IT Regie (Nyenrode | InterExcellent)

(NICP Thesis Nyenrode IT Regie mei 2015 v1.0f DEF.docx)

Welke factoren zijn van belang voor het borgen van de kwaliteit van informatie bij de ICT centralisatie in een decentrale veiligheidsorganisatie.

Een exploratief onderzoek

Interimpoint BV

(versie 1.0)

Inhoudsopgave

Documentgegevens

Versies

Versie	Auteur	Bedrijfsnaam	Wijzigingen	Datum
1.0	H. Stiekema	Interimpoint BV	Eerste versie	24-05-15

Akkoord Nyenrode

Inleiding

Het succes van ondernemingen en de mogelijkheden van digitalisering worden in zowel commerciële - en binnen lokale - en centrale overheden breed onderkend. Waar 5 jaar geleden het overgrote deel van de bestuurders en directies, digitalisering nog kwalificeerden als een ICT ontwikkeling, wordt nu dezelfde digitalisering gezien als het fundament onder toekomstige, flexibele, open organisaties met een sterke samenwerkingsprofiel en moderne operating – en bedrijfsmodellen. De bedrijfseconomische prestaties van een onderneming worden in hoge mate afhankelijk gesteld van de mate waarin een organisatie deel uitmaakt van de informatie samenleving en moderne IP-technologie wordt geïntegreerd in de 'technostructuur' (Mintzberg, 1983) van een organisatie. Daarmee wordt een belangrijk deel van deel van het coördinatie-mechanisme van een organisatie van binnen naar buiten verplaatst en dat beïnvloedt de aard van de organisatie sterk. Om mee te liften op de belofte van de waarde van een moderne 'techno-structuur' migreren publieke – en private ondernemingen van de eigen intern, meer technische georiënteerde ICT functie, naar een vorm van centrale ICT dienstverlening. Hierdoor wordt de 'techno-structuur' versterkt, zonder torenhoge investeringen en krijgt de interne organisatie maximale ruimte voor haar focus op: communicatie, delen van informatie en samenwerking.

De beweging naar centrale ICT dienstverlening is ook waar te nemen bij publieke diensten in het algemeen en specifiek binnen de veiligheidsregio's[1], om zodoende het hoofd te kunnen bieden aan de: bedrijfseconomische druk ten gevolge van de laag conjunctuur, vraag naar flexibiliteit en bewegelijkheid van een organisatie in een complexe samenleving, aansluiting krijgen op de informatiesamenleving, verbetering van informatie-uitwisseling over de veiligheidsorganisaties heen [Wvr, artikel 22] en het verlagen van de digitale kwetsbaarheid. Hoewel ICT centralisatie een rekbaar begrip is tussen: het centraal fysiek hosten van een technische infrastructuur en het maken van gemeenschappelijke afspraken of werken volgens eenzelfde architectuur, is de praktijk dat een ICT centralisatie uitgaat van het centraal consolideren van decentrale ICT functies in één datacenter op één geografische locatie.

Het voorkomen van een crisis en het mitigeren van de gevolgen van een crisis is hét primaire proces van veiligheidsregio's. Tijdens crises zijn communicatie, samenwerking en besluitvorming essentiële aspecten voor positieve resultaten van het primaire proces. Deze aspecten hangen voor een belangrijk deel samen met de kwaliteit van de gebruikte informatie en zijn daarom per definitie geografisch *decentraal* georiënteerd.

De spanning die ontstaat, zodra binnen een decentrale governance de 'technostructuur', centraal wordt georganiseerd, wordt veroorzaakt door de spanning tussen politiek/bestuurlijke - , bedrijfseconomische motieven en motieven die samenhangen met de uitvoering van het primaire proces. In de bedrijfseconomische motieven wordt gekeken naar de systeemkant van de

[1] Samenwerkingsverband van de onder aansturing van de gemeente ten behoeve van fysieke veiligheid. In 2015 neemt het Algemeen Bestuur van de veiligheidsregio's een besluit over het de centralisatie van ICT voor de veiligheidsregio's (informatievoorziening 2015-2020)

oplossing, de hardware, de software en de connectiviteit, terwijl in primaire proces motieven de informatie en de kwaliteit daarvan belicht worden. Díe spanning is de moeite van het onderzoeken waard.

De probleemstelling van dit onderzoek is daarom om inzicht te krijgen óf het uitgangspunt dat een centrale ICT voorziening efficiënter is onderbouwd kan worden én inzicht te krijgen in de belangrijkste factoren voor het borgen van de kwaliteit van informatie in een centrale ICT organisatie binnen decentrale governance.

1 Context en relevantie van het onderzoek

De context van dit onderzoek wordt opgebouwd uit een aantal aspecten:

1. De ontwikkelingen van de informatiemaatschappij
2. De veiligheidsregio en de bestuurlijke context
3. Verschil tussen de koude – en warme fase van de veiligheidsregio's
4. De ICT ontwikkelingen binnen de veiligheidsregio's

Binnen deze context wordt gezocht naar de belangrijkste factoren voor het centraliseren van ICT in relatie tot de kwaliteit informatie voor veiligheidsregio's in Nederland.

De resultaten van dit onderzoek zijn relevant omdat het onderbouwt dat het verplaatsen van een decentrale ICT functie naar een gecentraliseerde ICT functie, niet alleen een kwestie is van kostenbeheersing. Juist de eisen aan de kwaliteit van informatie: juistheid, consistentie, betrouwbaarheid, snelheid, veiligheid en de mate waarin functionarissen de informatie vertrouwen en gebruiken, zijn essentiële uitgangspunten in de besluitvorming over ICT centralisatie.

1.1 De ontwikkelingen van de informatiemaatschappij

Het internet heeft zich in de afgelopen jaren ontwikkeld van een pre-millennium digitale encyclopedie tot een 21st eeuw moderne technische backbone voor elke organisatie (Stiekema, 2009) en is een essentieel medium gebleken voor het doorvoeren van organisatorische ontwikkelingen (Mihajlović, 2014). De informatiemaatschappij is gedefinieerd als: "een sociaal systeem waar productie en dienstverlening in hoge mate afhankelijk zijn van de toepassing van informatie technologie en de bekwaamheid van organisaties om kennis te gebruiken voor de ontwikkeling van de organisatie" (Vukašinović, 2014). Deze context is relevant omdat er in toenemende mate geografisch georiënteerde informatienetwerken ontstaan die heel veel[2] informatie leveren. De snelheid en kwaliteit waarmee dit informatienetwerk haar informatie ophaalt, distribueert, gebruikt en van betekenis kan voorzien kan een maat worden voor de kwaliteit van het primaire proces en daarmee voor de effectiviteit van een veiligheidsregio in haar geografische context.

