegenomen. Op alle niveaus is er nu sprake van onderlinge afhankelijkheden, waarvan bovendien een groot deel bij veel mensen totaal onbekend is. Niemand weet waar zijn voedsel vandaan komt, welke stappen er zijn gezet voordat het bij de klant kwam en over hoeveel schijven – en langs hoeveel kilometers – de verbindingen hebben geleid. Per saldo kan het mensen ook niet zoveel schelen, omdat het proces het voor hen mogelijk maakt om relatief duur vlees voor een acceptabele prijs te kopen. Totdat er een bacterie in het vlees aanwezig is, dat ook gevaarlijk is voor mensen: dan wordt ineens zichtbaar hoe 'vernetwerkt' iets schijnbaar eenvoudigs is als vlees dat zijn weg van een boerderij naar een winkel aflegt. De normaalste zaak van de wereld voor wie het proces van binnen kent, maar geheel ongezien door mensen die samen met elkaar het risico lopen van – bijvoorbeeld – de risico's van pandemieën via de voedselproductie.

Naast arbeidsdeling en steeds toenemende taakdifferentiatie die er mee samenhangt zijn er nog meer ontwikkelingen en arrangementen die ertoe leiden dat meer delen van de samenleving interacteren en dat de interacties intensiveren. We bespreken hier de belangrijkste.

Gevoelens van solidariteit hebben ervoor gezorgd dat partijen die getroffen zijn door onheil en ongeluk geholpen worden. Mensen worden in zekere zin ook geraakt door de schade die ze zelf niet leiden en het risico dat ze zelf verminderd lopen. Via solidariteit – al dan niet werkelijk gevoeld – die collectief georganiseerd is zijn mensen mede drager van de risico's die anderen lopen. De kosten van veel incidenten die mensen in het leven overkomen worden niet door hen zelf gedragen, maar worden omgeslagen over een groot aantal anderen. Kinderloze mensen betalen mee voor de kinderopvang, gezonden personen betalen de ziektekosten van hun buren en arbeidsongeschikten ontvangen een uitkering uit premies die door werkenden zijn opgebracht. Ouderen ontvangen AOW die voor hun gevoel zelf bijeen hebben gespaard, maar dat in werkelijkheid wordt omgeslagen uit premies die werkende betalen. Het 'risico' dat ze ouder worden dan gedacht ligt bij diezelfde anderen die de premies opbrengen, ongeacht de voorzieningen die de betreffende ouderen mogelijk zelf hebben getroffen. De solidariteit is deels een kwestie van welbegrepen eigen belang, want strikt genomen is arbeidsongeschiktheid een risico dat iedereen loopt. Het punt hier is vooral dat de kosten van een risico dat werkelijkheid wordt over grote groepen wordt verdeeld. Zo staan we niet alleen via de weg van productie en arbeidsdeling in verbinding, maar ook via de weg van het te delen leed en de daarmee verbonden kosten. **Het risico en de kosten van het incident worden uitgesmeerd over grote aantallen actoren. In dat proces treden mogelijk weer interacties op.** Zo worden de werkenden die in tijden van crisis de hogere premies en kosten moeten opbrengen zelf ook extra aangeslagen, ontvangen ze misschien minder loon en kunnen ze door de collectieve premies amper een eigen buffer opbouwen. Hun leven wordt gevaarlijker, mede door de risico's die ze van anderen overnemen. Met steeds als potentieel gevaar dat ze de solidariteit minder voelen en de bereidheid om er aan mee te doen verliezen.

Een andere factor die voor onderlinge verbondenheid zorgt is minder collectief en meer zelf gekozen. De meeste personen en organisaties kiezen voor verzekeringsarrangementen om een risico dat ze voorzien af te dekken door zich te vrijwaren voor de kosten van incidenten. Zij delen daarmee hun risico met anderen, in dit geval de verzekeringsmaatschappij – die het risico weer verhandelt of deelt met andere betalende klanten. Maar verzekeringsmaatschappijen verzekeren zich ook weer tegen de risico's die zij lopen, bijvoorbeeld bij een her-verzekeraar. **Zo zijn risico's en incidenten niet alleen het gevolg van lange ketens van interacties, maar doorloopt het verzekeren en dekken van de schade ervan een zelfde keten. En die keten die bedoeld is om voor partijen het risico te dekken kan zelf ook weer een nieuw vernetwerkt risico vormen**. Via de lange verzekeringslijnen plant een incident zich voort van de plek waar het incident plaatsvond naar verzekeraar en naar her-verzekeraar – en via die weg belandt het in markten, landen en sectoren waar het op zich helemaal niet plaatsvond. Als het aantal incidenten te groot wordt, zoals in de financiële crisis zichtbaar werd met de credit default swaps, dan gaan de partijen die 'groot' in het herverzekerde risico zitten failliet. In hun ondergang sleuren ze grote aantallen andere kleinere partijen mee, die op hun beurt voor hetzelfde effect zorgen in hun omgeving. De verzekering van risico's is altijd het delen van de pijn met anderen. In de goede tijden is dat met premies en goede hoop goed te verantwoorden en zolang de ernst van de situatie niet te groot is werkt het allemaal goed – en valt er voor partijen veel geld te verdienen. Maar als het incident te groot is, of dat via netwerkinteracties snel wordt, dan leidt de verzekering zelf tot oncontroleerbare risico's. Dat zorgt voor grote onzekerheid bij individuen en organisaties. Wat hen veilig zou moeten maken is een nieuwe bron van gevaar geworden en is bovendien in het geval van een échte, serieuze ramp ook niet zeker. We zijn gewend geraakt aan de ontbindende voorwaarde in een verzekeringspolis dat de schade van een kernoorlog niet gedekt wordt,

maar dat is een 'event' waar we niet serieus rekening mee houden. Als het zover is maakt die ene verzekering ook niet uit. Maar wat als financiële producten als hypotheken en spaarrekeningen worden meegesleurd in een val die wordt veroorzaakt door heel lokale problemen in banken en sectoren heel ver weg. **De paradox hier is dat de maatregelen die partijen nemen om zich in te dekken tegen risico's, weer nieuwe *vernetwerkte risico's* met zich meebrengen**. Een grote verzekeraar adverteert met "niet is zeker" en dan de eigen merknaam: inmiddels is de verzekeraar zelf een bron van nieuw risico geworden, omdat het mensen mede aansprakelijk maakt voor risico's die ze niet dachten te lopen en omdat de zekerheid van de verzekering zelf onzeker is geworden.

Een derde ontwikkeling die zorgt voor steeds verdere verwevenheid tussen partijen is het feit dat, mede door de hiervoor beschreven problemen van verzekeringen en collectieve arrangementen, overheden steeds meer verantwoordelijkheid nemen voor risico's en incidenten. Ze worden in dat opzicht steeds actiever op de markt voor onzekerheid en risico. Ze deden dat al met regulering, toezicht en handhaving, dus in de poging om risico's te voorkomen. Maar inmiddels is die verantwoordelijkheid verbreed naar 'garantstelling' voor allerlei risico's. Overheden nemen steeds meer verantwoordelijkheid voor risico's en kosten van incidenten, ook als die rechtstreeks terug te voeren zijn op gevaarlijk en onverantwoord gedrag van de veroorzaker er van. Om het systeem overeind te houden stappen overheden in, nemen ze kosten op zich, die ze vervolgens omslaan naar alle betrokkenen in hun systeem: belastingbetalers, burgers, bedrijven, iedereen die baat heeft van de overheid en die ergens iets verliest. Soms doet de overheid net iets anders en ontwikkelt men dwingende arrangementen voor partijen om elkaars risico's te dragen, bijvoorbeeld in het geval van de woningcorporaties die moeten opdraaien voor elkaars faillissement. Nooit helemaal, maar het is een vorm waarin de overheid partijen dwingt om de risico's van de ander te dragen. Vaak echter is de overheid zelf toch de laatste 'redder'. Zo lopen spaarders het risico hun spaargeld te verliezen indien hun bank failliet gaat. De overheid heeft geregeld dat iedere spaarder de garantie heeft dat hij tot 100.000 euro terug krijgt indien de bank waar zijn deposito loopt, failliet gaat. De andere banken draaien op voor deze schade en indien ook deze in gebreke blijven, de overheid. Een soortgelijk arrangement geldt tussen woningbouwcorporaties, onderwijsinstellingen en ook voor gemeenten. De schade die ontstaat bij een in gebreke blijven van een corporatie wordt gedragen door de collega corporaties en indien dat niet mogelijk is door overheden. Op internationaal niveau geldt de facto een soortgelijk arrangement. Een euro lidstaat die in de problemen komt, krijgt financiële steun van andere landen. Partijen draaien voor elkaar op, vanuit de logica dat het voor alle betrokkenen uiteindelijk duurder is om niet in te grijpen en de partij écht om te laten vallen. Tegelijkertijd heeft de euro-crisis geleerd dat er ook aan de rol van de overheid als redder grenzen liggen. Ook landen kunnen failliet gaan en door de financiële markten – waar het overigens allemaal begon – naar de rand van de afgrond worde gedreven. Soms zelfs bewust. Daarnaast ligt in deze rol steeds de *moral hazard* op de loer. Als anderen garant staan voor het risico, en er tegelijk het nodige te winnen is met gevaar, waarom zouden partijen zich dan voorzichtig gedragen. **De overheid ziet zichzelf als redder voor als het echt niet meer anders kan, maar is 'gewoon' een schakel in het netwerk die voor een vergroting van het vernetwerkte risico zorgt.**

De laatste factor die we hier noemen voor de toenemende interdependentie zijn schaalvergroting en de toenemende internationalisering van veel actoren. Ook kleine bedrijven en heel gewonde producten maken inmiddels deel uit van een netwerk van relaties dat internationaal is. Een van de bizarre ontdekkingen van de monitoring van data door de NSA is niet zozeer dat het gebeurt, maar

vooral dat er zoveel informatie ergens langs Amerikaanse servers beweegt – en dus onder de bepalingen van de Patriot Act valt. Een wet die overigens niet los te zien is van een andere vernetwerkt incident, de aanval op de Twin Towers. Informatie, productie, bepaalde onderdelen of diensten zwermen uit over de wereld en zwermen terug voor lokale assemblage richting de klant. Zo worden organisaties waarop regelingen betrekking hebben steeds groter en internationaler worden. Een internationaal opererende bank die in een land een andere bank moet helpen, kan financieel zo verzwakken dat ook de operaties in andere landen hierdoor aangetast worden. **Het probleem verplaatst zich zo razendsnel over de wereld en een lokaal probleem kan eenvoudig tot een wereldprobleem worden dat landen en bedrijven aantast die niets van doen hadden met het oorspronkelijke probleem**

Het World Forum wijst in dit verband op het fenomeen van *risk squeezing*. [25] Hierbij worden negatieve effecten van risico's naar andere gebieden overgebracht. Dat gaat in dat geval niet om financiele producten, maar om bijvoorbeeld het dumpen van kernafval en pesticiden in arme en slecht gecontroleerde gebieden in de wereld om daar voort te woekeren. Uiteindelijk moeten ze daar dan toch weer opgeruimd moeten worden, maar tegen veel hogere kosten en met grote gezondheidsschade. **Risk squeezing staat voor grensoverstijgende afwenteling van problemen in productieprocessen.** De minst aantrekkelijke arbeid, de ongezonde restanten, de niet afbreekbare afvalstoffen en alles wat vies, risicovol of onbruikbaar is wordt overgebracht naar de delen van de wereld of het systeem waar het het makkelijkst weg kan. Landen zonder strikte regels, met weinig toezicht, of met regimes en lokale bevolking die blij zijn met de instroom van kapitaal en werkgelegenheid die met de vieze handel gepaard gaat. Zo worden vaak heel expliciete risico's over de wereld gedeeld. Tegelijkertijd leert de theorie van het netwerk ook dat de kans klein is dat ze daarmee voorgoed uit beeld zijn. Het tegenovergestelde is veel meer waarschijnlijk. Op termijn keren ze terug en slaan ze als een boemerang in in het systeem waar ze vandaan komen.

B. Tightly coupled systems

Het tweede element dat volgens Perrow zorgt voor de snelle verspreiding van risico's door netwerken is het organiseren van tight coupling. Het denken in termen van tight en weak couplings is eerder uitgewerkt door Weick, die stelt dat in het moderne organiseren een grote drang zichtbaar is om processen steeds 'strakker' te organiseren.[26] Vanuit de idee van efficiency en rationaliseren van processen wordt bijna letterlijk alle lucht en overlap uit het systeem geperst. Taken, onderdelen en verantwoordelijkheden worden zo georganiseerd dat ze precies in elkaars verlengde liggen. Niet over elkaar heen, ook niet te ver van elkaar af, en met één of twee aangewezen back-up routes voor als er een fout optreedt. Zo kan een systeem in statische toestand heel efficiënt worden ingericht.

Tight couplings werken goed in stabiele en voorspelbare systemen, waarin geen al te grote verstoringen optreden. Als de stroom uitvalt dan zet automatisch het noodaggregaat in en kan de productie gewoon verder gaan. Lastiger wordt het als de verstoring groter of minder statisch is dan hiervoor bedoeld. Wat nou als niet alleen de stroom uitvalt, maar ook de kabel naar het noodaggregaat gebroken is. Of als het aggregaat niet meer werkt, bijvoorbeeld als gevolg van een aardbeving. In een tightly coupled system gebeuren dan tweed dingen die maken dat de verspreiding van het probleem veel sneller gaat en de gevolgen er van al heel snel heel groot zijn. Perrow benoemt dat als *cascading failures*. **Systeemdelen zijn *tightly coupled* als er nauwelijks buffers en *time lags* bestaan tussen**

[25] World Economic Forum (2008), Global Risks 2008. A Global Risk Network Report
[26] Weick, Sensemaking in Organizations, 1995; Weick & Sutcliffe, Managing the Unexpected, 2001.

deze delen. Dat betekent dat systeemdelen letterlijk dichter tegen elkaar aan liggen. Het probleem met de stroomvoorziening in één deel maakt dat meteen alle daarop volgende delen en alles wat er omheen ligt in problemen komen. Er zijn geen buffers, dus elke schok klinkt meteen maximaal door. Daar ontstaat een tweede probleem, namelijk dat tightly coupled systemen hun redundantie hebben weggesneden. Redundantie, het hebben van een zekere overlap, klinkt vanuit rationalisatie als verspilling, maar in tijden van crisis kan het erg prettig zijn als er bepaalde kwaliteiten of vermogens dubbel bezet zijn. Een 'niet-zo-strak-georganiseerd' systeem heeft misschien nog wel ergens een nood-aggregaat staan, in gebruik door een afdeling die het handig vond om zelf een voorziening te hebben. Of er is overlap in bepaalde capaciteiten, zodat het stil komen te liggen van afdeling 1 wordt opgevangen doordat afdeling 2 nog gewoon draait en die ongeveer hetzelfde kan doen. Let wel, dat kan bewust georganiseerde overlap zijn, maar vaak gaat het ook 'gewoon' om improvisatievermogen dat in de organisatie is. Op een niet zo zwaar gecontroleerde werkplaats kan maar net materiaal aanwezig zijn om het probleem te verhelpen: niet dankzij een 'noodprotocol', maar met dank aan de ruimte die er is voor mensen om hun omgeving te personaliseren en zelf te handelen op het moment dat de nood aan de man is. Tight couplings gaat dus niet alleen om het fysiek of organisatorisch dichtbij organiseren van processen en het korter maken van de tijd tussen processtappen; het gaat ook om het bieden van ruimte aan individuen in de organisatie om hun eigen omgeving in te richten, zelf na te blijven denken, zelf betekenis te geven aan wat er om hen heen gebeurt en van daaruit improviserend te reageren op wat er gebeurt. Tightly coupled system hebben die ruimte – fysiek, tijd, persoonlijk – uit alle processen weg geperst, teneinde deze zoveel mogelijk te rationaliseren. Bij verstoringen die net buiten het vooraf bedachte schema passen zorgt dat acuut voor problemen, die dus in veel gevallen als een cascade door het hele systeem gaan.

