Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Aan de slag met het kwantificeren van cyber-risico's

TNO innovation for life

Aan de slag met het kwantificeren van cyberrisico's

Inleiding

Achtergrond

TNO heeft in opdracht van het NCSC een methode ontwikkeld voor het kwantificeren van de kans op, en impact van, specifieke cyberrisico's. De resulterende methode bouwt voort op een risicomanagementmethode ontwikkeld binnen het Shared Research Programma Cybersecurity, een samenwerkingsverband tussen TNO en een aantal Nederlandse (financiële) instellingen: ABN AMRO, Rabobank, ING, De Volksbank, en Achmea. Eind 2022 leverde dat een methode en deze stapsgewijze handleiding voor de toepassing van de methode op voor organisaties die hiermee aan de slag willen.

Waarom het kwantificeren van cyberrisico's?

Veel risicoanalyses leveren een kwalitatieve inschatting op van mogelijke risico's, bijvoorbeeld in de vorm van heat-maps of laag-midden-hoog verdelingen. Nu is dit beter dan helemaal geen risicoanalyse doen, maar kwantitatieve methodes hebben de volgende voordelen vergeleken met kwalitatieve methodes:

- Je kan de effectiviteit van beheersmaatregelen doorrekenen, wat risico's beheersbaarder maakt.
- Je kan gedeelde risico's tussen organisaties in kaart brengen.
- Je kan organisaties met elkaar vergelijken.
- Je kan sectorale risicobeelden ontwikkelen.
- Je kan de methode makkelijker automatiseren wat het uitvoeren van trendanalyses makkelijker en efficiënter maakt.
- Met het voltooide model is het mogelijk om gevoeligheidsanalyses uit te voeren waarmee je onder meer inzicht kan krijgen in de relevantie van verschillende mitigerende maatregelen, alsmede de gevolgen van onzekerheden in de input.
- Je kan geïnformeerde beslissingen maken met betrekking tot investeringen om cyberrisico's af te dekken.

Deze methode in het kort

De door TNO en het NCSC ontwikkelde methode omvat een aantal stappen die je doorloopt om gegevens te verzamelen en te analyseren voor het kwantificeren van cyberrisico's. Een cyberrisico is in dit geval de kans op, en schade door, een cyberaanval. Voor de uitwerking kies je één relevante dreiging. Vervolgens verzamel je de nodige basisinformatie die binnen de organisatie al aanwezig is en structureer je de informatie aan de hand van een door TNO opgezet basismodel. Zo kom je tot een organisatiespecifiek model dat zowel gegevens over de impact, frequentie en aard van het gekozen cyberrisico omvat, alsook bedrijfsspecifieke mitigerende maatregelen meeneemt die bijdragen aan de weerbaarheid van de digitale infrastructuur van de organisatie. De methode maakt later gebruik van interactieve workshops met experts uit verschillende afdelingen binnen de

Inleiding

organisatie om voor het organisatiespecifieke model gezamenlijk de benodigde risico-inschattingen te maken, eventuele ontbrekende informatie te verzamelen, en de reeds verzamelde informatie te valideren. Om de methode uit te voeren kan je gebruik maken van data uit openbare bronnen, maar ook van gegevens uit eigen onderzoek of inschattingen. Vervolgens kan je de verzamelde gegevens verwerken in een Bayesian Belief Network (BBN) rekenmodel om de waarschijnlijkheid van het optreden van een bepaald cyberrisico te duiden. Deze handleiding beschrijft de voor de methode benodigde stappen en verwijst naar een BBN tool en een aantal voorbeelden van rekenmodellen waarmee je direct zelf aan de slag kan gaan om cyberrisico's in de organisatie te kwantificeren.

Naast de door TNO en het NCSC ontwikkelde methode bestaan er ook andere kwantitatieve methoden, zoals de FAIR methode en Hubbard en Seiersen's methode. In deze methode is ervoor gekozen om de kwantitatieve berekeningen van cyberrisico's met behulp van een BBN uit te voeren en via de processenstappen zoals beschreven in de handleiding tot de nodige data te komen. Uit verschillende case studies die tijdens het opzetten van de methode gedaan werden, kwam naar voren dat de processtappen een belangrijke rol spelen in het duidelijk maken van de risico's voor de stakeholders en dat het kwantificeren van risico's via BNNs deze stappen toegankelijker maakt.

Voor wie is de methode?

De opzet van de TNO/NCSC methode is speciaal gericht op organisaties in de vitale sector om het risico van specifieke dreigingsscenario's voor de eigen infrastructuur te kunnen inschatten. Het kwantificeren van risico's is voor beginnende organisaties echter niet de makkelijkste methode om mee te beginnen. In het volwassenheidsmodel informatiebeveiliging van de Ledengroep Interne en Overheidsaccountants-diensten van de Nederlandse Beroepsorganisatie voor Accountants (NBA-LIO), en NOREA (de beroepsorganisatie van IT-Auditors), dient een methode zoals deze zich aan op volwassenheidsniveau 4, waar correlaties en dreigingsanalyses worden gecombineerd **(figuur 1)**.

Organisaties met een lager volwassenheidsniveau hebben meer aan de blogs van Hugo of de NCSC factsheet risico's beheersen.

Wat levert de methode op?

De resultaten van de methode kunnen op verschillende manieren worden toegepast binnen de organisatie. Denk bijvoorbeeld aan een betere onderbouwing van (cybersecurity) beleid en het kunnen maken van geïnformeerde beslissingen met betrekking tot cyber investeringen. Daarnaast stelt de ontwikkelde methode je in staat om niet alleen cyberrisico's kwantitatief in kaart te brengen, maar ook om de eigen organisatie

Aan de slag met het kwantificeren van cyberrisico's

Inleiding

orga
benc
infor
Om c
bron
Verv
Netv
een k
meth
voor
om c

Naas
ande
Seie
tieve
en vi
nodi
van c
een belangrijke rol spelen in het duidelijk maken van de risico's voor de stakeholders en maken de stap deze risico's te kwantificeren via BBN toegankelijker.

Figuur 1: Kenmerken van volwassenheid in risico-analyse

Kader sluiten ✖

Area	ID	Control Name/ Control Objective	Maturity Indication Level 1 **Initial** Controls are not, or only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	Maturity Indication Level 2 **Repeatable** Controls are in place and executed in a structured and consistent, but informal, manner.	Maturity Indication Level 3 **Defined** Controls are documented and executed in a structured and formal manner. Execution of control can be proved, is tested and effective.	Maturity Indication Level 4 **Managed and measurable** The effectiveness of the control is periodically assessed an improved when necessary. This assessment is documented.	Maturity Indication Level 5 **Continuous improvement** An enterprise wide risk and control programme provides continuous and effective control and risk issues resolution.
	RM.02	**Risk assessment** Risk assessments are executed to determine actual risk profiles regarding business objectives. The likelihood and impact of all identified risks are assessed on a recurrent basis, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risks are determined per category, on a portfolio basis.	– Information risk assessments are rarely carried out and rely heavily on individuals. – In some cases, risk assessments are executed as part of the project plan.	– Risk assessments are executed as part of the risk management process and risks are identified qualitatively and/or quantitatively. – The likelihood and/or impact are mostly determined based on general criteria and not fully aligned with the organization's business objectives. – Risk assessments (as part of project) are documented concisely.	– Consistent and recurrent execution of risk assessments is enforced by clear and appropriate instructions, as part of the information risk management process and related information risk framework. – The risk assessment methodology is in line with the business and ensures that key business risks, including "crown juwels", are identified. – The identified information risks are qualitatively and/or quantitatively assessed by the risk management process / framework or good practice sources. – Deviations in risk appetite / profile regarding risk mitigation are reported to (senior) management.	In addition: – The correlations between identified risks are (cross-functional) analyzed and documented. For example results of cyber security threat analysis are incorporated in the overall risk heat map. – Risk assessment methodology is evaluated on a periodic basis.	In addition: Information risk assessment methodology is fully supported via automated tooling, automatic workflow processing and integrated dashboards.

geïnformeerde beslissingen met betrekking tot cyber investeringen. Daarnaast stelt de ontwikkelde methode je in staat om niet alleen cyber-risico's kwantitatief in kaart te brengen, maar ook om de eigen organisatie

Inleiding

en afhankelijkheden tussen bedrijfsprocessen beter in beeld te krijgen. Het kan je inzicht geven in welke maatregelen je (aanvullend) zou moeten treffen, of welke bestaande maatregelen slechts een minimale vermindering van cyberrisico's opleveren.
Daarmee omvat deze methode een aantal stappen uit het risicomanagementproces, specifiek uit het risicobeoordelingsgedeelte. De methode stelt je in staat om risico's die relevant zijn voor een dreigingsscenario te identificeren en mitigerende maatregelen te analyseren. Met de informatie die je daaruit verkrijgt kan je de risico's evalueren en vervolgens eventuele vervolgstappen ondernemen. Zodoende is deze methode een waardevol onderdeel van het risicomanagementproces.

Deze handleiding

Dit document is de handleiding voor het gebruik van de methode. Achtereenvolgens worden de volgende stappen beschreven:

- Doelstelling en planning
- Verzamelen basisinformatie
- Vormgeving van het basismodel aan de hand van de eigen gegevens
  - Dreiging, impact en processen
  - ICT infrastructuur en bedrijfsspecifieke maatregelen
  - Kwantitatieve inschattingen
- Invullen en analyse van het rekenmodel

Om kwantitatieve cyberrisicoanalyses te kunnen maken dien je een bijbehorend rekenmodel uit te werken en in te vullen. Dit doe je aan de hand van de bovengenoemde stappen, die verderop in detail zijn beschreven. In bijlage 1 → van deze handleiding staan de instructies omtrent het ontwikkelen en bouwen van de bijbehorende rekentool in een BBN. Alhoewel deze handleiding het commerciële programma GeNie gebruikt voor het ontwikkelen van een BBN, bestaan hiervoor niet-commerciële open-source alternatieven zoals MSBNx en UnBBayes. Beide programma's zijn gratis, maar UnBBayes lijkt het beste alternatief voor GeNIe vanwege de functionaliteit en omdat er actief aan gewerkt wordt. Bijlage 1 omvat ook instructies voor het installeren van het GeNIe programma, die je het beste door kan lopen alvorens je met de methode begint.

Bijlage 2 → van deze handleiding omvat een korte uitleg van BBNs en een aantal voorbeeld BBN-modellen. Twee van deze modellen zijn gebaseerd op echte data aangaande cyberaanvallen, afkomstig van Temple University in de VS en Queensland University in Australië. De voorbeeld BBN-modellen laten zien hoe een volledig uitgewerkt rekenmodel opgebouwd is, en beschrijven welke mogelijkheden bestaan om tot een compleet model te komen.

Gebruik dit figuur om door de handleiding te navigeren.

Aan de slag met het kwantificeren van cyberrisico's

1.

Doelstelling

In deze stap stel je de doelstelling, planning en werkwijze van het kwantificerings-traject vast.

2.

Verzamelen basisinformatie

In deze stap verzamel en analyseer je informatie die binnen de organisatie beschikbaar is.

3.

Vormgeving van het model

In deze stap maak je een organisatiespecifiek model op basis van gegevens uit je eigen organisatie.

4.

Invullen en analyse van het rekenmodel

In de laatste stap neem je de kwantitatieve gegevens op in het rekenmodel.

5.

Bijlage 1: GeNIe

In de eerste bijlage staan instructies voor het ontwikkelen van een rekenmodel in het programma GeNIe.

6.

Bijlage 2: BBN voorbeeld modellen

In deze bijlage staan voorbeeld-modellen en hoe deze gebruikt kunnen worden.

| Referenties / bronnen | Colofon |

Aan de slag met het kwantificeren van cyberrisico's

Terug naar navigatie figuur

1. Doelstelling en planning

WAT In deze voorbereidende stap stel je de beoogde doelstelling en randvoorwaarden voor de kwantificering vast. Daarnaast dien je in deze stap afspraken te maken over de planning en werkwijze.

WAAROM Wanneer een organisatie besluit om een deel van de cyberrisico's te kwantificeren is het van belang om hiervoor in deze voorbereidende fase de doelstelling vast te stellen en om duidelijke afspraken te maken over de werkwijze en de planning van de benodigde werkzaamheden.

WIE In deze fase dien je de kaders voor de toepassing van de methode vast te stellen. Hierbij is het belangrijk om in ieder geval de volgende rollen te benoemen:

- De interne opdrachtgever: de opdrachtgever stelt de doelstelling voor het kwantificeringsproject vast en functioneert als de eindverantwoordelijke voor het project.
- Het projectteam en de projectleider: voor de uitvoering van de werkzaamheden wordt een projectteam samengesteld dat in ieder geval uit een projectleider bestaat en uit één of meer cybersecurity analisten.

TIP:

Bij het vaststellen van de doelstelling behoor je aandacht te besteden aan:

- De risicomanagement methoden die de organisatie gebruikt, en op welke punten de inzichten rond cyberrisico's dienen te worden aangescherpt,
- De beschikbare informatie en tools voor risicomanagement in de organisatie,
- Ervaren knelpunten rond risicomanagement binnen de organisatie,
- Op welke punten meerwaarde van kwantificering wordt verwacht (bijvoorbeeld ter onderbouwing van investeringsbeslissingen; voor vergelijkingen met andere soorten risico's zoals finan-cieel, safety, en onderhoud; voor vergelijkingen met andere organisaties binnen de sector; ...).

1. Doelstelling en planning

HOE De opdrachtgever en het projectteam stellen de doelen vast die ze met het kwantificeren van cyberrisico's willen bereiken, en maken een planning voor de bijhorende activiteiten.

De interne opdrachtgever en het projectteam kiezen het te behandelen dreigingsscenario, bijvoorbeeld: 'ongeautoriseerde toegang voor externe leveranciers' of 'ransomware aanval'.

Op basis van die gezamenlijk overeengekomen doelstelling stelt de projectleider een projectplan op met de uit te voeren werkzaamheden. De stappen in deze handleiding dienen hiervoor als richtsnoer.

Bij deze werkzaamheden zijn ook een drietal workshops van toepassing die georganiseerd moeten worden. Daarbij zijn experts vanuit verschillende gebieden vereist die tijdig geïnformeerd moeten worden over hun deelname. Expertise op verschillende gebieden is noodzakelijk zoals:

- Kennis over de bedrijfsprocessen en de mogelijke impact van verstoringen; deze kennis is bijvoorbeeld beschikbaar bij crisismanagers en business continuity managers.
- Kennis over de cyberdreiging en mogelijke aanvalsvectoren, oftewel de manier waarop actoren toegang zouden kunnen krijgen tot de infrastructuur van de organisatie; deze kennis is vaak beschikbaar bij ICT en cyber experts, bijvoorbeeld op het gebied van Cyber Threat Intelligence.
- Kennis over de IT (en eventueel OT) infrastructuur binnen de organisatie; dit betreft experts uit zowel de algemene ICT als de operationele technologie, bijvoorbeeld met kennis op architectuurniveau.

TIP:

Let bij het inplannen op voldoende doorlooptijd tussen de workshops. Tussen de workshops heeft het projectteam tijd nodig om de informatie te verwerken en de daaropvolgende workshops voor te bereiden.

TIP:

De laatste trends en dreigingen op het gebied van cyber in Europa zijn beschikbaar in het Cybersecuritybeeld Nederland (CSBN), op de website van ENISA en bij (commerciële) threat intelligence feeds en cybersecurity trendrapportages.

1. Doelstelling en planning

Tevens dien je in deze fase afspraken te maken over de vertrouwelijkheid van de informatie en over de wijze waarop deze wordt behandeld.

Na het opstellen van de werkzaamheden kan het projectplan worden aangevuld met een tijdslijn. Je kan daarvoor deze **voorbeeldplanning** als startpunt gebruiken.

TIP:

In het geval van begeleiding van het traject door een externe organisatie kan het raadzaam zijn om een Non-Disclosure Agreement (NDA) op te stellen.

› RESULTAAT Deze stap levert een afbakening voor de toepassing van de methode, met in ieder geval de volgende componenten:

- De doelstelling voor de toepassing van de methode,
- Een uitgewerkte projectplanning, inclusief de planning voor de workshops.

Kader sluiten

Voorbeeld van een mogelijk planning van het gehele traject:

Week	Activiteit	Projectteam	Interne opdrachtgever	Benodigde expertise buiten projectteam
T	Voorbereiding overleg over doelstelling en planning	X	X	
T+2	Verzameling basisinformatie		X	
T+4	Vormgeving van het basismodel aan de hand van de eigen gegevens	X		
T+4	Overleg (bespreken feedback basismodel)	X	X	
T+5	Workshop 1: Dreiging, impact en processen	X	X	Experts met kennis van de bedrijfsprocessen en de mogelijke impact van verstoringen
T+6	Workshop 2: ICT infrastructuur en bedrijfsspecifieke maatregelen	X	X	Experts met kennis van de IT en OT infrastructuur
T+8	Workshop 3: Kwantitatieve inschattingen	X	X	Experts met kennis van de IT en OT infrastructuur
T+10	Invullen en analyse van het rekenmodel	X		
T+11	Bespreken resultaten	X	X	

Aan de slag met het kwantificeren van cyberrisico's

Terug naar navigatie figuur

2. Verzamelen basisinformatie

WAT In deze stap inventariseer je informatie die beschikbaar is binnen de organisatie (bijvoorbeeld over de bedrijfsprocessen en de essentiële ICT-systemen) en algemene informatie (bijvoorbeeld over de frequentie van de dreiging en mogelijke aanvalsvectoren).

WAAROM Het verzamelen van basisinformatie is een voorbereidende stap voor de modelvorming. Binnen een organisatie is in het algemeen informatie beschikbaar die als startpunt kan dienen voor de kwantificering. Het is van belang om deze informatie voorafgaand aan de volgende stappen in het kwantificeringstraject te verzamelen en te analyseren zodat hierop optimaal kan worden voortgebouwd. Onder het kopje 'HOE' staat welke informatie van belang kan zijn.

WIE De interne opdrachtgever kan aangeven welke relevante informatie beschikbaar is. Het projectteam zal deze verzamelen en analyseren.

HOE Om deze informatie te verkrijgen analyseer je de bestaande documentatie binnen de organisatie en openbare bronnen. Je gebruikt dus niet een bestaand format, maar verzamelt en analyseert wat beschikbaar is binnen de organisatie en informatie over de specifieke dreiging in openbare bronnen. In zijn algemeenheid zullen dit documenten zijn over bijvoorbeeld:

- Resultaten van eerder door de organisatie uitgevoerde risicoanalyses en business impact analyses;
- Beschrijvingen van de bedrijfsprocessen en de ICT infrastructuur;
- Trendanalyses van de dreiging (bijvoorbeeld CSBN, ENISA dreigingsanalyses);
- Analyses van mogelijke aanvalsvectoren voor het beschouwde dreigingsscenario.

TIP:

De laatste trends en dreigingen op het gebied van cyber in Europa zijn beschikbaar in het Cybersecuritybeeld Nederland (CSBN), op de website van ENISA en bij (commerciële) threat intelligence feeds en cybersecurity trendrapportages.

RESULTAAT Het resultaat van deze stap is een overzicht van alle beschikbare gegevens die waardevol zijn voor het bouwen van een organisatiespecifieke versie van het basismodel in stap 3.

Doelstelling en planning

Vormgeving van het model

3. Vormgeving model aan de hand van eigen gegevens

WAT In deze stap maak je een organisatiespecifiek model op basis van gegevens van de eigen organisatie, het geselecteerde dreigingsscenario en overige informatiebronnen.

WAAROM Voor de kwantificering is het van belang om een aantal belangrijke factoren op een gestructureerde manier aan bod te laten komen. Deze belangrijke factoren zijn vormgegeven in het basismodel (figuur 2). Om de relevante eigenschappen van de eigen organisatie voldoende te representeren dien je dit basismodel uit te werken tot een organisatie-specifiek model.

HOE Wanneer je de benodigde voorbereidingen hebt getroffen, kan je een begin maken aan het ontwikkelen van een organisatiespecifiek model. Om het proces te versimpelen kan je hiervoor als uitgangspunt het basis-model (figuur 2) gebruiken. Het basismodel is een vereenvoudigde grafische weergave van de belangrijkste elementen, opgesplitst in drie blokken, en helpt om gestructureerd gegevens per blok te verzamelen en te analyseren:

1. Gegevens m.b.t. de mogelijke impact van cyberdreigingen;
2. Gegevens m.b.t. frequentie en aard van cyberdreigingen;
3. Weerbaarheid van de infrastructuur van de organisatie.

Zoals het kwantificeringsproces (figuur 3) illustreert, dien je in aanvulling op de gegevens uit de eerdere algemene inventarisatie de aanvullende benodigde gegevens te verzamelen door middel van interactieve workshops met de relevante experts uit de organisatie. De workshops worden gebruikt voor toetsing, aanscherping en aanvulling van het organisatiespecifieke model. Om de discussie tijdens de workshops zo efficiënt mogelijk te kunnen houden zal je aan de workshops moeten beginnen met een stevige basis voor het model, gebaseerd op de analyse in stap 2. Zodoende is het model ook voor

3. Vormgeving model aan de hand van eigen gegevens

alle deelnemers herkenbaar. De workshops dienen dus om van een al tot 80% uitgevoerde uitwerking van het organisatiespecifieke model tot een 100% uitgevoerde uitwerking te kunnen komen.

TIP:
Voor optimaal verloop van de workshops wordt een groepsgrootte van ca. 6 personen aanbevolen.

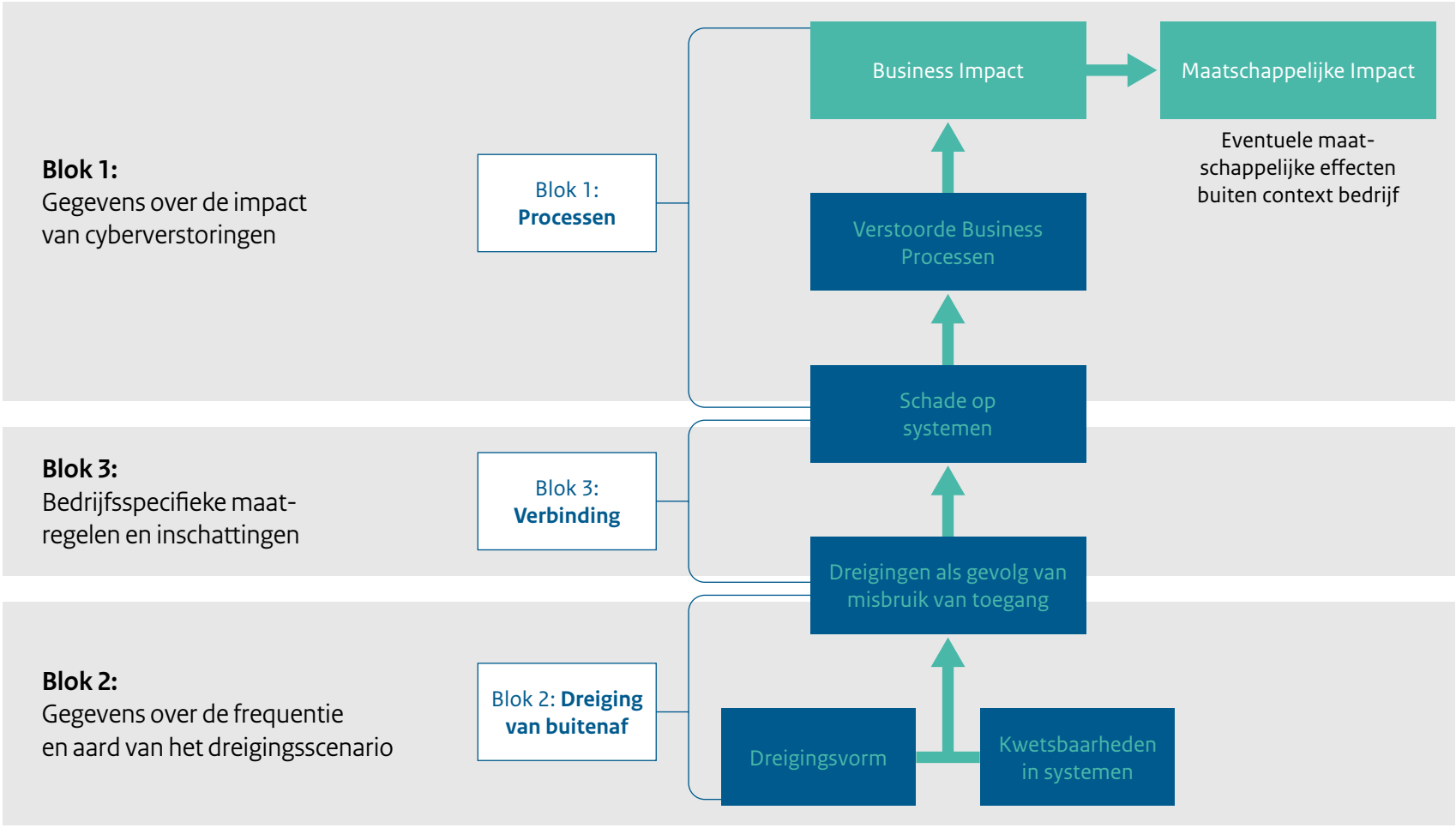
Er zijn minimaal drie workshops aanbevolen. De eerste twee workshops dienen ertoe om het dreigingsscenario voor de eigen infrastructuur verder uit te werken, waarvoor de volgende aspecten relevant zijn:

- Alle relevante bedrijfsprocessen en systemen;
- Mogelijke aanvalsvectoren en actoren;
- De verwachte impact van een manifestatie van de cyberdreiging.

In de derde workshop zet je de verzamelde informatie om in kwantitatieve inschattingen die later in het BBN rekenmodel verwerkt worden.
Elke workshop zal ongeveer een halve dag duren.

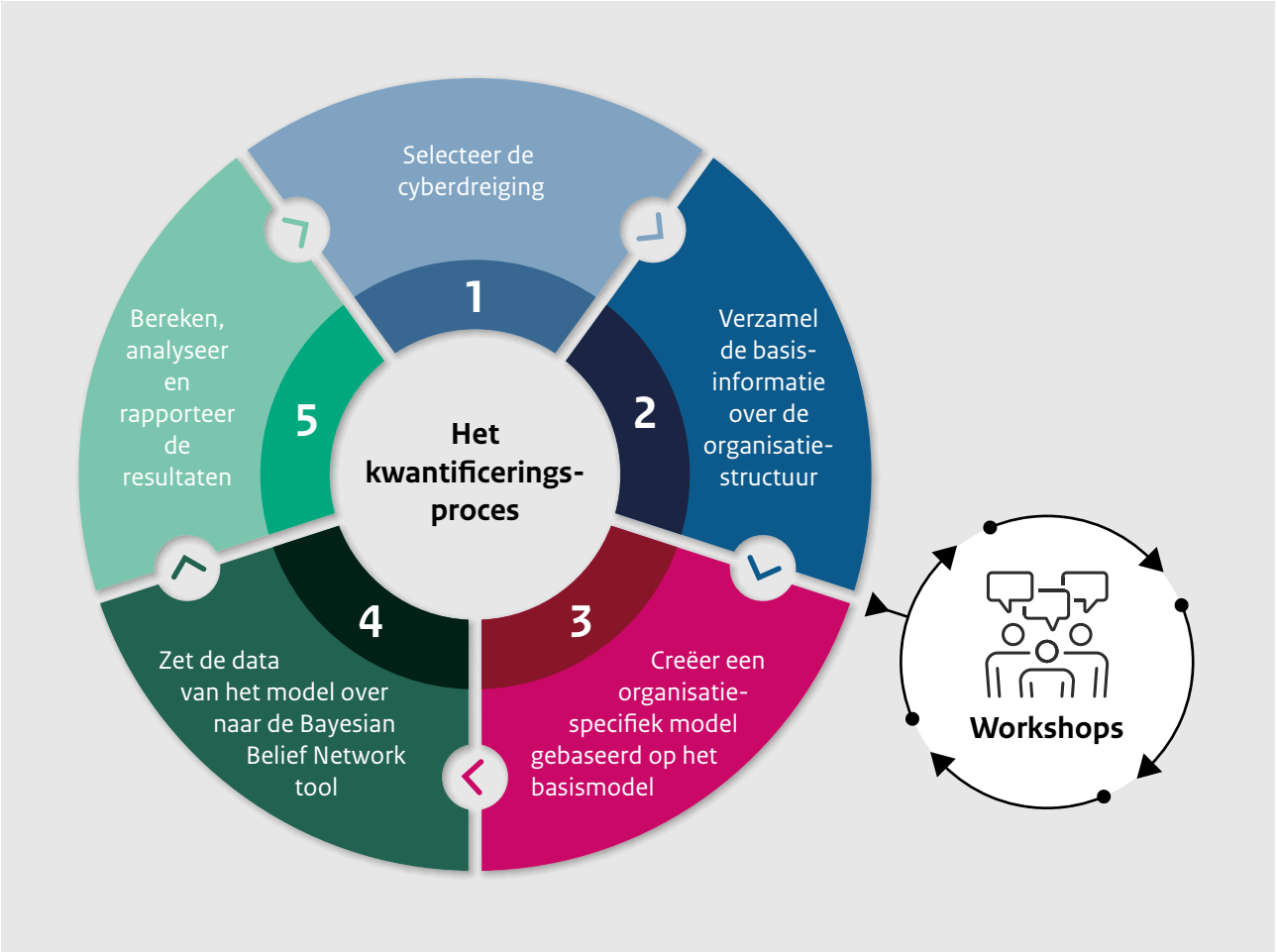
Kader sluiten

Figuur 2: Basismodel



Kader sluiten

Figuur 3: Het kwantificeringsproces



alle deelnemers herker
dus om van een al tot 8
van het organisatiespe
uitgevoerde uitwerking

Er zijn minimaal drie
De eerste twee worksh
dreigingsscenario voo
verder uit te werken, v
aspecten relevant zijn:

- Alle relevante bedri
- Mogelijke aanvalsv
- De verwachte impa

In de derde workshop
inschattingen die later
Elke workshop zal ong

3. Vormgeving model aan de hand van eigen gegevens

Workshop 1: Dreigingen, impact en processen

WAT In deze workshop verzamel je informatie over zowel impact en processen, alsook details over het dreigingsscenario. Dit levert de benodigde gegevens voor blokken 1 en 2 in het basismodel op om tot het organisatiespecifieke model te komen. Het gaat hierbij om:

- De verschillende bedrijfsprocessen;
- De categorieën van impact waarmee u mogelijk te maken krijgt indien de processen/systemen uitvallen;
- Overige relevante factoren met betrekking tot de cyberdreiging.

Deze stap is gericht op de core business van de organisatie. Vraag jezelf bijvoorbeeld af: "Bij verstoring van wat voor processen ervaar je een 'impact', en voor wat voor soorten actoren ben je een interessant doelwit?"

WIE Voor deze workshop heb je experts nodig die inzicht hebben in de core business van de organisatie en de staat van de organisatie (positie in de markt, zichtbaarheid in media, etc.), en personen die goed op de hoogte zijn van het cyberdreigingslandschap in relatie tot de organisatie.

HOE Een deel van deze informatie zal reeds beschikbaar zijn middels de eerder verzamelde basisinformatie. Daarnaast verzamel je tijdens deze workshop, samen met de experts, informatie over impact, processen en dreigingen van buitenaf.

In het eerste deel van de workshop breng je de **primaire bedrijfsprocessen** in kaart, en vervolgens het type **impact** als één of meer van deze processen verstoord worden. Deze informatie is relevant voor blok 1 in het basismodel. In het tweede deel van de workshop onderzoek je welke **actoren** op welke manier de processen kunnen **verstoren**. Deze informatie is relevant voor blok 2 in het basismodel.

RESULTAAT Aan het eind van de workshop heb je een gezamenlijk beeld geschetst van het dreigingsscenario en de mogelijke impact van verstoring van de primaire bedrijfsprocessen. Verder heb je het basismodel specifieker uitgewerkt voor de organisatie en voor het dreigingsscenario. Zie Figuur 4
Daarnaast bouw je een meer specifiek beeld over het dreigingsscenario op, met een gezamenlijk beeld van de relevante actoren en aanvalsvectoren. Zie Figuur 5

Workshop 2

Aan de slag met het kwantificeren van cyberrisico's

Kader sluiten

Eerste deel workshop 1: Impact en processen

1. Je inventariseert met de deelnemers van de workshop de primaire bedrijfsprocessen van de organisatie.

TIP:

Hierbij is het belangrijk om aandacht te besteden aan de volgende punten:

- De mate van afhankelijkheid tussen de processen;
- De mogelijkheid tot afbakening van de processen.

2. Wanneer de processen in kaart zijn gebracht, kan je na gaan denken over wat voor type impact verstoringen van de primaire bedrijfsprocessen op de organisatie zouden kunnen hebben. Evalueer met de experts hoeveel schade zou kunnen ontstaan als de net opgestelde bedrijfsprocessen door de eerder gekozen cyberdreiging geraakt zouden worden in een worst-case scenario.

TIP:

Er kunnen verschillende typen impact worden onderscheiden:

- Financiële schade;
- Veiligheid en gezondheid;
- Duurzaamheid en milieu;
- Stakeholderbelangen;
- Etc.

Workshop 2

Aan de slag met het kwantificeren van cyberrisico's

Kader sluiten

Tweede deel workshop 1: Relevante actoren

Je bepaalt samen met de deelnemers welke actoren voor de cyberdreiging verantwoordelijk zouden kunnen zijn.
In het geval van ransomware kan gedacht worden aan cybercriminelen, scriptkiddies of een insider threat, zoals een corrupte medewerker.
De informatie die eerder is verzameld kan je gebruiken ter beantwoording van deze vraag.

Voor de dreiging dien je een overzicht te maken van de mogelijke aanvalsvectoren.

TIP:

Hierbij kunnen de volgende vragen belangrijk zijn:

- Zou een crimineel bijvoorbeeld in de systemen kunnen komen via phishing mails?
- Ben je afhankelijk van een externe leverancier die mogelijk zijn beveiliging niet op orde heeft?
- Zijn er kwetsbaarheden in de systemen waardoor actoren toegang kunnen krijgen?

Work
Dreig

› WA
proces
benod
organi
- De
- De
pro
- Ove

Deze s
van wa
actore

› WI
core bu
markt, zichtbaarheid in media, etc.), en personen die goed op de hoogte zijn van het cyberdreigingslandschap in relatie tot de organisatie.

dels
ieze
n, en
deze
het
elke
natie
k
odel
rio.

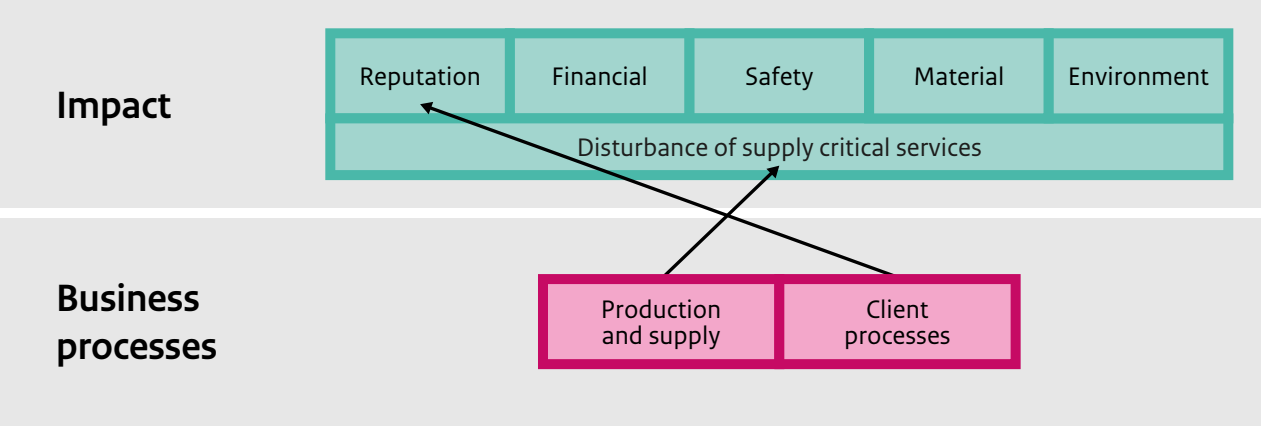
Daarnaast bouw je een meer specifiek beeld over het dreigingsscenario op, met een gezamenlijk beeld van de relevante mogelijke actoren en aanvalsvectoren. Zie Figuur 5

3. Vormgeving model aan de hand van eigen gegevens

Kader sluiten

Figuur 4: Voorbeeld bedrijfsprocessen en mogelijke verstoringen

Voor een organisatie uit de vitale sector bleek de verstoring van de levering van het vitale product de grootste impact te hebben. Ook de verstoring van de klantrelatie werd relevant geacht vanwege de impact op de reputatie. De financiële gevolgen werden minder belangrijk ingeschat.



core business van de organisatie en de staat van de organisatie (positie in de markt, zichtbaarheid in media, etc.), en personen die goed op de hoogte zijn van het cyberdreigingslandschap in relatie tot de organisatie.

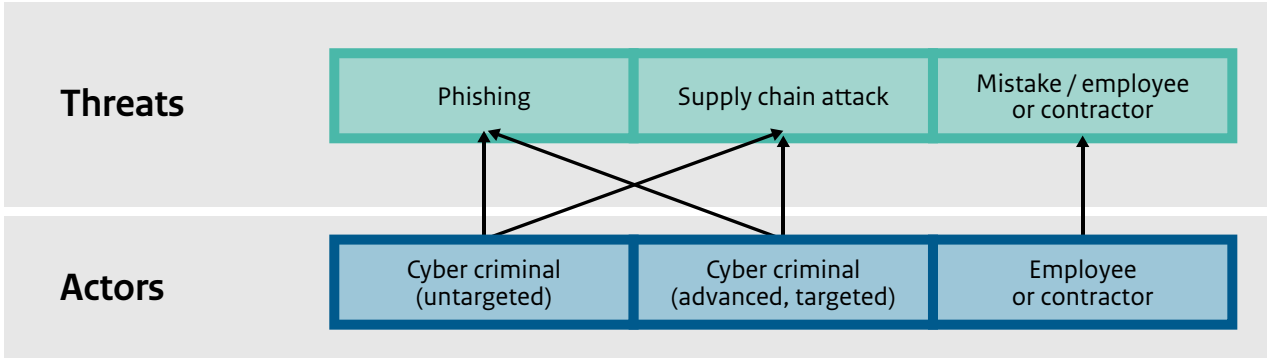
Zie Figuur 4

Daarnaast bouw je een meer specifiek beeld over het dreigingsscenario op, met een gezamenlijk beeld van de relevante mogelijke actoren en aanvalsvectoren. Zie Figuur 5

3. Vormgeving model aan de hand van eigen gegevens

Kader sluiten

Figuur 5: Voorbeeld mogelijke actoren en aanvalsvectoren voor een ransomware scenario



Work
Dreig

> WA

proces
benod
organi

- De
- De
  pro
- Ove

Deze s
van wa
actore

> WIE Voor deze workshop heb je experts nodig die inzicht hebben in de core business van de organisatie en de staat van de organisatie (positie in de markt, zichtbaarheid in media, etc.), en personen die goed op de hoogte zijn van het cyberdreigingslandschap in relatie tot de organisatie.

dels
ieze
n, en

deze
het
elke
natie

k

verstoring van de primaire bedrijfsprocessen. Verder heb je het basismodel specifieker uitgewerkt voor de organisatie en voor het dreigingsscenario. Zie Figuur 4

Daarnaast bouw je een meer specifiek beeld over het dreigingsscenario op, met een gezamenlijk beeld van de relevante mogelijke actoren en aanvalsvectoren. Zie Figuur 5

3. Vormgeving model aan de hand van eigen gegevens

Workshop 2:
ICT infrastructuur en bedrijfsspecifieke maatregelen

› WAT In deze workshop behandel je informatie over de organisatiespecifieke infrastructuur en de maatregelen die de organisatie gebruikt om cyberdreigingen te mitigeren of te voorkomen. Het doel van deze workshop is om inzichten te verzamelen over blok 3 van het basismodel (figuur 2). Dit blok richt zich op de verbinding tussen de cyberdreiging enerzijds en de bedrijfsprocessen anderzijds. Daar zitten de assets (infrastructuur e.d.) tussen die getroffen kunnen worden door de aanval.

Je wil weten:

- Welke systemen draaien er (op hoofdlijnen) binnen de organisatie?
- Wat is de hoofdstructuur van de ICT-infrastructuur (bijvoorbeeld onderverdeling IT en OT)?
- Welke systemen zijn van belang voor de primaire bedrijfsprocessen?
- Hoe kunnen actoren via de aanvalsvectoren die systemen exploiteren?
- Wat zijn specifieke (directe) gevolgen van een manifestatie van de cyberdreiging?
- Welke specifieke preventieve/reactieve maatregelen heeft de organisatie genomen om de cyberdreiging te mitigeren/voorkomen?

Aan de hand van het dreigingsscenario uit workshop 1 kan je de mogelijke consequenties voor de verschillende assets en systemen analyseren. Hierin behoor je ook de specifieke maatregelen mee te nemen. Je behandelt in deze stap voornamelijk blok 3 van het basismodel, maar vanwege de koppeling tussen aanvalsvectoren en systemen en tussen systemen en processen bestaat er enige overlap met blok 1 en 2.