[2] Ontwikkeling van big data, sensortechnologie en het brontobyte-tijdperk (10^{27} bytes)

1.2 De veiligheidsregio en de bestuurlijke context

Een veiligheidsregio is in Nederland een geografisch gebied waarin gemeentelijke besturen en veiligheidsdiensten samenwerken op het terrein van brandweerzorg, crisisbeheersing en rampenbestrijding en de regionale geneeskundige hulpverleningsorganisatie (GHOR). De coördinerende functie op de handhaving van de openbare orde en fysieke veiligheid is gebaseerd op de Wet Gemeenschappelijke Regelingen (Wgr)[3] en de Wet op de Veiligheidsregio's (Wvr)[4]. In Nederland zijn 25 min of meer onafhankelijke veiligheidsregio's ingericht.

De Wvr is een Nederlandse wet die op 1 oktober 2010 in werking is getreden. Deze wet vervangt de Brandweerwet, de Wet geneeskundige hulpverlening bij ongevallen en rampen (Wghor) en de Wet rampen en zware ongevallen (Wrzo). De wet bepaalt de taken van het bestuur van een veiligheidsregio en stelt basiseisen aan de organisatie van de hulpdiensten en de kwaliteit van het personeel, informatievoorziening en het materieel. De wet regelt onder andere dat:

- de burgermeester de algemene bevoegdheid heeft tot handhaving van de openbare orde (Gw, Artikel 172) en daarbij de veiligheidsregio als coördinatie mechanisme gebruikt. De besturen van brandweer en GHOR zijn samengevoegd tot een hulpverleningsbestuur die, verplicht, de gemeentebesturen adviseren op crisis – en rampenbestrijding en ondersteuning verlenen aan de burgemeester in geval van een calamiteit,
- de burgermeester de verantwoordelijkheid heeft over alle hulpverleners die bij het incident betrokken zijn en de veiligheidsstructuur aanstuurt,
- de burgermeester verantwoordelijk is voor de kwaliteit en uniformiteit van communicatie - en informatievoorzieningen binnen de veiligheidsstructuur.

Deze context is relevant omdat er gedurende crisissituaties: strategische –, tactische – en operationele besluiten genomen worden, waarvoor informatie én de kwaliteit van de informatie, die ten grondslag ligt aan de besluiten, gebonden zijn binnen de jurisdictie[5] van het bestuur.

[3] WGR, wet van 20 december 1984, Wet gemeenschappelijke regelingen (Wgr) is een Nederlandse wet, waarin samenwerkingsverbanden worden geregeld tussen openbare lichamen zoals gemeenten, provincies en waterschappen.
[4] Wvr, wet van 11 februari 2010, houdende bepalingen over de brandweerzorg, de rampenbestrijding, de crisisbeheersing en de geneeskundige hulpverlening (Wet veiligheidsregio's)
[5] Met jurisdictie wordt de rechtsmacht bedoelt en heeft betrekking op het gebied waarover een overheidsorgaan bevoegd is, in casu de burgermeester is dat zijn gemeente of een aantal gemeenten als het een overstijgend incident betreft. Maar altijd is de jurisdictie geografisch gebonden.

1.3 Verschil tussen de koude – en warme fase van de veiligheidsregio's

Het verschil tussen de koude – en warme fase van de veiligheidsregio's, of veiligheidsorganisaties in het algemeen, is relevant voor dit onderzoek. De koude fase van de organisatie ligt tussen momenten van calamiteiten in en kenmerkt zich door voorbereiding, training en bedrijfsvoerings-aspecten. Tijdens deze fase wordt constructief gewerkt aan de professionaliteit door met elkaar te oefenen, simuleren en te organiseren.

In de warme fase van de organisatie is er sprake van een incident of calamiteit. Afhankelijk van de aard en omvang van het incident wordt de organisatie opgeschaald en werken meerdere veiligheidsorganisaties met elkaar. Het verschil in de beide fasen is relevant voor het onderzoek omdat er tijdens de warme fase andere eisen worden gesteld aan de kwaliteit van informatie dan in de koude fase. Binnen dit onderzoek wordt uitsluitend gekeken naar de: *warme fase*.

1.4 De ICT ontwikkelingen binnen de veiligheidsregio

Door de organisatorische – en bedrijfseconomische ontwikkelingen van de afgelopen jaren is het ICT complex bij veiligheidsregio's regionaal ingericht, kwetsbaar en wordt het dikwijls beschouwd als een facilitaire kostenpost. De doorontwikkeling van het ICT complex naar een volwassen centrale crisismanagement ondersteuning (Dobel, 2010) is technisch noodzakelijk, functioneel zeer gewenst, en, gegeven de stand van technologie, mogelijk. De noodzaak voor door-ontwikkeling is zeker opportuun en tegelijkertijd wordt dit versterkt door actuele bedrijfs-economische - en strategische argumenten. De verwachtingen van ICT centralisaties zijn overigens vaak veelbelovend, maar worden zeker nog niet altijd waargemaakt (Janssen & Joha, 2006).

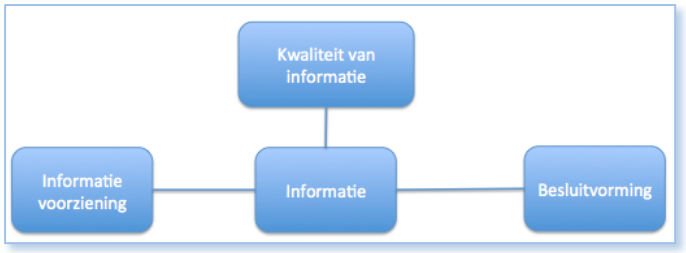
Deze ontwikkelingen zijn relevant omdat het centraliseren van ICT nu wordt gezien als een kosten – en beheersingsmaatregel. Organisaties die overstappen op een centraal ICT-model moeten daarnaast nog veel uitdagingen overwinnen zoals: informatie-kwaliteit, beveiliging, privacy, connectiviteit, interoperabiliteit en transitie (Avram, 2014).

2 De onderzoeksvraag

De hoofdvraag van dit onderzoek is: “Welke factoren zijn van belang voor het borgen van de kwaliteit van informatie bij de ICT centralisatie in een decentrale veiligheidsorganisatie”. De secundaire vraag of centralisatie van ICT bedrijfseconomisch efficiënter is wordt eveneens getoetst.

Binnen dit onderzoek wordt de relatie onderzocht tussen 2 concepten: centrale IT organisatie en de kwaliteit van informatie. Met centrale ICT organisatie wordt in dit onderzoek het gemeenschappelijke datacenter bedoeld, waarin voor 25 veiligheidsregio’s de technische infrastructuur, applicaties en data ter beschikking worden gesteld en beheerd.

