Defensie & Veiligheid
Oude Waalsdorperweg 63
2597 AK Den Haag
Postbus 96864
2509 JG Den Haag

www.tno.nl

T +31 88 866 10 00

TNO-rapport

TNO 2021 R10245

Vraagstukken en perspectieven voor ICT SCRM – een initiële verkenning

Datum	Februari 2021
Auteur(s)	P.E. van den Brink MSc Dr. H.L. Duijnhoven I.N. Melman MSc B. Poppink MSc Ir. A.C.M. Smulders CISSP
Aantal pagina's	40 (incl. bijlagen)
Aantal bijlagen	1
Opdrachtgever	NCSC
Projectnaam	Supply Chain Risico
Projectnummer	060.43105/01.03

Inhoudsopgave

1 Inleiding 4
1.1 Achtergrond 4
1.2 Doel 4
1.3 Aanpak 5
1.4 Leeswijzer 6

2 Het begrip supply chain in het digitale domein 7
2.1 Supply Chain management als nieuw paradigma 7
2.2 Supply Chain Management en ‘Cybersecurity’ 8
2.3 Supply Chain Risk Management in een digitale wereld 10

3 Inventarisatie ICT SCRM methoden 13
3.1 Doelstelling van methoden in inventarisatie 15
3.2 Activiteiten beschreven in methoden 16
3.3 Benodigde input voor uitvoeren van methoden 17
3.4 Uiteindelijk resultaat na uitvoer van methoden 17

4 Resultaten interviews 19
4.1 Hoe wordt naar ICT SCRM vraagstukken gekeken? 19
4.2 Hoe wordt ICT SCRM aangepakt? 20
4.3 Behoeften en verbeterpunten ICT SCRM 23

5 De basis voor een analysekader 26
5.1 Van een “veelkoppig monster” naar vijf behapbare perspectieven op de supply chain risico beheersing 26
5.2 De vijf perspectieven 29

6 Conclusie 32

7 Referenties 34

8 Ondertekening 38

Bijlage(n)
A Geïnterviewde organisaties en interviewvragenlijst

Managementsamenvatting

Door toenemende (digitale) verstrengeling van toeleverings- en productieketens kunnen verstoringen in deze ketens grote impact hebben. Organisaties zijn voor de continuïteit en veiligheid van hun processen in toenemende mate afhankelijk van een netwerk van aanbieders, waar ze niet altijd een contract mee hebben. Het belang van het in kaart brengen van afhankelijkheden en bijbehorende risico's in supply chains wordt in meerdere documenten benadrukt (CSBN, 2019; WRR, 2019). Risicomanagement op al die afhankelijkheden in de supply chain wordt steeds belangrijker, zowel om risico's inzichtelijk te maken als de beheersing met mogelijke maatregelen. Daarom is het onderwerp supply chain risico's in ICT supply chains als een belangrijk onderwerp aangemerkt in de onderzoeksagenda van het NCSC voor de periode 2019-2022. De scope van dit onderzoek is initieel om ICT supply chain risico's te identificeren.

In dit onderzoek zijn vraagstukken rondom supply chain risico's in kaart gebracht door enerzijds methoden met betrekking tot supply chain risico te analyseren en anderzijds inzichten uit de praktijk op te halen door een aantal grote Nederlandse organisaties te interviewen. Op basis van de inzichten die tijdens het onderzoek zijn opgedaan, is geconcludeerd dat er verschillende perspectieven op ICT supply chains zijn 'ingebed' in de methoden en praktijk die zijn geanalyseerd. Door de grote complexiteit van het onderwerp lopen deze perspectieven door elkaar heen en worden termen rondom supply chains, ICT supply chains en ICT SCRM (SCRM) veelal door elkaar heen gebruikt. Dit creëert een uitdaging om de vraagstukken die binnen het onderwerp spelen uit elkaar te halen en om een gezamenlijk beeld te vormen van wat deze vraagstukken precies inhouden.

Om deze reden worden deze perspectieven op ICT supply chains expliciet gemaakt. Het resultaat van dit onderzoek is een eerste aanzet voor een analysekader, waarin vijf perspectieven zijn onderscheiden. De perspectieven luiden als volgt:

- Actorenperspectief;
- ICT-producten perspectief;
- Informatieperspectief;
- ICT-diensten perspectief;
- Productiemiddelen perspectief.

Met deze perspectieven (en verdere uitwerking naar een analysemodel) kunnen bestaande ICT SCRM aanpakken en ICT supply chain risico's onderzocht en beter geduid worden om mogelijke lacunes of blinde vlekken te identificeren en gedeeld begrip te ontwikkelen. In nader onderzoek zal worden onderzocht in hoe de perspectieven ICT supply chain risico's, bestaande methodieken en de in de praktijk ervaren knelpunten kunnen analyseren en duiden.

In vervolgonderzoek zal dit analysekader verder worden ontwikkeld en toegepast. Er zal worden onderzocht of er meer perspectieven kunnen worden onderscheiden, op welke manieren het kader gebruikt kan worden en hoe het toegepast wordt om risico's te identificeren en te beheersen. Dit zal worden gedaan door het kader toe te passen op zowel casestudies in de praktijk als op methoden uit de literatuur.

1 Inleiding

1.1 Achtergrond

Het belang van het in kaart brengen van afhankelijkheden en risico's in en voor supply chains wordt in meerdere documenten benadrukt. Het CSBN 2019 wijst er nadrukkelijk op dat de afhankelijkheid van aanbieders risico's met zich meebrengt en de controleerbaarheid zeer complex is (NCTV, 2019: p.12). De WRR benadrukt dat nieuwe kwetsbaarheden door toenemende digitalisering verstoringen kunnen veroorzaken. De impact van een dergelijke verstoring kan groot zijn, aangezien organisaties deelnemen aan complexe en grensoverschrijdende toeleverings- en productieketen (WRR, 2019: p. 48). In het recentelijk gepubliceerde CSBN 2020 staat het begrip weerbaarheid centraal en worden afhankelijkheden en kwetsbaarheden in de ICT supply chain als belangrijke risico's genoemd (NCTV 2020). Maar welke organisaties, processen en digitale diensten zijn van elkaar afhankelijk? Organisaties nemen ICT als dienst af of zijn voor hun kritieke dienstverlening afhankelijk van anderen. Organisaties zijn voor de continuïteit en veiligheid van hun processen in toenemende mate afhankelijk van een netwerk van aanbieders, waar ze niet altijd een contract mee hebben. Risicomanagement op al die afhankelijkheden in de supply chain wordt steeds belangrijker. Daarom is het onderwerp ICT SCRM als een belangrijk onderwerp aangemerkt in de onderzoeksagenda van het NCSC voor de periode 2019-2022 en focust dit onderzoek zich op vraagstukken rondom het beheersen van risico's in ICT supply chains.

1.2 Doel

In dit onderzoek staan de risico's centraal die samenhangen met de steeds complexere, vaak grensoverschrijdende digitale supply chains waar wij als samenleving van afhankelijk zijn. De complexiteit komt onder andere voort uit steeds meer organisaties die gebruik maken van digitale ondersteuning, de relaties tussen organisaties in supply chains wijder verspreid raken, waar deze relaties steeds minder duidelijk worden en doordat de uitvoering en eigenaarschap van ICT-systemen vervaagd. Deze aspecten creëren een voortdurend veranderende supply chain of ook wel een web aan chains. Omgaan met de verschillende typen risico's die voortkomen uit deze complexe supply chains vergt aandacht en begrip op verschillende aspecten en niveaus van de ICT supply chain, terwijl nu juist onzekerheid heerst over de mate waarin men grip heeft op deze risico's, denk aan digitale soevereiniteit (min BZ, 2018; Min J&V, 2019). Het doel van dit onderzoek is om de vraagstukken rondom supply chains in kaart te brengen, bestaande methoden met betrekking tot SCRM te analyseren en de verschillende perspectieven die nodig zijn om naar de vraagstukken te kijken inzichtelijk te maken. De onderzoeksvragen die centraal staan zijn als volgt:

1 Welke methoden bestaan er om risico's in (ICT) supply chains te identificeren?
2 Welke supply chain-vraagstukken kunnen er worden onderscheiden?
3 Vanuit welke perspectieven kunnen ICT supply chains en de risicomanagement-aanpakken op deze supply chains inzichtelijk worden gemaakt?

1.3 Aanpak

De aanpak van dit onderzoek is iteratief en bestaat uit de volgende onderzoeksactiviteiten:

1.3.1 Uiteenzetting van begrippen in het speelveld van ICT SCRM

Aan de hand van een literatuurverkenning zijn de begrippen supply chain, keten, digitale keten en risico management verkend. Daarbij werd al snel duidelijk dat er geen eenduidig onderscheid gemaakt kan worden tussen fysieke en digitale ketens, aangezien de verwevenheid van digitale en fysieke systemen steeds verder toeneemt.

Na de literatuurverkenning zijn interne gesprekken gevoerd met TNO-experts, waarmee een beeld is gevormd over wanneer er wordt gesproken over ICT supply chains en wat de mogelijke vraagstukken en uitdagingen binnen dit onderwerp zijn. De conclusie uit deze interviews is dat SCRM geen eenduidige term is, er verschillende manieren zijn om dit in te regelen en er diverse vraagstukken leven.

1.3.2 Analyse van bestaande methoden voor SCRM

De eerste stap bestond uit een quick scan van diverse methoden, richtlijnen, handleidingen, guidelines en stappenplannen die zich enigszins richten op supply chain risico's, al dan niet binnen het digitale domein. Hiervoor is naar bronnen gezocht middels zoekwoorden als "SCRM", "ketenanalyses" en "ketensamenwerkingen". De gevonden bronnen zijn gecategoriseerd op basis van relevantie. De relevantie is beoordeeld op basis van de scope van de supply chain die in de methode wordt onderzocht, of er specifiek naar het ICT-landschap werd gekeken, of de methode inzicht biedt in risico's, de mate waarin een bron een methodische aanpak beschreef en de doelgroep waar de methode zich op richtte.

Dit heeft geresulteerd in de selectie van zes bronnen die een methode omschrijven om supply chain-analyses uit te voeren en risico's te identificeren. Alle methoden hebben een specifieke focus op het digitale domein. Deze zes methoden zijn geanalyseerd op basis van vier aspecten: doel, activiteiten, input en resultaat. Het doel van deze analyse was om een overzicht te krijgen van hoe in deze methoden naar het vraagstuk wordt gekeken en welke perspectieven daarbij worden gehanteerd. Deze analyse gaf weer dat het vraagstuk veelzijdig is en dat er een behoefte is om inzicht in de praktijk te ontwikkelen en grip te krijgen op de verschillende perspectieven waarmee naar ICT supply chains kan worden gekeken.

1.3.3 Inzicht in supply chain-vraagstukken uit de praktijk met behulp van interviews

Er zijn interviews gehouden met acht grote Nederlandse organisaties om in een vroeg stadium een beeld te vormen over hoe organisaties zelf naar vraagstukken over ICT SCRM kijken, wat hun behoeften zijn en welke aanpakken zij in de praktijk gebruiken. In alle gevallen is gesproken met één of meerdere personen die betrokken zijn bij ICT SCRM in de eigen organisaties, denk aan CISO's en medewerkers van CISO offices. In de interviews zijn de volgende onderwerpen besproken:

- ICT SCRM en de relatie tot algemeen risicomanagement in de organisatie;
- Rolverdeling, verantwoordelijkheden en mandaat met betrekking tot ICT SCRM in de organisatie;
- Welke (supply chain)risicoanalyses worden uitgevoerd en op welke wijze;

- Welke methoden, tooling, en/of instrumenten in de organisatie worden toegepast binnen dit onderwerp en waar nog behoefte aan is;
- De interactie met (keten)partners;
- De meest relevante risico's en dreigingen voor de eigen supply chain(s) en kennis over concrete typen (supply chain)risico's.

1.3.4 Ontwikkeling van een concept analysekader om naar huidige SCRM aanpakken en vraagstukken te kijken

Uit de literatuurverkenning, interne gesprekken met TNO experts en een eerste toetsing bij stakeholders kwam naar voren dat SCRM een veelzijdig vraagstuk is. Wat er onder supply chain wordt verstaan en hoe de complexiteit er uit ziet, om wat voor risico's het gaat en wanneer men kan spreken van ICT supply chains en haar risico's is een zoektocht. Het onderwerp is een parapluterm voor veel aspecten van ICT supply chain risico's. Deze bevinding is de aanleiding om hier meer duiding aan te geven en een analysekader te ontwikkelen om meer grip te krijgen op de verschillende aspecten van ICT supply chain risico's. In dit rapport wordt een concept-analysekader uiteengezet dat verschillende perspectieven duidt om naar ICT SCRM te kijken. De perspectieven bestaan uit het (1) actorenperspectief, (2) ICT-productenperspectief, (3) informatieperspectief, (4) ICT-dienstenperspectief, en (5) productiemiddelenperspectief. Deze perspectieven worden in dit rapport verder toegelicht.

1.4 Leeswijzer

In hoofdstuk drie wordt het begrip supply chain in het digitale domein uiteengezet en wordt de basis gelegd voor de vijf perspectieven. In hoofdstuk vier wordt een overkoepelende analyse gegeven van de methoden die zijn geïnventariseerd. Deze analyse geeft een overzicht van de methoden, waaruit blijkt dat er behoefte is om in de praktijk vanuit meerdere perspectieven naar deze methoden te gaan kijken. In hoofdstuk vijf worden de belangrijkste inzichten uit de interviews uiteengezet. Daarbij wordt ingegaan op hoe er binnen de organisaties van de geïnterviewden naar ICT supply chain vraagstukken wordt gekeken, hoe ICT SCRM wordt aangepakt en waar men behoefte aan heeft. In hoofdstuk zes wordt het concept analysekader gepresenteerd, waarbij wordt ingegaan op de vijf perspectieven. In hoofdstuk zeven wordt gereflecteerd op hoe deze onderzoeksresultaten samen komen en worden onderzoeksrichtingen voor de toekomst gepresenteerd.