› WIE Voor deze workshop is het van belang dat er personen deelnemen met diepgaande kennis over de infrastructuur van de organisatie, de afhankelijkheid van bedrijfsprocessen van bepaalde systemen, e.d., bijvoorbeeld ICT of security architecten. Wanneer de organisatie zowel over IT als OT beschikt dienen beide onderdelen door experts gerepresenteerd te worden.

Aan de slag met het kwantificeren van cyberrisico's

Terug naar navigatie figuur

3. Vormgeving model aan de hand van eigen gegevens

Workshop 1: Dreigingen, impact en processen | **Workshop 2: ICT infrastructuur en bedrijfsspecifieke maatregelen** | **Workshop 3:** Kwantitatieve inschattingen

HOE In het eerste deel van workshop 2 richt je je op de (**primaire**) **systemen** die van belang zijn om de in workshop 1 geïdentificeerde processen uit te kunnen voeren. Deze informatie is relevant voor blok 3 van het basismodel. In het tweede deel van workshop 2 dien je te kijken naar de mogelijke **consequenties** van de cyberdreiging voor de primaire systemen en bedrijfsprocessen binnen de organisatie, en welke **preventieve/reactieve maatregelen** de organisatie heeft getroffen en zou kunnen treffen om de impact van de cyberdreiging te mitigeren/voorkomen. Deze informatie is relevant voor blok 3.

RESULTAAT Het resultaat van deze workshop is een gezamenlijk beeld van de belangrijkste systemen en de manieren waarop actoren via de aanvalsvectoren kwetsbaarheden binnen de organisatie kunnen exploiteren. Zie Figuur 6

TIP:

Bij de start van de **tweede workshop** is het verstandig om de resultaten van de vorige workshop kort samen te vatten, zeker wanneer de samenstelling van de deelnemersgroep anders is. Denk hierbij aan de volgende punten:

- De verschillende processen van de organisatie;
- Mogelijke typen impact voor de organisatie als gevolg van verstoorde bedrijfsprocessen;
- Relevante factoren van de cyberdreiging (actoren en aanvalsvectoren).

Aan de slag met het kwantificeren van cyberrisico's

Kader sluiten

Eerste deel workshop 2: (Primaire) systemen

Gerelateerd aan de in workshop 1 geïdentificeerde processen, laat je de deelnemers uitzoeken welke systemen binnen de bedrijfs-processen gebruikt worden.

TIP:

Hierbij besteed je aandacht aan de volgende punten:

- Welke systemen zijn essentieel;
- Hoe ziet de hoofdindeling van de systemen eruit (bijvoorbeeld procesautomatisering, kantoorautomatisering, etc.);
- Zijn systemen gekoppeld aan (meerdere) processen;
- Is er sprake van onderliggende relaties/ afhankelijkheden;
- Is er sprake van relevante onder-verdelingen (bijvoorbeeld een koppeling met verschillende locaties, of afbakening van systeemtypen).

3. Vormgeving model aan de hand van eigen gegevens

Kader sluiten

Tweede deel workshop 2: Consequenties en bedrijfsspecifieke maatregelen

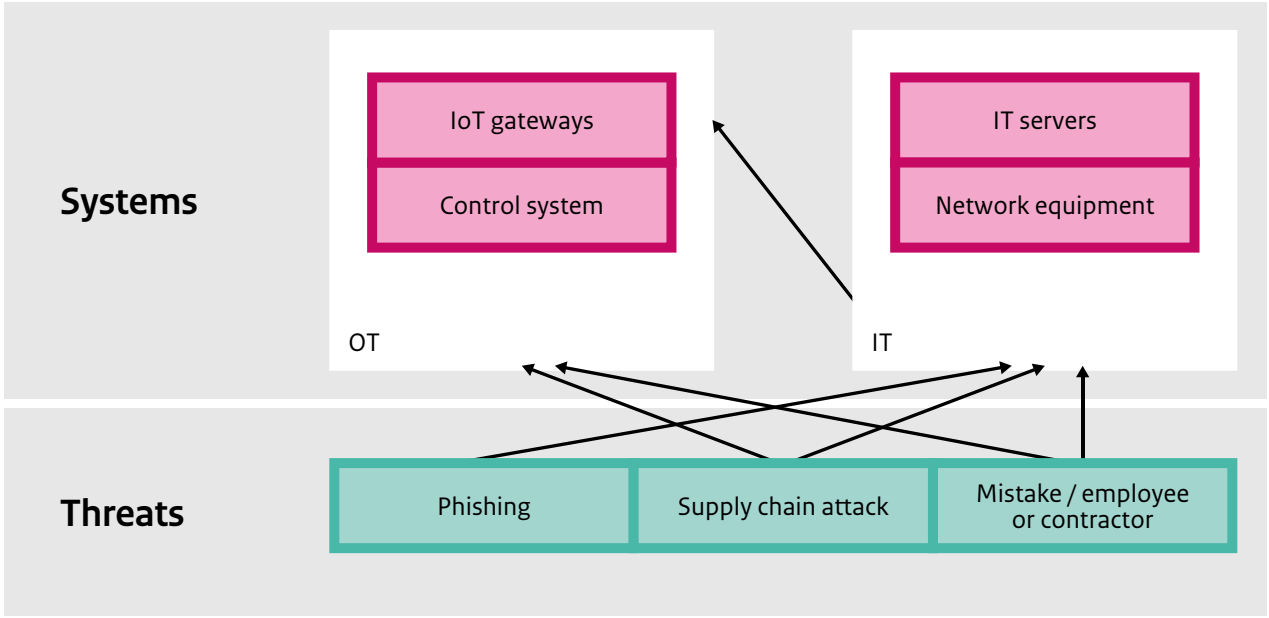
Een belangrijke vraag die je samen met de experts in dit deel dient te beantwoorden is welke systemen schade kunnen oplopen of anderszins getroffen kunnen worden ten gevolge van de cyberdreiging. Daarnaast is het zaak om na te gaan welke maatregelen de organisatie heeft genomen om kwetsbaarheden in de systemen te mitigeren en de cyberdreiging te voorkomen.

TIP:

Bestaat er bijvoorbeeld multi-factor authenticatie voor toegang? Maakt de organisatie gebruik van sterke spamfilters? Gebeuren er regelmatig software updates? Is er netwerk-segmentatie tussen IT en OT of zijn er data back-up procedures?

Kader sluiten

Figuur 6: Voorbeeld van de ICT-infrastructuur van een organisatie en mogelijke aanvalsvectoren voor het dreigingsscenario



3. Vormgeving model aan de hand van eigen gegevens

Workshop 3: Kwantitatieve inschattingen

WAT In deze stap verrijk je de informatie die is verzameld in de eerste twee workshops met kwantitatieve data, zodat je de resultaten later in het rekenmodel kan invoeren. Het doel is om te komen tot kwantitatieve inschattingen waarvoor concrete cijfers niet beschikbaar zijn. In deze gevallen zullen experts tot een inschatting moeten komen, bijvoorbeeld op basis van historische gegevens of door vergelijking met een ander scenario waarover wel gegevens beschikbaar zijn. Het gaat hier bijvoorbeeld over inschattingen over de (relatieve) incidentfrequenties voor verschillende actoren.

WIE Voor deze stap heb je experts nodig met inzicht in de afhankelijkheden van processen en systemen binnen de organisatie. Bij voorkeur zijn dit medewerkers die ervaring hebben met risicoanalyses en die comfortabel zijn met het werken met hypothetische scenario's, omdat veel van de vragen in de vorm van "stel dat... hoe ziet dit er dan uit?" zullen zijn.

HOE De concrete vragen die je in deze fase moet stellen zijn afhankelijk van het opgestelde model, specifiek de informatie die ontbreekt om het model in te kunnen vullen. In algemene zin gaat het om vragen omtrent verwachte incidentfrequenties en gevoeligheden van het model voor genomen maatregelen. Bijvoorbeeld, bepaal je per mogelijke aanvalsvector de kans hierop, gegeven de verschillende mogelijke actoren (hierbij kan onder meer worden gekeken naar historische trends, naburige landen, of informatie over vergelijkbare sectoren), of voor elk systeem hoe waarschijnlijk het ontregeld zou kunnen worden, gegeven een aanvalsvector in combinatie

TIP:

Zeker in het begin kan het lastig zijn nauwkeurige getallen in te vullen. Begin in dat geval met ruwe (meer kwalitatieve) inschattingen, bijvoorbeeld 0%, 33%, 67%, of 100%. Deze waarden kan je in een later stadium (geleidelijk) verfijnen wanneer aanvullende informatie beschikbaar is.

3. Vormgeving model aan de hand van eigen gegevens

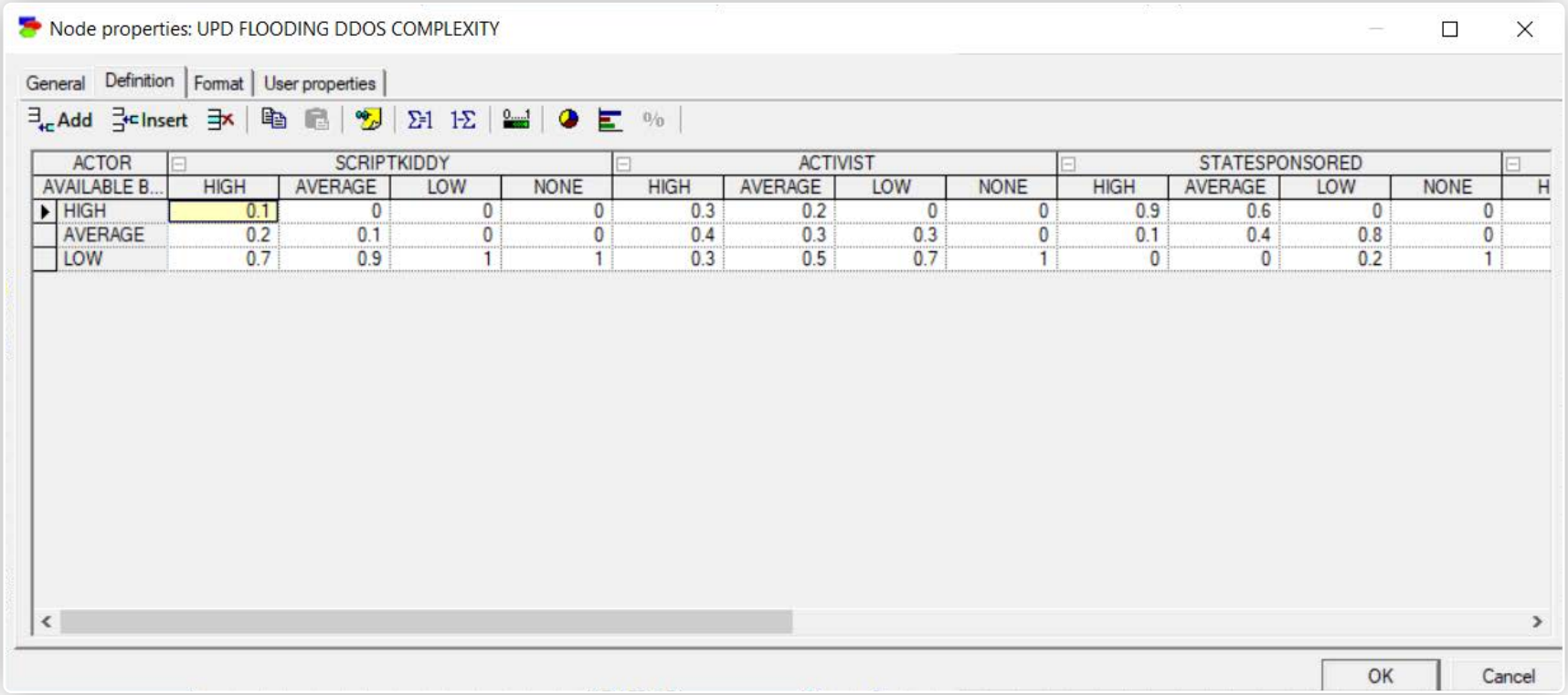
met het wel/niet succesvol zijn van geïdentificeerde mitigerende maatregelen. Om het idee en de werkwijze te verduidelijken zijn er enkele voorbeeldmodellen met toelichting beschikbaar. De toelichting kan je in bijlage 2 vinden. De voorbeeldmodellen kan je op de website van het NCSC downloaden.

RESULTAAT Als resultaat van deze workshop stel je één of meer kanstabellen al dan niet gedeeltelijk op en creëer je een gezamenlijk beeld over de wijze waarop verdere kwantitatieve inschattingen door het projectteam kunnen worden gemaakt. Zie **Figuur 7**

Kader sluiten

Figuur 7: Voorbeeld van een kanstabel voor een 'DDoS complexiteit' node in een model

In dit model hangt de complexiteit af van het soort actor (vaardigheidsniveau) en de beschikbare botnet capaciteit. Hogere vaardigheid en grotere capaciteit maken een complexere DDoS aanval waarschijnlijker.



ACTOR	SCRIPTKIDDY				ACTIVIST				STATESPONSORED				
AVAILABLE B...	HIGH	AVERAGE	LOW	NONE	HIGH	AVERAGE	LOW	NONE	HIGH	AVERAGE	LOW	NONE	H
HIGH	0.1	0	0	0	0.3	0.2	0	0	0.9	0.6	0	0	
AVERAGE	0.2	0.1	0	0	0.4	0.3	0.3	0	0.1	0.4	0.8	0	
LOW	0.7	0.9	1	1	0.3	0.5	0.7	1	0	0	0.2	1	

4. Invullen en analyse van het rekenmodel

WAT In de laatste stap dien je de kwantitatieve gegevens die zijn verkregen uit verschillende databronnen en die verzameld zijn in de derde workshop op te nemen in het rekenmodel. Het rekenmodel is een BBN waarmee je de waarschijnlijkheid van een impact ten gevolge van een cyberdreiging kan bepalen. Een toelichting over BBNs kan je in bijlage 2 van deze handleiding vinden.

WAAROM Om de waarschijnlijkheid en impact van de gekozen cyberdreiging daadwerkelijk kwantitatief te kunnen berekenen, moet je de gegevens die in de eerdere stappen zijn verzameld invoeren in het rekenmodel en analyseren.

WIE De analisten uit het projectteam dienen de analyse voor deze stap uit te voeren. De resultaten bespreken ze met en rapporteren ze aan de interne opdrachtgever.

HOE Voor het maken, invullen en doorrekenen van BBNs zijn verschillende tools beschikbaar. In bijlage 1 van deze handleiding is een instructie opgenomen voor het programma GeNIe. Je kan de instructie doorlopen om de basiskennis voor het programma op te doen en om zelfstandig een BBN te bouwen voor de cyberdreiging. Daarnaast heeft het NCSC enkele modellen met toelichting beschikbaar gesteld op hun website, die als voorbeeld, inspiratie of startpunt kunnen dienen.

Wanneer je de kanstabellen van het model hebt ingevuld, is het mogelijk het model door te rekenen of het model voor andere analyses in te zetten. Je kan bijvoorbeeld een gevoeligheidsanalyse uitvoeren, waarmee het effect van een verandering in een waarde in het model wordt gemeten. Hierdoor kan je inzichtelijk maken hoe groot of klein de onzekerheid is aangaande de uitkomsten van het model, alsook de meerwaarde van incrementele verbeteringen in de effectiviteit van getroffen maatregelen. Zodoende kan je verschillende maatregelen testen om een effect door de organisatie heen in te zien.

4. Invullen en analyse van het rekenmodel

RESULTAAT De samengevoegde resultaten van de doorgelopen stappen leiden tot een gezamenlijk beeld van de wijze waarop de organisatie kwetsbaar is voor een specifiek dreigingsscenario en van de mogelijke impact hiervan. Zie **Figuur 8** Door het opstellen van het model heeft de organisatie inzicht in de afhankelijkheden tussen assets en/of bedrijfsprocessen, mogelijke aangrijpingspunten voor het specifieke dreigingsscenario en de effectiviteit van mogelijke maatregelen om de dreiging te mitigeren. Zie **Figuur 9**

Let op: Bij het gebruik van kwantitatieve methoden is het belangrijk te waken voor valse zekerheid. Een getal, zeker met een paar cijfers achter de komma suggereert een grote precisie, maar is pas echt wat waard als ook de onzekerheidsmarge bekend is. Idealiter zijn onzekerheidsmarges in de output duidelijk aangegeven, maar dit is niet altijd het geval. Het is belangrijk om te realiseren dat onzekerheidsmarges in de input doorwerken in de output, en de mate waarin kan variëren. Om meer inzicht te krijgen in de impact van (mogelijke) onzekerheden in de input kunnen gevoeligheidsanalyses worden ingezet.

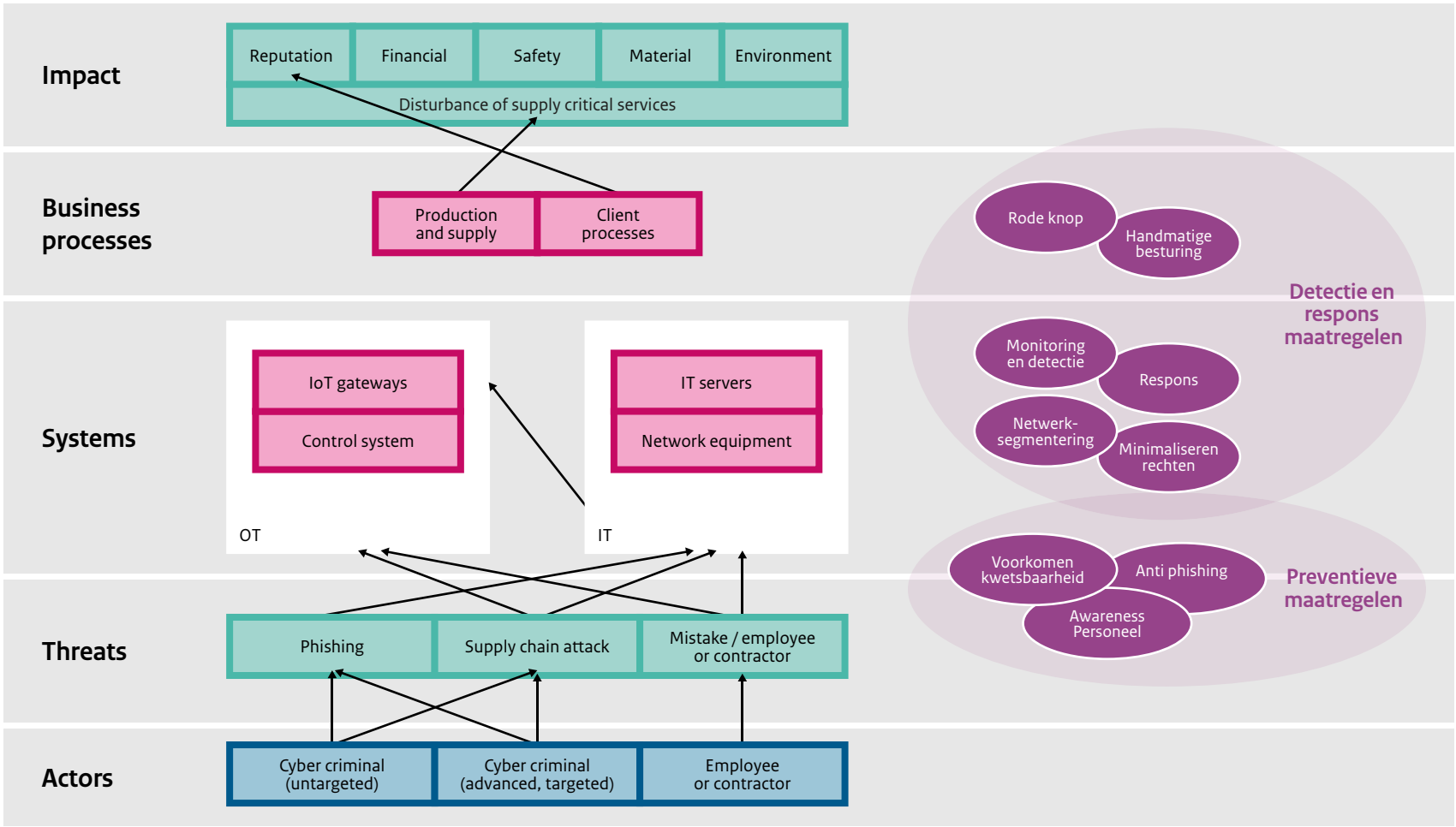
TIP:

Een voltooid model kan in de loop der tijd worden aangevuld, gewijzigd of verfijnd om wijzigingen in de organisatie te reflecteren of om te komen tot nauwkeuriger voorspellingen.

Kader sluiten

Figuur 8: Voorbeeld van een organisatiespecifiek model

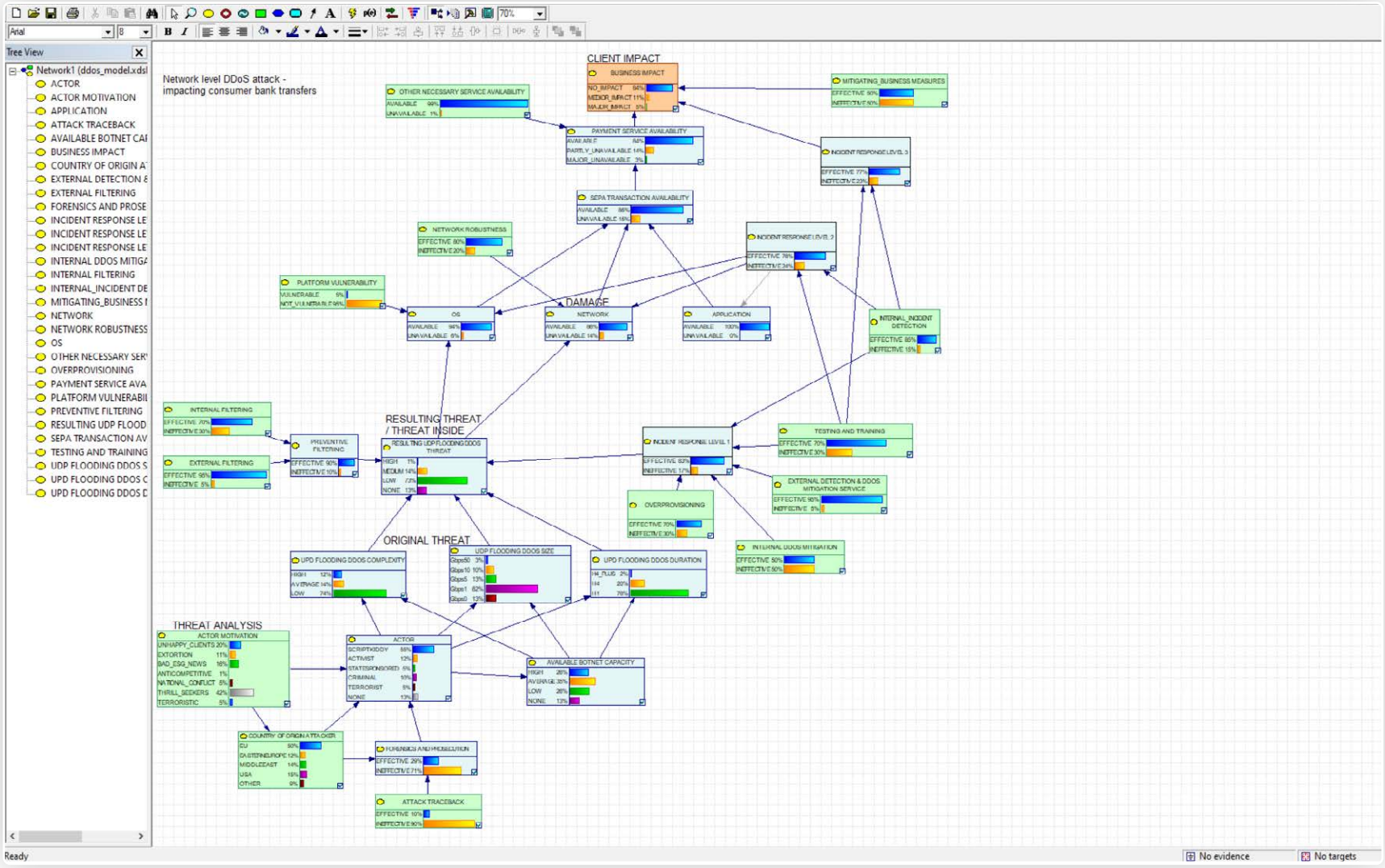
Een organisatiespecifiek model voor de manier waarop een organisatie kwetsbaar is voor een ransomware scenario.



Kader sluiten

Figuur 9: Voorbeeld van een ingevuld rekenmodel in GeNie voor het effect van een DDoS aanval

Geopend in GeNIe, een rekenmodel voor het effect van een DDoS aanval op banktransacties van consumenten [9].



Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Wat is GeNIe?

GeNIe is een programma waarmee op interactieve wijze modellen gemaakt en getest kunnen worden.

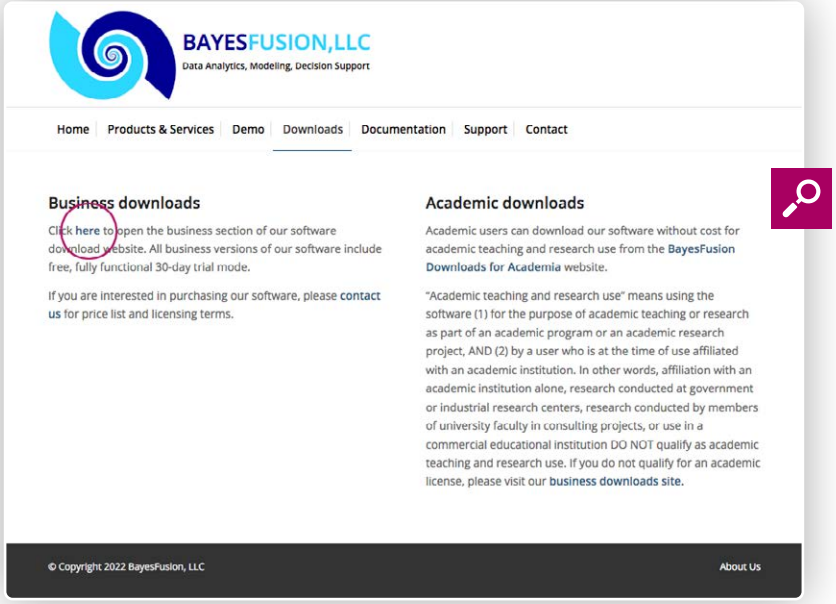
Specifiek biedt het een grafische gebruikersomgeving (GUI) voor grafische modellen zoals Bayesian netwerken.

Een Bayesian Belief Network is een datastructuur die gebruikt wordt om kansverdelingen te modelleren, om zo de waarschijnlijkheid van het optreden van een gekozen gebeurtenis te kunnen voorspellen.
Het programma GeNie dient ertoe om dit soort modellen grafisch te ontwikkelen.

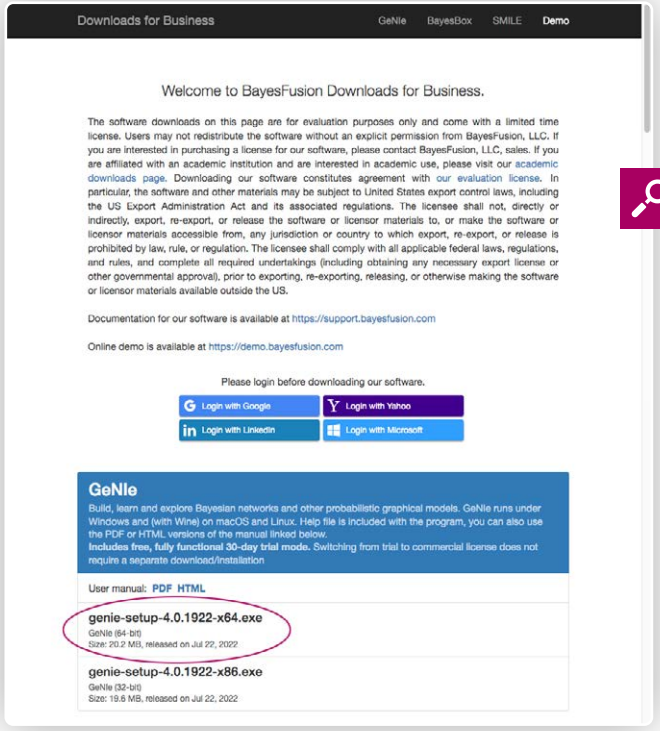
Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Hoe installeer je GeNIe?

Ga naar bayesfusion.com/downloads.
Klik op **'here'** onder het kopje Business downloads.

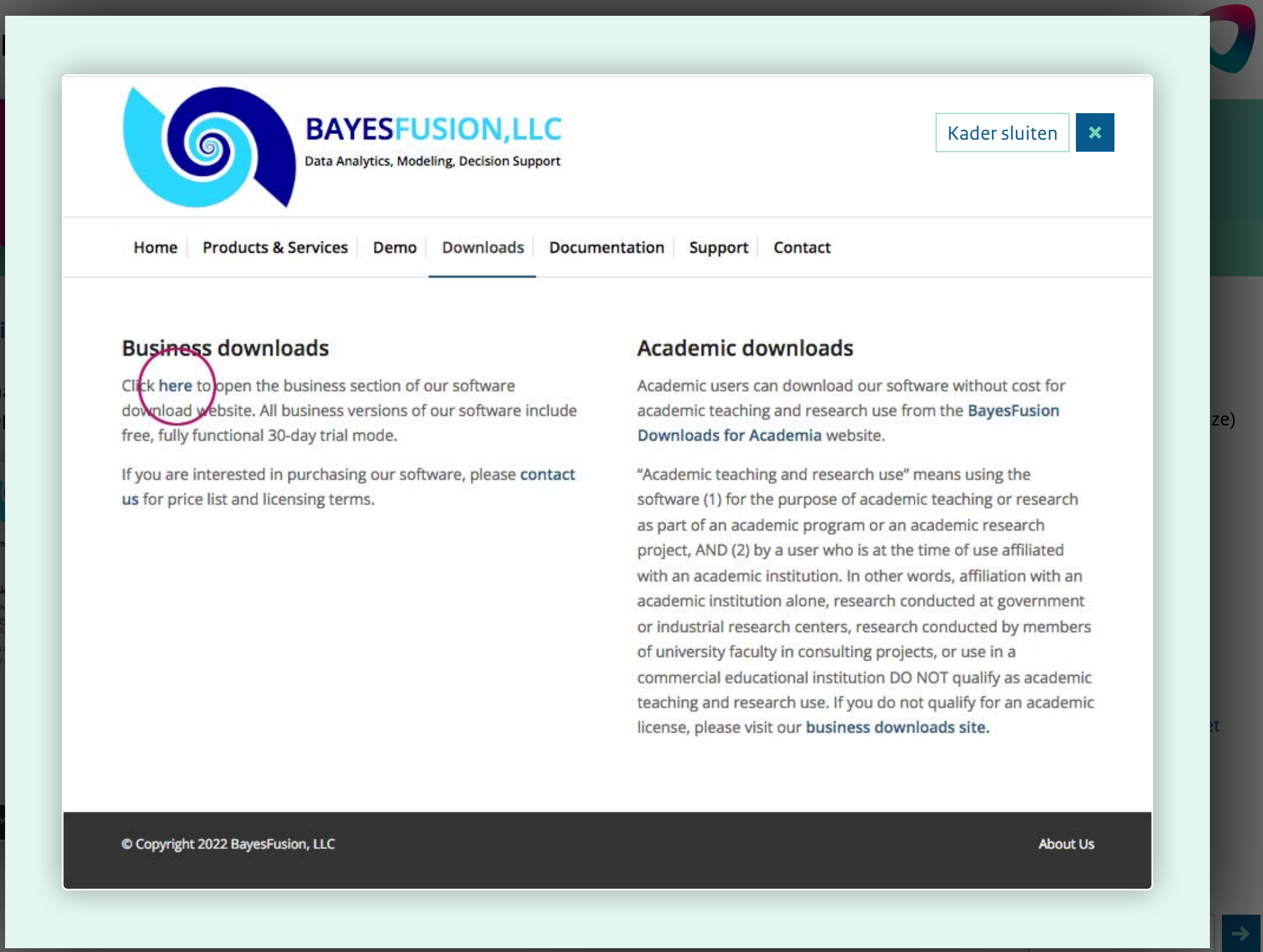


Scroll naar beneden totdat je bij het **kopje GeNIe** bent.
Klik op **genie-setup** om het programma te downloaden. (**64- bit** is de beste keuze)



Let op: Het aanmaken van een account is vereist voordat je het programma kan downloaden.

Bouw je eerste BBN


BAYESFUSION,LLC
Data Analytics, Modeling, Decision Support
Kader sluiten
Home
Products & Services
Demo
Downloads
Documentation
Support
Contact
Business downloads
Click here to open the business section of our software download website. All business versions of our software include free, fully functional 30-day trial mode.
If you are interested in purchasing our software, please contact us for price list and licensing terms.
Academic downloads
Academic users can download our software without cost for academic teaching and research use from the BayesFusion Downloads for Academia website.
"Academic teaching and research use" means using the software (1) for the purpose of academic teaching or research as part of an academic program or an academic research project, AND (2) by a user who is at the time of use affiliated with an academic institution. In other words, affiliation with an academic institution alone, research conducted at government or industrial research centers, research conducted by members of university faculty in consulting projects, or use in a commercial educational institution DO NOT qualify as academic teaching and research use. If you do not qualify for an academic license, please visit our business downloads site.
© Copyright 2022 BayesFusion, LLC
About Us

Aan de

Hoe installe

Ga naar baye

Klik op **'here'**

ste keuze)

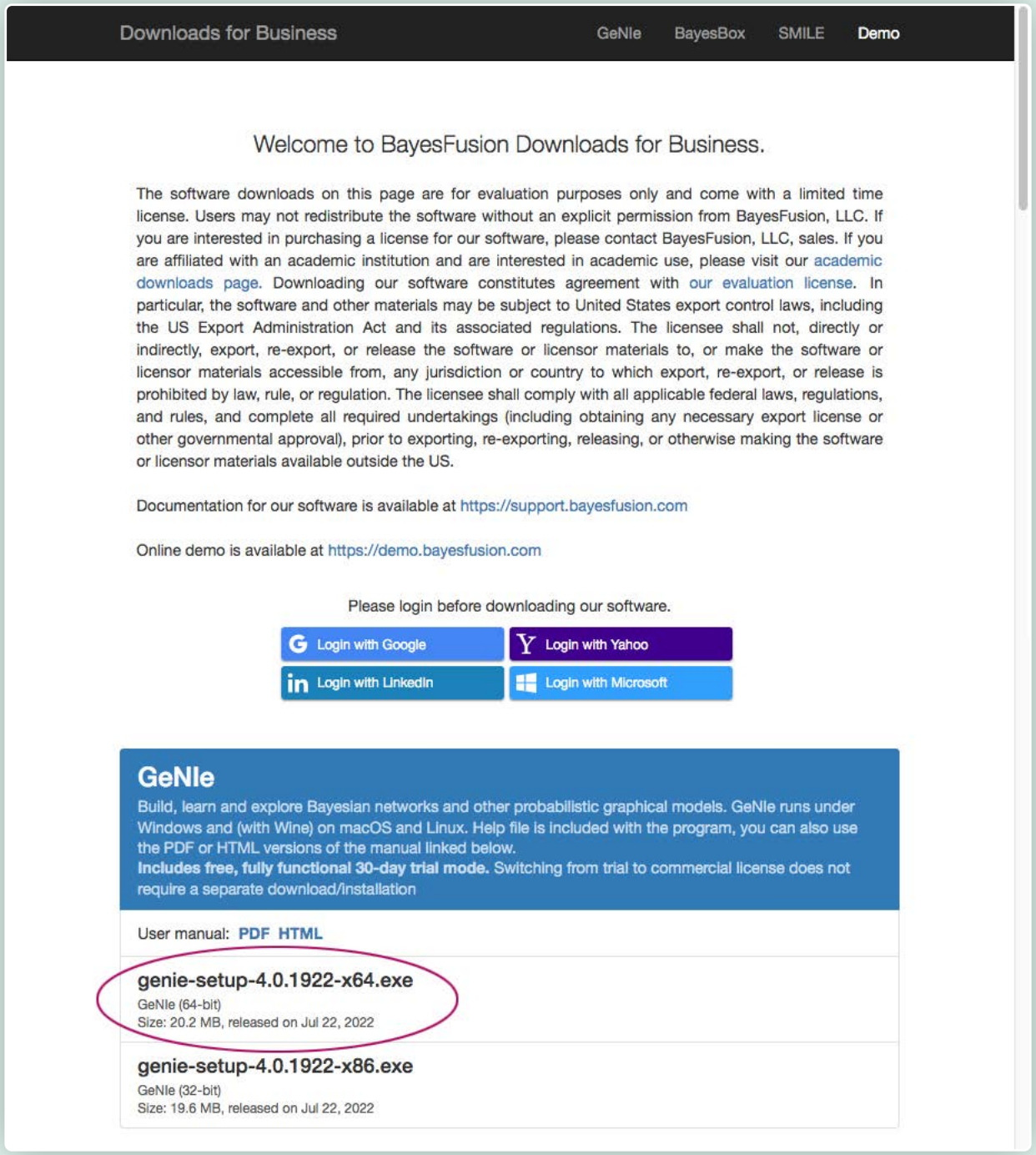
van een

dat je het

loaden.

e BBN

Kader sluiten



Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Nu GeNIe is geïnstalleerd, is het tijd om een Bayesian Belief Network (BNN) te bouwen. Wij nemen je stap voor stap mee in het proces en laten aan de hand van een eenvoudig voorbeeld zien hoe een BBN tot stand komt. Zodoende behandelen we in de komende 7 stappen de essentiële functies van GeNIe. Voor meer informatie over het gebruik van GeNIe verwijzen we naar de uitstekende ingebouwde handleiding.

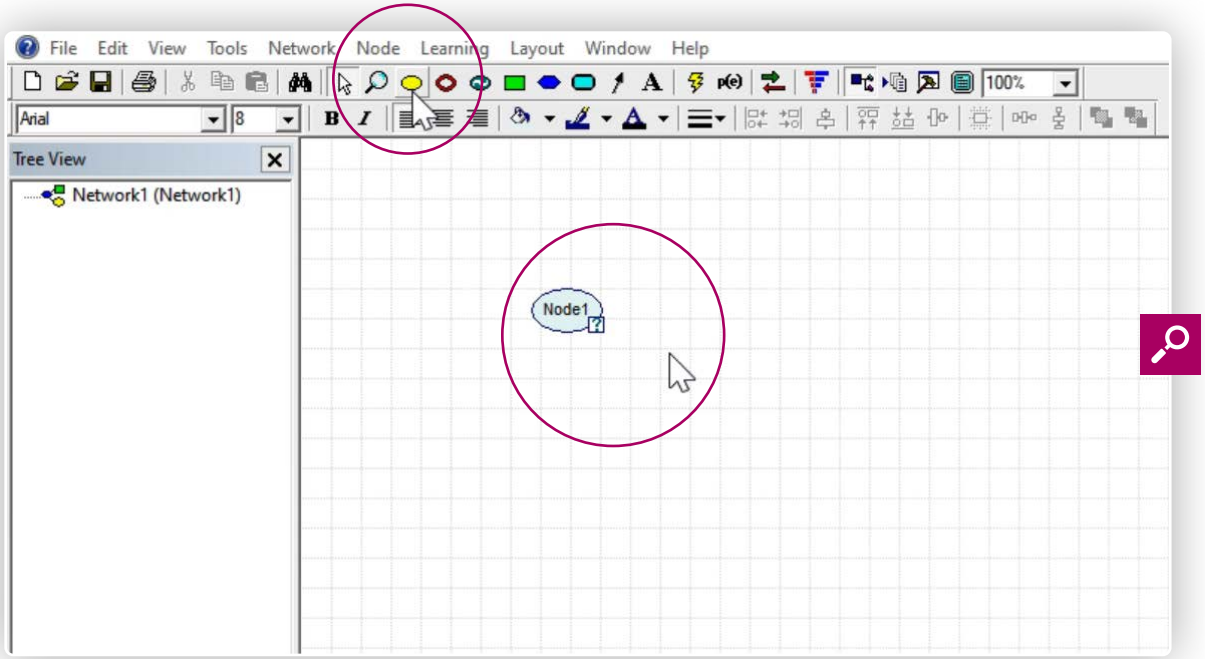
In deze tutorial zal het voorbeeld een dreigingsscenario betreffen. Hierbij wordt gekeken naar actor, technische expertise en aanvalstype/aanvalsvector .

Het creëren van nodes

Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Het creëren van nodes

De eerste stap betreft het creëren van de absolute basis van het netwerk: de nodes.
Nodes representeren een variabele die je mee wilt nemen in het berekenen van een cyberrisico, bijvoorbeeld een bepaalde cyber actor of aanvalstype.