De notie van tight couplings was altijd een element van individuele organisaties. Het werk van Weick is oorspronkelijk ook op dat niveau gericht.[27] Kenmerkend voor de netwerksamenleving is echter dat het organisatieprincipe van tight couplings – met de achterliggende motieven van rationalisering en efficiency – ook dominant is geworden in de verhoudingen en verbindingen tussen organisaties. Zo zijn lange ketens ontstaan van afzonderlijke organisaties die niet juridisch één zijn, maar die via hun primaire of ondersteunende processen zeer nauw met elkaar verbonden zijn. En die verbinding is nog niet alles. Zoals we in het deel over interactive complexity al lieten zien staan organisaties ook implicet – zonder de bewuste bedoeling daartoe – in verbinding met allerlei andere partijen: bijvoorbeeld via mechanismen om risico's te delen, zoals verzekeringen, garantstellingen of via tweede orde effecten in de systeemdynamiek (een bankencrisis legt uiteindelijk ook de reële economie en vervolgens ook het maatschappelijk verkeer stil). We zijn in dat opzicht veel meer *tightly coupled* dan we denken en met veel meer partijen dan we vermoeden. Tenminste drie vormen van dergelijke verbindingen zijn aan de orde.

De meest directe en voelbare koppeling doet zich voor wanneer systemen fysiek aan elkaar gekoppeld zijn. Grootschalige stroomuitval zal het internet uitschakelen en daarmee ook een groot gedeelte van het financiële verkeer. Dit gebeurt doordat het energie systeem, het internet en het financiële systeem nauw gekoppeld zijn. Gebieden waar veel risicovolle bedrijven geclusterd zijn op een klein oppervlak, kunnen ook risicovol zijn in de zin dat problemen bij het ene bedrijf (emissie gevaarlijke stoffen, brand) gemakkelijk overslaan naar andere bedrijven. Hoge bevolkingsdichtheid en hoge bedrijvendichtheid in gebieden die nu eenmaal aantrekkelijk zijn (bijv. delta-gebieden) zijn een

[27] Weick, Social Psychology of Organizing, 1995

vruchtbare voedingsbodem voor het ontstaan van dit soort problemen. Dat verhoogt ook de kans dat er één of meer gevaarlijke stoffen vrij komen die een direct gevaar vormen voor de omgeving van het gebied.

Maar naast fysieke koppeling kan het ook goed zijn dat een juridisch arrangement voor koppeling tussen systemen zorgt. Juridische regels die partijen verplichten in geval van een incident bij te springen kunnen de helpende organisatie in de problemen brengen wat op zijn beurt derde partijen kan raken. Voorbeelden hiervan zijn de borgingsarrangementen die spaarders garanderen dat zij hun spaargeld terugkrijgen indien onverhoopt de bank waar zij hun gestald hebben, failliet gaat. Zo ontstaat lange linten van juridische afspraken die maken dat er bij één incident een lange schokgolf door het gehele arrangement gaat. Een voorbeeld daarvan was de 'haircut' in Griekenland in 2011, waarin een groot deel van de Griekse obligaties werd afgeschreven. Er was direct grote discussie over de vraag of dit wel of geen *credit event* was: vanuit het juridisch perspectief is de ene afschrijving de andere niet. In geval van een gewone afschrijving zijn de consequenties beperkt, in die zin dat alleen de obligatiehouders verlies moeten nemen. In geval van de juridische status van 'credit event' worden de 'credit default swaps' geactiveerd, die functioneren als verzekeringen voor de 'default' van de obligatiegever. Die swaps zijn weer verdeeld in heel veel kleine delen en tegen een bepaalde waarde verhandeld door financiële instellingen over heel de wereld. Waarbij bovendien niet op voorhand te zeggen is waar en bij wie ze zijn, er bestaat geen overzichtelijk register van. Zo kan een uiteindelijk zeer lokale en op zich ook overzichtelijke afschrijving op Grieks staatspapier via de credit default swaps over heel de wereld gaan en als een sneeuwbal een nieuwe kredietcrisis in gang zetten. En de bepalende factor daarvoor was uiteindelijk het juridische label van de afschrijving. Uiteindelijk overigens gold de Griekse afschrijving *niet* als een credit event.

Incidenten waar ook ter wereld worden vandaag de dag erg snel wereldwijd bekend. Internet en meer specifiek massa media dragen hier sterk aan bij. Het gevolg hiervan is dat veel partijen na een incident razendsnel reageren. Zij doen wat zij kunnen doen. Zij leggen verklaringen af naar aanleiding van het incident, zij verleggen geldstromen indien zij dat opportuun achten, zij gaan op de vlucht of gaan juist kijken. Waar het hier om gaat is dat heel veel mensen zeer snel horen over een incident waarna een gedeelte hiervan daadwerkelijk tot actie over gaat wat, in tweede instantie, weer tot extra verstoringen kan leiden. Het betekent ook dat betrokkenheid, affiniteit en kennis over incidenten amper meer te maken heeft met fysieke nabijheid. Wel voor de *direct* betrokkenen, maar voor de aandacht ervoor en de 'cascades' van gevolgen gaat het om andere dingen. Sommige natuurrampen gaan letterlijk de wereld over, waar andere onzichtbaar blijven. Voor het ene incident komen direct aandacht en middelen vrij, waar het andere incident bijna onzichtbaar blijft en dus ook amper hulp ontvangt. Zo is koppeling tussen systemen en netwerken dus ook steeds meer een virtueel fenomeen geworden, dat gaat over de zichtbaarheid, invoelbaarheid en over de media waarin wij waarnemen wat elders gebeurt. Zo verandert afstand van een fysieke afstand in een virtuele afstand en is voor de mate van loose of tight coupling uiteindelijk de virtuele afstand bepalen voor de mate van cascade die een incident in gang zet.

3.3 Dimensionering van vernetwerkte risico's

Net als gewone risico's hoeven *vernetwerkte risico's* niet per definitie negatief uit te pakken. De vermenigvuldiging van kans maal effect kan ook hier zowel negatief als positief zijn. Een voorbeeld daarvan biedt het internet. Het internet zoals wij dat nu kennen, is de resultante van een grote verscheidenheid aan interfererende veranderingen waarvan nooit zeker was of en hoe die zouden gebeuren. Internet heeft gezorgd voor allerlei nieuwe gevaren, lasten en kosten, maar brengt per saldo enorme welvaartsgroei. Dat neemt niet weg dat vernetwerkte risico's in het algemeen geassocieerd zullen worden met negatieve en schadelijke effecten en dan zelfs nog een graadje erger dan bij gewone risico's.

Wat dit type risico's bijzonder maakt is dat het niet zozeer betrekking heeft op één mogelijkheid die voortkomt uit één relatie, maar op een veelheid aan mogelijkheden die ontstaat in de interferentie van verschillende relaties. Dat zorgt voor een veelheid aan mogelijke uitkomsten. **Steeds geldt dat wat *vernetwerkte risico's* bijzonder maakt is dat er sprake is van een zekere disproportionaliteit.**

We zijn gewend geraakt aan het idee dat oorzaak en gevolg een bepaalde samenhang hebben. Een bepaalde oorzaak heeft een gevolg dat daarmee min of meer in verhouding is. Een groot gevolg heeft een grote oorzaak, zoals een kleine oorzaak doorgaans een beperkt gevolg heeft. En dat is meer dan alleen een uitdrukking van schaal: het gaat ook om nabijheid, de idee dat oorzaak en gevolg zich in direct contact met elkaar bevinden en dus ook letterlijk bij elkaar in de buurt zijn. Er kan fysieke afstand zijn, maar de causale afstand blijft klein. Oorzaak en gevolg zijn direct bij elkaar te brengen en te herleiden tot concrete aanwijsbare handelingen, besluiten of passiviteit van iets of iemand. Voor *vernetwerkte risico's* geldt dat die relatie veel minder duidelijk is. Er is weliswaar sprake van causaliteit, maar die voltrekt zich in lange(re) causale ketens waarin verschillende schakels aan de orde zijn. En ergens in die keten is er sprake van het 'overhoppen' van een gevolg naar een domein dat er niet direct nabij gelegen is. Een oorzaak werkt bijvoorbeeld via het netwerk veel langer en dieper door dan op basis van de individuele oorzaak logisch was. Of de oorzaak slaat over naar gevolgen in domeinen die er vanuit een sectoraal perspectief eigenlijk nauwelijks iets mee te maken hebben. **Het netwerk produceert interacties die zorgen voor gevolgen die disproportioneel zijn aan de oorspronkelijke aanleiding. Ze reiken verder, zijn groter, duren langer of strekken zich uit tot domeinen waartoe ze logischerwijs niet behoren**. We bespreken hier drie dimensies van *vernetwerkte risico's*, die we illustreren aan de hand van concrete voorbeelden. Het gaat hierbij om: interferentie tussen interne en externe risico's, interferentie tussen technische en sociale systeemrisico's en interferentie tussen korte en lange termijnrisico's.

A. Interferentie tussen interne en externe risico's

De eerste dimensie van waaruit vernetwerkte risico's te begrijpen zijn ligt in de vermenging van interne en externe risico's. Een risico heeft altijd ergens zijn oorsprong. Zo kan een risico onder meer binnen de organisatie huizen of juist van buiten komen. Bij het maken van een reguliere risicoanalyse worden die twee vaak apart genomen. Er zijn interne en externe risico's, die vervolgens in een risicoprofiel bij elkaar worden opgeteld. Een organisatie met een hoog intern risico en een laag extern risico verkeert niet in bijzondere gevaren. Het interne risico moet goed gemanaged worden, maar er is geen bijzondere reden voor zorg. Zo zorgen organisaties vaak voor back-up systemen voor het geval

er een intern systeem uitvalt. Als dat gebeurt, dan kunnen ze toch verder. **Interessant aan vernetwerkte risico's is dat ze de grenzen van intern en extern overschrijden, of dat er onverwachte accumulatie van interne of externe risico's optreedt.**

De kwestie voor de organisatie is dan dat interne en externe problemen zich tegelijkertijd voordoen en de organisatie in dat proces zijn weerbaarheid verliest. De interferentie maakt dat twee afzonderlijke kwesties die ieder op zichzelf te managen zouden zijn toch leiden tot onbeheersbare problemen. Onderstand voorbeeld illustreert dit. Het gaat hier om de DSB Bank, die in 2009 uiteindelijk failliet gaat op een – op het geheel der dingen – toch relatief kleine oorzaak: 'gedoe' over een woekerpolis. Die aanleiding was niet nieuw, bestond al heel lang, en de bank was druk doende om dat incident te managen. Toen raakte het ineens vermengd met een externe ontwikkeling en begonnen die twee processen op elkaar in te werken. De bank verloor zijn geloofwaardigheid en dat proces versterkte zichzelf razendsnel, tot een situatie waarin de bank letterlijk niet meer te redden was.

Begin 2009 raakte DSB Bank in opspraak. Klanten zochten contact met de media nadat zij in de problemen waren geraakt door een hypotheeklening bij DSB Bank. Deze problemen waren ontstaan door een koppelverkoop van overlijdensrisicoverzekeringen en arbeidsongeschiktheidsverzekeringen in de vorm van een of meer koopsompolissen. De koopsom werd aan DSB betaald uit een verhoging van de hypotheeklening. Ondanks de hogere hypotheek leken de maandlasten in eerste instantie mee te vallen, de klanten van DSB gingen hierbij af op de in reclame en/of promotie vermelde (lagere) hypotheekrente voor de beginperiode. De lage hypotheekrente was echter van korte duur, al snel (gemiddeld na één jaar) werd conform het contract de rente verhoogd.

Op 1 oktober 2009 om 7.45 uur deed Pieter Lakeman van de Stichting Hypotheekleed een oproep in het KRO-programma Goedemorgen Nederland. Hij riep alle rekeninghouders op om hun tegoeden bij DSB Bank weg te halen: 'DSB moet failliet', aldus Lakeman. Volgens hem was dat de enige manier voor gedupeerden om nog wat van hun geld terug te krijgen, omdat dan een curator de zaak eerlijk zou afhandelen. De oproep van Lakeman trok veel aandacht in de media. De bank was kwetsbaar omdat veel kort spaargeld was aangetrokken om langlopende hypotheken te dekken. Tien dagen na de oproep van Lakeman bleken de problemen bij DSB aanzienlijk. In drie dagen hadden rekeninghouders 317 miljoen opgenomen, hetgeen was opgelopen tot 664 miljoen op het moment dat de rechtbank tot een noodregeling besloot.

Op zondagavond 11 oktober 2009 om 19.00 uur heeft De Nederlandsche Bank een verzoek ingediend bij de rechtbank te Amsterdam om op de DSB Bank de noodregeling als bedoeld in de Wet op het financieel toezicht (Wft) van toepassing te verklaren. Minister Wouter Bos van Financiën was die nacht urenlang op het hoofdkantoor van DNB. Dit bezoek van Bos en de commotie binnen DNB is kennelijk uitgelekt naar de pers. Het verzoek van DNB werd in eerste instantie (maandag 12 oktober om 01.00 uur) afgewezen. Volgens de rechtbank was de situatie weliswaar zorgelijk maar had de bank nog voldoende liquide middelen. In de ochtend van 12 oktober werd de aanvraag van DNB alsnog gehonoreerd. De rechtbank verklaarde de noodregeling van toepassing en bepaalde de duur op anderhalf jaar. Tevens werden direct twee bewindvoerders aangesteld, die vanaf dat moment de bedrijfsvoering overnamen. In deze beschikking werd door de rechtbank gesteld: "De liquiditeit van DSB ontwikkelt zich

> thans op gevaarlijke wijze en er is geen vooruitzicht op verbetering van die ontwikkeling". Door berichten in de pers was er nl. vanaf 05.00 uur opnieuw een bankrun op gang gekomen (ongeveer 30 miljoen op maandagochtend). Op verzoek van de bewindvoerders heeft de rechtbank DSB Bank op 19 oktober 2009 failliet verklaard. [28]

Op zich was de problematiek met de woekerpolissen en een zekere ontevredenheid van groepen klanten voor DSB niets nieuws. Het bedrijfsmodel hield er tot op zekere hoogte ook al rekening mee, aangezien een aantal producten van de bank expliciet inspeelden op een voor klanten moeilijk te doorgronden verdienmodel. Het bedrijfsmodel van DSB kende het risico dat klanten na enige tijd ontevreden zouden worden, omdat na lage beginkosten de kosten zouden toenemen. Dit externe risico van ontevredenheid, klachten, klachtprocedures en compensaties was op zich beheersbaar. Met ontevreden klanten valt te praten en desnoods zijn ze in ieder geval gedeeltelijk te compenseren voor schade. DSB liep extern het nodige risico, maar het leek een ieder sterk dat daarmee de bank in zijn grondvesten zou worden aangetast. Daarnaast was er een tweede risico, namelijk dat DSB veel kort geld had aangetrokken om langlopende hypotheken te dekken. DSB had hiermee een weloverwogen marktrisico genomen en ook dit was in de systemen bekend en op zich beheersbaar. Maar toen kwamen daar de andere externe risico's bij. Eerst was er de oproep van Lakeman, die plots de groep ontevreden klanten een collectieve stem gaf en hen bovendien een voor de bank in potentie destructief instrument in handen gaf: ineens behoorde de *bankrun* tot de mogelijkheden. Die zorg werd ineens meer reëel toen het tweede risico zich voordeed, namelijk dat er bedoeld of onbedoeld het beeld werd gevestigd dat er bij DSB 'iets aan de hand was'. Het uitlekken van het gerucht dat minister van Financiën Bos in noodberaad was bij de DSB was hier de trigger. Ineens werd de bankrun realiteit, en zoals we weten van bankruns zorgt dat er voor dat het proces niet meer te stoppen is. Die ontwikkeling bleek teveel voor het strak gefinancierde model van DSB, dat kort daarop bezweek. Niet omdat het model zelf te kwestbaar was voor enkelvoudige risico's, maar wel doordat het niet opgewassen was tegen de cocktail van gebeurtenissen die uiteindelijk de bankrun inzette. Het bracht Scheringa er in ieder geval toe om in de persconferentie over het faillissement aan te geven dat de bank tot zinken was gebracht en niet zelf was verdronken. Hij had er tot op zekere hoogte ook gelijk in, alleen niet op de manier die hij zelf bedoelde. DSB was niet door Bos, andere banken of DNB geliquideerd, maar werd het slachtoffer van een reeks op elkaar inwerkende ontwikkelingen die ieder voor zich nooit sterk genoeg waren geweest om de bank te laten vallen.