2 Het begrip supply chain in het digitale domein

2.1 Supply Chain management als nieuw paradigma

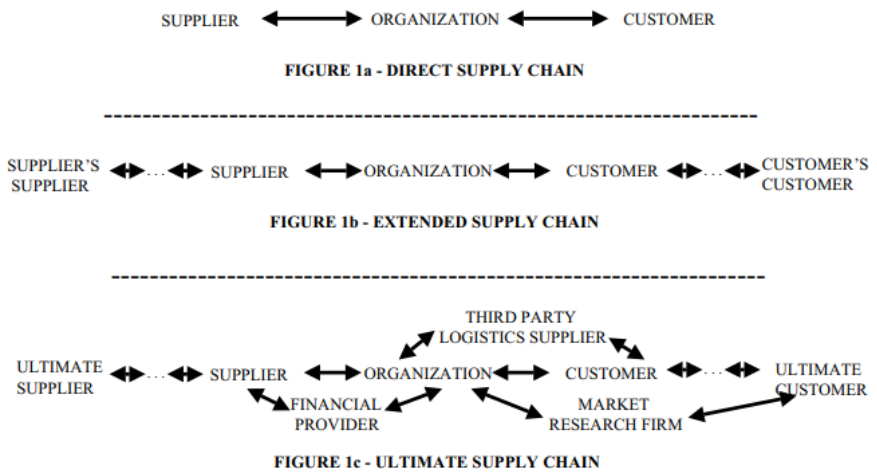
Het begrip supply chain en de gerelateerde term supply chain management hebben in de laatste jaren van de 20ste eeuw een steeds prominentere plaats gekregen in wetenschappelijk onderzoek op het gebied van onder andere business management, logistiek en operationele analyse (Mentzer et al., 2001). Deze toenemende aandacht voor supply chain en supply chain management hangt samen met globalisering waardoor steeds meer elementen van supply chains over de hele wereld verspreid zitten en er in algemene zin door bedrijven anders moest worden gekeken naar de effectiviteit van bedrijfsprocessen en inkomende en uitgaande stromen. Het betekende dat bedrijven meer aandacht gingen schenken aan de relaties met hun suppliers omdat dit als belangrijke sleutel werd gezien voor de betrouwbaarheid en continuïteit van hun eigen levering aan klanten (Mentzer et al., 2001). Ook technologische en economische ontwikkelingen hebben ertoe bijgedragen dat er meer aandacht is gekomen voor managementconcepten om supply chains efficiënter en betrouwbaarder te organiseren (Mentzer et al., 2001). Lambert & Cooper (2000) spreken in dit kader over een van de belangrijkste paradigmaverschuivingen in het moderne business management. Concurrentieposities gaan niet langer uitsluitend over het succes van het ene bedrijf ten opzichte van het andere bedrijf, maar over het succes (efficiëntie en betrouwbaarheid) van de ene supply chain ten opzichte van de andere supply chain. Zelfs zijn er vrijwel geen bedrijven meer die als volledig autonome entiteiten functioneren omdat elk bedrijf op één of andere manier onderdeel is van één of meerdere supply chains (Lambert & Cooper 2000).

> *"In this emerging competitive environment, the ultimate success of the single business will depend on management's ability to integrate the company's intricate network of business relationships"* (Lambert & Cooper 2000: 65).

In hun meta-analyse merken Mentzer et al. (2001: 2-3) op dat er veel verschillende definities en conceptualisaties van supply chain en supply chain management worden gehanteerd, wat in hun ogen niet bijdraagt aan de ontwikkeling en verbetering van supply chain management-aanpakken. In de basis is een supply chain een systeem dat is opgebouwd uit alle organisaties, mensen, technologie, activiteiten, informatie en bronnen (grondstoffen, hupmiddelen) die benodigd zijn om een product of een dienst aan een (eind)gebruiker te leveren (ENISA, 2015; Van Ruijven & Keijser, 2017). Vaak wordt in definities benadrukt dat het gaat om het totale systeem van opwaartse en neerwaartse stromen van producten, diensten, financiering en informatie tussen de betrokken entiteiten die er gezamenlijk voor zorgen dat het eindproduct bij de klant terecht komt (Mentzer et al., 2001).

Naast een analyse van verschillende definities van het begrip supply chain geven Mentzer et al. (2001: 5) ook aan dat er verschillende gradaties van complexiteit zijn waarmee men naar een supply chain kan kijken (figuur 1). In de meest basale vorm (*direct supply chain*) wordt een supply chain gezien als een simpele keten tussen een organisatie en haar directe toeleveranciers enerzijds en de directe afnemers

(klanten) anderzijds. In de volgende gradatie van complexiteit spreken Mentzer et al. van een *extended supply chain* en worden ook de toeleveranciers van de toeleveranciers en de afnemers van de afnemers meegenomen als onderdeel van de supply chain (2001: 5). In de meest complexe vorm (*ultimate supply chain*) moet de supply chain worden gezien als een netwerk waarin ook alle andere entiteiten worden meegenomen die een rol spelen in de voortbrenging van een product of dienst.



Figuur 1 Gradaties van complexiteit van het begrip supply chain (Mentzer et al., 2001:5).

Ook Lambert & Cooper (2000) benadrukken dat een supply chain in feite niet een simpele keten is van één-op-één relaties tussen partijen, maar een netwerk van meerdere bedrijven en typen relaties.

2.2 Supply Chain Management en 'Cybersecurity'

In deze artikelen wordt de rol van informatiestromen wel als onderdeel van de supply chain benoemd en er wordt ook al langer aandacht besteed aan specifieke digitale aspecten in supply chain management (zoals e-facturatie, uniforme product- of barcodes, tracking & tracing). Toch wordt pas in 2000 het eerste artikel gepubliceerd waarin expliciet gesproken wordt over een 'cyber supply chain' (Ghadge et al., 2019). Vanaf dat moment krijgen cyber-gerelateerde supply chain vraagstukken in toenemende mate aandacht. Hierbij zijn verschillende begrippen en concepten ontstaan die wel gerelateerd zijn, maar verschillende kanten van het vraagstuk benadrukken of specifieke afbakeningen hanteren.

Het gaat hierbij om uiteenlopende begrippen zoals 'e-supply chains', 'cyber supply chains', 'IT system supply chains', 'information security in supply chains', 'supply chain cyber security', of 'digital supply chains', waarbij deze begrippen niet altijd expliciet gedefinieerd worden, sommige termen voor verschillende zaken worden gebruikt én soms verschillende termen gebruikt worden om hetzelfde aan te duiden (e.g. Ghadge et al., 2019; Johnson, 2019).

Kijkend naar de manier waarop de toenemende aandacht of urgentie van cyber-gerelateerde supply chain-onderwerpen wordt toegelicht of onderbouwd, kunnen er grofweg drie invalshoeken worden onderscheiden:

1 Aandacht voor het toenemend gebruik van informatie technologie om (klassieke) supply chains efficiënter te maken;
2 Aandacht voor de toenemende verwevenheid van fysieke en digitale systemen (cyber-physical systems);
3 Focus op de supply chain van ICT-producten en diensten zelf.

In alle gevallen geldt dat wordt benadrukt dat de relaties in het netwerk van supply chain-entiteiten door de toename van informatietechnologie veranderen en vaak nog complexer zijn geworden en dat er ook nieuwe (cyber)risico's en kwetsbaarheiden zijn ontstaan. Hieronder wordt elk van deze invalshoeken kort toegelicht. Overigens laten deze drie invalshoeken zien dat er in de literatuur verschillende aspecten worden benadrukt van het belang van de relatie tussen cybersecurity en supply chains. Het betreffen geen tegengestelde opvattingen of definities. De onderwerpen die worden benadrukt zijn complementair en laten vooral zien dat het onderwerp complex en veelzijdig is.

2.2.1 Cyber als toevoeging aan klassieke supply chains

Het is niet eenvoudig om duidelijk af te bakenen wanneer er sprake is van een cyber supply chain of wanneer het een 'gewone' (logistieke of fysieke) supply chain betreft. Immers, in vrijwel alle toeleveringsketens wordt in enige mate gebruik gemaakt van ICT-diensten en -producten. Organisaties gebruiken in toenemende mate informatie technologie om producten, diensten en processen effectiever en efficiënter uit te voeren (Barlow & Li, 2007; Büyüközkan & Göçer, 2018; Kahn & Sepúlveda Estay, 2015; Smith et al., 2007). Dit betekent dat in elke supply chain enige mate van 'cyber' aanwezig is.

> *"…technology and Internet infrastructure have advanced to the point that well-functioning, efficient supply chains are dependent on a range of software and hardware working in tandem, gathering and transmitting vital data about shipments, inventory, and even the condition of equipment used to manufacture parts." (Wainstein, 2018).*

Desalniettemin maken Ghadge et al. (2019) een onderscheid tussen traditionele, fysieke supply chains enerzijds en cyber supply chains anderzijds. Bij fysieke supply chains ligt de nadruk op de beweging van producten, financiën en informatie tussen entiteiten (Peck, 2006). In een cyber supply chain wordt intensief gebruik gemaakt van ICT om processen te optimaliseren, waardoor partijen op allerlei manieren direct (en indirect) verbonden zijn en de 'bureaucratische laag' er voor een deel uit is verdwenen (Smith et al., 2007). Ghadge et al. (2019) erkennen dat ICT ook in een traditionele supply chain incidenteel een rol speelt, maar niet in dezelfde mate als in een cyber supply chain. Er is hier dus wellicht eerder sprake van een continuüm dan van een duidelijk onderscheid. Wat duidelijk is, is dat supply chains in toenemende mate gebruik maken van informatie technologie en dat verandert de manier waarop supply chains opereren. Dit breng ook andere typen kwetsbaarheden en risico's met zich mee.

2.2.2 Cyber-physical supply chains

In een ander deel van de literatuur wordt niet zozeer gekeken naar het verschil tussen een fysieke of cyber supply chain, maar wordt aandacht gevestigd op de toenemende verwevenheid van de fysieke en digitale aspecten binnen een supply chain. Door vergaande digitalisering raken bedrijfsprocessen en informatievoorziening steeds meer met elkaar verweven. Het zijn geen aparte systemen meer maar er is sprake van een cyber-fysiek systeem (DiMase et al., 2015; Van Ruijven en Keijser, 2017). Zo kan bijvoorbeeld ook steeds minder goed onderscheid gemaakt worden tussen software en fysieke informatiesystemen (hardware) omdat deze grenzen meer vervagen (software en hardware zijn veel vaker vervlochten) waardoor er met meerdere aspecten rekening moet worden gehouden, ook als men kijkt naar supply chains (Gelevert et al., 2017). Dit zorgt er ook voor dat risicobeheersing in de context van *cyber-physical systems* en supply chain management steeds complexer wordt (e.g. DiMase et al., 2015; Wells et al., 2014).

2.2.3 ICT supply chain

Tenslotte gaat een groot deel van de literatuur specifiek over de supply chain van ICT-producten en -diensten. Hierbij wordt benadrukt dat het landschap van ICT-leveranciers steeds complexer wordt en dat het daardoor voor afnemers van ICT-producten moeilijk is om grip te krijgen op de toeleverende partijen (e.g. Bartol, 2014; Boyson, 2014; Linton et al., 2014).

ICT supply chains bestaan uit organisaties die hardware, software en (informatie) diensten produceren en verkopen, bijvoorbeeld ICT-dienstverleners of softwareleveranciers. Een ICT supply chain begint bij het ontwerpen van een ICT-product of -dienst en omvat handelingen en processen aangaande ontwikkeling, inkoop, productie en distributie (Boyens et al., 2015a). ICT-producten en -diensten bestaan doorgaans uit veel componenten die bij verschillende leveranciers vandaan komen. Daarnaast is het belangrijk om de gebruiker van deze diensten en producten ook als onderdeel van de supply chain te zien, zij passen deze producten en diensten toe in hun eigen context (gericht op hun primaire bedrijfsprocessen). Een andere factor die maakt dat ICT supply chains complex zijn is dat bij digitale producten, in tegenstelling tot fysieke producten, de ‘grondstoffen’ (halffabricaten) oneindig hergebruikt kunnen worden en aangepast op elk punt in de keten. Doordat ook de productiemiddelen (tools om software te maken en informatie te verwerken) vaak breed voorhanden zijn, is er ook een diversiteit aan partijen dat deze halffabricaten en producten maakt en aanpast. Het samenstellen van halffabricaten (informatie/software-producten of -diensten) kan vervolgens ook weer op verschillende manieren plaatsvinden.

2.3 Supply Chain Risk Management in een digitale wereld

Voorgaande paragrafen laten zien dat het begrip supply chain een diffuus karakter heeft en dat dit door de toenemende aandacht voor ‘cyber’ of ‘digitale’ aspecten van supply chain management alleen maar complexer wordt. Voor organisaties betekent deze digitalisering dat er ook allerlei nieuwe vormen van supply chain risico’s ontstaan. Zo introduceert het toenemend gebruik van ICT bijvoorbeeld meer directe koppelingen tussen (systemen van) partijen zonder dat daar nog een bureaucratisch proces tussen zit (Smith et al., 2007). Daarnaast worden veel digitale diensten uitbesteed aan derde partijen (en in toenemende mate in de vorm

van cloud diensten), vaak ook in een ander land, waardoor activiteiten meer op afstand van de organisatie komen te staan (Boyson, 2014; Büyüközkan & Göçer, 2018; Wainstein, 2018; Windelberg, 2016). De ICT-middelen die door organisaties worden gebruikt komen tot stand in een complex netwerk van leveranciers, waardoor het voor organisaties moeilijk is om zicht te hebben op de oorsprong, werking, betrouwbaarheid en veiligheid ervan (e.g. Bartol, 2014; Boyson, 2014; Linton et al., 2014).