Kwaliteit wordt door het Stichting Nederlands Normalisatie instituut (NEN) gedefinieerd als: ”de mate waarin het geheel van eigenschappen van een product of dienst, tot stand gekomen in een bepaald proces, voldoen aan de daaraan gestelde eisen, welke voortvloeien uit een bepaald gebruiksdoel.” In deze definitie gaat het kennelijk om de waardering die men heeft voor het product of dienst uitgaande van het gebruiksdoel. Informatie kan worden gedefinieerd als het ‘product’ van een informatievoorziening (Wang, Lee, Pipino, & Strong, 1998). Door middel van het product: ‘informatie’, zal de informatievoorziening bijdragen aan de doelstellingen van de veiligheidsorganisatie. De kwaliteit van informatie levert daarmee een bijdrage aan de kwaliteit van de besluitvorming en daarmee de kwaliteit van het primaire proces (Afbeelding 1). Zodra informatie als een product wordt beschouwd is het definiëren van een informatie levenscyclus evident en een belangrijke basis om informatie up-to-date te houden. Kwalitatieve informatie zorgt voor vertrouwen en is essentieel in het gebruik van informatie in real-time processen.



Afbeelding 1 Relatieschema tussen informatie en besluitvorming

Wang et al. [1998] identificeren 16 informatie kwaliteitsdimensies die zij verdelen over 4 categorieën: de intrinsieke kwaliteit van de informatie, de toegang tot de informatie, de context waarbinnen de informatie betekenis krijgt en de presentatie van de informatie. Een van de vier categorieën is gerelateerd aan de technische kant van de informatievoorziening en een onderwerp van discussie in de ICT centralisatie. De andere drie categorieën zijn meer gericht op de feitelijke situatie waar de informatie wordt gebruikt; decentraal.

3 Theoretische afbakening en hypotheses

Veiligheidsregio's zijn ingericht om gecoördineerde veiligheid te bieden aan een geografische omgeving. Die organisatorische transformatie van veel verschillende veiligheidsorganisaties naar 25 veiligheidsregio's is zo goed als afgerond. Het is evident dat deze organisaties continue kijken naar meer efficiency, waardoor op dit moment beoordeeld wordt op welke wijze ICT centralisatie een bijdrage kan leveren aan het verbeteren van de efficiency, effectiviteit en flexibiliteit van de veiligheidsorganisaties.

Hypothese I: *ICT centralisatie heeft een positieve invloed op de efficiency en technische beschikbaarheid van informatie.*

Uit een rapport over data center consolidaties op basis van een kosten benchmark (Computer economics, 2014, pp. 1-15) blijkt dat 53% van de kosten van een data center opgaan aan hardware en software. Ruim 31% wordt gebruik voor personeel en een kleine 8% aan de fysieke locatie en 'disaster recovery' maatregelen beide. Datacenter faciliteiten in kleine organisaties eisen een relatief hoger percentage van de IT kosten dan voor grote organisaties. In de benchmark komt verder naar voren dat organisaties met een datacenter voor de hele organisatie ongeveer 10% minder uitgeven aan ICT dan organisaties met meerdere data centers. Gegeven het feit dat op basis van de benchmark overheden en non-profit organisaties, als sector, in de middenmoot zitten voor wat betreft data center kosten, zijn deze percentages goed bruikbaar voor veiligheidsregio's.

De afgelopen 10 jaar is de digitale kwetsbaarheid een groeiende zorg. Het groeiend aantal aanvallen op publieke doelen, kritische infrastructuren en de mate van weerstand daarin versterken de bezorgdheid zelfs voor de veiligheid van burgers. Informatiebeschikbaarheid is een belangrijk aspect en daarmee de continuïteit van de informatievoorziening. Die beschikbaarheid is omgekeerd evenredig met het aantal objecten waarvoor beschikbaarheid gegarandeerd moet worden (Manadhata, 2008). Borrett et al. ondersteunen de stelling dat informatieveiligheid het best in een netwerk van samenwerkende organisaties aangepakt kan worden (Borrett, Carter, & Wespi, 2013). Rai et al. beargumenteren juist dat informatieveiligheid door de 'board of directors' vanuit een strategische – en bedrijfsbreed perspectief gemanaged moet worden (Rai & Mar, 2014).

Desai (2013) beargumenteert dat moderne data management technologieën data een betere beschikbaarheid garanderen door data juist niet op één fysieke locatie te houden, maar door deze continue 'rond te pompen'. Dat staat op gespannen voet met de genoemde jurisdictie en de huidige decentrale IT governance.

Weill et al. plaatsen de 'corporate governance' en de 'IT governance[6]' in een samenhangend

[6] Weill en Ross plaatsen de technische infrastructuur en de informatie objecten binnen het domein van de IT governance

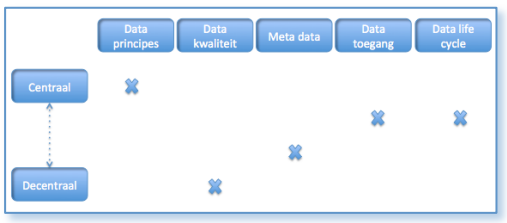
framework, waarbij de verantwoordelijkheidslijnen binnen dat framework niet verbroken mogen worden. Zij beargumenteren daarmee dat de corporate governance in lijn moet blijven met de IT governance (Weill & Ross, 2004). De keuze tussen centraal, decentraal of een hybride vorm is complex en wordt afhankelijk gesteld van de specifieke business context (McElheran, 2012).

De conclusies uit de benchmark en diverse publicaties versterken de hypothese dat efficiency, beschikbaarheid en veiligheid gemeenschappelijk, centraal en vanuit het topmanagement georganiseerd moeten worden. Dat onderbouwt de ontwikkeling naar een centrale ICT functie voor veiligheidsregio's.

Hypothese II: *Data – en informatie governance heeft een positief effect op de kwaliteit van informatie*

De juistheid en consistentie van de onderliggende databronnen bepaalt voor een belangrijk deel de kwaliteit van informatie daarmee de kwaliteit van besluitvorming en als gevolg daarvan het resultaat van het primaire proces. De relatie tussen data en informatie is beschreven in de DIKW hiërarchie (Rowley, 2007). Rowley definieert 'data' als een feit dat verifieerbaar en controleerbaar is en 'informatie' als gestructureerde data die op een of andere manier is bewerkt zodanig dat de informatie relevantie heeft in een specifieke context en daardoor betekenisvol, waardevol en bruikbaar is.

Khatri et al. definiëren data governance (Afbeelding 2) als het beleid dat de beslissings-bevoegdheid voor – en sturing op databronnen vastlegt (Khatri & Brown, 2010). Zij hebben en framework van 5 domeinen gedefinieerd: data principes, data kwaliteit, meta data, data toegang en data lifecycle, die 1:1 gerelateerd zijn aan het IT governance framework en verdeeld is over centrale – en decentrale verantwoordelijkheden (Weill & Ross, 2004). Het domein 'data kwaliteit' is een belangrijk domein omdat de daarin gedefinieerde dimensies: 'juistheid', 'tijdigheid' en 'betrouwbaarheid', dimensies zijn voor het (eind)gebruik van informatie en hebben een invloed op het vertrouwen in, en de reputatie van, informatie.



