Veiligheidsregio's en de voorbereiding op cyberincidenten

Een onderzoek naar barrières en interventies om de voorbereiding van veiligheidsregio's op de (gevolg)bestrijding van interne en externe cyberincidenten te verbeteren.

Bachelorscriptie E.T. Brouwer

Integrale Veiligheidskunde Hogeschool Saxion
In opdracht van Het Instituut Fysieke Veiligheid.

Begeleiding Saxion: dr. Y.A. van Houten & G.L. van Ginkel MSc
Begeleiding IFV: J. Domrose MSc

Juni 2021

Colofon

Ellis Brouwer (2021). *Veiligheidsregio's en de voorbereiding op cyberincidenten. Een onderzoek naar barrières en interventies, om de voorbereiding van veiligheidsregio's op de (gevolg)bestrijding van interne en externe cyberincidenten te verbeteren.* Hengelo

Opdrachtgever:	Lectoraat Crisisbeheersing Instituut Fysieke Veiligheid
Contactpersoon:	Ellis Brouwer – student 450843
Contactinformatie:	Ellis.Brouwer@ifv.nl, 450843@student.saxion.nl
Titel:	Veiligheidsregio's en de voorbereiding op cyberincidenten
Datum:	4 juni 2021
Status:	Definitief
Auteur:	E.T. Brouwer
Begeleiding IFV:	J. Domrose MSc – junior onderzoeker
Begeleiding Hogeschool Saxion:	dr. Y.A. van Houten – hoofddocent/onderzoeker
	G.L. van Ginkel MSc – docent/onderzoeker

Voorwoord

Trots presenteer ik u mijn scriptie, die ik in opdracht van het Instituut Fysieke Veiligheid heb geschreven: “Veiligheidsregio’s en de voorbereiding op cyberincidenten”. Ten aanzien van deze scriptie heb ik onderzoek gedaan naar barrières binnen veiligheidsregio’s en de mogelijkheden voor interventies, om de voorbereiding van veiligheidsregio’s op de (gevolg)bestrijding van interne en externe cyberincidenten te verbeteren.

De scriptie is geschreven in het kader van mijn afstuderen aan de opleiding Integrale Veiligheidskunde aan Hogeschool Saxion te Enschede. Het Instituut Fysieke Veiligheid (IFV) is de opdrachtgever van dit onderzoek en heeft mij tevens van februari 2021 tot en met juni 2021 opgenomen als stagiair. Naast het onderzoek voor deze scriptie heb ik ook mee mogen werken met lopende onderzoeken van het lectoraat Crisisbeheersing, waarvan het onderzoek naar cyberkennis en -kunde binnen veiligheidsregio’s het meest prominente onderzoek is.

Het instituut Fysieke Veiligheid heeft mij volledig vrij gelaten in de keuze voor mijn onderzoeksrichting en onderzoeksopzet voor deze scriptie. Het onderwerp en de aanpak heb ik dus zelf gekozen en ontworpen, waarbij ik in een vroeg stadium ondersteuning heb gekregen van de leden van het Lectoraat Crisisbeheersing van het IFV en de begeleiders van Saxion Hogeschool. Ook tijdens het verzamelen van data en het werven van respondenten, wat tijdens de coronacrisis niet gemakkelijk was, hebben zij mij gesteund en geadviseerd.

Voor alle ondersteuning, feedback, mogelijkheden en gezelligheid wil ik daarom het lectoraat Crisisbeheersing van het IFV bedanken, maar met name mijn praktijkcoach Jana Domrose. De afgelopen maanden heb ik ontzettend veel geleerd en ik kijk met veel enthousiasme terug op deze periode. Daarom ook dank aan alle collega’s van het IFV voor het warme welkom. Ook wil ik alle respondenten bedanken voor hun belangrijke bijdrage aan dit onderzoek. Zonder deze mensen en hun uitgebreide reacties had ik dit onderzoek nooit kunnen voltooien.

Tevens wil ik ook meneer Van Houten en mevrouw Van Ginkel heel erg bedanken voor de feedback, sturing en fijne begeleiding. Het contact verliep erg prettig en de feedback heb ik als nuttig, bruikbaar en leerzaam ervaren.

Tot slot, dank aan allen die mij hebben gesteund, van wie ik raad heb gekregen of met wie ik heb kunnen sparren over mijn onderzoek. Mijn dank gaat hiervoor uit naar mijn familie, vrienden, studiegenoten, stagegenoten en collega’s.

Ik wens u veel plezier met het lezen van deze scriptie en ik hoop u te boeien en verrassen met de, in mijn ogen razend interessante, resultaten en conclusies.

Ellis Brouwer

Hengelo, 31 mei 2021

Samenvatting

De dreigingen en kwetsbaarheden uit het digitale domein nemen toe en worden steeds meer zichtbaar door het toenemende aantal cyberincidenten. De voorbereiding op deze digitale crisistypen is voor veiligheidsregio's een uitdaging, waardoor de weerbaarheid van veiligheidsregio's in verhouding achterblijft met de dreigingen en kwetsbaarheden. Veiligheidsregio's zijn (nog) zoekende naar een geschikte wijze om zich voor te bereiden op interne en externe cyberincidenten. Met interne cyberincidenten worden cyberincidenten binnen de eigen organisatie van veiligheidsregio's bedoeld en met externe cyberincidenten worden de cyberincidenten binnen de regio, het verzorgingsgebied, van veiligheidsregio's bedoeld.

De doelstelling van dit onderzoek is het aanreiken van interventies die zijn gericht op de ervaren barrières, om de voorbereiding van veiligheidsregio's op de (gevolg)bestrijding van interne en externe cyberincidenten te verbeteren. Om dit te realiseren is de volgende hoofdvraag opgesteld:

"Op welke manier kan de voorbereiding van veiligheidsregio's, op de (gevolg)bestrijding van interne en externe cyberincidenten, worden verbeterd?"

Om deze vraag te beantwoorden is gebruik gemaakt van een getrianguleerd ontwerp, waarbij zowel kwalitatieve en kwantitatieve dataverzamelingsmethoden zijn toegepast. Zo zijn de kwalitatieve gegevens middels interviews met medewerkers van veiligheidsregio's, leden van vakgroepen en andere experts verzameld. De kwantitatieve gegevens zijn middels twee enquêtes verzameld. Hierbij zijn de leden van de VR-ISAC bevraagd over de voorbereiding op de bestrijding van interne cyberincidenten en zijn de leden van de werkgroep digitale ontwrichting en cyber bevraagd over de voorbereiding op de gevolgbestrijding van externe cyberincidenten. Daarnaast is ook gebruik gemaakt van deskresearch, waarbij relevante literatuur met betrekking tot interventiemogelijkheden volgens de sneeuwbalmethode is verzameld.

Met de uitkomsten van het onderzoek wordt een beter beeld geschetst van de mate waarin veiligheidsregio's zich bewust zijn van de dreigingen uit het digitale domein. Daarnaast wordt duidelijk welke capaciteit-, motivatie- en gelegenheids- gerelateerde barrières veiligheidsregio's ervaren bij de voorbereiding op de (gevolg)bestrijding van interne en externe cyberincidenten. Tot slot zijn deze barrières gekoppeld aan bijpassende en gerichte interventies, die veiligheidsregio's kunnen helpen bij de voorbereiding op de (gevolg)bestrijding van interne en externe cyberincidenten.

Uit de antwoorden op de vragenlijsten in de interviews en enquêtes bleek onder andere dat de barrières die werden/worden ervaren bij de voorbereiding op interne cyberincidenten vooral liggen bij de motivatie en dat de barrières die werden/worden ervaren bij de voorbereiding op externe cyberincidenten vooral liggen bij de samenwerking.

Op basis hiervan wordt voor de verbetering van de voorbereiding op interne cyberincidenten onder andere aanbevolen om een verdiepend onderzoek uit te voeren naar de achterliggende oorzaken van de motivatie van veiligheidsregio's voor het al dan niet uitvoeren van voorbereidend gedrag. Voor het verbeteren van de voorbereiding op de gevolgbestrijding van externe cyberincidenten wordt onder andere geadviseerd om een regionaal en landelijk netwerk op te zetten, waarin een combinatie wordt gemaakt van technische kennis en vaardigheden en 'crisiskennis en -vaardigheden'.

Inhoud

Separate documenten

Bijlage 11 Uitwerkingen, fragmenten en coderingen interviews (Excel)

Figurenlijst

Tabellenlijst

Afkortingen

BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CERT	Computer Emergency Respons Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COT	Instituut voor Veiligheids- en Crisismanagement
CSBN	Cybersecuritybeeld Nederland
EPPM	Extended Parralel Processing model
ICT	Informatie- en Communicatietechnologie
IFV	Instituut Fysieke Veiligheid
ISAC	Information Sharing and Analysis Center
J&V	Ministerie van Justitie en Veiligheid
KOOP	Kennis- en exploitatiecentrum Officiële Overheidspublicaties
LOCC	Landelijk Operationeel Coördinatiecentrum
NCSC	Nationaal Cyber Security Center
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
PMT	Protectie Motivatie Theorie
RCDV	Raad van Commandanten en Directeuren Veiligheidsregio's
SOC	Security Operations Center
VNG	Vereniging van Nederlandse Gemeenten
VNOG	Veiligheidsregio Noord- en Oost-Gelderland
VR-CERT	Veiligheidsregio Computer Emergency Respons Team
VR-ISAC	Veiligheidsregio Information Sharing and Analysis Center
VR-SOC	Veiligheidsregio Security Operations Center

1 Inleiding

Dit hoofdstuk geeft inzicht in de aanleiding, het doel, de probleemstelling, de afbakening en de betrokkenen en belanghebbenden bij en/of van dit onderzoek.

1.1 Aanleiding

Afgelopen jaar hebben cyberincidenten bij veiligheidsregio Noord- en Oost-Gelderland (VNOG) en gemeente Hof van Twente laten zien hoe groot de gevolgen van een cyberincident voor overheden kunnen zijn. Door de gijzelsoftware-aanval op de VNOG werden interne systemen geraakt en werden met name de kantoorprocessen ernstig verstoord (Veiligheidsregio Noord- en Oost-Gelderland, 2020). De cyberaanval in gemeente Hof van Twente had nog grotere gevolgen. Niet alleen lag de dienstverlening van de gemeente ruim twee weken stil doordat servers met gegevens ontoegankelijk waren, maar ook kan tot op de dag van vandaag niet met zekerheid worden gezegd dat de (privacy-) gevoelige gegevens niet zijn bekeken of verspreid (Gemeente Hof van Twente, 2020).

De economische en maatschappelijke kansen van digitalisering worden steeds groter, maar tegelijkertijd nemen kwetsbaarheden en dreigingen in het digitale domein toe (NCTV, 2018). Zo liggen dreigingen als sabotage, informatiemanipulatie, informatiediefstal, spionage, storing of lek tegenwoordig constant op de loer (NCTV, 2020a). Afhankelijk van de oorzaak kunnen deze dreigingen op verschillende manieren tot uiting komen. Zo worden DDos-aanvallen, Ransomware-aanvallen of fraude-aanvallen zoals phishing regelmatig door criminelen toegepast (NCSC, 2021). Toch hoeft er niet altijd sprake te zijn van moedwil, maar kan een incident ook worden veroorzaakt door het falen van mensen of systemen (IFV, 2019). Zo ontstaan de meeste cyberincidenten door menselijke fouten, mede omdat gemak door naïviteit en gebrek aan kennis voor de meeste mensen zwaarder weegt dan digitale veiligheidsmaatregelen (Digital Trust Center, z.d.). Daarnaast is de storing bij KPN in 2019 een goed voorbeeld van een cyberincident waar technisch falen de oorzaak was. Door deze storing was het alarmnummer 112 ruim drie en een half uur onbereikbaar (NOS, 2019). De storing had voor een aantal mensen medische gevolgen, maar heeft niet tot grote maatschappelijke impact geleid (IFV, 2020b). Wel blijkt uit deze casus dat grootschalige, landelijke cyberincidenten realistisch zijn.

Naast de toename van de dreiging nemen ook de kwetsbaarheden in het digitale domein toe (NCTV, 2018). Deze kwetsbaarheden zijn eigenschappen die een aanvaller de mogelijkheid biedt een cyberaanval uit te voeren of zijn eigenschappen die kunnen leiden tot uitval. Dit kan zich voordoen in een specifiek proces of systeem, zoals slecht beveiligde software of verbindingen, maar kan zich ook voordoen in de samenleving als geheel. Zo zorgen digitale ontwikkelingen, zoals digitale communicatie en via het internet verbonden apparaten, ervoor dat de fysieke wereld en digitale wereld steeds meer met elkaar vervlochten raken (NCTV, 2018). Deze toename van menselijke afhankelijkheid van digitale processen kan bij een cyberincident leiden tot directe schade aan de economie of nationale veiligheid. Denk bijvoorbeeld aan een cyberincident bij een waterkering of een storing waardoor geen enkele pinautomaat meer werkt. Niet voor niets wordt in het Cybersecuritybeeld Nederland 2020 de nadruk gelegd op mogelijke maatschappij-ontwrichtende schade ten gevolge van cyberincidenten (NCTV, 2020a). De dreiging neemt derhalve toe: maatschappelijke processen kunnen door de digitale ontwikkelingen makkelijker op grote schaal worden verstoord (NCTV, 2018).

"Het mag geen verrassing zijn dat de digitale dreiging op Nederland niet is afgenomen. Het valt niet uit te sluiten dat ontwrichting door cyberaanvallen of grootschalige uitval in Nederland zal plaatsvinden, ook al is dat nog nooit het geval geweest."

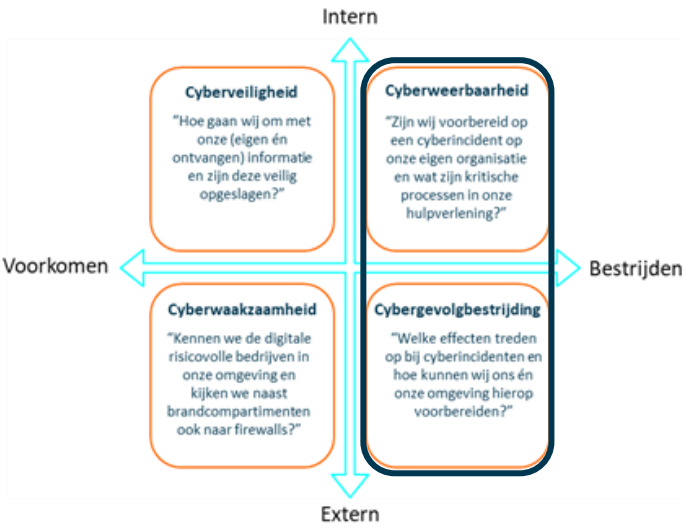
Minister van Justitie en Veiligheid Ferd Grapperhaus (Rijksoverheid, 2020)

Ook (overheids-) organisaties lijken kwetsbaar te zijn voor cyberincidenten (NCTV, 2020a). Uit onderzoek van het Instituut Fysieke Veiligheid blijkt dat ook de cyberweerbaarheid van veiligheidsregio's kan worden vergroot (IFV, 2019). Deze cyberweerbaarheid behelst de voorbereiding op en de uitvoering van de bestrijding van interne cyberincidenten. Dat de cyberweerbaarheid van veiligheidsregio's nog kan worden vergroot betekent niet dat er binnen veiligheidsregio's nu geen sprake is van cyberweerbaarheid of dat er sprake is van een gevaarlijke situatie, maar houdt wel in dat veiligheidsregio's zich beter kunnen voorbereiden op de bestrijding van cyberincidenten binnen de eigen organisatie. Zoals uit de recente incidenten blijkt, is de cyberweerbaarheid ook voor de 25 veiligheidsregio's in Nederland een belangrijk onderwerp. De veiligheidsregio's zijn immers verantwoordelijk voor de bestrijding van branden en de coördinatie, bestrijding en beheersing van rampen en crisis in de eigen regio's (art. 10 Wet veiligheidsregio's). Wanneer de eigen organisatie van (een van) de veiligheidsregio's wordt geveld door een cyberaanval, kan dit negatieve gevolgen hebben voor het aanbod van de hulpverlening in de regio.

"De weerbaarheid blijft achter ten opzichte van de ontwikkeling van de dreiging."

(NCTV, 2018)

Ook de voorbereiding op externe cybergevolgbestrijding van veiligheidsregio's kan volgens een ander onderzoek van het Instituut Fysieke Veiligheid worden vergroot (IFV, 2020a). Zo bleek dat veiligheidsregio's hun eigen preparatie op cybergevolgbestrijding slechts met een 6/10 beoordelen. Cybergevolgbestrijding omvat alle activiteiten in het kader van het bestrijden van de effecten van een incident waarvan de oorzaak en/of het gevolg in het digitale domein ligt/liggen (IFV, 2019). In tegenstelling tot cyberweerbaarheid, is de cybergevolgbestrijding juist gericht op cyberincidenten binnen de regio, maar buiten de eigen organisatie: externe cyberincidenten. Hierbij kan onder andere worden gedacht aan de uitval van vitale infrastructuur zoals elektriciteit, internet, drinkwater of betalingsverkeer binnen de regio. De uitval van dergelijke vitale infrastructuur kan ernstige maatschappelijke ontwrichting en bedreiging voor de nationale veiligheid tot gevolg hebben (NCTV, z.d.). In dit geval zullen (en moeten) de betreffende veiligheidsregio's de effecten van het incident bestrijden (maatschappelijke ontwrichting), terwijl de oorzaak hiervan in het digitale domein ligt.



De cyberweerbaarheid en cybergevolgbestrijding zijn dus beide gericht op de (gevolg)bestrijding en niet op het voorkomen van cyberincidenten. Zoals te zien in Figuur 1 zijn deze aandachtspunten binnen het donkere kader in het cyberkwadrant weergegeven. De focus ligt dus op zowel de interne als externe (gevolg)bestrijding. Dit cyberkwadrant en de andere aandachtspunten worden in het theoretisch kader toegelicht.