Al deze ontwikkelen zorgen ervoor dat organisaties voor de continuïteit en veiligheid van hun bedrijfsvoering in toenemende mate afhankelijk zijn van een netwerk van ICT-aanbieders en -gebruikers, wat het aanvalsoppervlak voor cyberaanvallen met keteneffecten via derde partijen vergroot (e.g. ENISA, 2015; AON, 2019; Soare, 2020; Ghadge et al., 2019). Naar schatting vindt zo'n 80% van de cyberaanvallen wereldwijd plaats via de supply chain (Boyens, 2016).

Een bekend voorbeeld van een ICT supply chain incident is de ontdekte kwetsbaarheden in de systemen van Citrix (2019), waarbij een groot aantal organisaties wereldwijd risico liep om gehackt te worden en (vergaande) maatregelen moesten treffen. In Nederland zijn naar schatting zo'n 3700 organisaties getroffen (NCTV, 2020). Ook het incident NotPetya (2018) zorgde ervoor dat via veelgebruikte administratiesoftware een wiperware zich kon verspreiden over een groot aantal organisaties wereldwijd (Crosignani et al., 2020; Greenberg, 2018; NCTV, 2019). De LockerGoga ransomware aanvallen (2019) gericht op industriële controle systemen, hadden vergaande gevolgen op de logistieke en productieprocessen van de getroffen industriële organisaties (Reich, 2020). Deze gebeurtenissen, hoewel slechts een kleine selectie, zorgen voor steeds meer onzekerheid en zorgen over de risico's in de (digitale) supply chains en de weerbaarheid tegen deze risico's. In recente publicaties van onder andere de NCTV, de WRR, de Cyber Security Raad en het CBS wordt gewezen op de risico's die samenhangen met de steeds complexere, vaak grensoverschrijdende digitale supply chains waar wij als samenleving van afhankelijk zijn en de onzekerheid die heerst over de kennis en mate van grip die men heeft op deze risico's (NCTV, 2019; 2020; WRR, 2019; Cyber Security Raad, 2016; CBS, 2018).

Deze ontwikkelingen roepen de vraag op wat dit betekent voor de beheersing van deze risico's? Vergen deze typen risico's een andere aanpak dan 'normale' risicomanagementprocessen?

Risicomanagement is een proces dat in organisaties wordt toegepast om te bepalen wat adequate maatregelen zijn om ongewenste situaties te voorkomen. In de kern bestaat risicomanagement uit de volgende stappen:

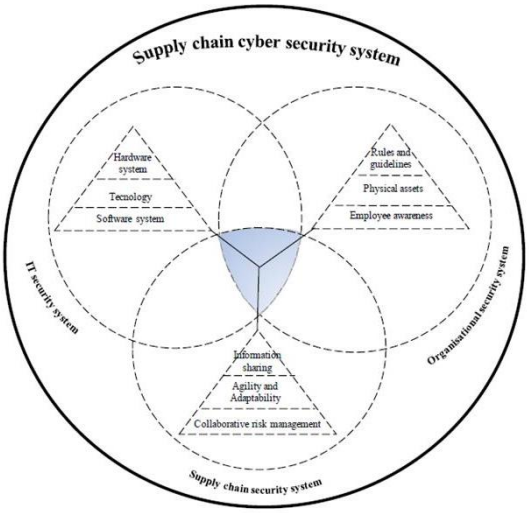
- Het identificeren van risico's (dreigingen) voor het behalen van een bepaalde doelstelling (of set van doelstellingen);
- Het beoordelen wat de kans/waarschijnlijkheid is van optreden van die gebeurtenissen;
- Het inschatten wat de impact is als deze gebeurtenissen zich voordoen;
- Het bepalen van adequate maatregelen (preventie, beheersing) adequaat zijn (kosten-baten afweging).

De manier waarop risicomanagement wordt ingericht kan grofweg worden opgesplitst in twee benaderingen: 1) een aanpak waarbij verschillende soorten

risico's afzonderlijk worden geadresseerd en 2) een integrale aanpak waarbij alle risico's vanuit een gezamenlijk, strategisch kader worden beschouwd en behandeld (e.g. Hoyt & Liebenberg, 2011; Nocco & Schultz, 2006). De laatste jaren heeft de integrale aanpak aan populariteit gewonnen, hoewel het nog sterk verschilt in welke mate van detail de integratie van verschillende typen risico's plaatsvindt.

Kijkend naar het vraagstuk van (cyber) SCRM, is hiervoor ook een integrale aanpak nodig (Boyson, 2014; Curkovic et al., 2013; DiMase et al, 2015; Ghadge et al., 2012; Ghadge et al., 2019). Het feit dat ICT geïntegreerd is in vrijwel alle bedrijfsprocessen zorgt ervoor dat er eigenlijk geen andere optie is dan risico's integraal te beschouwen. Toch wordt (cyber) SCRM in toenemende mate ook als aparte aanpak of methode geadresseerd (zie hiervoor onze analyse in het volgende hoofdstuk). Hierbij wordt in sommige gevallen expliciet benoemd dat het belangrijk is om de implementatie daarvan te integreren met organisatie-brede risicomanagement-processen (e.g. Boyens et al., 2015b).

In veel van de publicaties over ICT/cyber SCRM wordt de nadruk gelegd op een specifiek aspect van de thematiek, zoals het management van de risico's die voortkomen uit de complexiteit van de ICT-producten en -diensten supply chain of de risico's die voortkomen uit de toenemende afhankelijkheid van ICT voor supply chains. Deze verschillende specifieke invalshoeken bieden goede aanknopingspunten en verdieping, maar lijken er ook voor te zorgen dat het overzicht en de integratie ontbreekt. Ghadge (2019) introduceert een holistisch conceptueel model voor cyber security van supply chains waarbij ze de nadruk leggen op de relatie tussen IT security, organisatie security en supply chain security (zie figuur 2).



Figuur 2 Conceptueel model voor 'supply chain cyber security system' (Ghadge et al., 2019).

Deze denkrichting is een goed startpunt, maar geeft nog weinig houvast voor risicomanagement processen. De complexiteit van supply chain cyberrisico's vraagt eerst om een duidelijk analysekader alvorens de thematiek goed te integreren met risicomanagement processen (al dan niet gebruikmakend van specifieke onderliggende methoden). De aanzet tot een analysekader zoals in hoofdstuk 5 wordt gepresenteerd is hiervoor een eerste stap.

3 Inventarisatie ICT SCRM methoden

Naast het raadplegen van literatuur waarin het begrip (ICT) supply chain wordt besproken is het ook van belang om een beeld te vormen bij bestaande methoden om ICT SCRM toe te passen. Hiervoor is een inventarisatie gedaan van enkele bestaande methoden. Het doel van deze inventarisatie is een beeld te vormen van de aspecten van SCRM die er in deze methoden worden belicht, hoe deze methoden (globaal) werken en wat de scope van de methoden is met betrekking tot het ICT-landschap. Deze inventarisatie heeft geholpen bij het verder inzichtelijk maken van de veelzijdigheid van het vraagstuk van ICT SCRM.

Om te komen tot een selectie van methoden voor de inventarisatie is als eerste breed gezocht naar literatuur en overige documentatie die enigszins gericht zijn op supply chain-risico's, al dan niet binnen het digitale domein. Dit was een quick scan en resulteerde in een longlist. Hierbij is gebruik gemaakt van zoekwoorden met betrekking tot SCRM, ketenanalyses en ketensamenwerkingen. Er is zowel gezocht naar Nederlandse bronnen als internationale Engelstalige bronnen. De gevonden bronnen zijn gecategoriseerd op basis van relevantie voor verdere analyse. Voor het bepalen van de relevantie hebben we verschillende aspecten meegenomen, namelijk:

- Past de genoemde scope/definitie van de supply chain in de bron bij ons onderzoek? Behandelt de bron de ICT supply chain of wordt expliciet aandacht besteed aan het digitale domein?
- Beschrijft de bron een algemeen uitvoerbare aanpak (methode)? Eenmalige analyses van een specifieke supply chain, of andere soortgelijke publicaties zijn minder relevant dan documenten die een toepasbare methode of aanpak toelichten.
- Richt de methode zich op het verkrijgen van verbeterd inzicht en/of verbeterde beheersing van risico's gerelateerd aan ICT supply chains?

Twee overige aspecten die impliciet zijn meegenomen bij de selectie van bronnen zijn de betrouwbaarheid van de bron en de kwaliteit van de publicatie. Bij het selecteren van relevante methodes is geen assessment gedaan van welke methodes veel gebruikt worden door de doelgroepen van het NCSC. Dit viel voor dit onderzoek buiten scope.

Dit heeft geresulteerd in de selectie van zeven bronnen die een methode omschrijven om de beheersing van supply chain risico's te verbeteren, of in ieder geval één of meer aspecten die daar aan bijdragen. Deze methoden zijn specifiek gericht op het identificeren van risico's in supply chains met een focus op ICT. De in deze bronnen beschreven methoden zijn op basis van diverse aspecten zoals scope, doel, aanpak en benodigdheden bekeken, met als doel een eerste samenvattend beeld te krijgen van de methoden die bruikbaar zijn voor het onderling vergelijken van methoden en het identificeren van mogelijke 'gaps'. Ook droeg de inventarisatie van deze methoden bij aan het verkrijgen van inzicht in de veelzijdigheid van het vraagstuk. De volgende paragrafen beschrijven de resultaten van deze inventariserende analyse van de geselecteerde methoden. In tabel 1 staat een kort overzicht per methode.

Tabel 1 Overzicht methoden voor (ICT) SCRM[1]

	Doel	Activiteiten	Input	Resultaat
NIST	Methode voor het integreren van SCRM in bestaande risico management activiteiten, binnen de scope van ICT-producten en -diensten, specifiek gericht aan Federale agentschappen in de VS.	In de methode worden de volgende stappen beschreven: • Framing van de risico's. • Identificeren en beoordeling risico's. • Selecteren, personaliseren en implementeren van maatregelen. • Continue monitoren risico's.	Er worden stakeholders en uit te voeren activiteiten geformuleerd voor drie 'tiers' (strategie, operatiën/bedrijfsprocessen, informatiesystemen).	In kaart brengen en beoordelen van supply chain risico's.
MITRE 1	Catalogus/framework voor het in kaart brengen van mogelijke kwetsbaarheden bij aankoop en/of ontwikkeling van ICT-systemen, specifiek gericht op het Ministerie van Defensie van de VS.	Het document biedt een framework/catalogus met uitleg over aanvalspatronen. Ook wordt het framework toegepast op een voorbeeld om duidelijk te maken hoe het kan worden gebruikt.	Informatie over de componenten (e.g. hardware, software, firmware) van een aan te schaffen ICT-systeem.	Een overzicht van mogelijke technische aanvallen waar een specifiek ICT-systeem kwetsbaar voor kan zijn.
MITRE 2	Dit is een vervolg op MITRE 1-methode, waarbij de catalogus wordt aangevuld met mitigatie maatregelen uit een bestaand framework (MITRE Cyber Resiliency Engineering Framework (CREF)) om mogelijke mitigatie maatregelen te bepalen voor aankoop en/of ontwikkeling ICT-diensten.	Het document biedt een voorbeeld en richtlijnen om voor een gekozen ICT-systeem te bepalen wat de mogelijke mitigatie maatregelen zijn a.d.h.v. CREF.	Expert kennis over ICT-systeem en kennis van MITRE CREF framework om deze methode toe te passen en daarmee de beste mitigatie maatregelen te bepalen voor een ICT-systeem.	Voor alle fases in het aankoop/ontwikkel proces een inventarisatie van kwetsbaarheden en mogelijke mitigatie maatregelen.
CSR-SCR	Methode voor het, gezamenlijk met directe ketenpartners, in kaart brengen en opstellen van beheersingsmaatregelen van cyberrisico's in informatieverwerkingssystemen voor de vooraf geïdentificeerde kritieke bedrijfsprocessen voor een specifieke keten, gericht op NLD vitale infrastructuur.	De methode onderscheid de volgende stappen: • Bepalen scope, • Beschrijven keten, • Bepalen impact verstoring keten, • Vaststellen omvang cyberdreigingen en -risico's, • Opstellen maatregelen.	Informatie van experts in betrokken de organisaties.	Kwalitatief onderbouwd overzicht van processen en systemen van een supply chain en benodigde maatregelen.
MITIGATE	Methode voor het, gezamenlijk met ketenpartners, in kaart brengen en opstellen van beheersingsmaatregelen van cyberrisico's in ICT-systemen van alle betrokken organisaties, ontwikkeld voor maritieme sector.	De methode omvat deze stappen: • In kaart brengen supply chain, • Analyse cyberdreigingen, • Analyse kwetsbaarheden, • Impactanalyse, • Risicoanalyse, • Opstellen maatregelen.	Informatie van experts in betrokken organisaties en expertise over de diverse wiskundige modellen die in de methode worden gebruikt.	Kwantitatief onderbouwde risico inschatting en mitigerende maatregelen.
ISO	Methode voor het reduceren en beheersen van risico's voor zowel aanbieders als afnemers van ICT-diensten en -producten, bedoeld voor elk type organisatie die deel uit maakt van een supply chain, met name voor de acquisitie van ICT-diensten en -producten.	Deze methode bevat een standaard van hoe men het afnemen/aanbieden van ICT-diensten/-producten veiliger maakt. Speciale aandacht gaat uit naar inbedding in organisatorische processen en focus op eenduidige hantering van risico management binnen de organisatie en/of keten.	Er wordt gesteld dat expertise en middelen beschikbaar gesteld moeten worden. De benodigde expertise en middelen worden niet expliciet gemaakt.	Inzicht in en veilig maken van de afname/aanbieding van ICT supply chain, met name de gebruikte ICT-producten en -diensten.
CISA	Voorbeeld hoe NIST-methode gebruikt kan worden om dreigingen die samenhangen met ICT-leveranciers, ICT-producten en ICT-diensten (aansluiten bij C-SCRM) in kaart te brengen.	In deze methode komen de volgende stappen aan bod: • Dreigingen identificeren, • Dreigingen categoriseren, • Scenario's ontwikkelen, • Scenario's beoordelen en documenteren.	Inzet van experts om genoemde activiteiten uit te voeren.	Opsomming en categorisering van (algemene) dreigingen/risico's gerelateerd aan ICT-leveranciers.