Afbeelding 2 Data governance matrix (Khatri & Brown, 2010)

Wang et al. zien informatie als een volwaardig product. Zij koppelen dit aan de strategische doelen van een organisatie en beargumenteren dat ondernemingen: informatie als een product moeten managen en informatieprocessen ('life cycle') en informatie-governance moeten inrichten. Zij benadrukken juist de contextuele – en subjectieve aspecten van informatie (Wang, Lee, Pipino, & Strong, 1998).

Hypothese III: *Crisismanagement organisaties ontwikkelen zich door ICT centralisatie tot professionele netwerkorganisaties.*

Dobel stelt in zijn onderzoek naar crisismanagement vast dat crisismanagement in de komende 5 tot 10 jaar zal groeien naar een netwerk georiënteerde multidisciplinaire organisatie met een sterke afhankelijk van een moderne technische infrastructuur, 'early warning'-systemen en sensor – en satelliet communicatie. In zijn onderzoek stelt hij met name dat: professionalisme, vertrouwen én ICT systemen, de ruggengraat vormen van moderne crisismanagementorganisaties. Dit impliceert ondermeer dat deze gecentraliseerd, gestandaardiseerd, geïntegreerd, veilig en redundant zijn uitgevoerd (Dobel, 2010).

Crisismanagementorganisaties ontwikkelen zich van lokaal georiënteerd, min of meer op zichzelf staande organisaties, naar een netwerkorganisatie die georiënteerd is op: samenwerking, communicatie, informatie en technologie, binnen de 'quadruple helix'[7] (Alfonso, Thomson, & Monteiro, 2012). Het positieve effect van goede communicatie en informatiedeling bij grote calamiteiten in de offshore olie industrie op het onderlinge vertrouwen is in 2012 aangetoond door Ibrahim et al. Zij concludeerden dat, tijdens een crisis, het vertrouwen hersteld kan worden door effectievere communicatie en informatiedeling uitgaande van de situationele context (Ibrahim & Allen, 2012).

De toekomst de informatiemaatschappij is afhankelijk van ontwikkelingen van oa.: 'the internet of everything (IoE)', big data en 'the internet of signs' (O'Leary, 2013). De ontwikkeling van het internet van signalen ('signs') met real-time sensoren is vooral belangrijk voor veiligheidsorganisaties in het preventief voorkomen van, of snel geattendeerd worden op, situaties die potentieel uit de hand kunnen lopen. Real-time business intelligence en decision support systemen winnen daardoor aan terrein om beslissingsprocessen te ondersteunen op basis van real-time data (Dobrev & Hart, 2014). Intelligence wordt door Liew (2013) benoemd als de 'missing link' in de bestaande DIKW piramide van Rowley (2007) en breidt dit uit naar het DIKIW[8] model door aan het bestaande model 'intelligence' aan toe te voegen als essentieel onderdeel voor intelligente organisatievormen; netwerken.

3.1 Interpretatie van de literatuur

Enerzijds wordt een centrale ICT context bepleit vanuit: kosten, complexiteit, standaardisatie, integratie en veiligheid. Gevoelsmatig klopt dat ook zolang de centrale ICT voorziening het fundament is waarop de 'technostructuur' (Mintzberg, 1983) van de veiligheidsorganisaties draait en gezien wordt als een generieke infrastructurele nutsvoorziening binnen de corporate governance van de organisatie.

Door toename aan informatiebronnen (sensoren, (Dobel, 2010)) en informatie ontstaat een fijnmazig decentraal informatiegrid waar veiligheidsorganisaties, met de juiste tools veel beter

[7] Met de quadruple helix wordt het samenwerkingsverband aangeduid tussen burgers, bedrijfsleven, overheid en kennisinstellingen.
[8] DKIW: Data, Informatie, Kennis, Intelligence en Wijsheid

dan nu, preventief en pro-actief kunnen handelen in samenwerking met lokale burgers, bedrijven en kennisinstituten.

De basis om kwalitatief de juiste beslissingen te nemen en adequaat te handelen blijft echter de kwaliteit van de informatie en onderliggende data. De relatie die Rowley (2007) aanlegt tussen data en informatie en de centrale – en decentrale sturing, op verschillende aspecten van data (Khatri & Brown, 2010), versterkt de kwaliteit van data en daardoor de intrinsieke kwaliteit van informatie. Door informatie als een product te beschouwen, de informatie-governance decentraal in te richten én de decentrale -, situationele[9] - en subjectieve aspecten van informatie te benadrukken, wordt de kwaliteit van informatie het best geborgd (Wang et al.).

In een netwerk georiënteerde crisismanagementorganisatie (Dobel, 2010) is er geen sprake van een keuze tussen centrale - of decentrale ICT functie, maar een combinatie van beiden verbonden in een netwerk. De centrale ICT functie wordt bestuurd vanuit de centrale governance en richt zich op de ontwikkeling van de ICT functie als nutsvoorziening, terwijl de decentrale ICT functie bestuurd wordt vanuit een decentrale governance en zich juist richt op de kwaliteit van informatie, het gebruik, de reputatie en het lokale netwerk. Beide vormen van governance interacteren continue.

[9] geografisch, jurisdictie, governance of aard en omvang van een crisis

4 Het empirisch onderzoek

4.1 Aanpak

Voor de aanpak van het empirisch onderzoek zijn een aantal functionarissen van de veiligheidsregio's, het IFV[10] en het veiligheidsberaad gevraagd te participeren. Het IFV is een landelijke organisatie dat bijdraagt aan een veilige fysieke samenleving door het versterken van de veiligheidsregio's en professionaliseren van mensen en middelen. Het veiligheidsberaad bestaat uit de voorzitters van de veiligheidsregio's en sturen de prioriteiten van de veiligheids-regio's via een strategische agenda.

Door middel van een aantal interviews is kwalitatieve data verzameld op de gestelde onderzoeks-vraag. Gedurende de interviews zijn antwoorden gegeven op voorbereidde vragen, maar zijn ook nieuwe invalshoeken ontdekt. Hierdoor is de initiële onderzoeksvraag aangescherpt en zijn de resultaten van de interviews samengevat in een exploratief model (Afbeelding 4) en getoetst aan het informatiemodel van Wang et al. (1998).

4.2 Proces

De interviews rondom het onderzoek zijn vlot gepland, afgenomen en zijn de resultaten samen-gevat in een exploratief model. Voorafgaand aan de interviews zijn de geïnterviewden geïnfor-meerd over de Nyenrode opleiding, het doel, de onderzoeksvraag en geheimhouding. Zij hebben het definitief concept rapport ontvangen en hierop positief gereageerd. De geïnterview-den zijn geïnteresseerd in het eindrapport omdat het een toegevoegde waarde kan hebben in het actuele besluitvormingsproces (juni 2015) rondom de het ontwerp en de implementatie van het strategisch programma Informatievoorziening voor de veiligheidsregio's 2015-2020 (Lanser, 2014).