Figuur 1 Cyberkwadrant-model (ontwerp door veiligheidsregio IJsselland)

Over het algemeen zijn veel veiligheidsregio's nog zoekende naar een geschikte wijze om zich voor te bereiden op digitale verstoringen (IFV, 2019). Zo heerst er nog onduidelijkheid over de rollen, taken en bevoegdheden van alle betrokkenen bij de voorbereiding op de bestrijding van interne en externe cyberincidenten. Daarnaast is gebleken dat niet alle veiligheidsregio's over de benodigde kennis en kunde beschikken om zich goed te kunnen voorbereiden op zowel interne als externe cyberincidenten. Dit zijn een aantal barrières, die door veiligheidsregio's worden ervaren bij de voorbereiding op de bestrijding van cyberincidenten, maar zijn ongetwijfeld niet alle. Zo kunnen barrières volgens het triademodel van Poiesz worden geïnventariseerd en benaderd op basis van drie factoren: capaciteit, motivatie en gelegenheid. Een inventarisatie van de barrières die veiligheidsregio's ervaren bij de voorbereiding op de bestrijding van interne en externe cyberincidenten kan een beter beeld geven van de mogelijke verbeterpunten in deze voorbereiding. Met behulp van hetzelfde triademodel kunnen ook verschillende interventies worden gekoppeld aan de ervaren barrières, waardoor de verbeterpunten direct vorm krijgen in gerichte interventies: de leren-, motiveren- en faciliteren-gerelateerde interventies. Het triademodel van Poiesz en de theorie over barrières en interventies is in het theoretisch kader toegelicht.

Voor het Instituut Fysieke Veiligheid is het, als landelijke ondersteuningsorganisatie voor de veiligheidsregio's, van belang om veiligheidsregio's te helpen bij de versterking van de bestrijding van interne en externe cyberincidenten. Zo zijn via de Wet veiligheidsregio's verschillende taken overgeheveld naar het IFV, waaronder het ontwikkelen van kennis, het opleiden en vakbekwaam houden en het verwerven en beheren van materieel van/voor veiligheidsregio's (art. 68 lid 1 Wet veiligheidsregio's). Binnen het IFV houden voornamelijk de onderzoekers van het lectoraat Crisisbeheersing zich bezig met dit soort vraagstukken rondom crisisbeheersing. Wanneer veiligheidsregio's bij de voorbereiding op interne en externe cyberincidenten door barrières worden beperkt, kan het lectoraat hierin ondersteunen. Een inventarisatie van deze barrières kan het lectoraat een beter beeld geven van de leren-, motiveren- en faciliteren-gerelateerde interventies die het IFV kan uitvoeren om veiligheidsregio's te ondersteunen.

De toenemende dreiging, die steeds meer zichtbaar wordt door de toename van het aantal incidenten, en de in verhouding achterblijvende weerbaarheid van veiligheidsregio's vormen samen de aanleiding van dit onderzoek.

1.2 Doelstelling

De doelstelling van dit onderzoek is het aanreiken van interventies die zijn gericht op de ervaren barrières, om de voorbereiding van veiligheidsregio's op de (gevolg)bestrijding van interne en externe cyberincidenten te verbeteren. Hierbij kan worden gedacht aan inhoudelijke punten die moeten worden meegenomen in toekomstige interventies.

Met de uitkomsten van het onderzoek wordt een beter beeld geschetst van de mate waarin veiligheidsregio's zich bewust zijn van de dreigingen uit het digitale domein. Daarnaast wordt duidelijk welke capaciteit-, motivatie- en gelegenheids- gerelateerde barrières veiligheidsregio's ervaren bij de voorbereiding op de (gevolg)bestrijding van interne en externe cyberincidenten. Tot slot ontstaat, door de barrières te koppelen aan bijpassende en gerichte interventies, meer duidelijkheid over de interventies die veiligheidsregio's kunnen helpen bij de voorbereiding op de (gevolg)bestrijding van interne en externe cyberincidenten.

Uiteindelijk draagt de verbetering van de voorbereiding op de (gevolg)bestrijding van interne en externe cyberincidenten door veiligheidsregio's, bij aan een veilig en weerbaar Nederland.

1.3 Probleemstelling

Uit de aanleiding is gebleken dat de voorbereiding op digitale crisistypen voor veiligheidsregio's een uitdaging is. Terwijl de dreiging steeds groter lijkt te worden, zijn veiligheidsregio's nog zoekende naar een geschikte wijze om zich voor te bereiden op interne en externe cyberincidenten. De hoofdvraag van dit onderzoek luidt daarom als volgt:

"Op welke manier kan de voorbereiding van veiligheidsregio's, op de (gevolg)bestrijding van interne en externe cyberincidenten, worden verbeterd?"

1.4 Onderzoeksvragen

Om de hoofdvraag te beantwoorden zijn de volgende onderzoeksvragen opgesteld:

Onderzoeksvraag 1: "In hoeverre bestaat binnen veiligheidsregio's bewustzijn van intern- en extern-gerichte dreigingen uit het digitale domein?"

Onderzoekvraag 2: "Welke barrières ervaren veiligheidsregio's bij de voorbereiding op de bestrijding van interne cyberincidenten?"

Onderzoekvraag 3: "Welke barrières ervaren veiligheidsregio's bij de voorbereiding op de gevolgbestrijding van externe cyberincidenten?"

Onderzoeksvraag 4: "Welke gerichte interventies kunnen veiligheidsregio's helpen bij de voorbereiding op de bestrijding van interne cyberincidenten?"

Onderzoeksvraag 5: "Welke gerichte interventies kunnen veiligheidsregio's helpen bij de voorbereiding op de gevolgbestrijding van externe cyberincidenten?"

1.5 Afbakening

Binnen dit onderzoek ligt de focus op de voorbereiding van de (gevolg)bestrijding van interne en externe cyberincidenten door veiligheidsregio's. Het gaat dus om de mate waarin veiligheidsregio's voorbereid zijn op een cyberincident tegen de eigen organisatie, 'cyberweerbaarheid', maar ook om de mate waarin veiligheidsregio's voorbereid zijn op een cyberincident in de regio, 'cybergevolgbestrijding'. Hierbij ligt de focus met name op de voorbereidende activiteiten op de bestrijding en minder op de bestrijding van cyberincidenten zelf. Hierbij kan bijvoorbeeld worden gedacht aan het vergaren van kennis en de organisatie van oefeningen.

De activiteiten van veiligheidsregio's die betrekking hebben op het voorkomen van cyberincidenten worden door de onderlinge samenhang wel in het rapport benoemd, maar zijn niet specifiek onderzocht. De activiteiten van veiligheidsregio's binnen het cyberdomein en de samenhang tussen deze activiteiten wordt in het theoretisch kader verder toegelicht.

Ook zijn zowel cyberaanvallen, technische fouten en menselijke fouten bij dit onderzoek meegenomen, aangezien dit allemaal valt onder de definitie van cyberincident. Hierbij wordt niet specifiek ingegaan op alle mogelijke soorten dreigingen, omdat een dergelijke lijst niet uitputtend is. De digitale dreiging bestaat immers uit zogenoemde 'ongekende' risico's, die elke dag weer veranderen (Evaluatiecommissie Wet veiligheidsregio's, 2020). Daarnaast blijkt uit afgenomen interviews met crisisbeheersingsambtenaren van veiligheidsregio's, (gepland in het kader van een lopend onderzoek van het IFV naar cyberkennis en -kunde binnen veiligheidsregio's) dat een specifieke oorzaak van een cyberincident voor de veiligheidsregio's vaak niet relevant is voor de (gevolg)bestrijding van het incident. Het begrip 'cyberincident' en de typen dreigingen worden in het theoretisch kader toegelicht.

Tot slot wordt er voor het beantwoorden van de probleemstelling van uitgegaan dat de voorbereiding van veiligheidsregio's, op de (gevolg)bestrijding van interne en externe cyberincidenten, kan worden verbeterd door interventies aan te reiken die aansluiten bij de verbeterpunten (barrières). De mate waarin de uitvoering van interventies, die in de aanbeveling worden aangereikt, in de praktijk aan de verbetering bijdraagt is op korte termijn vrijwel onmogelijk te meten en zal eventueel op een later moment door het IFV kunnen worden geëvalueerd.

1.6 Betrokkenen en belanghebbenden

Dit hoofdstuk geeft inzicht in de betrokkenen en belanghebbenden bij dit vraagstuk en de belangen van deze partijen.

1.6.1 Het Instituut Fysieke Veiligheid

Het Instituut Fysieke Veiligheid is uiteraard als opdrachtgever betrokken bij dit vraagstuk, maar is ook zeker een belanghebbende. Het IFV heeft als landelijke ondersteuningsorganisatie voor de veiligheidsregio's baat bij de versterking van de aanpak op het terrein van crisisbeheersing. Via de Wet veiligheidsregio's zijn immers verschillende taken overgeheveld naar het IFV (art. 68 lid 1 Wet veiligheidsregio's). Onder andere het ontwikkelen van kennis, het vakbekwaam blijven en worden en het verwerven en beheren van materieel is hier onderdeel van. Het lectoraat Crisisbeheersing van het IFV voert synchroon aan dit onderzoek, een onderzoek uit naar benodigde cyberkennis en -kunde binnen veiligheidsregio's. Dat onderzoek van het lectoraat wordt in opdracht van de portefeuillehouder Digitale ontwrichting en Cyber binnen de Raad van Commandanten en Directeuren Veiligheidsregio's (RCDV) uitgevoerd. De resultaten van dit onderzoek naar de barrières en interventies bij de voorbereiding op de (gevolg)bestrijding van interne en externe cyberincidenten zijn ook relevant voor het advies richting de opdrachtgever van het onderzoek van het lectoraat.

1.6.2 De veiligheidsregio's

Veiligheidsregio's kunnen ook als betrokkenen worden aangemerkt. Niet alleen vormen zij het onderwerp van dit vraagstuk, maar ook zijn werknemers van veiligheidsregio's benaderd voor de verzameling van gegevens en informatie. De veiligheidsregio's kunnen daarnaast ook als belanghebbende worden aangemerkt. De 25 veiligheidsregio's in Nederland zetten zich in voor de veiligheid van de inwoners en bezoekers van hun eigen gebied/regio. Volgens art. 10 Wet veiligheidsregio's zijn de veiligheidsregio's verantwoordelijk voor:

- Het voorkomen en bestrijden van branden
- Het voorbereiden op risico's, rampen en crises
- De coördinatie, beheersing en bestrijding van rampen en crises

De veiligheidsregio's hebben in het kader van de bovenstaande taken en verantwoordelijkheden uiteraard baat bij de versterking van de aanpak op het terrein van crisisbeheersing en specifiek de verbetering van de eigen positie bij de voorbereiding op de (gevolg)bestrijding van interne en externe cyberincidenten. Uiteindelijk draagt de verbetering van de voorbereiding op de (gevolg)bestrijding van interne en externe cyberincidenten door veiligheidsregio's, bij aan de vergroting van de veiligheid van inwoners en bezoekers in de Nederlandse veiligheidsregio's.

1.6.3 Burgemeesters

Burgemeesters kunnen als belanghebbenden worden aangemerkt. Volgens art. 2 Wet veiligheidsregio's is de burgemeester verantwoordelijk voor een goede aanpak bij een brand, ramp of crisis in de eigen gemeente. Daarnaast is elke burgemeester ook verantwoordelijk voor de aanpak van de effecten van verstoringen op de openbare orde en veiligheid (IFV, 2019). Tevens is de burgemeester van de grootste gemeente in elke regio de voorzitter van de veiligheidsregio. Wanneer

een brand, ramp of crisis in meerdere gemeentes tegelijk plaatsvindt, dan is de voorzitter van de veiligheidsregio volgens art. 39 Wet veiligheidsregio's verantwoordelijk voor de aanpak van deze verstoring in deze regio.

Door de verbetering van de positie van veiligheidsregio's bij de voorbereiding op de (gevolg)bestrijding van interne en externe cyberincidenten, kunnen fysieke effecten van digitale verstoringen mogelijk worden voorkomen. Deze verbetering helpt de burgemeesters dus bij het voldoen aan de in de Wet veiligheidsregio's vastgestelde verantwoordelijkheden.

1.6.4 Medeoverheden

Medeoverheden kunnen voor de (gevolg)bestrijding van zowel interne als externe cyberincidenten als belanghebbenden worden aangemerkt. Partijen als het Nationaal Cyber Security Center (NCSC), de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Landelijk Operationeel Coördinatiecentrum (LOCC) zijn gericht op het vergroten van de digitale weerbaarheid of het verlenen van bijstand tijdens crisissituaties (Rijksoverheid, z.d.). Het verbeteren van de positie van veiligheidsregio's bij de voorbereiding op de (gevolg)bestrijding van interne en externe cyberincidenten kan deze partijen daarom helpen bij het behalen van de doelen (vergroten van de cyberweerbaarheid door het NCSC) of het ontlasten tijdens crisissituaties (LOCC/NCTV).

1.6.5 Landelijke voorzieningen en netwerken

Landelijke voorzieningen zoals de veiligheidsregio Information Sharing and Analysis Center (VR-ISAC) kunnen voor de (gevolg)bestrijding van zowel interne als externe cyberincidenten als belanghebbenden worden aangemerkt. Dit Information Sharing and Analysis Center voor veiligheidsregio's is een samenwerkingsverband waarbij informatiespecialisten uit de 25 veiligheidsregio's en het IFV kennis en expertise uit op het gebied van digitale dreigingen en incidenten uitwisselen (IFV, 2020d). Daarnaast kunnen ook landelijke netwerken zoals de werkgroep Digitale ontwrichting of de vakgroep Informatieveiligheid voor de bestrijding van zowel interne als externe cyberincidenten als belanghebbenden worden aangemerkt. De werkgroep bestaat (voornamelijk) uit leden van verschillende veiligheidsregio's, waarbinnen thema's als digitale ontwrichting en cybergevolgbestrijding veelvuldig worden besproken (IFV, 2019). Het verbeteren van de positie van veiligheidsregio's bij de voorbereiding op de (gevolg)bestrijding van interne en externe cyberincidenten kan deze landelijke voorzieningen en netwerken helpen bij het behalen van de doelen, zoals het vergroten van de cyberweerbaarheid of het ondersteunen van veiligheidsregio's bij (de voorbereiding op) de bestrijding van cyberincidenten. De leden van de VR-ISAC en de werkgroep Digitale ontwrichting zijn daarnaast ook als respondenten betrokken bij dit onderzoek.

1.6.6 Vitale partners

Vitale partners kunnen voor de gevolgbestrijding van externe cyberincidenten als belanghebbenden worden aangemerkt. Cyberverstoringen bij vitale partners kunnen ervoor zorgen dat sectoren als energie, drinkwater, telecom en watermanagement hun vitale processen niet meer kunnen aanbieden. Een soortgelijke situatie kan grote maatschappelijke impact tot gevolg hebben. Door de verbetering van de positie van veiligheidsregio's bij de voorbereiding op de gevolgbestrijding van externe cyberincidenten, kunnen maatschappelijke gevolgen van digitale verstoringen bij vitale partners mogelijk worden voorkomen.

1.6.7 Private kennis- en adviesbureaus

Het Instituut voor Veiligheids- en Crisismanagement kan voor de (gevolg)bestrijding van interne en externe cyberincidenten als betrokkene worden aangemerkt, aangezien een senior adviseur onderzoeker van het COT heeft deelgenomen aan een interview. Het COT is als instituut betrokken bij onderzoek naar de versterking van het cybercrisisvermogen van organisaties (COT, z.d.).

2 Theoretisch kader

Dit hoofdstuk geeft inzicht in de centrale begrippen en de relaties tussen de centrale begrippen. Onder andere de toename van dreiging binnen het cyberdomein, cyberincidenten en de activiteiten van veiligheidsregio's binnen het cyberdomein komen aan bod. Daarnaast verschaft dit hoofdstuk ook duidelijkheid over het gebruik van het triademodel waar tijdens dit onderzoek gebruik van wordt gemaakt.

2.1 Toename van dreiging in het digitale domein

Zoals benoemd in de aanleiding worden de economische en maatschappelijke kansen van digitalisering steeds groter (NCTV, 2018). Communicatie via de digitale weg en de mogelijkheden van 'Internet of Things' (met het internet verbonden apparaten) zijn door de digitalisering bijna niet meer weg te denken, maar zorgen daardoor ook voor een toename van de dreiging (NCTV, 2018). De toename van menselijke afhankelijkheid van digitale processen kan bij een cyberincident namelijk leiden tot directe schade aan de economie of nationale veiligheid (NCTV, 2018). De dreiging uit het digitale domein neemt hierdoor toe, omdat maatschappelijke processen door de digitale ontwikkelingen makkelijker op grote schaal kunnen worden verstoord (NCTV, 2018).

Dit digitale domein is de complexe omgeving die het resultaat is van de interactie tussen mensen, software en diensten op het internet, ondersteund door wereldwijd gedistribueerde fysieke informatie- en communicatietechnologie (ICT) -apparaten en verbonden netwerken (NCTV, 2020a). De dreiging binnen dit domein bestaat uit de mogelijkheid dat een of meerdere cyberincidenten zich gelijktijdig of opeenvolgend voordoen (NCTV, 2020a). Hierbij kan volgens het Nationaal Crisisplan Digitaal en het Cybersecuritybeeld Nederland (CSBN) onder andere worden gedacht aan:

- Verstoring/sabotage: het opzettelijk aantasten van de beschikbaarheid van informatie, informatiesystemen of –diensten;
- Informatiemanipulatie: aantasting van de integriteit van informatie door het opzettelijk wijzigen van informatie;
- Informatiediefstal: aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie;
- Spionage: aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie door statelijke actoren;
- Storing/uitval: aantasting van de integriteit of beschikbaarheid van informatie, informatiesystemen of -diensten als gevolg van natuurlijk, technisch of menselijk falen;
- Lek: aantasting van de vertrouwelijkheid van informatie, informatiesystemen of -diensten als gevolg van natuurlijk, technisch of menselijk falen (NCTV, 2020b; NCTV, 2020a).