Een ongeluk komt nooit alleen, zegt men wel eens en in deze categorie is dat waar het op uitdraait. Technische installaties bijvoorbeeld worden ontworpen om bepaalde rampen te weerstaan. Ze zijn bestand tegen een aardbeving, een inslag van een vliegtuig, een bomaanslag en een vloedgolf. Maar hoe zit het met de combinaties van die externaliteiten? De ramp in Fukushima illustreert hoe lastig het is als een installatie wordt getroffen door twee zware rampen die ieder op zichzelf zijn 'ingeboekt' om eens per 500 jaar te gebeuren – en niet tegelijk.

> De kernramp in Fukushima, Japan was het gevolg van een zeebeving bij Sendai en de daarop volgende tsunami van 11 maart 2011. De drie operationele reactoren in de centrale werden binnen enkele seconden na het begin van de aardbeving automatisch stilgelegd door middel van een noodstop. Dat was een standaard-procedure die het risico bij een zware aardbeving

[28] Wikipedia

moest verkleinen. Het gewone elektriciteitsnet was beschadigd en daarom moesten de koelpompen voor de centrales draaien op elektriciteit van een noodstroomvoeding. Maar door de tsunami, die op de aardbeving volgde, kwamen deze generatoren onder water te staan en werkten ze niet goed meer. De koeling op accu's stopte na enkele uren doordat de accu's leeg waren. Er volgde een serie ongelukken in verschillende reactoren in het complex, waaronder explosies van waterstofgas. In enkele reactoren heeft ook een kernsmelting plaatsgevonden: brandstofelementen zijn gedeeltelijk gesmolten en kernbrandstof is op de bodem van de reactoren terechtgekomen.

Hoewel maatregelen om de kerncentrale tegen een aardbeving te beschermen goed hadden gefunctioneerd, bleken maatregelen om de centrale tegen een hoge vloedgolf te beschermen onvoldoende. Bij de bouw werd er rekening gehouden met een mogelijke vloedgolf van 5,7 meter hoog, de vloedgolf was echter waarschijnlijk meer dan 14 meter hoog. Door de vloedgolf ontstond er schade aan de gebouwen en raakten de noodaggregaten op één na buiten werking.[29] Eenmaal in gang gezet bleek er geen houden meer aan. Ook al omdat niet alleen de kerncentrale maar een groot deel van het land zwaar getroffen waren was het bovendien bijna onmogelijk om snel met adequate 'containment'-maatregelen te beginnen.

Hier interfereerden twee externe, onwaarschijnlijk geachte incidenten, te weten een extreem zware zeebeving en een extreem hoge vloedgolf. Deze twee incidenten samen vernietigden de interne reguliere systemen en de noodsystemen, met desastreuze gevolgen. De organisatie werd pas echt getroffen doordat dit externe incident interfereerde met interne risico's, maar dat is in zekere zin altijd het geval. Immers, een organisatie kan pas getroffen worden door een extern risico indien het uiteindelijk ook aangrijpt op een intern risico. Indien dat interne risico zou ontbreken zou de organisatie onkwetsbaar zijn, wat onmogelijk is.

Let wel, het risico is hier buiten de organisatie ontstaan. Maar de grens tussen intern en extern kan ook elders, breder, worden getrokken. Tussen economische sectoren of tussen domeinen in het algemeen bijvoorbeeld. Stel de elektriciteit valt uit als gevolg waarvan het internetverkeer stilvalt waarmee e-bankieren onmogelijk wordt. Een probleem in het energie domein springt over naar internet en springt vervolgens weer over naar de financiële sector. Of denk aan een ziekte die altijd alleen overdraagbaar leek tussen dieren blijkt ineens besmettelijk te zijn voor mensen. Dit gebeurde met BSE en met Q-koorts. Ook hier springen risico's van de ene sector naar de andere sector waar ze grote schade kunnen aanrichten. Juist omdat alle veiligheidssystemen het perspectief van de ene sector of het domein hanteren ontstaat bij het 'overspringen' van risico's meteen grote problemen.

Bij de interferentie van risico's kan ook spelen dat een aantal interne processen die ieder op zichzelf nog wel te managen zijn, in combinatie zorgen voor nieuwe en veel moeilijker beheersbare risico's. Bijvoorbeeld als een proces dat eerst maakte dat een bepaald risico beheerst werd zelf ook wordt veranderd en het wegvalt. De betekenis ervan voor de organisatie wordt mogelijk pas duidelijk als het te laat is en het andere risico zich voordoet. Het onderstaande voorbeeld illustreert in dat opzicht een interferentie van interne risico's. In dit geval gaat het om twee reorganisaties, waarin de tweede reorganisatie betekent dat een mogelijkheid voor herstel van bepaalde schade uit de eerste reorganisatie wordt weggenomen. Op zichzelf kunnen beide reorganisaties op zichzelf niet zo heel

[29] Wikipedia

veel kwaad en lijken er voldoende veiligheidskleppen aanwezig. In tweede instantie blijken ze precies door hun interferentie uit te monden in een gevolg dat de oorspronkelijke aanleiding sterk ontstijgt.

> Een commerciële organisatie introduceert een nieuw integraal business system dat geïntegreerd rapporteert over slaagkansen van offertes, voortgang van projecten, gemaakte uren op het project en projectresultaat. Het systeem produceert o.m. zelf facturen. Het nieuwe systeem geeft een andere inschatting van projectresultaten dan de oude manier van werken. Indien het systeem goed werkt en de medewerkers gaan er goed mee om, dan geeft het een beter beeld van de stand van zaken in de projecten, van de hoeveelheid werk die er is en van de financiële positie van de onderneming als geheel. Het risico bij de introductie van het systeem is dat medewerkers er nog mee moeten leren werken en dat ze veel beter en nauwkeuriger en sneller dan voorheen moeten rapporteren over wat ze hebben gedaan in een project en hoe de gemaakte uren zich verhouden tot de begrote uren, in relatie tot de voortgang van het project.
>
> Stel nu eens dat tegelijkertijd met de introductie van dit systeem een reorganisatie plaatsvindt. De organisatie wordt gekanteld en er komen nieuwe leidinggevenden. Deze nieuwe leidinggevenden missen de ervaring van hun voorgangers die door hun jarenlange ervaring in staat waren uit weak signals en kleine indicaties conclusies te trekken over of het wel of niet goed gaat met de organisatie.
>
> De risico's van de beide veranderingen kunnen maar al te gemakkelijk interfereren. Bijvoorbeeld: het systeem wordt de eerste maanden slecht ingevuld. Onwennigheid en onwetendheid zijn de belangrijkste oorzaken, maar een additionele oorzaak is dat leidinggevenden meer gericht zijn op de reorganisatie en wat die voor henzelf gaat betekenen dan dat ze bezig zijn hun medewerkers aan te sporen hun urenbriefjes adequaat in te vullen en het systeem goed te voeden. Het gevolg is dat de prognoses die het systeem genereert, niet deugen. Ook worden er minder facturen geproduceerd dan mogelijk zou zijn gezien het werk dat gedaan is. De leiding van de organisatie ziet de inkomsten dalen maar weet niet goed wat de oorzaak is. Is er minder werk gedaan? Of is er veel werk gedaan, maar is de factuur nog niet geproduceerd vanwege het onvolledig invoeren van data? En wat is de betekenis van de werkvoorraad die er zou zijn volgens het systeem? Hoe verhoudt deze zich tot de data waar men gewend is mee te werken. De leiding kan geen beroep meer doen op ervaren leidinggevenden die wellicht op grond van hun tacit knowledge zouden kunnen zien wat er aan de hand is. De problemen met de facturering brengen de organisatie aan de rand van de afgrond, omdat de kasstroom tot stilstand komt en er binnen korte tijd liquiditeitsproblemen ontstaan. De organisatie is niet in de problemen door een gebrek aan kracht in de markt, of gecontracteerde omzet, maar door een combinatie van interne administratieve processen. Secundaire processen brengen in korte tijd de organisatie in grote problemen.

B. Interferenties tussen technische en sociale systeemrisico's

Vernetwerkte risico's manifesteren zich waar risico's van technische en sociale systemen met elkaar interfereren. Er zijn risico's die zich voordoen zonder dat er interventies van mensen of organisaties aan te pas komen. Denk aan een aardbeving of een andere natuurramp. Aan de andere kant zijn er ook risico's die in principe losstaan van fysieke of technische systemen. Een conflict tussen mensen

of organisaties kan daarvan het voorbeeld zijn. Bij *vernetwerkte risico's* werken beide op elkaar in. Een crisis op de beurs biedt hiervan een mooie illustratie.

Wat vernetwerkte risico's waarin zowel technische als sociale systemen betrokken zijn, zo ingewikkeld maakt is dat ze niet volgens een overeenkomstige logica hoeven handelen. Technische systemen werken langs de lijnen van natuurwetten of in ieder geval volgens een voorgeprogrammeerde lijn: een aardbeving zet een tsunami in, die vervolgens een bepaalde kracht heeft die de beschermingswal van de reactor wel of niet wegvaagt. Bij sociale systemen ligt dat anders. Zij reageren via een complex proces van betekenisgeving, waarbij ze zich afvragen wat er aan de hand is, welke intenties de anderen hebben, ze een beperkt beeld hebben van de mogelijke handelingsopties én ze daarbinnen volgens vaak onoverzichtelijke patronen voorkeuren ontwikkelen. Ze denken na over wat er speelt en stemmen af over wat er aan de hand is en wat er onder de omstandigheden mogelijk is, maar op een beperkte wijze. Ze proberen hun weg te vinden in de ambiguïteit van de situatie en van daaruit opties te ontwikkelen die het goed zouden kunnen doen.

Ingewikkeld aan vernetwerkte risico's is dat deze beide logica's elkaar ontmoeten en met elkaar interacteren. Een voorbeeld daarvoor bieden de moderne beurzen. Op deze beurzen zijn als vanouds handelaren actief die gebeurtenissen observeren, zich bewust zijn van risico's en soms actie ondernemen, dat wil zeggen *kopen* en *verkopen*. Om deze handelaren werk uit handen te nemen zijn algoritmes ontwikkeld die opdracht geven om te kopen en te verkopen indien de koersen bepaalde waarden halen. Er zijn zelfs algoritmes die nieuwssites scannen op bepaalde woorden met voor de beurskoers positieve of negatieve associaties waarna aankoop of juist verkoopopdrachten volgen. Wereldwijd wordt inmiddels meer dan 70 procent van de aandelen verhandeld via algoritmes. Deze programma's reageren razend snel en massaal op bepaalde gebeurtenissen wat ook weer tot reacties kan leiden van handelaren. Een explosief mengsel, waarin de systemen soms letterlijk op hol slaan en tegen elkaar opbieden op een manier die de markt heel sterk beïnvloedt. Zo kunnen kleine schommelingen leiden tot grote uitslagen in koersen, die weer een zichzelf versterkend effect hebben.

C. Interferentie tussen korte en lange termijnrisico's

De factor tijd is eveneens belangrijk voor het doorgronden van de dimensies die verbonden zijn met vernetwerkte risico's. Sommige risico's bouwen zich geleidelijk op. Er is tijd voor observatie en analyse. De organisatie kan zich voorbereiden op wat er gebeurt of er tijdig op reageren. Andere risico's ontstaan acuut en ontwikkelen zich razendsnel tot incident. Via het netwerk kan plotselinge versnelling of vertraging optreden, die maakt dat ontwikkelingen en effecten lastiger te voorzien zijn. En dat maakt het omgaan met vernetwerkte risico's ingewikkeld. Andersom geldt hetzelfde ook voor de aanpak van risico's en incidenten. Ook hier treden op het eerste gezicht onverklaarbare versnelling en vertraging op. Sommige incidenten vereisen een snelle aanpak, om erger te voorkomen. Andere incidenten bieden meer tijd, soms zelfs zo veel tijd dat interventies getest kunnen worden op hun effectiviteit zodat na een serie van maatregelen de beste interventie geselecteerd kan worden. Soms zorgt het netwerk voor een enorme hefboom in de aanpak en neutraliseert een incident sneller dan verwacht. Soms werkte het andersom en loopt een op beheersing van het risico of incident letterlijk vast in het netwerk. Het netwerk kan de oplossing bespoedigen maar ook vertragen. Steeds geldt hier dat het netwerk niet alleen de *achtergrond* is waartegen interacties plaatsvinden, maar dat de tijd zelf van invloed is op de ontwikkeling van de risico's, het incident of de aanpak.

Als we tijd uitdrukken als *afstand* dan kun je zeggen dat in netwerken de afstand meer variabel en veranderlijk wordt. Tijd is dan niet meer lineair, maar werkt met versnellingen of vertragingen die elkaar afwisselen. Neem bijvoorbeeld de introductie van elektrische auto's. Dat kan een proces zijn waarin druppel voor druppel de emmer heel langzaam volloopt. Tegelijkertijd kan het ook door interacties in het netwerk heel anders uitpakken. Als er eenmaal enkele op de weg zijn en bepaalde mensen op knooppunten in het netwerk worden er enthousiast over, dan kan ineens een hele groep overstappen. Dat hoeft niet eens het effect te zijn van nieuwe maatregelen of een bepaald nieuw model, maar gebeurt dan 'gewoon' door interne dynamiek in het netwerk. En zodra er eenmaal een versnelling optreedt wordt de elektrische auto steeds meer 'normaal', wat ook weer zorgt voor nieuwe versnelling. Mensen zien het niet meer als afwijkende keuze, maar juist als het gewone om te doen. Zo kunnen de bijzonder ambitieuze doelen voor de aantallen elektrische auto's op de weg in 2020 alleen worden gehaald als er ergens een grote versnelling optreedt. Normaliter, via lineaire causale relaties is dat eigenlijk niet mogelijk, maar het kan zijn dat er via de dynamiek in het netwerk ineens momentum ontstaat. Eerder hebben we het gezien in de telecom en bij social media websites, die op een moment door een 'tipping point' heen breken waardoor het gebruik ineens explodeert. Tegelijkertijd zien we ook dat het netwerk andersom ineens een gevestigde realiteit heel snel kan afbreken. Het gebruik van een voorziening komt door interacties in het netwerk ineens geheel tot stilstand, zonder aanwijsbare aanleiding. Onderstaande tabel brengt de verschillen in beeld.