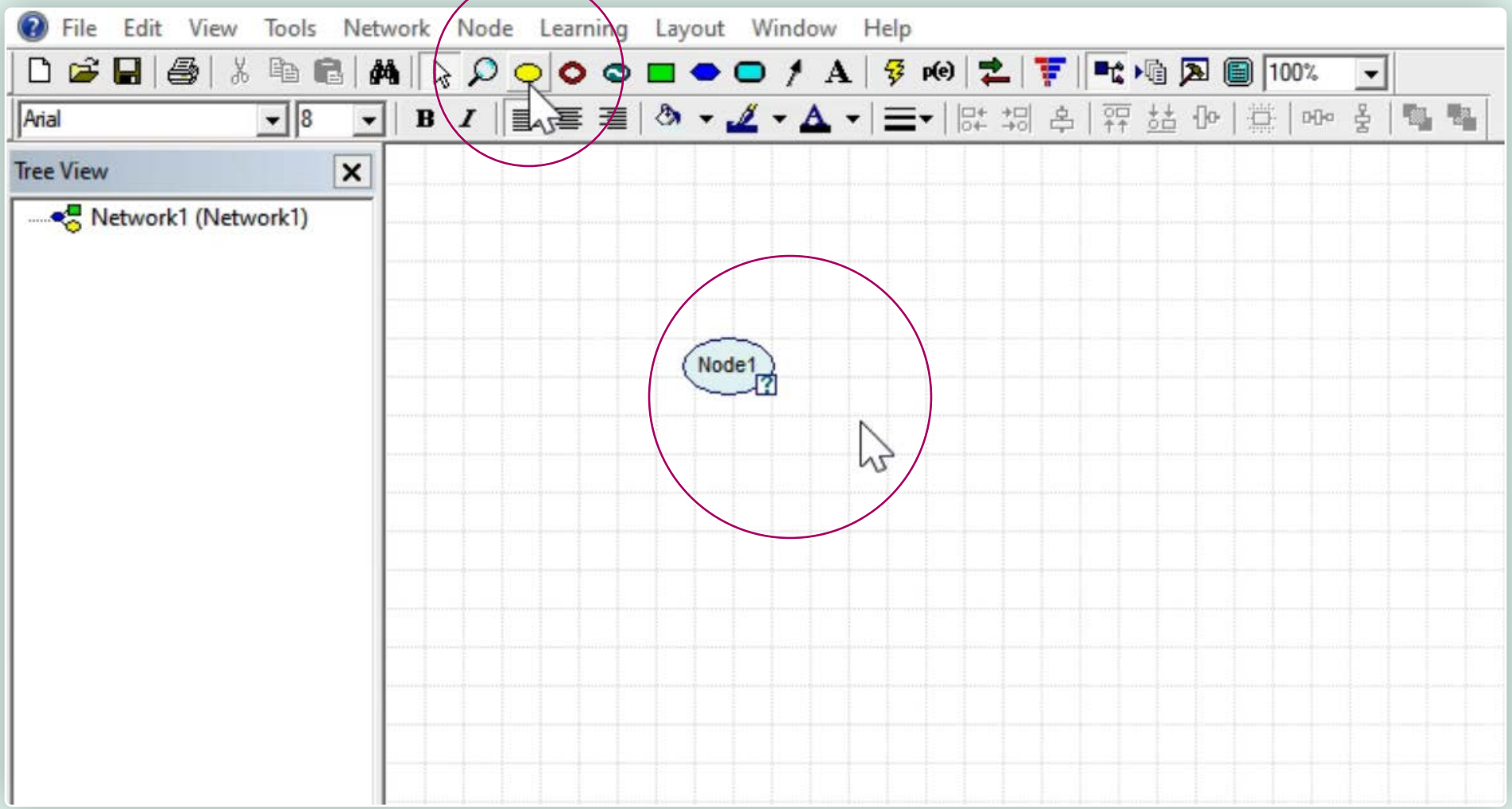
1.1 Creëer een 'Chance node'

Om een 'Chance node' aan te maken klik je op de gele ovaal in de toolbar en vervolgens op het canvas (graph view).

Aan de slag met het kwantificeren van cyberrisico's

Terug naar navigatie figuur

Kader sluiten

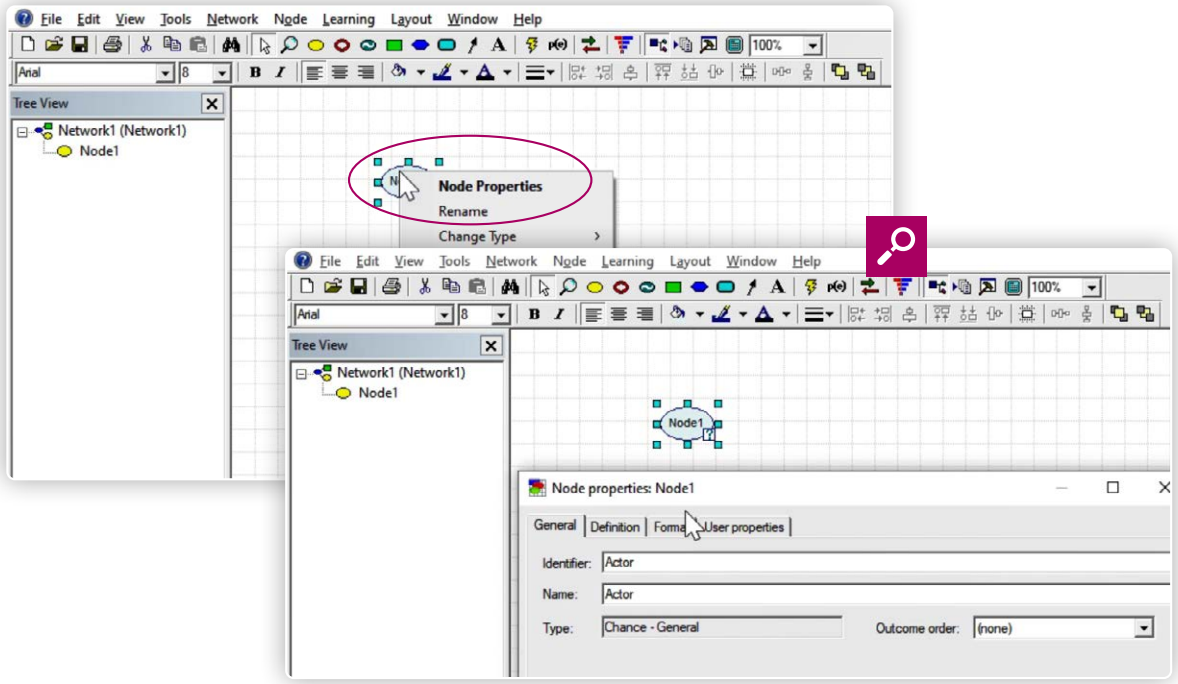


Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Het creëren van nodes

1.2 Geef een naam aan de node

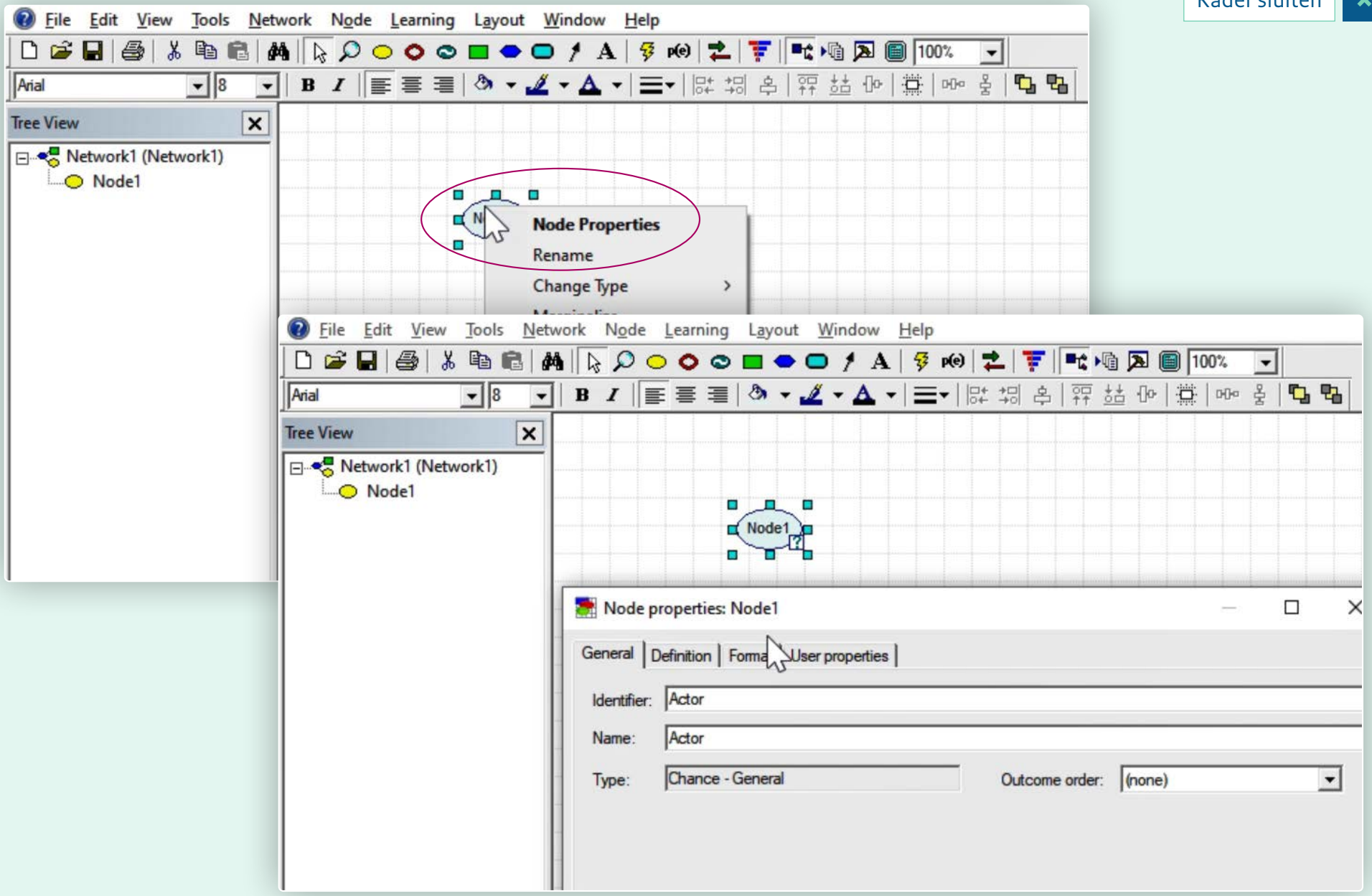
Klik rechts op de node en selecteer 'Node Properties'. Hier wordt de node een identifier en een name gegeven. Hoewel deze van elkaar kunnen verschillen, en enkel de identifier uniek hoeft te zijn, is onze suggestie om voor identifier en name dezelfde waarde in te vullen. In dit geval willen wij een actor node maken, dus vullen wij bij zowel identifier en name 'Actor' in.



Let op: de waarde moet beginnen met een letter en mag enkel bestaan uit letters, cijfers en underscores.

Terug naar

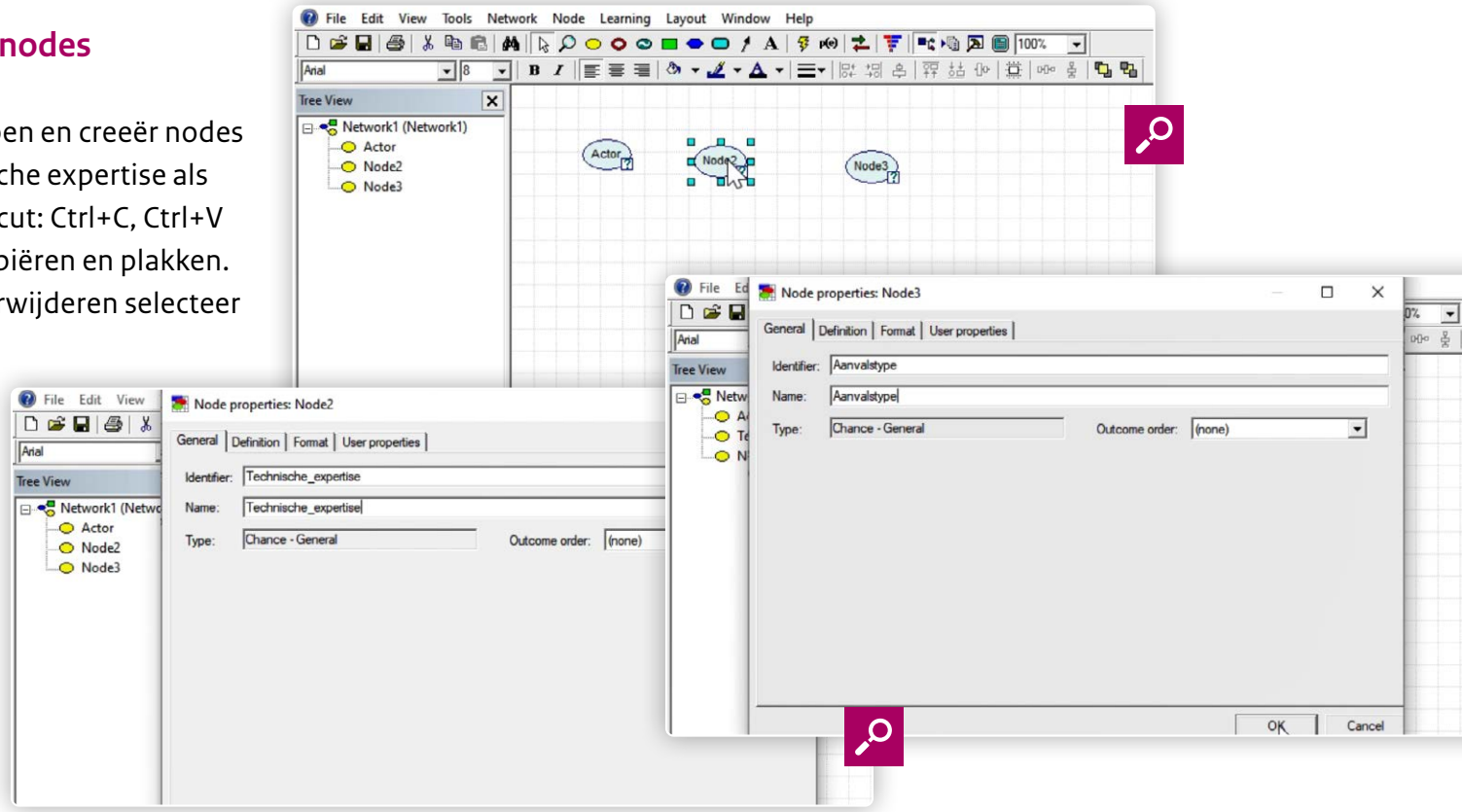
Kader sluiten



Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Het creëren van nodes

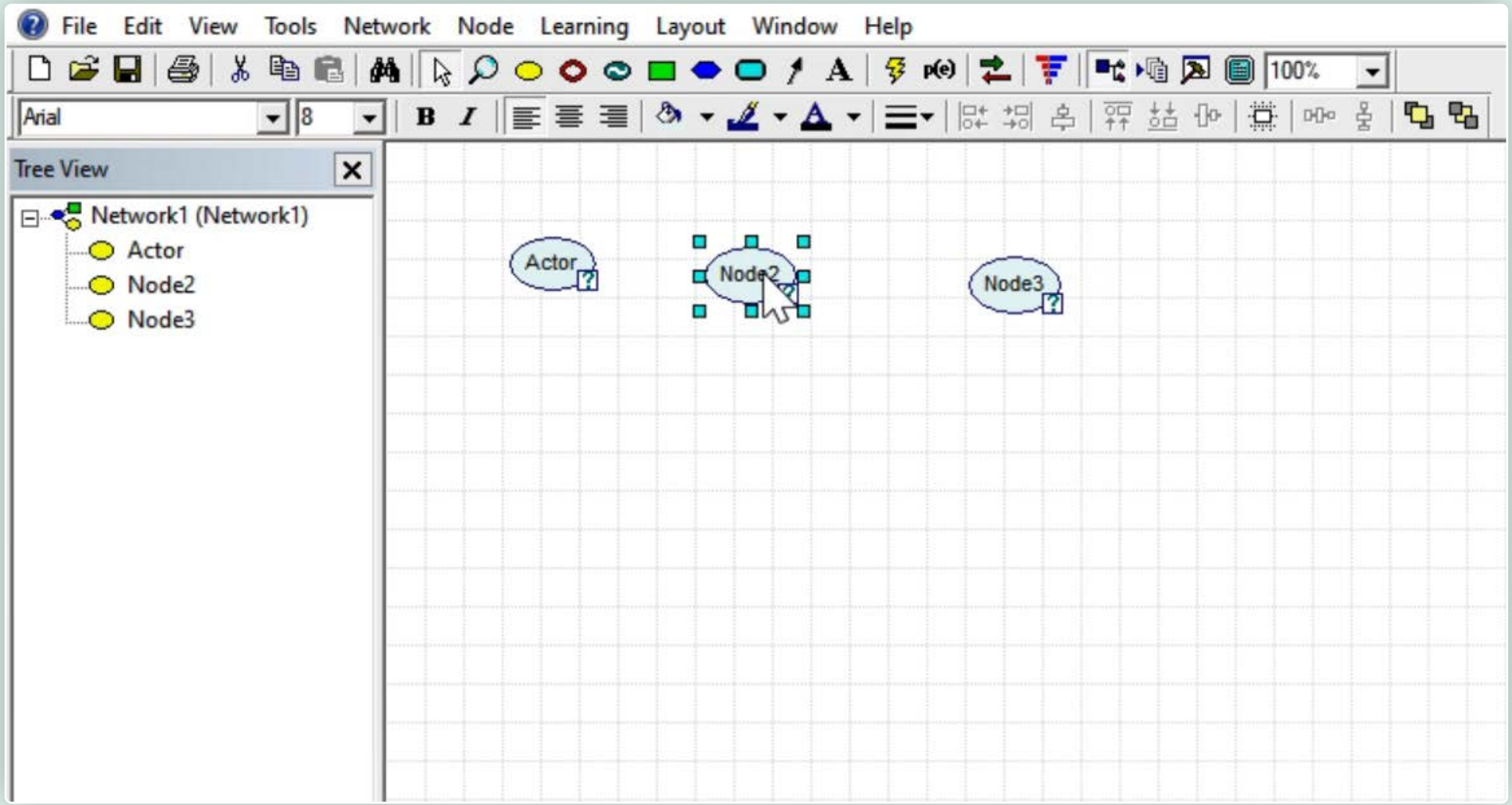
Herhaal deze stappen en creeër nodes voor zowel technische expertise als aanvalstype. Shortcut: Ctrl+C, Ctrl+V om een node te kopiëren en plakken. Om een node te verwijderen selecteer je deze + Del.



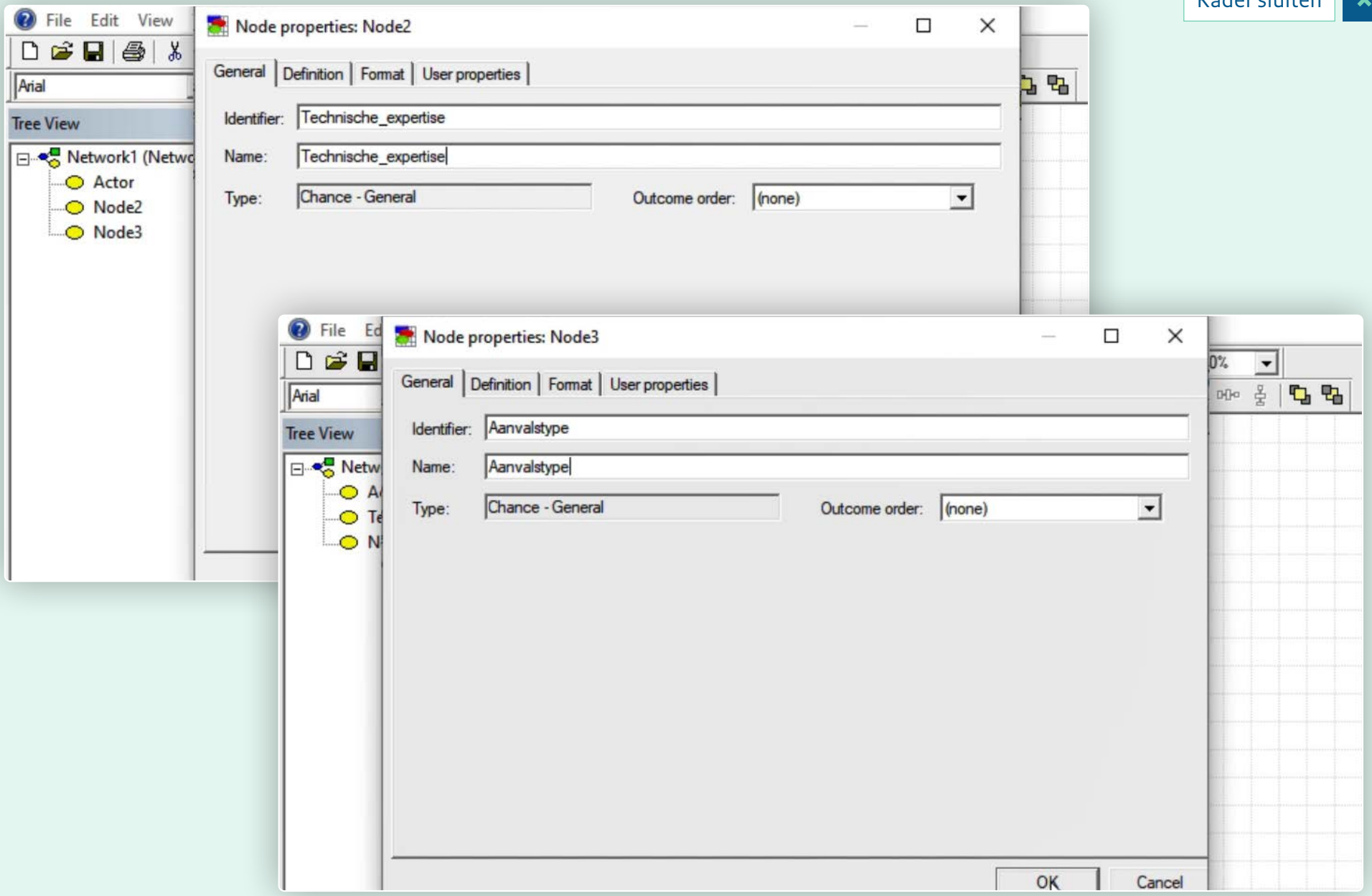
Aan de slag met het kwantificeren van cyberrisico's

Terug naar navigatie figuur

Kader sluiten



Kader sluiten

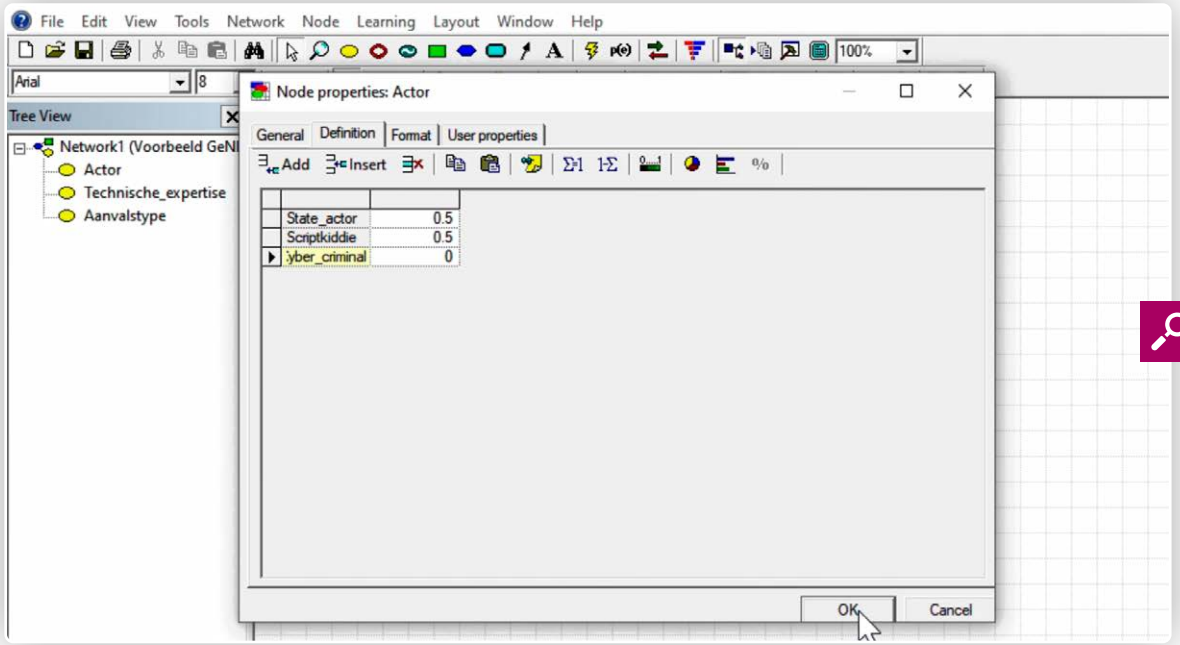


Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Het creëren van nodes

1.3 'States' toevoegen aan de node

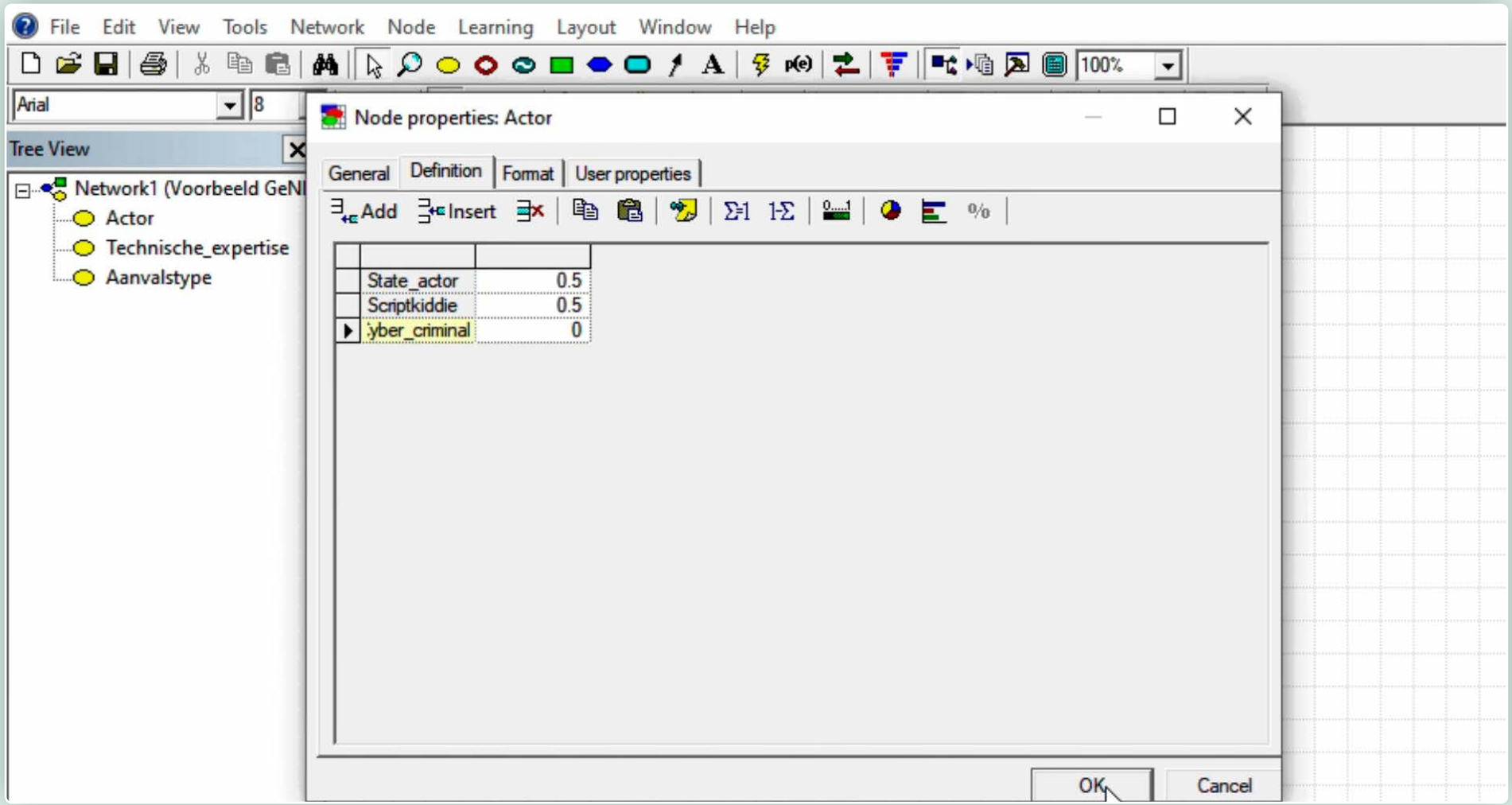
De volgende stap is om states toe te voegen aan de nodes. Klik rechts op een node (ter illustratie: de node 'Actor') en selecteer 'Node Properties'.



Navigeer vervolgens naar 'Definition'. Hier kan je de default waarden (state0, state1) vervangen door eigen states en eventueel nieuwe toevoegen. De actor node bestaat uit de volgende drie states: state actor, scriptkiddie, en cyber criminal. Om een extra state toe te voegen klik je op 'add' of 'insert'. Dubbelklik vervolgens op de te veranderen state en wijzig de naam. Ook hier geldt: enkel letters, cijfers en underscores.

Aan de slag met het kwantificeren van cyberrisico's

Kader sluiten

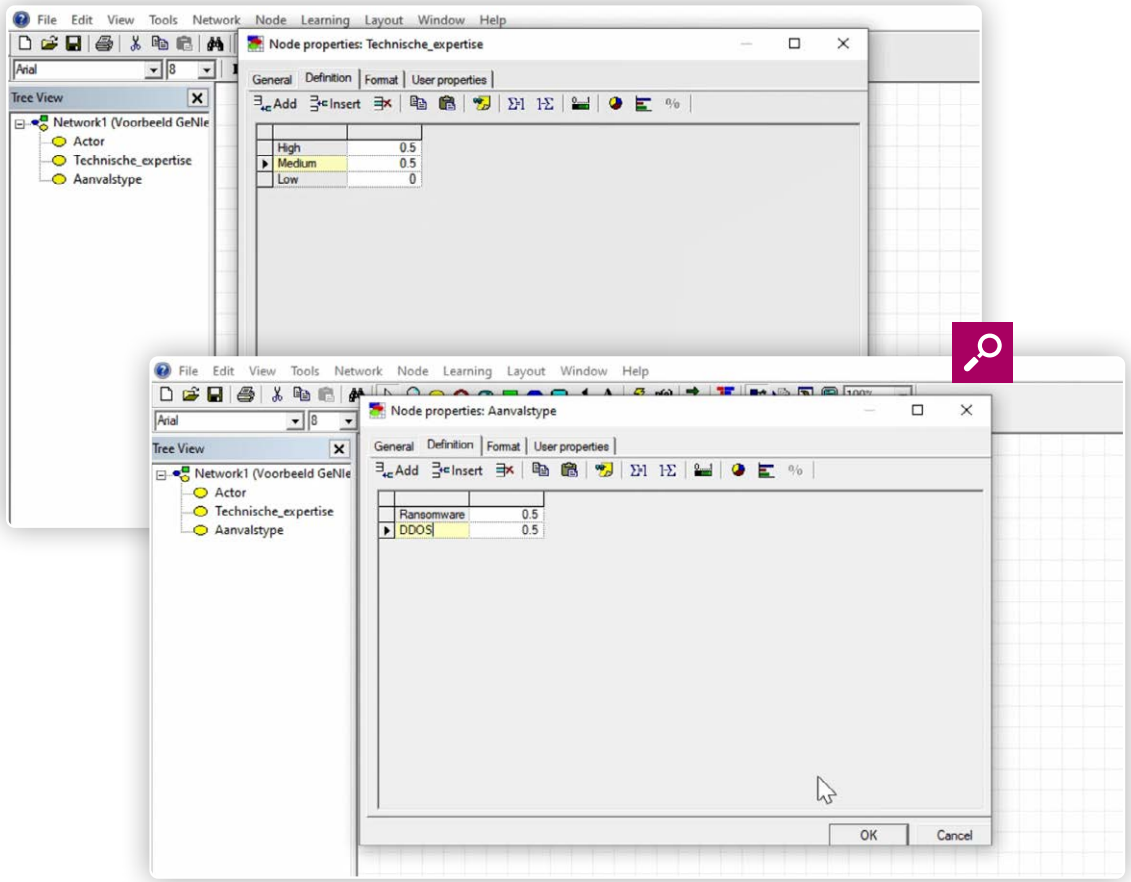


Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

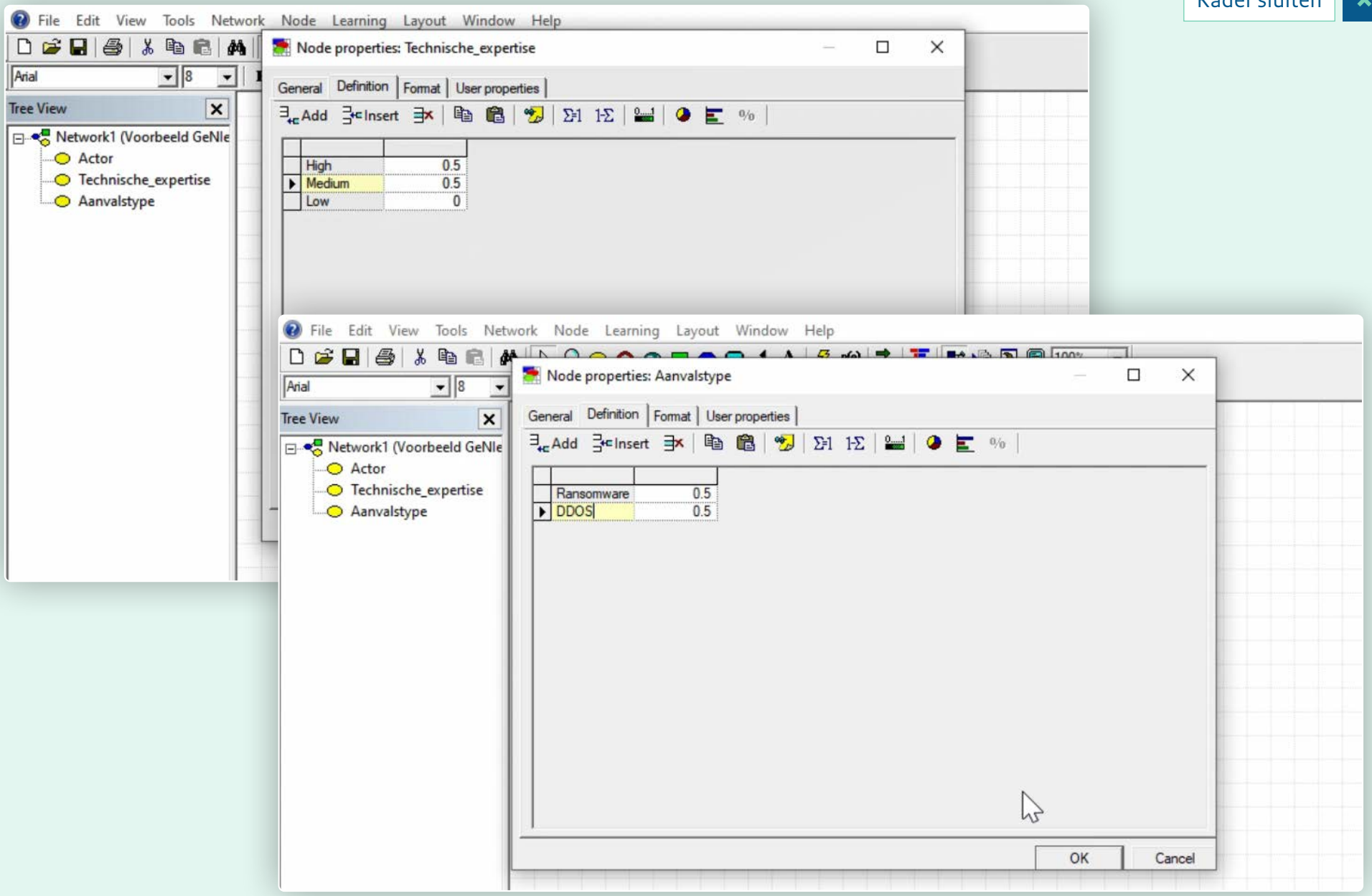
Het creëren van nodes

Herhaal de eerdere stap voor zowel de technische expertise als de aanvalstype node. De nodes bestaan uit de volgende states:

- Technische expertise: High/ medium/ low.
- Aanvalstype: Ransomware/ DDoS.



Kader sluiten

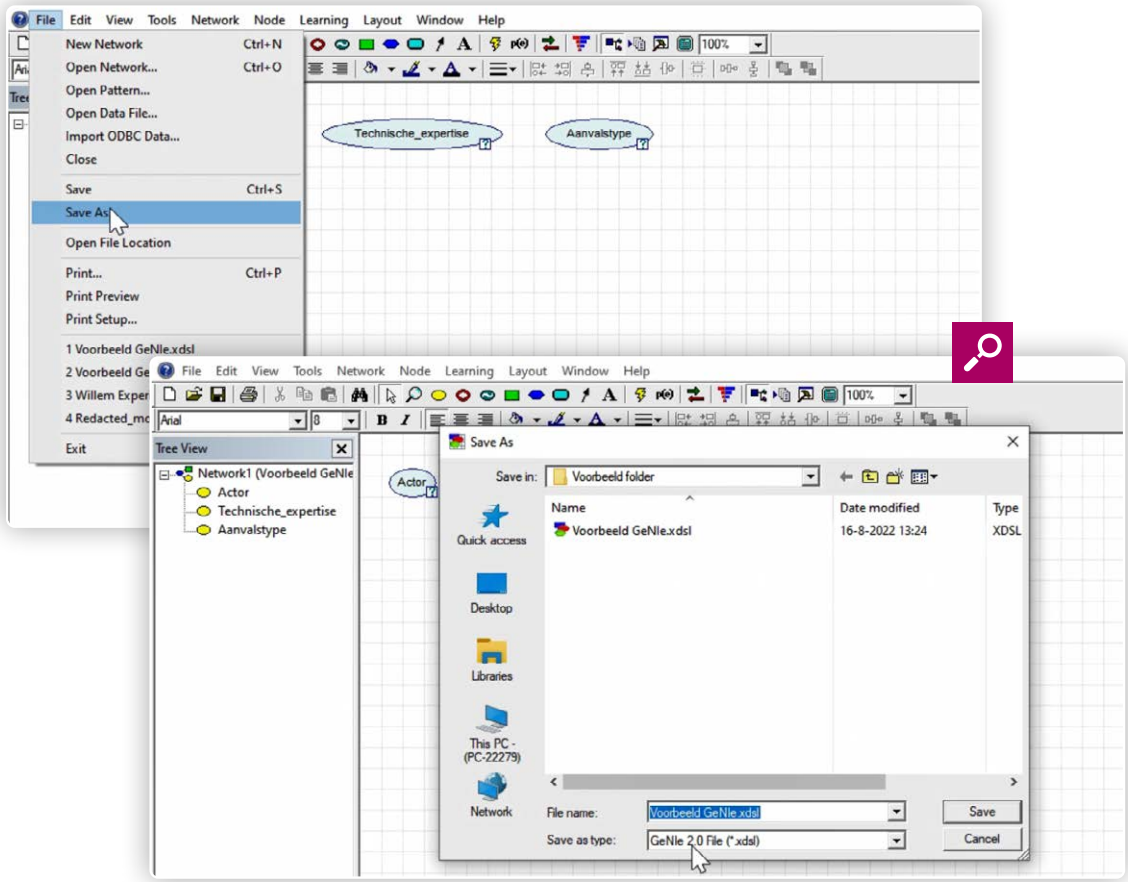


Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

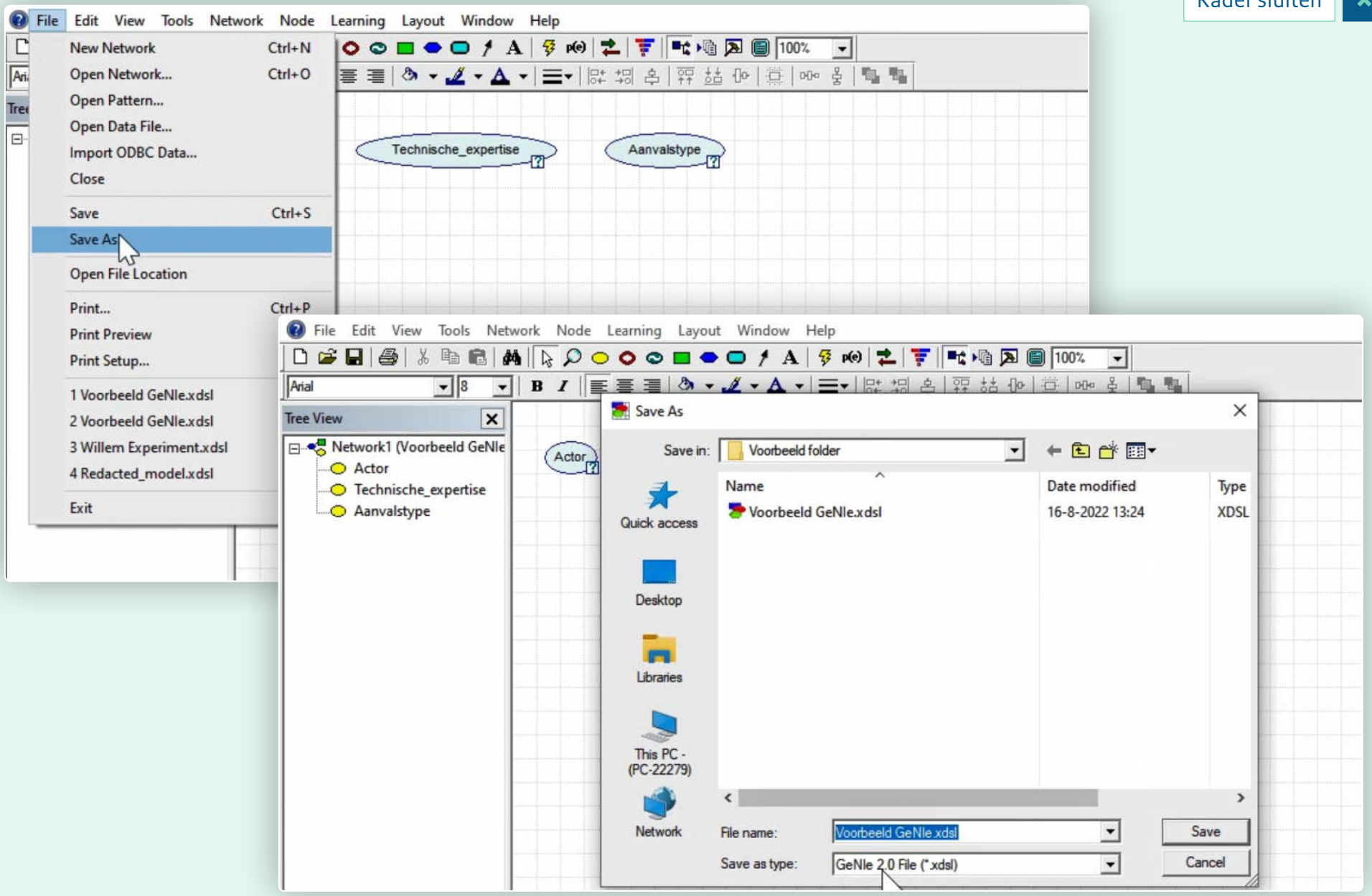
Netwerk opslaan/openen

2.1 Opslaan

Klik linksboven op 'File', en vervolgens op 'Save As'. Bestanden worden standaard opgeslagen als GeNIe 2.0 File (*.xdsl), met volledige ondersteuning voor alle features van GeNIe. Voor compatibiliteit met andere programma's zijn er desgewenst enkele andere opties beschikbaar.