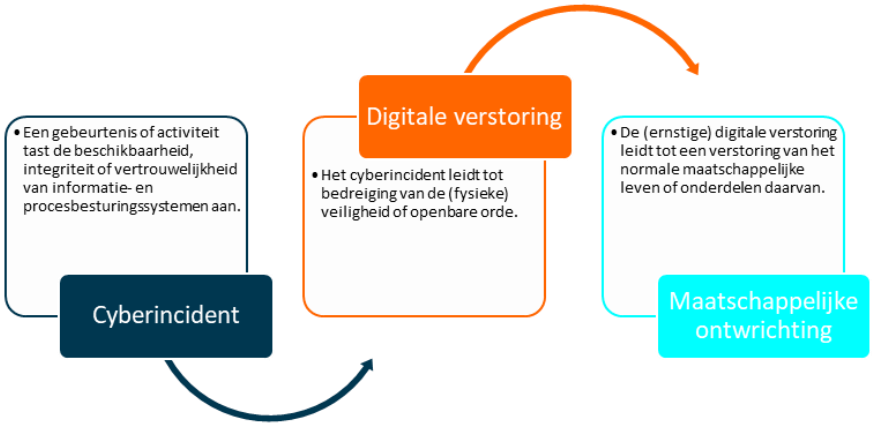
2.2 Cyberincidenten, digitale verstoring en maatschappelijke ontwrichting

Een cyberincident hoeft niet altijd een cyberaanval te zijn die wordt veroorzaakt door moedwillig handelen, maar kan ook worden veroorzaakt door het falen of uitvallen van systemen (IFV, 2019). De gijzelsoftware-aanval op de VNOG en de cyberaanval in gemeente Hof van Twente zijn voorbeelden van cyberincidenten met moedwillig handelen als oorzaak (Veiligheidsregio Noord- en Oost-Gelderland, 2020; Gemeente Hof van Twente, 2020). Wanneer moedwillig handelen niet de oorzaak is van een cyberincident, kan er onder andere sprake zijn van menselijk of systemisch falen. Een voorbeeld van een dergelijke situatie is de storing bij KPN waardoor het alarmnummer 112 ruim drie en een half uur onbereikbaar was (NOS, 2019). Hierbij was geen sprake van moedwillig handelen, maar het falen van een systeem door een storing. Over het algemeen kan worden gezegd dat er sprake is van een cyberincident wanneer een gebeurtenis of activiteit de beschikbaarheid, integriteit of vertrouwelijkheid van informatie- en procesbesturingssystemen aantast. (NCTV, 2020a). Wanneer

een cyberincident leidt tot bedreiging van de (fysieke) veiligheid of openbare orde in een veiligheidsregio, is er sprake van digitale verstoring (Werkgroep Digitale ontwrichting, 2019). In dit geval kan een ernstige digitale verstoring leiden tot maatschappelijke ontwrichting (Werkgroep Digitale ontwrichting, 2019).

Een eenduidige definitie van maatschappelijke ontwrichting lijkt niet te bestaan, maar het Instituut Fysieke Veiligheid gebruikt de volgende definitie in een onderzoek naar de versterking van veerkracht: “Maatschappelijke ontwrichting refereert aan een proces waarbij een relatief grote groep mensen in een gemeenschap bemerkt, vreest of tot de overtuiging komt dat de voorzieningen, die voor hen van elementair belang zijn, niet beschikbaar (zullen) zijn en vervolgens hun dagelijks handelingsrepertoire aanpast waardoor de situatie wordt bestendigd of zelfs verergert” (IFV, 2020c). Kort gezegd is er sprake van maatschappelijke ontwrichting wanneer het normale maatschappelijke leven of onderdelen daarvan ernstig worden verstoord.

De verschillen en samenhang tussen de begrippen; cyberincident, digitale verstoring en maatschappelijke ontwrichting is in het onderstaande Figuur 2 weergegeven.



Figuur 2 Samenhang tussen cyberincidenten, digitale verstoring en maatschappelijke ontwrichting (E.T. Brouwer,2021)

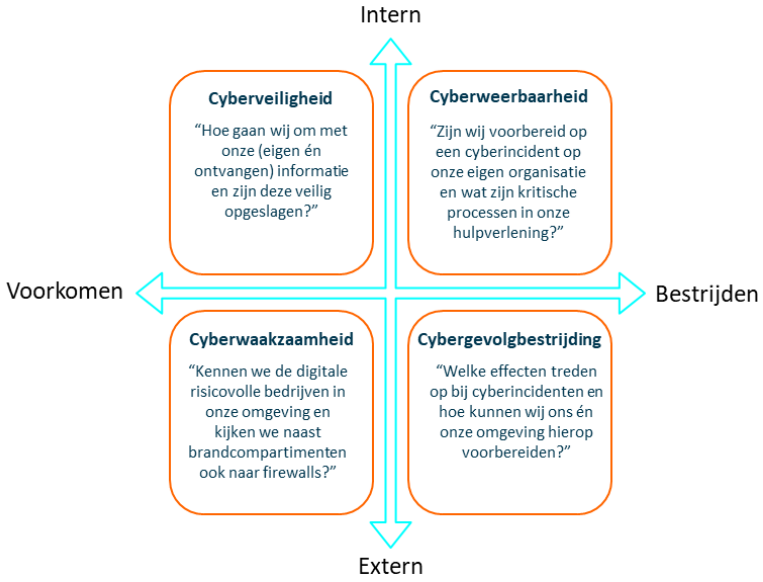
2.3 Activiteiten en aandachtspunten van veiligheidsregio’s binnen het cyberdomein

Een toename van dreiging binnen het digitale domein, waarvan inmiddels bijna iedereen dagelijks gebruikmaakt, is een probleem waar ook veiligheidsregio’s mee te maken krijgen. Om deze reden zijn de bestuurlijke opgaven van veiligheidsregio’s binnen het cyberdomein in 2019 door het Veiligheidsberaad vastgesteld (Veiligheidsberaad, 2019). Deze bestuurlijke opgaven en activiteiten kunnen worden onderverdeeld in voorkomende en bestrijdende activiteiten en zijn zowel intern als extern gericht. De volgende activiteiten zijn te onderscheiden: cyberveiligheid, cyberwaakzaamheid, cyberweerbaarheid en cybergevolgbestrijding.

- Cyberveiligheid is gericht op het voorkomen van interne cyberincidenten. Het gaat hierbij om het kennen van de risico’s in de eigen organisatie, waarbij informatiemanagement en informatieveiligheid voorop staan (IFV, 2019). De vraag hoe wordt omgegaan met eigen (en ontvangen) informatie en de manier waarop dit veilig wordt opgeslagen speelt bij cyberveiligheid een grote rol.
- Cyberwaakzaamheid is gericht op het voorkomen van externe cyberincidenten. Cyberwaakzaamheid wordt door het IFV gedefinieerd als: “Het kennen van risico’s met een digitale component in de samenleving” (IFV, 2020a). Dit is extern op de regio gericht en heeft daarom onder andere betrekking op kwetsbare ICT-knooppunten, diensten en objecten (IFV, 2020a).

- Cyberweerbaarheid is gericht op het bestrijden van interne cyberincidenten. Het gaat hierbij om de activiteiten in het kader van de bestrijding van een cyberincident in de eigen organisatie (IFV, 2019). Het vormen van een duidelijk beeld van de kritische processen binnen de organisatie en het maken/up-to-date houden van een continuïteitsplan zijn voorbeelden van dergelijke activiteiten (IFV, 2019).
- Cybergevolgbestrijding is gericht op het bestrijden van externe cyberincidenten. Het IFV omschrijft cybergevolgbestrijding als volgt: "Alle activiteiten in het kader van bestrijden van de effecten van een incident waarvan de oorzaak en/of gevolg in het digitale domein ligt" (IFV, 2019).

De verschillende activiteiten en aandachtspunten van veiligheidsregio's binnen het cyberdomein zijn zoals te zien in Figuur 3 in een zogenoemd 'cyberkwadrant' weergegeven.



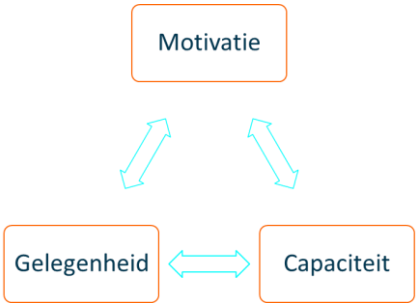
Figuur 3 Cyberkwadrant-model (ontwerp door veiligheidsregio IJsselland)

Alle activiteiten staan met elkaar in verbinding en een koppeling tussen de vier activiteiten is volgens het IFV essentieel voor een goede bescherming tegen cyberincidenten (IFV, 2019). Binnen dit onderzoek ligt de focus op de voorbereiding van de (gevolg)bestrijding van interne en externe cyberincidenten door veiligheidsregio's. Het gaat dus om de mate waarin veiligheidsregio's voorbereid zijn op een cyberincident tegen de eigen organisatie, 'cyberweerbaarheid', maar ook om de mate waarin veiligheidsregio's voorbereid zijn op een cyberincident in de regio, 'cybergevolgbestrijding'.

Bij voorbereidende activiteiten met betrekking tot de bestrijding van interne cyberincidenten kan worden gedacht aan opleidingen, trainingen of oefeningen over: het inventariseren van mogelijke dreigingen uit het cyberdomein op de eigen organisatie, het inventariseren van mogelijke effecten van een intern cyberincident, het in beeld brengen van de verbondenheid van/tussen verschillende interne systemen en het inventariseren van belangrijke interne processen (Berenschot, 2020a; Berenschot, 2020b). Bij voorbereidende activiteiten met betrekking tot de gevolgbestrijding van externe cyberincidenten kan worden gedacht aan opleidingen, trainingen of oefeningen over: het inventariseren van mogelijke dreigingen uit het cyberdomein op de regio, het inventariseren van mogelijke maatschappelijke effecten van een extern cyberincident en het inventariseren van maatschappelijk belangrijke externe processen en bedrijven (denk aan vitale infrastructuur zoals elektriciteit, internet, drinkwater of betalingsverkeer) (Berenschot, 2020a; Berenschot, 2020b).

2.4 Triademodel van Poiesz

Het voorbereidende 'gedrag' van veiligheidsregio's op de (gevolg)bestrijding van cyberincidenten en de barrières die hierbij worden ervaren, wordt op basis van het triademodel van Poiesz onderzocht. Het Triade-model van Poiesz is een verklarend model dat uitgaat van drie vaste en noodzakelijke oorzaken van gedrag: motivatie, capaciteit en gelegenheid (Poiesz T. , 1999). Deze drie factoren zijn in hun onderlinge samenhang verantwoordelijk voor de totstandkoming, de kwaliteit en de continuïteit van (gewenst) gedrag (Bogaerts & Poiesz, 2007). Binnen veiligheidsregio's bepaalt het gedrag van individuen binnen de organisatie, zoals het management en werknemers, het 'gedrag' van de organisatie. Zo bepalen motivatie, capaciteit en gelegenheid de waarschijnlijkheid van nieuw gedrag en de kwaliteit van bestaand gedrag. Deze drie factoren en de samenhang tussen deze factoren is te zien in Figuur 4.



Figuur 4 Triade van Poiesz

De samenhang van de factoren blijkt uit de onderlinge afhankelijkheid: wanneer één van de drie factoren afwezig is, is gedragsverandering zeer moeilijk of zelfs onmogelijk (Poiesz T. , 1999; Bogaerts & Poiesz, 2007). Daarnaast is er sprake van een zekere interactie tussen de motivatie, capaciteit en gelegenheid (Nederstigt, 2011). Wanneer een persoon of groep bijvoorbeeld een grote motivatie heeft om iets te bereiken, zal deze persoon of groep hier waarschijnlijk tijd voor vrij maken (gelegenheid) en meer leren en oefenen (capaciteit) om het doel te bereiken.

Motivatie wordt door Poiesz gedefinieerd als de mate waarin een persoon belangstelling heeft voor (het resultaat van) het vertonen van bepaald gedrag (Poiesz T. , 1999). Motivatie kan worden opgedeeld in intrinsieke motivatie en extrinsieke motivatie. Intrinsieke motivatie ontstaat uit eigen verlangens van de persoon of groep, terwijl extrinsieke motivatie wordt opgewekt door factoren buiten deze persoon of groep (Bogaerts & Poiesz, 2007). Hierbij kan onder andere worden gedacht aan beloningen of erkenning. Concreet wordt de motivatie van veiligheidsregio's bijvoorbeeld geuit in de mate waarin de voorbereiding op interne en externe cyberincidenten prioriteit heeft.

Capaciteit is de mate waarin een persoon over de eigenschappen, vaardigheden, macht en instrumenten beschikt om het gedrag te vertonen (Poiesz T. , 1999). Capaciteit kan ook worden opgedeeld in intrinsieke capaciteit en extrinsieke capaciteit. Intrinsieke capaciteit gaat hierbij om de eigen kwaliteiten en vaardigheden van een persoon of groep, terwijl extrinsieke capaciteit gaat om de bijstand van buitenaf die de mogelijkheden van de persoon kan vergroten of beperken (Bogaerts & Poiesz, 2007). Zo kan in dit kader worden gedacht aan netwerken en samenwerkingen die een persoon of groep kunnen helpen bij het tot stand komen van bepaald gedrag. De capaciteit zoals kennis, vaardigheden en samenwerking die veiligheidsregio's nodig hebben bij (de voorbereiding op) de (gevolg)bestrijding van interne en externe cyberincidenten is te vinden in Bijlagen 3 en 4.

Gelegenheid betreft de mate waarin de buiten een persoon gelegen omstandigheden stimulerend of belemmerend inwerken op bepaald gedrag (Poiesz T. , 1999). Ook gelegenheid betreft zowel intrinsieke als extrinsieke factoren. Met intrinsieke gelegenheid worden omstandigheden bedoeld die de betreffende persoon of groep zelf kan bepalen (Bogaerts & Poiesz, 2007). Binnen het bedrijfsleven kan hierbij bijvoorbeeld worden gedacht aan standplaats of werktijden. Met extrinsieke gelegenheid worden omstandigheden bedoeld die de betreffende persoon of groep niet kan bepalen, zoals de beschikbaarheid van middelen, geld of tijd (Bogaerts & Poiesz, 2007).

Om een bepaald gewenst gedrag te laten voltrekken, verbeteren of voortduren moet de persoon of groep in kwestie dus beschikken over voldoende motivatie, capaciteit en gelegenheid. Anderzijds is

het uitblijven van bepaald gewenst gedrag ook afhankelijk van deze factoren. Zo blijkt uit een onderzoek van de Haagse Hogeschool en NHL Stenden, dat het gebrek aan samenwerking en oefening binnen gemeenten zorgt voor een matige voorbereiding op cybercrises (Leeuw, 2021). Of deze capaciteit ook voor veiligheidsregio's de barrière vormt, kan met het triademodel worden onderzocht.

Met behulp van het Triade-model kan systematisch worden onderzocht welke uitdagingen/barrières door veiligheidsregio's worden ervaren bij de voorbereiding op interne en externe cyberincidenten. Op basis van het Triade-model van Poiesz kan worden verondersteld dat veiligheidsregio's zich alleen voorbereiden op de (gevolg)bestrijding van interne en externe cyberincidenten als veiligheidsregio's:

- gemotiveerd zijn om zich voor te bereiden op de (gevolg)bestrijding van cyberincidenten;
- in staat zijn om zich voor te bereiden op de (gevolg)bestrijding van cyberincidenten;
- door omstandigheden in de gelegenheid worden gesteld om zich voor te bereiden op de (gevolg)bestrijding van cyberincidenten.

Naast het inventariseren van de mogelijke barrières binnen de bovenstaande factoren, biedt het triademodel ook de mogelijkheid om deze barrières weg te nemen met behulp van gerichte interventies (Secura, z.d.). Welke (samenstelling) van de interventies het beste kan worden ingezet, wordt dus bepaald door de analyse van de barrières:

- is men binnen veiligheidsregio's (nog) niet voldoende gemotiveerd om zich voor te bereiden op de (gevolg)bestrijding van cyberincidenten? → interventie richten op motiveren
- is men binnen veiligheidsregio's (nog) niet voldoende in staat om zich voor te bereiden op de (gevolg)bestrijding van cyberincidenten? → interventie richten op leren
- is men binnen veiligheidsregio's (nog) niet in de gelegenheid om zich voor te bereiden op de (gevolg)bestrijding van cyberincidenten? → interventie richten op faciliteren

Bij een interventie die wordt gericht op motiveren kan worden gedacht aan een campagne over het belang van het gewenste gedrag, een beloning voor het uitvoeren van gewenst gedrag of juist strengere regels of straffen wanneer het uitvoeren van gewenst gedrag uitblijft. Bij een interventie die wordt gericht op leren kan worden gedacht aan opleidingen, trainingen of oefeningen waarin de ontbrekende kennis en vaardigheden voor het uitvoeren van het gewenste gedrag worden toegepast. Bij een interventie die wordt gericht op faciliteren kan worden gedacht aan het aanreiken of beschikbaar stellen van bepaalde middelen, tijd of geld.

Met behulp van het triademodel kunnen dus (inhoudelijke punten voor) interventies worden aangereikt, die zijn gericht op de ervaren barrières, om de voorbereiding van veiligheidsregio's op de (gevolg)bestrijding van interne en externe cyberincidenten te verbeteren.

3 Methode van onderzoek

Dit hoofdstuk geeft inzicht in de methoden en instrumenten die tijdens dit onderzoek zijn gebruikt voor de beantwoording van de hoofdvraag. Daarnaast zijn de geoperationaliseerde onderzoekseenheden en variabelen in dit hoofdstuk te vinden en wordt beargumenteerd waarom de gekozen methode tot betrouwbare en valide gegevens heeft geleid.

3.1 Methode

Om inzicht te verkrijgen in de mogelijke manieren waarop de voorbereiding van veiligheidsregio's op de (gevolg) bestrijding van cyberincidenten kan worden verbeterd, moet de geformuleerde hoofdvraag en de bijbehorende onderzoeksvragen worden beantwoord. De hoofdvraag: "Op welke manier kan de voorbereiding van veiligheidsregio's, op de (gevolg)bestrijding van interne en externe cyberincidenten, worden verbeterd?", neigt naar zowel kwantitatief als kwalitatief onderzoek. Met behulp van kwantitatieve gegevens konden namelijk zowel de beschrijvende als verklarende onderzoeksvragen worden beantwoord (Verhoeven, 2011). Zo konden conclusies worden getrokken over 'wat-vragen' en 'hoe komt het dat-vragen', waardoor ook causale relaties konden worden onderzocht. In het kader van dit onderzoek kan hierbij worden gedacht aan vragen over de activiteiten die door veiligheidsregio's worden uitgevoerd, de barrières die hierbij worden ervaren, de mate waarin veiligheidsregio's zichzelf voorbereid vinden en de mogelijke redenen hiervoor. Om ook te kunnen achterhalen wat de beweegredenen van veiligheidsregio's zijn voor het al dan niet uitvoeren van voorbereidende activiteiten binnen het cyberdomein, is ook een kwalitatief onderzoeks-deel uitgevoerd. De resultaten bestaan daarom uit kwantitatieve gegevens, die waar nodig/gewenst zijn aangevuld met kwalitatieve gegevens. Er is daarom sprake van triangulatie: een combinatie tussen kwalitatieve en kwantitatieve dataverzamelingsmethoden (Verhoeven, 2011).