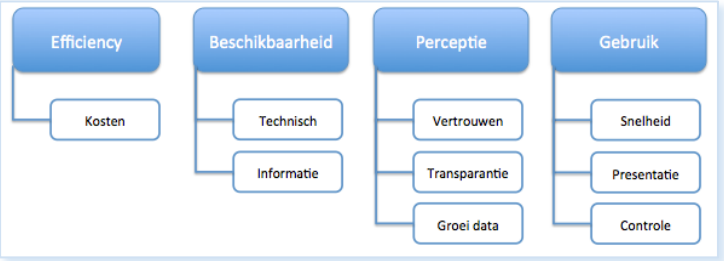
4.3 Resultaten en interpretatie van de interviews[11]

Over het algemeen gesproken [*] werd de vraag: "is een centrale ICT voorziening efficiënter dan een decentrale ICT voorziening" terughoudend positief (60%) beantwoord op basis van ervaringen met andere publieke ICT centralisaties. De vraag: "is de kwaliteit van informatie van belang in de besluitvorming over de ICT centralisatie", werd overwegend positief (80%) beantwoord. De vraag: "in welke mate de kwaliteit van informatie op dit moment meespeelt in de besluitvorming", werd echter niet of negatief (100%) beantwoord. Deze resultaten bevestigen het vermoeden dat de geïnterviewden het onderwerp: kwaliteit van informatie, wel belangrijk vinden, maar dat de bedrijfseconomische argumenten de boventoon voeren en dat zij weinig

[10] IFV is het Instituut voor Fysieke Veiligheid
[11] De referentie tussen [] verwijst naar Bijlage 1

vertrouwen hebben op efficiency van centrale voorzieningen. Het onderbouwt ook de relevantie van de onderzoeksvraag.

In Afbeelding 3 is de structuur opgenomen van de onderzoeksfactoren en kenmerken die besproken zijn met de geïnterviewden.



Afbeelding 3 Onderzoeksresultaten gemodelleerd naar factoren en kenmerken

Het onderzoeksfactor *beschikbaarheid* valt uiteen in twee kenmerken. Enerzijds is dat de technische beschikbaarheid in de zin van: 'kan ik erbij als ik het nodig heb'. Anderzijds is dat de informatie-beschikbaarheid om de eigen informatievoorziening te kunnen verrijken met informatie van ondermeer directe ketenpartners, bedrijven en social media.

Ten aanzien van het eerste kenmerk, de *technische beschikbaarheid* (continuïteit) wordt een centrale ICT voorziening door alle geïnterviewden [*] gezien als een verbetering van de huidige situatie. Het feit dat mensen wel of niet bij de informatie kunnen is een zeer belangrijk aspect tijdens crisissituaties. Bij de geïnterviewden zijn diverse ervaringen met beschikbaarheid van landelijke ICT voorzieningen [2][4][5]. Ervaringen van landelijke meldkamer-voorzieningen of het landelijk crisis – en communicatie systeem C2000 zijn overwegend positief, maar bevatten ook zeker negatieve ervaringen. Op de vraag naar de oorzaak van de negatieve ervaring wordt initieel de vinger gewezen naar de technologie. Op het moment dat de geïnterviewden een genuanceerder antwoord formuleren blijkt ook wel dat de technologie wel naar behoren werkt, maar het gebruik van de technologie vaker de oorzaak is van verstoring. Het algemene beeld valt wel positief uit naar een centrale voorziening, maar wel met de kanttekening dat bij een centrale voorziening het management team van de voorziening voor alle zaken verantwoordelijk is, daardoor een hele volle agenda hebben en de individuele veiligheidsregio's in het gedrang kunnen komen [3][4]. Aan de andere kant is er de constatering dat bij het decentrale model het management team de ICT voorzieningen 'erbij' doen en daarom niet tot de noodzakelijke kwaliteit of innovaties komen [2].

Enkele geïnterviewden hebben vanuit hun financiële verantwoordelijkheid voor henzelf vastgesteld dat zij de lokale ICT functie zeer moeilijk op een kwalitatief niveau kunnen onderhouden. En overwegen op dit moment de lokale ICT uit de regio te willen migreren. Afgezien van momentum zou de centralisatie van de ICT functie daarvoor een prima oplossing zijn. In de tussentijd overwegen veiligheidsregio's samen te werken of voor delen van de functionaliteit te migreren naar de cloud [1].

Met de huidige dreiging van cyber aanvallen zijn de geïnterviewden het helemaal eens en dat is dat centralisatie van ICT de beschikbaarheid van de ICT functie absoluut zal verbeteren. De bekende DDOS aanvallen en andere vormen van cyber criminaliteit, zoals crypto-locking, spreken zeker tot de verbeelding, maar tegelijkertijd hebben ze het inzicht dat zij in een decentraal model de ontwikkelingen nooit kunnen bijhouden [1][3]. Hiervoor zijn de financiële middelen niet voorhanden, maar ook niet de vereiste professionaliteit om controle maatregelen te bedenken, te implementeren en te beheren. Naast de technologische faciliteiten zijn ook: beleid, standaarden, afspraken, regels en richtlijnen centraal veel effectiever te maken, te implementeren en te beheren [2]. Overwegend werd de centralisatie van de ICT organisatie als positief beoordeeld vanuit het risicoperspectief.

De *informatie-beschikbaarheid* werd genoemd als het tweede kenmerk en wordt meer decentraal gewaardeerd. De geïnterviewden zijn van mening dat je landelijk niet alle data van ketenpartners kúnt en hoeft vast te leggen. Deels is de beschikbaarheid van informatie tegenwoordig dermate omvangrijk dat het onbetaalbaar wordt, maar belangrijker is het argument dat het niet hoeft. Het gaat om slim combineren van databronnen binnen en buiten de organisatie voor het beste resultaat op lokaal niveau [1]. Een goed voorbeeld is de informatie die nodig is voor crowd management. Het is in dit kader wel van belang dat de landelijke organisatie hiervoor mechanismen bedenkt en implementeert, maar vooral niet over alle informatie binnen de muren van de centrale ICT organisatie moet willen beschikken. Het ontwikkelen van eigen - of aftappen van basisregistraties [5] van andere veiligheidsorganisaties is daarin een belangrijke stap. Zodra de centrale ICT organisatie maatregelen implementeert om adequaat interne –, externe -, nationale - en lokale informatie slim te koppelen, stijgt het vertrouwen in een landelijke ICT organisatie [1].

Het onderzoeksfactor *perceptie* is een van de meest invloedrijke aspecten voor de conclusie en aanbevelingen gebleken uit de interviews. Perceptie heeft op basis van de interviews vooral een relatie met de kenmerken: vertrouwen, transparantie en de groei van data. Daarnaast wordt de perceptie beïnvloed door de technische beschikbaarheid [4] van informatiesystemen en door het gebruik.