Kader sluiten

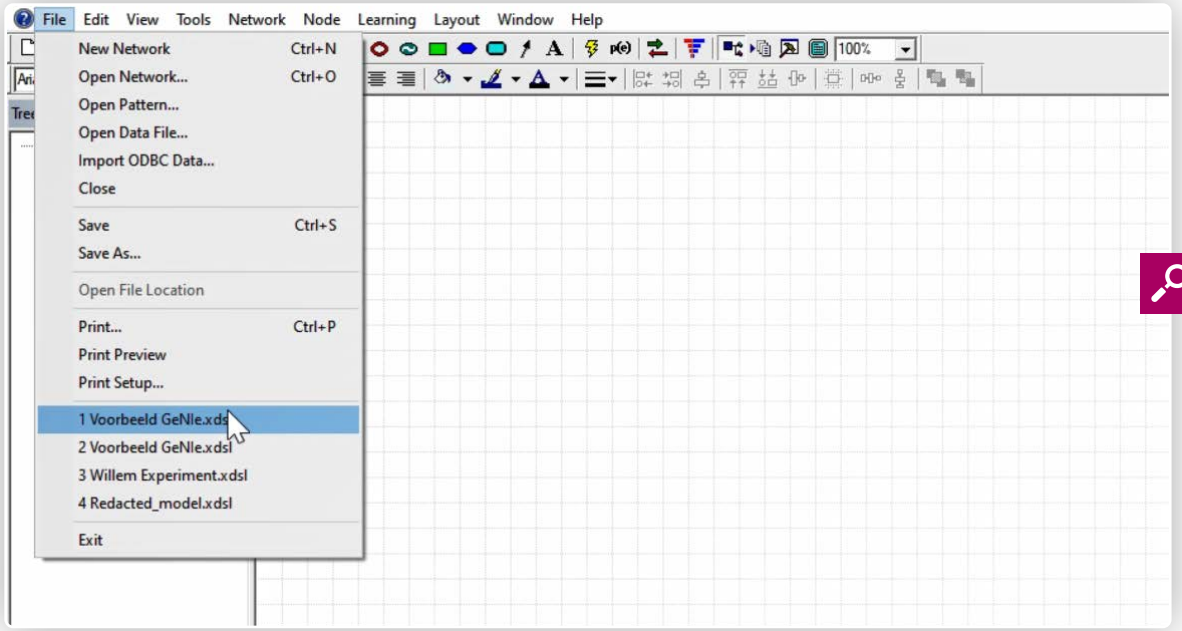


Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Netwerk opslaan/openen

2.2 Openen

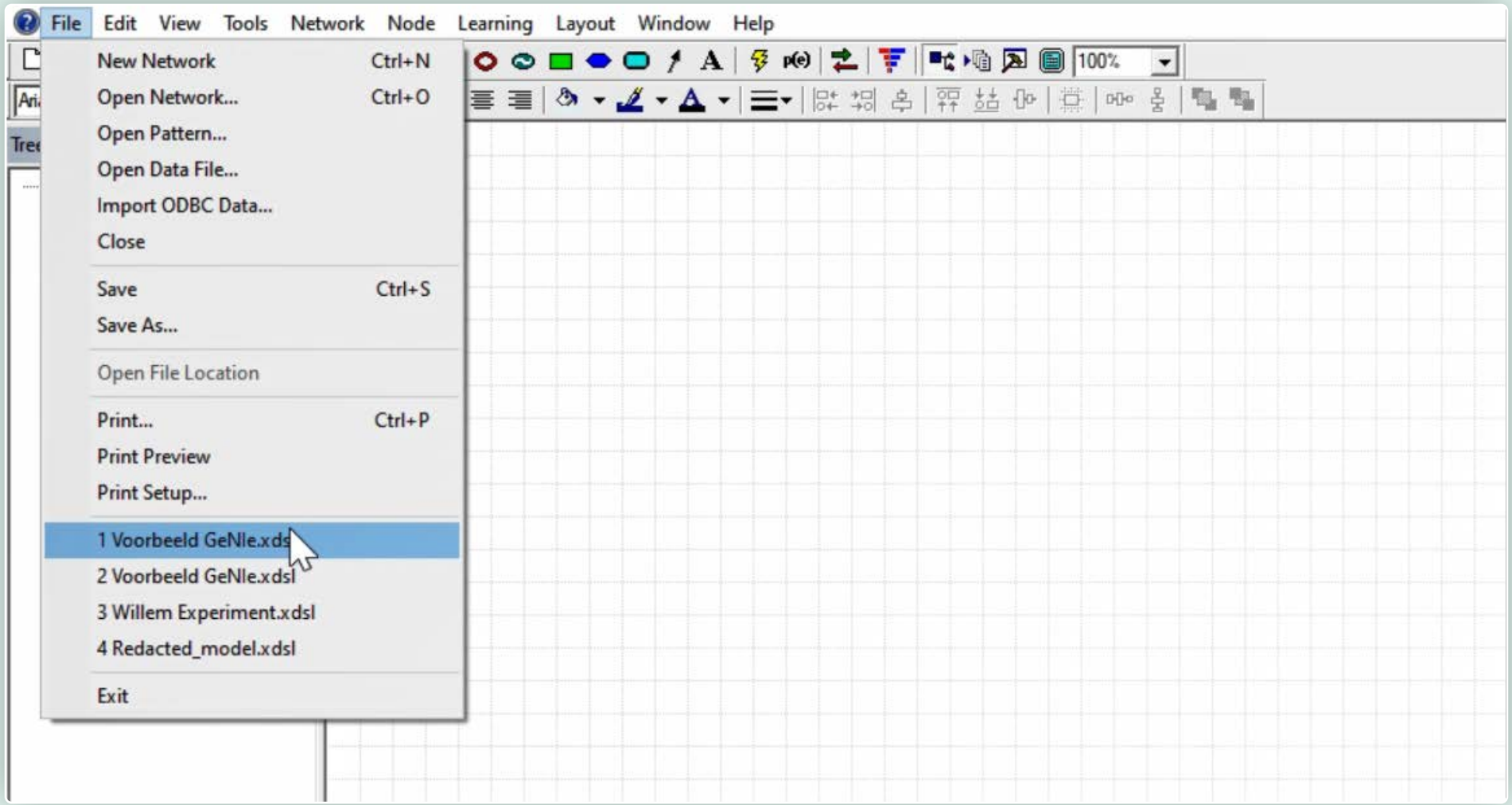
Wanneer je na een onderbreking je werk wil hervatten kun je een eerder opgeslagen bestand openen. Onder 'File' staan de 8 meest recente bestanden, kies anders voor 'Open Network' (ctrl+O). (Alternatieven zijn: .xdsl bestand in explorer openen met GeNIe (.xdsl associëren met GeNIe, of Open with), of drag and drop van explorer in GeNIe.



Aan de slag met het kwantificeren van cyberrisico's

Terug naar navigatie figuur

Kader sluiten

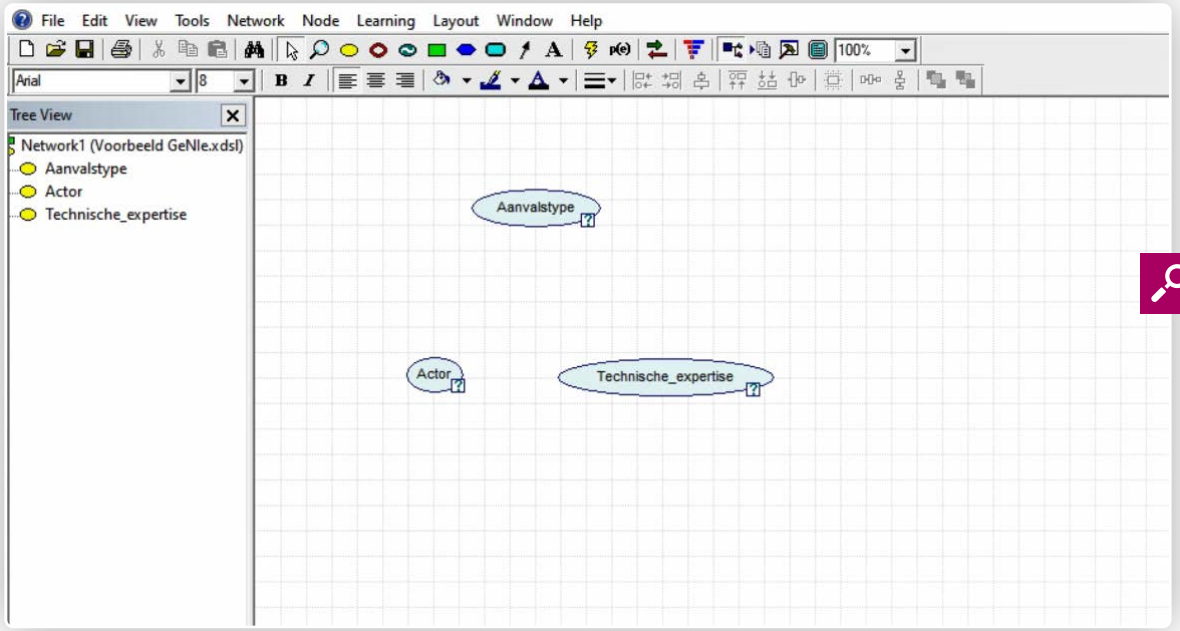


Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Nodes verbinden

3.1 Positionering

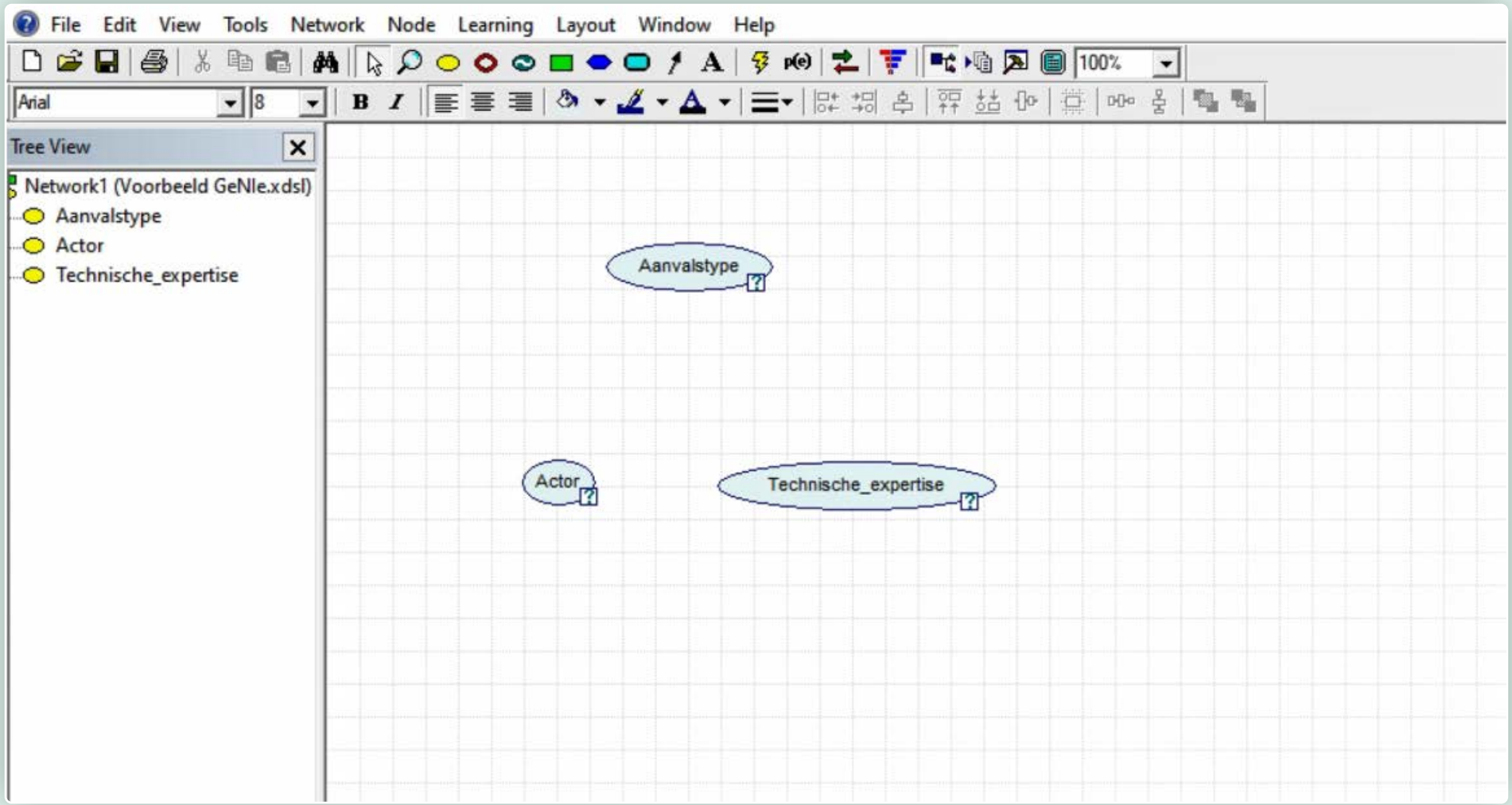
Voor het overzicht is het handig om de nodes op een logische plaats in het netwerk te positioneren. In dit geval nemen wij aan dat zowel de actor als technische expertise node dienen als input voor de aanvalstype node en plaatsen deze daarom op gelijke hoogte.
Deze input wordt aangetoond door pijltjes te trekken naar de desbetreffende node waar input voor nodig is. Dit zie je op de volgende slide



Tip: Om een node te verplaatsen klik op een node met je linker muisknop en hou deze vast om te verplaatsen.

Aan de slag met het kwantificeren van cyberrisico's

Kader sluiten



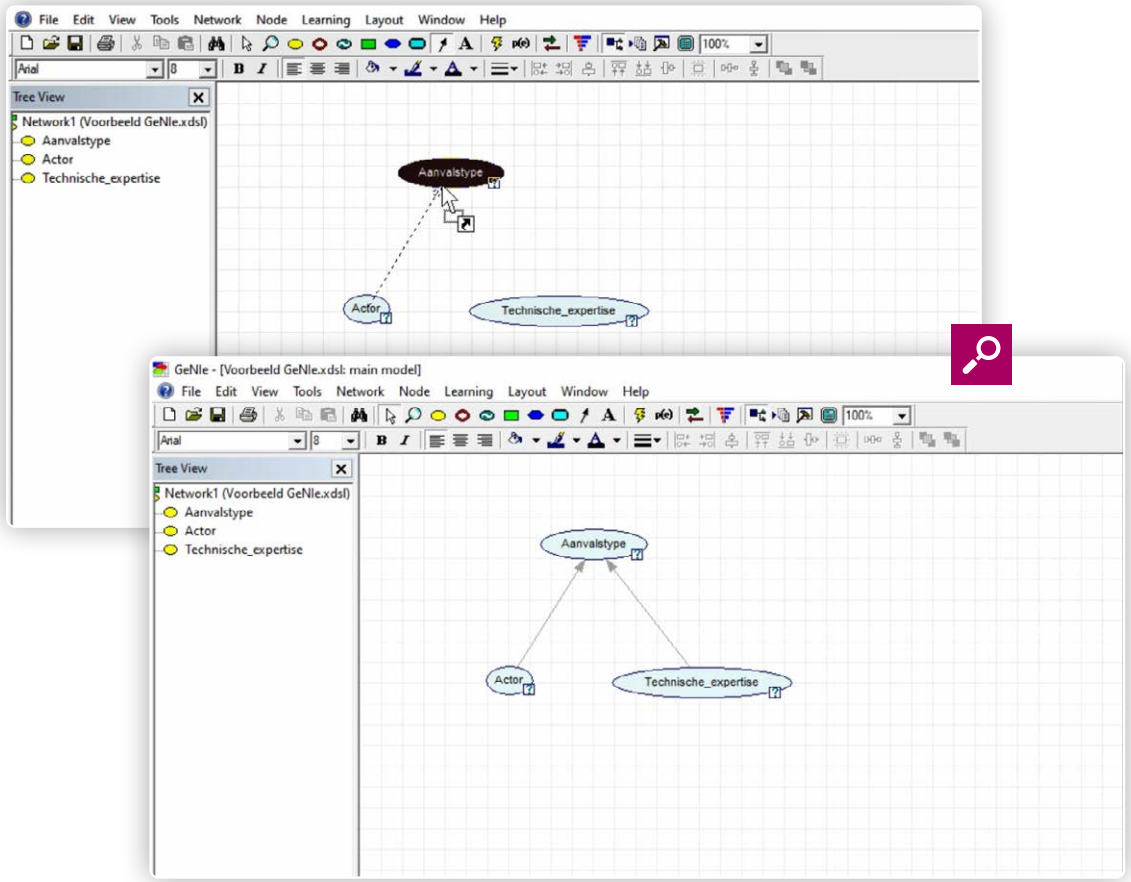
Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Nodes verbinden

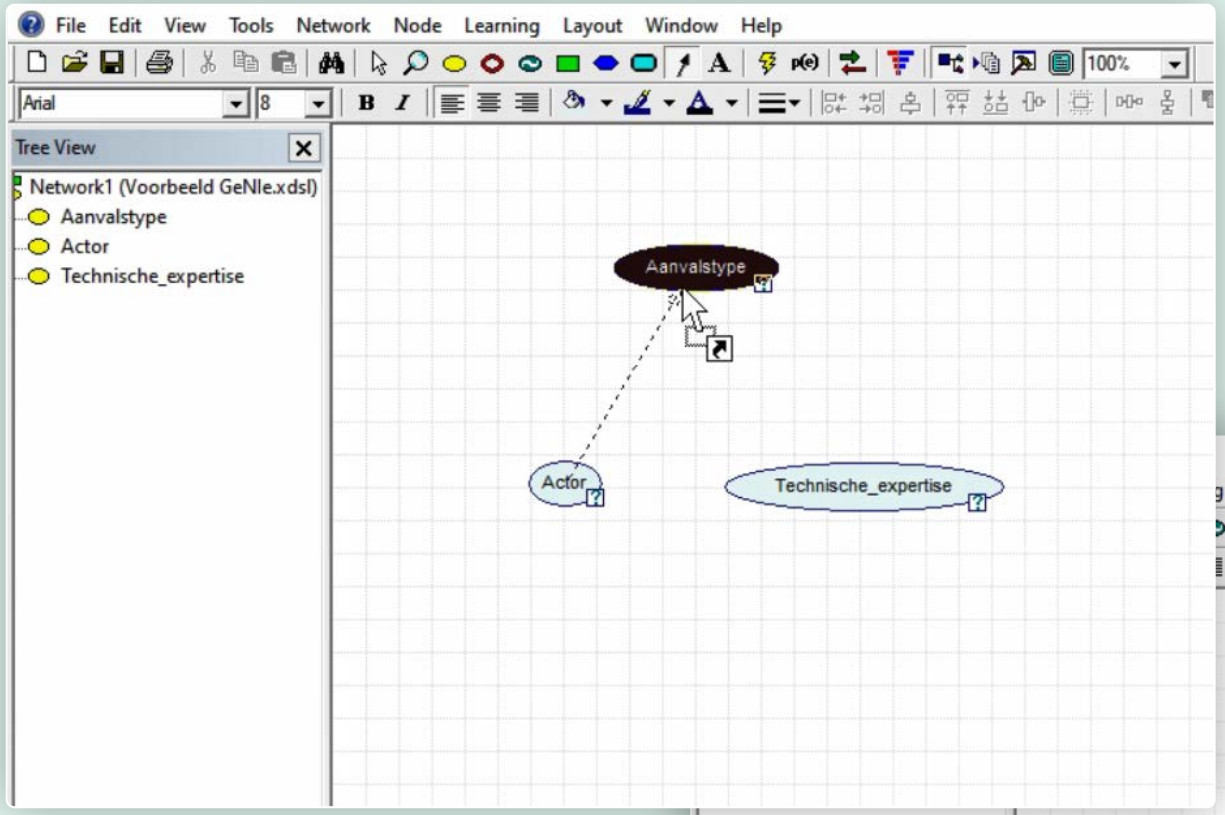
3.2 Verbinden

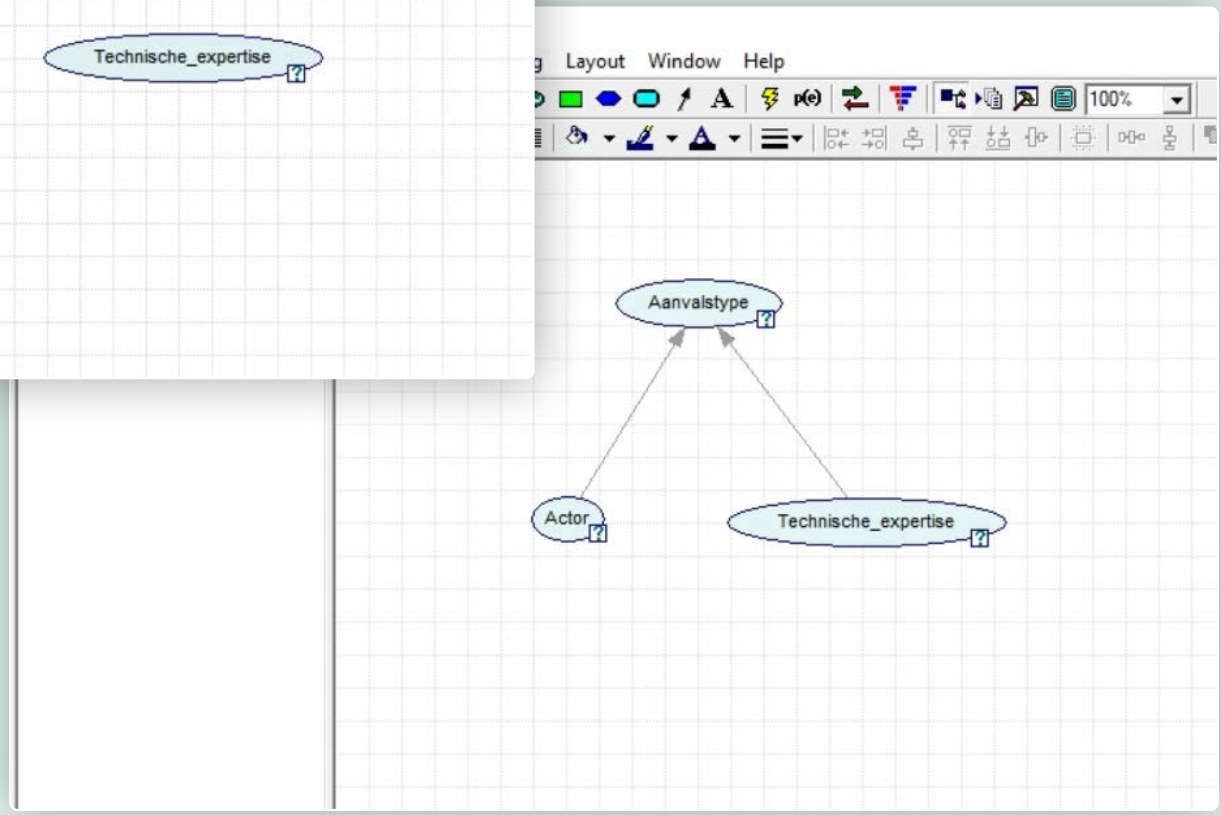
Om nodes te verbinden selecteer je de zwarte pijl in de toolbar (alternatief: Tools ➔ Arc). Vervolgens klik je op de actor node, sleep het pijltje naar de aanvalstype node en laat de cursor los. Herhaal hetzelfde proces voor de technische expertise node naar de aanvalstype node.

Tip: Om een pijltje of ander element te verwijderen, selecteer deze + Del of klik rechts en selecteer 'Delete'



Kader sluiten

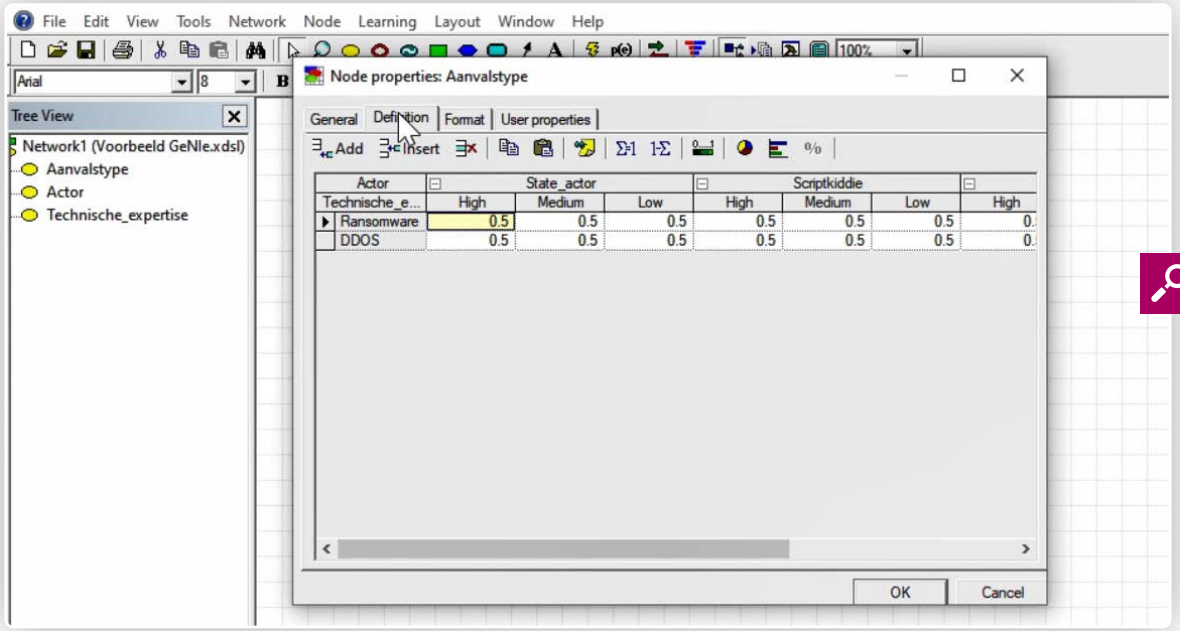




Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Nodes verbinden

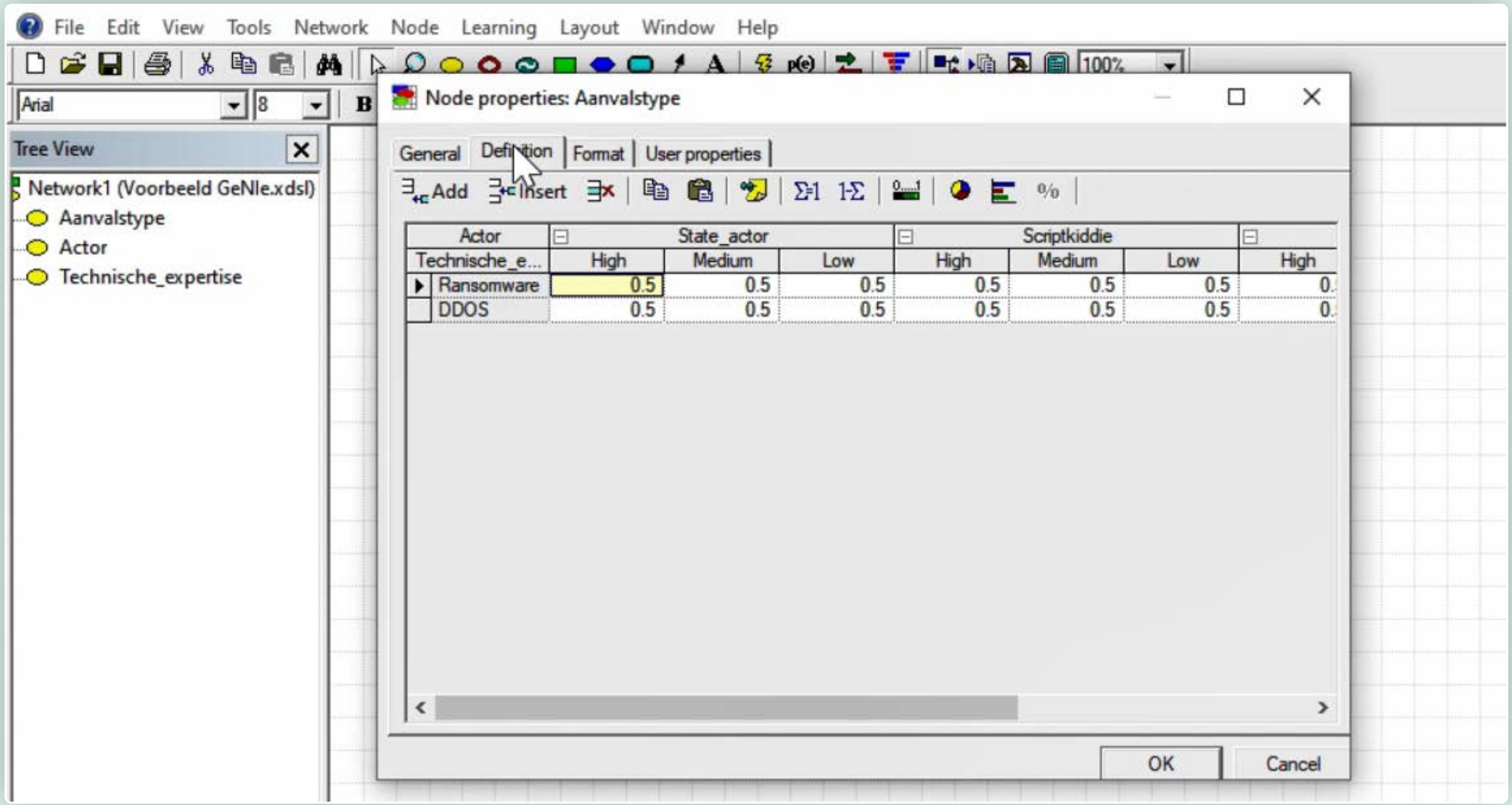
Klik met de rechtermuisknop op de aanvalstype node en selecteer 'Node Properties'. Navigeer naar 'Definition'. Je ziet in deze tabel hoe de onderlinge nodes zich tot elkaar verhouden op basis van de getrokken pijlen.



Aan de slag met het kwantificeren van cyberrisico's

Terug naar navigatie figuur

Kader sluiten



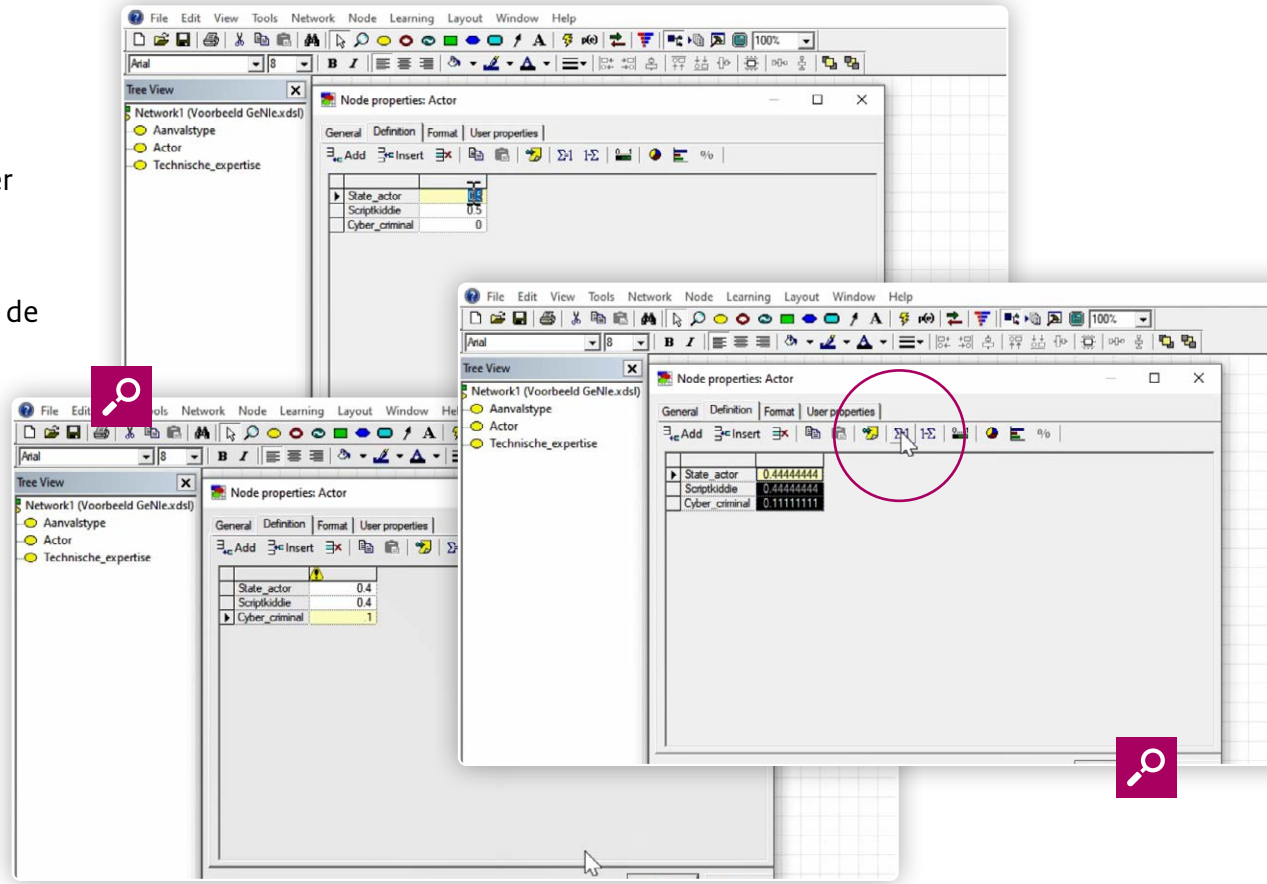
Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Invullen van states

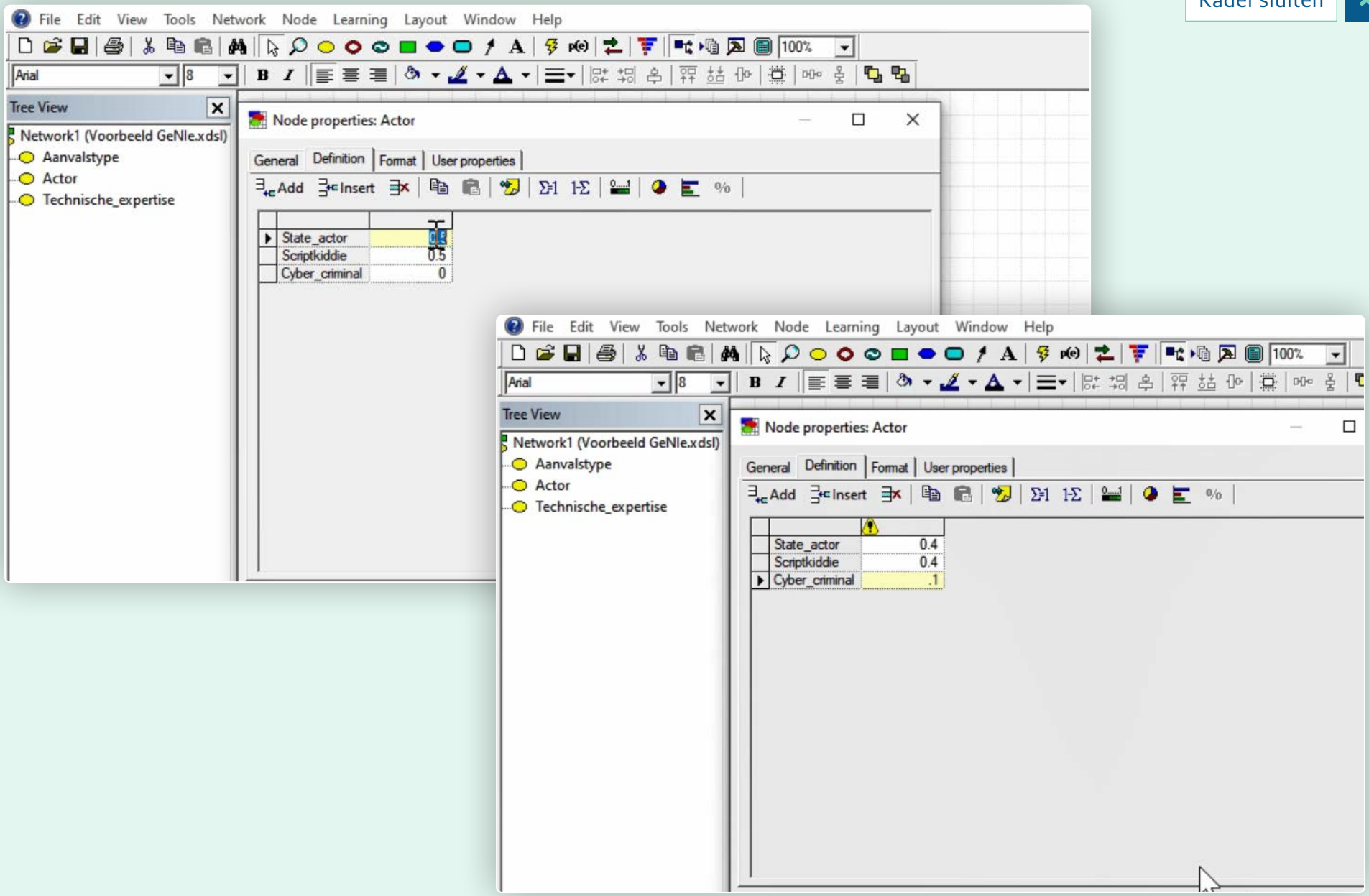
4.1 Waarden van states

Klik rechts op de actor node, selecteer 'Node Properties' en navigeer naar 'Definition'. Hier kan je de relatieve waarden van de states invullen naast de eerder ingevoerde namen van de states. De som van de waarden van de states moet (per kolom) uiteindelijk gelijk zijn aan 1.

Je kan desgewenst werken met grotere of kleinere onge-normaliseerde getallen; het programma biedt de mogelijk-heid om de ingevulde waarden te normaliseren middels de Σ=1 knop in de toolbar.