Voor alle onderzoeksvragen is gebruik gemaakt van fieldresearch, waarbij zowel kwalitatieve als kwantitatieve gegevens zijn verzameld. De kwalitatieve gegevens zijn middels interviews met medewerkers van veiligheidsregio's, leden van vakgroepen en andere experts verzameld. De samenstelling van deze groep respondenten wordt in de komende hoofdstukken toegelicht. De kwantitatieve gegevens zijn middels twee enquêtes verzameld. Hierbij zijn de leden van de VR-ISAC bevraagd over de cyberweerbaarheid en zijn de leden van de werkgroep digitale ontwrichting en cyber bevraagd over de cybergevolgbestrijding. De samenstelling van deze groepen respondenten wordt ook in de komende hoofdstukken toegelicht. Voor onderzoeksvraag vier en vijf is hiernaast ook gebruik gemaakt van deskresearch, waarbij relevante literatuur volgens de sneeuwbalmethode is verzameld. De specifieke kenmerken van dit onderzoeks-deel wordt ook in de komende hoofdstukken toegelicht. In Tabel 1 is te zien welke dataverzamelingsmethoden tijdens dit onderzoek zijn toegepast en welke toevoegingen deze methoden hebben voor de betreffende onderzoeksvraag.

Tabel 1 Toegepaste dataverzamelingsmethoden (Brouwer, 2021)

Onderzoeks-vragen	Deskresearch: eerdere onderzoeken	Fieldresearch: interviews	Fieldresearch: enquêtes
Onderzoeks-vraag 1		Dit kwalitatieve onderzoeks-deel kon onder andere inzicht geven in de achterliggende gedachten en visies van veiligheidsregio's met betrekking tot de grootte en ernst van de dreiging.	Dit kwantitatieve onderzoeks-deel kon onder andere inzicht geven in de cijfermatige gemiddelden en verdelingen van de manier waarop de grootte en ernst van de dreiging wordt ingeschat.

Onderzoeks-vraag 2		Dit kwalitatieve onderzoeks-deel kon voor deze onderzoeksvraag onder andere inzicht geven in de capaciteit-, motivatie- en gelegenheids-gerelateerde barrières die veiligheidsregio's ervaren bij de voorbereiding op de bestrijding van interne cyberincidenten.	Dit kwantitatieve onderzoeks-deel kon voor deze onderzoeksvraag onder andere inzicht geven in de cijfermatige verdelingen van de mate waarin de verschillende barrières worden ervaren. Zo kon bij de vierde onderzoeksvraag onder andere worden gefocust op de barrières die het meest worden ervaren of het grootste probleem vormen.
Onderzoeks-vraag 3		Dit kwalitatieve onderzoeks-deel kon voor deze onderzoeksvraag onder andere inzicht geven in de capaciteit-, motivatie- en gelegenheids-gerelateerde barrières die veiligheidsregio's ervaren bij de voorbereiding op de gevolgbestrijding van externe cyberincidenten.	Dit kwantitatieve onderzoeks-deel kon voor deze onderzoeksvraag onder andere inzicht geven in de cijfermatige verdelingen van de mate waarin de verschillende barrières worden ervaren. Zo kon bij de vijfde onderzoeksvraag onder andere worden gefocust op de barrières die het meest worden ervaren of het grootste probleem vormen.
Onderzoeks-vraag 4	Dit onderzoeks-deel kon voor deze onderzoeksvraag onder andere inzicht geven in de mogelijke interventies die kunnen helpen bij de specifieke barrières die veiligheidsregio's ervaren. Hierbij is ingegaan op leren-, motivatie- en faciliteren-gerelateerde interventies, die aansluiten op de ervaren barrières.	Dit kwalitatieve onderzoeks-deel kon voor deze onderzoeksvraag onder andere inzicht geven in welke interventies de experts zouden toepassen en nodig achtten voor een verbetering van de voorbereiding op interne cyberincidenten.	Dit kwantitatieve onderzoeks-deel kon voor deze onderzoeksvraag onder andere inzicht geven in de cijfermatige gemiddelden en verdelingen van de interventies die de experts nodig achten voor de verbetering van de voorbereiding van veiligheidsregio's op interne cyberincidenten.
Onderzoeks-vraag 5	Dit onderzoeks-deel kon voor deze onderzoeksvraag onder andere inzicht geven in de mogelijke interventies die kunnen helpen bij de specifieke barrières die veiligheidsregio's ervaren. Hierbij is ingegaan op leren-, motivatie- en faciliteren-gerelateerde interventies, die aansluiten op de ervaren barrières.	Dit kwalitatieve onderzoeks-deel kon voor deze onderzoeksvraag onder andere inzicht geven in welke interventies de experts zouden toepassen en nodig achtten voor een verbetering van de voorbereiding op externe cyberincidenten.	Dit kwantitatieve onderzoeks-deel kon voor deze onderzoeksvraag onder andere inzicht geven in de cijfermatige gemiddelden en verdelingen van de interventies die de experts nodig achten voor de verbetering van de voorbereiding van veiligheidsregio's op externe cyberincidenten.

3.1.1 Eerdere onderzoeken

Zoals hierboven is beschreven, is in dit onderzoek gebruik gemaakt van zowel kwalitatieve als kwantitatieve data die is verkregen uit eerdere onderzoeken. Het was voor de vierde en vijfde onderzoeksvraag relevant om te kijken naar eerdere onderzoeken en theorieën over geschikte interventies, die specifiek kunnen helpen bij de barrières die veiligheidsregio's ervaren bij voorbereiding op cyberincidenten. Daarnaast hebben het IFV, de NCTV en Berenschot al onderzoek gedaan naar veiligheidsregio's binnen het cyberdomein. Informatie uit deze bronnen is in/bij de aanleiding, het theoretisch kader, de opzet van de enquêtevragen en de beantwoording van de onderzoeksvragen gebruikt. Hierbij kan worden gedacht aan informatie over de benodigde kennis en vaardigheden voor (de voorbereiding op) cyberincidenten.

3.1.2 Interviews

De interviews is de eerste dataverzamelingsmethode waarvan binnen dit onderzoek gebruik is gemaakt. Deze interviews vonden plaats in het kader van een lopend onderzoek van het lectoraat Crisisbeheersing van het IFV naar cyberkennis en -kunde binnen veiligheidsregio's. Wegens de raakvlakken tussen het bovenstaande onderzoek van het IFV en dit onderzoek, werden deze interviews gezamenlijk gevoerd. Dit onderzoek mocht in de voorbereiding meebeslissen over de topiclijst, zodat voor beide onderzoeken de juiste gegevens werden opgebracht. De topiclijst is dus in samenwerking met het lectoraat tot stand gekomen. Hierbij is ervoor gekozen om gebruik te maken van half-gestructureerde interviews, waardoor er voor de respondent ruimte is voor eigen inbreng. Wegens de timing met het lopende onderzoek van het lectoraat Crisisbeheersing van het IFV zijn een aantal van deze interviews, in overleg met de schoolcoach meneer Van Houten, in een vroegtijdig stadium van dit onderzoek gevoerd. De interviews vonden daarom plaats tussen 22 februari en 4 maart 2021. Met behulp van deze interviews konden de beweegredenen van de respondenten worden achterhaald en kon extra informatie worden verzameld (Verhoeven, 2011). Zo konden de resultaten uit dit onderzoeks-deel inzicht geven in de redenen waarom veiligheidsregio's zich wel of niet voorbereid voelen en duidelijk maken waarom bepaalde barrières worden ervaren. Daarnaast zorgde de vroege timing van deze interviews voor de mogelijkheid om de enquêtes (voor de afname) op basis van de informatie uit deze interviews aan te passen. Van deze mogelijkheid is ook gebruik gemaakt. De topiclijst diende hierbij als richtlijn en niet als vast schema. Het doel van de interviews was dan ook het verkrijgen van meer informatie, zodat deze informatie kon dienen als oriëntatie voor de richting en antwoordopties van de enquêtes. De topiclijst voor de interviews is te vinden in Bijlage 2.

3.1.3 Enquêtes

De twee enquêtes vormen samen de tweede dataverzamelingsmethode waarvan binnen dit onderzoek gebruik is gemaakt. Voor deze volgorde is gekozen, omdat de kwalitatieve resultaten uit de interviews aanleiding konden geven voor de aanvulling van antwoordopties in de enquêtes. Tevens waren de interviews al gepland in het kader van een lopend onderzoek van het IFV, waardoor de enquêtes als tweede dataverzamelingsmethode werden toegepast. Deze dataverzameling vond plaats tussen 29 maart en 16 april 2021.

De enquêtes zijn op verzoek van het IFV en op basis van eerdere onderzoeken van het IFV waarbij enquêtes werden gebruikt, zo kort mogelijk gehouden. Het was daarom wenselijk dat een respondent er ruwweg maximaal tien minuten over deed om de enquête in te vullen. Langere enquêtes zorgden in het verleden namelijk voor een hoger percentage 'afvallers', oftewel respondenten die vroegtijdig stoppen met het invullen van de enquête. Om de enquêtes kort te houden, is daarom niet specifiek ingegaan op alle mogelijke soorten dreigingen. Daarnaast is een dergelijke lijst niet uitputtend, aangezien de digitale dreiging bestaat uit zogenoemde 'ongekende'

risico's, die elke dag weer veranderen (Evaluatiecommissie Wet veiligheidsregio's, 2020). Ook waren de vragen in de enquêtes voornamelijk subjectief, aangezien met name is ingegaan op de barrières die veiligheidsregio's volgens de respondenten mogelijk ervaren bij de voorbereiding op de (gevolg)bestrijding van interne en externe cyberincidenten. De enquêtevragen zijn op basis van de triade van Poiesz, literatuuronderzoek en de uitkomsten van de interviews tot stand gekomen. Zo is op basis van de interviews en literatuur zoals het Nationaal Crisisplan Digitaal, de Nederlandse Cybersecurityagenda en de Handreiking Cybergevolgbestrijding eerst onderzocht welke factoren nodig zijn voor de voorbereiding op interne en externe cyberincidenten. De benodigde factoren voor de cyberweerbaarheid zijn te vinden in Bijlage 3 en de benodigde factoren voor de cybergevolgbestrijding zijn te vinden in Bijlage 4. Op basis van deze factoren zijn vervolgens de enquêtes ontworpen, waarin het triademodel van Poiesz leidend was voor de indeling en het chronologische verband leidend was voor de volgorde van de vraagstelling.

Daarnaast is bijvoorbeeld ook ingegaan op wat de respondenten denken/verwachten dat veiligheidsregio's nodig hebben om invulling te geven aan de voorbereiding op cyberweerbaarheid/gevolgbestrijding; de interventies. De keuze voor een subjectieve benadering is in overleg met de opdrachtgever gemaakt. Uit eerdere onderzoeken van het IFV bleek dat de mate van 'sociaal gewenste antwoorden' bij deze doelgroep en respondenten zeer beperkt bleef. Zo bleek bijvoorbeeld dat veiligheidsregio's hun eigen preparatie op cybergevolgbestrijding slechts met een 6 beoordeelden (IFV, 2020a). De enquêtes zijn binnen het programma Qualtrics opgebouwd en zijn door de respondenten binnen dit programma ingevuld. De vragenlijsten voor de enquêtes zijn te vinden in Bijlagen 5 en 6.

3.2 Selectie van eenheden

3.2.1 De respondenten

De groep waarover, op basis van de resultaten van dit onderzoek, uitspraken worden gedaan zijn de 25 veiligheidsregio's in Nederland. Het is normaal gesproken belangrijk dat de respondenten een afspiegeling zijn van deze groep, zodat dan op basis van de resultaten uit de interviews en enquêtes conclusies over de doelgroep kunnen worden getrokken. De steekproef moet daarom in een bepaald aantal kenmerken lijken op de doelgroep. Toch was deze populatievaliditeit in dit geval lastig te bereiken. Veiligheidsregio's zijn immers geen personen die je kan benaderen voor een enquête of kan interviewen. Om deze reden zijn verschillende 'experts' benaderd als respondent. De experts werden, vanuit hun functie of vanuit hun deelname aan een werkgroep, benaderd om deel te nemen aan het interview of een enquête. Er is dus sprake van een selecte steekproef, waardoor meestal niet wordt voldaan aan de betrouwbaarheids- en validiteitseisen. Echter was het doel van de interviews en de enquêtes niet om conclusies te generaliseren naar de populatie (onmogelijk, want de populatie is geen groep mensen), maar om de resultaten binnen het IFV en de veiligheidsregio's te gebruiken.

In dit geval zijn de respondenten niet de 'juiste' afspiegeling van deze groep, maar zijn wel in staat om iets te zeggen over deze groep; te weten de voorbereiding op de (gevolg)bestrijding van cyberincidenten binnen veiligheidsregio's. Hierbij zijn de respondenten niet gevraagd om *namens* de organisatie te spreken, maar wel *over* de organisatie en hun ervaringen daarbinnen.

3.2.2 De selectie en benadering van de respondenten voor de interviews

De selecte steekproef voor de interviews is met behulp van de zogenoemde 'purposive-methode' getrokken. Dit houdt in dat de respondenten werden geselecteerd op basis van bepaalde kenmerken, waardoor de informatie dáár is gehaald waar deze zit (Verhoeven, 2011). In dit geval zijn personen benaderd die bijvoorbeeld werkzaam zijn binnen een veiligheidsregio of (binnen hun functie) partner zijn van een veiligheidsregio, waardoor deze personen kennis hebben over de crisisstructuur binnen

veiligheidsregio's en de bestrijding van cyberincidenten. Zo zijn medewerkers van veiligheidsregio Fryslân, veiligheidsregio Twente en veiligheidsregio Utrecht geïnterviewd. Daarnaast is met een medewerker van het Instituut voor Veiligheids- en Crisismanagement gesproken voor een nationaal beeld en met een medewerker van de Vereniging van Nederlandse Gemeenten gesproken voor een lokaal/regionaal beeld. Een lijst met de namen, functies en organisaties van de respondenten die deelnamen aan de interviews is te vinden in Bijlage 2.1.

De respondenten zijn in overleg met de opdrachtgever geselecteerd, waarbij specifiek is gekeken naar de onderwerpen die de betreffende respondent binnen zijn/haar veiligheidsregio in de portefeuille heeft. Zo zijn wel ambtenaren gekozen met 'cybergevolgbestrijding' in de portefeuille, maar geen ambtenaren met 'brandweerzorg'. De respondenten zijn via de mail benaderd, met daarbij de vraag of ze wilden deelnemen aan een gesprek van ongeveer een uur. Bij een positieve reactie werd in verband met Covid-19 een Teams-afspraak ingepland.

3.2.3 De selectie en benadering van de respondenten voor de enquêtes

De selecte steekproef voor de enquêtes zijn ook met behulp van de zogenoemde 'purposive-methode' getrokken. Voor de ene enquête waarbij de cyberweerbaarheid van veiligheidsregio's centraal staat, zijn de leden van de VR-ISAC bevraagd. Dit Information Sharing and Analysis Center voor veiligheidsregio's is een samenwerkingsverband waarbij informatiespecialisten uit de 25 veiligheidsregio's en het IFV kennis en expertise uit op het gebied van digitale dreigingen en incidenten uitwisselen (IFV, 2020d). Hierdoor kan binnen vertrouwelijke setting informatie over cyberincidenten, dreigingen, kwetsbaarheden en maatregelen onderling worden uitgewisseld. Uit het bovenstaande blijkt dat deze groep respondenten kennis heeft van de (voorbereiding op) interne cyberweerbaarheid van veiligheidsregio's. Daarom werden de leden van deze groep (+/- 25 personen) benaderd voor deelname aan de enquête over cyberweerbaarheid. De opdrachtgever verwachtte, op basis van eerdere uitvragen met behulp van enquêtes, dat de respons rond de 75% zou liggen. Echter hebben 12 personen uit deze groep gereageerd, wat neerkomt op zo'n 50%.

Voor de andere enquête, waar de cybergevolgbestrijding van veiligheidsregio's centraal staat, zijn de leden van de werkgroep Digitale ontwrichting bevraagd. De werkgroep bestaat (voornamelijk) uit leden van verschillende veiligheidsregio's, waarbinnen thema's als digitale ontwrichting en cybergevolgbestrijding veelvuldig worden besproken (IFV, 2019). Uit het bovenstaande blijkt dat deze werkgroep kennis heeft van de (voorbereiding op) externe cybergevolgbestrijding van veiligheidsregio's. Daarom zijn de leden van deze werkgroep (+/- 20 personen) benaderd voor deelname aan de enquête over cybergevolgbestrijding. De opdrachtgever verwachtte, op basis van eerdere uitvragen met behulp van enquêtes, dat de respons rond de 75% zou liggen. Echter hebben 14 personen uit deze groep gereageerd, wat neerkomt op zo'n 70%.

Deze groepen respondenten zijn via de mail benaderd, met daarbij de vraag om de enquête binnen twee weken in te vullen. De mail bevatte een link van het programma Qualtrics waarbinnen de enquête door de respondenten kon worden ingevuld. Tussentijds is een herinnering naar deze groepen gestuurd en na de tweede week is een extra herinnering gestuurd, waarna de enquête nog een week kon worden ingevuld.

3.3 Operationalisering

De onderzoeksvragen zijn allemaal gedeeltelijk beantwoord op basis van informatie uit de interviews en de enquêtes. In deze paragraaf wordt per onderzoeksvraag uitgelegd wat de variabelen zijn en welke indicatoren zijn gebruikt voor de beantwoording van de onderzoeksvragen. De eenheid van elke onderzoeksvraag omvat de 25 veiligheidsregio's in Nederland. De indicatoren die afkomstig zijn van de interviews zijn bedoeld als richtlijn, aangezien tijdens deze interviews uiteraard is

doorgevraagd. De topiclijst voor deze interviews is te vinden in Bijlage 2. De indicatoren van de enquêtes stonden wel grotendeels vast. De stellingen in de enquêtes zijn op basis van een Likertschaal (5 punten) beantwoord. Duidelijke overzichten van de enquêtes zijn in Bijlagen 5 en 6 te raadplegen.