Het kenmerk *vertrouwen* komt deels voort uit *ervaringen* uit het verleden en heeft heel erg met de menselijke factor te maken. Het beeld is dat des te verder de ICT van de eigen organisatie georganiseerd wordt, des te minder de functionarissen de informatievoorzieningen en informatie vertrouwen [5]. Een van de genoemde oorzaken was dat zodra ICT centraal is georganiseerd het management van die ICT organisatie alle aspecten van een ICT organisatie moet afdekken en de beleving is dat dit team dan ver af staat van ad-hoc en real-time events. Zonder maatregelen om de behoeften van individuele regio's 'te zien', wordt een decentrale ICT voorziening positiever gewaardeerd door de directe grip op de technische beschikbaarheid en het vertrouwen. Op het kenmerk van de technische beschikbaarheid is een verschil waargenomen tussen de rationele overwegingen en subjectieve argumenten [3].

Het geven van betekenis aan informatie is heel erg afhankelijk van de lokale fysieke situatie, waar de aard, omvang en omstandigheden van de calamiteit bepalen welke waarde of betekenis toegekend wordt aan informatie. Dit beïnvloedt het aspect vertrouwen. Met een 'centrale

database' is er wel veel informatie voorhanden, maar onduidelijk binnen welke context die informatie is vastgelegd. Die context verandert in andere omstandigheden, waardoor andere conclusies kunnen worden getrokken dan origineel bedoeld. Volgens de geïnterviewden kan door meta-data toe te voegen of de informatiebronnen per regio te scheiden het vertrouwen positief worden beïnvloed [3][5].

Het belangenmodel representeert de verschillende belangen op dezelfde informatiebronnen. Binnen veiligheidsorganisaties is er op dit aspect geen wantrouwen uitgesproken, maar wel richting andere publieke organisaties, commerciële bedrijven of terroristische groeperingen [1]. Zodra informatie centraal staat is het belang om goedschiks of kwaadschiks binnen te komen bij de centrale ICT organisatie vele malen groter en interessanter dan wanneer dat niet zo is. Informatie kan ondermeer door andere publieke organisaties met een heel andere doelstelling worden gebruikt en dat wekt geen vertrouwen. Het uithanden geven van informatie autonomie, buiten de jurisdictie van de betreffende veiligheidsregio, leidt niet tot het opbouwen van vertrouwen. Informatie kan ook commercieel interessant zijn voor derden en de informatie, over bijvoorbeeld het traject van een chloortrein, kan potentieel ook interessant zijn voor een terroristische organisatie. Het belangenmodel in combinatie met de geografische gebonden verantwoordelijkheid van een veiligheidsregio leidt tot de voorkeur voor een decentraal model. Het vertrouwen in een centrale oplossing kan worden versterkt door aandacht te schenken aan eigenaarschap van informatie en gescheiden informatieopslag per veiligheidsregio [5].

Het volgende kenmerk dat is besproken met de geïnterviewden is de *transparantie*. Transparantie wordt gezien als een harde randvoorwaarde voor centralisatie in die zin dat iedereen centraal werkt of niemand. Centralisatie is geen optie voor de deelnemers, maar een eis aan alle veiligheidsregio's in die zin dat elke deelnemer zijn informatie 'inlevert' en iedere deelnemer bij alle informatie kan. Onvolledige – of niet gedragen transparantie in de besluitvorming, of het transitieproces, leidt tot het vasthouden van 'eigen' informatie en machtsverstoringen, wat weer leidt tot lagere transparantie en toenemende weerstand op de centralisatie [4]. De suggestie is gedaan de centralisatie daarom te organiseren in een coöperatieve organisatievorm en moet derhalve op het niveau veiligheidsberaad worden geadresseerd.

Een vorm van *controlerende of toezichthoudende macht*, op de te vormen landelijke ICT organisatie, is als essentieel benoemd. Zodra de technische infrastructuur en informatie-voorzieningen worden centraal worden georganiseerd, moet op een of andere manier objectief toezicht gehouden kunnen worden. Het vertrouwen neemt toe zodra het toezicht georganiseerd wordt vanuit de individuele veiligheidsregio's [1][4]. In die zin sluit dat aan bij de coöperatieve organisatievorm [4].

Tot slot wordt de *groei van beschikbare informatie* genoemd als laatste kenmerk in de perceptie op de kwaliteit van informatie. Door de wet van de grote getallen wordt de kans vergroot dat de gepresenteerde informatie goed bruikbaar is. Informatie tijdens crises kent op dit moment een lage mate van betrouwbaarheid en beschikbaarheid [1]. De autonome groei van data, door de ontwikkelingen in de informatiemaatschappij, moet leiden tot een hogere informatie beschikbaar-heid en daarmee een hogere mate van betrouwbaarheid. Over het algemeen neigen de

geïnterviewden vanuit het onderzoeksfactor: perceptie, meer naar een decentrale of coöperatieve vorm van ICT organisatie. Door maatregelen te treffen op die kenmerken wordt een positief sentiment gevoed.

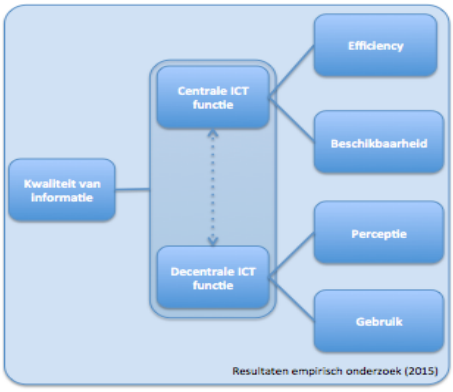
Het laatste onderzoeksfactor is het *gebruik* van informatie en richt zich met name op de menselijke factor in het gebruiken van informatievoorzieningen in relatie tot de kwaliteit van de informatie. *Snelheid* is als een van de meest essentiële kenmerken genoemd in het gebruik van informatie en het nemen van beslissingen. Hoewel Ramamoorti et al., de integriteit van informatie de hoogste prioriteit toekennen, boven presentatie en nut (Ramamoorti & Nayar, 2013), is tijdens de interviews gebleken dat tijdens crises, snelheid de belangrijkste factor is [1]. Crises zijn real-time en onverwacht, waarbij de aard, omvang en omstandigheden zeer onduidelijk is. Geïnterviewden vonden tot op zekere hoogte snelle voorziening van informatie belangrijker dan het hebben van de enige juiste informatie. Operationele besluitvorming moet binnen minuten plaatsvinden en niets doen is geen optie. Tijdens de brand in Moerdijk kwam het RIVM enige dagen na de brand met een gedegen en wetenschappelijk onderbouwde risicoanalyse van de brand. De juistheid van dat rapport stond niet ter discussie, maar het rapport was vanuit het kenmerk snelheid onbruikbaar. De geïnterviewden achten de snelheid waarmee informatie ter beschikking gesteld kan worden omgekeerd evenredig met de afstand van de ICT organisatie tot de betreffende veiligheidsregio en hebben vanuit het aspect snelheid het liefst alle informatie zelf op de telefoon of tablet.