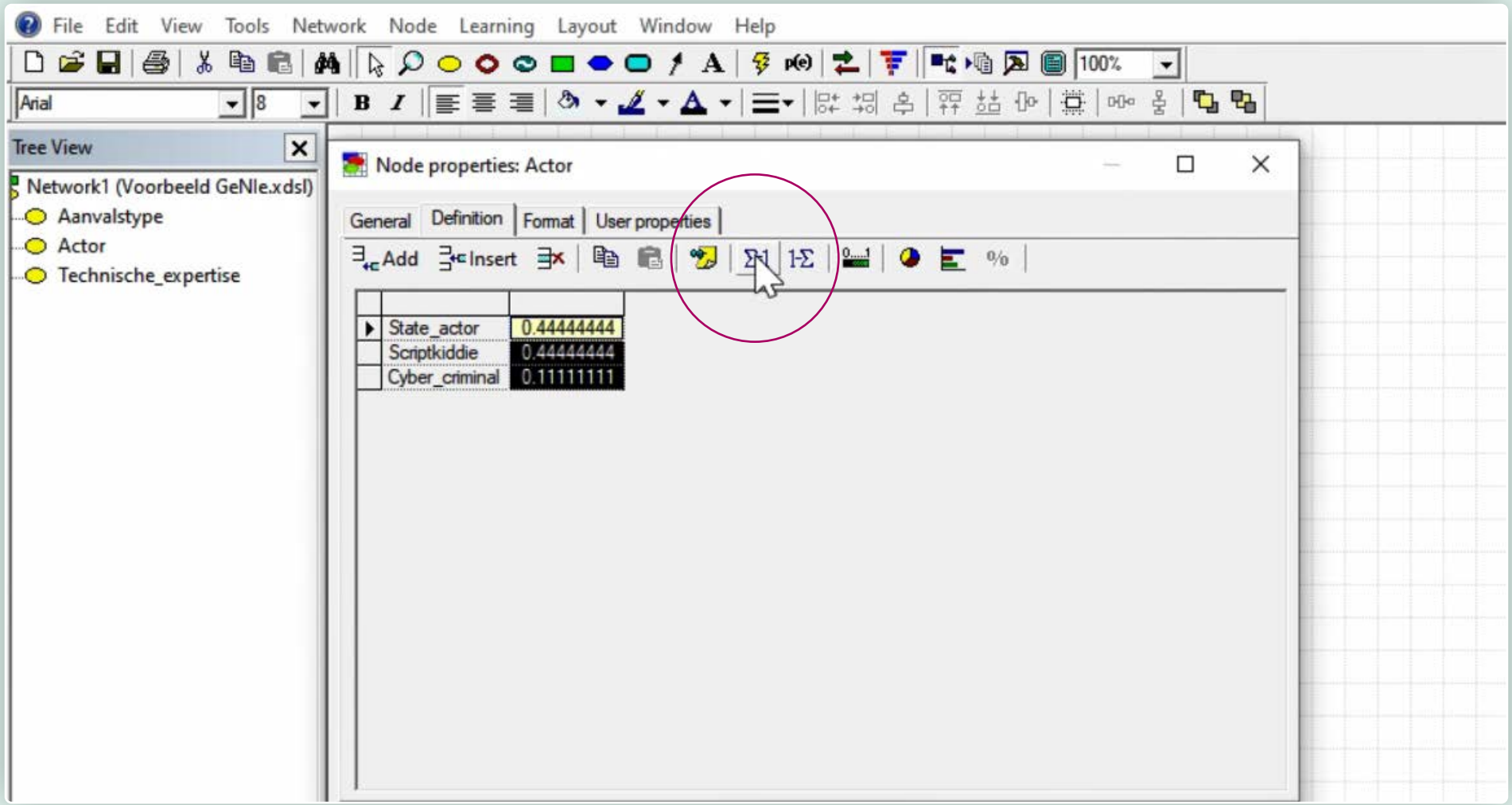
Kader sluiten



Aan de slag met het kwantificeren van cyberrisico's

Terug naar navigatie figuur

Kader sluiten



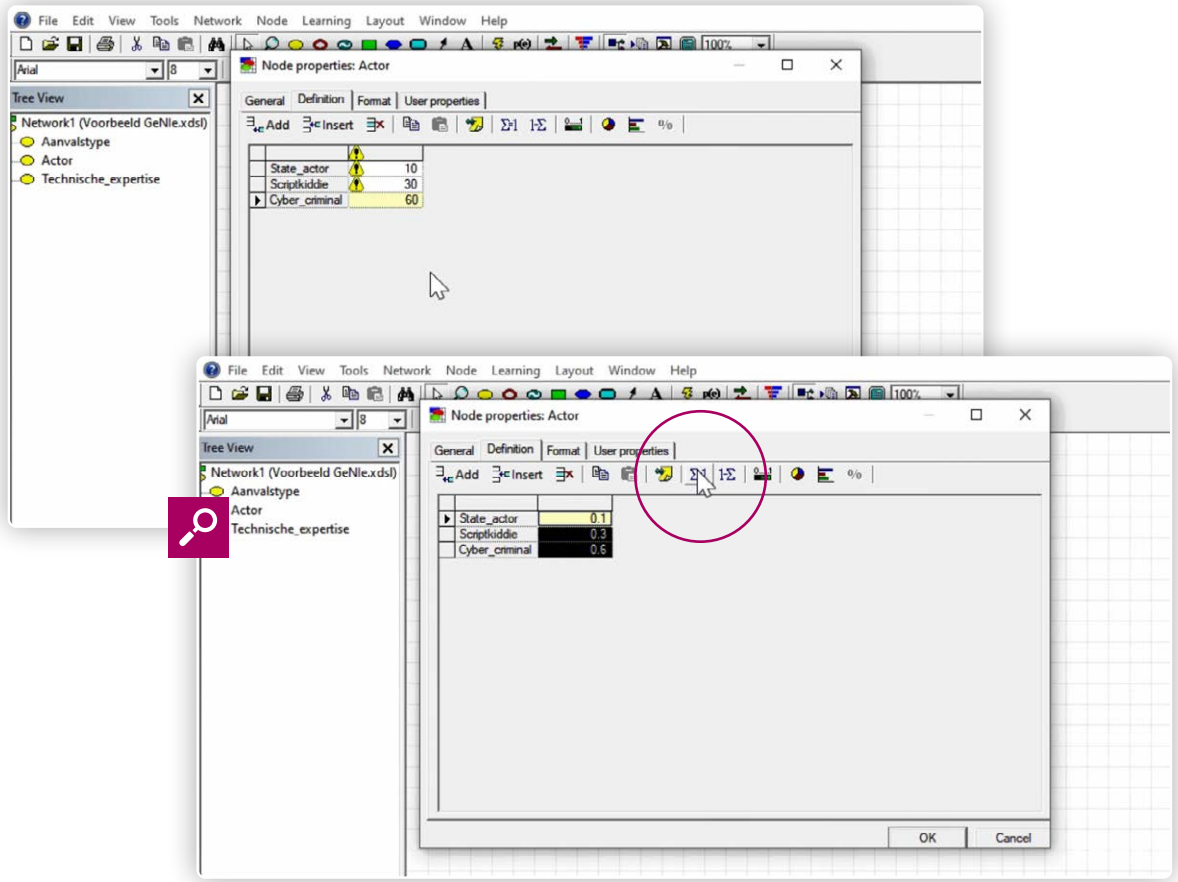
Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Invullen van states

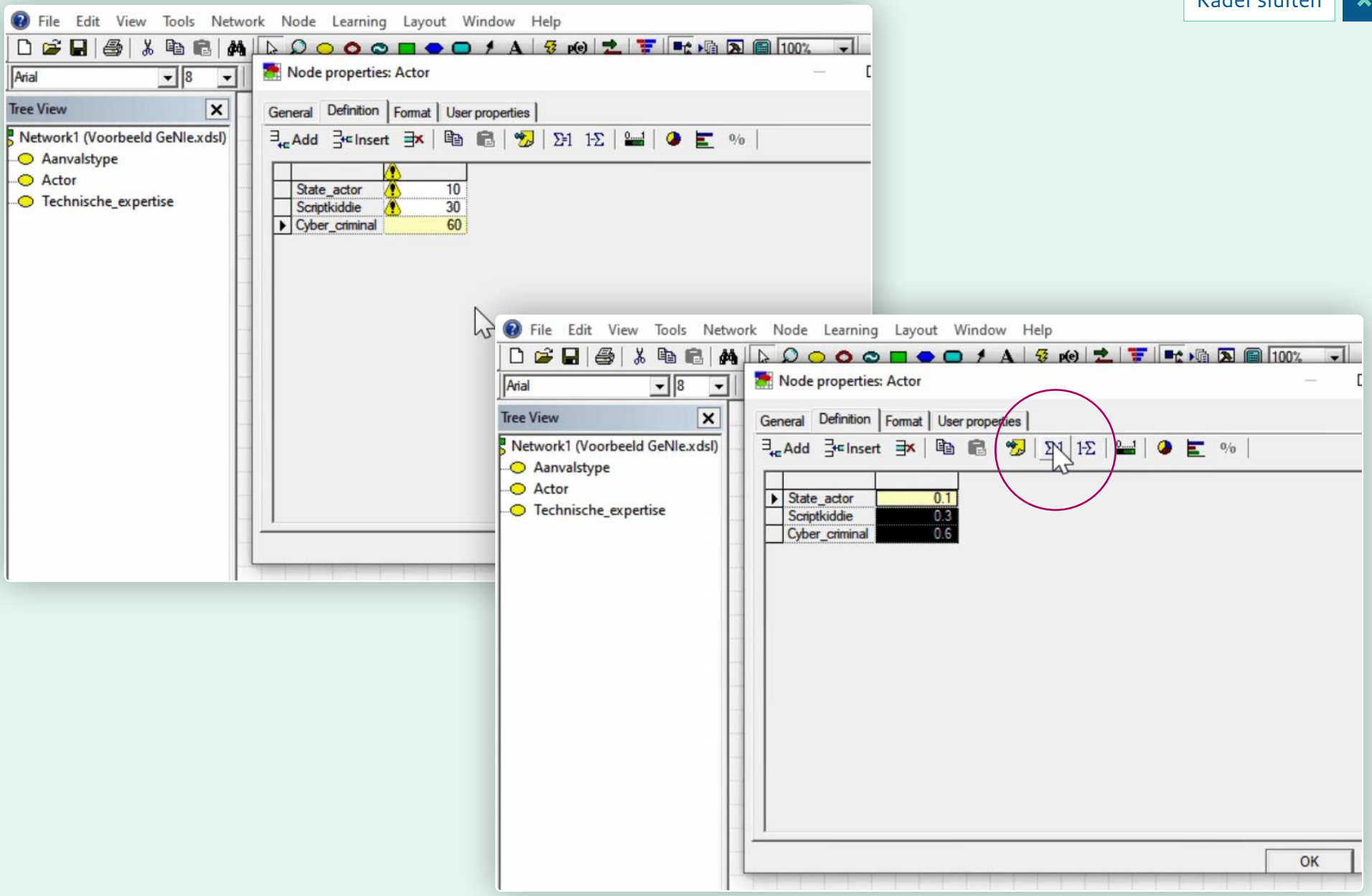
4.2 Waarschijnlijkheden

Bedenk wat de meest waarschijnlijke actor is die een gevaar zal vormen voor jouw organisatie. Hoe dichter een state bij het getal één is hoe groter is de kans.

In dit geval geven wij de state actor een waarde van 10, de scriptkiddie 30 en de cyber criminal 60. Vervolgens is het zaak om de waarden te normaliseren.



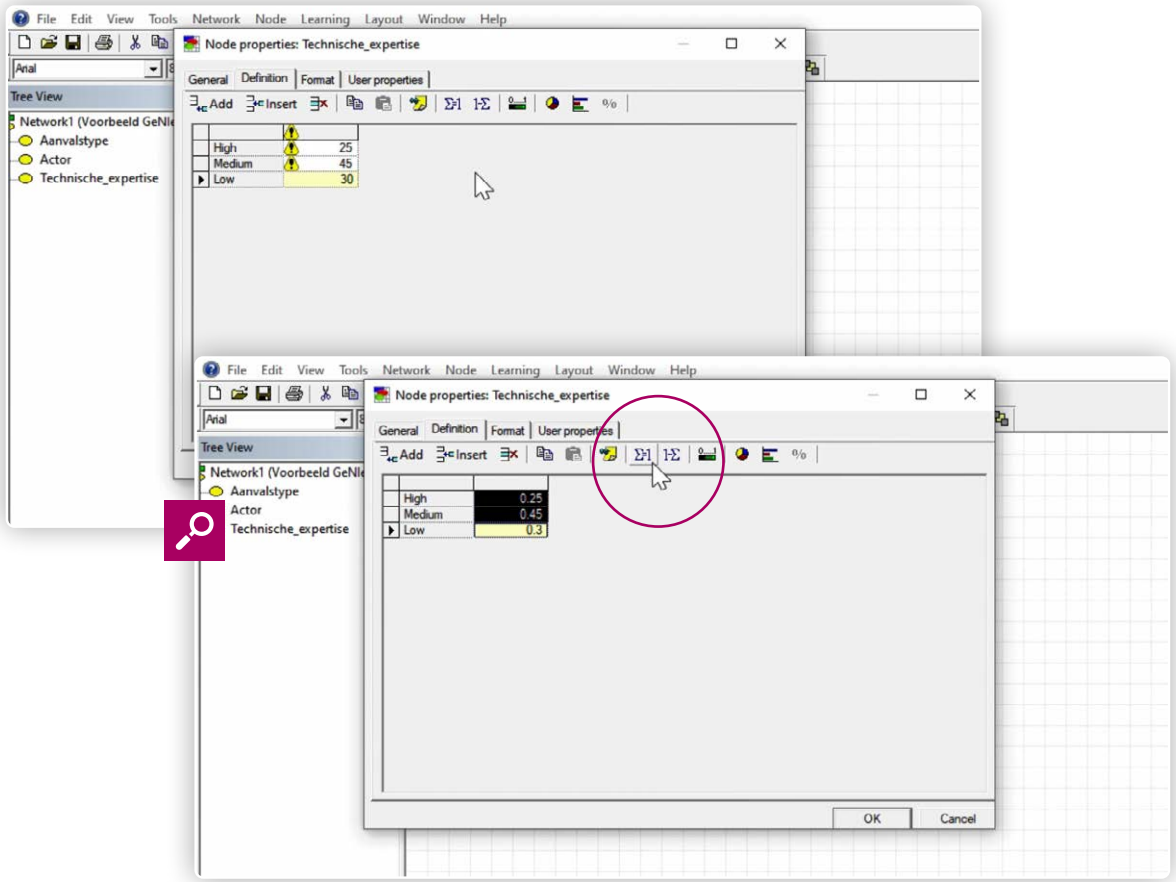
Kader sluiten



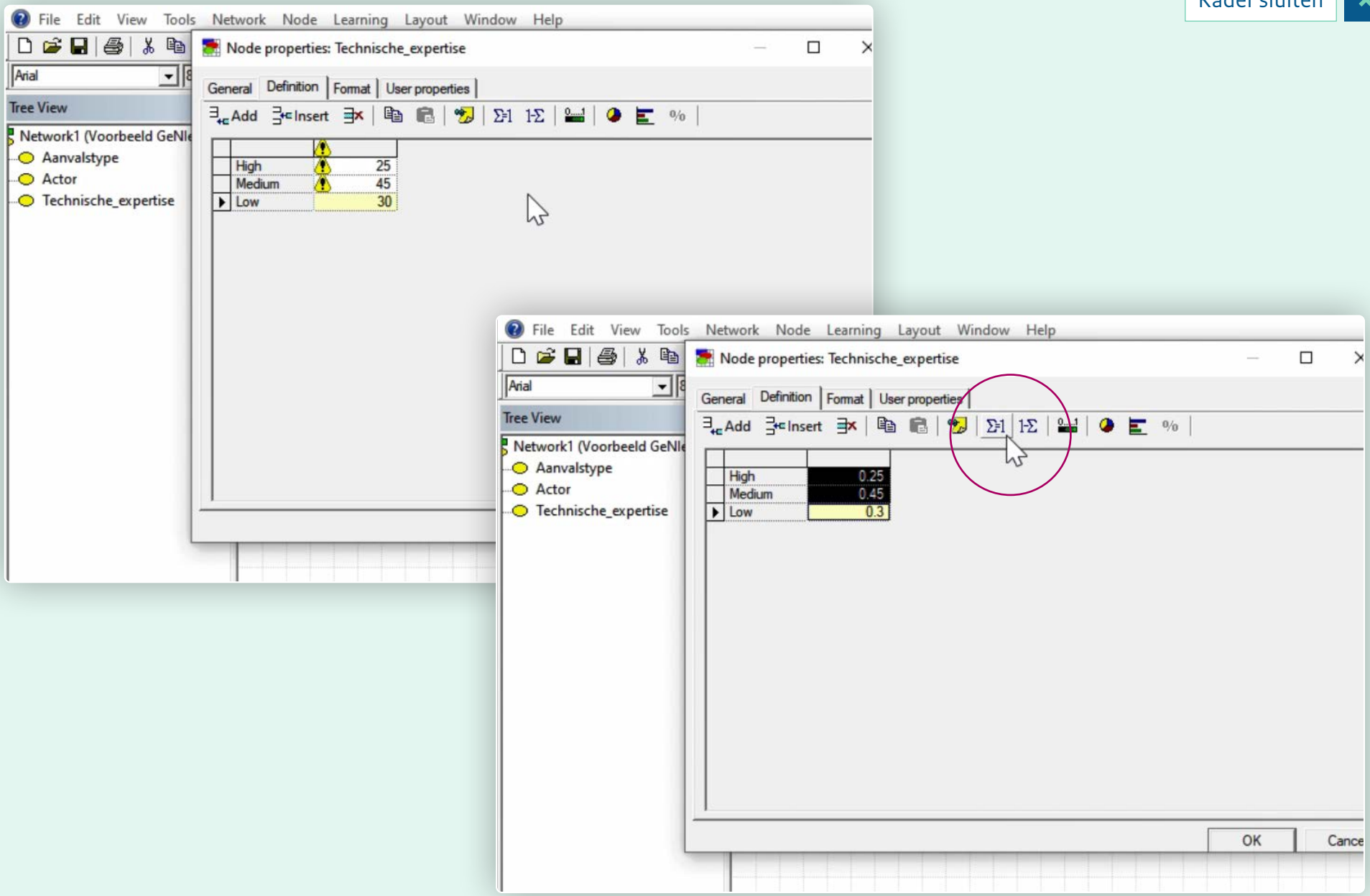
Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Invullen van states

Herhaal de eerdere stappen voor de technische expertise node. In ons voorbeeld geven wij high een waarde van 25, medium 45 en low 30.



Kader sluiten



Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Invullen van states

4.3 Parent en child nodes

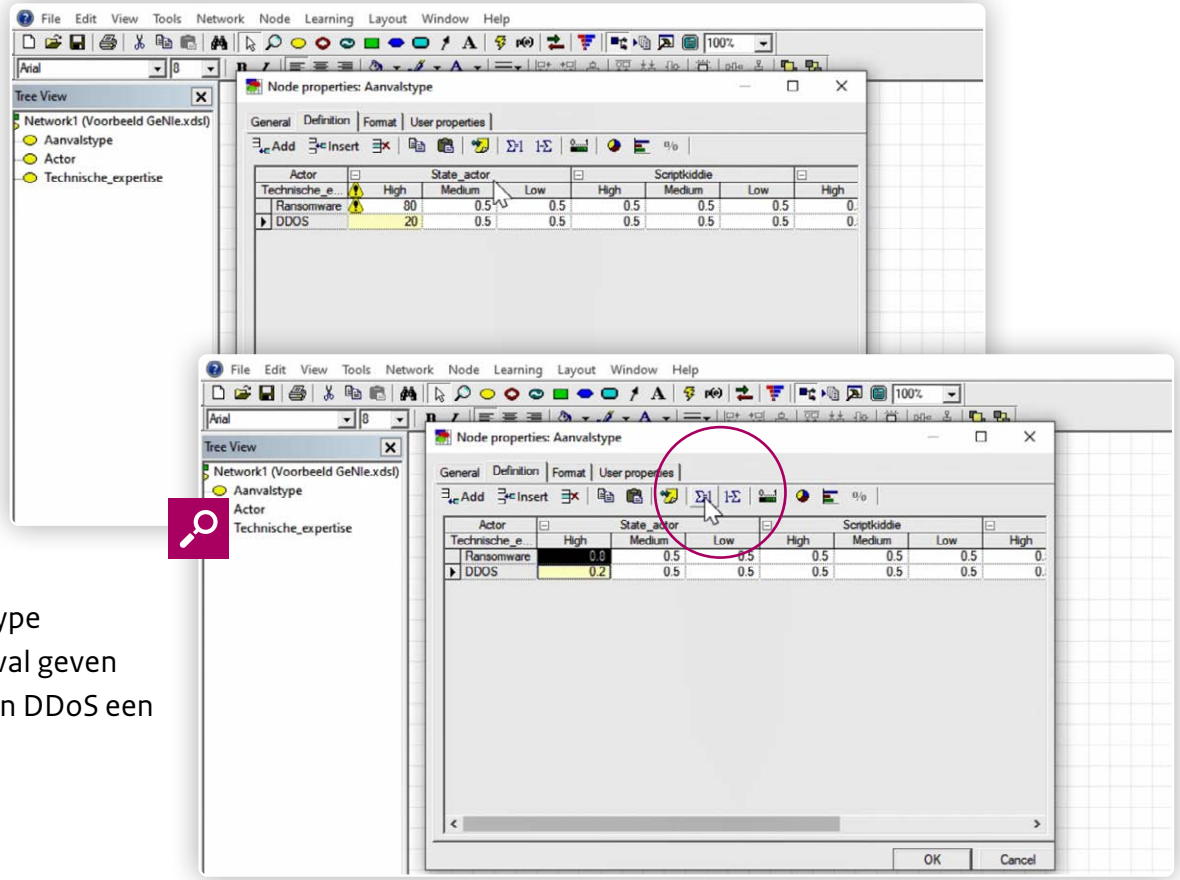
Klik rechts op de aanvalstype node, selecteer 'Node Properties' en navigeer naar 'Definition'. Zowel de actor node als de technische expertise node zijn input nodes en zijn relatief eenvoudig in te vullen. Ze zijn de parent nodes van attack type, een output node, en deze laatste ziet er dan ook anders uit. Child nodes (process nodes en output nodes) zoals aanvalstype zijn afhankelijk van de input van hun parents.

Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Invullen van states

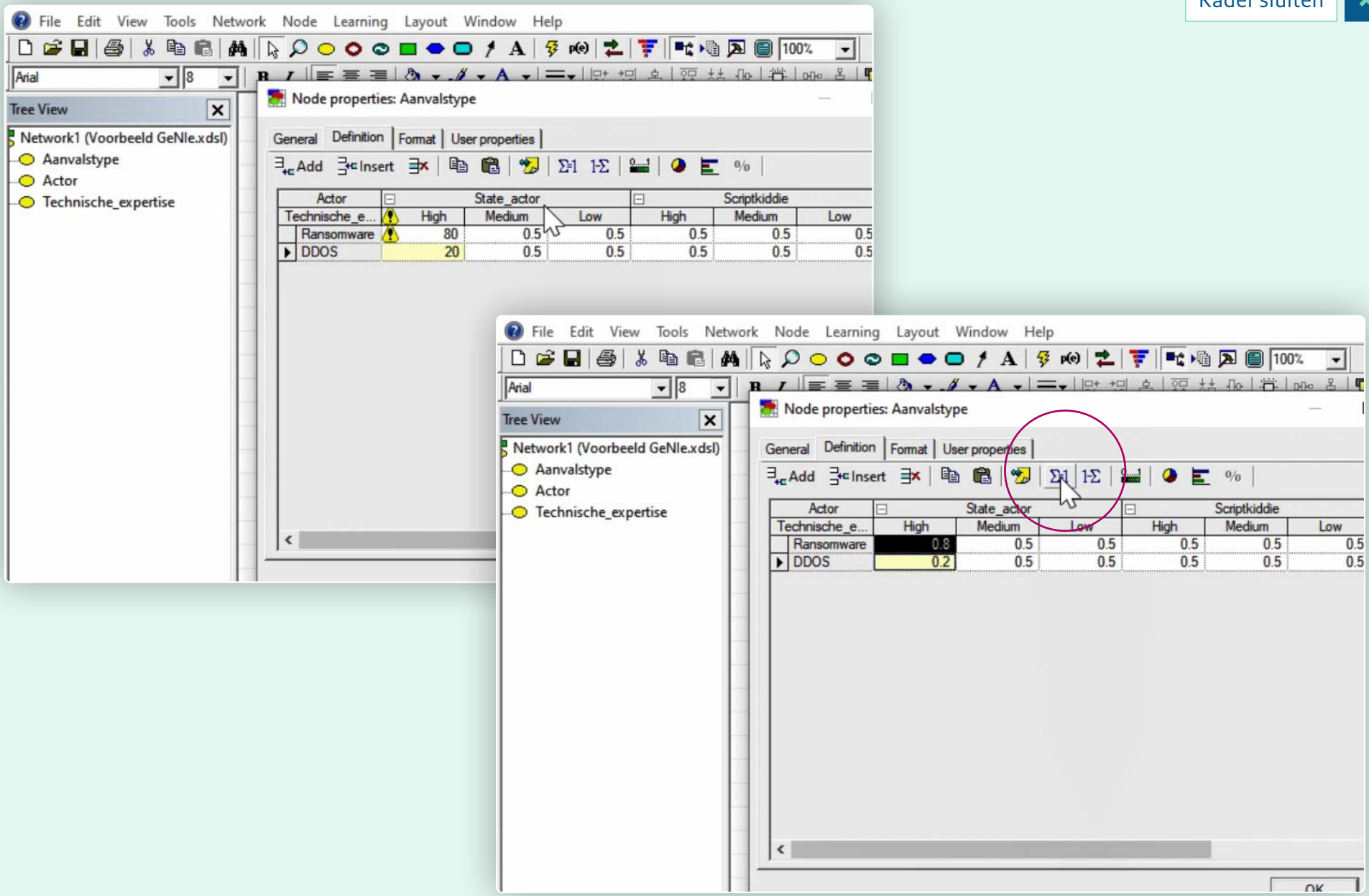
4.4 Combinaties van states

Bij het invullen van de waarden van de states van de aanvalstype node moeten de states van de andere nodes in beschouwing worden genomen. Zo ontstaat er een tabel met een kolom voor iedere combinatie van parent states. Ter illustratie: gegeven dat er sprake is van een state actor met hoge technische expertise, hoe groot is de kans dat het aanvalstype ransomware/ DDoS zal zijn? In dit geval geven wij ransomware een waarde van 80 en DDoS een waarde van 20.



Terug naar

Kader sluiten



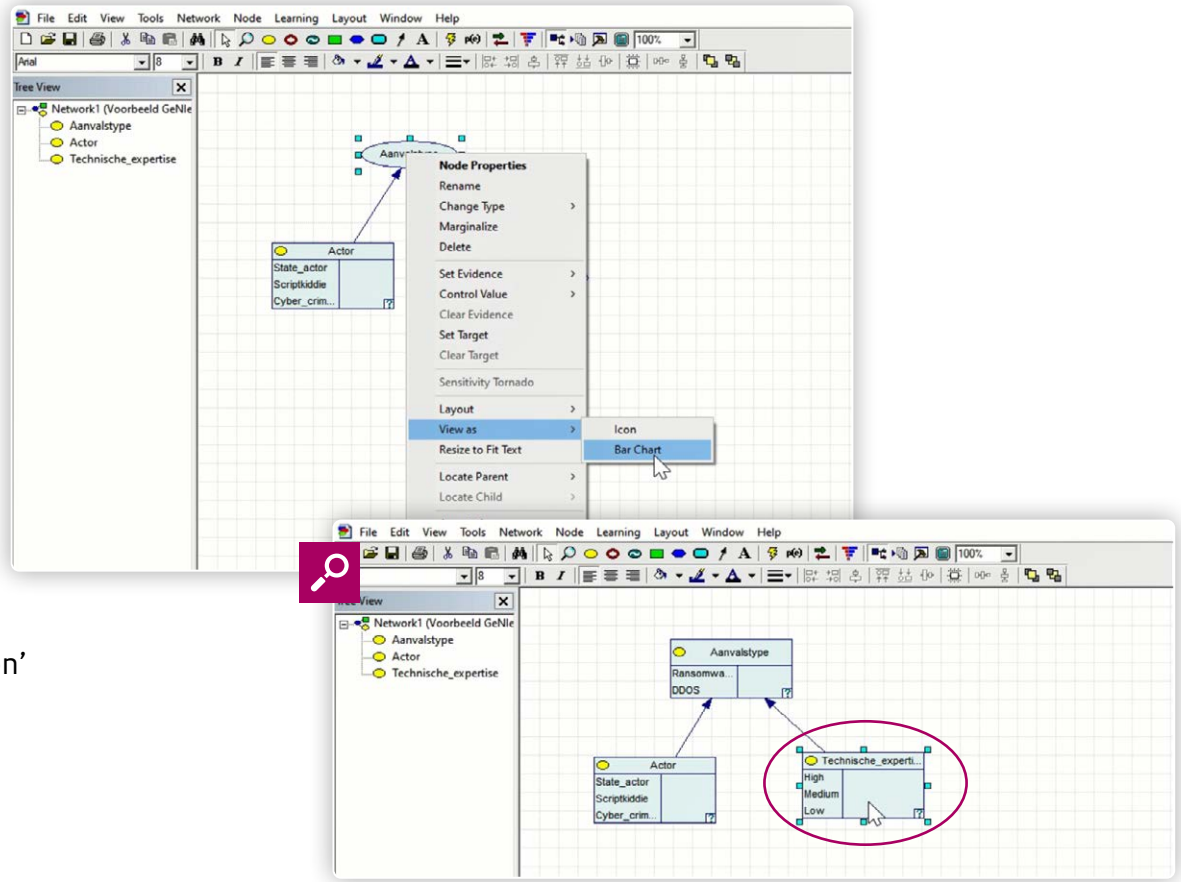
Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Netwerk doorrekenen

5.1 Aanzicht aanpassen

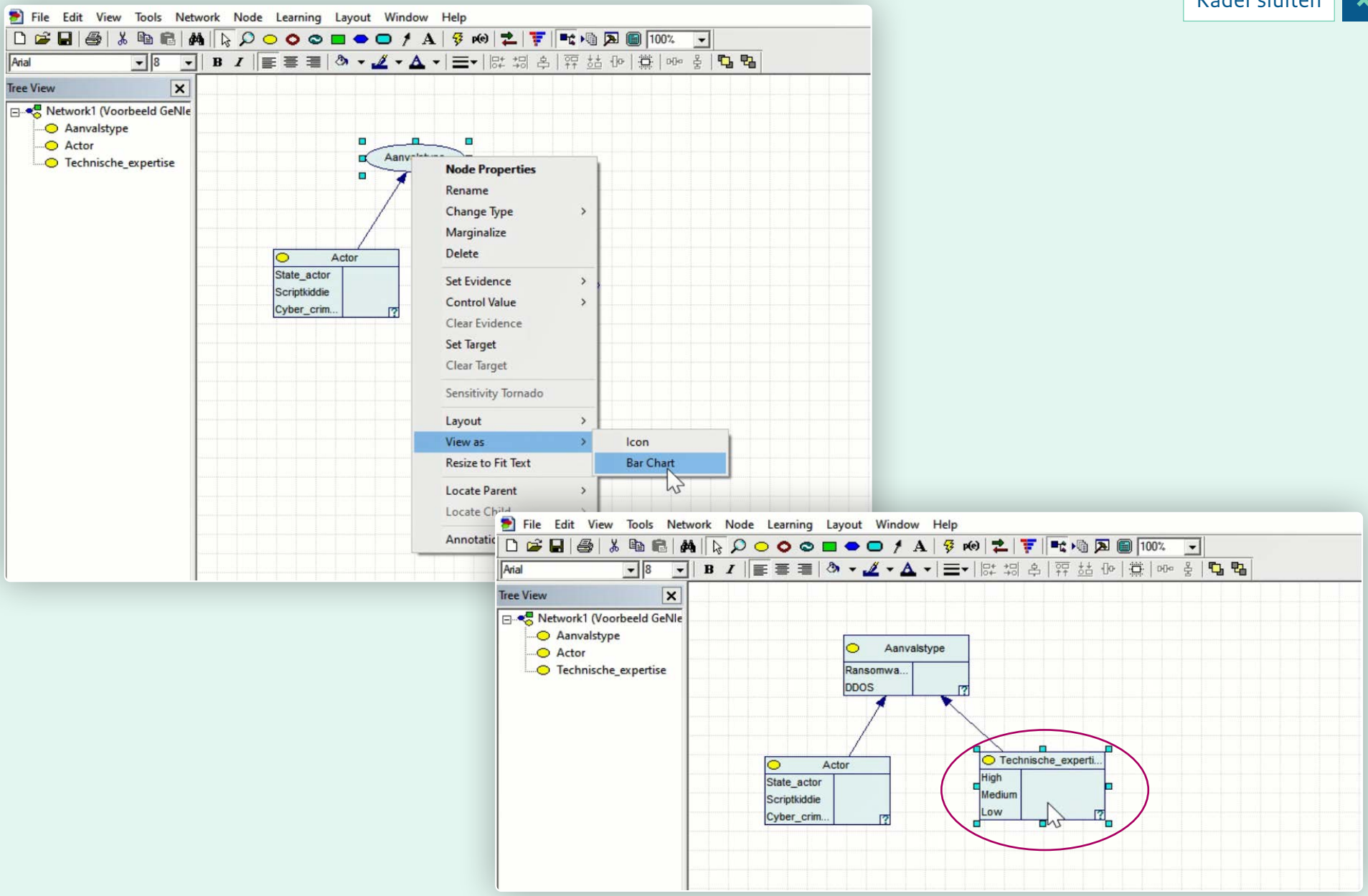
Het netwerk staat: de nodes zijn gecreëerd, de onderlinge relaties zijn vastgelegd en de relatieve waarden van de states zijn toegekend. De volgende stap is om het netwerk door te rekenen, zodat de kans dat een bepaalde aanvalstype voorkomt wordt bepaald.

Rechterklik eerst op alle nodes en verander de 'View As' setting van 'Icon' naar 'Bar Chart'.



Terug naar

Kader sluiten



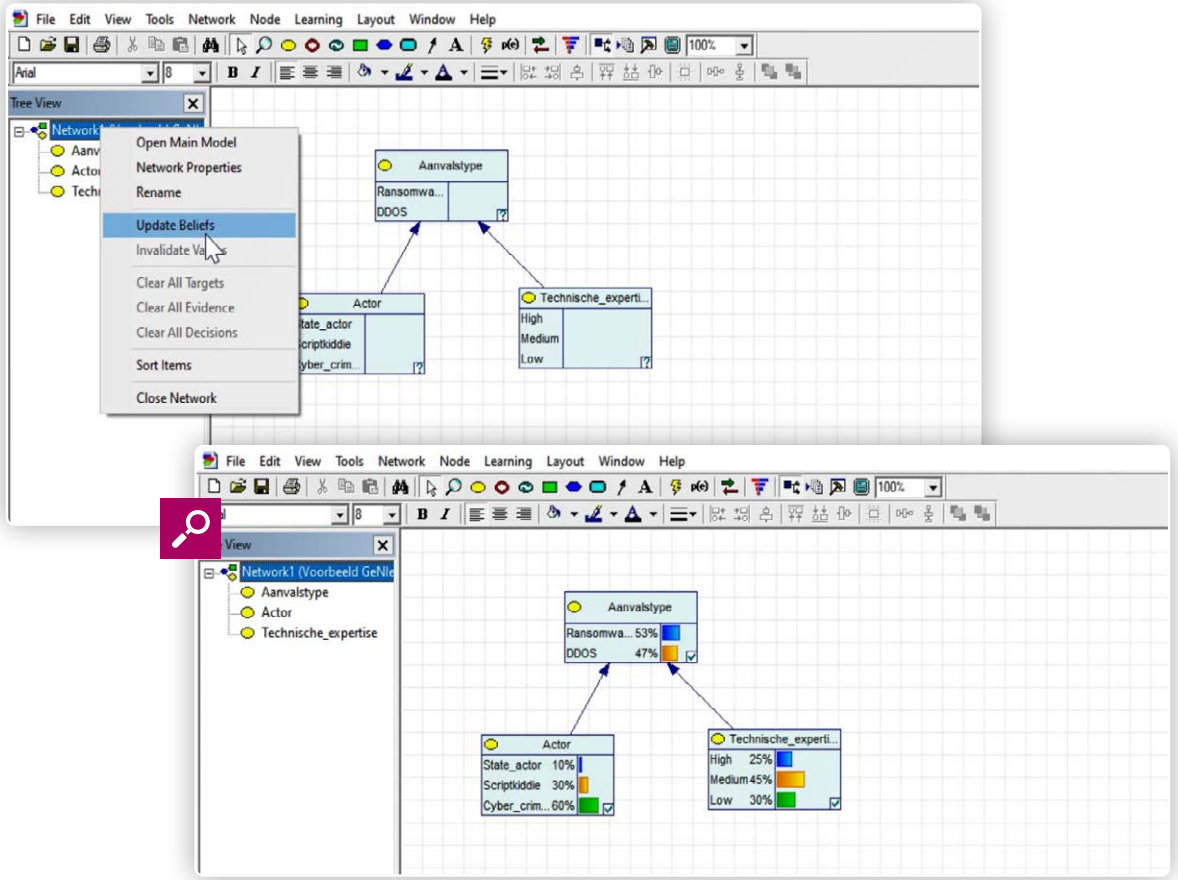
Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Netwerk doorrekenen

5.2 Berekening

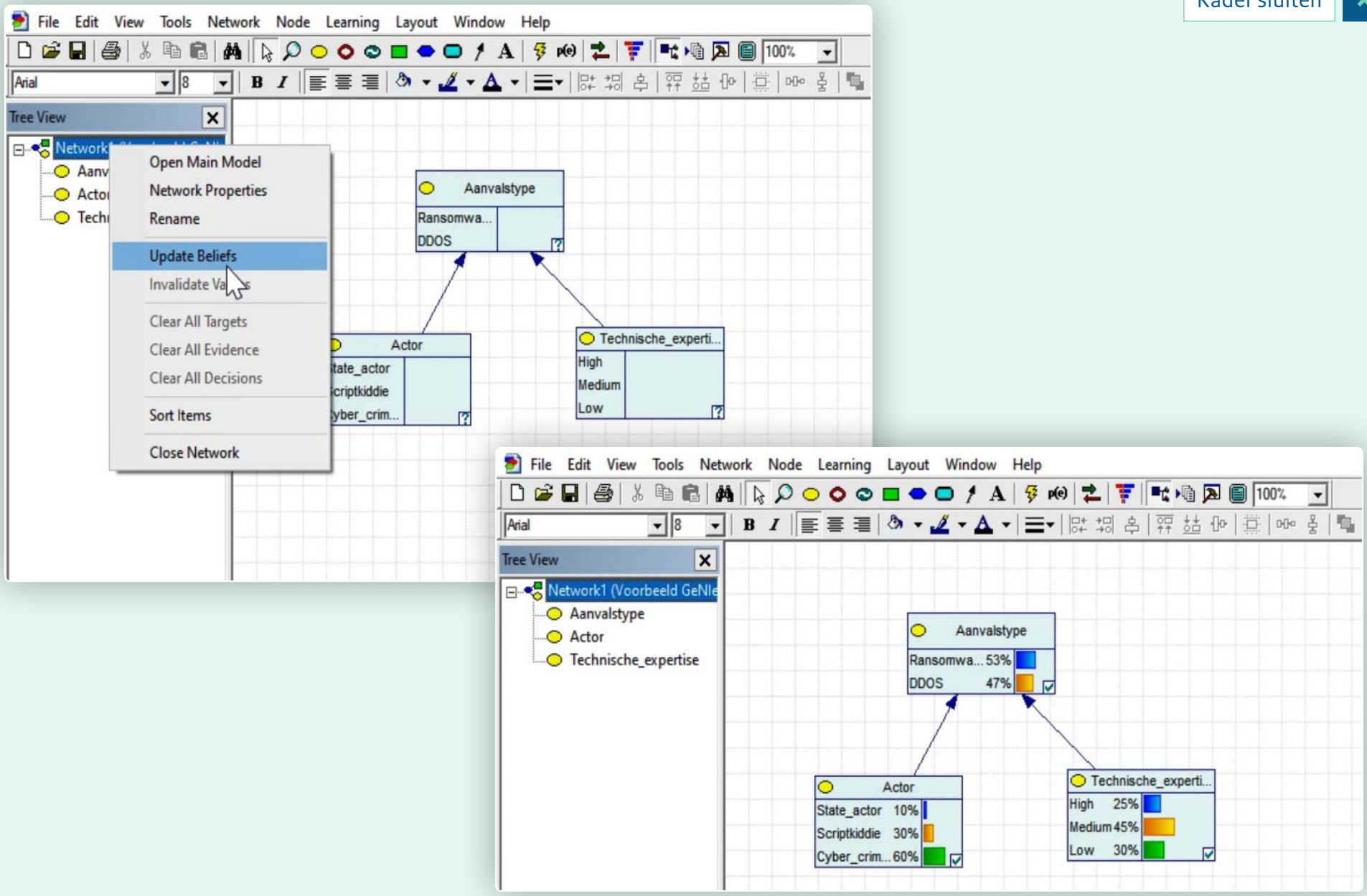
Selecteer Network in het navigatiemenu en rechterklik vervolgens op 'Update Beliefs'.