3.3.1 Indicatoren onderzoeksvraag 1

De eerste onderzoeksvraag: “In hoeverre bestaat binnen veiligheidsregio’s bewustzijn van intern- en extern-gerichte dreigingen uit het digitale domein?”, bestaat uit één variabele. Deze variabele is de mate waarin binnen veiligheidsregio’s bewustzijn bestaat van de dreigingen uit het digitale domein.

Om deze variabele te onderzoeken is gebruik gemaakt van meerdere dataverzamelingsmethoden. Zo is in de interviews gebruik gemaakt van een aantal indicatoren om er achter te komen in hoeverre binnen veiligheidsregio’s bewustzijn bestaat van de dreigingen uit het cyberdomein. Deze indicatoren zijn te vinden in Bijlage 2. Ook in de enquêtes is ingegaan op deze vraag. Zo is in de enquête over cyberweerbaarheid gebruik gemaakt van meerdere indicatoren om er achter te komen in hoeverre binnen veiligheidsregio’s bewustzijn bestaat van de dreigingen uit het cyberdomein op de eigen organisatie. Hierbij kan worden gedacht aan stellingen over de mate waarop het management of mensen op operationeel niveau bewust zijn van de dreiging op de eigen organisatie. Deze indicatoren zijn te vinden in Bijlage 5. Daarnaast is in de enquête over cybergevolgbestrijding gebruik gemaakt van indicatoren, om er achter te komen in hoeverre binnen veiligheidsregio’s bewustzijn bestaat van de dreigingen uit het cyberdomein op de regio. Hierbij kan worden gedacht aan stellingen over de mate waarop het management of mensen op operationeel niveau bewust zijn van de dreiging op de regio. Deze zijn te vinden in Bijlage 6.

3.3.2 Indicatoren onderzoeksvraag 2

De tweede onderzoeksvraag: “Welke barrières ervaren veiligheidsregio’s bij de voorbereiding op de bestrijding van interne cyberincidenten?”, bestaat uit drie variabelen. De eerste variabele is de mate waarin veiligheidsregio’s motivatie-gerelateerde barrières ervaren bij de voorbereiding op de bestrijding van interne cyberincidenten. De tweede variabele is de mate waarin veiligheidsregio’s capaciteit-gerelateerde barrières ervaren bij de voorbereiding op de bestrijding van interne cyberincidenten. De derde variabele is de mate waarin veiligheidsregio’s gelegenheids-gerelateerde barrières ervaren bij de voorbereiding op de bestrijding van interne cyberincidenten.

Om deze variabelen te onderzoeken zijn meerdere dataverzamelingsmethoden toegepast. Zo zijn in de interviews verschillende indicatoren gebruikt om er achter te komen welke motivatie-, capaciteit- en gelegenheids-gerelateerde barrières worden ervaren. Deze zijn te vinden in Bijlage 2 en zijn onder andere toegespitst op het urgentiebesef, de kennis en de vaardigheden binnen de veiligheidsregio’s. Daarnaast is in de enquête over cyberweerbaarheid ingegaan op de mate waarin binnen de veiligheidsregio’s motivatie, kennis, kunde, samenwerking, middelen, tijd en geld aanwezig is voor (de voorbereiding op) de bestrijding van interne cyberincidenten. Hierbij kon bij de beantwoording uiteraard ook worden aangegeven wanneer dit niet aanwezig was en of dit als barrière werd gezien. Deze indicatoren zijn te vinden in Bijlage 5.

3.3.3 Indicatoren onderzoeksvraag 3

De derde onderzoeksvraag: “Welke barrières ervaren veiligheidsregio’s bij de voorbereiding op de gevolgbestrijding van externe cyberincidenten?”, bestaat uit drie variabelen. De eerste variabele is de mate waarin veiligheidsregio’s motivatie-gerelateerde barrières ervaren bij de voorbereiding op de gevolgbestrijding van externe cyberincidenten. De tweede variabele is de mate waarin veiligheidsregio’s capaciteit-gerelateerde barrières ervaren bij de voorbereiding op de gevolgbestrijding van externe cyberincidenten. De derde variabele is de mate waarin

veiligheidsregio's gelegenheids-gerelateerde barrières ervaren bij de voorbereiding op de gevolgbestrijding van externe cyberincidenten.

Om deze variabelen te onderzoeken zijn meerdere dataverzamelingsmethoden toegepast. Zo zijn in de interviews verschillende indicatoren gebruikt om er achter te komen welke motivatie-, capaciteit- en gelegenheids-gerelateerde barrières worden ervaren. Deze zijn te vinden in Bijlage 2 en zijn onder andere toegespitst op het urgentiebesef, de kennis en de vaardigheden binnen de veiligheidsregio's. Daarnaast is in de enquête over cybergevolgbestrijding ingegaan op de mate waarin binnen de veiligheidsregio's motivatie, kennis, kunde, samenwerking, middelen, tijd en geld aanwezig is voor (de voorbereiding op) de gevolgbestrijding van externe cyberincidenten. Hierbij kon bij de beantwoording uiteraard ook worden aangegeven wanneer dit niet aanwezig was en of dit als barrière werd gezien. Deze indicatoren zijn te vinden in Bijlage 6.

3.3.4 Indicatoren onderzoeksvraag 4

De vierde onderzoeksvraag: "Welke gerichte interventies kunnen veiligheidsregio's helpen bij de voorbereiding op de bestrijding van interne cyberincidenten?", bestaat uit drie variabelen. De eerste variabele is de mate waarin leren-gerelateerde interventies veiligheidsregio's kunnen helpen bij de voorbereiding op de bestrijding van interne cyberincidenten. De tweede variabele is de mate waarin motivatie-gerelateerde interventies veiligheidsregio's kunnen helpen bij de voorbereiding op de bestrijding van interne cyberincidenten. De derde variabele is de mate waarin faciliteren-gerelateerde interventies veiligheidsregio's kunnen helpen bij de voorbereiding op de bestrijding van interne cyberincidenten.

Om de variabelen te onderzoeken zijn meerdere dataverzamelingsmethoden toegepast. Zo is in de interviews gebruik gemaakt van verschillende indicatoren om er achter te komen welke interventies veiligheidsregio's kunnen helpen. Zo is onder andere ingegaan op de manieren waarop kennis en kunde kan worden vergroot en welke rol oefeningen, scenario's en netwerken hierin hebben. Deze indicatoren zijn te vinden in Bijlage 2. Daarnaast is in de enquête over cyberweerbaarheid ingegaan op de mogelijke interventies die veiligheidsregio's kunnen helpen bij de vergroting van de voorbereiding op de bestrijding van interne cyberincidenten. Deze indicatoren zijn te vinden in Bijlage 5. Tot slot is in het literatuuronderzoek gezocht naar mogelijke en geschikte interventies, die specifiek kunnen helpen bij de barrières die veiligheidsregio's ervaren bij voorbereiding op de bestrijding van interne cyberincidenten. Hierbij kan worden gedacht aan onderzoeken bij andere organisaties waarbij met behulp van het Triade-model van Poiesz is gezocht naar geschikte interventies waardoor de cyberweerbaarheid kan worden vergroot. Zo is (afhankelijk van de barrières) onder andere gebruikgemaakt van de volgende indicatoren, in dit geval zoekopdrachten, om er achter te komen welke interventies veiligheidsregio's kunnen helpen:

Interventies vergroten cyberweerbaarheid	Motivatie vergroten cyberweerbaarheid
Capaciteit vergroten cyberweerbaarheid	Kennis vergroten cyberweerbaarheid
Vaardigheden vergroten cyberweerbaarheid	Netwerk vergroten cyberweerbaarheid
Samenwerking vergroten cyberweerbaarheid	Gelegenheid vergroten cyberweerbaarheid

3.3.5 Indicatoren onderzoeksvraag 5

De vijfde onderzoeksvraag: "Welke gerichte interventies kunnen veiligheidsregio's helpen bij de voorbereiding op de gevolgbestrijding van externe cyberincidenten?", bestaat uit drie variabelen. De eerste variabele is de mate waarin leren-gerelateerde interventies veiligheidsregio's kunnen helpen bij de voorbereiding op de gevolgbestrijding van externe cyberincidenten. De tweede variabele is de mate waarin motivatie-gerelateerde interventies veiligheidsregio's kunnen helpen bij de voorbereiding op de gevolgbestrijding van externe cyberincidenten. De derde variabele is de mate

waarin faciliteren-gerelateerde interventies veiligheidsregio's kunnen helpen bij de voorbereiding op de gevolgbestrijding van externe cyberincidenten.

Om de variabelen te onderzoeken zijn meerdere dataverzamelingsmethoden toegepast. Zo is in de interviews gebruik gemaakt van verschillende indicatoren om er achter te komen welke interventies veiligheidsregio's kunnen helpen. Zo is onder andere ingegaan op de manieren waarop kennis en kunde kan worden vergroot en welke rol oefeningen, scenario's en netwerken hierin hebben. Deze indicatoren zijn te vinden in Bijlage 2. Daarnaast is in de enquête over cybergevolgbestrijding ingegaan op de mogelijke interventies die veiligheidsregio's kunnen helpen bij de vergroting van de voorbereiding op de gevolgbestrijding van externe cyberincidenten. Deze indicatoren zijn te vinden in Bijlage 5. Tot slot is in het literatuuronderzoek gezocht naar mogelijke en geschikte interventies, die specifiek kunnen helpen bij de barrières die veiligheidsregio's ervaren bij voorbereiding op de gevolgbestrijding van externe cyberincidenten. Hierbij kan worden gedacht aan onderzoeken bij andere organisaties waarbij met behulp van het Triade-model van Poiesz is gezocht naar geschikte interventies waardoor de cybergevolgbestrijding kan worden vergroot. Zo is (afhankelijk van de barrières) onder andere gebruikgemaakt van de volgende indicatoren, in dit geval zoekopdrachten, om er achter te komen welke interventies veiligheidsregio's kunnen helpen:

Interventies vergroten cybergevolgbestrijding	Motivatie vergroten cybergevolgbestrijding
Capaciteit vergroten cybergevolgbestrijding	Kennis vergroten cybergevolgbestrijding
Vaardigheden vergroten cybergevolgbestrijding	Netwerk vergroten cybergevolgbestrijding
Samenwerking vergroten cybergevolgbestrijding	Gelegenheid vergroten cybergevolgbestrijding

3.4 Kwaliteitscriteria

Naast de criteria voor bruikbaarheid van het onderzoek, moet het onderzoek ook voldoen aan formele criteria; de betrouwbaarheid en validiteit. In dit hoofdstuk wordt beargumenteerd waarom de gekozen methode tot betrouwbare en valide gegevens heeft geleid en welke maatregelen hiervoor zijn genomen.

3.4.1 Betrouwbaarheid

Een aantal maatregelen zijn genomen om ervoor te zorgen dat dit onderzoek geen toevallige fouten bevat. Deze maatregelen zorgen ervoor dat het onderzoek herhaalbaar is en in dat geval leidt tot dezelfde resultaten (Verhoeven, 2011). Zo is tijdens dit onderzoek gebruik gemaakt van een getrianguleerd ontwerp: een combinatie tussen kwalitatieve en kwantitatieve dataverzamelingsmethoden (Verhoeven, 2011). Door gebruik te maken van dit ontwerp wordt de betrouwbaarheid groter, aangezien de resultaten van de ene methode kunnen worden gecontroleerd met de andere methode. Daarnaast is bij de enquêtes gebruik gemaakt van standaardisering, waardoor de betrouwbaarheid wordt vergroot. Zo werd in de vragenlijst onder andere gebruik gemaakt van de Likertschaal. Bij de interviews en de enquêtes is eveneens de betrouwbaarheid vergroot doordat voor de officiële dataverzameling eerst een pilot werd afgenomen (Verhoeven, 2011). Deze pilot zorgt ervoor dat de betrouwbaarheid van de topiclijst en vragenlijst wordt vergroot. Tot slot is de betrouwbaarheid van de algehele onderzoeksmethode vergroot door middel van peer examinations. Dit houdt in dat collega-onderzoekers de onderzoeksmethode en resultaten van dit onderzoek hebben nalezen.

3.4.2 Validiteit

Ook zijn maatregelen genomen die ervoor zorgen dat dit onderzoek geen systematische fouten bevat. Deze maatregelen zorgen ervoor dat het onderzoek waarheidsgetrouw is (Verhoeven, 2011).

Om ervoor te zorgen dat de resultaten intern valide zijn en dat de juiste conclusies konden worden getrokken, zijn verschillende maatregelen genomen. Zo werd groei (ook wel maturation genoemd) tijdens het onderzoek zo veel mogelijk voorkomen, door het onderzoek binnen 17 weken af te ronden. Deze groei is gericht op veranderingen binnen de respondenten tijdens de onderzoeksperiode, die een negatief effect hebben op de resultaten. Zo kunnen gebeurtenissen tijdens de onderzoeksperiode of vermoeidheid van de respondenten van invloed zijn op de respondenten en hun respons. Het afnemen van de interviews en enquêtes in een korte periode zorgt ervoor dat aanpassingen in meningen of gedrag over de tijd zo veel mogelijk worden voorkomen, waardoor de validiteit toeneemt. Ook met behulp van consistente instrumentatie is de validiteit voor dit onderzoek vergroot. Zo zijn de vragenlijsten bij de enquêtes niet meer veranderd nadat de officiële dataverzameling is gestart (na de laatste aanpassingen op basis van de pilot). Hierdoor kreeg elke respondent een identieke vragenlijst, waardoor er geen vertekening van de resultaten ontstaat en de validiteit dus wordt vergroot (Verhoeven, 2011).

Om ervoor te zorgen dat de resultaten extern valide zijn, moet de steekproef de juiste afspiegeling vormen van de populatie (Verhoeven, 2011). De steekproef moet dus in een bepaald aantal kenmerken lijken op de doelgroep. Toch was deze populatievaliditeit in dit geval lastig te bereiken. Veiligheidsregio's zijn immers geen personen die je kan benaderen voor deelname aan een interview of enquête. Om deze reden zijn experts benaderd als respondenten. Deze experts hebben bijvoorbeeld kennis over de crisisstructuur binnen veiligheidsregio's, zijn binnen hun functie partner van een veiligheidsregio, zijn zelf werkzaam binnen een veiligheidsregio of hebben kennis over de bestrijding van cyberincidenten. In dit geval zijn de respondenten geen 'exacte' afspiegeling van de doelgroep, maar wel een 'juiste' afspiegeling. Ze zijn immers in staat om iets te zeggen over de voorbereiding op de (gevolg)bestrijding van cyberincidenten binnen veiligheidsregio's.

3.5 Data-analyse

Dit hoofdstuk geeft inzicht in de manier waarop de verzamelde data is verwerkt tot bruikbare informatie voor de beantwoording van de onderzoekvragen en hoofdvraag. Hierbij wordt onderscheid gemaakt tussen de kwalitatieve dataverzamelingsmethode (de interviews) en de kwantitatieve dataverzamelingsmethode (de enquêtes).

De resultaten uit de interviews zijn met behulp van protocolanalyse geanalyseerd. Dit houdt in dat de interviews op basis van de opnames zijn getranscribeerd: uitgeschreven tot een stuk tekst. Deze tekst is eerst per interview uitgeschreven in Word en is daarna duidelijk en overzichtelijk samengevoegd in één Excelbestand onder het tabblad 'Invoer'. Dit Excel bestand is te vinden in separate Bijlage 11. De teksten zijn vervolgens doorgenomen, waarbij irrelevante informatie is verwijderd. De overgebleven relevante teksten zijn vervolgens op basis van het onderwerp opgedeeld in fragmenten. Deze fragmenten zijn in het Excelbestand onder een nieuw tabblad 'Fragmenten' weergegeven. Vervolgens zijn de fragmenten open gecodeerd, wat inhoudt dat de fragmenten zijn voorzien van labels. Deze labels geven het onderwerp van het fragment weer en laten dus met weinig woorden zien waar het fragment over gaat. De labels zijn in het Exelbestand achter de betreffende fragmenten genoteerd in een nieuw tabblad 'Codering'. Nadat de fragmenten zijn voorzien van de labels, zijn axiale codeerschema's gemaakt. Hierbij zijn de labels geordend en weergegeven in een bepaalde volgorde/hiërarchie. Deze codeerschema's zijn met behulp van de SmartArt- graphic in Word ontworpen en zijn te vinden in Bijlage 7. Op basis van deze schema's konden de kwalitatieve resultaten worden geanalyseerd en kon de tekst specifiek voor de onderzoeksvragen worden herschreven.

De resultaten uit de enquêtes zijn statistisch geanalyseerd. Dit rekenwerk is door de computer gedaan binnen het programma Qualtrics. Hierbij is per enquêtevraag een rapport opgesteld en zijn de resultaten met behulp van grafieken en tabellen overzichtelijk weergegeven. Daarnaast kunnen binnen dit programma filters worden gebruik om gegevens uit meerdere vragen aan elkaar te koppelen. Hierdoor konden ook de verbanden tussen verschillende variabelen worden onderzocht. De gegevens uit deze rapporten zijn vervolgens per enquête verwerkt in kleine rapporten, die dienden als basis voor de beantwoording van de onderzoeksvragen. Het basisrapport van de resultaten uit de enquête over cyberweerbaarheid is te vinden in Bijlage 8 en het basisrapport van de resultaten uit de enquête over cybergevolgbestrijding is te vinden in Bijlage 9.

4 Resultaten

Om de voorbereiding van veiligheidsregio's op de (gevolg)bestrijding van interne en externe cyberincidenten te verbeteren moeten geschikte interventies worden gevonden, ontworpen en uitgevoerd. Om deze reden wordt in dit hoofdstuk antwoord gegeven op de onderzoeksvragen, die inzicht geven in de geschikte interventies. Zo wordt eerst de eerste onderzoeksvraag beantwoord, waarin wordt ingegaan op de mate waarin veiligheidsregio's zich bewust zijn van de dreigingen uit het digitale domein. Vervolgens wordt uit de beantwoording van onderzoeksvraag twee en drie duidelijk welke capaciteit-, motivatie- en gelegenheids- gerelateerde barrières veiligheidsregio's ervaren bij de voorbereiding op de (gevolg)bestrijding van interne en externe cyberincidenten. Tot slot blijkt uit de beantwoording van onderzoekvraag vier en vijf welke bijpassende en gerichte interventies veiligheidsregio's kunnen helpen bij de voorbereiding op de (gevolg)bestrijding van interne en externe cyberincidenten.