Het volgende kenmerk is *presentatie* van informatie. De informatie is nu veelal opgeslagen in Office documenten van allerlei soorten en staat zeer versnipperd opgeslagen binnen het ICT domein. Zodra informatie adequaat wordt gepresenteerd kunnen functionarissen veel beter betekenis verlenen aan de informatie en is het handelingsperspectief eerder duidelijk. De presentatie wordt wel gekoppeld aan kwaliteit van informatie, maar een centrale – of decentrale voorziening is niet onderscheidend op dit punt volgens de geïnterviewden. Zij zien centralisatie van de ICT organisatie als een reële kans om de totale informatievoorziening te professionaliseren en waarderen dit kenmerk dus positief.

Het gebruik van data wordt tot slot volgens de geïnterviewden beïnvloed door het kenmerk: *controle*, binnen de Nederlandse overheid. Vanuit het belangenmodel en de meet – en afrekencultuur [4] hebben andere overheidsorganisaties interesse in de informatiebronnen van veiligheidsregio's. Doordat functionarissen weten dat informatie met een andere doelstelling wordt gebruikt dan binnen de veiligheidsregio's is bedoeld, voeren functionarissen informatie niet of niet volledig in. Een centrale ICT organisatie kan door 'buitenstaanders' eenvoudiger worden benaderd en het managementteam benadert dit vraagstuk anders. Mogelijk zijn zij veel eerder geneigd informatie te delen met andere overheidsorganisaties dan de veiligheidsregio's zelf zouden doen. Op dit deelaspect neigt men naar een decentrale of coöperatieve oplossing.

5 Analyse van de interviews

Op basis van de interviews is een exploratieve model ontwikkeld, dat de relatie aangeeft tussen: centralisatie of decentralisatie van de ICT functie en kwaliteit van informatie en de daarin benoemde factoren. De kwaliteit van informatie wordt bepaald door enerzijds objectieve technische factoren zoals beschikbaarheid, efficiency en veiligheid, die centraal georganiseerd moeten worden en anderzijds meer subjectieve – en contextgevoelige factoren die decentraal georganiseerd moeten worden (Afbeelding 4).



Afbeelding 4 Exploratief model

Dit resultaat wordt ondersteund door het informatie kwaliteitsmodel van Wang et al., waarin de subjectieve aspecten (geloofwaardigheid, reputatie, waarde, interpretatie, begrip, presentatie) van informatie onderscheiden worden van de objectieve aspecten (toegang, technisch en veiligheid).

Dat ICT centralisatie de efficiency, veiligheid en beschikbaarheid positief beïnvloed, wordt ondersteund door de benchmark over data center consolidaties (Computer economics, 2014) en het onderzoek van Rai et al. (2014), (Manadhata, 2008) en (Dobel, 2010). Borrett et al. (2013) en (McElheran, 2012) beargumenteren juist een hele sterke wisselwerking tussen centraal en decentraal, wat een netwerktopologie suggereert, waarin beide vormen van governance (centraal en decentraal) aanwezig zijn, continue interacteren en onderling congruent blijven (Weill et al. (2004)). Die relatie wordt in Afbeelding 4 als gestippelde lijn weergegeven.

De onderzoeken van (Khatri & Brown, 2010) en (Weill & Ross, 2004) beargumenteren dat de kwaliteit van informatie ook positief beïnvloed door het samenspel tussen een centrale – en decentrale governance. De netwerktopologie wordt ook ondersteund door het onderzoek van (Dobel, 2010) en (Alfonso, Thomson, & Monteiro, 2012), waarbij de nadruk op de lokale, subjectieve en contextuele situatie benadrukt wordt door (Ibrahim & Allen, 2012). De nadruk op dit laatste argument blijkt ook goed uit het empirisch onderzoek.

Hypothese I wordt volledig ondersteund (Tabel 1) door de resultaten van het onderzoek en de literatuur. Beschikbaarheid, veiligheid en efficiency worden positief beïnvloed door ICT

centralisatie . De onderzoeksfactoren ‘perceptie’ en ‘gebruik’ ondersteunen ICT centralisatie niet onmiddellijk.

Hypothese II wordt ondersteund door de onderzoeksresultaten, waarbij juist de interactie tussen een centrale – en decentrale governance vanuit een decentrale, subjectieve informatie context van doorslaggevende betekenis is.

Hypothese III wordt deels ondersteund door de onderzoeksresultaten. Crisismanagement-organisaties ontwikkelen zich tot netwerk georiënteerde multidisciplinaire organisaties ((Dobel, 2010) en daarin past wel centrale ICT, maar niet een volledige ICT centralisatie zoals in de uitgangspunten van dit onderzoek is bedoeld. De ICT centralisatie houdt dán onvoldoende rekening met de subjectieve – en contextuele aspecten van de kwaliteit van informatie.

	Efficiency	Beschikbaarheid		Perceptie			Gebruik		
	Kosten	Technisch	Informatie	Vertrouwen	Transparantie	Groei data	Snelheid	Presentatie	Controle
Hypothese I	+	+	N	-	-	-	-	-	-
Hypothese II	N	N	+	+	+	+	N	N	+
Hypothese III	N	+	+	N	N	N	N	N	N

(legenda: + = ondersteunt positief, +/- = ondersteunt deels, - = ondersteunt niet, N = Niet van toepassing)

Tabel 1 Relatie tussen hypotheses en empirisch onderzoek

Samenvattend kunnen de volgende relaties worden gelegd tussen de resultaten van het empirisch onderzoek en de hoofdvraag van dit onderzoek (Tabel 2).

	Efficiency	Beschikbaarheid		Perceptie			Gebruik		
	Kosten	Technisch	Informatie	Vertrouwen	Transparantie	Groei data	Snelheid	Presentatie	Controle
ICT Centralisatie	+	+	+/-	-	-	+/-	-	+	-

(legenda: + = ondersteunt positief, +/- = ondersteunt deels, - = ondersteunt niet, N = Niet van toepassing)

Tabel 2 Relatie tussen ICT centralisatie en kwaliteit van informatie

6 Conclusie en aanbevelingen

In de onderzoek wordt inzicht gegeven in de belangrijkste factoren die van belang zijn voor het borgen van informatiekwaliteit bij ICT centralisaties. De conclusie is: dat het is goed om ICT te centraliseren (efficiency en beschikbaarheid), maar de mate waarin dit effectief wordt is afhankelijk van de mate waarin de subjectieve – en contextgevoelige aspecten, van het gebruik van informatie, worden meegenomen in het ontwerp van de centralisatie. Dit adresseert de spanning tussen de bedrijfseconomische (efficiency) doelen en de doelen van het decentrale primaire proces (effectiviteit).

Een belangrijke aanbeveling is om landelijk zover als mogelijk te centraliseren, maar niet verder dan dat, en vooral aandacht te schenken aan de factoren: ‘perceptie’ en ‘gebruik’ van informatie, en afspraken te maken over de wijze waarop informatie door andere overheidsinstellingen gebruikt kan en mag worden om het vertrouwen optimaal te faciliteren. Gebrek in vertrouwen leidt tot vertraging, weerstand en het onvoldoende gebruik van de centrale voorziening, waardoor zowel de efficiency en de effectiviteit van de centralisatie afnemen.