	Netwerk ***vertraagt* de aanpak**	Netwerk ***versnelt* de aanpak**
Netwerk ***versnelt* de verspreiding**	De 'Bulgarenfraude' is een vorm van uitkeringsfraude die zich via netwerken heel snel over een zeer grote populatie uitspreidde. Het idee op zich was niet nieuw en in zekere zin ook ingecalculeerd in het design van de toeslagenregeling. Wat niet verwacht was, was dat bendes 'bulgaren' zo snel zulke grote aantallen deelnemers zouden weten te mobiliseren. Via het netwerk explodeerde de omvang van de fraude enorm. Vervolgens bleek het bijna onmogelijk om de fraude te herstellen en daders op te sporen. Via het netwerk worden zij onzichtbaar voor de opsporing en dankzij het netwerk kunnen de fraudeurs snel informatie uitwisselen over hoe ze de opsporingsambtenaren kunnen ontlopen.	De SARS-epidemie verspreidde zich snel via intercontinentaal vliegverkeer. Zo groeide het incident heel snel uit van een lokale nieuwe variant van een virus, naar een 'global outbreak' van pandemische proporties. Vervolgens lag in samenwerkende netwerken – snelle uitwisseling en bundeling van onderzoek, afgestemde rampenbestrijding, communicatie – wel de basis voor de bestrijding. Bijvoorbeeld in detectie van nieuwe besmettingen, geïmproviseerde quarantaines en de communicatie met getroffenen. De uitbraak versnelde via het netwerk, maar werd mede middels de kanalen van het netwerk ook getemd.
Netwerk ***vertraagt* de verspreiding**	Door het steeds meer openstellen van data kan het publiek beter en tijdiger zien welke ontwikkelingen er in een domein zijn. Bijvoorbeeld hoe de kwaliteit van het onderwijs op een school is. Ze kunnen daardoor zelf aan de bel trekken en de school corrigeren, waardoor de reactietijd bij kwaliteitsverlies veel korter is. Zo vertraagt het netwerk het risico van snel groot kwaliteitsverlies in het onderwijs. Tegelijkertijd bemoeilijkt het netwerk ook de aanpak van verlies van onderwijskwaliteit. Scholen maken deel uit van complexe netwerken waarin interventies van de Inspectie soms heel snel uitdoven in interacties tussen partijen.	Crisis-communicatie: via social media worden mensen gewaarschuwd om de plaats van de ramp te mijden en lukt het om sneller bekenden te lokaliseren of het probleem scherp te krijgen.

Een volgend complicerend element van vernetwerkte risico's is de uiteenlopende tijdshorizon en tijdsbesef van partijen. Partijen opereren allemaal in dezelfde kloktijd – hooguit in andere tijdzones – maar tegelijkertijd is de klok niet bepalend voor hoe de temporele dimensie door betrokkenen wordt beleefd. Voor de één is een procedure kort en snel, waar hij voor een ander vanuit een andere context heel anders overkomt: dat duurt erg lang, veel langer dan nodig. I**n netwerken komen personen, organisaties en systemen met uiteenlopend tijdsbesef – met een andere gevoelde klok – met elkaar in aanraking. Het verschillende tijdsbesef kan gevolgen hebben voor hoe risico's zich ontwikkelen en voor hoe ze worden ingeschat.** De financiële crisis heeft gezien hoe het omgaan met grote financiële verliezen en afschrijvingen meteen de verschillen in tijdoriëntatie op scherp zet. Pensioenfondsen dachten zich vooral te concentreren op lange termijn rendement en houdbaarheid, waardoor men minder gevoelig was voor korte termijn schommelingen. Totdat de korte termijn verliezen zo groot werden dat ook het lange termijn pad ter discussie kwam te staan, doordat fondsen collectief door de dekkingsgraden zakten. Dat maakte een voor alle betrokkenen ongemakkelijke afweging los waarin korte termijn belangen tegenover lange termijn komen te staan. Dat kan zomaar leiden tot een volgend – en veel groter – risico voor pensioenfondsen, namelijk dat met name de jongeren er uit proberen te blijven. Zolang de fondsen geen nieuwe instroom hebben, of zelfs te maken krijgen met uitstroom van jongeren is het lastig om het fonds op niveau te houden. De discussies over tijdhorizon en de lange termijn effecten van maatregelen die op de korte termijn tot resultaat moeten leiden zorgen er zodoende voor dat er voor de pensioenfondsen een belangrijk nieuw risico is ontstaan: het risico van het verlies van draagvlak en steun voor de gedachte van collectief sparen voor pensioen.

Een ander voorbeeld van divergerend tijdsbesef en van uiteenlopende tijdhorizon is een bedrijf dat te maken krijgt met activistische aandeelhouders. Het bestuur denkt te werken aan een zorgvuldig intern afgestemde strategie van behoedzame groei en neemt de tijd om het bedrijf sterk te maken. Tegelijkertijd zijn er activistische aandeelhouders die de beperkte aandeelhouderswaarde agenderen en eisen dat het bedrijf nu meer waarde aan investeerders uitkeert. Ze zijn niet geïnteresseerd in de lange termijn, maar willen nu bediend worden. Ze vinden bovendien gehoor bij een aantal op korte termijn incentives afgerekende managers in de organisatie die ook liever zien dat het bestuur zich meer op het heden gaat richten. De lange termijn is leuk, maar je kunt er niet van leven, wordt in de wandelgangen gefluisterd. Zo ontstaan in de organisatie letterlijk wisselende snelheden die zorgen voor nieuwe dynamiek. Door de netwerkcontext die organisaties steeds meer geworden zijn is het bijna onmogelijk om de tijdhorizon te stroomlijnen en te synchroniseren. Het is steeds meer een kwestie van het omgaan met verschillende snelheden en perspectieven en het tijdig herkennen waar 'gewoon' de belangen uiteen lopen en waar uiteenlopend tijdsbesef aan de orde is.

Nog een complicerend element van vernetwerkte risico's dat samenhangt met tijd is het verschil in tempo tussen het risico enerzijds en de aanpak ervan anderzijds. Onderstaande tabel toont de vier conceptueel te onderscheiden varianten.

	***Geleidelijke* aanpak mogelijk/ reactie als te bespreken mogelijkheid**	***Hoge snelheid* in aanpak vereist/ reactie moet in real time plaatsvinden**
***Geleidelijk* hoger wordend risico/ incident ontstaat geleidelijk**	Klimaatverandering	Power failure met kans op uitval internet, bancaire diensten etc
***Snel* hoger wordend risico/ acuut incident**	Oliecrisis in 1972	Financiële risico's

Een eerste type risico kent een geleidelijke aanloop en biedt tevens tijd om het probleem op te lossen. Het is dus vooral een kwestie van lange adem, waarin er de nodige tijd is om een nog onduidelijk, want ontwikkelend, risico van een adequaat antwoord te voorzien.

> Klimaatverandering is een probleem dat langzaam ontstaat, in feite over een periode van decennia. De situatie wordt slechter en slechter maar van een acute mondiale ramp is geen sprake. Maatregelen om de oorzaak aan te pakken (reductie uitstoot broeikasgassen) en adaptie maatregelen kunnen ook in enige rust worden genomen.

Ondanks dat er dus behoorlijk wat reactietijd is, is het zeker niet gezegd dat dit risico eenvoudiger te managen is. Het 'risico van dit type risico' is dat de urgentie altijd laag is en dat de aanpak van acute risico's en incidenten iedere keer weer voorrang krijgt. Zo is het lastig om de aandacht vast te houden en toch nog tijdig te beginnen. Dat leidt er toe dat ook voor dit type over een lange tijd uitgestelde risico's er toch nog tijdnood kan ontstaan. Een voorbeeld van dat laatste is de voorbereiding op de vergrijzing, waar ondanks de al decennia voorzienbare demografische ontwikkeling toch pas heel laat is begonnen met pensioenhervormingen. In die zin is het risico van de traagheid hier vooral een kwestie van de aankap van het risico: lukt het om voldoende urgentie te mobiliseren om tijdig te beginnen – juist als het risico in de tijd nog ver weg is.

Een tweede type probleem is een snel escalerend risico waarna voor de oplossing wel weer enige tijd beschikbaar is. Het risico groeit snel uit, maar er zijn door bepaalde voorbereidingen of kenmerken van het risico mogelijkheden om het antwoord nog even uit te stellen. De crisis komt dan in volle hevigheid op, maar doordat er buffers en reserves zijn – fysiek, economisch, in termen van reputatie – kunnen partijen nog even wachten met reageren. Daarmee ontstaat een 'waiting game' waarbij partijen wachten tot een ander in beweging komt. Vaak neemt wie als eerste beweegt de meeste kosten op zich en loopt deze partij het grootste risico. Meer reactietijd levert zodoende nieuwe strategische dilemma's op en kan ook betekenen dat er uiteindelijk alsnog tijdnood ontstaat. Tegelijkertijd is de positieve variant van de vorm natuurlijk dat partijen door voorzienig beleid net wat meer tijd hebben om een adequaat antwoord te formuleren op de crisis die hen treft. Ze kunnen bijvoorbeeld verbindingen met elkaar aangaan om met een gezamenlijk antwoord te komen. Dat kan ook als de crisis acuut is, maar nu is er meer ruimte voor reflectie en nadenken over de mogelijke oplossingen.

> In 1973 had een Arabische coalitie de Grote Verzoendag (Jom Kippoer) uitgekozen om Israel binnen te vallen. Even zag het er naar uit dat Israel zou bezwijken onder de Arabische druk. Maar er kwam hulp in de vorm van een luchtbrug die wapens van de VS aanvoerde en er kwam ook steun van Westerse landen zoals Nederland. Uit solidariteit met de Arabische landen begon de OPEC (organisatie van olie-exporterende, Arabische landen) traag maar zeker de oliekraan dicht te draaien. De uitvoer naar landen die werden verdacht van medewerking met Israel werd drastisch beperkt, met als gevolg schaarser wordende olie en een stijging van de prijs. In 1972 was de prijs nog 3 dollar per vat van 159 liter, maar tegen het einde van 1973 was dat al meer dan 7 dollar.
>
> Na de inval in Israël besloot op 18 oktober 1973 de OAPEC (de vereniging van alleen Arabische olieproducerende en -exporterende landen), om zonder overleg met de oliemaatschappijen eenzijdig de olieprijs met 70% te verhogen. Bovendien werd besloten om de productie van ruwe olie met telkens 5% per maand te verminderen: 'Totdat Israël zich uit alle bezette

Arabische gebieden heeft teruggetrokken en de rechten van het Palestijnse volk in ere zijn hersteld'. 'Landen die de Arabische zaak steunen' kregen een speciale voorkeursbehandeling. President Nixon, van de Verenigde Staten, zei op 19 oktober 1973 aan Israël omvangrijke militaire steun toe. Dat was voor Libië, Abu Dhabi en Saoedi-Arabië reden om twee dagen later alle olieleveranties aan de Verenigde Staten stop te zetten. De olieboycot was een feit. Ook Nederland werd door de boycot getroffen. Algerije besloot op 20 oktober 1973 tot een volledig stopzetting van de olietoevoer aan Nederland, gevolgd door Koeweit en nog 6 andere Arabische landen. Saoedi-Arabië volgde op 30 oktober. Voor het Botlek/Europoortgebied, waar vijf olieraffinaderijen waren gevestigd, leek de boycot een katastrofe: 54% van de Nederlandse olieaanvoer kwam uit Saoedi-Arabië en Koeweit. In Europa en in de VS leidden de prijsstijgingen van de OPEC in de jaren 1972-1973 o.a. tot dreigende schaarste aan benzine. De Nederlandse regering nam maatregelen, waarvan de twee voornaamste waren de autoloze zondagen en rantsoenering van benzine d.m.v. een systeem met bonnen

Bij Shell en bij de andere oliemaatschappijen waren de opslagtanks van ruwe olie vol. Ze hadden er immers al rekening mee gehouden, dat de prijs van ruwe aardolie exorbitant zou stijgen. Al voor de crisis werden de opslagtanks met zoveel mogelijk nog goedkope olie gevuld. In de maanden voor de sterke prijsstijging en de boycot was er een grote aanvoer van ruwe aardolie. De schaarste aan olieproducten, zoals benzine, werd door de oliemaatschappijen zelf veroorzaakt. Zij hielden er rekening mee, dat na de prijsstijging van aardolie, ook de prijs van olieproducten (hun afzetproduct) zou stijgen. Ze klaagden over lage prijzen voor olieproducten (benzine, nafta, ethyleen, enz.) en over de hoge vervoerskosten: stookolie voor tankers. Hun zorg betrof de winstmarge.

De werkelijkheid was anders dan de oliemaatschappijen aan de overheid lieten weten. Een vermindering van de aanvoer kon niet eerder dan eind november/begin december merkbaar zijn: 5 á 6 weken na het instellen van de boycot: de tijd die olietankers nodig hadden om na belading hun bestemming te bereiken. De kapiteins van de olietankers ontvingen hun bestemming soms pas in volle zee en die kon later nog gewijzigd worden. Voor de Arabische landen was het moeilijk om de bestemming van de schepen te controleren. Chevron Petroleum Maatschappij Nederland ving de stagnerende aanvoer uit Saoedi-Arabië (80 % van hun aanvoer) en uit Libië (10% van hun aanvoer) op door een grotere aanvoer uit andere landen. Voor andere oliemaatschappijen, die minder afhankelijk waren van Saoedi-Arabië en Koeweit, zoals Shell, Esso, BP en Gulf, was het gemakkelijker om te switchen. Zij hadden meer raffinaderijen in Europa. In februari 1974 kwam er minder ruwe olie uit Saoedi-Arabië en Koeweit, maar meer uit andere olielanden.[30]

De oliecrisis en boycot mogen dan vrij snel en onverwacht manifest zijn geworden. Door voorraden en door de sleutelposities van andere partijen dan de boycottende landen vielen de effecten mee en was er tijd beschikbaar om alternatieve oplossingen te ontwikkelen die de negatieve effecten sterk temperden. Zo kon een in potentie enorme bedreiging voor het internationale systeem uiteindelijk toch relatief gemakkelijk worden opgevangen. Het is de vraag hoe dat in het hedendaagse economische en politieke netwerk zou gaan.

[30] Wikipedia

Voor een derde type risico geldt dat de aanloop naar het probleem wellicht enige tijd kan duren, maar als het incident er eenmaal is, dan moet er heel snel worden ingegrepen. Partijen voorzien dat een risico er steeds meer aan zit te komen, kunnen er nog weinig aan doen, maar weten tegelijkertijd dat als het zover is zij meteen in actie moeten komen. Het is als met de eerste hulp of oefenen voor een crisissituatie. Als het zover is dan moet het snel en goed, liefst in één keer. Er is geen tijd meer voor discussie, nadenken of reflectie, er moet gehandeld worden. Let wel, dat hoeft dus niet te gaan over een klein deel van een systeem, zoals een woning die afbrandt of een ziekenhuis dat een probleem heeft. Het kan juist ook gaan om de onderliggende infrastructuur. Dus niet één ziekenhuis, maar een heel cluster of een onderliggende voorziening die maakt dat een hele reeks ziekenhuizen en andere instellingen niet meer goed kunnen functioneren. Het gebeurt niet vaak, maar als het gebeurt is het nodig om meteen te reageren.