4.1 Bewustzijn van de dreiging binnen veiligheidsregio's

In dit hoofdstuk is beschreven in hoeverre veiligheidsregio's zich bewust zijn van de grootte en ernst van de dreiging uit het digitale domein op zowel de eigen organisatie als de regio. Hierdoor kan worden onderzocht óf en zo ja wélke interventies de voorbereiding van veiligheidsregio's op de (gevolg)bestrijding van interne en externe cyberincidenten kan verbeteren. Om deze reden wordt in dit hoofdstuk de eerste onderzoeksvraag beantwoord:

> *"In hoeverre bestaat binnen veiligheidsregio's bewustzijn van intern- en extern-gerichte dreigingen uit het digitale domein?*

4.1.1 Bewustzijn van de dreiging op de eigen organisatie

Om als veiligheidsregio gemotiveerd te zijn, de capaciteit te winnen en/of hebben en in de gelegenheid te zijn of worden gesteld om voor te bereiden op interne en externe cyberincidenten, moet er sprake zijn van een bepaald bewustzijn: het bewustzijn van de dreiging.

Volgens de respondenten uit de VR-ISAC is het management van de gemiddelde veiligheidsregio redelijk bewust van de dreiging uit het digitale domein op de eigen organisatie. Zo was 58% van de respondenten het enigszins of helemaal eens met de stelling dat het management bewust is van de dreiging uit het digitale domein op de eigen organisatie. Procentueel gezien is dit niet een heel hoog aantal. Ook uit de interviews is gebleken dat het management van de gemiddelde veiligheidsregio niet altijd bewust is van de drieging op de eigen organisatie. Zo komt de dreiging die op volle breedte wordt gevoeld niet altijd verder dan Ransomware of DDoS, terwijl de dreiging groter en breder is. Zo wordt in het Nationaal Crisisplan Digitaal bijvoorbeeld gehint op kwaadwillende statelijke actoren. Wel geven respondenten in zowel de interviews als de enquête aan dat het bewustwordingsniveau, mede dankzij de media-aandacht en het toenemende aantal incidenten, binnen veiligheidsregio's toeneemt.

Uit dezelfde enquête kwam naar voren dat de mensen op operationeel niveau binnen de veiligheidsregio's bewust lijken te zijn van de dreiging op de eigen organisatie. Zo is 67% van de respondenten het enigszins of helemaal eens met de stelling dat mensen op operationeel niveau bewust zijn van de dreiging op de eigen organisatie. Wel is in Figuur 5 te zien dat, ten opzichte van de stelling over het bewustzijn van het management, opvallend weinig respondenten het helemaal eens zijn met de stelling. Daarnaast blijkt uit de interviews dat er nog niet veel aandacht wordt besteed aan de bewustwording van het personeel. Volgens meerdere respondenten moeten mensen binnen de veiligheidsregio's meer bewust worden van de risico's en de manier waarop ze zich veilig moeten gedragen.

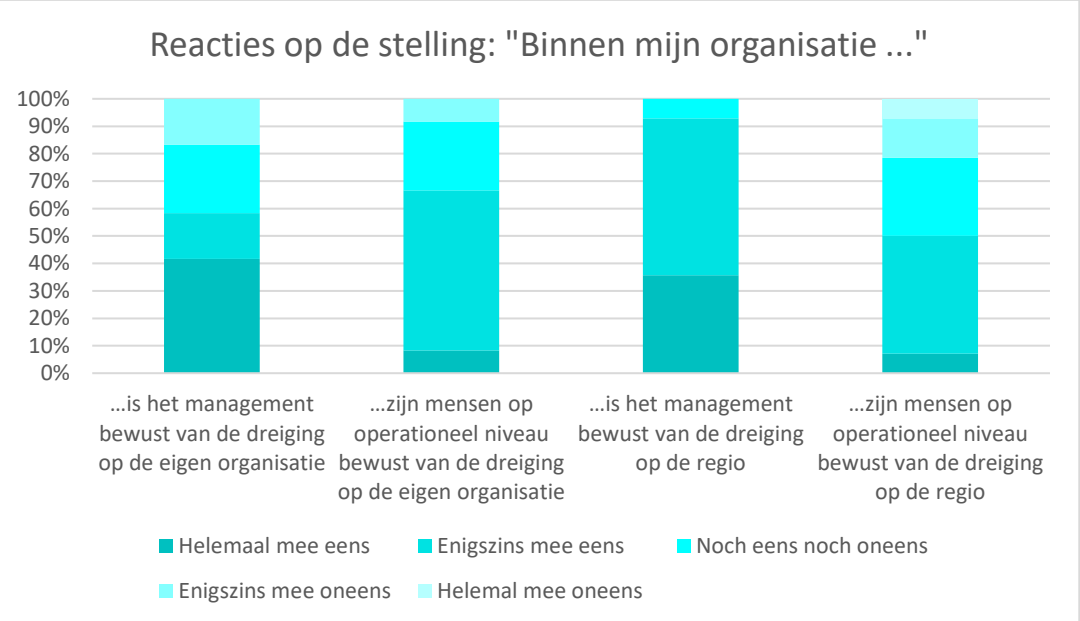
"AL IS HET ALLEEN MAAR DAT JE EEN MENS MEEGEEFT DAT JE DE PC MOET SLUITEN OF LOCKEN ALS JE EVEN EEN KOPJE KOFFIE HAALT. DIT WORDT OOK NIET TEGEN ELKAAR GEZEGD EN DUS HANG DEZE SFEER DAAR OOK HELEMAAL NIET."

Naast de ICT-afdeling, is de technische kennis op het gebied van cyber binnen de veiligheidsregio's vrij laag. De dreigingen landen daardoor niet altijd op de juiste plek en bij de juiste personen, waardoor veiligheidsregio's over het algemeen redelijk relaxed op de fiets zitten. Ondanks deze (verbeter)punten zijn de respondenten redelijk positief over het bewustzijn van de dreiging uit het digitale domein op de eigen organisatie.

4.1.2 Bewustzijn van de dreiging op de regio

Het bewustzijn van de dreiging uit het digitale domein op de regio lijkt nog groter te zijn. Volgens de respondenten uit de werkgroep digitale ontwrichting en cyber is het management van de gemiddelde veiligheidsregio meer dan bewust van de dreiging uit het digitale domein op de regio. Zo is 93% van de respondenten het enigszins of helemaal eens met de stelling dat het management bewust is van de dreiging uit het digitale domein op de regio. Opvallend is dat de mensen op operationeel niveau hier volgens deze respondenten minder bewust van zijn. Zo is de helft van de respondenten het enigszins of helemaal eens met de stelling dat mensen op operationeel niveau bewust zijn van de dreiging op de regio. Dit verschil van bewustzijn tussen deze groepen is goed te zien in Figuur 5.

Volgens de respons uit de interviews komt dit mede door de onveranderde wettelijke taken van veiligheidsregio's. In de basis bestaat dat uit het redden van mensenlevens en de situatie zo snel mogelijk terugbrengen naar normaal. Een digitaal incident in de regio is, als het in het digitale domein blijft, voor veiligheidsregio's niet relevant. Er gaan in dat geval geen mensenlevens verloren, er is geen gevaar voor de volksgezondheid en de onrust blijft beperkt. Pas wanneer er sprake is van een maatschappelijke impact, te weten maatschappelijke onrust en/of maatschappelijke ontwrichting, zal een veiligheidsregio ingrijpen en de gevolgen bestrijden. Mede door deze scheiding is het voor veiligheidsregio's lastig om in te schatten wanneer welke verplichtingen van toepassing zijn en welke dreigingen daarbij spelen. Daarnaast is de oorzaak van een incident of de dreiging niet altijd relevant voor de gevolgbestrijding.



Figuur 5 Het bewustzijn van de dreiging op de eigen organisatie en de regio

4.2 Barrières bij de bestrijding van interne cyberincidenten

In dit hoofdstuk is beschreven welke motivatie-, capaciteit- en gelegenheids- gerelateerde barrières veiligheidsregio's ervaren bij de voorbereiding op de bestrijding van interne cyberincidenten. Hierdoor kan worden onderzocht óf en zo ja wélke interventies de voorbereiding van veiligheidsregio's op de bestrijding van interne cyberincidenten kan verbeteren. Om deze reden wordt in dit hoofdstuk de tweede onderzoeksvraag beantwoord:

> *"Welke barrières ervaren veiligheidsregio's bij de voorbereiding op de bestrijding van interne cyberincidenten?"*

4.2.1 Motivatie

De motivatie van veiligheidsregio's om voor te bereiden op de bestrijding van interne cyberincidenten lijkt onderling te verschillen. Volgens slechts de helft van de respondenten vindt het management en de mensen op operationeel niveau deze voorbereiding belangrijk. Daarnaast is de mate waarin de voorbereiding op interne cyberincidenten prioriteit krijgt binnen de veiligheidsregio's niet altijd hoog. Zo geeft een derde van de respondenten aan dat zijn/haar veiligheidsregio beperkt prioriteit geeft aan de voorbereiding op interne cyberincidenten.

Als daarnaast wordt gekeken naar de manier waarop de motivatie tot uiting komt, door te kijken of cyberincidenten worden meegenomen in de continuïteitsplannen van de veiligheidsregio's, blijkt dat dergelijke scenario's niet altijd worden meegenomen in de planvorming. Volgens enkel de helft van de respondenten wordt dit plan door veiligheidsregio's geschreven met het besef van cyber en de mogelijke dreiging, waarbij bijvoorbeeld de uitval van ICT en elektriciteit wordt meegenomen. Daarnaast blijkt dat deze plannen niet altijd mee gaan met de tijd. In het plan is een uitwijklocatie bijvoorbeeld wel beschreven, maar daarbij wordt niet aangegeven of de software dan mee gaat en of dat dan nog past als de veiligheidsregio geraakt wordt. Het besef is er volgens de meeste respondenten absoluut, maar als hard wordt gevraagd naar stukken of maatregelen die zijn genomen, dan is dat volgens hen in mindere mate terug te vinden. Dat is echter wel per veiligheidsregio anders en over het algemeen kan volgens de respondenten worden gezegd dat de bewustwording en motivatie bij zowel het management als mensen op operationeel niveau groeit.

4.2.2 Capaciteit

Zoals in het theoretisch kader is beschreven, is de capaciteit van veiligheidsregio's voor (de voorbereiding op) de bestrijding van interne cyberincidenten afhankelijk van kennis, vaardigheden en samenwerking.

Kennis

De kennis die nodig is om voor te bereiden op mogelijke interne cyberincidenten is volgens de meerderheid van de respondenten binnen de veiligheidsregio's aanwezig. Waar volgens de respondenten met name de moeilijkheden liggen, is de kennis die nodig is voor de bestrijding zelf. Deze is volgens de respondenten niet altijd aanwezig. Zo wordt van onder andere het in beeld brengen van de keteneffecten (verbondenheid van het geraakte systeem met andere systemen), het inschatten van de mogelijke oorzaak (technische storing, menselijke fout of doelbewuste aanval) en het inventariseren van de schade op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie (zoals verlies van vertrouwelijke gegevens) door de meerderheid van de respondenten aangegeven dat de kennis voor deze activiteiten niet of beperkt aanwezig is binnen de veiligheidsregio's.

Daarnaast geeft de meerderheid van de respondenten aan dat deze kennis idealiter intern wordt belegd, wat aangeeft dat het kennisniveau voor de bovenstaande activiteiten kan en zou moeten

worden vergroot. Met name de ICT-medewerkers en/of de CISO zijn volgens de respondenten geschikte personen om de kennis intern bij te beleggen. Volgens de respondenten zou hierbij (daarnaast) met name moeten worden gefocust op de kennis van afhankelijkheden, processen en effecten op deze processen, de kennis van cyberrisicomanagement (het signaleren, beoordelen en treffen van maatregelen) en forensische kennis.

Vaardigheden

De meeste vaardigheden om voor te bereiden op mogelijke interne cyberincidenten zijn volgens de meerderheid van de respondenten ook binnen de veiligheidsregio's aanwezig. Enkel de vaardigheden voor het opstellen van scenario's voor cyberoefeningen zijn volgens de respondenten in mindere mate aanwezig, terwijl de meerderheid wel aangeeft deze vaardigheden idealiter intern te willen beleggen.

Wat betreft de vaardigheden voor het bestrijden van een intern incident, zijn de vaardigheden voor het inschatten van de mogelijke oorzaak (technische storing, menselijke fout of doelbewuste aanval) en de vaardigheden voor het vormen van een (technisch)oplossingsperspectief volgens de respondenten nauwelijks aanwezig binnen de veiligheidsregio's. Zo is respectievelijk enkel 17% en 25% van de respondenten van mening dat hun veiligheidsregio de vaardigheden voor deze activiteiten bezit. Ook de vaardigheden voor het in beeld brengen van de keteneffecten (verbondenheid van het geraakte systeem met andere systemen), het inventariseren van de schade op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie (zoals verlies van vertrouwelijke gegevens) en het bestrijden of verkleinen van de gevolgen/effecten van het incident zijn volgens de respondenten in mindere mate aanwezig binnen de veiligheidsregio's. Bij al deze activiteiten met betrekking tot de bestrijding van een intern cyberincident, is door de meerderheid van de respondenten aangegeven dat de vaardigheden die hiervoor nodig zijn idealiter intern worden gelegd. Net als bij kennis zijn met name de ICT-medewerkers en/of de CISO volgens de respondenten geschikte personen om de vaardigheden intern bij te beleggen.

Samenwerking

De samenwerking die nodig is bij (de voorbereiding op) de bestrijding van interne cyberincidenten is volgens gemiddeld 70% van de respondenten in goede staat. Veel respondenten geven aan dat een groot deel van de kennis en vaardigheden idealiter extern wordt belegd en dat veel van de ICT binnen de veiligheidsregio's is uitbesteed, wat volgens de respondenten vraag om goede afspraken met externe partners, partijen en leveranciers. De regie ligt daarom in (de voorbereiding op) de bestrijding van een cyberincident bij de betreffende veiligheidsregio, waarbij de technische oplossing het beste extern kan worden verkregen. Met name de Private kennis-/adviesbureaus (100%),de landelijke voorziening Veiligheidsregio Information Sharing and Analysis Center (96%) en het Nationaal Cyber Security Center (92%) zijn volgens de respondenten geschikte externe partijen om in de voorbereiding en tijdens de bestrijding mee samen te werken.

Het feit dat veel kennis en vaardigheden extern kan worden belegd betekend volgens de respondenten niet dat veiligheidsregio's niks meer hoeven te doen of te weten. Het leren van 'lessons learned' van andere veiligheidsregio's is volgens hen een belangrijk aandachtspunt. Zeker aangezien een kwart van de respondenten van mening is dat veiligheidsregio's beperkt zicht hebben op interne deskundigen voor de incidentbestrijding van een intern cyberincident.

4.2.3 Gelegenheid

Zoals in het theoretisch kader is beschreven, is de gelegenheid van veiligheidsregio's voor (de voorbereiding op) de bestrijding van interne cyberincidenten afhankelijk van middelen, tijd en geld.

Middelen

De middelen die voor veiligheidsregio's beschikbaar zijn en/of beschikbaar worden gesteld om voor te bereiden op de bestrijding van interne cyberincidenten is volgens de respondenten erg beperkt. Zo vindt 67% van de respondenten dat veiligheidsregio's onvoldoende technische middelen (zoals systemen) en hulpmiddelen (zoals handreikingen, methodieken en protocollen) bezitten om voor te kunnen bereiden op interne cyberincidenten. Daarnaast geeft 92% van de respondenten aan dat veiligheidsregio's onvoldoende personeel bezitten, dat is toegerust om voor te bereiden op interne cyberincidenten.

"HET EEN EN ANDER IS IN WORDING, MAAR DE HUIDIGE SITUATIE IS ONVOLDOENDE."

Uit zowel de interviews als de enquête blijkt dat het onderwerp 'cyberweerbaarheid' de afgelopen jaren onderbelicht is geweest. Deels heeft dit volgens de respondenten geresulteerd in een achterstand van kennis, kunde en middelen.

Tijd

Volgens alle respondenten reserveren de veiligheidsregio's beperkt of onvoldoende tijd voor de voorbereiding op interne cyberincidenten. Zo is een derde van de respondenten het enigszins oneens met de stelling dat veiligheidsregio's voldoende tijd reserveren voor (de voorbereiding op) de bestrijding van interne cyberincidenten en is twee derde het zelfs helemaal oneens met deze stelling.

Geld

Ook de hoeveelheid financiële middelen die veiligheidsregio's reserveren voor de voorbereiding op de bestrijding van interne cyberincidenten is volgens 83% van de respondenten beperkt of onvoldoende. De financiële middelen uit de structurele beleidsmatige cyclus, afkomstig van de gemeenten binnen de regio, zijn volgens de respondenten niet makkelijk te verkrijgen aangezien de meeste gemeenten op een bezuinigingsspoor zitten. De financiële middelen voor trajecten, afkomstig van onder andere het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), het ministerie van Justitie & Veiligheid (J&V) en het NCSC, worden volgens een aantal respondenten ook niet optimaal benut. Veel ministeries stellen volgens hen wel voldoende geld beschikbaar, maar praten onderling nauwelijks over de randvoorwaarden waar dit geld voor is bedoeld. Zo heeft BZK en J&V een pot voor het versterken van de cyberweerbaarheid. Bij de aanvraag van deze middelen moeten veiligheidsregio's wel een plan schrijven voor de besteding van het geld, maar interdepartementaal is er weinig aandacht voor wat de ministeries daarmee willen bereiken. Zo speculeren een aantal respondenten over de mogelijkheden voor het oprichten van een landelijk Security Operations Center (SOC) en een Computer Emergency Respons Team (CERT) voor de veiligheidsregio's, wanneer deze financiële middelen van verschillende ministeries wordt gebundeld.

In Bijlage 10 is in een overzichtelijke tabel te zien welke barrières binnen veiligheidsregio's spelen bij de voorbereiding op de bestrijding van interne cyberincidenten; de cyberweerbaarheid.