De centrale ICT organisatie zich vooral richt op de basis technische infrastructuur, architectuur, gegevensmodel, beschikbaarheid, integratie, inkoop en beveiliging en richt de technologie zodanig in dat lokale samenwerking, communicatie en uitwisseling van informatie optimaal kan plaatsvinden op de meest efficiënte manier. De decentrale organisaties kunnen zich dan meer focussen op het gebruik – en verrijken van informatie, informatiemanagement, het doorvoeren van innovaties binnen het lokale (veiligheids)systeem en de effectiviteit van het primaire proces.

Het verschil in de besturing van: de decentrale veiligheidsregio’s (‘corporate’), een centrale technische voorziening (‘capability’) en de decentrale borging van kwaliteit van informatie (‘value’) moet samenkomen in een transparant governance stelsel. Een coöperatieve – of netwerkgeörienteerd stelsel is een mogelijke oplossing.

7 Reflectie op het onderzoek

Ik heb met veel plezier, inzet en ambitie dit onderzoek uitgevoerd. De combinatie tussen een wetenschappelijke basis, de resultaten van de interviews en een eigen opvatting zijn de uitdaging geweest. Nadenken over een relevant onderzoek en dat uitwerken heeft mij behoorlijk veel tijd en denkvermogen gekost. Vanuit de exploratiefase terug redeneren naar het theoretisch kader was superleuk en waardevol om te doen.

De wijze waarop een wetenschappelijk artikel geschreven moet worden en de ervaring die ik heb met het schrijven van artikelen vanuit een adviesrol zat enigszins in de weg. Door enkele gesprekken met dr. Bas Kodden en prof. dr. Robert Jan Blomme is die barrière weggenomen en verder aangescherpt door de beoordeling op de eerste versie van het rapport door prof. dr. Lineke Sneller. Vanuit die ervaring heb ik veel waardering gekregen voor wetenschappers die een onderwerp zo kunnen uitdiepen en beschrijven dat deze in toonaangevende journals worden gepubliceerd. Chapeau!!

Al met al was het de moeite zeker waard, ik ben tevreden met het resultaat en draagt dit korte onderzoek naar mijn mening zeker bij in de ICT ontwikkelingen van de veiligheidsregio's.

8 Literatuurlijst

Mihajlović, I. D. (2014). *The internet as medium for improving organisational development.* Sinteza.

Vukašinović, J. (2014). *Role of knowledge in information society.* Serbia: Sinteza.

Wang, R., Lee, Y., Pipino, L., & Strong, D. (1998). *Manage your information as a product.* Sloan Management Review.

Weill, P., & Ross, ,. (2004). *IT governance: How top performers manage IT decision rights for superior results.* Boston, MA: Harvard Business School Press.

Avram, M.-G. (2014). *Advantages and challenges of adopting cloud computing from an enterprise perspective* (Vol. Procedia Technology 12). ScienceDirect.

Alfonso, O., Thomson, M., & Monteiro, S. (2012). *Quadruple helix.*

Borrett, M., Carter, R., & Wespi, A. (2013). *How is cyber threat evolving and what do organisations need to consider?* (Vol. Vol. 7 Issue 2). Journal of Business Continuity & Emergency Planning.

Computer economics. (2014). *Making the case for data center consolidaton with IT spending Benchmarks* (Vol. 36). EBSCO.

Computer, E. (2014). *Making the case for data center consolidaton with IT spending Benchmarks* (Vol. 36). EBSCO.

Desai, D. (2013). *Beyond Location: Data security in the 21st centrury* (Vol. 56). Communications of the ACM.

Dobel, J. (2010). *Mission Integrity in Disaster Management* (Vol. Special Issue). Public Administration Review.

Dobrev, K., & Hart, M. (2014). *Implementation and Benefits of Real-Time Business Intelligence.* (B. S. Complete, Red.) Proceedings of the European Conference on Information Management & Evaluation.

Ibrahim, N., & Allen, D. (2012). *Information sharing and trust during major incidents: Findings from the oil industry* (Vol. Volume 63, Issue 10). Journal of the American Society for Information Science and Technology.

Janssen, M., & Joha, A. (2006). Motives for establishing shared service centers in public administrations. *International Journal of Information Management 26* , 102-115.

Khatri, V., & Brown, C. (2010). *Desinging Data Governance* (Vol. 53). Communications of the ACM.

Lanser, H. e. (2014). *Programma Informatievoorziening Veiligheidsregio's 2015-2020.* Leiden: Veiligheidsberaad.

Liew, A. (2013). *DIKIW: Data, Information, Knowledge, Intelligence, Wisdom and their Interrelationships* (Vol. Vol.2, No.10). Business Management Dynamics.

Manadhata, P. (2008). *An Attack Surface Metric.*

Martin Borrett, R. C. (2013). *How is cyber threat evolving and what do organisations need to consider?*

McElheran, K. (2012). *Decentralisation versus centralisation in IT governance* (Vol. 55). Communications of the ACM.

Mintzberg. (1983). *Designing Effective Organizations.*

O'Leary, D. (2013). *Big data, the internet of things and the internet of signs* (Vol. Vol 20 Issue 1). Intelligent Systems in Accounting, Finance & Management.

Schaefer, T. (2014). *Selecting the right cloud operating model* (Vol. Vol 3). ISACA.

Stiekema, H. (2009). *Breakout! Living in the new unreality.* Apeldoorn: Interimpoint BV.

Rai, S., & Mar, S. (2014). *Cybersecurity and the board.* IT Audit.

Ramamoorti, S., & Nayar, M. (2013). *The importance of information Integrity.* (P. Sobel, Red.) Internal Auditor.

Rowley, J. (2007). *The wisdom hierarchy: representations of the DIKW hierarchy* (Vol. 33). Journal of Information Science.

Bijlage I : Lijst met geïnterviewden

Het nummer in kolom 2 is een referentienummer dat wordt gebruikt in paragraaf 4.3 om te verwijzen naar opmerkingen van een specifiek persoon door het nummer tussen [] te plaatsen. Een verwijzing naar alle geïnterviewden wordt aangegeven als [*]

Kandidaat	Ref	Functie
Dhr. C. Post	1	directeur veiligheidsregio Zuid Holland Zuid (VR ZHZ)
Dhr. H. Lenferink	2	vz veiligheidsregio's Hollands Midden en portefeuillehouder Informatievoorziening en meldkamers binnen het db veiligheidsberaad van de veiligheidsregio's.
Dhr. W. Papersen	3	Directeur Bedrijfsvoering Instituut Fysieke Veiligheid (IFV)
Dhr. E van Zuidam	4	Directeur veiligheidsregio Groningen
Mevr. E. Langerak	5	Hoofd IM veiligheidsregio Rotterdam (VR RR)

Bijlage II : Lijst met afbeeldingen

Bijlage II : Lijst met tabellen