> Een elektriciteitsnet wordt gedurende jaren steeds zwaarder en intensiever benut en langzamerhand raakt overbelast. Dit kan resulteren in een toch nog onverwachte uitval van elektriciteit die lang dreigt te duren en het internet uitschakelt, waardoor internet bankieren niet mogelijk is. Dit incident zou een buitengewoon verstorende werking hebben op het dagelijkse zakelijke betalingsverkeer en, onder gevoelige condities, tot een vertrouwenscrisis leiden. Het voorkomen van de stroomuitval zou zeer snelle interventies vragen en ook, nadat het incident er is, is snelle actie vereisen om erger te voorkomen.

Het meest tijd-kritisch zijn risico's die zeer snel in omvang groeien en waarvan de aanpak ook een snelle, real time oplossing vraagt. Het risico ontwikkelt zich snel en verandert gaandeweg mogelijk nog van vorm. Ondertussen moet er een aanpak gevonden worden die de actuele onrust te lijf gaat, het momentum tot stilstand brengt en het begin van een meer duurzame oplossing biedt. De financiële crisis is daarvan natuurlijk een ultiem voorbeeld.

> Voor een aantal financiële risico's geldt dat ze het gevolg zijn van langjarige verwaarlozing van problemen. De zwakke balansen van banken en de verslechterende financiële positie van landen, zijn al jaren zichtbaar. Op enig moment lijken de problemen een kritisch punt gepasseerd waarna de problemen in heel hoog tempo toenemen en onbeheersbaar worden. Er moet dan erg snel worden geïntervenieerd. Vergelijk Klaas Knot directeur Nederlandse Bank over het controversiële plan van de ECB om ongelimiteerd staatsobligaties op te kopen: Er zijn.".. momenten waarop financiële markten irrationeel handelen en waarop sprake is van collectief vertrouwensverlies. Dan creëert de snelheid waarmee rentes < van landen> oplopen een wanordelijkheid waarmee ook het democratisch proces wordt doorkruist…. Op zo'n moment is snelheid essentieel omdat je de geest niet uit de fles wilt halen. We wilden die ontwikkeling in de kiem smoren, want als de rentes eenmaal boven de acht, negen, tien procent komen, dan krijg je ze heel moeilijk weer terug.[31]

Dit soort risico's die tijdkritisch zijn en om een snelle real-time oplossing vragen lijkt in omvang toe te nemen, mede als gevolg van het toenemend vernetwerkte karakter van de samenleving waardoor actoren en systemen steeds meer en steeds indringender met elkaar verbonden zijn. Dit maakt dat gebeurtenissen en berichten zich razendsnel kunnen verspreiden en grote effecten kunnen hebben. *Social media* en meer algemeen internet zijn belangrijk dragers van deze informatiestromen. In de

[31] In: Financieel Dagblad 6 oktober 2012.

financiële wereld heeft dit geleid tot omvangrijke stromen flitskapitaal en tot gevaarlijke en verstorende virtuele *bankruns*. Steeds geldt daarvoor dat een ontwikkeling plots opkomt, dan versnelt en overslaat naar andere domeinen of sectoren, waarbij de druk op een snelle interventie sterk toeneemt. Die interventie is vervolgens bijna per definitie ingewikkeld, want moet een snel antwoord bieden, onder hoge druk, en met medenemen van een veelheid aan partijen. Dat was ook precies wat veel mensen ten tijde van de financiële crisis angst inboezemde: enerzijds de mogelijkheid tot snelle totale instorting van het financiële systeem, maar anderzijds ook het relatieve onvermogen van overheden om daar snel en adequaat op te reageren. Geruststellend – tot op zekere hoogte - is dan wel weer om achteraf toch ook de veerkracht van het systeem vast te stellen

4. Management van vernetwerkte risico's

4.1 Interferentie tussen incidenten

Vernetwerkte risico's worden net als gewone risico's pas zichtbaar wanneer ze zich manifesteren in incidenten. Daarvoor is het risico er wel, maar blijft de beleving ervan abstract. Bij de *vernetwerkte risico's* komt daar nog eens bij hier ook de vervlechting tussen de risico's onvoorzien en tot op zekere hoogte zelfs onvoorstelbaar is. De *trigger* kan onverwacht of voorzien zijn, maar de werkelijke verrassing zit in de keten van gevolgen die er uit voortkomt. Die interactie-effecten zijn extra verrassend doordat risicomanagement in een organisatie zich doorgaans richt op individuele risico's. Risico's worden al dan niet bewust separaat gemanaged en niet in de onderlinge vervlechting. **Pas op het moment dat de risico's zichtbaar worden als incidenten, blijkt dat de incidenten met elkaar samenhangen en elkaar versterken.** Achteraf trekt men dan de conclusie dat er sprake was van interferentie. Met de positionering van het begrip *vernetwerkte risico's* willen we die wijsheid achteraf naar voren halen en het bewustzijn van netwerkeffecten van risico's vergroten. **Door vooraf al rekening te houden met de mogelijke interactie-effecten en met interdependenties is het mogelijk om ook deze categorie risico's mee te wegen en er wellicht meer gericht op te sturen.**

Om de stap naar een meer vooruitziende manier van omgaan met *vernetwerkte risico's* te zetten is het mogelijk om gebruik te maken van inzichten uit een aantal flankerende disciplines. Zo is het bij strategieontwikkeling en lange termijn planning niet ongebruikelijk om vooraf na te denken over mogelijke interacties die voor tot nu toe nog ongekende effecten kunnen zorgen. Toekomstverkenningen, 'early warning systematiek' en scenario-studies zijn manieren om gericht op zoek te gaan naar de interacties en interdependenties die in een systeem spelen en die voor discontinuïteit kunnen zorgen. In dergelijke studies wordt de toekomst bewust niet opgevat als een extrapolatie van het heden, maar als een afwijking daarvan. Daartoe brengen onderzoekers in kaart welke mogelijke variabelen of fenomenen met elkaar kunnen zorgen voor ontwikkelingen die er nu nog niet zijn of effecten die nu nog moeilijk voorstelbaar zijn. De Shell-scenario's uit de oliecrisis zijn breed bekend, maar het eerder genoemde voorbeeld van Singapore en Sars is ook interessant. Eén van de lessen die de Singaporese overheid heeft getrokken uit de SARS-epidemie is dat het nodig én mogelijk is systematisch te denken over toekomstige ontwikkelingen – en dan met name de interacties tussen nu al bestaande fenomenen die voor onverwachte toekomst kunnen zorgen. Het RAHS-programma 'scant' een lange reeks variabelen op hun ontwikkelingen en in causale modellen probeert men inzichtelijke te maken hoe onderlinge verbanden liggen en wat op welke manier op elkaar inwerkt. Men probeert daarmee de toekomst niet zozeer te voorspellen, maar wel al vroeg een zeker gevoel te ontwikkelen voor hoe bepaalde zaken op elkaar inwerken en welke mogelijke gevolgen daaruit kunnen voortkomen.

Wat ingewikkeld is aan het vooraf inzichtelijk maken van *vernetwerkte risico's* is dat het lastig is om de geloofwaardigheid en accuratesse ervan te beoordelen. Veel pogingen om toekomstige ontwikkelingen in complexe systemen te voorzien monden uit in onrealistische of overdreven doemscenario's. Het enige effect van dergelijke analyses is dat de wenkbrauwen worden opgetrokken en de beslissers en beleidsmakers door gaan met wat ze al deden – en voor de volgende keer niet meer om advies vragen. Om systeemdynamiek te voorzien is het nodig om gevoel te ontwikkelen voor de interactie-effecten in systemen die schijnbaar kleine aanleidingen tot grote gevolgen brengen. Maar evengoed is het nodig om zicht te krijgen op de mogelijke dempende krachten in het systeem en de interacties die effecten niet doen opzwellen maar juist mitigeren. Dat immers is de kern van netwerken en van

interacties: er treden leereffecten op, die maken dat de eerste gevolgen van oorzaken snel opgevangen worden, ingekapseld raken en dat actoren leren. Ook dat was één van de lessen van SARS. De epidemie verspreidde zeer snel, maar 'dankzij' de snelle openbaring van het virus (de klachten traden snel na de besmetting al zichtbaar op) lukt het ook om met maatregelen de verspreiding te remmen. De maatregelen waren enorm, zeker in Azië, maar uiteindelijk lukte het wel om een vaccin te ontwikkelen en de verspreiding tegen te gaan. En ook bij de kredietcrisis was dat uiteindelijk mogelijk, hoe 'traag' het ook ging en hoe hoog de kosten daarvan ook waren – en nog steeds zijn.

Omgaan met *vernetwerkte risico's* is een delicate kwestie. Wie probeert de gevolgen in te schatten moet een balans zien te vinden tussen het voorzien van mogelijke discontinuïteit, maar ook kijken naar de mogelijkheden van het netwerk om zelf dynamiek te neutraliseren of interactie-effecten te kanaliseren. Een befaamd voorbeeld is de rapportage van de Club van Rome waarin een omvattend model van de wereld werd gepresenteerd waaruit zou moeten blijken dat risico's in een deel van de wereld zich zouden voortplanten over de rest met als resultaat een ineenstorting van de wereldeconomie.[32] Dit scenario werd niet bewaarheid omdat allerlei interferenties, in het bijzonder feedback mechanismen, over het hoofd waren gezien. Dat ging deels om feedback mechanismen in het systeem zelf, die als automatische stabilisatoren werken. Maar het ging ook om sociaal leervermogen, om mensen die hun gedrag kunnen aanpassen en daarmee het scenario juist doordat ze er in geloven – of er vrees voor hebben – onwaar maken. Zo is de tragiek van veel toekomstvoorspellingen dat ze niet uitkomen, juist doordat ze serieus worden genomen, mensen of organisaties hun gedrag aanpassen en ze daarmee voorkomen dat de voorspelling uitkomt. **Met *vernetwerkte risico's* is het net zo: door de dynamiek in het systeem in te schatten is het mogelijk om bepaalde cascades van gevolgen van incidenten te neutraliseren, zodat het networked incident zich uiteindelijk niet of heel beperkt voordoet.** Juist als organisaties en systemen zich beter bekwamen in het voorzien en omgaan met *vernetwerkte risico's* bestaat de kans dat ze steeds minder serieus genomen worden. Net zoals de beschouwingen over de audit society en de angst voor risico suggereren dat de aandacht voor *vernetwerkte risico's* eenvoudig kan leiden tot overreageren en tot het optuigen van systemen die maken dat we per saldo slechter af zijn en meer dan eerst bloot komen te staan aan de risico's van interacties in netwerken. **Het doel van onze beschouwing is om daarin een werkbaar midden te vinden: de risico's serieus nemen zonder verkramping en overreactie**.

4.2 Niet perse grotere, wel andersoortige risico's

De gecombineerde ontwikkeling naar wat in de literatuur is omschreven als de netwerksamenleving, de risicomaatschappij en de audit society vormt een vruchtbare voedingsbodem voor de opkomst van deze *vernetwerkte risico's*. In het idee van de netwerksamenleving is geïmpliceerd dat onderdelen van de samenleving meer dan voorheen vervlochten zijn met andere delen van de samenleving. Het concept van de risicomaatschappij maakt duidelijk dat er ook nieuwe risico's verbonden zijn aan die onderlinge vervlochtenheid, terwijl de notie van de audit society ons duidelijk kan maken dat het streven naar de beheersing hiervan ook juist een omgekeerd effect kan hebben. Meer risico's dus die zich gemakkelijker dan voorheen kunnen verspreiden en die maar moeilijk te beheersen zijn.

Het voorbeeld van de financiële sector ligt voor de hand. Banken zijn in het recente verleden steeds meer risico's gaan nemen en vervolgens hebben die risico's zich kunnen voortplanten binnen het netwerk. Dit kon gebeuren door de internationalisering van banken en het financiële verkeer in het

[32] Club van Rome (1972), The limits to growth, a global challenge

algemeen *en* door de vervlechting van banken en staten, wat uiteindelijk heeft geresulteerd in het bijpassend concept van 'systeembanken'. Door het dominant worden van dit frame kon het risico niet worden gealloceerd bij de normale risicodragers, te weten klanten van banken en aandeelhouders van banken, maar moesten andere actoren (andere banken en overheden) de risico's wel overnemen. Zo werden de risico's niet beheerst of ingekapseld, maar verspreidden deze zich juist over het gehele systeem. Risico's en schade plantten zich voor in delen van de samenleving die niets van doen hebben met het ontstaan van de risico's. Ze hebben amper te maken bij het ontstaan ervan, maar ondertussen dragen ze wel de schade er van. De lange en complexe ketens van verbindingen die in de netwerksamenleving zijn ontstaan, maken dat actoren die het risico veroorzaken steeds verder af komen te staan van de actoren die de schade dragen als het risico zich manifesteert en tot incident wordt. De netwerksamenleving zorgt er voor dat de reikwijdte van de risicomaatschappij wordt vergroot. **Het aangaan van risico's is niet nieuw (het is één van de kenmerkende eigenschappen van de risicomaatschappij die het afgelopen decennium is ontstaan), de snelle verspreiding ervan over lange afstanden van domein, tijd, plaats en de toenemende onvoorspelbaarheid ervan is dat wel.**

Vernetwerkte risico's roepen allerlei nieuwe vragen. Denk bijvoorbeeld aan de klassieke notie van de aansprakelijkheid: die gaat uit van de basisgedachte dat er voor een schade een verantwoordelijke veroorzaker is aan te duiden. Het is soms even goed zoeken, maar uiteindelijk is er iets of iemand die met een handeling of nalaten zorgt voor een schade elders. Bij vernetwerkte risico's zal dat vaak anders werken. Er zijn weliswaar handelingen, maar die leiden pas via complexe interacties tot schade. Die is amper meer te relateren aan de oorspronkelijke handeling. Nalatigheid, onbezonnenheid of domweg gevaarlijk gedrag bestaan nog steeds, maar in de netwerksamenleving zijn ze lastiger aanwijsbaar. Zo ontstaat een ingewikkelde praktijk waarin oorzaak en gevolg pas na verschillende schakels van interferentie bij elkaar komen. Als door vernetwerkte risico's een betrekkelijk geringe nalatigheid tot niet te voorziene schade leidt, kan de veroorzaker dan daarvoor aansprakelijk worden gehouden? Kan een fraudeur bij een bank die bijdraagt aan het omvallen van zijn bank waardoor vervolgens ook andere bedrijven in de problemen komen, aansprakelijk voor de schade worden gesteld? Of is het toch de bank, die weliswaar niet zelf aan de fraude meewerkte maar wel verantwoordelijk was voor zijn aanstelling – en handelen? En wat als de bank inbrengt dat deze niet verantwoordelijk gehouden kan worden voor de reacties van de markt op handelen van de bank, en al helemaal niet voor de soms ronduit overspannen reacties daarop van anderen in de markt. Een bank met een lage credit rating kan in de gevarenzone voor een bankrun komen, maar is het niet ook zo dat de échte motor achter een run on the bank toch de zichzelf versterkende dynamiek is van mensen die in elkaars paniek de bevestiging zien van dat het écht niet goed gaat bij de bank. We praten makkelijk over self-fulfilling prophecies en nemen ze ook empirisch waar, maar ze zijn buitengewoon lastig ter vertalen in consequenties in termen van schuld, verantwoordelijkheid en aansprakelijkheid. Tegelijkertijd is ook de consequentie van deze redenering moeilijk houdbaar. Als we de veroorzaker de schade niet kunnen aanrekenen, dan betekent dat min of meer automatisch dat de schade voor rekening van het slachtoffer is. Die kan er al helemaal niets aan doen. Hoe dan ook: de rekening moet worden betaald en iedere betrokkene heeft een verhaal waarom hij niet hoeft te betalen. Uiteindelijk is het dan het probleem van de partijen die met de schuld achterblijven en niet in staat zijn om de kosten tijdig op een andere partij af te wentelen.