4.3 Barrières bij de gevolgbestrijding van externe cyberincidenten

In dit hoofdstuk is beschreven welke motivatie-, capaciteit- en gelegenheids- gerelateerde barrières veiligheidsregio's ervaren bij de voorbereiding op de gevolgbestrijding van externe cyberincidenten. Hierdoor kan worden onderzocht óf en zo ja wélke interventies de voorbereiding van veiligheidsregio's op de gevolgbestrijding van externe cyberincidenten kan verbeteren. Om deze reden wordt in dit hoofdstuk de derde onderzoeksvraag beantwoord:

> *"Welke barrières ervaren veiligheidsregio's bij de voorbereiding op de gevolgbestrijding van externe cyberincidenten?"*

4.3.1 Motivatie

De motivatie van veiligheidsregio's om voor te bereiden op de gevolgbestrijding van externe cyberincidenten lijkt groot te zijn. Zo vindt 93% van de respondenten dat het management deze voorbereiding belangrijk vindt. Dit besef van belang ligt bij de mensen op operationeel niveau iets lager. 57% van de respondenten vindt dat de mensen op operationeel niveau de voorbereiding belangrijk vinden. Ondanks het bewustzijn en de mate waarin de voorbereiding belangrijk wordt gevonden, krijgt het onderwerp niet altijd prioriteit binnen de veiligheidsregio's. Eén op de vijf respondenten is van mening dat zijn/haar veiligheidsregio beperkt prioriteit geeft aan de voorbereiding op externe cyberincidenten.

Als daarnaast wordt gekeken naar de manier waarop de motivatie tot uiting komt, door te kijken of daadwerkelijk aandacht wordt besteed aan cybergevolgbestrijding middels oefeningen, blijkt dat de motivatie de afgelopen jaren sterk is gestegen. Er wordt binnen een aantal veiligheidsregio's veel geoefend met cyber en het onderwerp staat bij veel veiligheidsregio's op de agenda, alleen verschilt dit onderling sterk. Daarnaast ontstaat bij het onderwerp 'cybergevolgbestrijding' snel discussie over de taakomschrijving en verantwoordelijkheden. Volgens de Wet veiligheidsregio's zijn veiligheidsregio's bij een extern cyberincidenten alleen aan zet wanneer er sprake is van maatschappelijke ontwrichting ten gevolge van dit incident. De belemmering hierin is de vraag 'waar willen we van zijn', omdat deze vraag per veiligheidsregio anders kan worden beantwoord. Hoe ver veiligheidsregio's bijvoorbeeld willen gaan in de voorbereiding op deze taak of het voorkomen van externe cyberincidenten in de regio is per veiligheidsregio verschillend. Het besef van de eigen taak met betrekking tot de cybergevolgbestrijding is volgens de respondenten een belangrijke factor voor de mate waarin voorbereiding hierop belangrijk wordt gevonden.

4.3.2 Capaciteit

Zoals in het theoretisch kader is beschreven, is de capaciteit van veiligheidsregio's voor (de voorbereiding op) de gevolgbestrijding van externe cyberincidenten afhankelijk van kennis, vaardigheden en samenwerking.

Kennis

De meeste kennis die nodig is om voor te bereiden op mogelijke externe cyberincidenten is volgens de meerderheid van de respondenten binnen de veiligheidsregio's aanwezig. Wel is het volgens hen nog zoeken naar de dreigingen en risico's die voor de veiligheidsregio's relevant en noodzakelijk zijn om te kennen. Hierbij ligt de focus op vitale bedrijven, maar daarnaast zijn veiligheidsregio's volgens een aantal respondenten onvoldoende bewust van de mogelijke gevaren die schuilgaan bij andere externe bedrijven als gevolg van een cyberincident.

"IK DENK DAT WE ONS ONVOLDOENDE BEWUST ZIJN VAN MOGELIJKE ANDERE GEVAREN DIE SCHUILEN BIJ ANDERE (EXTERNE) BEDRIJVEN ALS GEVOLG VAN EEN CYBERAANVAL. DAARNAAST IS HET LASTIG TE BEPALEN IN HOEVERRE DE VEILIGHEIDSREGIO DAARVOOR AAN DE LAT STAAT EN WAT WIJ DAARIN KUNNEN BETEKENEN."

Daarnaast geven de respondenten aan dat de kennis die nodig is voor de gevolgbestrijding zelf, ook grotendeels aanwezig is. Echter speelt ook hier de al dan niet onduidelijke taakomschrijving en de invulling van deze taak een rol bij de mate waarin kennis aanwezig is binnen de veiligheidsregio's. Niet alleen bij de voorbereiding op de gevolgbestrijding, door bijvoorbeeld te kijken naar mogelijke dreigingen, maar ook bij de gevolgbestrijding zelf is het voor de crisisfunctionarissen niet altijd duidelijk wat mogelijke cascade/domino-effecten van een cyberincident in de regio zijn. Hiervoor is volgens de respondenten een tekort aan technische kennis bij de functionarissen van de regionale crisisorganisatie, maar moet ook de focus blijven liggen op de effectbestrijding en niet de bestrijding van het incident.

Vaardigheden

De meeste vaardigheden om voor te bereiden op mogelijke externe cyberincidenten zijn volgens de meerderheid van de respondenten ook binnen de veiligheidsregio's aanwezig. Opvallend is dat de vaardigheden voor het vooraf inventariseren van mogelijke maatschappelijke effecten van een extern cyberincident, ten opzichte van de kennis ,in mindere mate aanwezig is. Zo gaf 29% van de respondenten aan dat de vaardigheden voor deze activiteit niet aanwezig zijn. Volgens een aantal respondenten houdt dit verband met de beperkte mate waarin externe bedrijven (die niet vitaal zijn, maar bij een cyberincident wel kunnen zorgen voor maatschappelijk ontwrichting) in beeld zijn. Hierdoor ontstaat de vraag welke maatschappij ontwrichtende schade een cyberincident bij een bedrijf teweeg kan brengen en wat de veiligheidsregio's hier in de voorbereiding of tijdens de gevolgbestrijding mee kunnen.

Wat betreft de vaardigheden voor de gevolgbestrijding zelf, zijn volgens de respondenten veel van deze aanwezig. Daarnaast zijn alle respondenten het ermee eens dat deze vaardigheden idealiter intern worden belegd bij medewerkers crisisbeheersing. Volgens een aantal respondenten zou hierbij wel meer moeten worden gekeken naar vaardigheden voor het managen van atypische en langdurige maatschappelijk ontwrichtende incidenten, aangezien veiligheidsregio's over het algemeen veel zijn gericht op kortstondige incidenten.

Samenwerking

De samenwerking die nodig is bij (de voorbereiding op) de bestrijding van interne cyberincidenten is volgens de respondenten niet optimaal. Zo hebben veiligheidsregio's volgens 36% van de respondenten geen zicht op interne deskundigen voor de gevolgbestrijding. Daarnaast vindt 36% dat veiligheidsregio's onvoldoende weten waar ze verantwoordelijk voor zijn bij de gevolgbestrijding van externe cyberincidenten en vindt 29% dat veiligheidsregio's onvoldoende weten welke verantwoordelijkheden de andere betrokken teams hebben bij de gevolgbestrijding van externe cyberincidenten.

Ook voor de samenwerking lijkt de onduidelijkheid met betrekking tot de taakomschrijving en de invulling van deze taak een rol te spelen. Respondenten geven in zowel de enquête als de interviews aan dat het hierdoor lastig is om in te schatten wie waarmee kan helpen en welke verhouding er is met partners binnen het cyberdomein. Het is hierdoor lastig om uit te zoeken welke netwerkpartners relevant kunnen zijn voor (de voorbereiding op) de gevolgbestrijding van externe cyberincidenten. Ook is het hierdoor lastig om onderling afspraken te maken over bijvoorbeeld bereikbaarheid en verantwoordelijkheden ten tijde van een extern cyberincident.

"KENNISSEN IN HET DIGITALE DOMEIN IS MISSCHIEN NOG WEL BELANGRIJKER DAN EIGEN KENNIS."

Daarnaast geven respondenten aan dat nog onvoldoende externe expertise op zowel regionaal als nationaal niveau wordt ingeschakeld. Zo zijn er regionaal goede contacten met de partners over operationele voorbereiding, maar dit omvat niet de ICT-specialisten.

4.3.3 Gelegenheid

Zoals in het theoretisch kader is beschreven, is de gelegenheid van veiligheidsregio's voor (de voorbereiding op) de gevolgbestrijding van externe cyberincidenten afhankelijk van middelen, tijd en geld.

Middelen

De middelen die voor veiligheidsregio's beschikbaar zijn en/of beschikbaar worden gesteld om voor te bereiden op de gevolgbestrijding van externe cyberincidenten zijn volgens de respondenten erg beperkt. Zo vindt 57% van de respondenten dat veiligheidsregio's onvoldoende technische middelen (zoals systemen) en hulpmiddelen (zoals handreikingen, methodieken en protocollen) bezitten om voor te kunnen bereiden op interne cyberincidenten. Daarnaast geeft 79% van de respondenten aan dat veiligheidsregio's onvoldoende personeel bezitten, dat is toegerust om voor te bereiden op interne cyberincidenten.

Tijd

Volgens 79% van de respondenten reserveren veiligheidsregio's beperkt of onvoldoende tijd voor de voorbereiding op externe cyberincidenten. Daarnaast zijn veiligheidsregio's volgens een aantal respondenten wel gemotiveerd, tótdat het geld of capaciteit kost.

Geld

Ook de hoeveelheid financiële middelen die veiligheidsregio's reserveren voor de voorbereiding op de gevolgbestrijding van interne cyberincidenten is volgens 86% van de respondenten beperkt of onvoldoende. De financiële middelen uit de structurele beleidsmatige cyclus, afkomstig van de gemeenten binnen de regio, zijn volgens de respondenten niet makkelijk te verkrijgen aangezien de meeste gemeenten op een bezuinigingsspoor zitten. Het maken van een afweging tussen wat belangrijk is en wat minder belangrijk is, is volgens de respondenten voor de lokale bestuurders lastig.

> "GELD KAN MAAR EEN KEER WORDEN UITGEGEVEN EN WANNEER DIT JAAR EEN PANDEMIE HEERST, VOLGEND JAAR EEN BOSBRAND EN HET JAAR DAARNA EEN OVERSTROMING…"

In Bijlage 10 is in een overzichtelijke tabel te zien welke barrières binnen veiligheidsregio's spelen bij de voorbereiding op de gevolgbestrijding van externe cyberincidenten; de cybergevolgbestrijding.

4.4 Interventies voor de bestrijding van interne cyberincidenten

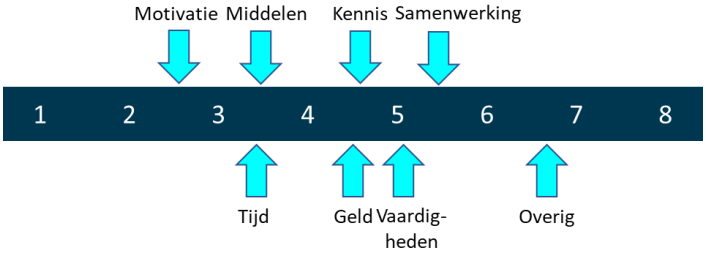
In dit hoofdstuk is op basis van de barrières uit onderzoeksvraag twee (hoofdstuk 4.2), beschreven welke bijpassende en gerichte interventies veiligheidsregio's kunnen helpen bij de voorbereiding op de bestrijding van interne cyberincidenten. In dit hoofdstuk wordt de vierde onderzoeksvraag beantwoord:

> *"Welke gerichte interventies kunnen veiligheidsregio's helpen bij de voorbereiding op de bestrijding van interne cyberincidenten?"*

Met behulp van het Triade-model is in hoofdstuk 5.2 systematisch onderzocht welke uitdagingen/barrières door veiligheidsregio's worden ervaren bij de voorbereiding op interne cyberincidenten. De volgende barrières bij (de voorbereiding op) de bestrijding van interne cyberincidenten worden volgens de respondenten het meeste ervaren:

- Er is sprake van een lage tot matige motivatie, die echter wel steeds groter wordt. → interventie richten op motiveren
- De kennis voor het in beeld brengen van de keteneffecten (verbondenheid van het geraakte systeem met andere systemen), het inschatten van de mogelijke oorzaak (technische storing, menselijke fout of doelbewuste aanval) en het inventariseren van de schade op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie (zoals verlies van vertrouwelijke gegevens is niet of beperkt aanwezig. → interventie richten op leren
- De vaardigheden voor het inschatten van de mogelijke oorzaak (technische storing, menselijke fout of doelbewuste aanval) en de vaardigheden voor het vormen van een (technisch)oplossingsperspectief is niet of beperkt aanwezig. → interventie richten op leren
- De technische middelen (zoals systemen) en hulpmiddelen (zoals handreikingen, methodieken en protocollen) zijn niet of beperkt aanwezig en het aantal personeelsleden dat is toegerust om voor te bereiden op interne cyberincidenten in onvoldoende. → interventie richten op faciliteren
- Er is onvoldoende of beperkt tijd en geld beschikbaar om voor te bereiden op de bestrijding van interne cyberincidenten. → interventie richten op faciliteren

Nu de bovenstaande barrières bekend zijn, is het mogelijk om deze (gedeeltelijk) weg te nemen met behulp van gerichte interventies. De respondenten hebben daarbij zelf hun voorkeur aangegeven voor de onderwerpen en richtingen van interventies, die uiteraard zijn meegenomen in de uitwerking van de interventies. Als het aan de respondenten ligt worden deze interventies vooral gericht op het vergroten van de motivatie bij zowel hat management als mensen op operationeel niveau. Daarnaast wordt ook het vergroten van de hoeveelheid beschikbare tijd en middelen veel genoemd als aandachtspunten voor mogelijke interventies. Geld, kennis, vaardigheden en netwerken/samenwerking zijn minder vaak genoemd. In Figuur 6 is te zien op welke plek de respondenten de verschillende aandachtpunten gemiddeld hebben neergezet, met op nummer 1 de belangrijkste aandachtpunten en op nummer 8 de minst belangrijke aandachtspunten.



Figuur 6 Aandachtspunten interventies cyberweerbaarheid

4.4.1 Interventie(s) gericht op motiveren: theorieën, onderzoek en gesprek

Motivatie wordt door de respondenten het belangrijkste aandachtspunten gevonden voor interventies om de voorbereiding op interne cyberincidenten te verbeteren. Daarnaast krijgt cyberweerbaarheid binnen veel veiligheidsregio's geen prioriteit en de motivatie om voor te breiden op interne cyberincidenten is binnen veel veiligheidsregio's beperkt of matig, terwijl het besef van de dreiging aanwezig lijkt te zijn.

Volgens het Extended Parralel Processing model (EPPM) van Witte en de Protectie Motivatie Theorie (PMT) van Rogers bestaat deze motivatie echter niet alleen uit het inzien van de dreiging (Witte, 1992; Rogers, 1975). Volgens deze theorieën moeten veiligheidsregio's bewust zijn van:

1. De eigen kwetsbaarheid ten opzichte van de dreiging
2. De ernst van de dreiging
3. De effectiviteit van het aanbevolen/gewenste gedrag (voorbereiding op de bestrijding)
4. De eigen effectiviteit met betrekking tot de uitvoering van dit aanbevolen/gewenste gedrag

Veiligheidsregio's moeten dus niet alleen bewust zijn van het gevaar, maar ook van de effectiviteit van voorbereidende maatregelen. Uit de beantwoording van de eerste onderzoeksvraag is gebleken dat veiligheidsregio's volgens de respondenten redelijk bewust zijn van de dreiging. Wat echter niet is getest, is de mate waarin het management van de gemiddelde veiligheidsregio bewust is van de eigen kwetsbaarheid en de effectiviteit van de voorbereiding op de bestrijding van interne cyberincidenten. Het zou kunnen zijn dat het management van veel veiligheidsregio's bewust is van de dreiging, alleen niet direct bewust is van het feit dat de eigen organisatie vatbaar is voor deze dreiging, waardoor voorbereidend gedrag uitblijft. Daarnaast kan het zijn dat het management bewust is van de dreiging en kwetsbaarheden, maar niet inziet dat voorbereidend gedrag effectief of mogelijk is. Daarnaast kan de motivatie ook samenhangen met gebrek aan middelen en menskracht of kennis over verantwoordelijkheid en bevoegdheden.

In dit opzicht is verdiepend onderzoek nodig naar de achterliggende oorzaken van de motivatie van veiligheidsregio's voor het al dan niet uitvoeren van voorbereidend gedrag, waarbij met behulp van het EPPM en de PMT wordt gesproken met het management van de veiligheidsregio's. Daarnaast kan nader statistisch onderzoek naar de samenhang van de verschillende factoren zoals kennis, vaardigheden, samenwerking en motivatie ook meer duidelijkheid geven. De prioritering van de voorbereiding op interne cyberincidenten kan hier tevens ook goed in worden meegenomen.

> "IK DENK DAT OP DIT VLAK (CYBERWEERBAARHEID) NOG VEEL TE WINNEN IS. DAT HEEFT ALLES TE MAKEN MET BEWUSTZIJN VAN HET PROBLEEM EN IN STAAT ZIJN DE JUISTE BEVEILIGINGSMAATREGELEN TE TREFFEN, EN HIER OOK OP HET HOOGSTE NIVEAU IN DE ORGANISATIE AANDACHT VOOR HEBBEN. MEER BEWUSTZIJN IN ALLE LAGEN VAN DE ORGANISATIE KAN EEN BELANGRIJKE ROL SPELEN OM DIT TE VERBETEREN, JUIST OOK AAN DE BESTUURSTAFEL."
>
> HESTER SOMSEN, PLAATSVERVANGEND NATIONAAL COÖRDINATOR TERRORISMEBESTRIJDING EN VEILIGHEID (NCTV) EN DIRECTEUR CYBERSECURITY EN STATELIJKE DREIGINGE (NCSC, 2021).