[1] Zie referentielijst voor expliciete methoden.

3.1 Doelstelling van methoden in inventarisatie

Ondanks dat alle methoden beogen op enige manier bij te dragen aan het verbeteren van de beheersing van ICT supply chain risico's, verschillen de methoden in doelstelling, scope en doelgroep.[2]

Zo beoogt zowel de NIST- als de ISO-methode een integrale oplossing voor ICT SCRM. NIST richt zich hier specifiek tot federale agentschappen in de VS en beperkt de supply chain scope tot ICT-diensten en -producten. Dit impliceert dat NIST zich vooral richt op het afnemers perspectief van SCRM aangezien federale agentschappen vooral ICT-diensten en -producten afnemen. In tegenstelling tot de NIST-methode, richt ISO zich niet tot een specifieke doelgroep. Bovendien is ISO zowel te gebruiken voor afnemers als aanbieders van ICT-diensten en -producten. Beide methoden besteden ook aandacht aan het inbedden van SCRM in bestaande risicomanagementprocessen.

Alle andere behandelde methodieken focussen op een deelaspect van ICT SCRM. Zo beperkt MITRE 1 zich slechts tot het in kaart brengen van kwetsbaarheden in ICT-systemen die ontstaan vanuit de supply chain, expliciet voor de acquisitie fase en/of ontwikkelingsfase van een systeem. Hierbij richten de auteurs zich specifiek tot het Ministerie van Defensie van de VS. Het voordeel van deze beperkte focus is dat deze methode dieper in gaat op dit deelaspect van ICT SCRM. MITRE 2 is een vervolg op MITRE 1 en breidt de methode uit met een methodiek voor het bepalen van beheersingsmaatregelen voor de geïdentificeerde kwetsbaarheden in de MITRE 1-methode.

De CSR-SCR- en MITIGATE-methoden dienen een soortgelijk doel als de MITRE 2-methode, namelijk het in kaart brengen van risico's die ontstaan vanuit de supply chain en vervolgens het bepalen van beheersingsmaatregelen voor deze risico's. Echter adviseren de CSR- en de MITIGATE-methode om dit gezamenlijk met andere ketenpartners op te pakken. Zo kunnen namelijk ook ketenafhankelijkheden gemakkelijker en op een integrale manier in kaart worden gebracht. De CSR SCR-methode richt zich specifiek tot aanbieders van (Nederlandse) vitale processen en is bedoeld voor het identificeren en beheersen van supply chain risico's voor informatieverwerkingssystemen maar ook de continuïteit van bedrijfsprocessen. MITIGATE, daarentegen, is ontwikkeld voor de maritieme sector, en beperkt zich daarbij tot het identificeren en beheersen van supply chain risico's voor IT-systemen van de betrokken ketenpartners.

Naast de hierboven beschreven methodieken is er ook een bron geraadpleegd waarin de eerder beschreven NIST-methodiek wordt toegepast op een specifiek voorbeeld, in de CISA-publicatie. Het kan door de lezer gebruikt worden als voorbeeld voor hoe men de NIST-methodiek kan toepassen in de praktijk.

[2] De geanalyseerde methoden gebruiken verschillende termen (zoals ICT-systemen, informatieverwerkingssystemen, of IT-systemen). Deze termen zijn niet direct synoniemen aan elkaar noch zijn ze allen verschillend. In dit hoofdstuk is per methode de terminologie van de betreffende publicatie aangehouden.

3.2 Activiteiten beschreven in methoden

Alle behandelde publicaties beschrijven op enige wijze een methodische aanpak. In dit hoofdstuk zullen de verschillende activiteiten in deze methodieken worden toegelicht.

De NIST-methode omschrijft bijvoorbeeld vier belangrijke activiteitencategorieën, namelijk, framing van risico's & context bepaling, identificeren & beoordelen van risico's, respons op risico's en continue monitoring van risico's. Per activiteitencategorie geeft NIST suggesties voor specifieke strategische, operationele en technisch inhoudelijke activiteiten. Bij de beschrijving van deze activiteiten is speciale aandacht voor de inbedding van de ICT SCRM-activiteiten met reguliere risico management activiteiten. Zo wordt geadviseerd om op strategisch niveau, onder de categorie framing van risico's & context bepaling, naast het maken van beleid op ICT SCRM ook te zorgen dat dit beleid wordt geïntegreerd in het algemene risico management beleid van de organisatie.

De MITRE1- en MITRE2-methoden beschrijven geen duidelijke chronologische methodische aanpak, maar bieden een framework om mee te werken. Deze publicaties beschrijven de activiteiten in relatie tot het ICT-systeem zelf. Daarbij ligt de focus bij activiteiten die technisch van aard zijn, zoals het categoriseren van de verschillende componenten van een systeem in hardware, software, firmware en systeeminformatie. Het organisatorisch borgen van deze activiteiten in een continu proces binnen de organisatie valt niet binnen de scope van beide methoden.

De CSR SCR-methode bestaat uit zes stappen, waarin een te onderzoeken keten wordt geselecteerd en geïnventariseerd, dreigingen en risico's worden beoordeeld en maatregelen worden opgesteld. Ook voor deze stappen wordt niet expliciet aangegeven hoe die organisatorisch geborgd kunnen worden. Wel wordt een stap benoemd waarbij wordt vastgelegd hoe de verdeling van wie welke maatregelen voor de keten moet implementeren.

De MITIGATE-methode bestaat eveneens uit zes stappen die vergelijkbaar zijn met de stappen uit de CSR SCR-methode. In de MITIGATE-methode wordt echter gebruik gemaakt van verschillende (gespecialiseerde) wiskundige modellen. Hiervoor lijkt specifieke kennis voor die modellen nodig te zijn om ze goed toe te kunnen passen. De nadruk ligt op de methodiek en het uitvoeren van een analyse.

De in ISO beschreven methode bevat zeer uitgebreide richtlijnen voor het inbedden van activiteiten in organisatorische processen. Het document geeft richtlijnen voor stappen die men in het acquisitieproces moet ondernemen en gaat in op de technische vereisten van een product of dienst. Daarbij wordt benadrukt dat om de methode in een keten toe te kunnen passen de betrokken organisaties dezelfde methode moeten hanteren.

Uit de CISA-publicatie kunnen vier stappen worden afgeleid: eerst worden dreigingen vanuit een leverancier, product of dienst geïdentificeerd en gecategoriseerd. Vervolgens worden scenario's voor deze dreigingen opgesteld en wordt de impact hiervan beoordeeld. Ook bij de CISA-methodiek is de inbedding van de methodiek in bestaande processen of organisatorische borging als onderwerp niet expliciet beschreven.

3.3 Benodigde input voor uitvoeren van methoden

Om deze methoden toe te passen in de praktijk is het nuttig om een inschatting te kunnen maken van de benodigde input voor het uitvoeren van een methode. Helaas specificeren de meeste methoden niet expliciet welke input en middelen er nodig zijn voor het uitvoeren van een methode. Daarom is getracht om op basis van de beschreven activiteiten af te leiden wat de benodigde input is per methode.

Alle methoden vereisen de input van experts binnen de eigen organisatie. Welke experts geschikt zijn voor het leveren van input verschilt dan wel weer per methode. Zo is voor de NIST-methode input vereist uit verschillende lagen in de organisatie. Deze methode geeft aan dat er stakeholders aangewezen dienen te worden op zowel strategisch, operationeel en als technisch niveau.

In MITRE1 en MITRE2 specificeren de auteurs niet expliciet welke input nodig is voor het uitvoeren van de verschillende activiteiten. In de MITRE1-methode is het in ieder geval nodig dat er technisch inhoudelijke input over het aan te schaffen/ontwikkelen systeem vereist is. Bij het aanschaffen van een systeem of het “out-house” ontwikkeling van een systeem zal dit ook input vereisen van de leverancier/ontwikkelaar. In de MITRE2-methode komt daar bij dat het nuttig is om experts te betrekken met kennis van cyber resilience engineering, idealiter experts die bekend zijn met het MITRE Cyber Resilience Engineering Framework.

De CSR SCR-methodiek geeft niet expliciet aan welke informatie als basis dient voor de analyse. Deze inbreng wordt overgelaten aan de per organisatie betrokken experts en de kennis die zij meebrengen in het proces. Het inbrengen van relevante informatie voor de analyse ligt ook bij deze experts. Ook bij de MITIGATE-methodiek is het aan de deelnemende organisaties om expertise/kennis te identificeren en in te brengen.

In de ISO-methodiek wordt geen expliciete beschrijving gegeven van de benodigde informatie voor het uitvoeren van de methodiek. Wel wordt in de stappen procesmatig en organisatorisch geborgd dat expertise en middelen beschikbaar gemaakt worden om de methodiek uit te kunnen voeren. Of en welke informatie uit het genoemde Software Lifecycle-proces benodigd is wordt niet expliciet benoemd.

De CISA-methodiek maakt aan de hand van een voorbeeld duidelijk welke informatie gebruikt kan worden.

3.4 Uiteindelijk resultaat na uitvoer van methoden

Voor elk van de methoden is gekeken naar welke resultaten verwacht kunnen worden na het uitvoeren van de methode in de praktijk.

Zo beschrijft NIST dat het resultaat van de methode verschillende elementen bevat. Zo is één van de beoogde resultaten het identificeren van supply chain risico’s. Het tweede resultaat is het identificeren en koppelen van de juiste mitigatie maatregelen. Deze dienen vervolgens geïmplementeerd te worden in de eigen organisatie.

Het resultaat van de methodiek beschreven in MITRE1 is een overzicht van mogelijke technische aanvallen die relevant zijn voor het onderzochte ICT-systeem. Dit vormt de basis voor het vaststellen van technische mitigerende maatregelen. Het resultaat van MITRE2 is een overzicht van aanvallen en mitigerende maatregelen voor elke stap van het acquisition lifecycle process.

Met de methodiek CSR SCR wordt gewerkt naar een kwalitatief onderbouwd overzicht van processen en systemen. Aan dat overzicht worden relevante cyberrisico's op de gehele keten gekoppeld. Tenslotte worden te nemen mitigerende maatregelen voor de keten verdeeld over de betrokken organisaties. Het beoogde eindresultaat is een overzicht van de te treffen maatregelen en welke ketenorganisatie daarvoor verantwoordelijk is.

De MITIGATE-methodiek, heeft als eindresultaat een kwantitatief onderbouwde risico inschatting en mitigerende maatregelen. Detail informatie over processen en systemen in de keten inclusief dreigingen, kwetsbaarheden en de ingeschatte impact op de keten.

Het beoogde resultaat van de ISO-methodiek is inzicht in de ICT supply chain en dan specifiek op de oorsprong van gebruikte ICT-producten en -services. In geval van data, is het resultaat dat bij data die gecompromitteerd wordt duidelijk wordt welke data gecompromitteerd is en wie de betrokken partijen zijn.

Na het uitvoeren van de CISA-methodiek is het resultaat een opsomming en categorisering van de (algemene) risico's die men in acht moet nemen, gerelateerd aan ICT-leveranciers.

4 Resultaten interviews

Om een beeld te krijgen bij wat organisaties doen om ICT supply chain risico's te beheersen, maar ook om te inventariseren waar ondersteuningsbehoeften liggen, is met een beperkt aantal partijen diepte-interviews afgenomen (zie bijlage 1). In dit hoofdstuk zal eerst worden ingegaan op hoe verschillende organisaties nu kijken naar vraagstukken rond ICT supply chain-risico's. Vervolgens wordt een aantal in de praktijk gevolgde aanpakken besproken. Ten slotte zal worden ingegaan op de behoeften die binnen dit thema zijn uitgesproken door respondenten tijdens de interviews.

4.1 Hoe wordt naar ICT SCRM vraagstukken gekeken?

4.1.1 Wat wordt er in de praktijk verstaan onder ICT supply chains?

In algemene zin komt naar voren dat de geïnterviewde organisaties supply chains vanuit verschillende aspecten benaderen: vanuit de eigen organisatie en haar relaties, een (toeleverings- of productie)keten of sector, of vanuit een (eco)systeem benadering waarin vele relaties van complexe aard met elkaar zijn verbonden.

Het verschilt per partij welke organisaties worden meegenomen binnen ICT SCRM en wat men onder ICT supply chains verstaat, voor de een zijn het hele specifieke partijen en voor andere valt iedereen daar onder. Alle partijen beschouwen leveranciers als onderdeel van hun supply chain, waar zij ook risico's identificeren en kijken vanuit de eigen organisatie naar de relaties met andere partijen. Bij de vraag wat supply chain betekent, is vaak naar voren gekomen dat het dan gaat om leveranciersmanagement (1^{e} lijn). Er wordt soms een onderscheid gemaakt in ketenpartners en sectorpartners die in ogenschouw genomen worden binnen een ICT supply chain. Binnen eenzelfde sector komt het voor dat de ene partij zijn sectorpartners wel ziet als ketenpartner en een andere partij niet. Het belang van samen optrekken met partners uit de sector is herhaaldelijk benadrukt, bijvoorbeeld door samen afspraken te maken met dezelfde leveranciers, informatie uit te wisselen over risico's of in gesprek te gaan met overheidspartijen.

De respondenten geven aan dat een brede blik op supply chain risico's van belang is, maar dat dit in de praktijk soms lastig te organiseren is en zeker nog niet altijd goed belegd is. De complexiteit van supply chains zorgt ervoor dat maar een deel van de leveranciers en afhankelijkheden in kaart kan worden gebracht. Gaat het om een product van een leverancier of over één van de componenten, zoals firmware of chips, gaat het in op uitbestedingen of zelfs over de subcontractors? Men heeft niet de capaciteit om meer in kaart te brengen dan de eerste lijn leveranciers in de eigen ICT ketens en daarnaast is de complexiteit van deze relaties te groot. De behoefte om hier meer grip op te krijgen en hierin met bijvoorbeeld sectorpartners in op trekken is duidelijk naar voren gekomen tijdens de interviews.