Het netwerk wordt nu door-gerekend. Met de actor tabel ingevuld zoals we dat hier doen, krijgen we de relatieve kansen van verschillende soorten aanvallen, gegeven het feit dat er een aanval plaatsvindt.



Terug naar

Kader sluiten



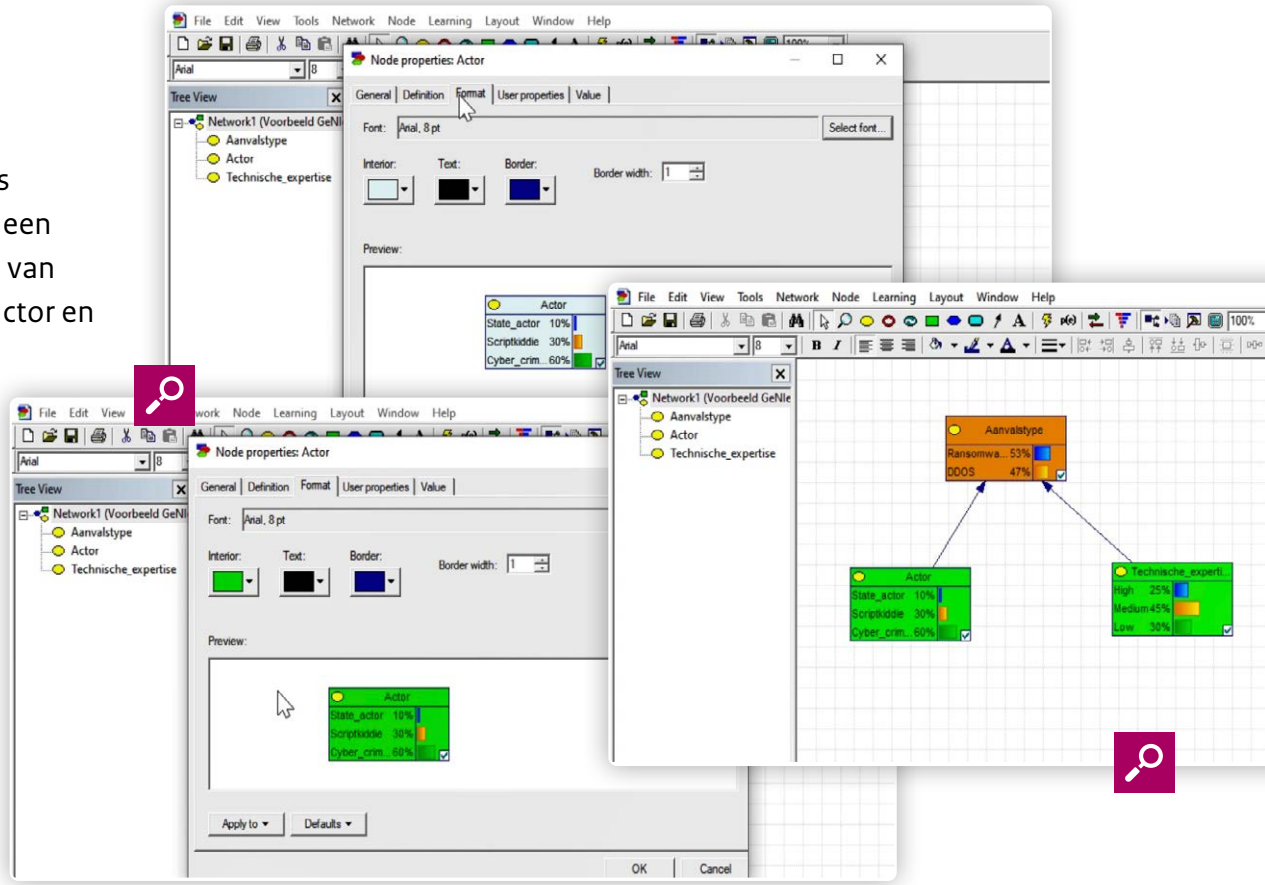
Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Styling / layout

6.1 Kleuren per node

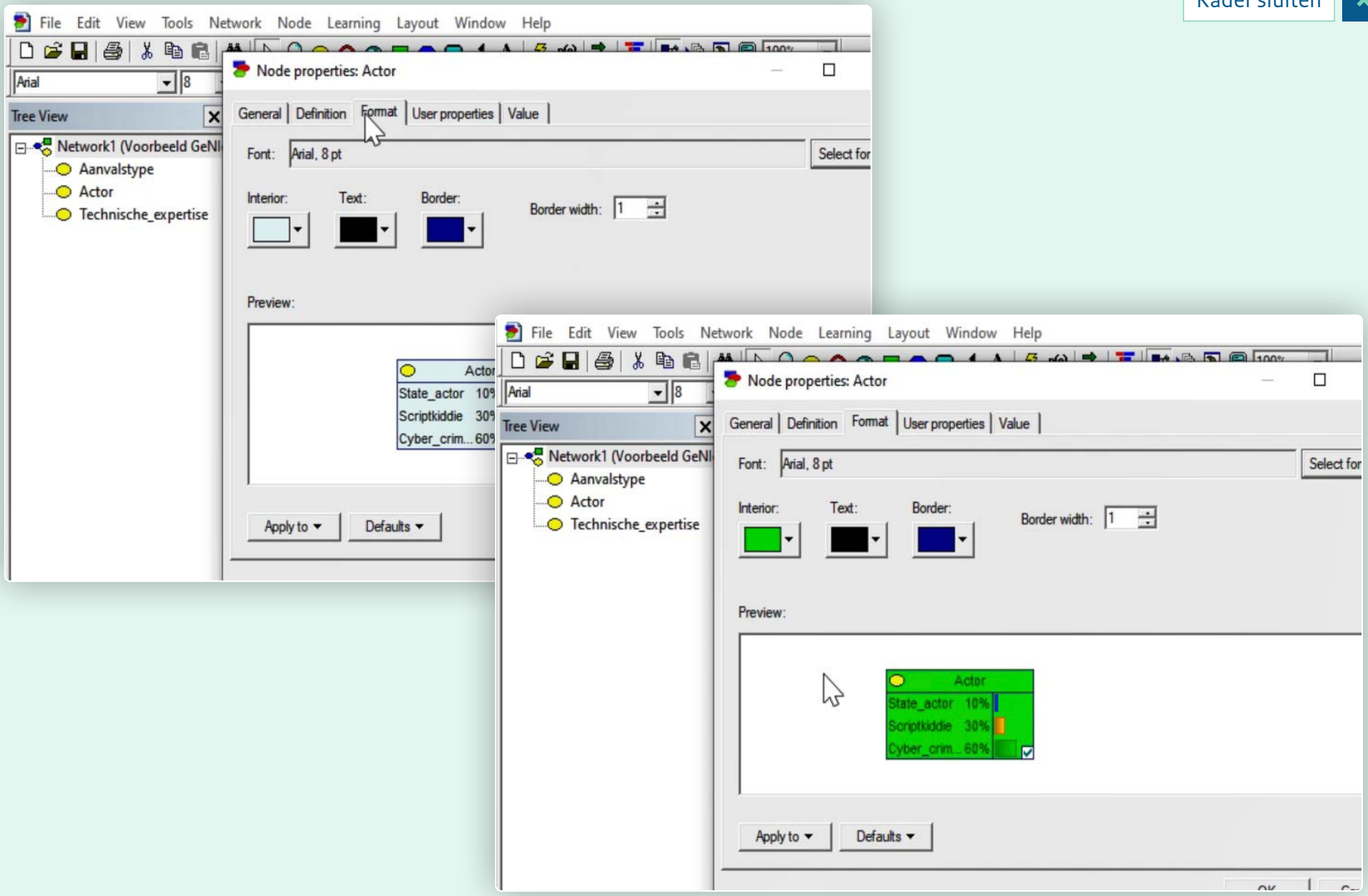
Het is aan te raden om de input nodes enerzijds en output nodes anderzijds een verschillende kleur te geven. Bij wijze van suggestie geven wij de input nodes (actor en technische expertise) de kleur groen en de output node (aanvalstype) de kleur oranje, en de tussen-liggende nodes lichtblauw.

Klik rechts op de node en selecteer 'Node Properties'. Navigeer vervolgens naar 'Format'. Hier kan je de kleur aanpassen van de nodes, alsmede de tekstkleur, lettertype, font size en omranding.



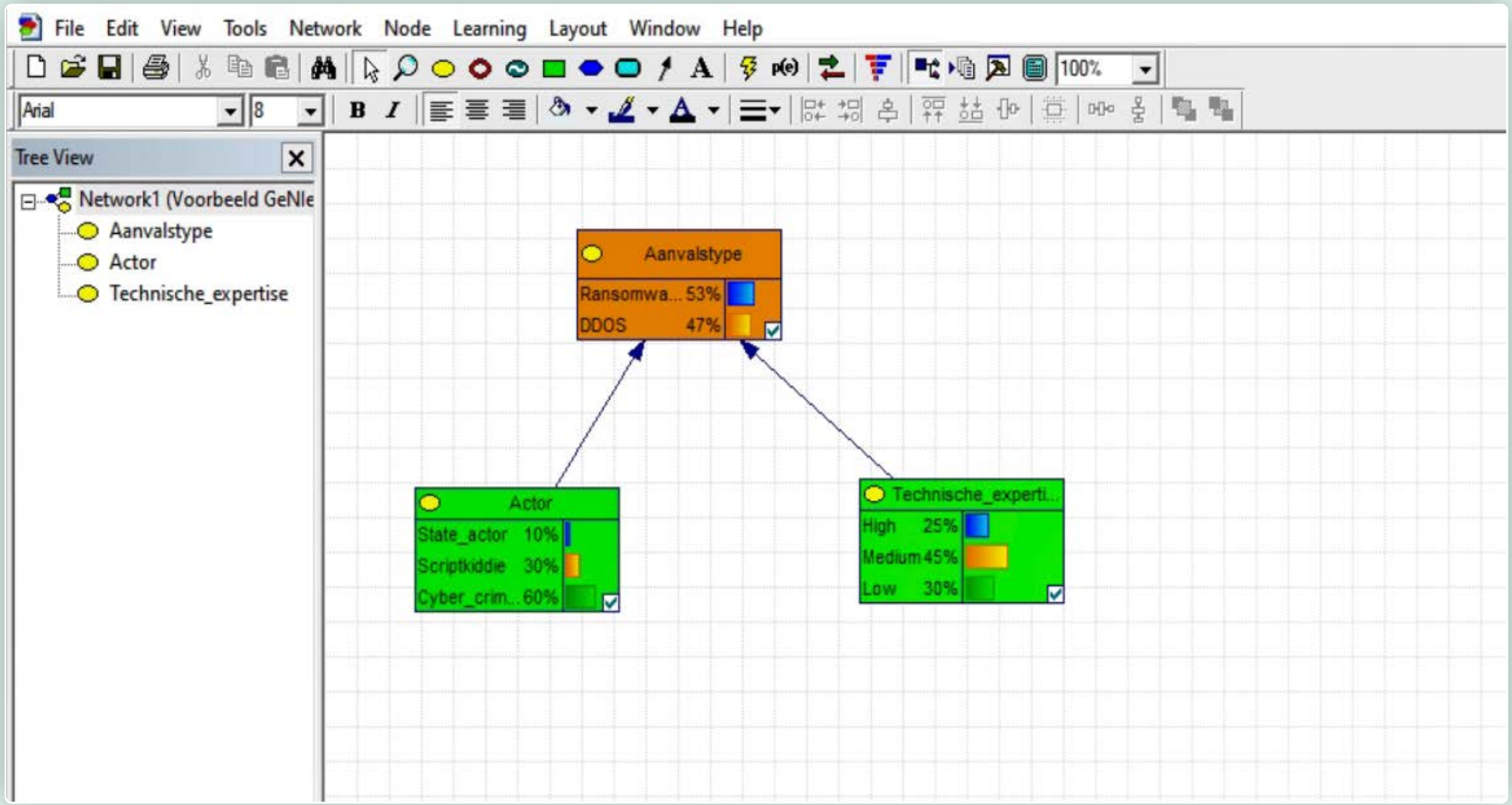
Terug naar

Kader sluiten



Aan de slag met het kwantificeren van cyberrisico's

Kader sluiten



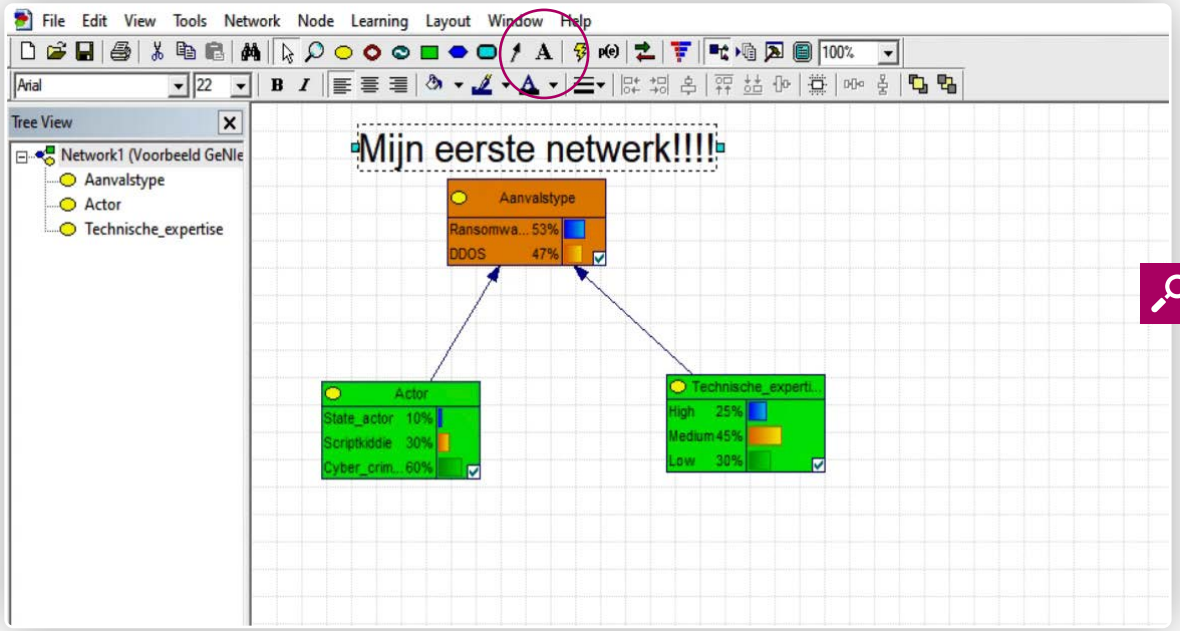
Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Styling / layout

6.2 Titel toevoegen

Het is mogelijk om een titel toe te voegen aan je netwerk.

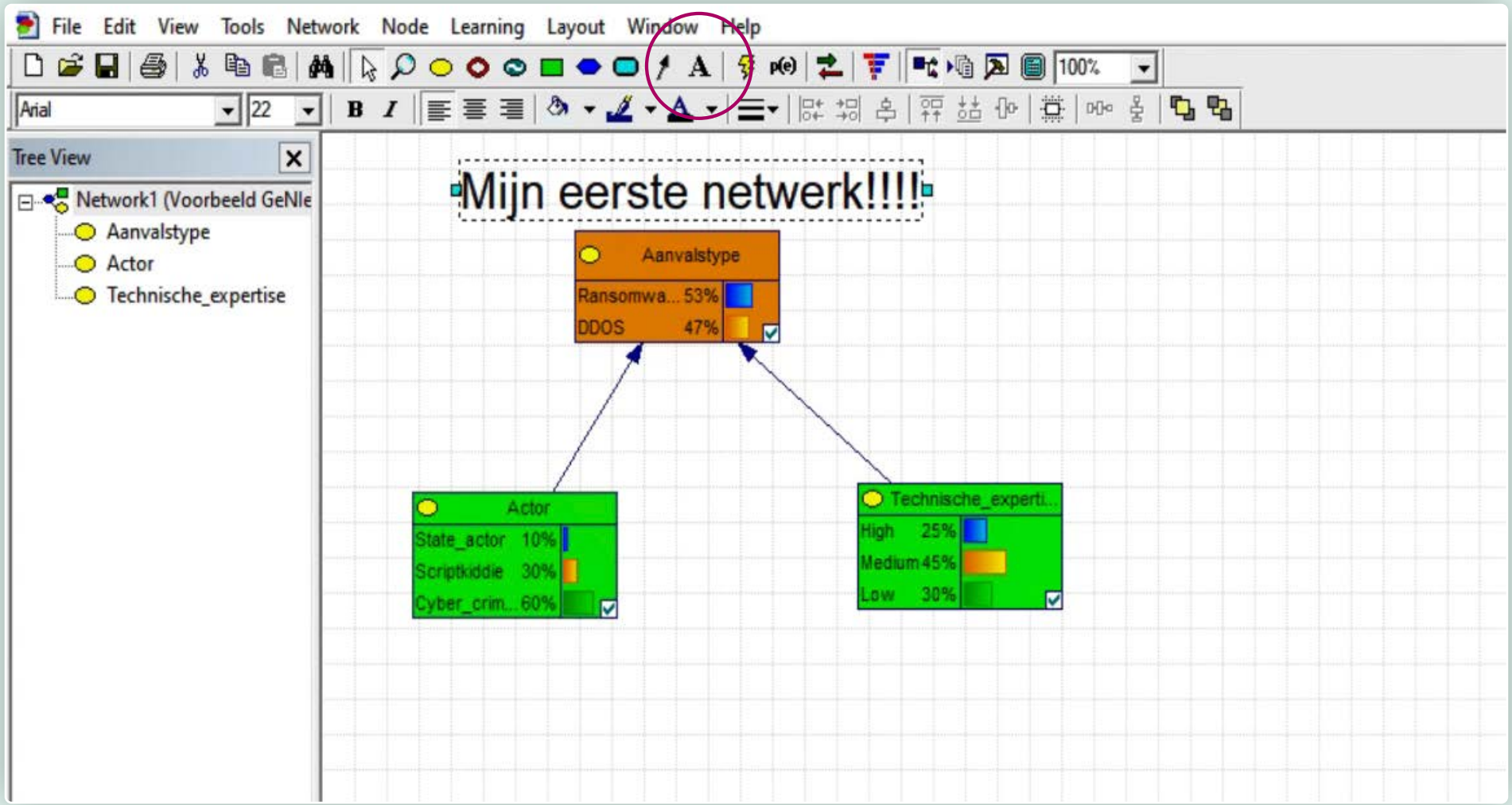
Klik op de zwarte hoofdletter 'A' in de toolbar. Door vervolgens op het veld te klikken verschijnt er een tekstbox. De styling van de tekstbox kan worden aangepast middels de toolbar (denk aan lettertype, font size, tekstkleur en uitlijning).



Uiteraard zijn er nog veel meer opties voor styling en layout die wij niet bespreken in deze handleiding.
Kijk voor een uitgebreid overzicht in de GeNIe Modeler user manual.

Aan de slag met het kwantificeren van cyberrisico's

Kader sluiten



Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

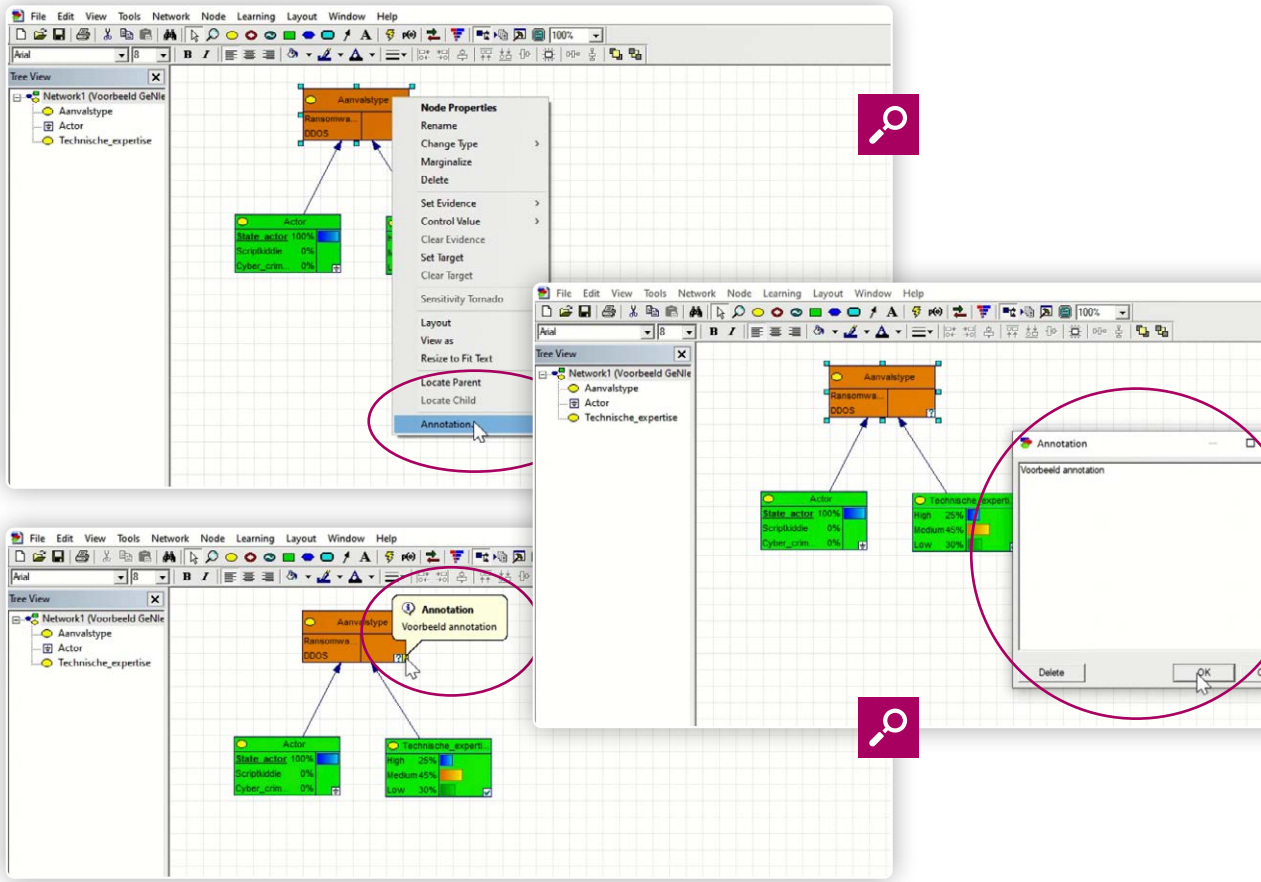
Extra functionaliteiten

7.1 Commentaar toevoegen

Het is mogelijk om commentaar toe te voegen aan de nodes (bijvoorbeeld referenties naar bronnen, namen van experts die de inschattingen hebben gemaakt, ...).

Klik rechts op een node en selecteer 'Annotation'. Er verschijnt een veld waarin opmerkingen kunnen worden geplaatst.

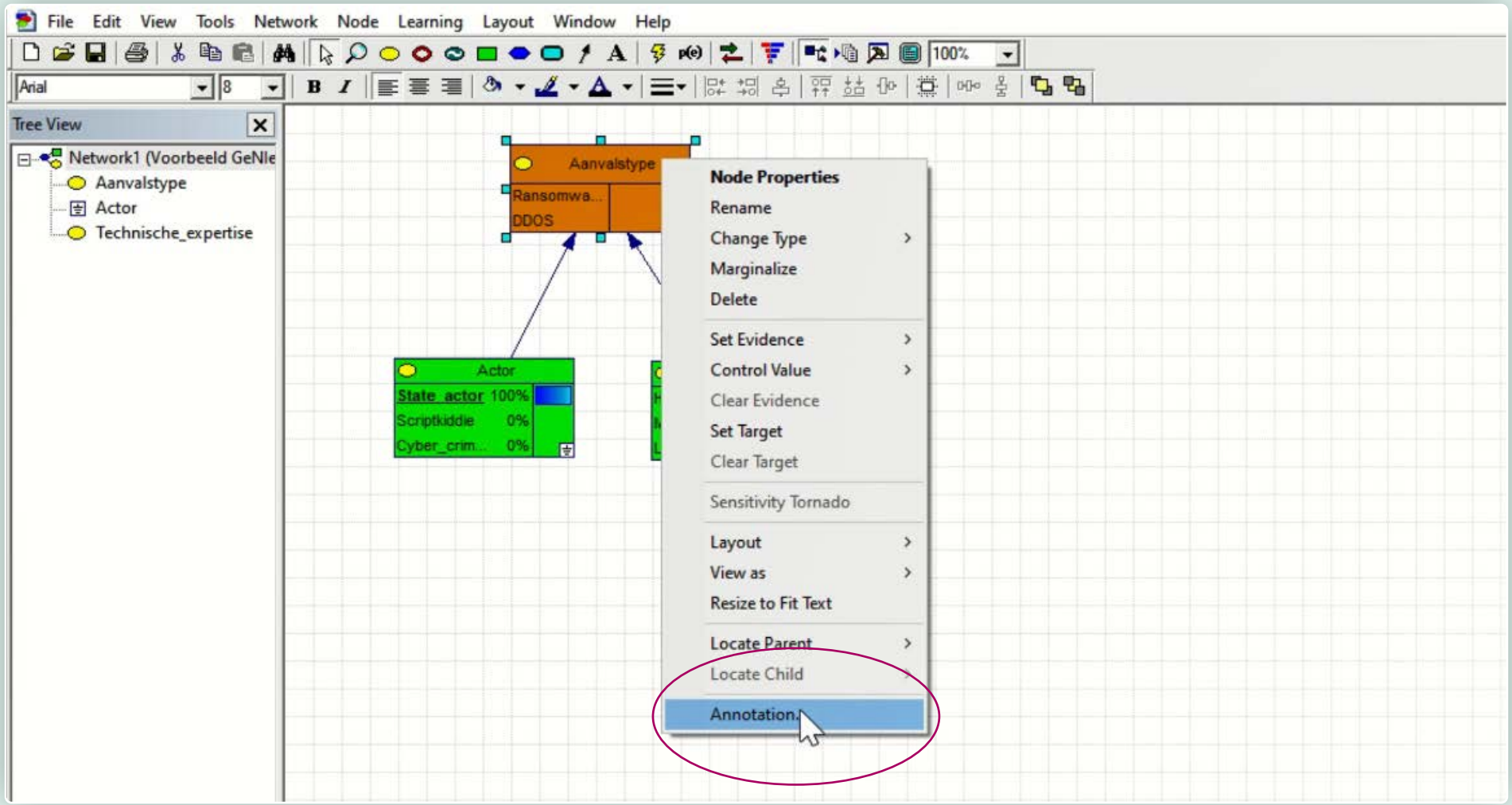
Er wordt vervolgens een notitie icoontje in de node geplaatst.
De annotatie verschijnt wanneer je de cursor boven het notitie icoontje houdt.



Aan de slag met het kwantificeren van cyberrisico's

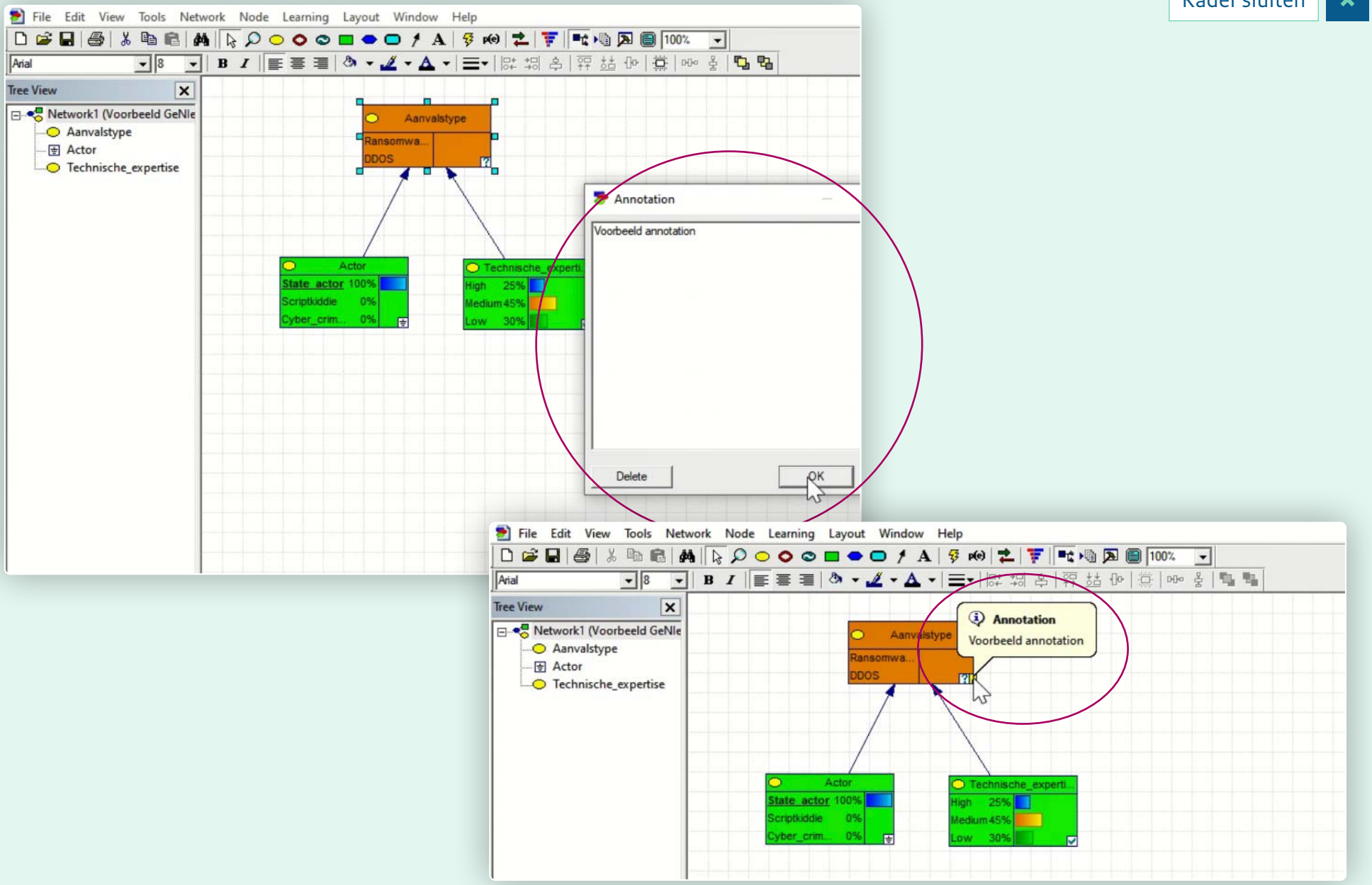
Terug naar navigatie figuur

Kader sluiten



Terug naar

Kader sluiten

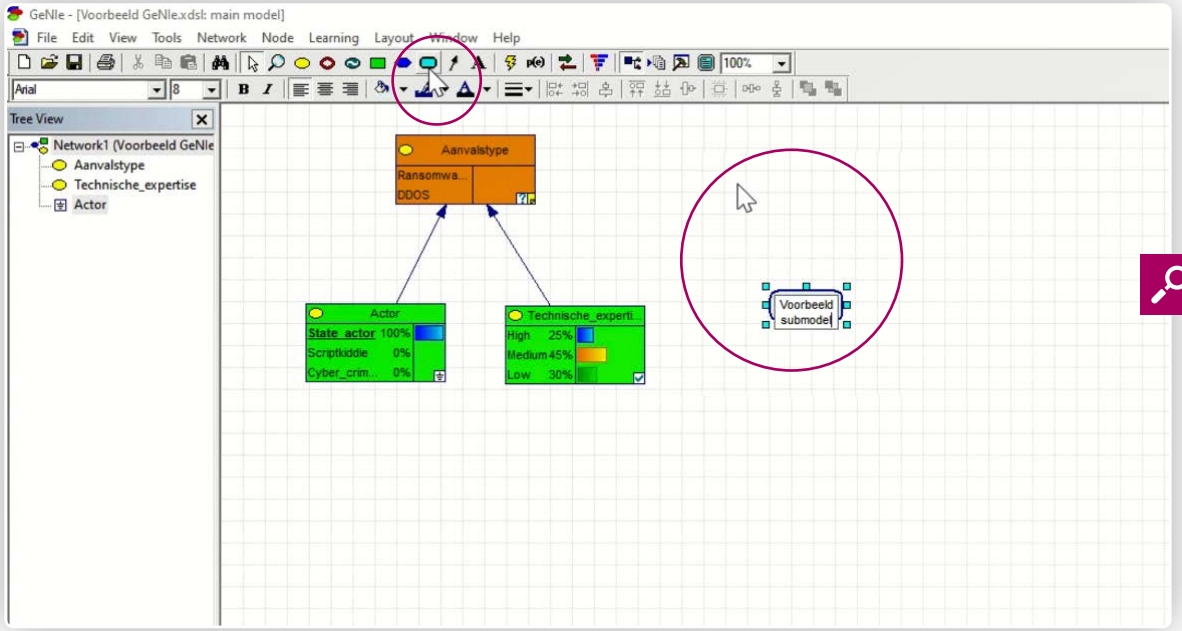


Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Extra functionaliteiten

7.2 Submodel creëren

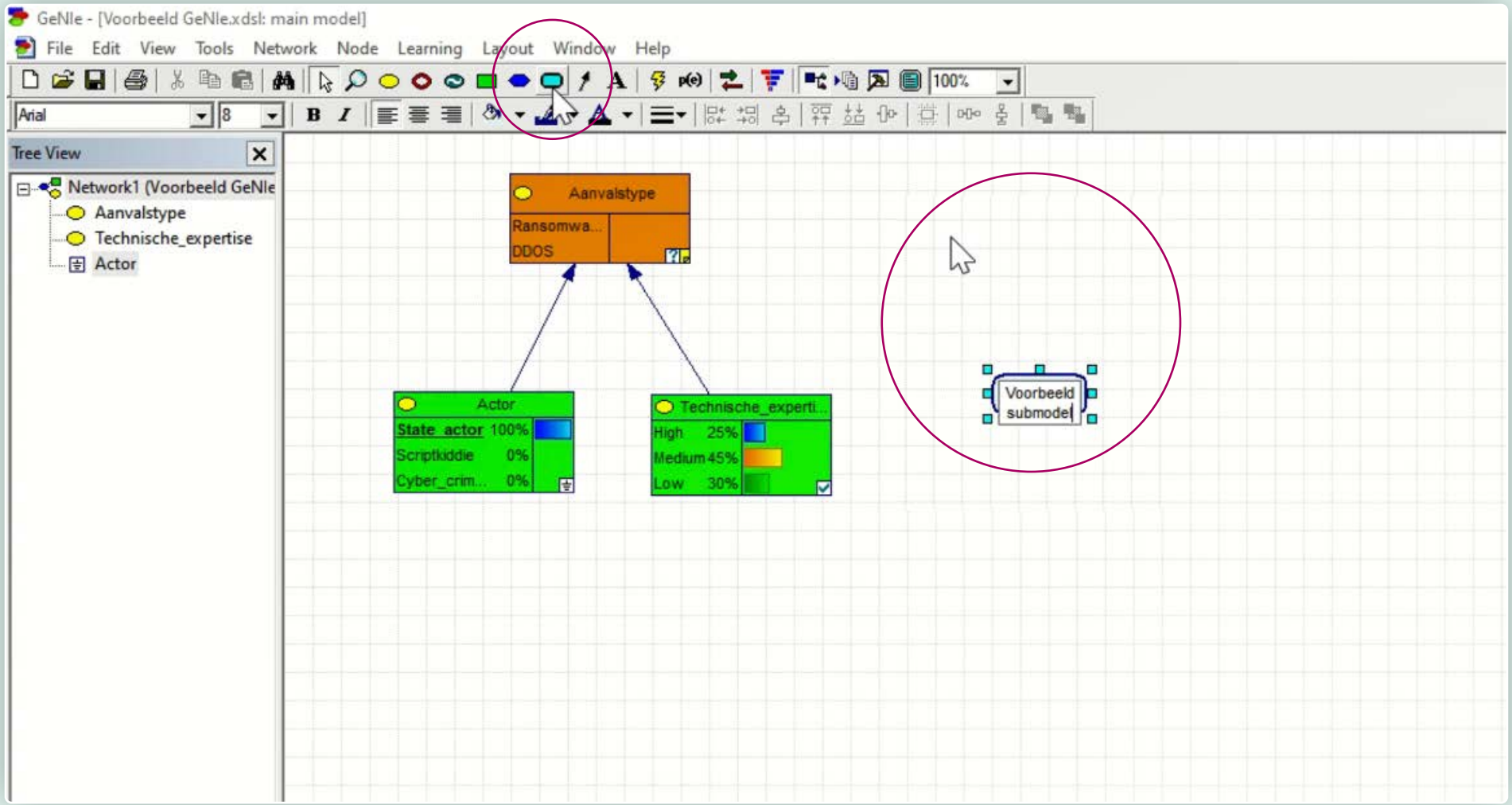
Een andere functionaliteit is een formele ondersteuning om een submodel te creëren. Submodellen veranderen niets aan de werking van het model, maar zijn een manier om overzicht te houden over grotere modellen, en om delen van een model makkelijk in een ander model te hergebruiken.



Een submodel kan worden toegevoegd met de lichtblauwe afgeronde rechthoek in de toolbar. Submodellen voegen een hiërarchie toe vergelijkbaar met de mappenstructuur op de computer.