Vernetwerkte risico's zijn hiervoor geduid een bijzondere categorie van meer dan "gewoon" ingewikkelde risico's. Zo zou het beeld kunnen ontstaan van een categorie risico's waar eigenlijk maar weinig aan te doen is. Dat beeld is tot op zekere hoogte juist, het gaat soms om hele grote risico's zonder veel mogelijkheden tot beheersing, maar dat is niet de bijzonderheid van vernetwerkte risico's. De kern van ons betoog is niet dat de risico's groter zijn, maar dat het gaat om risico's die **anders** zijn. Met een andere dynamiek, een andere verdeling en andere vaak onverwachte gevolgen van interventies om het risico te managen. Onze stelling is dat een beter begrip van de mechanismen van vernetwerkte risico's leidt tot een betere mogelijkheid tot het management ervan. Daarmee wordt het risico kleiner, bijvoorbeeld doordat het vernetwerkte aspect ervan – wat zorgt voor de snelle en bijna oncontroleerbare verspreiding – beter getemd wordt. Daarmee nemen zowel kans als effect af, en dus ook het totale risico.

We zien dus mogelijkheden voor het management van vernetwerkte risico's, mits daarvoor "het andere" van vernetwerkte risico's de basis vormt.[33] In dit hoofdstuk gaan we in op de zoekrichting voor de beheersing van vernetwerkte risico's. Belangrijk daarbij is wel om te onderkennen dat de ervaring met vernetwerkte risico's beperkt is. Dat wil zeggen, dit type risico is een direct gevolg van ontwikkelingen die relatief recent zijn – in ieder geval in de schaal waarop ze optreden. De netwerksamenleving in zijn radicale vorm is een ontwikkelend fenomeen. Dat betekent dat de context van de risico's die we beschrijven continu verandert, maar ook dat de praktische ervaring met bijvoorbeeld het managen van cascade-risico's nog beperkt is. Enerzijds legt dat een beperking op de mogelijkheid om 'tested interventions' te presenteren, anderzijds benadrukt het de noodzaak om snel te komen tot nieuw handelingsrepertoire voor het management van vernetwerkte risico's.

4.3 Frames voor vernetwerkte risico's

Om meer te begrijpen van de wijze waarop vernetwerkte risico's effectief kunnen worden benaderd, is het van belang na te gaan hoe deze risico's worden geframed, welke taal en welke metaforen worden gebruikt om de *vernetwerkte risico's* te beschrijven en te begrijpen. Hoe we de vernetwerkte risico's denken is van grote invloed op de richting van het management. Grofweg zien we drie mogelijke frames voor de conceptualisering van vernetwerkte risico's.

A. Vernetwerkte risico's als waterbed.

Het eerste frame benadert vernetwerkte risico's als een *waterbed*. Het risico is dan als het ware een groot gewicht dat op het waterbed ligt en elke keer als het op de ene plek wordt weggedrukt verschuift naar een ander deel. Het risico blijft aanwezig, de vraag is alleen waar het uiteindelijk door de bodem zakt. Het risico is niet weg te nemen, alleen te verplaatsen. Dat maakt het voor partijen belangrijk om er voor te zorgen dat het risico niet op hun plek belandt. **Het aantrekkelijke van dit frame is dat het aangeeft dat een risico tot op zekere hoogte te managen is, namelijk door het een andere kant op te duwen. Tegelijkertijd impliceert het waterbed ook dat elke keer als het hier verdwijnt het elders weer op-popt.** Wie de financiële crisis bestrijdt door een getroffen partij te steunen haalt weliswaar dáár de schade weg, maar die verplaatst vervolgens naar een andere partij in een ander deel van het netwerk. Het managen van risico is dan het verschuiven van de last. **Wat dat betreft is het waterbed-frame een *fatalistisch* frame: het risico en de last zijn er, zo komen uiteindelijk ergens terecht, daar is verder geen ontsnappen aan.** De interventiemogelijkheden zijn beperkt

[33] Zie ook: Weick en Suthcliffe, Managing the Unexpected, 2005

tot de landing van het risico en last. Een tweede probleem van het waterbed-frame is ernstiger. Het beeld van het waterbed suggereert dat de randen begrensd zijn. Het risico beperkt zich tot het bed en het bed houdt ergens op. Eén van de opvallende en in potentie gevaarlijke kenmerken van vernetwerkte risico's is juist dat ze overslaan naar domeinen waar ze amper directe en gedachte relatie mee hebben. Ze springen – om in het beeld te blijven – van het bed over naar de slaapkamer en via de slaapkamer valt het hele huis om. Het blijft niet bij schade aan het bed, maar via het bed komt het hele gebouw in de problemen. (Overigens is dat op zich wel vergelijkbaar met een lekkend waterbed – dan heeft het hele huis schade.) Het waterbed-frame biedt weinig ruimte voor dat uitwaaierende en overspringende effect van vernetwerkte risico's. Het is wat te fatalistisch over de mogelijkheid om aan last te ontsnappen, maar tegelijkertijd wat naïef over de begrenzingen van het risico.

B. Vernetwerkte risico's als cascade

Een tweede ook door ons al veel gebruikte frame voor het denken over vernetwerkte risico's is dat van de *cascade*: een lange keten van oorzaak en gevolg, waar steeds het ene omvallende steentje het andere omstoot – en het risico zo steeds verder voort gaat en gaandeweg in omvang en kracht toeneemt. De kracht van dit frame is dat het heel beeldend weergeeft hoe het risico zich door het netwerk beweegt en gevolgen heeft tot ver van de plek waar het de cascade is ingezet. Als een rollende sneeuwbal gaat het risico van de helling, waardoor uiteindelijk een gebied ver van de top in gevaar komt. Onderweg groeit het risico aan en gaat letterlijk de rem er af. De cascade maakt het dynamische en (vooral) aanzwellende karakter van vernetwerkte risico's zichtbaar. Toch kent ook deze metafoor beperkingen. De belangrijkste is dat de cascade suggereert dat je het verloop van het risico kunt voorspellen. De lawine beweegt een bepaalde kant op, neemt in snelheid toe en buigt niet ineens af. De dominosteentjes die omvallen staan in een lange rij achter elkaar. Het pad van het risico is wanneer de cascade begonnen is goed te voorspellen. Gewoon de helling af kijken of de rij dominosteentjes aflopen. Het is misschien niet zeker hoe groot het wordt en hoe ver het reikt, maar de baan is te voorzien. **De cascade is dus een beeld van een last die groter en gevaarlijker wordt, maar doet dat vanuit voorspelbaarheid. In dat opzicht is het een opgeruimd beeld. De oplossing die uit het beeld van de cascade volgt ligt daar mee in lijn. Door het pad te volgen en er een paar stappen op vooruit te komen is het mogelijk om de cascade te stoppen.** Door te zorgen dat een paar schakels worden weggenomen is het mogelijk om de ontwikkeling te onderbreken. Dat klinkt aannemelijk, maar het gaat één aspect voorbij: het vermogen van vernetwerkte risico's om van het ene naar het andere domein te springen, door onverwachte bewegingen te maken en uit zichzelf nieuwe emergente kwesties te produceren. Dat maakt het risico veel meer beweeglijk dan de sneeuwbal die zich al rollend tot lawine ontwikkelt.

C. *Vernetwerkte risico's als besmettelijke ziekte*

Het beeld van het vernetwerkte risico als besmettelijke ziekte laat meer ruimte voor juist die beweeglijkheid, misschien ook wel omdat een epidemie als SARS zo zichtbaar heeft gemaakt hoe vernetwerkte risico's zich kunnen ontwikkelen. **Het virusframe is sterk in de zin dat het het grillige aspect van vernetwerkte risico's goed weergeeft. Er kan van alles gebeuren, mensen die elkaars pad toevallig kruisen kunnen elkaar besmetten en maken dat de ziekte zich in tegengestelde richting beweegt. Het virusframe impliceert ook een reflexieve ontwikkeling, waarin het risico kan doven maar ook kan muteren en weer oplaaien.** Het interacteert met zijn omgeving en kan zorgen voor nieuwe vormen en nieuwe gevaren: het SARS-virus trof niet alleen "patiënten", maar trof ook de

dokters en verplegers die hen moesten verzorgen. Waar de ziekenhuizen volliepen met slachtoffers bleven de verplegers en artsen thuis. Dat zorgde voor een nieuw probleem, in de sociale organisatie die het virus zou moeten bestrijden. Het oog voor dat soort sociale dynamiek is de kracht van het frame van het vernetwerkte risico als virus. Ook de maatregelen die voortvloeien uit deze metafoor lijken in eerste instantie sterk. Hoe pak je besmettelijke ziektes aan? Het begint met preventieve maatregelen, zoals reserves en goede hygiëne. Bij een uitbraak begint de zoektocht naar een vaccin en quarantaine van de slachtoffers. De kunst is om het overspringen van het virus te voorkomen, door contact te vermijden. Dat ligt dicht aan tegen het idee van de loose couplings en het aanbrengen van ruimte tussen partijen. Toch voldoet ook deze metafoor niet geheel. Bij besmettelijke ziektes is er toch bijna altijd wel een element van fysieke nabijheid. SARS verspreidde zich snel, maar wel via fysieke overdracht, zoals via de airco van vliegtuigen. Dat bracht een element van lokaliteit in dat voor vernetwerkte risico's minder aan de orde is. En ook de maatregel *quarantaine* is wat te eenvoudig voor vernetwerkte risico's. Was het maar zo eenvoudig. Het kenmerk van vernetwerkte risico's is dat de ontwikkeling verloopt via 'dragers' die niet eenvoudig te isoleren zijn. En in de financiële crisis hebben we gezien dat er helemaal geen equivalent van quarantaine was. Zwakke banken waren bekend, maar daarmee verdwenen hun problemen niet. Ook vanuit een geïsoleerde positie – na een nationalisering – sloegen de risico's toch over naar de rest van de sector. Misschien zelfs als gevolg van de quarantaine, want dat ging direct ten koste van het vertrouwen. Een tweede probleem van het virus is nog ernstiger. Een virus is vernetwerkt, in die zin dat het zich snel over grote groepen kan verspreiden. Maar het is en blijft een enkelvoudig en kenbaar organisme. Iedereen die er door besmet raakt is anders, maar de besmetting komt voor iedereen door hetzelfde virus en is nagenoeg identiek. Dat maakt universele behandeling mogelijk. Het is even zoeken, met hoge kosten, maar uiteindelijk is er een vaccin of geneesmiddel tegen het virus. En voor veel virus-infecties geldt dat de schade zich na het uitschakelen van het virus goeddeels herstelt. Het lichaam is ziek zolang het virus in het lichaam is, maar zodra het virus weg is herstelt het lichaam zich in veel gevallen weer. Het is de vraag of dat beeld ook op gaat voor de netwerken waarin de hier besproken risico's zich voordoen. In het geval van de financiële crisis is in ieder geval niet goed te zeggen wat nu precies het virus was. Lehmann Brothers? Banken? De schuldpositie van landen? Of ging het in verschillende fasen en delen van de crisis om verschillende oorzaken en problemen? Is het vernetwerkte risico in dat opzicht niet meer een golf van steeds veranderende problemen die door het netwerk rolt. De problemen komen min of meer voort uit dezelfde aanleiding, maar zijn later in het proces van een heel andere aard en orde dan in het begin.

4.4 Ontwerpkeuzes en beheersmaatregelen

De voorgaande verkenning van veel gebruikte 'frames' voor vernetwerkte risico's laten zien dat er voor vernetwerkte risico's niet één goed passende generatieve metafoor is. So what, het is maar een mefafoor zullen sommigen denken, maar juist die beelden doen er toe. Een globale notie van wat vernetwerkte risico's zijn - welke eigenschappen en patronen aan de orde zin – is de basis van een strategie voor het omgaan er mee. **Zo stelt elk frame andere eigenschappen van networked risks centraal en ligt de nadruk bij de interventies op andere elementen.** De ene metafoor is niet meer waar dan de ander, ze benadrukken allemaal andere aspecten van hetzelfde vraagstuk, waarmee ze elk hun eigen nut hebben.

De kracht van de *cascade*-metafoor is dat het de aanzwellende kracht van het risico centraal stelt: kleine incidenten groeien uit tot systeem-problemen. Het frame van het *waterbed* wijst op de last die

hoe dan ook ergens genomen moet worden en de onmogelijkheid om het risico weg te duwen. Het popt uiteindelijk steeds weer ergens op. Het beeld van het *virus* laat zien hoe het risico alle kanten op beweegt en overspringt van de één op de ander. Maar elk van de beelden heeft ook zijn beperkingen, vooral in de begrenzing van de dynamiek van het risico en de mogelijkheden voor management die er uit voortvloeien. Het bed is een afgebakende eenheid, met vaste renden die het vernetwerkte risico niet heeft. Het ontkent de mogelijkheid om een probleem te verkleinen, waar risico in termen van kans maal effect wel degelijk in zijn uitkomst beïnvloedbaar is. De cascade slaat bij nadere beschouwing de dynamiek van het risico wel erg plat tot een beweging van 'groot, groter grootst'. Die bovendien onvermijdelijk in één grote klap eindigt. De baan van de ontwikkeling wordt kenbaar verondersteld, wat leidt tot aanbevelingen die een hoge mate van voorspelbaarheid impliceren. Veel van de onverwachte dynamiek raakt daarmee buiten beschouwing: vernetwerkte risico's worden uiteindelijk relatief eenvoudige 'groter groeiende' risico's. Terwijl de realiteit toch ingewikkelder is dan dat. Het virus-frame kent vergelijkbare beperkingen. Uiteindelijk is een virus kenbaar en heeft elke besmetting dezelfde oorzaak. De lasten van vernetwerkte risico's zijn overal anders. Hun samenhang is dat ze voortkomen uit dezelfde aanleiding, maar zonder dat ze onderweg hetzelfde blijven. Ze zijn veranderlijk. En uiteindelijk is de oplossing er van relatief eenvoudig: quarantaine, geen contact, buffers rond de aan plaats gebonden besmettingshaard, om de tijd tot het vaccin te overbruggen. Vernetwerkte risico's zijn in werkelijkheid veel minder aan plaats gebonden én de equivalenten van quarantaine of een universeel vaccin zijn er niet.

Hoe kunnen, in aanvulling op het bruikbare gedeelte van de remedies die voortvloeien uit deze frames, *vernetwerkte risico's* worden voorkomen, ingedamd en gemanaged op een manier dat ze minder schadelijk worden? Welke beelden en begrippen kunnen helpen om te komen tot richtingen voor management en beheersing van vernetwerkte risico's? Bij het omgaan met vernetwerkte risico's gaat het om het positie kiezen op een spectrum van mogelijkheden voor organiseren. We bespreken de belangrijkste hier kort.[34]

Homogeniteit versus variëteit.