4.1.2 Is ICT SCRM een belangrijk onderwerp en welke risico's onderscheidt men?

De meeste respondenten herkennen zich in de relevantie van ICT SCRM. Er is echter weinig uniformiteit in de exacte definitie van de ICT supply chain. De meeste partijen beschouwen de afhankelijkheid van leveranciers en het gevoel onvoldoende grip te hebben op wat er achter deze leveranciers zit als voornaamste risico, en vragen zich af in hoeverre hun eigen leveranciers nieuwe aanvalspaden

creëren voor de eigen organisatie. Daarnaast ziet men de afhankelijkheid van grote leveranciers (zoals Microsoft of Google) waar weinig invloed op is als risico, met name omdat hier vele organisaties van afhankelijk zijn en de impact van een incident dus zeer groot kan zijn.

In veel gesprekken is het beheersen van risico's die voortvloeien uit het afnemen van clouddiensten als uitdaging naar voren gekomen. Meerdere respondenten gaven aan dat de trend van migratie van IT-infrastructuren naar clouddiensten een belangrijke rol gaat spelen in het SCRM vraagstuk. De afnemer van de clouddienst heeft namelijk geen zicht op welke leveranciers een bijdrage leveren aan productontwikkeling binnen de cloud-omgeving, wat juist ook de kracht is, de kennis ligt bij de leverancier en de afnemer hoeft zich hier geen zorgen over te maken, maar men heeft hier behoefte aan meer inzicht. Bovendien is er een beperkt aantal grote leveranciers van clouddiensten, waardoor verschillende organisaties dezelfde dienst bij dezelfde partij (gaan) afnemen. Dit levert een gedeelde afhankelijkheid op, waardoor een verstoring van deze dienst zich des te omvangrijker kan manifesteren. Aan de andere kant zijn over het algemeen deze grotere leveranciers wel betrouwbaar in clouddiensten en is dit ook de reden dat veel organisaties hier gebruik van maken.

Als er gekeken wordt naar wat voor soort risico's of uitdagingen men ziet, varieert dit van algemene cybersecurity-dreigingen, zoals datalekken, gehackte data, of een kwetsbaarheid die benut wordt als stepping stone, naar specifieke risico's. Denk hierbij aan privacy van data omdat er een verschuiving is van (persoonlijke) data die bij een derde partij wordt ondergebracht, waar ligt dan de verantwoordelijkheid over deze data en hoe zit dit met compliance?

Er zijn meerdere voorbeelden genoemd van incidenten om de risico's te duiden, die ingaan op kwetsbaarheden bij leveranciers, het gebruik van een ICT-product of -dienst door meerdere organisaties, etc. Het Citrix-incident is bijna door alle respondenten naar voren gebracht. Hier kwam naar voren dat bij een kwetsbaarheid als deze men de eigen zaken snel kan controleren. Men kan echter minder snel controleren in hoeverre men afhankelijk is van de leveranciers, en of Citrix überhaupt wordt gebruikt. Hierdoor kunnen wel degelijk grote (keten)effecten ontstaan.

4.2 Hoe wordt ICT SCRM aangepakt?

4.2.1 Wat doet men om ICT supply chain-risico's te identificeren?

Er worden diverse risico analyses uitgevoerd, afhankelijk van de prioriteit van de ketenpartner en de eigen bedrijfscontinuïteit. Voor elke leverancier worden generieke (risico) assessments uitgevoerd en deze worden besproken en opgenomen in afspraken als *service level agreements* (SLAs). Soms kan het voorkomen dat men extra assessments uitvoert. Een reden hiervoor kan zijn dat men een beter beeld wil krijgen van cloud- of hostingleveranciers, of dat men testen wil uitvoeren (bijvoorbeeld pentesten) om grip te krijgen op eventuele risico's. Voor het identificeren van risico's worden verschillende soorten risicomatrixen gebruikt. Daarbij worden er ook assurance-processen opgezet, zeker bij kritische uitbestedingen waarin de organisatie meerdere keren per jaar in gesprek gaat met de leverancier over risico's.

Het bijhouden van algemene risico's en kwetsbaarheden en zicht houden op het politieke klimaat is ook onderdeel van het identificeren en bespreken van risico's. Dit wordt deels binnen sectoren gedaan, waar bijvoorbeeld informatie wordt uitgewisseld binnen ISACs. Daarnaast wordt er gemonitord op diverse dreigingen en bij een bepaald risico of zelfs incident gekeken hoe dit binnen de eigen organisaties en leveranciers geregeld is. Zo worden er (meer)jaarlijks dreigingsbeelden opgezet en wordt er informatie gehaald uit diverse open bronnen, de sectorpartners en partijen als het NCSC.

Tot slot, worden in algemene zin met name het NIST-framework en ISO standaarden het meest gebruikt voor voor het inrichten van ICT risicomanagement processen voor de (ICT) supply chains. Het NIST-framework wordt gebruikt omdat het handvatten geeft om de cybersecurity risico's te vertalen naar de bedrijfsdoelen en dit te communiceren naar bestuurders. Daarnaast blijft het identificeren en beoordelen van de risico's een menselijk karakter hebben en worden er vaak experts ingeschakeld om risico's te beoordelen en te koppelen aan IT-specifieke doelen en deze vervolgens door te vertalen naar de bedrijfsdoelen.

4.2.2 Hoe prioriteert men naar welke ketens/partijen er wordt gekeken?

Uit de interviews komt naar voren dat het aantal (ICT-)leveranciers en zeker de toeleveranciers daarachter enorm is. Er is geen capaciteit om alle relaties vast te leggen en hierop risicoanalyses toe te passen. Hiervoor is het noodzakelijk om te prioriteren en de vraag te stellen hoe ver men zich in deze relaties moet verdiepen. In de praktijk wordt vooral gekeken naar de leveranciers uit de eerste lijn. Daarbij wordt voor de grote leveranciers, voor leveranciers waar veel van wordt afgenomen of leveranciers die belangrijk worden geacht expliciet aandacht gegeven aan supply chain risico's. Deze keuze hangt vaak samen met het beoordelen van het belang van leveranciers voor de bedrijfscontinuïteit. In de interviews wordt genoemd dat men met name naar grote of belangrijke leveranciers voor de organisatie kijkt, waardoor mogelijk de risico's die uit (vaak kleinere) zwakke schakels zouden kunnen komen over het hoofd worden gezien. Het zal een steeds grotere uitdaging worden om de juiste prioritering mee te nemen, omdat de onderlinge verwevenheid van relaties in deze supply chains steeds complexer en groter wordt. De behoefte is geuit om op basis van meerdere aspecten te prioriteren en meerdere relaties uit de supply chain mee te nemen, zonder dat dit betekent dat alle relaties meegenomen moeten worden.

Uit de interviews kwam ook naar voren men dat men prioriteert op basis van de eigen kritieke processen of diensten. Zo werd als voorbeeld genoemd dat Nederland is onderverdeeld in vitale processen die als ketens gezien kunnen worden. De energiesector is in essentie verantwoordelijk voor het leveren van de vitale dienst: elektriciteit. Het prioriteren van ketenpartners kan dan worden gekoppeld aan de continuïteit van deze dienst (al dan niet gericht op (ondersteunende) ICT). Hierin ligt dan de focus op bijvoorbeeld het op tijd uitbetalen van een factuur wellicht lager, dan dat een kernproces zoals het leveren van schoon drinkwater. Hier blijft wel de vraag of alle ondersteunende processen voldoende op waarde geschat kunnen worden en dus of er wel goed kan worden geprioriteerd.

4.2.3 Welke maatregelen past men toe voor het beheersen van ICT supply chain risico's?

In de interviews is ingezoomd op twee categorieën maatregelen die getroffen kunnen worden:

1 het maken van afspraken;
2 ervoor zorgen dat de afspraken worden nageleefd.

4.2.3.1 Afspraken maken

Het maken van afspraken komt bij alle partijen vooral tot uiting in de contractonderhandelingen met nieuwe of bestaande leveranciers van ICT-diensten of -producten, en kan gekarakteriseerd worden als leveranciersmanagement. Het resulteert bij alle partijen in tenminste het maken van afspraken en het vastleggen van een deel van deze afspraken in contracten of SLAs. Leveranciersmanagement valt ten minste uiteen in het bewaken van de services die door een leverancier geleverd worden, licentiemanagement voor het regelen van de verantwoordelijkheden van de betrokken organisaties, het maken van contracten met alle afspraken waarin de commerciële en juridische zaken worden vastgelegd en tot slot het leveranciersmanagement waarin de relaties worden onderhouden. Bij het maken van afspraken is het belangrijk om de begrippen vertrouwen en het besef van verschillende belangen niet uit het oog te verliezen.

Voorbeelden van afspraken rondom het beheersen van ICT-risico's die zich kunnen voordoen in een supply chain zijn afspraken met leveranciers over ongeplande pentesten, het voldoen aan de BIO-norm, de verplichting om incidenten te melden en afspraken rondom de bescherming van vertrouwelijke- en persoonsgegevens.

4.2.3.2 Naleving van afspraken

Om te bepalen of afspraken (met leveranciers of andere partners) worden nageleefd worden verschillende activiteiten genoemd, zoals audits, certificering, assurance, of samenwerken aan verbetering.

Uit de interviews komt naar voren dat audits vaak niet standaard of periodiek worden uitgevoerd, maar alleen als er een concrete aanleiding voor is. Het nadeel van audits is dat leveranciers erbij gebaat zijn om een zo positief mogelijk beeld te geven en de audits een momentopname zijn. Daardoor blijven altijd onzekerheden bestaan over de actuele veiligheid van het product of de dienst die wordt afgenomen. Het veelvoud aan leveranciers zorgt er ook voor dat er soms een onderscheid wordt gemaakt tussen grotere en kleinere leveranciers, of tussen belangrijke en minder belangrijke leveranciers. Het nadeel daarvan is dat niet alle leveranciersrisico's even goed worden beheerst, terwijl supply chain-incidenten juist vaak hun oorsprong vinden vanuit een onverwachte schakel in de keten.

Een andere maatregel is het eisen en controleren van certificering bij leveranciers. Door sommige geïnterviewden wordt aangegeven dat een certificering (bijvoorbeeld ISO-certificering) niet meteen duidelijkheid geeft over of een leverancier goed beveiligd is. Een leverancier kan namelijk (gedeeltelijk) ISO gecertificeerd zijn, maar niet voor het systeem of product dat wordt afgenomen. Hier moet een afnemer zelf scherp op zijn.

Een derde activiteit die vaak genoemd wordt in het kader van het beheersen van leveranciersrisico's is het toepassen van assurance. Als het gaat om assurance geven veel geïnterviewden aan dat het in de praktijk lastig is om de effectiviteit ervan te toetsen. Dit heeft als resultaat dat het niet altijd duidelijk is wat deze assurance-activiteiten opleveren, terwijl het wel veel middelen (tijd en geld) vergt

van zowel de afnemende partij als de leverancier. Er is behoefte om meer grip te krijgen op de effectiviteit van gemaakte afspraken en hier mogelijk ook activiteiten te bundelen.

Naast het maken van afspraken, of het uitvoeren van assurance-maatregelen, kwam in sommige gesprekken ook naar voren dat er in uitzonderlijke gevallen wordt samengewerkt met de leverancier om de veiligheid van een product of dienst te verbeteren. Als het genoemd wordt, doet men het alleen samen met de belangrijkste leveranciers waar invloed op uitgeoefend kan worden.

Tot slot, een door meerdere respondenten genoemd aspect bij het omgaan met leveranciers is vertrouwen. Er is altijd een bepaalde mate van vertrouwen nodig om zaken met elkaar te doen. Daarbij is het enerzijds zo dat een organisatie moet kunnen vertrouwen op een degelijk en veilig product, maar is het andersom ook zo dat de leverancier moet kunnen vertrouwen op goed gebruik. Door de complexiteit van beveiligingsvraagstukken vanuit individuele organisaties en de hoeveelheid aan leveranciers zit er een grens aan de hoeveelheid afspraken die gemaakt wordt en het aantal tests dat op een product uitgevoerd wordt, omdat er ook een bepaalde mate van vertrouwen tussen leverancier en afnemer is.

4.2.4 Hoe is ICT SCRM ingebed in organisaties?

Het varieert sterk per partij waar ICT SCRM belegd is. ICT SCRM wordt vaak geïntegreerd in een bestaand (risicomanagement-)proces. Voorbeelden hiervan zijn integratie in het ICT-risicomanagementproces, het procurement-/uitbestedingenproces, het business continuity managementproces, of in het algemene risicomanagementproces.

In de gesprekken werd bovendien aangegeven dat supply chain-risico's moeten worden vertaald van technische risico's die voortkomen uit de ICT naar duidelijke risico's voor de business-continuïteit, omdat dit de enige manier is om de aandacht van bestuurders voor deze risico's te krijgen.

Een aantal organisaties zegt dat er stappen worden gezet om ICT-risicomanagement te verbinden met business continuity management (BCM). Men voert dan een beoordeling uit om de belangrijkste, meest kritische bedrijfsprocessen en (ICT) assets in kaart te brengen. Eén van de geïnterviewden geeft aan dat het een uitdaging blijft om die risico afwegingen goed op elkaar te laten aansluiten.