Aan de slag met het kwantificeren van cyberrisico's

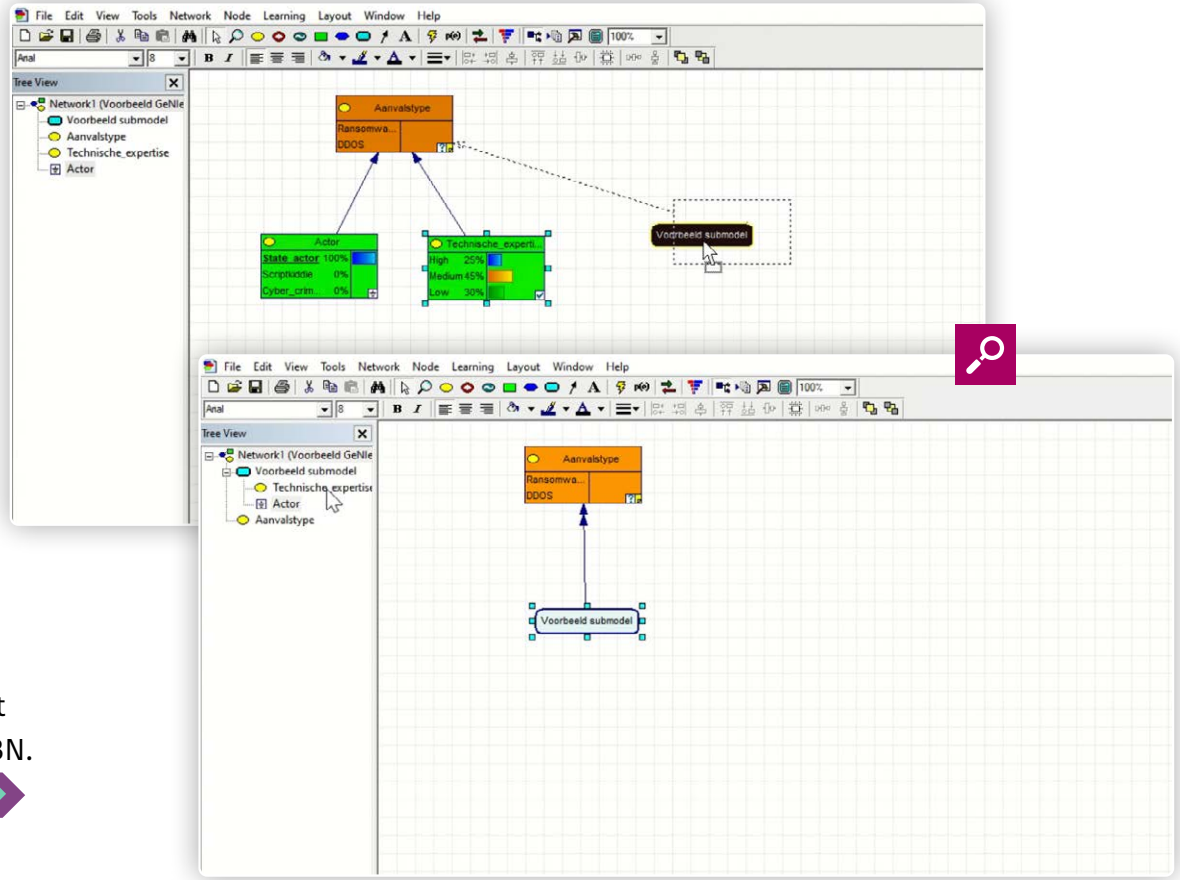
Kader sluiten



Bijlage 1: Instructies ontwikkelen van rekenmodel in het programma GeNIe

Extra functionaliteiten

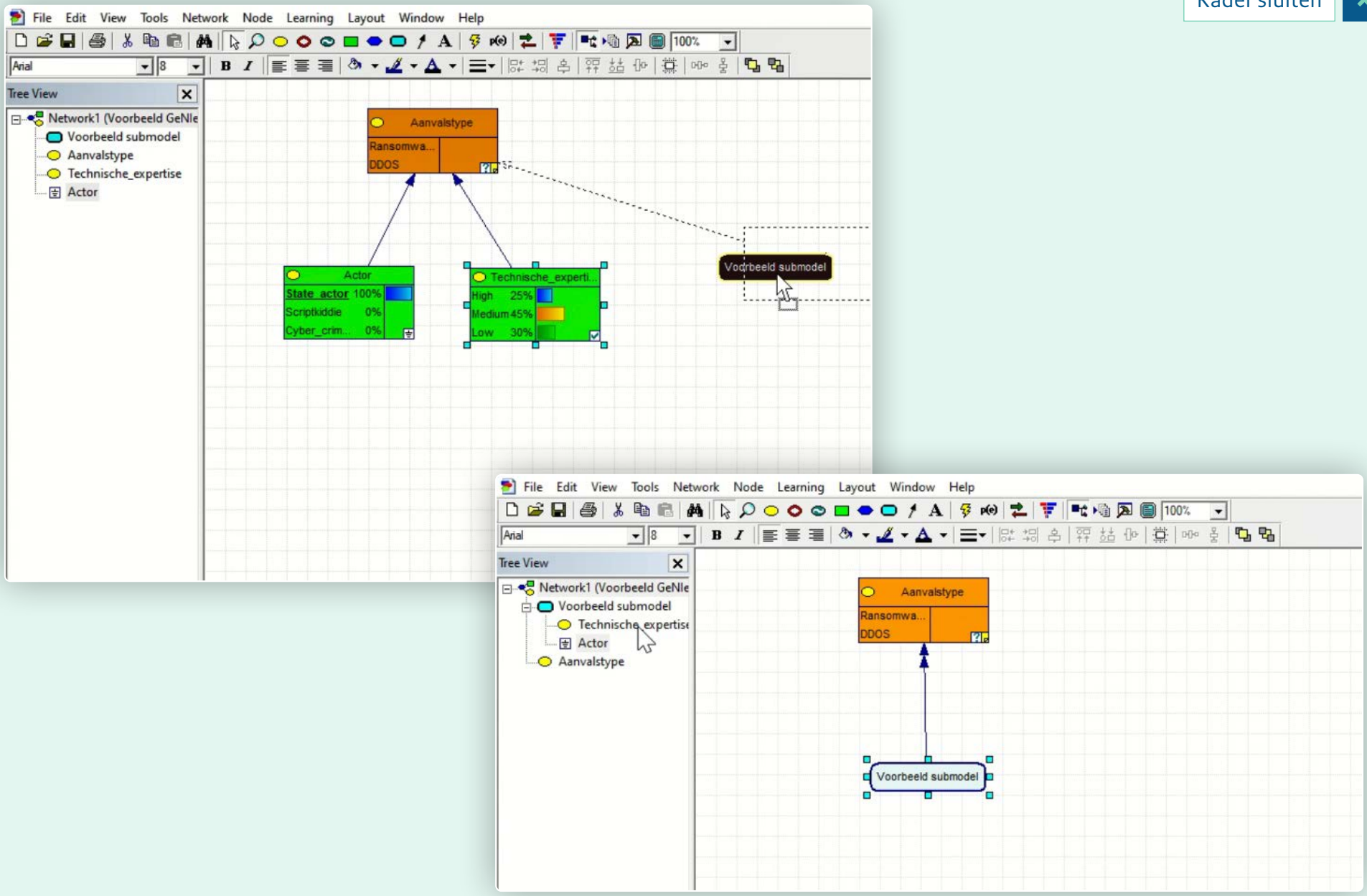
Door te dubbelklikken open je het submodel en kun je het submodel vormgeven zoals je een normaal model maakt. Daarnaast kunnen nodes binnen het submodel worden verbonden met nodes buiten het submodel.



Dit is het einde voor de instructies met betrekking tot het bouwen van een BBN. Ga terug naar het navigatie figuur om andere opties te bekijken.

Terug naar

Kader sluiten



Bijlage 2: BBN voorbeeldmodellen

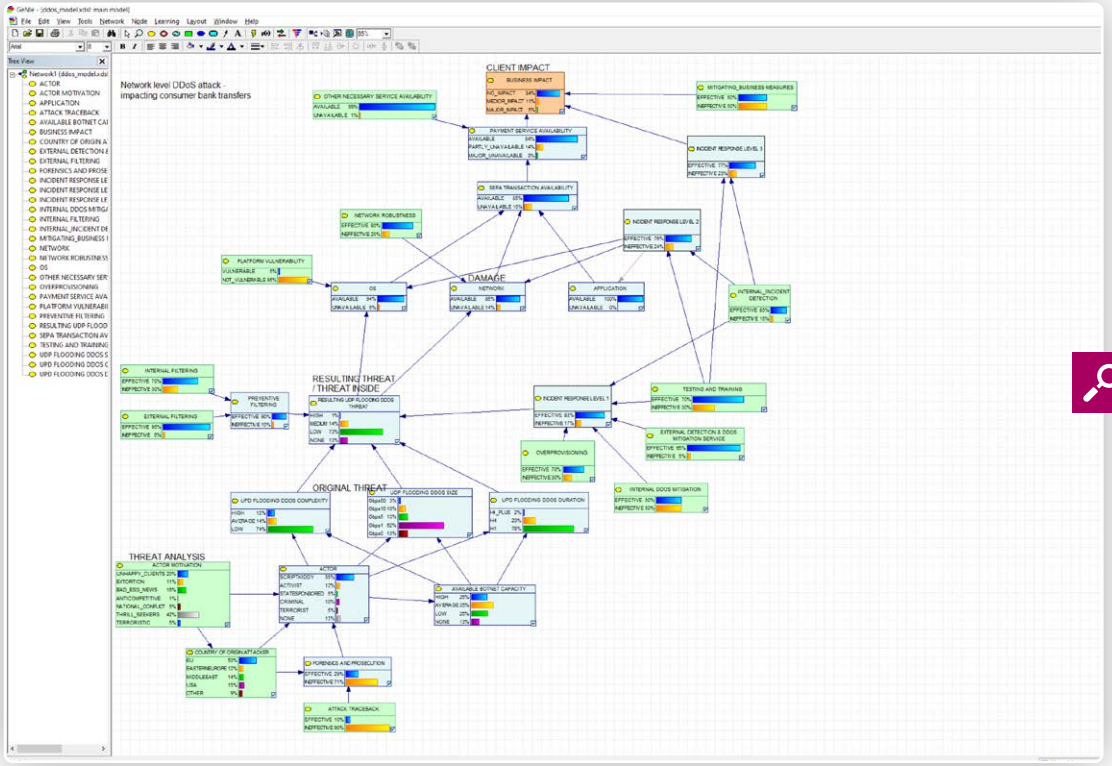
Om beter te begrijpen hoe je werkt met Bayesian Belief Modellen volgen hier enkele (voorbeeld)modellen met uitleg. Deze modellen zijn gemaakt in het programma GeNIe en opgeslagen in het native GeNIE 2.0 File (.xdls) bestandsformaat, alsmede in het breder ondersteunde Hugin File (.net) formaat (let wel dat in dit laatste formaat layout en opmaak niet behouden blijven).

Bijlage 2: BBN voorbeeldmodellen

Een volledig model

ddos_model.xdsl | ddos_model.net

Allereerst is er een volledig model bijgevoegd om te illustreren waar je met de methode naartoe werkt. Het betreft het network-niveau DDoS aanvalsmodel, zoals beschreven in [7] Dit model, gericht op de impact van een DDoS aanval op banktransacties van consumenten, is volledig uitgewerkt met een verscheidenheid aan input nodes (groen), waaronder eigenschappen van de potentiële aanvaller en mitigerende maatregelen, waarvan de invloed op de business impact (oranje) kan worden onderzocht.

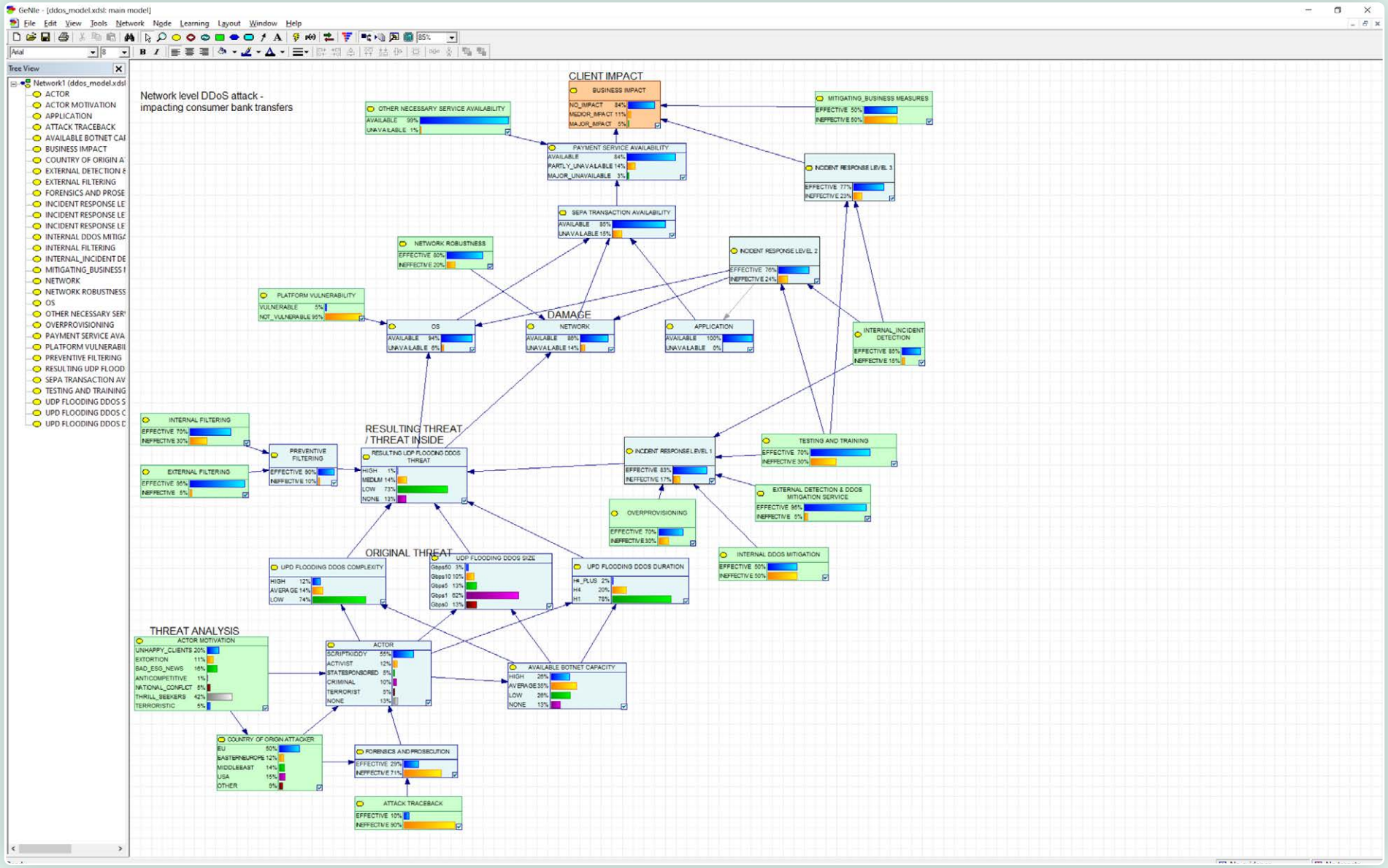


Een modulaire aanpak

Volledig model met als voorbeeld DDoS aanval.

Kader sluiten

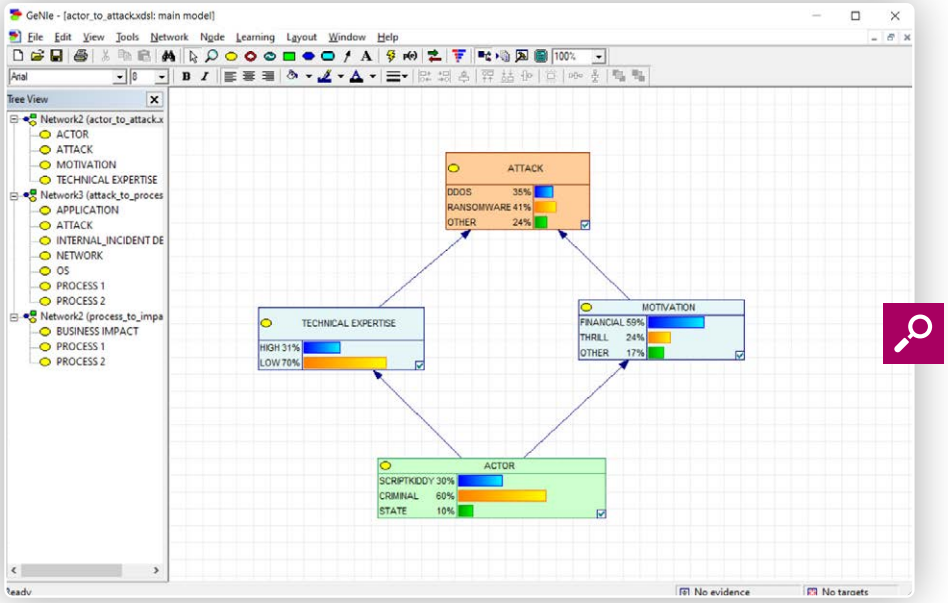
(Dit model is enkel bedoeld ter educatie. Aan dit model kunnen geen rechten worden ontleend.)



Bijlage 2: BBN voorbeeldmodellen

Een modulaire aanpak

De methode maakt een modulaire aanpak mogelijk waar verschillende delen van een model afzonderlijk kunnen worden uitgewerkt en uiteindelijk aan elkaar kunnen worden gekoppeld. Dit wordt nog makkelijker en overzichtelijker gemaakt door een "submodule" functionaliteit in GeNIe, die verderop beschreven staat. Om te illustreren hoe submodellen werken staat hieronder een voorbeeld van een eenvoudig model op basis van drie submodellen.



Submodel 1: Actor naar dreiging

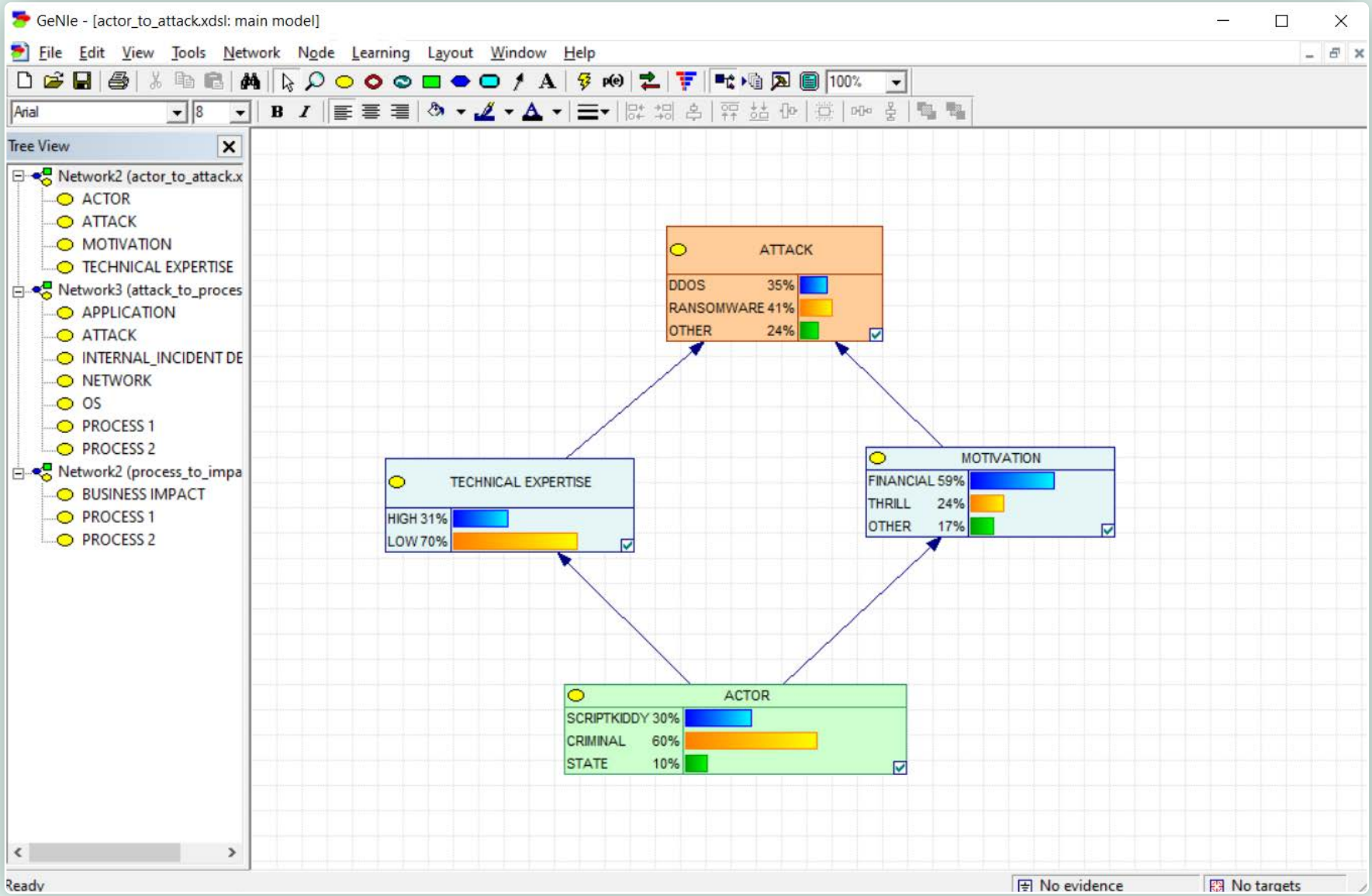
actor_to_attack.xdsl | actor_to_attack.net

Dit deelmodel beschrijft wat voor aanvalsvectoren waarschijnlijk zijn gegeven de input over de soorten mogelijke actoren. Het idee van dit model is dat de meest waarschijnlijke aanvalsvector bepaald wordt door de technische expertise en motivatie van de actor, die beiden op hun beurt afhankelijk zijn van het soort actor.

Terug naar

Kader sluiten

Submodel 1: Actor naar dreiging

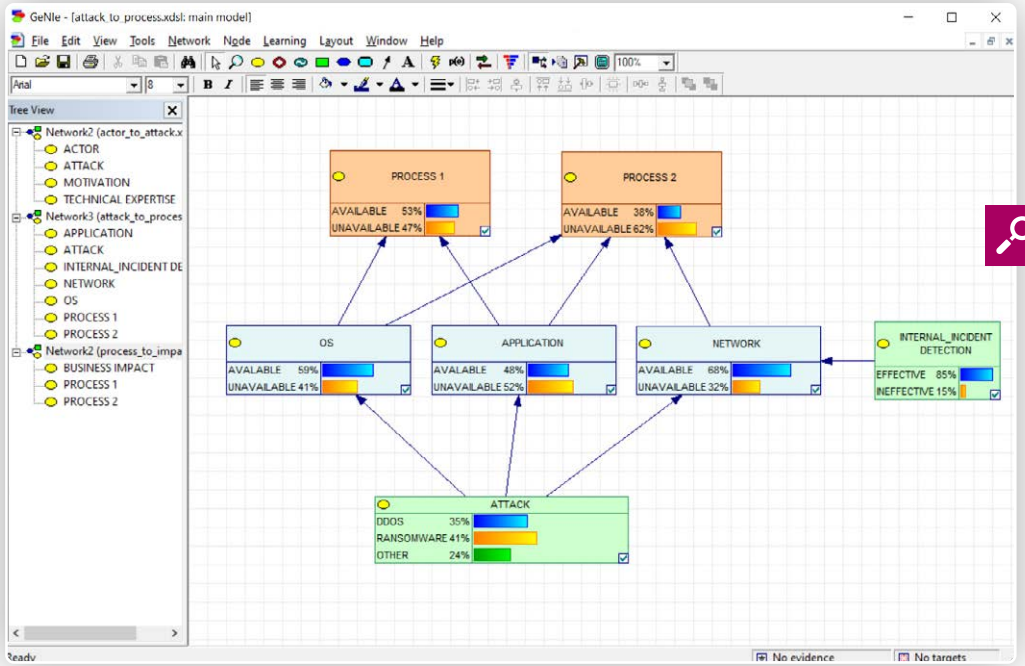


Bijlage 2: BBN voorbeeldmodellen

Een modulaire aanpak

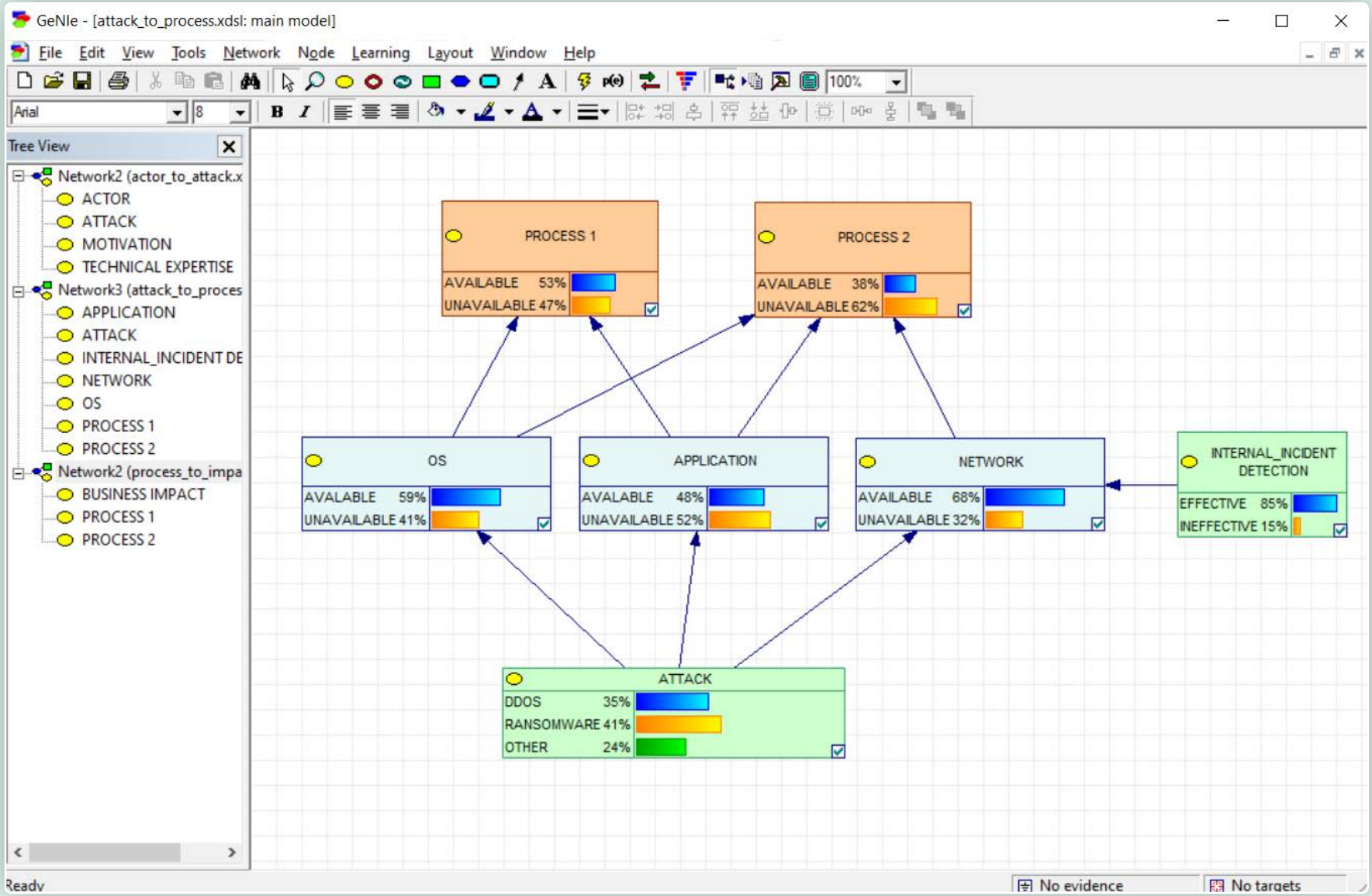
Submodel 2: Aanvalsvector van systemen naar processen
attack_to_process.xdsl | attack_to_process.net

Afhankelijk van de aanvalsvector is er een bepaalde mate van waarschijnlijkheid dat systemen ontregeld worden. Dit voorbeeld maakt een onderscheid tussen een aantal systemen: OS, Applicatie en Netwerk. Wanneer deze door een aanval niet beschikbaar zijn heeft dat consequenties voor de bedrijfsprocessen Process 1 en Process 2.



Kader sluiten

Submodel 2: Aanvalsvector van systemen naar processen

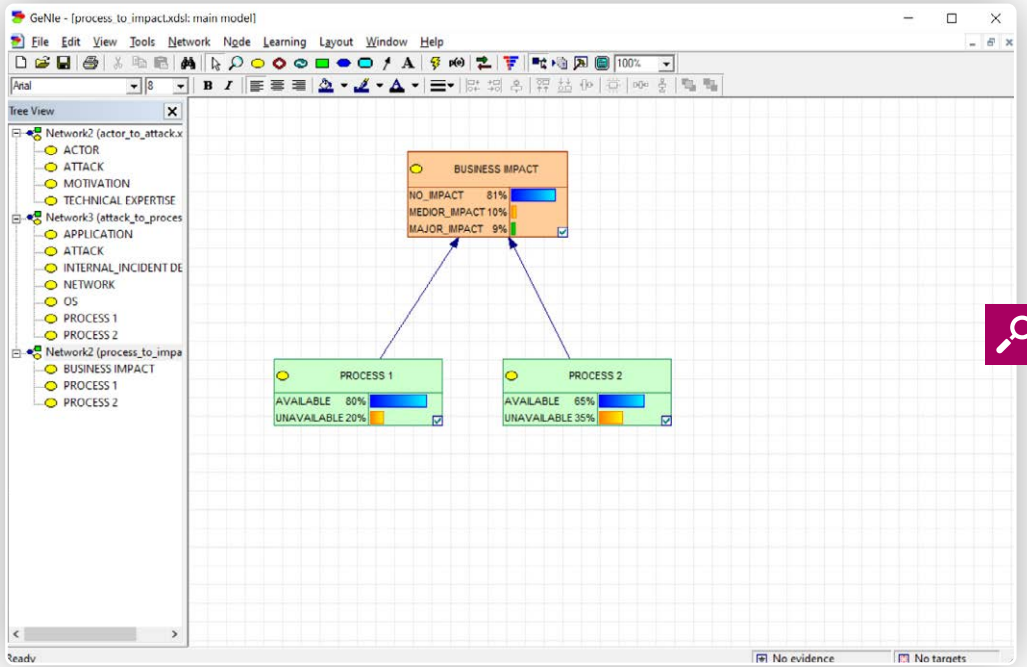


Bijlage 2: BBN voorbeeldmodellen

Een modulaire aanpak

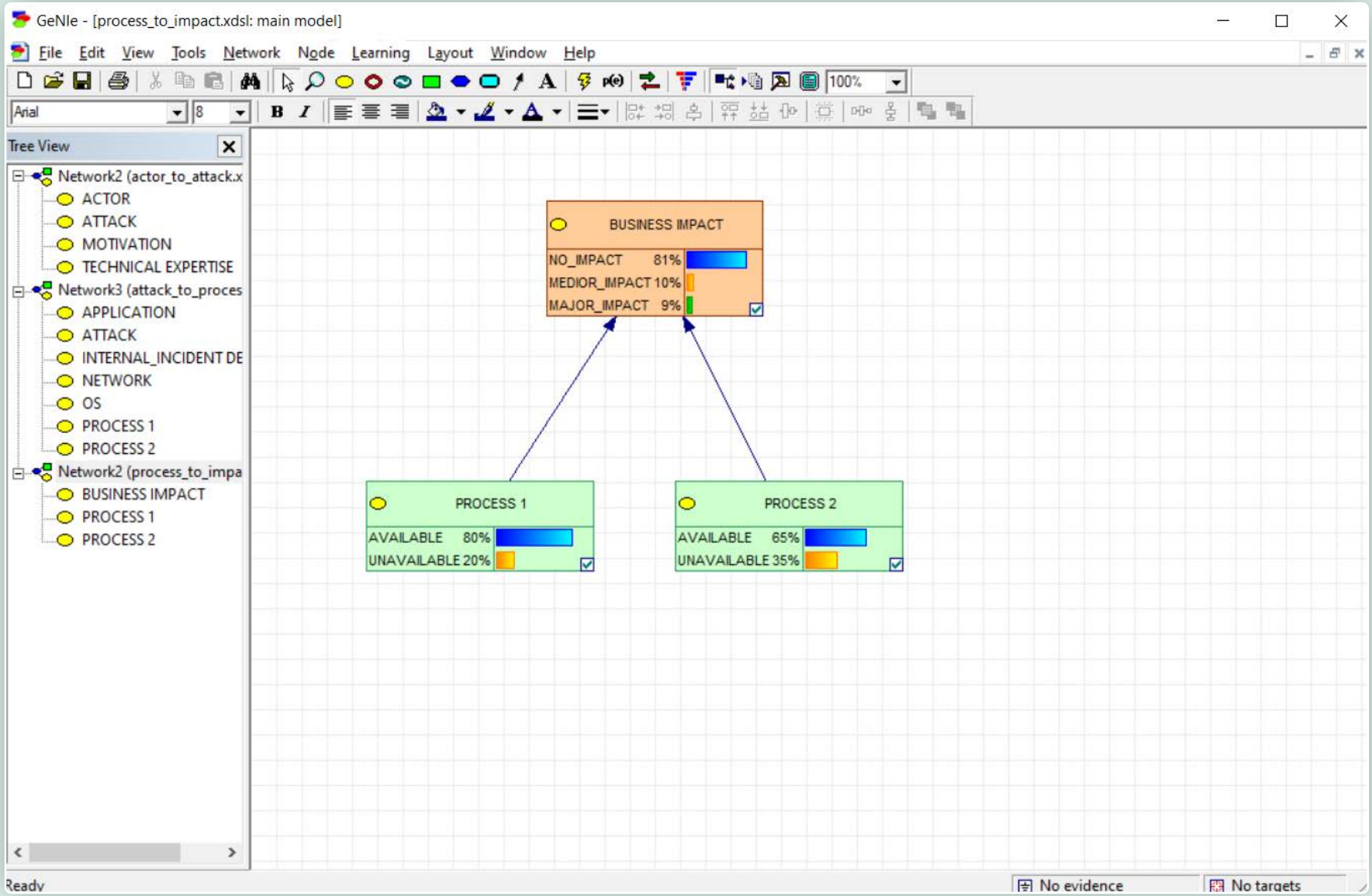
Submodel 3: Processen naar impact
process_to_impact.xdsl | process_to_impact.net

Wanneer bedrijfsprocessen onderbroken worden, kan dat leiden tot een significante negatieve impact voor de organisatie.



Kader sluiten

Submodel 3: Processen naar impact



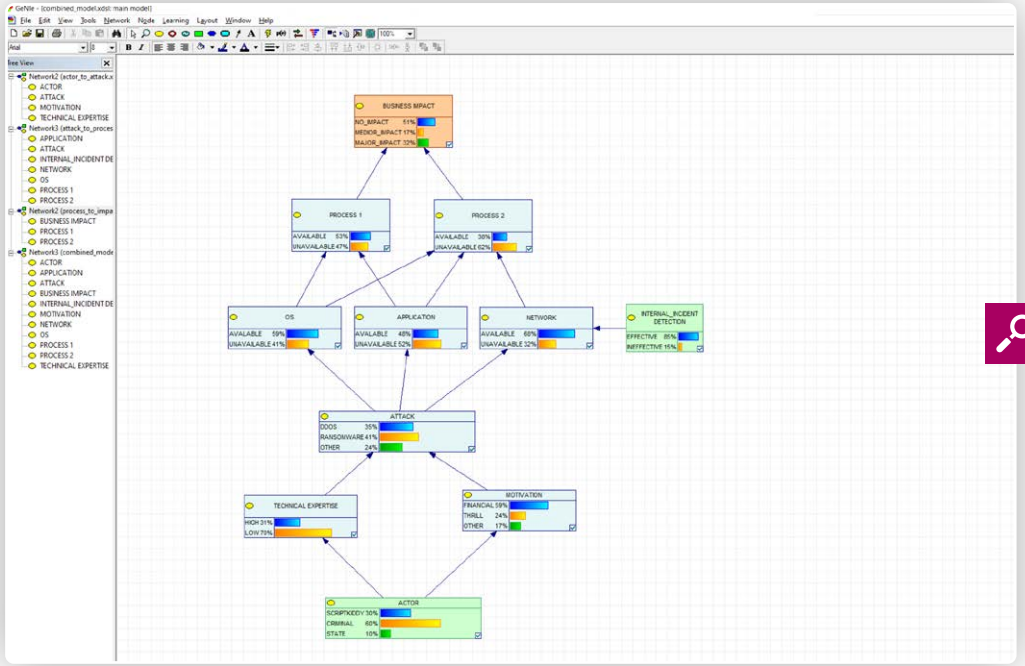
Bijlage 2: BBN voorbeeldmodellen

Een modulaire aanpak

Samengesteld model

combined_model.xdsl | combined_model.net

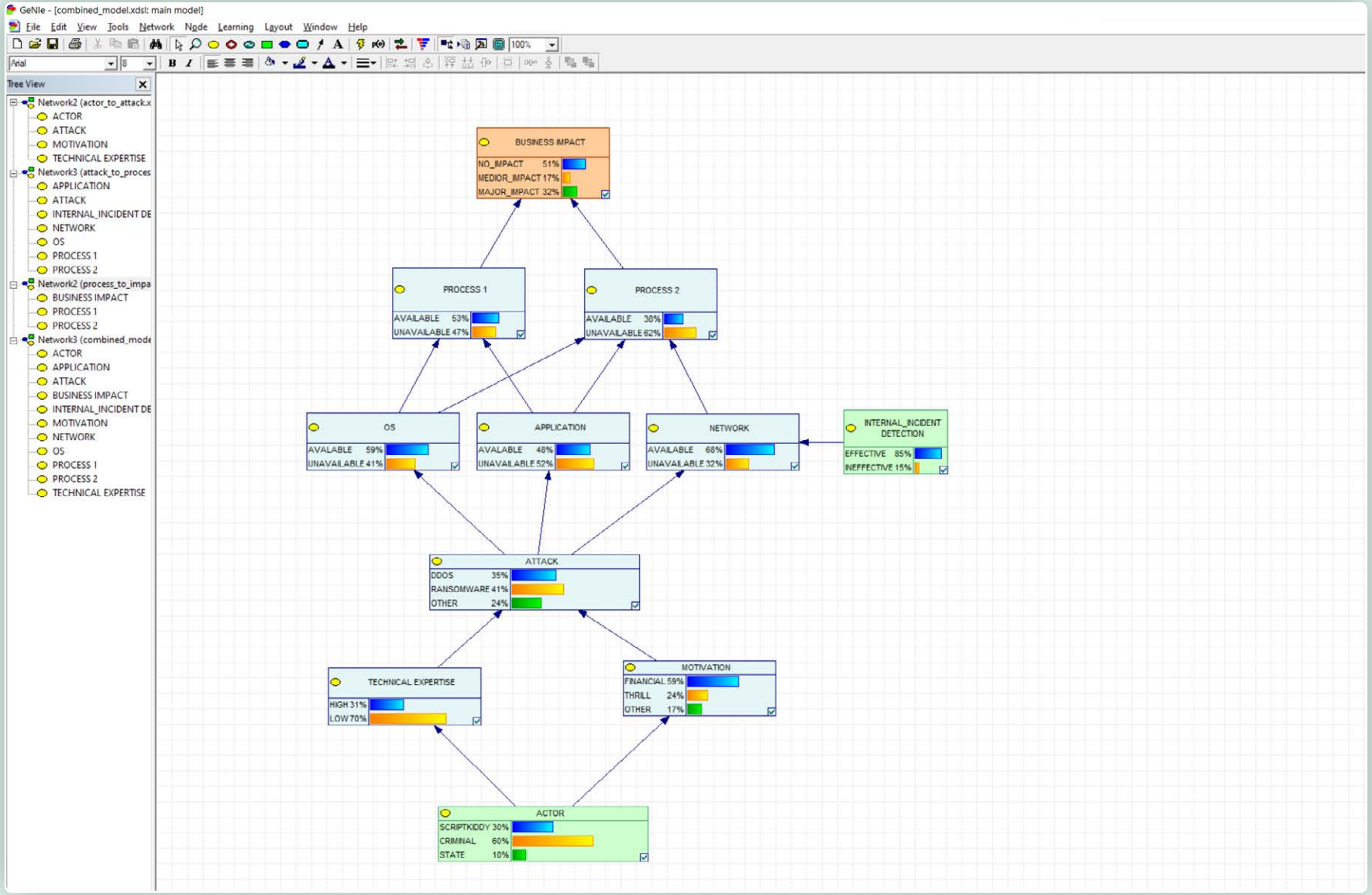
Ten slotte is het mogelijk om de bovenstaande drie deelmodellen te combineren. In het laatste deelmodel zijn Process 1 en Process 2 als input genomen, maar omdat die de uitkomst zijn van het tweede deelmodel, kunnen ze ook door submodel 2 vervangen worden. Daarnaast kan de Attack node in het tweede deelmodel vervangen worden door het eerste deelmodel, omdat die weer de uitkomst is van submodel 1. Zodoende vormen de drie submodellen één algeheel model dat van begin tot eind doorgerekend kan worden.



Terug naar

Kader sluiten

Samengesteld model



Bijlage 2: BBN voorbeeldmodellen

Een modulaire aanpak

Submodelfunctionaliteit in GeNIe
submodel.xdsl | submodel.net

Opmerking: deze functionaliteit is alleen ondersteund met het .xdsl bestandsformaat. Wanneer het bestand wordt opgeslagen als .net blijft het model behouden, maar gaat de indeling in submodellen verloren.

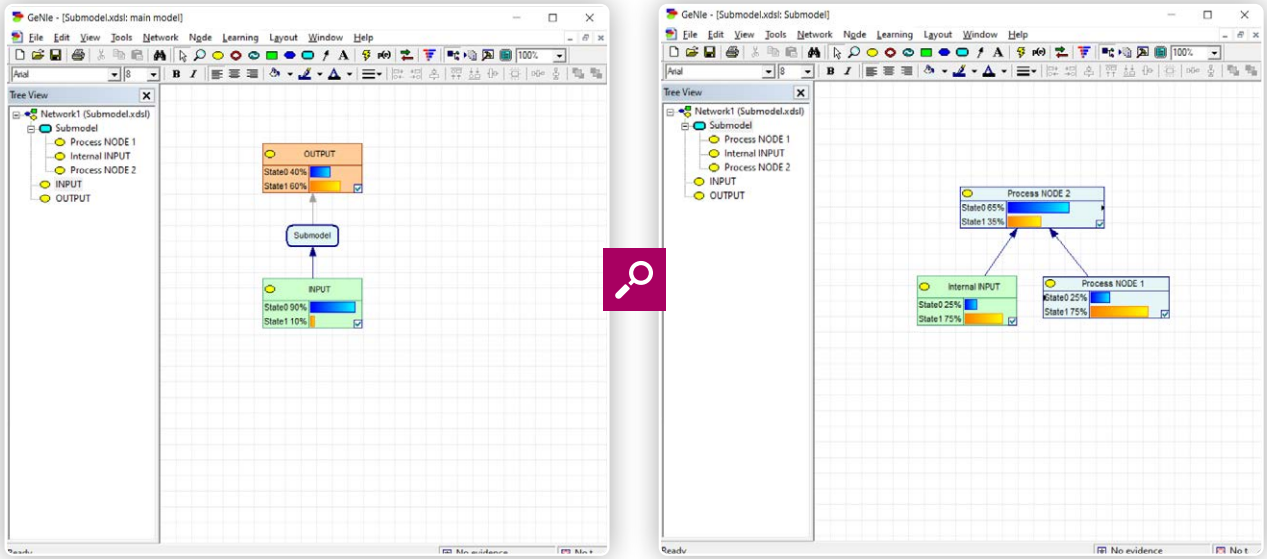
Submodellen veranderen niets aan de werking van het model, maar zijn een manier om overzicht te houden over grotere modellen, en om delen van een model eenvoudig in een ander model te hergebruiken. Submodellen voegen een hiërarchie toe die vergelijkbaar is met de mappenstructuur op een computer. Op het canvas kan dan op hoog niveau een model worden neergezet, waarbij de gedetailleerde berekeningen zijn ondergebracht in de submodules. Iedere submodule bevat als het ware zelf een (klein) model. Nodes binnen een submodel kunnen ook worden verbonden met nodes buiten het submodel of zelfs met nodes in andere submodellen, maar ze hebben een (veronderstelde) samenhang. Hierbij kan gedacht worden aan de uitwerking van een aanvalsvector zoals phishing, wat een 'module' oplevert die voor verschillende risicomodellen relevant kan zijn.