De trend in organiseren is onmiskenbaar richting homogenisering. Alle organisaties benoemen zichzelf als uniek, maar tegelijkertijd laat de praktijk zien dat organisaties steeds meer op elkaar gaan lijken. In sectoren kruipen partijen steeds dichter naar elkaars modellen toe, om van daaruit te concurreren op details – en vaak op marketing. Ze verschillen onderling steeds minder op het gebied van financiële modellen, organisatie van productie en interne organisatie. Ze volgen dezelfde ontwikkelingen en organiseren zich volgens dezelfde principes. Daarin volgen sectoren elkaar bovendien ook steeds meer. Modellen en voorkeuren waaien over. Internationalisering en massamedia maken het mogelijk dat actoren meer en meer elkaars gedrag imiteren. Best practice benaderingen en sturing op basis van benchmarks kunnen tot prestatie-verhoging leiden, maar gaan ook gepaard met imitatiegedrag. Dergelijke homogenisering heeft allerlei voordelen en reduceert alleen al door de enorme ervaring die met bepaalde modellen wordt opgedaan allerlei operationele en strategische risico's. Het is in dat opzicht een heel veilige vorm, die op kortere termijn de kans op bekende en waarschijnlijke risico's sterk verkleint.

Maar er is een keerzijde van homogenisering. Een systeem dat bestaat uit verschillende typen actoren is minder kwetsbaar voor onverwachte verstoringen dan een systeem dat bestaat uit identieke

[34] Zie ook: Weick en Suthcliffe, Managing the Unexpected, 2005.

actoren. Het beroemde voorbeeld van Scott over de "Normalbaum" is typerend voor dit fenomeen: de bijna fabrieksmatige bosbouw in Duitsland in de negentiende eeuw – met allemaal dezelfde en voor de houtkap ideaal doorgekweekte bomen – deed het jaren lang goed, tot een onbekende ziekte opkwam en alle "normaalbomen" stierven.[35] Behalve de bomen in de gemengde en voor de houtproductie veel minder efficiënte oerbossen. Een paar boomtypen werden ziek, maar heel veel anderen niet en de ziekte kon niet verspreiden. En de beperkte verspreiding maakte dat de uitbraak daar uiteindelijk ook doofde. Zo is het met alle eenvormige systemen. Ze zijn veilig, zolang ze geconfronteerd met dezelfde en bekende uitdagingen. Banken die hetzelfde business model hebben en in dezelfde markten actief zijn, zijn als geheel kwetsbaar. **Een gemengd systeem reduceert de kwetsbaarheid, om twee redenen. De gelijkvormigheid maakt dat ze allemaal even gevoelig zijn voor dezelfde risico's. Als zich een incident voordoet, wordt van *alle* banken het verdienmodel aangetast en komen ze allemaal in de(zelfde) problemen.** Dat verkleint de mogelijkheden tot onderlinge steun en vergroot de schaal van de crisis. Maar er is nog een tweede probleem. In gevarieerde systemen is de kans groot dat de oplossing voor een nieuw probleem ergens al aanwezig is. Niet alleen worden niet alle partijen aangetast door een nieuw risico, de kans is groot dat ergens in het systeem de oplossing al aanwezig is. Misschien in de vorm van een idee dat ergens op de plank ligt en nu de sleutel tot de oplossing blijkt te zijn. Als bepaalde banken in een crisis niet omvallen is daar kennis een element van de oplossing te vinden. Zo remt variëteit in het systeem niet alleen de verspreiding van de crisis af, het versnelt ook het vinden van de oplossing. Daarom is biodiversiteit van belang voor goede ecologie. Verschillende soorten hebben antistoffen tegen verschillende ziekten; bij elkaar opgeteld maakt die variëteit dat in het systeem uiteindelijk alles aanwezig is. Niet zo efficiënt voor massaproductie en kostenreductie, maar wel handig als een onverwachte verstoring zich voordoet.

Lean and mean versus redundantie.

Redundantie staat haaks op de tendens om organisaties, processen en structuren *lean and mean* vorm te geven. Redundantie is vanuit dat discours hetzelfde als *rommel*, overcapaciteit en productieverlies. Wat is de rationale voor bewust overlap, die extra kost en geen productiewinst oplevert? Lean and mean is efficiënt en dus goedkoop. Bij redundantie worden buffers ingebouwd, reserves gekweekt en voorzieningen verplicht gesteld die op het eerste gezicht, bij doorrekening van de bekende risico's, overdreven overkomen. Ze hebben een hoge prijs, want alles wat gereserveerd wordt kan niet worden geïnvesteerd – en brengt dus niets op. Reserveren is kostbaar. **Maar redundantie heeft ook opbrengsten. Het biedt het vermogen om ook aan in eerste instantie onbekende risico's, het hoofd te bieden.** Redundantie kan op vele manieren vorm krijgen en vanuit de twee perspectieven betekent het steeds iets heel anders: financiële buffers bij banken zijn voor de één een verstandige reserve, maar voor de ander 'dood geld' dat de bank verzwakt ten opzichte van concurrenten. Een overschot aan mensen is voor de één onderhoudsstaf 'op de bank' dat geld kost zonder opbrengt te genereren – een teken van verval van de organisatie – waar het voor een ander een handig reserveteam is dat in geval van nood paraat staan om uit te rukken. Wie niet precies weet waar de inzet nodig is de komende tijd is blij dat niet iedereen in langlopende contracten vast zit. Voor een manager die nu de korte termijn resultaten wil maximaliseren voelt dat heel anders. Redundantie maakt de organisatie op korte termijn misschien zwakker, maar voor onbekende bedreigen juist sterker.

[35] Scott, Seeing Like a State, 1998.

Lean and mean vergroot de marges of de mogelijkheden van nu, maar alleen zolang zich geen onverwachte ontwikkelingen voordoen.

Dezelfde principes van lean and mean en redundantie gelden ook tussen organisatie. Een veelheid aan relaties en onderlinge verzekeringen en garanties wordt dan ontworpen waarmee aan wel heel veel incidenten het hoofd kan worden geboden. Een hoge redundantie leidt tot een veerkrachtig (*resilient*) systeem. Een systeem dat een stootje kan hebben, waarbij het wel zo is dat met redundantie kosten gemoeid gaan. Het is nu eenmaal ingewikkelder om met heel veel partijen heel verschillende – en wat rommelige – relaties te onderhouden. In tijden van crisis is het mogelijk de redding van het systeem, maar in de periode zonder crisis voelt het overbodig en ongeorganiseerd aan.

Tight coupling versus loose coupling.

Systemen worden meer en meer *tightly coupled* ontworpen. We hebben hiervoor al laten zien hoe de schakels in processen steeds dichter bij elkaar komen te liggen en er procesmatige nabijheid ontstaat. Alles is zodoende niet alleen met alles verbonden, het ligt ook nog eens allemaal dicht tegen elkaar aan, met minimale marges. Dat zorgt voor efficiënte productie, maar het maakt ook dat de risico's zich wel heel gemakkelijk voortplanten door het systeem – en van daar naar andere systemen, want die liggen er al even dicht op.

Het principe van *loosely coupled* systemen biedt een alternatieve vorm van inrichten. Systemen zijn dan weliswaar niet geheel ontkoppeld, maar wel op enige afstand en niet 'automatisch'. Er zijn bijvoorbeeld buffers in de besluitvorming aangebracht, waardoor geen geautomatiseerde kettingreacties van besluiten optreden – zoals met geautomatiseerde beurshandel kan gebeuren. Dat zorgt voor wachttijd en langere reactietijd, maar die kan evengoed fungeren als bezinningsperiode en als tijd van reflectie. In de democratische instituties is de Eerste Kamer een voorbeeld van een uitdrukking van 'losse koppeling'. Natuurlijk kan wetgeving sneller, helemaal als allerlei procedurele doorlooptijden verkort of afgeschaft worden, en als er na de Tweede Kamer niet nog een tweede besluit nodig is. Maar met die versnelling treedt in potentie toekomstige schade op. Juist door de vertraging planten risico's zich niet zo gemakkelijk één op één voort. Het systeem kan zich bedenken, op de schreden terugkeren, of anderszins gedane zaken keren. Er komt een zekere traagheid in het systeem en/of de risico's worden niet in hun geheel doorgegeven. Dit biedt ruimte aan het systeem om te reageren op het incident en de kans op aantasting van aangrenzende systemen wordt wat kleiner. Dat klinkt als een beperkt effect, maar juist in vernetwerkte risico's kan dat heel veel uitmaken. Een paar dagen meer tijd aan het begin van de financiële crisis had veel schade kunnen voorkomen.

Concentratie of spreiding van risico's.

Risico's worden nu nogal eens geconcentreerd neergelegd bij een beperkt aantal partijen. Het risico wordt steeds verder doorgegeven naar één of enkele partijen, waar het vervolgens allemaal terecht komt. Her-verzekeraars en overheden zijn van die partijen die als *lender of last resort* dienen. Zij dragen uiteindelijk de risico's die van veel kanten op hen af kunnen komen. Dat biedt de mogelijkheid tot specialisatie en efficiëntie, maar zorgt voor acute problemen als er zich een meer dan gemiddelde crisis voordoet. Als het aantal claims – de totale schade – te groot wordt zal ook hun continuïteit in gevaar komen, met alle gevolgen van dien. Concentratie werkt goed, zolang de problematiek zich be-

perkt. En het inherente gevolg van concentratie is dat als de entiteit waar het risico is geconcentreerd in de problemen is, dan meteen het gehele systeem "ongedekt" is - al het risico, van iedereen, ligt immers op dezelfde plek.

Een alternatieve inrichting is om de risico's te spreiden. In feite is dit het geval indien de overheid het risico draagt. Uiteindelijk zal de overheid de kosten van het incident omslaan over de bevolking en het bedrijfsleven in dat land waarmee zo veel schouders de kosten dragen dat het weer dragelijk wordt. De overheid is in dat opzicht geen verzekeraar, maar een herverdeler. Het prettige aan concentratie is dat – in het beeld van het waterbed – de last uiteindelijk naar één punt zakt en dat alle partijen dat uiteindelijk ook weten. Het risico van dit arrangement is dat juist die kennis een prikkel voor prudent risico-management wegneemt en strategisch gedrag in de hand werkt – de *moral hazard* waar economen graag over spreken. Ook hier zou *loose coupling* in combinatie met radicale spreiding een interessante oplossingsrichting kunnen zijn. De kosten worden in dat geval niet direct en geheel omgeslagen, maar vertraagd en gedeeltelijk overgebracht naar andere delen van het systeem. Effecten zwermen nog steeds uit, maar veel langzamer en met veel langere reactietijd voor partijen. Dat dempt de interactie-effecten van partijen die sterk op elkaar reageren – vaak zonder precies te weten waarop precies – en verkleint de mogelijkheden tot strategisch gedrag van partijen die het risico willen opspelen.

Veroorzaker en drager van last

Wie is er verantwoordelijk voor het reduceren van risico en de last die er mogelijk uit ontstaat. Eén van de kenmerken van vernetwerkte risico's is dat er veel afstand bestaat tussen de plaats waar de lasten neer komen en waar het risico door iemand genomen wordt. Niet alleen doordat mensen blootgesteld worden aan risico's die ze niet in de hand hebben – zoals bij een mogelijke kernramp –, maar ook doordat ze via allerlei schakels in het netwerk onderdeel zijn van een causale kettingreactie waarvan ze dachten helemaal geen deel uit te maken. De vraag is dan wel wie primair verantwoordelijk is voor het risico. De eerste indruk zal altijd zijn dat de verantwoordelijkheid voor het risico zo dicht mogelijk moet liggen bij diegene die het risico aangaat. Door actoren die het risico *nemen* ook verantwoordelijk te maken voor de risico's die zij aangaan is het waarschijnlijk dat zij zich voorzichtiger zullen gedragen en *moral hazard* te voorkomen. Zo ontstaat noodgedwongen bewustzijn van risico's en een direct belang om incidenten te vermijden. Schuld, aansprakelijkheid en verantwoordelijkheid komen dan dicht bij elkaar te liggen. De hoop is dat de risico's er weliswaar zijn, maar dat de prikkel voor partijen zo groot mogelijk is om te zorgen dat de problemen zich niet voordoen.

De nabijheid van verantwoordelijkheid, schuld en aansprakelijkheid is de basis onder de manier waarop we op dit moment met risico's omgaan. Die basis is sterk verankerd in de arrangementen die we kennen, hoewel het verhandelen van risico's daar al op inbreekt. Ingewikkelder is echter dat via netwerken de verbanden tussen last en verantwoordelijke actor zo indirect en onduidelijk zijn geworden dat het lastig is om dit principe als basis te handhaven. Daar komt bij dat vernetwerkte risico's het snelst door het netwerk razen via besmetting van zogenaamde 'kritieke instituties': systeembanken, grote (her)verzekeraars, landen, grote woningcorporaties, het vliegverkeer. Allemaal systemen of organisaties die zo groot en cruciaal zijn voor de gemeenschap dat het bijna onmogelijk is om ze écht aan te slaan voor de last die ze veroorzakers. Dat is het probleem van *too big to fail*: de veroorzakers van het risico zijn zo groot dat ze eigenlijk boven elke werkelijke straf verheven zijn – en

dan ontneemt hen de prikkel om veilig te zijn, waarmee het risico van deze extreem gevaarlijke instituties groter wordt in plaats van kleiner. Dezelfde maatregel die het systeem als geheel veiliger moet maken, maakt het uiteindelijk minder veilig. Dat vertroebelt de mogelijkheid om risico en veroorzaker dicht bij elkaar te brengen en langs die weg de risico's te beheersen.

Daarom is het mogelijk zinvol om kijken naar een andere optie. Niet alleen de veroorzakers van het risico, maar ook de partijen die het risico lopen – ook als ze daar amper directe invloed of betrokkenheid mee hebben – kunnen zich actiever opstellen. Zij moeten zich bewust zijn van de risico's die ze via het netwerk lopen en zich daar meer activistisch n gedragen. Dat kunnen ze zelf doen, maar ook via de internationale over overstijgende instituties die we kennen – zoals de EU, het IMF, de vereniging van banken, grootschalige consumentenorganisaties, et cetera. Een andere weg is via de georganiseerde toezichthouders, maar dan op een activistische manier: nu gaat de gemiddelde consument, burger of gebruiker van een dienst er vaak van uit dat er ergens door een toezichthouder gezorgd wordt voor de veiligheid van het product. Door daar minder op te vertrouwen en meer naar te vragen – door consumentenmacht te ontwikkelen – kan een nieuwe dynamiek in het systeem ontstaat die disciplinerend werkt voor partijen die grote risico's aangaan. Daarmee verschuift de verantwoordelijkheid voor het risico en de last niet naar de gebruikers, maar ontstaat er wel een nieuwe impuls aan het geheel van checks en balances in het systeem.

Voor het managen van vernetwerkte risico's is het niet voldoende dat alleen de risicovolle organisaties zich minder risicovol gaan gedragen, maar dat *alle* partijen zich meer sensitief en activistisch tonen rond risico's die ze via het netwerk lopen. De kunst is om ook in dat nieuwe activisme de balans te vinden die maakt dat de baten van netwerkvorming en van het nemen van een bepaald risico in stand blijven, maar dat dat geborgd en met mate gebeurt – zonder dat risico's bewust of onbewust over het systeem worden uitgestrooid. Het gaat er dus niet om de risico's tot nul te reduceren, maar om sterke netwerken te organiseren waarin voldoende checks en balances aanwezig zijn om risico's in ieder geval zichtbaar en binnen perken te houden.