4.3 Behoeften en verbeterpunten ICT SCRM

4.3.1 Behoefte aan uniformering en standaardisering

Bijna alle respondenten hebben aangegeven dat er behoefte is aan het bundelen van de inspanningen die nu worden verricht op het gebied van ICT SCRM. Dit verbetert de efficiëntie en zal daarmee enorm veel (toekomstige) inspanning en geld kunnen besparen. Men doelt hierbij vooral op het uniformeren, of zelfs standaardiseren, van de ICT SCRM maatregelen die nu al worden getroffen: afspraken, contracten, SLAs, audits, certificering en assurance. Primair zal dit efficiëntiewinst opleveren, bijvoorbeeld door ervoor te zorgen dat er een standaard set aan eisen komt die aan een leverancier wordt gesteld, in plaats van dat iedere organisatie haar eigen eisen stelt. Het kan echter ook de kwaliteit en effectiviteit van deze maatregelen verhogen voor sommige partijen en daarmee de algehele supply

chain verstevigen. In een groot aantal gevallen werd er in de gesprekken ook genoemd dat de overheid hier een (primaire) rol in moet blijven spelen en dat dit de landsgrenzen overstijgt, dit moet dus in multilateraal of in EU-verband worden gedaan.

Het is niet gezegd dat uniformering en standaardisering gemakkelijk kunnen worden uitgevoerd. Respondenten wijzen op het feit dat belangen van organisaties soms conflicterend kunnen zijn, bijvoorbeeld bij een leveranciers-afnemer relatie. Voor het uniformeren van inspanningen zal moeten worden gezocht naar de gedeelde belangen van organisaties, zoals het verbeteren van de veiligheid op een kosteneffectieve manier. Daarnaast moeten organisaties onder ogen zien dat samenwerken in eerste instantie meer inspanning zal vergen, maar zich op den duur zal terugbetalen.

Eén van de respondenten oppert om uniformering op te pakken in de vorm van een trusted third party. Deze trusted third party zou alle ICT supply chain-risicomanagement inspanningen kunnen oppakken volgens de wensen van de aangesloten Nederlandse organisaties. Vervolgens kunnen deze organisaties bij deze onafhankelijke partij gemakkelijk verifiëren of het verantwoord is om zaken te doen met een leverancier. Bovendien is in sommige gesprekken benoemd dat de wens bestaat om partijen te kunnen vergelijken. Met een trusted third party die partijen uniform beoordeelt is dit gemakkelijker te realiseren.

4.3.2 Behoefte aan samenwerking

Naast uniformering en standaardisering is er ook een algemener belang om samen te werken aan ICT SCRM. Ten eerste noemen enkele respondenten dat de invloed op de supply chain vergroot kan worden door op sectoraal of nationaal niveau samen te werken. De respondenten opperden dat een sector of natie mogelijk iets kan afdwingen bij grote leveranciers, maar dat dit waarschijnlijk nog groter aangepakt moet worden.

Ook wordt door enkele respondenten genoemd dat er behoefte is om samen te werken op Europees niveau. De uniformering en standaardisering, besproken in de voorgaande subsectie, zou nog effectiever zijn als dit op Europees niveau wordt opgepakt. Bovendien kun je op Europees niveau meer invloed uitoefenen op grote leveranciers.

Een kanttekening bij de behoefte aan samenwerking en ook de behoefte aan uniformering en standaardisering is dat de belangen om dit te doen vaak nog te veel uiteenlopen. Hierdoor blijven in de praktijk de uitwerking en volgende stappen in samenwerking uit.

4.3.3 Overige behoeften

Ten eerste is genoemd dat men behoefte heeft aan een verduidelijking van de vraagstukken en bijbehorende problematiek. Deze behoefte is zowel op basis van de gesprekken met Nederlandse organisaties als op basis van de literatuur en methodieken vastgesteld. Denk hierbij bijvoorbeeld aan het uittekenen van “de supply chain” en een overzicht van concrete handvatten en handelingsperspectieven voor zowel afnemers als leveranciers.

Alle organisaties steken nu veel effort en middelen in leveranciersmanagement en assurance. Een behoefte die bij meerdere respondenten naar voren is gekomen, is om inzicht te krijgen op de effectiviteit van maatregelen die in het kader van

leveranciersmanagement en assurance worden genomen. Daarbij heeft men de vraag of er wellicht een verschuiving nodig is van de huidige effort en middelen om meer grip te krijgen op de risico's. Men zou meer kunnen inzetten op het testen van producten en/of leveranciers, mogelijk door een onafhankelijke partij of juist door organisaties meer samen te laten bundelen.

Ook is aangegeven dat er juist geen behoefte is aan een extra framework, of uitbreiding van een bestaand framework, bijvoorbeeld over ICT Supply Chain risk assessment. Wat veel nuttiger zou zijn is een duiding van de bestaande methodieken. Ook kan het nuttig zijn om "grote", hoog over frameworks uit te splitsen in concrete operationele acties. Bovendien kan het nuttig zijn om een (sectorale) baseline op te stellen qua wat men ten minste moet doen aan ICT SCRM.

Daarnaast is er behoefte aan een eerste aanzet op een Nederlandse standpunt op certificering en standaarden. Uiteindelijk kan dan een keuze gemaakt worden over welke certificering en standaarden omarmd worden op nationaal of sectoraal, niveau. Wat organisaties zal helpen bij het opstellen van beleid. Het blijft echter wel de vraag wat het beste gecertificeerd kan worden: hard- en software, organisaties, of mensen.

Ten slotte zijn organisaties geïnteresseerd in het delen van informatie over best-practices en praktijkvoorbeelden.

5 De basis voor een analysekader

Tijdens het uitvoeren van het onderzoek groeide het besef dat er verschillende perspectieven op digitale ketens ‘ingebed’ waren in de methoden en casussen die in de literatuur en interviews naar voren kwamen. Deze perspectieven lijken doorgaans impliciet te zijn, ze worden in ieder geval niet expliciet benoemd in methoden of interviews. Dit gaf aanleiding om deze perspectieven expliciet te maken en na te gaan of deze kunnen bijdragen aan het analyseren van de methodieken en de in de praktijk ervaren knelpunten. Het resultaat is een aanzet voor een analysekader, waarin een eerste vijf perspectieven worden onderscheiden. De benoemde perspectieven zijn:

- Actorenperspectief;
- ICT-producten perspectief;
- Informatieperspectief;
- ICT-diensten perspectief;
- Productiemiddelenperspectief.

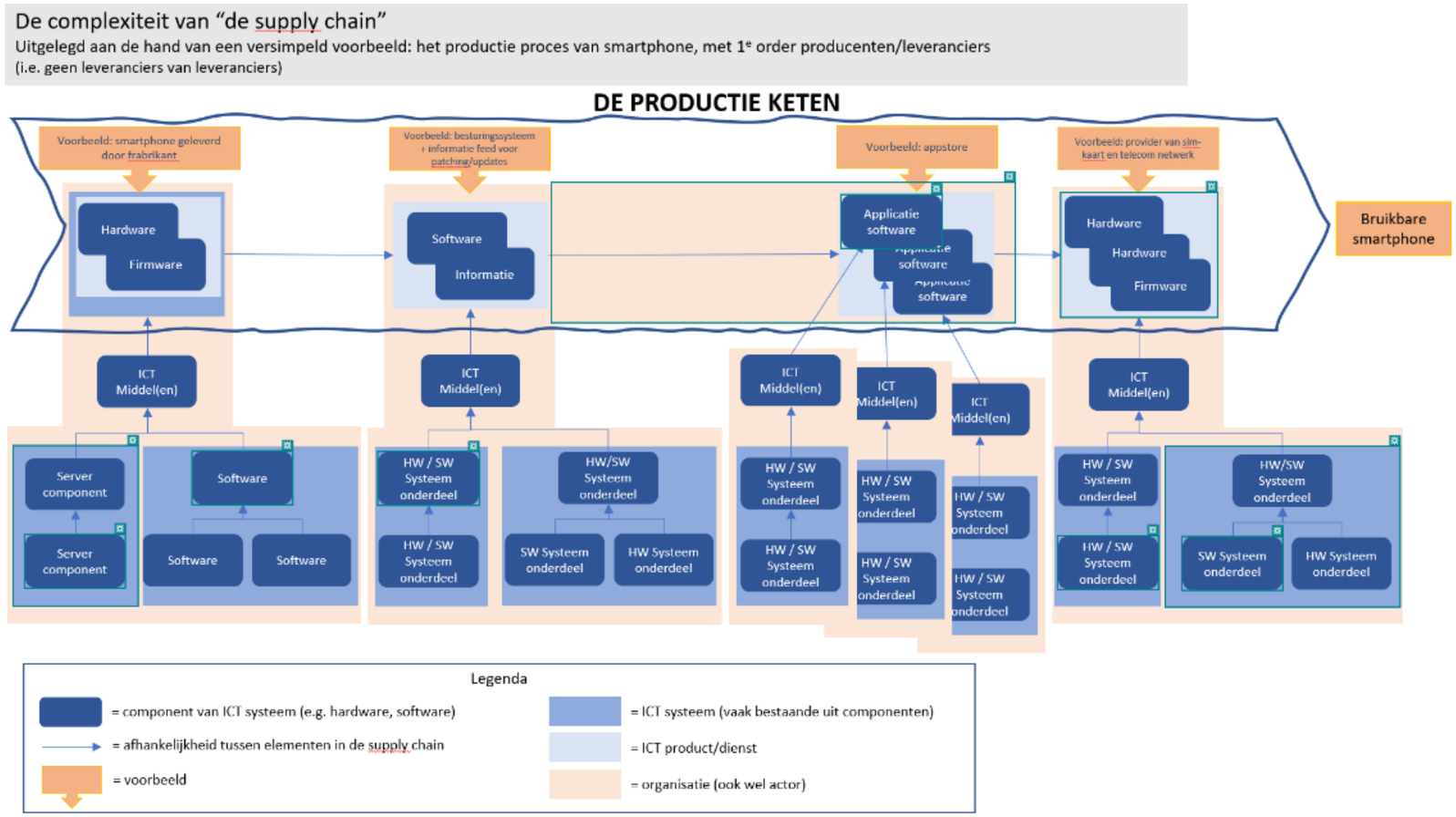
Met deze vijf perspectieven wordt, kijkend vanuit het digitale domein naar supply chains, beoogd om bestaande risicomanagement aanpakken te onderzoeken, beter te kunnen duiden en te identificeren waar mogelijke lacunes zitten. De achterliggende aanname is dat niet alle perspectieven door alle methoden worden afgedekt. Dat in samenwerkingsverbanden impliciet vanuit verschillende perspectieven gekeken wordt, maar dat dit niet altijd bekend is bij de betrokken partijen.

De nut en noodzaak voor het onderscheiden van verschillende perspectieven is drieledig. Ten eerste is het voor samenwerkingsverbanden belangrijk om sneller mogelijke lacunes te identificeren door expliciet inzicht te geven welke perspectieven (onbedoeld) niet meegenomen worden en gedeeld begrip te krijgen. Ten tweede om te toetsen hoe bestaande methoden en aanpakken deze perspectieven meenemen en hoe op een integrale wijze met het vraagstuk wordt omgegaan. Ten derde het kunnen identificeren en analyseren van supply chains vanuit de verschillende perspectieven om mogelijke (nieuwe) risico’s te identificeren.

In de volgende paragrafen worden de elementen van een supply chain geschetst en wordt getoond hoe deze in een analysekader kunnen worden weergegeven. Vervolgens wordt het concept analysekader uiteen gezet aan de hand van de vijf geïdentificeerde perspectieven.

5.1 Van een “veelkoppig monster” naar vijf behapbare perspectieven op de supply chain risico beheersing

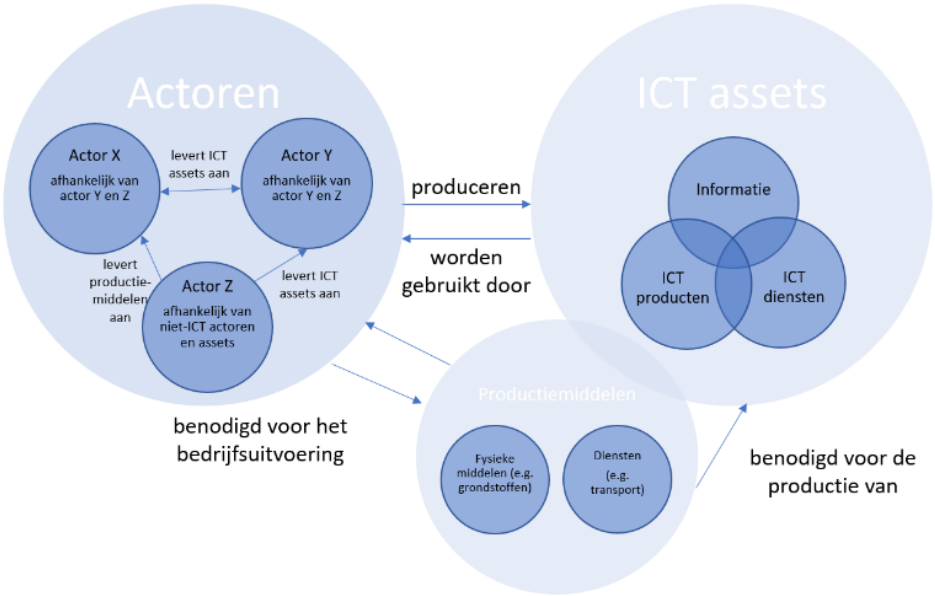
In algemene zin kan men een supply chain zien als een aaneenschakeling van activiteiten, goederenstromen, informatiestromen en de daarbij betrokken organisatie die leiden tot een product of dienst die een bepaalde behoefte van de afnemer vervult. Deze processen zijn afhankelijk van, of vervlochten met, ICT-functionaliteiten. In figuur 3 hieronder wordt middels een ruwe schets een dergelijke supply chain weergegeven.



Figuur 3 De complexiteit van “de (horizontale) supply chain”.

Alhoewel figuur 3 een sterk versimpelde, enkelvoudige supply chain weergeeft, is hier al sprake van een grote mate van complexiteit. De realiteit is echter nog weerbarstiger aangezien supply chains nooit geïsoleerd functioneren, maar altijd verknoopt zijn met andere supply chains. Zodoende vormen deze supply chains een netwerk, wat een nog veel omvangrijker productiestappen schema oplevert dan in bovenstaand figuur is weergegeven. Deze mate van complexiteit maakt het in de praktijk een grote uitdaging om grip te krijgen op de risico's die voortkomen uit de supply chain.