In de linkse figuur (volgende pagina) is het model op hoofdniveau te zien. In deze compacte weergave is een deel van het model geabstraheerd als submodel. De daadwerkelijke invulling van dit submodel is te zien in de figuur rechts. Binnen het submodel is een tweede Input node te zien die onafhankelijk is van het model waarbinnen het

Bijlage 2: BBN voorbeeldmodellen

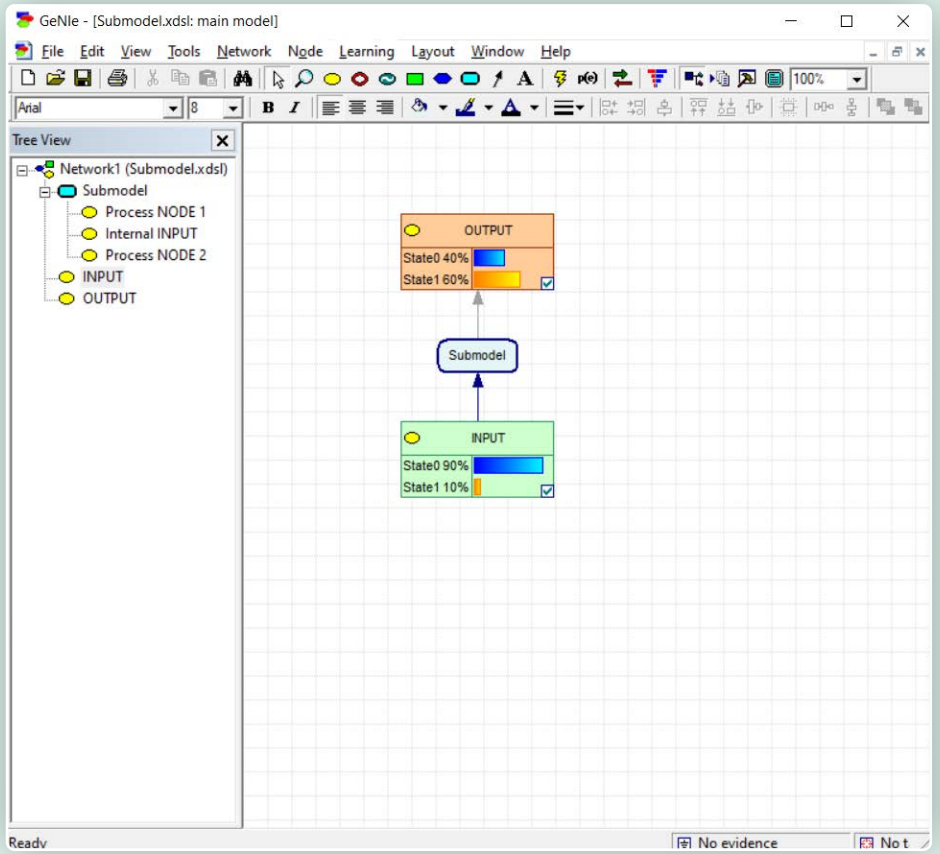
Een modulaire aanpak

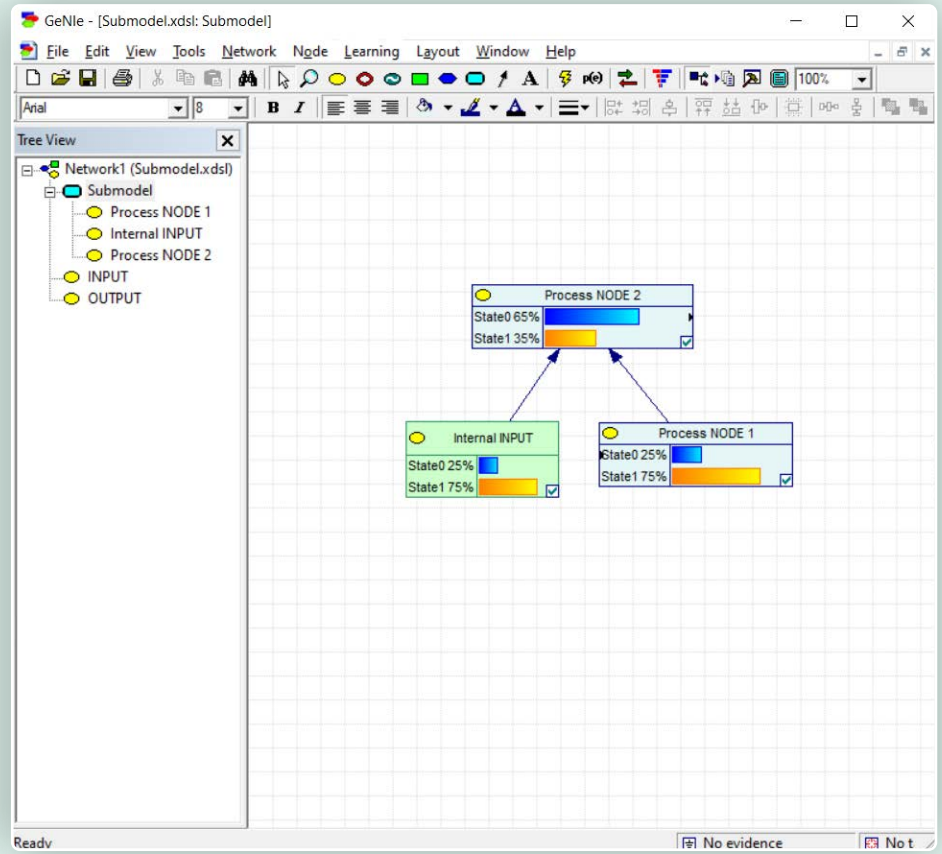
submodel wordt geplaatst, de andere nodes binnen het submodel zijn wel direct en indirect afhankelijk van de Input node buiten het submodel. Tot slot is de bovenste node in het submodel weer verbonden met de Output op hoofdniveau.



Submodelfunctionaliteit in GeNie

Kader sluiten





submodel weer verbonden met de Output op hoofdniveau.

Bijlage 2: BBN voorbeeldmodellen

Enkele overwegingen

BBNs kunnen op verschillende manieren vormgegeven worden. En alhoewel deze keuzes over het algemeen vrij duidelijk zijn, liggen andere overwegingen enigszins genuanceerd of hebben geen enkele consequentie voor het model als geheel. Om enkele nuances van het bouwen van modellen te illustreren, worden hier de afwegingen tussen states en nodes (wordt iets een state van een blok of een blok op zich), en tussen het parallel plaatsen van nodes tegenover in een keten (meerdere directe inputs voor één blok of een indirect effect via een keten van blokken) behandeld.

States of nodes?

states_or_nodes_1.xdsl, states_or_nodes_2.xdsl | states_or_nodes_1.net, states_or_nodes_2.net

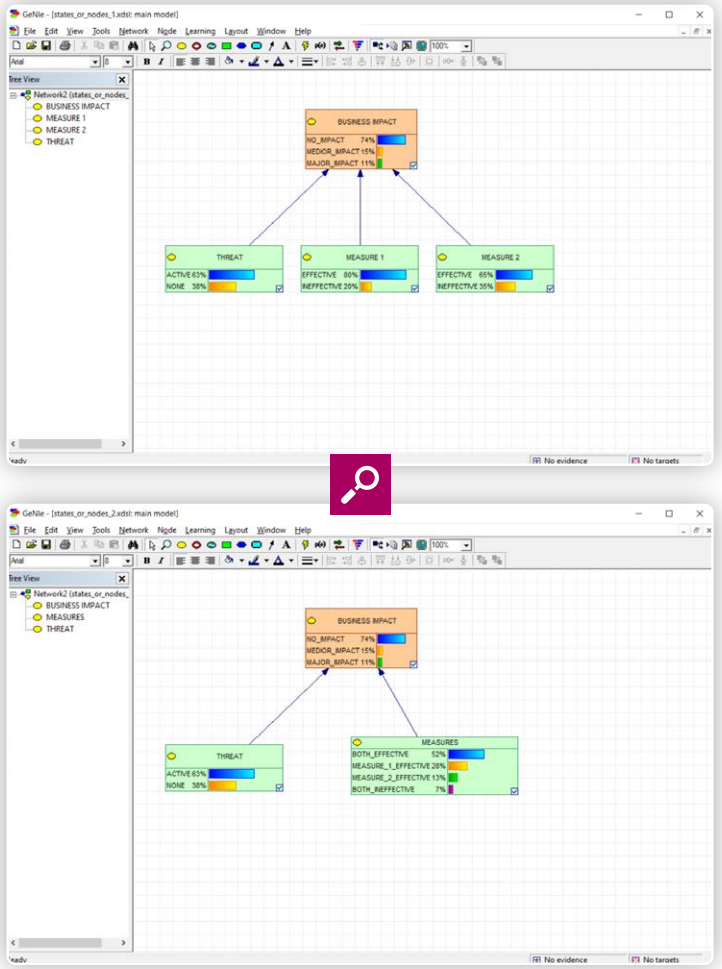
In de voorgaande voorbeelden is een groot aantal nodes te zien met een verscheidenheid aan states. Eén van de afwegingen bij het vormgeven van een BBN is of elementen moeten worden opgenomen als meerdere afzonderlijke nodes, of als states van een enkele node. Beiden zijn valide en er bestaat niet één juist antwoord. Veelal zal één van de twee opties logischer aanvoelen en het is prima om op intuïtie af te gaan; het is altijd mogelijk om achteraf op de indeling terug te komen.

Bijvoorbeeld, voor een dreigingsscenario is het denkbaar dat er meerdere maatregelen genomen kunnen worden die wel of niet effectief zijn. In de bovenste figuur hieronder zijn twee

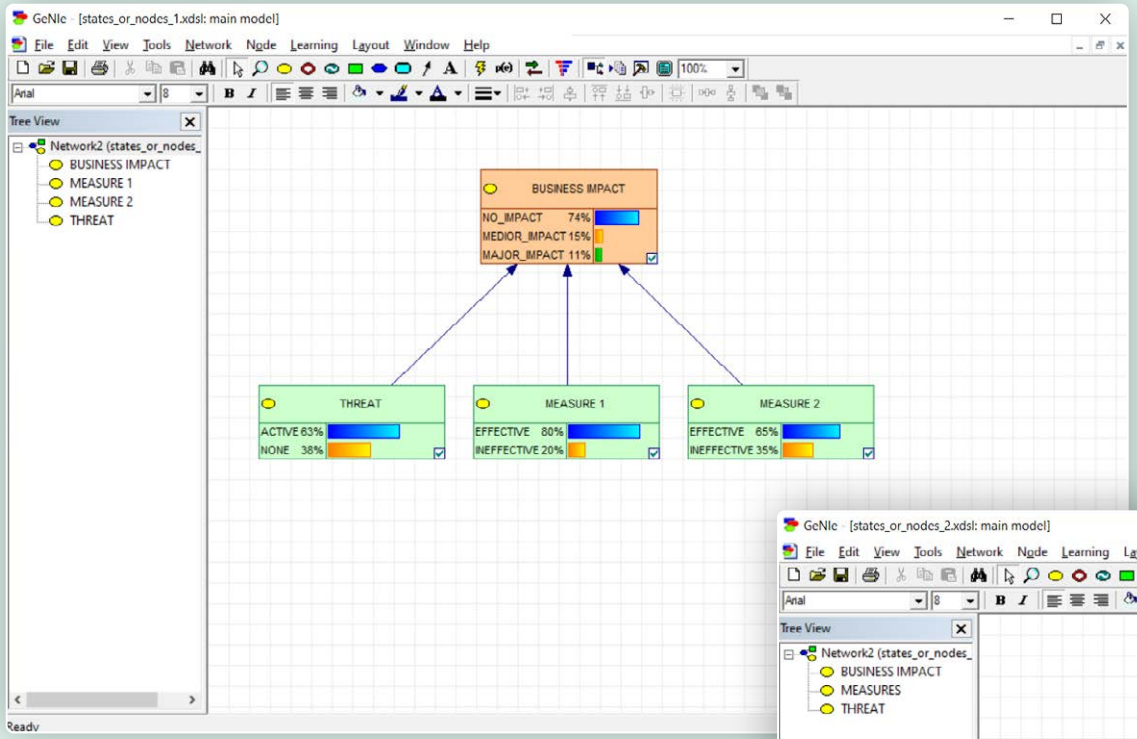
Bijlage 2: BBN voorbeeldmodellen

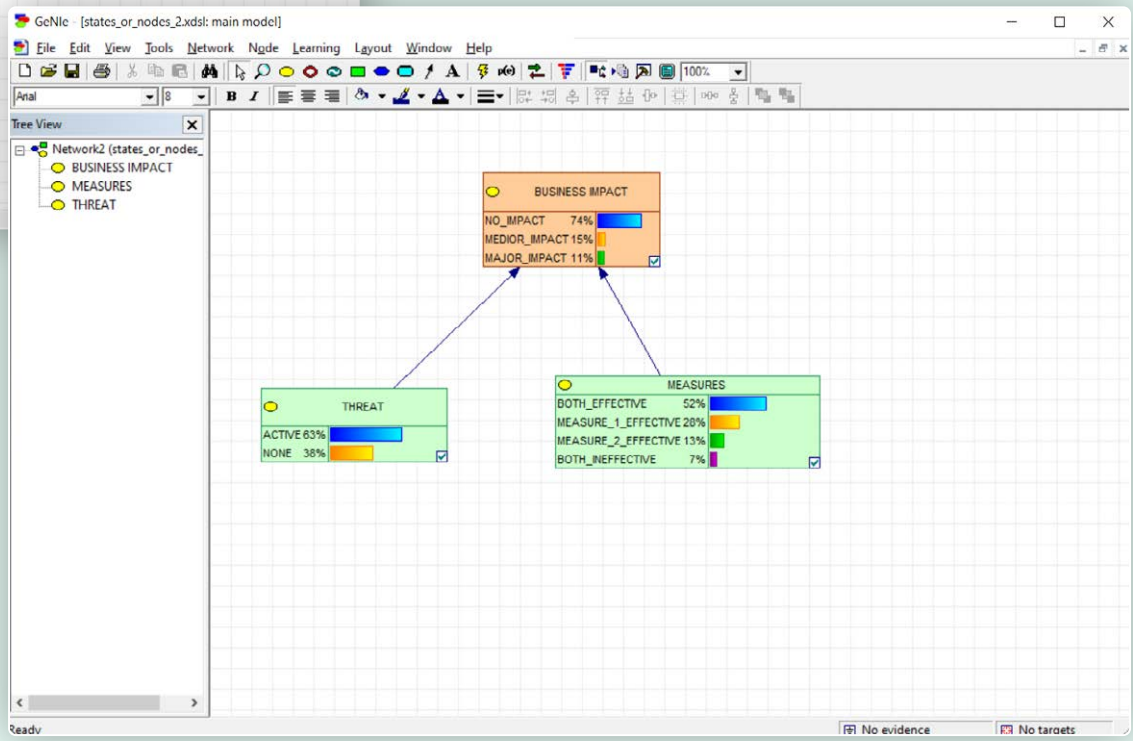
Enkele overwegingen

maatregelen als afzonderlijke nodes in het model opgenomen. De onderste figuur is equivalent aan de bovenste maar heeft één MEASURES node die een kanstabel bevat met waarschijnlijkheden voor de verschillende combinaties van de effectiviteit van maatregelen 1 en 2. Het is aan de ontwerper van het model om af te wegen welke optie het duidelijkst en het meest werkbaar is. Bij een grotere hoeveelheid maatregelen kan het bijvoorbeeld handiger zijn om de maatregelen in het model gescheiden te houden zodat de kanstabellen klein en overzichtelijk blijven, maar ten koste van meer blokken en verbindingen in het model.



Kader sluiten





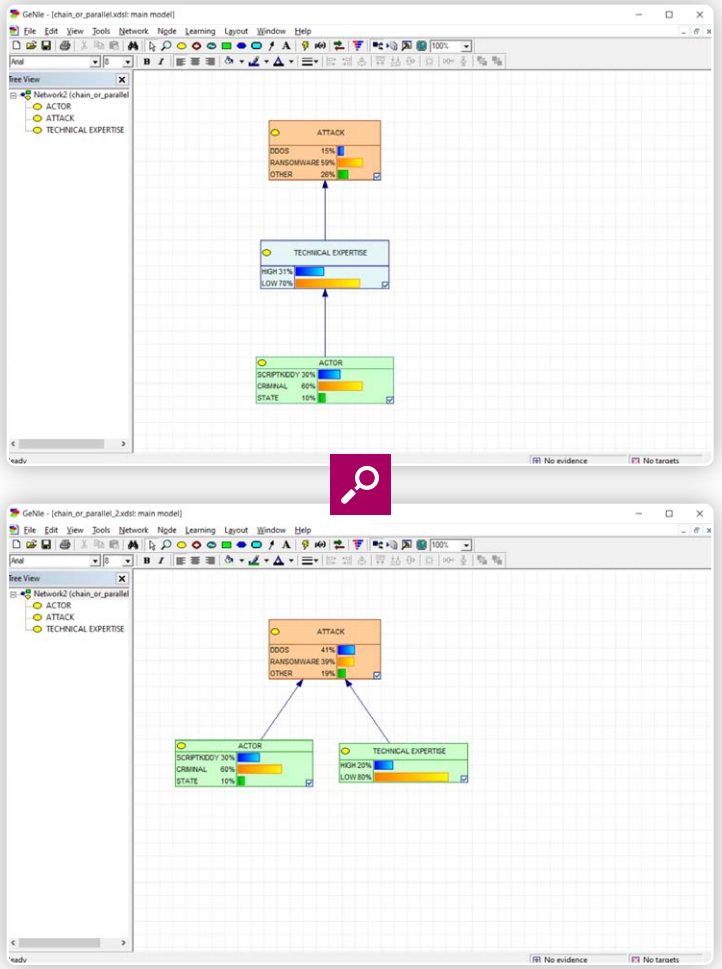
Voorbeelden opties tussen nodes of states

Bijlage 2: BBN voorbeeldmodellen

Enkele overwegingen

Keten of parallel?

chain_or_parallel_1.xdsl, chain_or_parallel_2.xdsl | chain_or_parallel_1.net, chain_or_parallel_2.net



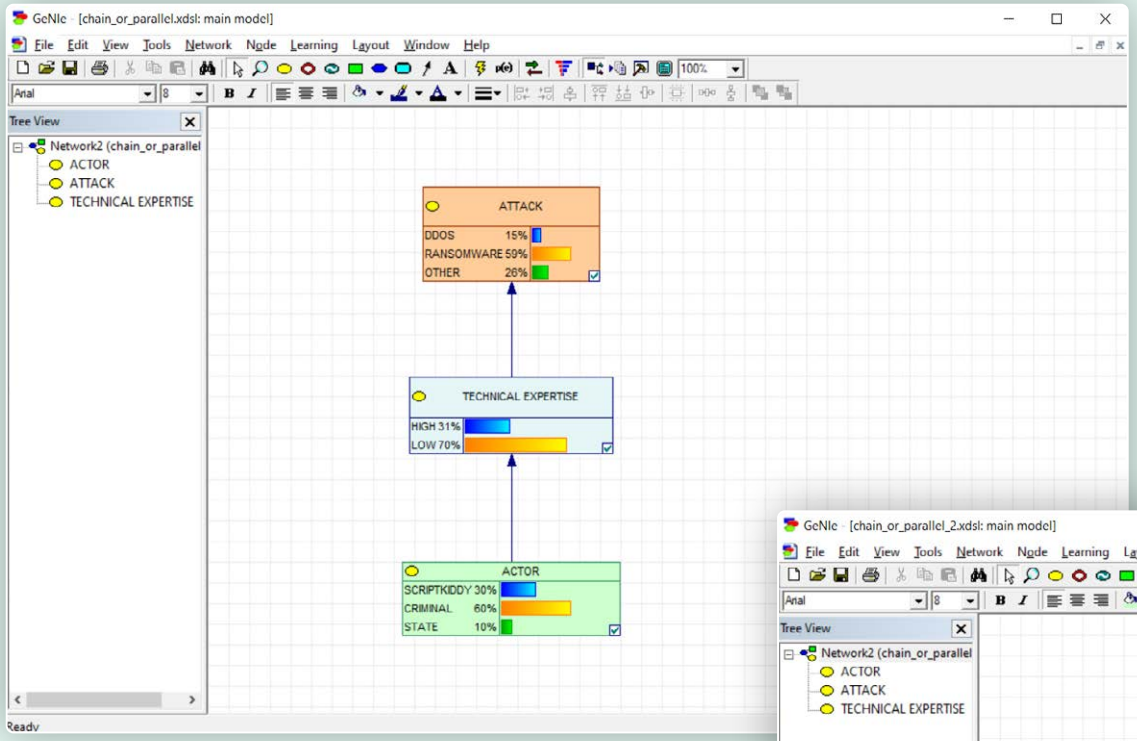
Een andere overweging is of nodes in een keten verbonden zijn, of dat meerdere nodes gezamenlijk de input vormen voor een volgende node. De onderstaande modellen bevatten dezelfde drie nodes maar met een verschillende ordening. In de bovenste figuur zijn de nodes in een keten geplaatst. Het idee hierbij is dat de aanvalsvector geïnformeerd wordt door de expertise van de aanvaller, en deze is weer afhankelijk van het type actor. In de onderste figuur zijn zowel Actor als Technical Expertise de directe input voor de Attack node. Het idee hierbij is dat er (deels) onafhankelijke informatie bestaat over de expertise achter de aanval en het type aanvaller. Het lijkt logisch hierin enig onderscheid te willen maken, want het is aannemelijk dat

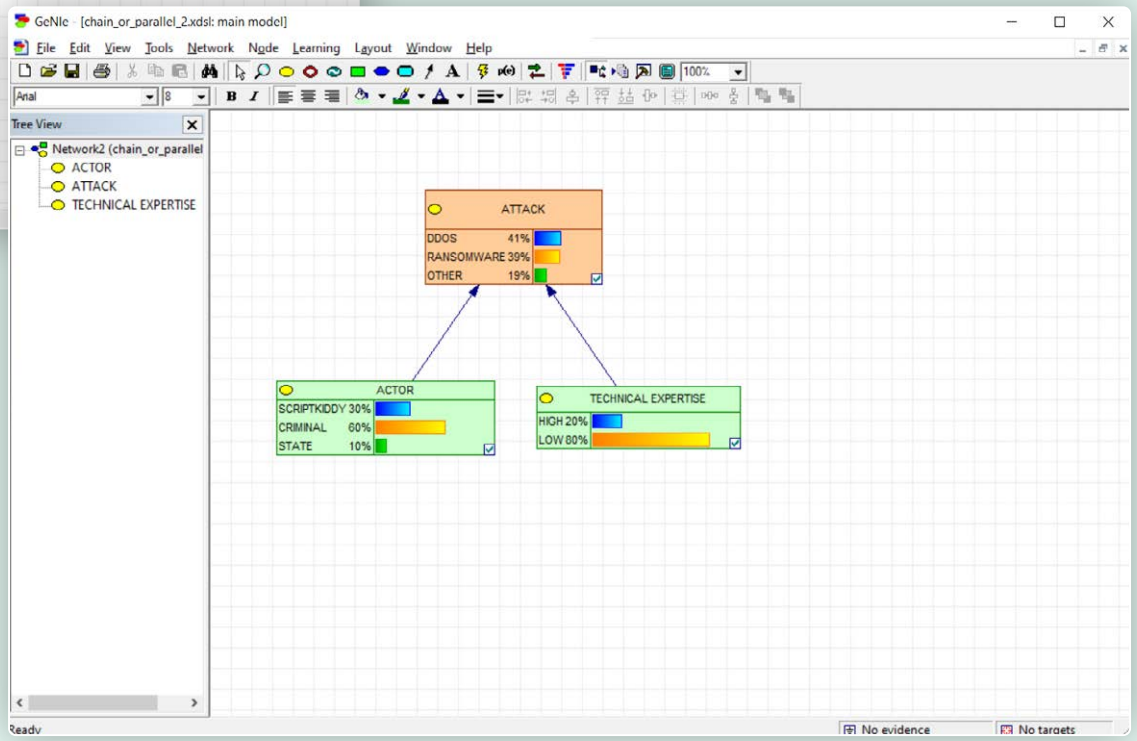
Bijlage 2: BBN voorbeeldmodellen

Enkele overwegingen

een crimineel en een script kiddy verschillende soorten aanvallen uit zullen voeren (in principe is dit mogelijk terug te herleiden naar een verschil in motivatie en kan het dan zinvol zijn een opzet te kiezen zoals in Submodel 1). Wederom hebben beide opties bestaansrecht, maar in dit geval is er een wezenlijk verschil in betekenis en heeft de keuze gevolgen voor de werking van het model.

Kader sluiten



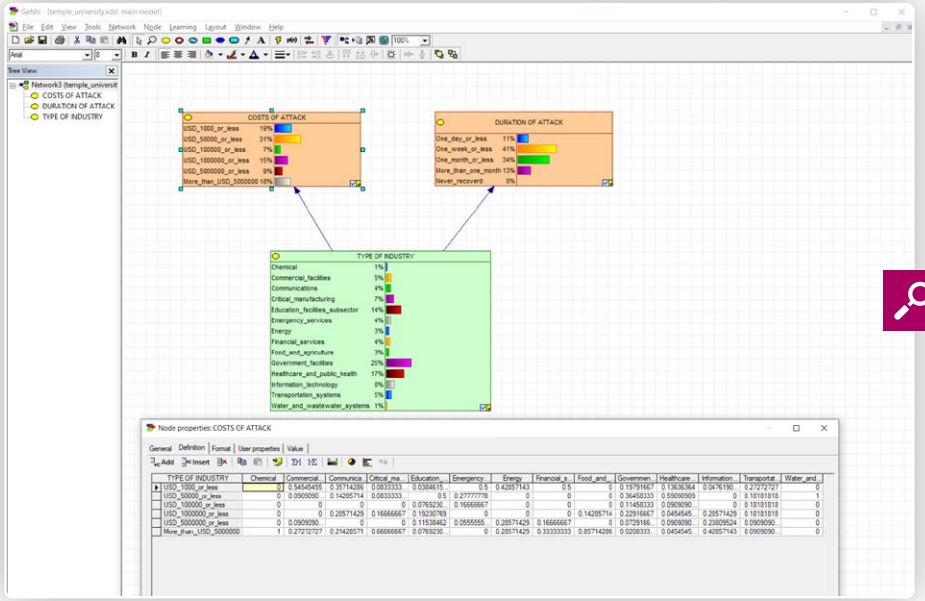


Voorbeeld nodes in een keten of parallel

Bijlage 2: BBN voorbeeldmodellen

Gebruik van data bij invullen kanstabellen

temple_university.xdsl, queensland_attack.xdsl | temple_university.net, queensland_attack.net



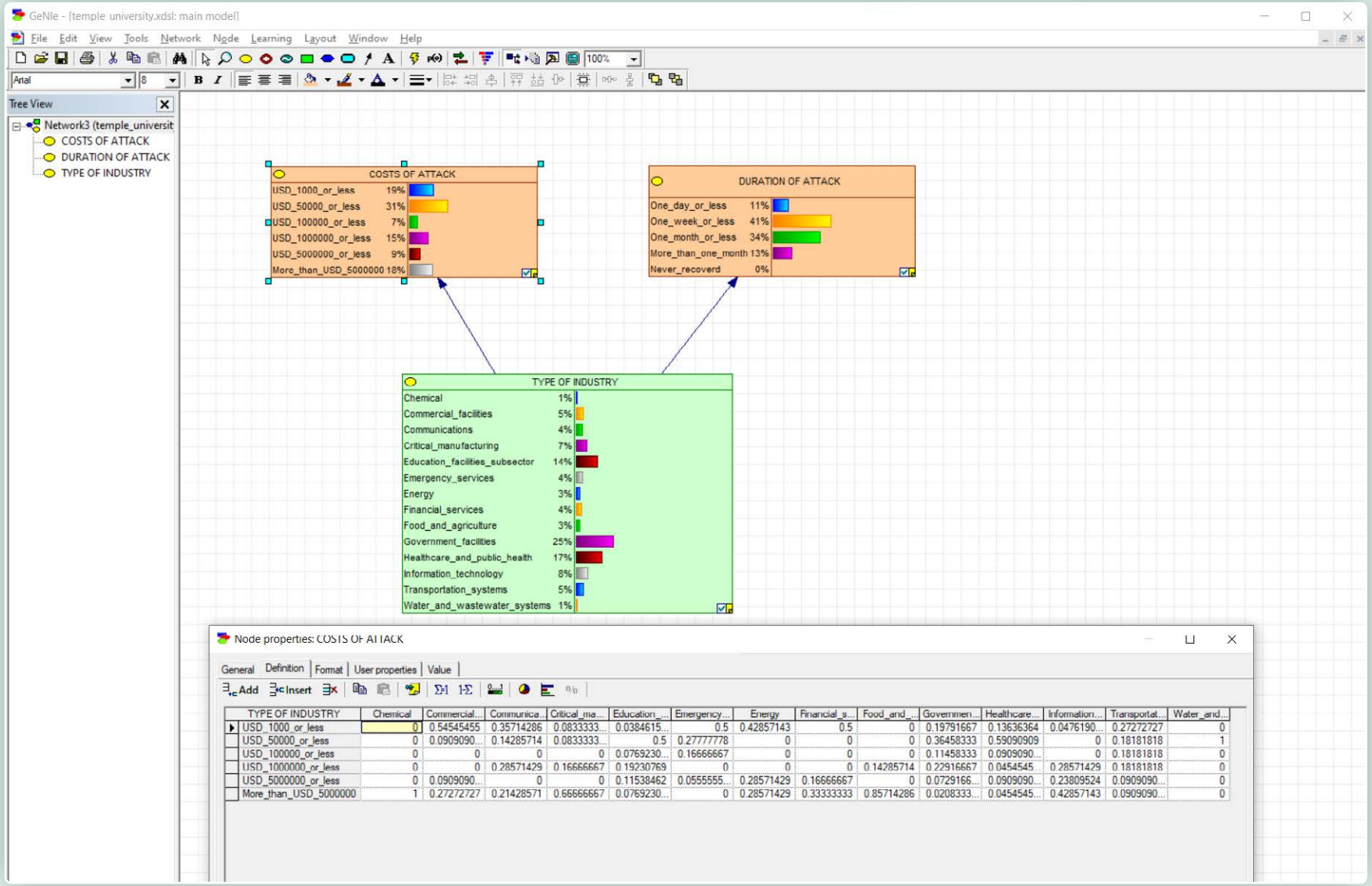
De voorbeelden tot dusver zijn ingevuld met gefingeerde data, maar uiteindelijk is het uiteraard de bedoeling om met echte cijfers te werken. Deels zal daarbij vertrouwd moeten worden op de inschattingen van experts, maar idealiter is het tenminste deels mogelijk om het model in te vullen met informatie uit betrouwbare bronnen. Historische gegevens en trends kunnen hiervoor een goede basis bieden.

Om te illustreren hoe kanstabellen kunnen worden ingevuld op basis van echte data zijn er enkele voorbeelden gemaakt gebaseerd op de Ransomware Repository van Temple University [9] en de cyberaanval-dataset van Queensland University [8]. De Ransomware Repository van Temple University bevat data over cyberaanvallen tegen een verscheidenheid aan bedrijven vanuit verschillende industrieën. In deze dataset kan er onderscheid gemaakt worden tussen de soorten getroffen industrieën, de gemiddelde kosten en de gemiddelde duur van de aanval. Deze data kan vervolgens worden uitgesplitst om te komen tot kanstabellen voor de Costs of Attack en Duration of Attack nodes in de figuur hierboven.

Terug naar

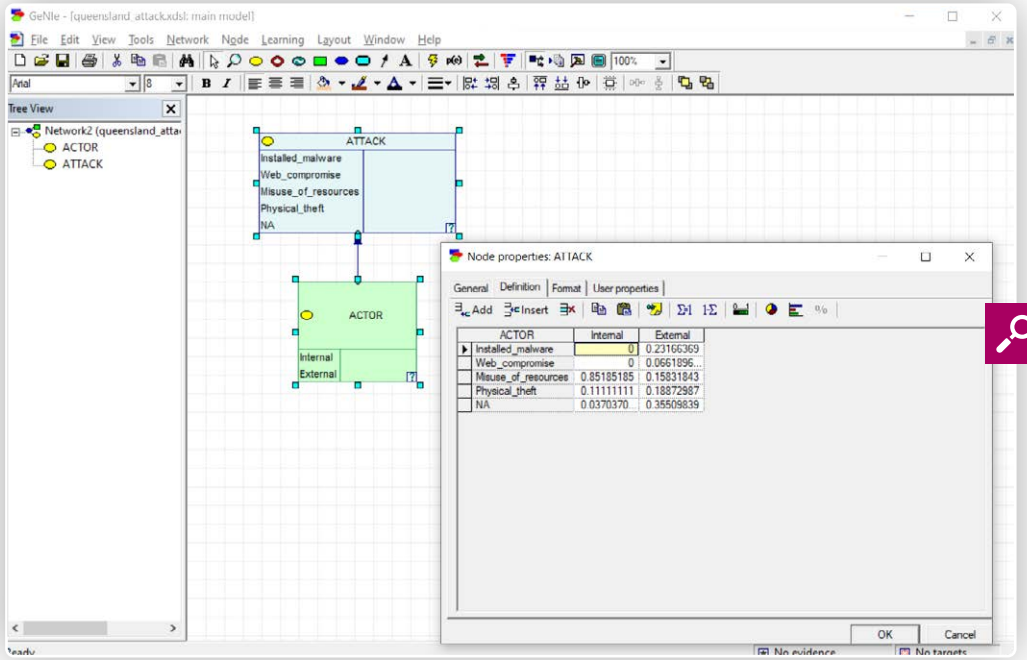
Kader sluiten

Data uit de Ransomware Repository van Temple University



Bijlage 2: BBN voorbeeldmodellen

Gebruik van data bij invullen kanstabellen

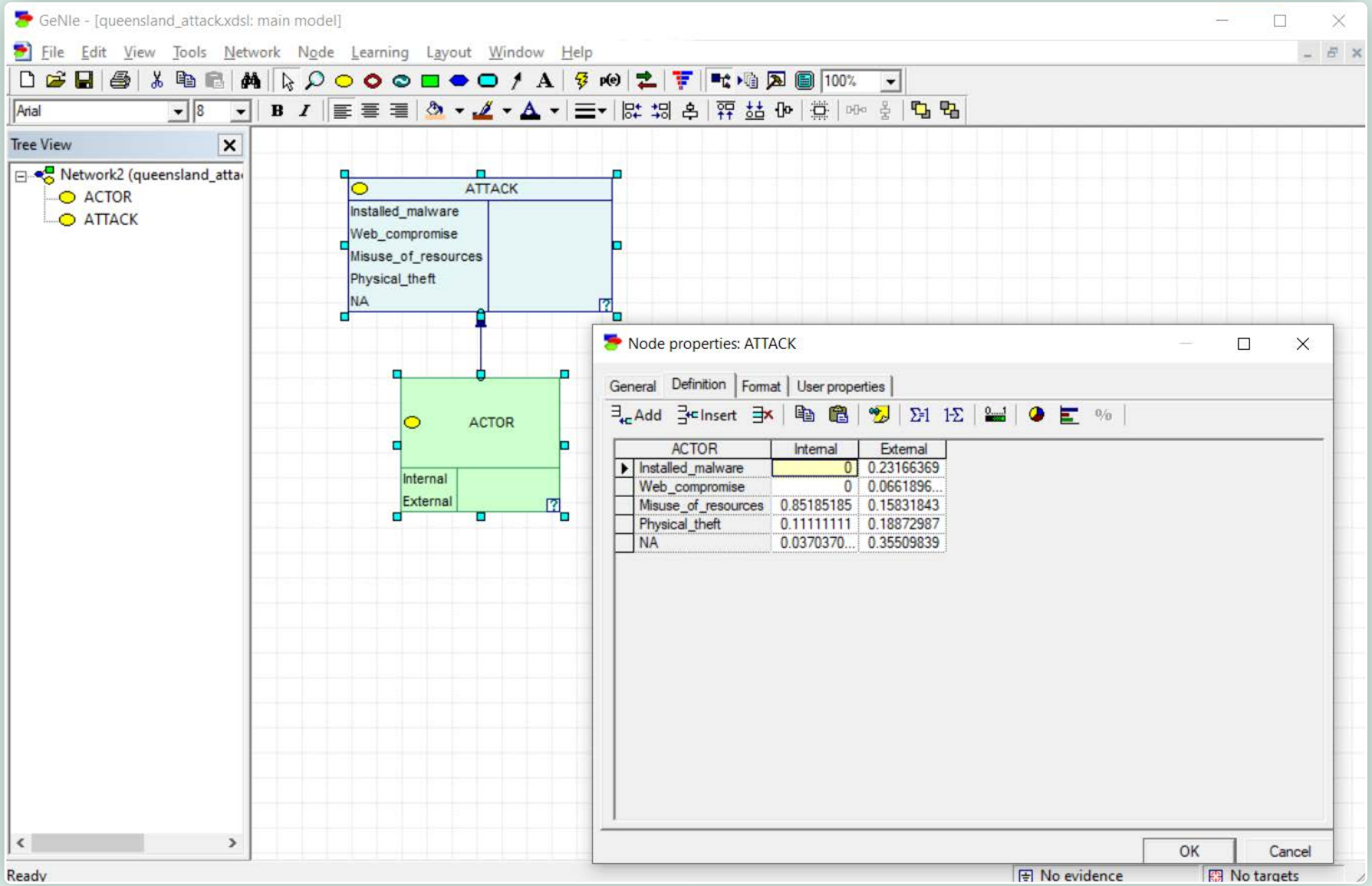


Verder bevat de cyberaanvaldataset van Queensland University een grote lijst van cyberaanvallen, met per aanval informatie over de aanval zelf en over het getroffen bedrijf. Hieruit kunnen verschillende soorten informatie gehaald worden die voor een model relevant zouden kunnen zijn, bijvoorbeeld een onderscheid tussen interne en externe actoren. Dit maakt het mogelijk om een kanstabel op te stellen voor de aanvalsvector op basis van het soort actor. Wanneer er op basis van eigen inschatting of andere informatie cijfers beschikbaar zijn voor de incidentfrequentie intern/extern, kan er beter ingeschat worden welke aanvalsvector zorgwekkend is.

Terug naar

Kader sluiten

Cyberaanval-dataset van Queensland University



Referenties / bronnen

[1] Langenkamp, van Egmond, Klaver, Kwantificering cyberrisico's: rapportage 2020, december 2020
[2] Verdaasdonk, Klaver, Langenkamp, TNO 2022 R10535, Kwantificering cyberrisico's: rapportage 2021 (P2108), April 2022
[3] TNO rapport, TNO 2022 R10535, Kwantificering cyberrisico's: rapportage 2021 (P2108), April 2022
[4] GeNIe modeler: https://www.bayesfusion.com/genie/
[5] Philipson et al., Alternative Initial Probability Tables for Elicitation of Bayesian Belief Networks, Math. Comput. Appl. 2021, 26, 54, https://doi.org/10.3390/mca26030054
[6] Philipson et al., A Framework for quantifying cyber security risks, Cyber Security: A Peer-Reviewed Journal, 4 (4), 302-316 (2021)
[7] Wolthuis et al., A Framework for quantifying cyber security risks, Cyber Security: A Peer-Reviewed Journal, 4 (4), 302-316 (2021)
[8] Tsen, E., Ko, R., & Slapnicar, S. (2004–2020). Dataset of data breaches and ransomware attacks over 15 years from 2004 [Dataset]. The University of Queensland. https://doi.org/10.14264/dfe5027
[9] Rege, A. (2013–2021, november). Critical Infrastructures Ransomware Attacks (CIRWAs) Incident Dataset (11.7) [Dataset]. Temple University College of Liberal Arts. https://sites.temple.edu/care/ci-rw-attacks/

Colofon

Deze handleiding "Aan de slag met het kwantificeren van cyberrisico's" is gemaakt door TNO in samenwerking met het Nationaal Cyber Security Centrum, en opgemaakt door Coek Design in opdracht van TNO en het Nationaal Cyber Security Centrum.

Auteurs:
Dr. ir. Peter Langenkamp
Willem Verdaasdonk
Dr. Marieke Klaver
Naomi Keja MSc
Niels Brink

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

TNO innovation for life

Voor vragen of meer informatie kan je contact opnemen met Gwen Jansen-Ferdinandus van TNO (gwen.ferdinandus@tno.nl) of met het NCSC (research@ncsc.nl)