5. Een agenda voor de auditor

5.1 Van analyse naar audit

Tot nu toe hebben we veel gesproken over hoe vernetwerkte risico's ontstaan, wat ze doen en hoe ze vaak tot ver buiten het oorspronkelijke domein van herkomst lasten veroorzaken. We hebben dat verhaal bovendien opgebouwd vanuit een abstract en overkoepelend perspectief (netwerksamenleving, risicomaatschappij, audit society), als een beschouwing van veraf naar dichtbij. Eerst een duiding van de bredere ontwikkelingen, daarna steeds dichter redeneren naar wat dat concreet betekent voor het ontwerp en management van organisaties. In dit laatste deel maken we in die redeneerlijn de laatste stap en kijken we naar wat de beschreven ontwikkelingen betekenen voor het vak van de auditor. Waar kan de auditor in een organisatie aandacht aan besteden bij het verrichten van toetsend onderzoek als het gaat om (het management van) vernetwerkte risico's?

5.2 Andere risico's: vernetwerkte risico's als uitdrukking van dynamiek

Om te beginnen hebben we laten zien dat vernetwerkte risico's bovenal *andere risico's* zijn. Ze kennen een ander onderliggend patroon en andere dynamiek dan de risico's waar we al uitgebreid mee rekening houden. Die dynamiek zorgt voor de grote en uitdijende gevolgen en maakt ook dat bestaande arrangementen voor de preventie en beheersing van risico's niet goed werken. De basis van vernetwerkte risico's is een interferentie en interactie tussen factoren. Zo ontstaat *interactieve complexiteit*, die niet zozeer het gevolg is van problemen in eerste aanleg – de directe gevolgen –, maar die voortkomt uit de wisselwerking in tweede of derde orde. Een omvallende bank is een risico, maar het vernetwerkte risico is dat via de omvallende bank andere banken failliet gaan en zo een kettingreactie door het financiële systeem gaat.

Vernetwerkte risico's gaan in essentie om interacties: om partijen of ontwikkelingen die op elkaar reageren en die maken dat een wisselwerking ontstaat die uiteindelijk het risico sterk vergroot. Daarbij kan het gaan om de interferentie van **interne en externe dynamiek**, om de verwevenheid tussen interacties binnen een organisatie die doorwerken in de interacties daarbuiten. Of het gaat om interacties tussen partijen of fenomenen buiten, die samen leiden tot een escalatie die terugslaat op wat zich afspeelt binnen de organisatie. Organisaties houden rekening met de bekende risico's binnen en buiten de organisatie, maar wat als die bekende risico's elkaar beïnvloeden tot ongekende en onverwachte nieuwe risico's?

De volgende factor die bij vernetwerkte risico's aan de orde is hebben we geduid als de interactie tussen **technische en sociale systemen**. We zijn geneigd om interacties te denken als actieve en bewuste handelingen van partijen – van mensen -, maar dat hoeft niet per se zo te zijn. Veel interacties in het netwerk zijn geprogrammeerde of in onze tijd geautomatiseerde reacties op vooraf afgebakende stimulu. Een aandeel dat door een koers zakt, een bod dat automatisch wordt beantwoord, een sluis die automatisch op en of dicht gaat. Vaak zelfs bedoeld om bepaalde risico's in de eerste ronde tegen te houden, maar vervolgens onbedoeld de veroorzaker van nieuwe dynamiek die het oorspronkelijke incident ver voorbij gaat. Mensen kunnen daar in interveniëren, maar dat maakt het soms weer erger. Het punt van deze factor is dat in netwerken het systeem zelf mee doet aan de interactie en deze soms zelfs opjaagt. Veel systemen zijn "snel" geworden, ontworpen om tijdig te kunnen handelen in de snelle dynamiek van het netwerk. Maar bij een zich ontwikkelend vernetwerkt

risico kan juist die snelheid voor nieuwe omvang van het risico zorgen. Technische en sociale systemen zorgen samen, in interactie, voor risico's die het oorspronkelijke risico ver te buiten gaan.

De factor **tijd** is in dat kader ook nog van interessante betekenis. Interacties in systemen kunnen door eigenschappen van het systeem ineens versnellen of door een bepaalde inrichting van het systeem juist vertragen. Ook de tijdhorizon van risico's en beheersmaatregelen loopt mogelijk uit. Acute risico's vragen deels om directe antwoorden, maar misschien juist ook wel om lange termijn oplossingen. Net zoals lange termijn effecten van interacties mogelijk op korte termijn interventies vereisen. Probleem en oplossing, risico en interventie kunnen op verschillende tijdsdimensies spelen, waarbij gevolgen van interacties nu in de tijd vervormen. Grote effecten lekken weg of doven uit, terwijl nu minimale effecten door complexe interacties kunnen oplaaien tot grote gevolgen in de toekomst. Of interacties hebben effecten die zich slapend houden en op termijn ineens ontwaken. Tijd is niet de context van risico's, maar is een dimensie op zichzelf. Voor vernetwerkte risico's geldt dat die factor van extra betekenis is.

5.3 Auditen van vernetwerkte risico's

Wat betekenen vernetwerkte risico's voor de werkpraktijk van de auditor? In de klassieke opvatting van het vak van de auditor levert deze aanvullende zekerheid aan het bestuur of management van de organisatie over de processen in de organisatie. Dat kan gaan om informatie over hoe de processen werken, wat ze opleveren en wat de kosten zijn die in de organisatie omgaan. Vaak vormen inschattingen van risico's en van de getroffen beheersmaatregelen ook onderdeel van de informatie die de auditor vanuit zijn positie onder het bestuur of management van de organisatie aanlevert. Die informatie toont de stand van zaken met de processen binnen de organisatie en geeft aan in hoeverre de organisatie nog in control van zijn processen – en risico's – is. De auditor kijkt dan naar de processen **binnen** de organisatie.

De meeste organisaties die opereren in netwerkverbanden zetten auditors ook in voor scans van de omgeving, meer in het bijzonder van de systemen die de organisatie heeft om de relatie met belangrijke externe partijen te monitoren en te beheren. Dat kan gaan om klanten, om opdrachtgevers, leveranciers, of meer generiek de belangrijke partijen die maken dat de organisatie wel of niet zijn werk goed kan doen – bijvoorbeeld de wetgever of een branche vereniging. Organisaties maken omgevingsanalyses of doen een stresstest waarin ze kijken of en hoe de externe omgeving voor risico's of verrassingen zorgt. De auditor kijkt dan naar de relaties **met** andere organisaties.

De theorie van vernetwerkte risico's richt de aandacht veel meer op een ander domein, namelijk de ruimte tussen organisaties. Niet als loze ruimte, maar juist als plaats waar interactie vorm krijgt tussen partijen die niet binnen de bestaande randen en kaders blijft, maar waarin zich nieuwe emergente ontwikkelingen kunnen voordoen. Welke risico's of mogelijkheden liggen daar? En wat kan de organisatie daar aan doen? Auditors richten zich van nature op processen of relaties die waarneembaar zijn, vindbaar in geformaliseerde documenten of beschrijvingen. Het kenmerk van vernetwerkte risico's daarentegen is dat het gaat om vaak impliciete en nog niet "geactiveerde" relaties. Ze zijn er in potentie wel, maar manifesteren zich nog niet. Zolang ze zich niet voor doen zijn ze letterlijk bij de organisatie niet in beeld, verschijnen ze niet in strategische documenten, en zijn ze dus bijvoorbeeld ook geen onderdeel van de stresstest die een organisatie mogelijk doet. Ze liggen voorbij de horizon – in de tijd, maar ook breder, in de mogelijkheden die de organisatie zich voorstelt – en blijven zo uit beeld. Totdat ze zich voordoen.

Auditors zouden daarom een belangrijke bijdrage kunnen leveren door zich meer dan nu te richten op de categorie risico's die voortkomt uit de interactie in netwerken. **Er is al veel aandacht voor risico's die ontstaan uit incidenten of enkelvoudige interacties: er is een oorzaak en die heeft een of meer gevolgen. Wat nog veel minder in beeld is, is dat er lange ketens van interacties zijn die zorgen voor meer, andere en grotere gevolgen dan gedacht.** Daar liggen mogelijkheden voor de auditor, in de tussenruimte tussen organisaties en systemen, waarin de interacties zich voordoen. We onderscheiden drie vormen van instrumenten of interventies die auditors hebben of zich eigen kunnen maken.

De eerste optie is het doen van een *stress-test voor vernetwerkte risico's*. Veel organisaties doen al een stress-test, maar vergeten daarbij om breder en verder te kijken dan de interacties in eerste ronde. Ze kijken naar enkelvoudige en eenzijdige interacties, zonder om te kijken naar wat de reacties en tegenreacties daarop zijn – en wat die weer voor volgende gevolgen hebben. Dat gaat niet alleen om risicovolle fenomenen, maar ook om de interactie-effecten van beheersmaatregelen die andere partijen in reactie daarop treffen. Vernetwerkte risico's verspreiden niet alleen door incidenten, maar ook door de maatregelen die anderen naar aanleiding daarvan nemen. Dat zijn allemaal zaken die analytisch in een stress-test verwerkt kunnen worden en die daarmee voor het bestuur of management van de organisatie inzichtelijk gemaakt kunnen worden.

De tweede optie is een analyse van het *frame* waarmee de organisatie – of verschillende elementen binnen de organisatie – in hun beschrijvingen en protocollen voor vernetwerkte risico's naar dat fenomeen kijken. Welk beeld hanteren ze: denken ze vanuit het beeld van het waterbed, de cascade of het virus? Of wellicht een ander beeld? Zelfs als ze vanuit dat betreffende beeld goede voorbereidingen hebben getroffen dan nog suggereert de bespreking van de frames dat het overhellen naar één van de frames een aantal tekorten produceert op andere relevante elementen. Auditors kunnen daar kritisch naar kijken en het bestuur of management informeren over de nadruk die de organisatie in zijn perceptie en in het risico-management hanteert. Idealiter zou dat in de primaire of strategische processen zelf al gebeuren, maar een kenmerk van frames is nu juist ook dat ze impliciet, niet bewust zijn. Mensen kiezen er niet voor, maar leven in het frame – ze zijn zich er niet van bewust dat ze een bepaald beeld hanteren, maar doen dat gewoon. Zonder er bij na te denken of te wegen wat andere frames zouden kunnen betekenen. Dit wordt versterkt door de padafhankelijkheid van eenmaal gevestigde frames: die worden omgezet in organisatieregels, in beleidsmaatregelen, in procedures en raken verankerd in de identiteit en in de mores van de organisatie. Er van afwijken wordt een interventie op zichzelf. Auditors staan van nature meer buiten die dagdagelijkse realiteit van het organiseren en zijn van daaruit in de positie om te reflecteren op wat ze de organisatie zien doen. Juist dat soort reflectie is wat organisaties vanuit het primaire proces, of de leiding zelf, vaak missen en wat achteraf in de evaluatie als het ernstig is misgegaan als eerste wordt benoemd: tunnelvisie, geen reflectie, geen ruimte voor afwijkende beelden. De auditor kan daar gevraagd of ongevraagd ruimte in nemen en de organisatie naast feitelijke rapportages ook op dat niveau een spiegel voorhouden.

De derde soort interventie die auditors concreet kunnen ondernemen is een analyse van de manier waarop de organisatie zich ten aanzien van vernetwerkte risico's organiseert en positioneert. We hebben eerder een aantal dimensies gepresenteerd met continua waarop organisaties een balans moeten vinden: homogeniteit versus variëteit, lean and mean versus redundantie, tight coupling versus loose coupling, concentratie of juist spreiding van risico's, inzetten op de veroorzaker of de drager van de last. Alle organisaties maken keuzes op dat vlak, bijvoorbeeld door te streven naar

strakke of juist lossere koppelingen en door de mate van overlap en redundantie die ze toestaan. We hebben laten zien dat hier vaak afwegingen rond de optimalisering van de dagelijkse werkprocessen als hefboom voor waardecreatie tegenover het goed voorbereiden op vernetwerkte risico's staat. Vanuit efficiëntie oogpunt is redundantie niet goed, vanuit het perspectief van snel interacterende en overspringende risico's is het een belangrijke buffer tegen snelle en niet meer te controleren verspreiding van een in eerste instantie nog lokaal risico. **Ook hier geldt dat keuzes weliswaar reëel in hun gevolgen zijn, maar lang niet altijd bewust en weloverwogen zijn gemaakt. Of ooit wel bewust gemaakt zijn, maar nu hun rationale verloren hebben. De auditor kan dit via toetsend onderzoek inzichtelijk maken voor het bestuur of het management van de organisatie en zo bijdragen aan het sterker en veerkrachtiger maken van de organisatie.**

Ter afsluiting willen we aansluiten bij de onlangs verschenen publieke managementletter van de NBA over risicomanagement. [36] In deze publieke managementletter wordt vastgesteld dat in het huidige risicomanagement onvoldoende aansluiting wordt gevonden bij de kwesties en zorgen die leven bij leiding, bestuur en toezicht. Risicomanagers zijn volgens de NBA op dit moment nog teveel bezig met operationele taken en hebben onvoldoende gevoel voor de afwegingen die spelen bij strategiebepaling en de vertaling daarvan in de feitelijke bedrijfsvoering. De NBA komt tot de conclusie dat risicomanagers meer aandacht moeten geven aan de ontwikkeling van nieuwe technieken, zoals scenarioanalyses, stresstesten en het doorrekenen van de effecten van meer of minder risicobereidheid. Het is onze stellige overtuiging dat juist auditors op basis van hun specifieke professionaliteit via toetsend onderzoek kunnen helpen bevorderen dat het ook nog eens zover komt.

[36] NBA, Risico's managen is mensenwerk, Risicomanagement en –verslaggeving bij grote ondernemingen van november 2013.

OVER DE AUTEURS

Prof. dr. Mark van Twist (1966) is wetenschappelijk directeur van de Internal Audit & Advisory opleiding van de Erasmus School of Accounting & Assurance (ESAA) aan de Erasmus Universiteit Rotterdam. Daarnaast is hij hoogleraar bestuurskunde aan diezelfde universiteit en is hij als bestuurder en decaan verbonden aan de Nederlandse School voor Openbaar Bestuur in Den Haag. Hij is verder onder meer buitengewoon lid van het College van de Algemene Rekenkamer. Vanuit zijn onderzoekspraktijk is hij nauw betrokken bij ingewikkelde kwesties die spelen op het grensvlak van bedrijfsleven en openbaar bestuur.

Dr. Martijn van der Steen (1977) is co-decaan en adjunct-directeur van de Nederlandse School voor Openbaar Bestuur (NSOB) en is directeur van de Denktank van de NSOB. Hij is decaan van een reeks executive opleidingsprogramma's en is verantwoordelijk voor wetenschappelijke en toepassingsgerichte onderzoeken van de NSOB. Hij publiceert onder andere over strategievorming, netwerksturing, verantwoording en langetermijnontwikkelingen.

Prof. mr. dr. Ernst F. ten Heuvelhof (1954) is professor of Public Administration at the Faculty of Technology, Policy and Management at Delft University of Technology (DUT). He has been director of the Education of the faculty of Technology, Policy and Management of the Delft University of Technology since September 2011. The Executive Board of TU Delft appointed Ernst ten Heuvelhof to take on the role of Director of Open and Online Education at the TU Delft Extension School from January 2014.

Erasmus Universiteit Rotterdam - Erasmus School of Accounting & Assurance (ESAA)
Post-Master opleidingen Internal Auditing & Advisory en IT-Auditing & Advisory
Burgemeester Oudlaan 50, Tinbergen building, H13-06
3062 PA Rotterdam
www.esaa.nl
esaa-auditing@ese.eur.nl

ESAA Erasmus School of Accounting & Assurance