Om meer grip te krijgen op de elementen in de supply chain en de relaties tussen deze elementen is er een eerste poging gedaan om de supply chain te vatten in een analysekader. In figuur 4 staan de verschillende elementen en relaties tussen deze elementen weergegeven in een geabstraheerd model.

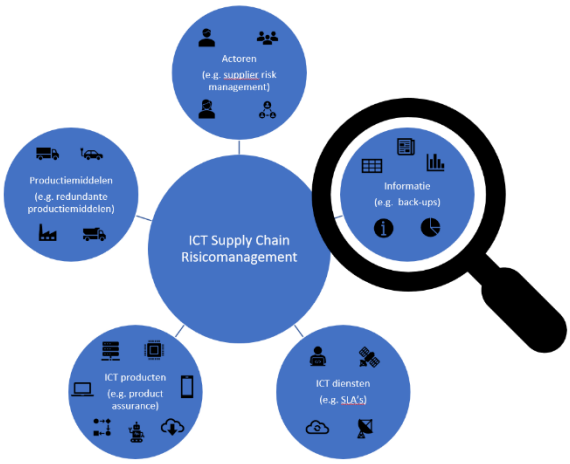


Figuur 4 Elementen en relaties van een supply chain.

In bovenstaande figuur wordt al snel duidelijk wat de elementen zijn die een rol spelen binnen de ICT supply chain en wat de relaties tussen deze elementen zijn. Volgens dit model bestaat de ICT supply chain uit 3 hoofdelementen, namelijk ***actoren***, ***ICT-assets*** en ***productiemiddelen***. Actoren kunnen ICT-assets leveren aan andere actoren, wat een wederzijdse leverancier en afnemer relatie oplevert. Daarnaast produceren actoren dus ICT-assets die kunnen worden ingedeeld in drie categorieën, namelijk ICT-producten, -diensten en -informatie. Actoren maken ook gebruik van ICT-assets voor de bedrijfsuitvoering. Bovendien zijn productiemiddelen nodig voor het produceren van ICT-assets, denk aan grondstoffen en constructiemachines, of aan een dienst in de vorm van transport. ICT-assets kunnen zelf echter ook weer productiemiddelen zijn, bijvoorbeeld chips in computers. Ten slotte hebben actoren productiemiddelen nodig voor de uitvoering van hun bedrijfsprocessen.

Bovenstaand model biedt handvatten om grip te krijgen op de complexiteit van de supply chain. Om hier vervolgens concrete aanknopingspunten te krijgen voor het identificeren en beheersen van de risico's die voortvloeien uit de supply chain, zijn

in onderstaande figuur vijf perspectieven aangegeven. De verwachting is dat meerdere perspectieven gecombineerd moeten worden om een antwoord te vinden op de verschillende vraagstukken rondom ICT SCRM.



Figuur 5 De basis voor een analysekader: vijf perspectieven.

5.2 De vijf perspectieven

5.2.1 Actorenperspectief

Wanneer men naar de ICT supply chain kijkt vanuit het perspectief van actoren kan men kijken naar het geheel van organisaties (leveranciers, afnemers) dat betrokken is in een ICT supply chain, om zo risico's in beeld te krijgen voor de continuïteit van het leveringsproces. Hierbij ligt de nadruk op het inzichtelijk krijgen in en afstemmen over de relaties tussen organisaties (afspraken tussen leverancier en afnemer, zicht op afhankelijkheden tussen verschillende leveranciers, etc.). De uitdaging hierbij is dat het afstemmen op het niveau van een keten alleen mogelijk is als de verschillende organisaties in die keten het belang daarvan voelen. Niet alle organisaties die bijdragen aan een supply chain zullen zichzelf nadrukkelijk zien als mede-eigenaar van het ketenbelang. Met name leveranciers die hun producten leveren aan heel veel verschillende partijen zullen het ketenbelang minder sterk voelen.

Een tweede manier om het actorenperspectief te hanteren is om vanuit één organisatie te kijken naar de verschillende ICT-toeleveringsketens waar de organisatie een rol in speelt (als afnemer, als leverancier, als dienstverlener, als toezichthouder, etc.). Voor elk van die rollen zal de organisatie op een andere manier maatregelen nemen. Als afnemer gaat het bijvoorbeeld om het maken van afspraken met de leveranciers (zoals SLAs). Als leverancier gaat het erom grip te krijgen op de risico's die tot gevolg kunnen hebben dat de organisatie haar afspraken met afnemers niet kan nakomen [13]. Voor elke rol zijn andere aspecten van belang en komen er ook andere risico's in beeld. Een belangrijke uitdaging hier is om te prioriteren op welke ICT supply chains men zich moet richten. De hoeveelheid aan ICT supply chains waar één organisatie een rol in speelt is namelijk enorm. Het is dus vrijwel onmogelijk om alle ketens waar een organisatie een rol in speelt volledig in kaart te brengen. Om hier meer richting aan te geven kunnen ook de overige perspectieven een waardevolle rol spelen.

5.2.2 ICT-producten perspectief

Een andere manier om naar ICT supply chain risico's te kijken is door te kijken vanuit de ICT-producten. Het gaat hierbij om de supply chains van ICT-producten variërend van een (relatief simpel) stuk software, zoals een telefoon, een autonoom functionerend voertuig of de automatische aansturing van operationele technologie (OT) voor vitale processen. In al deze producten komen verschillende systeemonderdelen samen vanuit verschillende leveranciers. Het kan zijn dat het product zelf (bijvoorbeeld in het geval van een softwarepakket) bij de afnemer weer wordt geïntegreerd of toegepast binnen een ander systeem. Bij het NotPetya incident [14] werd boekhoudsoftware vermoedelijk als aanvalsvector gebruikt om binnen te komen in een specifiek systeem. Maar omdat veel organisaties deze software gebruikten werden zij meegesleept in een (geopolitiek) conflict waar ze niets mee te maken hadden. Deze organisaties namen een softwarepakket af van een leverancier zonder dat zij zicht hadden op de achterliggende leveranciers en de mogelijke risico's daarvan. Uit meerdere gesprekken komt naar voren dat het vaak een uitdaging is om grip te krijgen op de keten van leveranciers achter een leverancier van een specifiek ICT-product. De vraag is dan ook in welke mate men zicht kan krijgen op wat er in de eigen organisatie aan ICT-producten wordt binnengehaald. Belangrijk hierbij is om zicht te hebben op de ICT-producten in de organisatie en de manier waarop zij bijdragen aan de bedrijfscontinuïteit van de organisatie. Welke producten zijn kritiek? Welke componenten horen er in het programma of systeem te zitten en wat zit er daadwerkelijk in?

5.2.3 Informatieperspectief

In het derde perspectief wordt vanuit de informatie naar een ICT supply chain gekeken. In dit perspectief wordt gekeken naar welke informatiestromen en informatieproducten (die tot stand zijn gekomen door gebruik te maken van ICT-middelen) een rol spelen bij de toelevering van een product of dienst, of bij de ondersteuning van bedrijfsprocessen. Voorbeelden zijn de totstandkoming van rapportages van de kwaliteitscontroles die nodig zijn om de levering van een chemisch product te autoriseren, informatiestromen uit sensoren die van belang zijn bij de aansturing of controle van bepaalde OT, of het delen van klantgegevens met een bezorgdienst voor de levering van producten. Bij MAERSK werden veel systemen geraakt door de NotPetya wiperware, waardoor ook de informatievoorziening richting de klanten werd verstoord [15]. Hierdoor werden ook organisaties geraakt die zelf niet geïnfecteerd waren omdat de informatie die zij voor hun processen nodig hadden niet (volledig of tijdig) beschikbaar was. Een ander aspect van het informatieperspectief is de opslag en het gebruik van data. Data is in toenemende mate niet meer in beheer van de eigen organisatie, of meerdere organisaties maken gebruik van dezelfde data. Dit heeft als gevolg dat meerdere organisaties worden geraakt als zich een incident voordoet met deze data of de plek van opslag. Als bijvoorbeeld de patiënten data van een medisch laboratorium wordt gemanipuleerd, kunnen patiënten in ziekenhuizen vanwege onjuiste data de verkeerde behandeling krijgen [16]. Hoe kan men achterhalen dat data is gemanipuleerd als deze data niet binnen de eigen organisatie wordt beheerd en hoe kan men hier op handelen? Door naar de belangrijke informatiestromen en producten te kijken.

5.2.4 ICT-diensten perspectief

In veel supply chains spelen ICT-diensten een rol, niet alleen als onderdeel van het toeleveringsproces van een product of dienst, maar ook als eindproduct van een

supply chain. ICT-diensten zijn diensten waar ICT-middelen voor nodig zijn om ze te kunnen gebruiken. Voorbeelden zijn telecom diensten, clouddiensten of het leveren van remote onderhoud op systemen. Een voorbeeld van een supply chain incident waarbij ICT-diensten een grote rol speelden is de DDoS aanval op de DNS provider Dyn in 2016 [17]. Door de aanval op Dyn was voor een groot deel van Noord-Amerika de toegang tot het internet gedurende bijna een hele dag verstoord en veel verschillende diensten en platformen, zoals Spotify, waren daardoor niet beschikbaar. Binnen dit ICT-dienstenperspectief is het feit dat erg veel organisaties afhankelijk zijn van een beperkt aantal grote ICT-dienstleveranciers een belangrijke uitdaging. Deze uitdaging geldt met name voor organisaties die van ICT-diensten afhankelijk zijn om hun bijdrage aan vitale processen te waarborgen. Denk aan de afhankelijkheid van een internet of telecommunicatie leverancier of een leverancier van cloudopslag.

5.2.5 Productiemiddelen perspectief

Tenslotte spelen ook andere (niet-ICT-)producten of -diensten een rol in ICT supply chains die afhankelijk zijn van ICT middelen. De bedrijfsprocessen waar deze productiemiddelen een rol in spelen hebben niet een directe koppeling met ICT-middelen, maar worden wel geleverd of aangestuurd met behulp van ICT-middelen. Denk aan een logistiek proces waarbij het transport zelf niet geautomatiseerd is, maar waarbij wel de logistieke planning met behulp van een ICT middel wordt uitgevoerd. Om grip te krijgen op ICT supply chain risico's is dit perspectief, samen met het informatie perspectief, extra interessant omdat dit een blinde vlek kan zijn bij het identificeren van ICT-risico's. Het incident NotPetya en de verstoringen bij MAERSK laten zien dat het transport van fysieke goederen van andere organisaties ook stil kwam te liggen, terwijl de logistieke processen van deze organisaties in veel gevallen op geen enkele manier verbonden waren met de ICT-systemen van MAERSK [14]. In dit perspectief ligt de nadruk op het in kaart brengen van producten en diensten waar bedrijfsprocessen van afhankelijk zijn, hoe die vervolgens afhankelijk zijn van andere (al dan niet ICT-)producten en -diensten. Doordat er niet uitsluitend naar ICT-afhankelijkheden wordt gekeken, kunnen risico's die eerder buiten beeld bleven mogelijk geïdentificeerd worden.

6 Conclusie

Het doel van het onderzoek was om supply chain vraagstukken te identificeren, methoden te analyseren die supply chain risico's onderzoeken en perspectieven te formuleren waarmee ICT supply chains en de risicomanagement aanpakken op deze supply chains inzichtelijk gemaakt kunnen worden.

Het onderzoek laat zien dat er een grote mate van complexiteit binnen supply chains bestaat, die in drie punten kan worden uitgesplitst:

- Voor klassieke supply chains wordt in toenemende mate gebruik gemaakt van ICT-systemen om de efficiëntie te vergroten;
- Er is een toenemende verwevenheid van fysieke en digitale systemen (cyber-physical systems);
- De supply chain van ICT-producten en -diensten zelf is enorm complex, door het groot aantal partijen dat benodigd is voor de levering van een product of dienst en de afhankelijkheden die hierdoor ontstaan.

Door de complexiteit van het onderwerp worden veel verschillende begrippen met betrekking tot supply chains op uiteenlopende manieren gebruikt. Vaak worden dezelfde termen gebruikt om verschillende zaken aan te duiden. Door de complexiteit en het door elkaar heen lopen van verschillende begrippen is het lastig de verschillende vraagstukken binnen het onderwerp uit elkaar te halen en overzichtelijk te maken. Om deze reden zijn binnen dit onderzoek vijf perspectieven onderscheiden die kunnen worden gebruikt om de complexiteit rondom supply chain vraagstukken te doorgronden. Deze perspectieven vormen samen de basis voor een analysekader, waarmee wordt beoogd om bestaande ICT SCRM aanpakken te onderzoeken, deze beter te kunnen duiden en te identificeren waar mogelijke lacunes zitten.

Om dit te kunnen bereiken moet het analysekader verder worden ontwikkeld. Zo moeten de perspectieven worden getoetst om te achterhalen of er nog meer perspectieven zijn die moeten worden toegevoegd. Daarnaast moet worden onderzocht of het analysekader kan bijdragen aan het analyseren van de methoden en de in de praktijk ervaren knelpunten, of dat er andere manieren zijn waarop het kan bijdragen aan het zicht krijgen op en onder controle krijgen van ICT supply chain risico's.

Verder onderzoek zal zich ook richten op welke manieren het kader analysekader gebruikt kan worden en aan het opstellen van een gezamenlijk begrippenkader. Tot slot zal er verder onderzoek gedaan worden naar ICT SCRM vanuit het analysekader, in de volgende richtingen:

- Verdieping zoeken op specifieke vraagstukken die in de interviews zijn genoemd, zoals de toenemende afhankelijkheid van cloudomgevingen, de effectiviteit van huidige risicomanagement aanpakken als assurance en SLAs of het analyseren van een ICT supply chain;
- Handelingsperspectieven ontwikkelen voor één of meerdere behoeften die in de interviews zijn genoemd, aanvullend op de vraagstukken uit het hierboven genoemde punt;
- Het analyseren van supply chain-risicomanagementmethoden. De methoden kunnen worden geanalyseerd op basis van de mate van toepasbaarheid in de

praktijk en welk perspectief zij aannemen (toepassing in de praktijk, keuze richtingen, inzicht in diversiteit en toepasbaarheid);
- Het analyseren van één supply chain vanuit de vijf perspectieven om de verschillende risico's te duiden en de meerwaarde van het analysemodel te toetsen.

7 Referenties

AON (2019). Cyber Perils in a Growing Market. White paper. Beschikbaar via https://www.aon.com/unitedkingdom/insights/cyber-perils-in-a-growing-market.jsp

Barlow, A. and Li, F. (2007). E-supply chains: understanding current and future opportunities and barriers, *International Journal of Information Technology and Management*, Vol. 6 No. 2-3-4, pp. 286-298.

Bartol, N. (2014). Cyber supply chain security practices DNA – filling in the puzzle using a diverse set of disciplines, *Technovation*, Vol. 34 No. 7, pp. 354-361.

Boyens, J. (2016). Integrating Cybersecurity into Supply Chain Risk Management. RSA Conference 2016, San Francisco. https://www.slideshare.net/cisoplatform7/integrating-cybersecurity-into-supply-chain-risk-management

Boyens, J., Paulsen, C., Moorthy, R., Bartol, N. & Shankles, S. (2015a). NIST special publication 800-161: Supply chain risk management practices for federal in-formation systems and organizations. *Gaithersburg: National Institute of Standards and Technology.*

Boyens, J., Paulsen, C., Feldman, L. & White, G. (2015b) Increasing Visibility and Control of your ICT Supply Chains. *ITL Bulletin for June 2015*. Information Technology Laboratory, National Institute of Standards and Technology. https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2015-06.pdf

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems, *Technovation*, Vol. 34 No. 7, pp. 342-353.

Büyüközkan, G. & Göçer, F. (2018). Digital Supply Chain: Literature review and a proposed framework for future research. Computers in Industry, 97, 157-177.

CBS (2018). Cybersecuritymonitor 2018. *Een verkenning van dreigingen, incidenten en maatregelen*. Den Haag: CBS. Beschikbaar via https://www.cbs.nl/nl-nl/publicatie/2018/38/cybersecuritymonitor-2018

Crosignani, M., Macchiavelli, M. & Silva, A.F. (2020). Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains. Federal Reserve Bank of New York Staff Reports, no. 937. Beschikbaar via: https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr937.pdf

Curkovic, S., Scannell, T., Wagner, B. & Vitek, M. (2013). Supply chain risk management within the context of cosco's enterprise risk management framework. *Journal of Business Administration Research*, 2(1), 15.

Cyber Security Raad (2016). Digitale ketenveiligheid krijgt veel te weinig aandacht. Beschikbaar via https://www.cybersecurityraad.nl/010_Actueel/digitale-ketenveiligheid-krijgt-veel-te-weinig-aandacht.aspx

DiMase, D., Collier, Z. A., Heffner, K. & Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. Environment Systems and Decisions, 35(2), 291-300.

ENISA (2015). Supply Chain Integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward. *European Union Agency for Network and Information Security.* Beschikbaar via https://www.enisa.europa.eu/publications/sci-2015

Gelevert, H., Smulders, A. & Van den Brink, P. (2017). *Digitaal Veilige Hard- en Software*. TNO 2017 R10865. Den Haag: TNO

Ghadge, A., Dani, S. & Kalawsky, R. (2012). Supply chain risk management: present and future scope. *The international journal of logistics management*. *23*(3), 313-339. DOI: 10.1108/09574091211289200.

Ghadge, A., Weiß, M., Caldwell, N.D. & Wilding, R. (2019). Managing cyber risk in supply chains: a review and research agenda. *Supply Chain Management*, Vol. 25 No. 2, pp. 223-240. https://doi.org/10.1108/SCM-10-2018-0357

Greenberg, A. (2018) The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*. Beschikbaar via: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Hoyt, R. E. & Liebenberg, A. P. (2011). The value of enterprise risk management. *Journal of risk and insurance*, 78(4), 795-822.

Johnson, K. (2019). What is digital supply chain management? *Bitsight*. Beschikbaar via: https://www.bitsight.com/blog/what-is-digital-supply-chain-management

Khan, O. & Sepúlveda Estay, D. A. (2015). Supply Chain Cyber-Resilience: Creating an Agenda for Future Research. *Technology Innovation Management Review*, 5(4): 6-12. http://doi.org/10.22215/timreview/885

Lambert, D. M., & Cooper, M. C. (2000). Issues in supply chain management. *Industrial marketing management*, *29*(1), 65-83.

Linton, J. D., Boyson, S., & Aje, J. (2014). The challenge of cyber supply chain security to research and practice. An introduction. *Technovation*, Vol. 34 No. 7, pp. 339-341.

Mentzer, J. T., DeWitt, W., Keebler, J. S., Min, S., Nix, N. W., Smith, C. D., & Zacharia, Z. G. (2001). Defining supply chain management. *Journal of Business logistics*, 22(2), 1-25.

Ministerie van Buitenlandse Zaken. 2018. Wereldwijd voor een veilig Nederland. Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022.

Ministerie van Justitie en Veiligheid. 2019. Nationale veiligheid strategie 2019.

NCTV (2019). Cybersecurity Beeld Nederland (CSBN) 2019. Den Haag: Ministerie van Justitie en Veiligheid. Beschikbaar via https://www.rijksoverheid.nl/documenten/rapporten/2019/06/12/tk-bijlage-cybersecuritybeeld-nederland-csbn-2019

NCTV (2020). Cybersecurity Beeld Nederland (CSBN) 2020. Den Haag: Ministerie van Jusitie en Veiligheid. Beschikbaar via https://www.rijksoverheid.nl/documenten/rapporten/2020/06/29/tk-bijlage-2-cybersecuritybeeld-nederland-csbn-2020

Nocco, B. W. & Stulz, R. M. (2006). Enterprise risk management: Theory and practice. *Journal of applied corporate finance*, *18*(4), 8-20.

Peck, H. (2006). Reconciling supply chain vulnerability, risk and supply chain management. *International Journal of Logistics Research and Applications*, Vol. 9 No. 2, pp. 127-142.

Reich, J. (2020). Nearly 300 cybersecurity incidents impacted supply chain entities in 2019. *TechRepublic*. Beschikbaar via: https://www.techrepublic.com/article/nearly-300-cybersecurity-incidents-impacted-supply-chain-entities-in-2019

Smith, G. E., Watson, K. J., Baker, W. H. & Pokorski Ii, J. A. (2007). A critical balance: Collaboration and security in the IT-enabled supply chain. *International Journal of Production Research*, Vol. 45 No. 11, pp. 2595-2613.

Soare, B. (2020). Supply Chain Cyber Security: What are the Risks? *Heimdal Security.* Beschikbaar via https://heimdalsecurity.com/blog/supply-chain-cyber-security/

Van Ruijven, T. & Keijser, B. (2017). Ketenweerbaarheid tegen cyberdreigingen. Whitepaper. Den Haag: TNO. Beschikbaar via: https://www.tno.nl/nl/aandachtsgebieden/defensie-veiligheid/roadmaps/nationale-veiligheid/cybersecurity-het-belang-van-integrale-oplossingen/cybersecurity-ketens-en-processen-in-beeld/whitepaper-ketenweerbaarheid-tegen-cyberdreigingen/

Wainstein, L. (2018). 7 Supply Chain Concerns to Address ASAP. *The Network Effect. Beyond Supply Chains.* https://supplychainbeyond.com/7-supply-chain-security-concerns-to-address-asap/

Wells, L. J., Camelio, J. A., Williams, C. B. & White, J. (2014). Cyber-physical security challenges in manufacturing systems. *Manufacturing Letters*, 2(2), 74-77.

Windelberg, M. (2016). Objectives for managing cyber supply chain risk. *International Journal of Critical Infrastructure Protection*, 12, 4-11.

WRR (2019). *Voorbereiden op digitale ontwrichting*. Wetenschappelijke Raad voor het Regeringsbeleid, Den Haag. Beschikbaar via https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting

Referenties methoden

Cybersecurity and Infrastructure Security Ageny (2018). Supply Chain Risks for Information and Communication Technology. Beschikbaar via Supply Chain Risks for Information and Communication Technology (cisa.gov).

Cyber Security Raad (2015). Cyber security supply chain risicoanalyse 2015. Beschikbaar via Cybersecurity_supply_chain_risico-analyse_DEF_tcm107-314472.pdf (cybersecurityraad.nl).

ISO/IEC 27036-3 (2013). Information technology – Security techniques – Information security for supplier relationships - Part 3: Guidelines for ICT supply chain security. Beschikbaar via ISO - ISO/IEC 27036-3:2013 - Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security.

National Institute of Standards and Technology (2015). Supply Chain Risk Management Practices for Federal Information Systems and Organizations.

Beschikbaar via SP 800-161, Supply Chain Risk Management Practices for Fed Info Sys and Orgs | CSRC (nist.gov)

MITRE (2014). Supply Chain Attack Framework and Attack Patterns. Beschikbaar via Supply Chain Attack Framework and Attack Patterns (mitre.org).

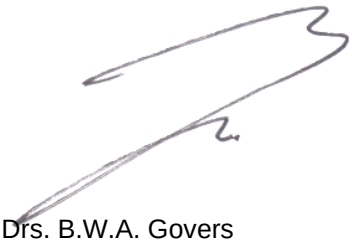
MITRE (2017). Guidance for System Security Engineers. Beschikbaar via The MITRE Systems Engineering Guide.

Schauer, S., Polemi, N., Mouratidis, H. (2019). MITIGATE: a dynamic supply chain cyber risk assessment methodology. *Journal of Transportation Security,* 12, 1-35. Beschikbaar via MITIGATE: a dynamic supply chain cyber risk assessment methodology | Request PDF (researchgate.net).

8 Ondertekening

Den Haag, februari 2021

TNO
Networked Organisations



Drs. B.W.A. Govers
Plv research manager

P.E. van den Brink MSc
Auteur

A Geïnterviewde organisaties en interviewvragenlijst

A.1 Geïnterviewde organisaties

Er is zijn acht diepte interviews gehouden met grote Nederlandse organisaties en overheidspartijen (zowel publiek als privaat).

A.2 Interviewvragenlijst

SCRM

1 Wat betekent supply chain (management) voor jou? Hoe is dit in jouw organisatie ingericht? (Als het heel specifiek ICT is, vraag hoe dit is gelinkt aan het bredere plaatje, en andersom).
2 Welke vraagstukken leven er op dit gebied? Waarom is supply chain management belangrijk? Welke (ICT) supply chain risico's zien jullie?
   a) Wat zien jullie als belangrijke dreigingen/risico's?
   b) Kunnen er voorbeelden van ketenrisico's benoemd worden?
   c) Kunnen er voorbeelden van de effecten van ketenrisico's benoemd worden die men zelf heeft meegemaakt?
3 Wat voor soort suppy chains brengen jullie in kaart? Waar richten jullie je dan op?
   a) Wie zien jullie als ketenpartners in deze keten(s)?
      i) Hoe kader je de afhankelijkheden van anderen af?
   b) Op welke manier interacteren jullie met deze partners (informatie uitwisseling, regulier afstemmen, samenwerking, etc.) (stel samenwerking, doorvragen).

Verantwoordelijkheden, taken en mandaat m.b.t. risicomanagement in de org.

1 Hoe is supply chain (risico) management onderdeel van risico management in jullie organisatie?
2 Hoe stem je de risico's af? En hoe is dit belegd? (Belangrijk om door te vragen, willen weten hoe het georganiseerd is)
3 Hoe worden de cyber (supply chain) risico's gerelateerd aan andere (business) risico's? (denk aan impact van IT systemen an sich, of dit door vertalen naar omzet of andere business continuïteit, of reputatie, etc.)
4 Zijn er dingen waar jullie tegenaan lopen, behoeften aan hebben?

Hoe zien de bestaande (keten)risico analyses eruit?

1 Hoe worden analyses uitgevoerd (aanpak), welke methoden worden gebruikt?
   a) Welke instrumenten heb je tot je beschikking? (tooling, standaarden, methoden, …).
2 Wat is het resultaat (en hoe wordt het verder gebruikt in de organisatie)?
3 Wordt ICT/Cyber SCRM apart uitgevoerd of valt dit onder het bredere risico management proces?
   a) Indien apart proces: hoe worden de resultaten van die risicoafweging vertaald naar de bedrijfsvoering? (let op: wordt er gekeken naar afnemer (operationele processen) en/of de leveranciers/contractors (en verder) van IT producten bij ketenanalyses en risico's).

4 Wie is er betrokken (ook externen (binnen (andere afdelingen) en buiten (leveranciers) de eigen organisatie)? Welke informatie wordt gebruikt van anderen en hoe stemmen jullie dit af?
5 Waar lopen jullie tegenaan bij het uitvoeren van (keten)risico analyses? Zijn er specifieke behoeften die jullie hebben (ondersteuning, andere methoden, informatiebehoeften, …)

Incident met keteneffecten

1 Welke procedures hanteren jullie op het moment van een incident waarbij keteneffecten een rol spelen? (zowel incident bij jullie als bij een ketenpartner).
   a. Op welke manier betrekken jullie ketenpartners (afspraken, info uitwisselen, alerteren, etc.).
   b. Teruggrijpen, indien benoemd, voorbeelden van concrete incidenten.
2 Zijn er dingen waar jullie tegenaan lopen, behoeften aan hebben?

Afsluiting

Introductie leidraad (structuur, overzicht, good practices, etc. en voorbeeld CVD)

1 Wanneer heeft een dergelijke leidraad meerwaarde voor jullie?
2 Waar zou een leidraad volgens jullie aan moeten voldoen?
3 Zijn er specifieke elementen of behoeften die jullie terug willen zien in een leidraad?
4 Wat moet er vooral niet in een leidraad komen te staan?