Vervolgens kan worden gekeken naar manieren waarop de voorbereiding kan worden vergroot. Volgens hoogleraar Gedragsverandering & Maatschappij Rick van Baaren en Smart Society-onderzoeker Kevin Hengstz bestaan vijf gedragsveranderingsstrategieën voor cyberdreigingen:

1. Meer informatie en bewustwording;
2. Mensen laten ervaren hoe kwetsbaar ze zijn;
3. Zorgen voor intrinsieke motivatie bij mensen;
4. Mensen snappen het wel, ze moeten het gewoon gaan doen;
5. Mensen ontzorgen en het zo makkelijk mogelijk maken (Motivaction, 2021).

Intrinsieke motivatie is van buiten af moeilijk te beïnvloeden, maar de andere vier strategieën kunnen op basis van de uitkomsten van het onderzoek naar achterliggende oorzaken voor de motivatie individueel en gecombineerd worden toegepast. Zo kan het eerste punt binnen veiligheidsregio's worden toegepast door zowel het management als medewerkers te informeren (middels bijvoorbeeld campagnes, netwerkdagen of Webinars) over de dreiging op de eigen organisatie en de huidige situatie wat betreft voorbereidingen. Het tweede punt kan eveneens middels campagnes, netwerkdagen of Webinars worden toegepast, door middel van cybergames. Een aantal van deze games zijn al beschikbaar voor veiligheidsregio's, waardoor leden van het management van veiligheidsregio's zelf kunnen ervaren wat kwetsbaarheden zijn, hoe deze kunnen worden aangevochten en wat de gevolgen van een cyberincident op de organisatie kunnen zijn. Het vierde en vijfde punt kunnen worden toegepast door te informeren en te laten zien hoe kan worden voorbereid op de bestrijding van interne cyberincidenten en hoe veel (en welke) middelen, tijd, geld en personeelsleden daarvoor benodigd zijn.

4.4.2 Interventie(s) gericht op faciliteren en leren: ontwikkeling van middelen

Naast het laten zien welke middelen benodigd zijn, zouden bepaalde technische middelen of hulpmiddelen zoals handreikingen, methodieken en protocollen ook daadwerkelijk kunnen worden aangereikt of samen met veiligheidsregio's kunnen worden ontwikkeld. Zeker aangezien veel respondenten aangeven, de interventies te willen richten op het ontwikkelen en beschikbaar stellen van middelen. Hierbij kan volgens de respondenten worden gedacht aan hulpmiddelen die houvast bieden voor het ontwikkelen van draaiboeken en scenario's voor oefeningen of hulpmiddelen voor het inzichtelijk maken van informatiestromen. Daarnaast is onder andere behoefte aan middelen voor de vergroting van:

- Kennis voor het in beeld brengen van de keteneffecten (verbondenheid van het geraakte systeem met andere systemen).
- Kennis en vaardigheden voor het inschatten van de mogelijke oorzaak (technische storing, menselijke fout of doelbewuste aanval).
- Kennis voor het inventariseren van de schade op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie (zoals verlies van vertrouwelijke gegevens).
- Vaardigheden voor het vormen van een (technisch)oplossingsperspectief.

Dit soort handreikingen, methodieken en protocollen zouden wat betreft de respondenten idealiter door of met behulp van kennis en vaardigheden van het NCSC, Private kennis-/adviesbureaus zoals Fox-IT en de VR-ISAC worden ontwikkeld. Mogelijk kunnen deze partijen daarnaast het IFV en veiligheidsregio's ondersteunen bij de ontwikkeling van opleidingen, trainingen en oefeningen voor de vergroting van de bovenstaande kennisaspecten en vaardigheden. Een combinatie van ICT-medewerkers en de CISO binnen elke veiligheidsregio is volgens de respondenten een geschikt construct om de (opgedane) kennis en vaardigheden en het beheer van middelen bij te beleggen.

De technische middelen zoals systemen zouden daarnaast idealiter extern belegd worden middels een VR-SOC en VR-CERT. De monitoring op dreigingen, ongeregeldheden en aanvallen vindt dan extern plaats, evenals de incidentbestrijding en werkzaamheden omtrent herstel. De uitbesteding van deze activiteiten en/of de opzet van dergelijke organisaties moet nog gerealiseerd worden, maar de mogelijkheden worden binnen het kader van 'het versnellingsplan' op dit moment onderzocht en beschreven.

4.5 Interventies voor de gevolgbestrijding van externe cyberincidenten

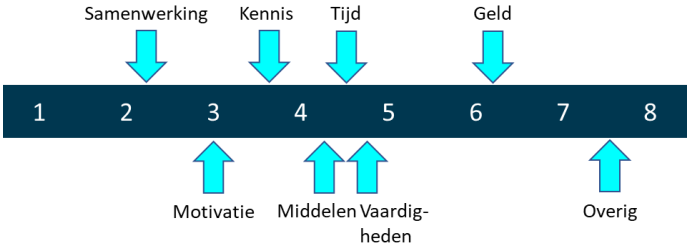
In dit hoofdstuk is op basis van de barrières uit onderzoeksvraag drie (hoofdstuk 4.3), beschreven welke bijpassende en gerichte interventies veiligheidsregio's kunnen helpen bij de voorbereiding op de gevolgbestrijding van externe cyberincidenten. In dit hoofdstuk wordt de vijfde onderzoeksvraag beantwoord:

> *"Welke gerichte interventies kunnen veiligheidsregio's helpen bij de voorbereiding op de gevolgbestrijding van externe cyberincidenten?"*

Met behulp van het Triade-model is in hoofdstuk 5.3 systematisch onderzocht welke uitdagingen/barrières door veiligheidsregio's worden ervaren bij de voorbereiding op externe cyberincidenten. De volgende barrières bij (de voorbereiding op) de gevolgbestrijding van externe cyberincidenten worden volgens de respondenten het meeste ervaren:

- Cyberweerbaarheid krijgt ondanks het bewustzijn en de motivatie niet altijd prioriteit binnen de veiligheidsregio's. → interventie richten op motiveren
- De kennis voor het in beeld brengen van de noodzakelijke en relevante dreigingen binnen de regio bij niet-vitale organisaties en de kennis voor het inschatten van mogelijke cascade-effecten van een cyberincident in de regio is beperkt. → interventie richten op leren
- De vaardigheden voor het vooraf inventariseren van mogelijke maatschappelijke effecten van een extern cyberincident is in mindere mate aanwezig. → interventie richten op leren
- De samenwerking die nodig is bij (de voorbereiding op) de bestrijding van interne cyberincidenten is beperkt, aangezien een deel geen zicht heeft op interne deskundigen voor de gevolgbestrijding en onvoldoende weet waar ze zelf en andere partijen verantwoordelijk voor zijn bij de gevolgbestrijding van externe cyberincidenten. → interventie richten op leren
- De technische middelen (zoals systemen) en hulpmiddelen (zoals handreikingen, methodieken en protocollen) zijn niet of beperkt aanwezig en het aantal personeelsleden dat is toegerust om voor te bereiden op externe cyberincidenten in onvoldoende. → interventie richten op faciliteren
- Er is onvoldoende of beperkt tijd en geld beschikbaar om voor te bereiden op de gevolgbestrijding van externe cyberincidenten. →interventie richten op faciliteren

Nu de bovenstaande barrières bekend zijn, is het mogelijk om deze (gedeeltelijk) weg te nemen met behulp van gerichte interventies. Daarnaast hebben de respondenten zelf hun voorkeur aangegeven voor de onderwerpen en richtingen van interventies, die uiteraard zijn meegenomen in de uitwerking van de interventies. Als het aan de respondenten ligt worden de interventies vooral gericht op het vergroten en verbeteren van de samenwerking en netwerken. Daarnaast wordt ook het vergroten van de motivatie en kennis veel genoemd als aandachtspunt voor mogelijke interventies. Middelen, tijd, vaardigheden en geld worden minder belangrijk gevonden. In Figuur 7 is te zien op welke plek de respondenten de verschillende aandachtpunten gemiddeld hebben neergezet, met op nummer 1 de belangrijkste aandachtpunten en op nummer 8 de minst belangrijke aandachtspunten.



Figuur 7 Aandachtspunten interventies cybergevolgbestrijding

4.5.1 Interventie(s) gericht op leren: samenwerking als grootste tandwiel

Op het gebied van kennis, vaardigheden en samenwerking worden binnen veiligheidsregio's barrières ervaren. Toch lijkt het erop dat deze barrières, die in eerste instantie op zichzelf lijken te staan, verband houden. Volgens de respondenten is de onduidelijkheid met betrekking tot de taakomschrijving en de invulling van deze taak een overeenkomstige achterliggende oorzaak voor deze barrières. Desondanks hoeft de interventie volgens een aantal respondenten niet per se te worden gericht op 'het aanscherpen van regelgeving', maar moet deze worden gericht op het maken van duidelijke afspraken met regionale en landelijke netwerkpartners. Juist de samenwerking moet volgens hen centraal staan bij het verbeteren van de voorbereiding op externe cyberincidenten.

De toenadering tot partners zorgt niet alleen voor een beter beeld van de taken, verantwoordelijkheden en wederzijdse verwachtingen, maar kan ook worden ingeschakeld voor externe expertise. Zo kan ook de kennis en vaardigheden middels goede samenwerking en netwerken worden vergroot. Op regionaal niveau zijn al veel goede contacten met de partners over operationele voorbereiding, maar dit omvat vaak niet de ICT-specialisten. Ondanks dat veel respondenten aangeven geen beeld te hebben van interne deskundigen, weten ze wel goed te verwoorden hoe deze regionale netwerken er idealiter uit komen te zien. Zo wordt graag een combinatie gemaakt van mensen met technische kennis en vaardigheden zoals ICT-medewerkers of CISO's en mensen met kennis en vaardigheden van/voor crisismanagement zoals de crisisfunctionarissen. Een dergelijk netwerk kan bijvoorbeeld helpen bij het inzichtelijk maken van de kwetsbaarheden en dreigingen en de (maatschappelijke) cascade/domino-effecten van een cyberincident in de regio. Daarnaast is dit netwerk uitermate geschikt om cyber-crisissituaties mee te oefenen, om ook de kennis en vaardigheden voor de gevolgbestrijding op te frissen en te vergroten.

Figuur 8 Samenwerking als grootste tandwiel

Ook is er behoefte aan een landelijk netwerk waarin afspraken kunnen worden gemaakt en kennis en vaardigheden kunnen worden uitgewisseld. Onder andere het NCSC, de VR-ISAC, de 25 veiligheidsregio's en vitale partners zijn gewenste deelnemers, waarmee een combinatie wordt gemaakt van technische kennis en vaardigheden en 'crisiskennis en -vaardigheden'. Het voordeel van een dergelijk landelijknetwerk is dat niet alle 25 veiligheidsregio's individueel hoeven te investeren in de vergroting van kennis en vaardigheden. Een landelijk netwerk kan ervoor zorgen dat de opgedane kennis en vaardigheden op landelijk niveau worden geborgd en gedeeld. Onder andere middels gezamenlijke opleidingen, trainingen en oefeningen waarin de volgende thema's centraal staan:

- Het in beeld brengen van de relevante dreigingen bij niet-vitale organisaties binnen de regio
- Het inschatten van mogelijke cascade-effecten van een cyberincident in de regio
- het vooraf inventariseren van mogelijke maatschappelijke effecten van een extern cyberincident.

"CRISISMANAGEMENT IS RELATIEMANAGEMENT: JE MOET ELKAAR WETEN TE VINDEN. OEFENEN IS HIERBIJ CRUCIAAL."

HESTER SOMSEN, PLAATSVERVANGEND NATIONAAL COÖRDINATOR TERRORISMEBESTRIJDING EN VEILIGHEID (NCTV) EN DIRECTEUR CYBERSECURITY EN STATELIJKE DREIGINGEN (NCSC, 2021).

4.5.2 Interventie(s) gericht op motiveren en faciliteren: theorieën, onderzoek en gesprek

Cybergevolgbestrijding krijgt ondanks het bewustzijn en de motivatie niet altijd prioriteit binnen de veiligheidsregio's. Volgens een aantal respondenten is er sprake van motivatie, maar zodra geld, tijd, middelen of capaciteit nodig is, is deze motivatie vaak snel verdwenen. Dit blijkt ook uit de (volgens de respondenten) beperkte aanwezigheid van technische middelen, hulpmiddelen, personeelsleden en financiële middelen. De ware grootte van de motivatie zou daarom wellicht nog wel eens tegen kunnen vallen, aangezien dit niet altijd tot uiting komt in de prioritering. De motivatie van het management, volgens de respondenten in dit geval de motivatie om te investeren in de voorbereiding op externe cyberincidenten, moet logischerwijs worden vergroot.

Zoals in bovenstaande onderzoeksvraag is beschreven kan verdiepend onderzoek naar de achterliggende oorzaken van de motivatie van veiligheidsregio's voor het al dan niet uitvoeren van voorbereidend gedrag, meer duidelijkheid geven. Met behulp van het EPPM en de PMT kan het beste met het management van de veiligheidsregio's worden gesproken over de eigen kwetsbaarheid ten opzichte van de dreiging, de ernst van de dreiging, de effectiviteit van het aanbevolen/gewenste gedrag en de eigen effectiviteit met betrekking tot de uitvoering van dit aanbevolen/gewenste gedrag (Witte, 1992; Rogers, 1975). Het management speelt immers een sleutelrol in het beschikbaar stellen van geld, tijd middelen en capaciteit.

Ook voor het beïnvloeden van de motivatie voor het voorbereidende gedrag op externe cyberincidenten kan gebruik worden gemaakt van de gedragsveranderingsstrategieën van hoogleraar Gedragsverandering & Maatschappij Rick van Baaren en Smart Society-onderzoeker Kevin Hengstz:

1. Meer informatie en bewustwording;
2. Mensen laten ervaren hoe kwetsbaar ze zijn;
3. Zorgen voor intrinsieke motivatie bij mensen;
4. Mensen snappen het wel, ze moeten het gewoon gaan doen;
5. Mensen ontzorgen en het zo makkelijk mogelijk maken (Motivaction, 2021).

Intrinsieke motivatie is van buiten af moeilijk te beïnvloeden, maar de andere vier strategieën kunnen individueel en gecombineerd worden toegepast. Zo kan het eerste punt binnen veiligheidsregio's worden toegepast door zowel het management als medewerkers te informeren (middels bijvoorbeeld campagnes, netwerkdagen of Webinars) over de dreiging op de regio en de huidige situatie wat betreft voorbereidingen. Het tweede punt kan eveneens middels campagnes, netwerkdagen of Webinars worden toegepast, door middel van cybergames. Een aantal van deze games zijn al beschikbaar voor veiligheidsregio's, waardoor leden van het management van veiligheidsregio's zelf kunnen ervaren wat kwetsbaarheden zijn, hoe deze kunnen worden aangevochten en wat de gevolgen van een cyberincident kunnen zijn. Het vierde en vijfde punt kunnen worden toegepast door te informeren en te laten zien hoe kan worden voorbereid op de gevolgbestrijding van externe cyberincidenten en welke middelen daarvoor benodigd zijn. Mogelijk zouden bepaalde technische middelen of hulpmiddelen zoals handreikingen, methodieken en protocollen kunnen worden aangereikt of samen kunnen worden ontwikkeld.

Bij veiligheidsregio's waar het bewustzijn laag is, kan eerst worden ingezet met punt één en bij veiligheidsregio's waar het bewustzijn groot is, maar nog geen actie wordt ondernomen, kan worden ingezet met punt vier en vijf. Daarnaast kan nader statistisch onderzoek naar de samenhang tussen factoren zoals gebrek aan middelen, menskracht, kennis over verantwoordelijkheid en kennis over bevoegdheden meer duidelijkheid geven. Extra onderzoek naar de achterliggende motieven voor de motivatie (en het al dan niet ondernemen van actie) en het gesprek aangaan met het management van de veiligheidsregio's is hierin dus een belangrijk onderdeel.

5 Conclusie

Op basis van de resultaten uit hoofdstuk 4, wordt in dit hoofdstuk de hoofdvraag beantwoord:

> *"Op welke manier kan de voorbereiding van veiligheidsregio's, op de (gevolg)bestrijding van interne en externe cyberincidenten, worden verbeterd?"*

Uit de beantwoording van de voorgaande onderzoeksvragen blijkt dat de voorbereiding op de (gevolg)bestrijding van interne & externe cyberincidenten op verschillende manieren mogelijk is:

Onderzoeksvraag 1: "In hoeverre bestaat binnen veiligheidsregio's bewustzijn van intern- en extern-gerichte dreigingen uit het digitale domein?"

Op basis van de beantwoording van deze eerste onderzoeksvraag, blijkt dat de problemen of moeilijkheden niet bij het bewustzijn van de dreiging liggen. Zowel het management als mensen op operationeel niveau zijn, met een gemiddeld percentage van 67%, aardig bewust zijn van de dreiging op de eigen organisatie en de regio.

Onderzoekvraag 2: "Welke barrières ervaren Veiligheidsregio's bij de voorbereiding op de bestrijding van interne cyberincidenten?"

Uit de beantwoording van de tweede onderzoeksvraag blijkt echter dat de motivatie om voor te bereiden op interne cyberincidenten, ondanks het bewustzijn, niet altijd groot is en dat deze voorbereiding regelmatig geen prioriteit krijgt binnen de veiligheidsregio's. Ook is gebleken dat er onvoldoende of beperkt tijd, geld, middelen en personeel beschikbaar is voor de voorbereiding op de bestrijding van interne cyberincidenten. Volgens de respondenten is dit een gevolg van de lage prioriteit die aan de voorbereiding op interne cyberincidenten wordt gegeven.

Daarnaast is er volgens de respondenten binnen de veiligheidsregio's beperkt kennis voor het in beeld brengen van de keteneffecten, het inschatten van de mogelijke oorzaak en het inventariseren van de schade op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Ook de vaardigheden voor het inschatten van de mogelijke oorzaak en de vaardigheden voor het vormen van een (technisch)oplossingsperspectief zijn volgens de respondenten niet of beperkt aanwezig.

Onderzoekvraag 3: "Welke barrières ervaren Veiligheidsregio's bij de voorbereiding op de gevolgbestrijding van externe cyberincidenten?"

Uit de beantwoording van de derde onderzoeksvraag blijkt dat de motivatie om voor te bereiden op externe cyberincidenten, ondanks het bewustzijn, ook niet altijd groot is en dat deze voorbereiding regelmatig geen prioriteit krijgt binnen de veiligheidsregio's. Daarnaast is ook voor de voorbereiding op de bestrijding van externe cyberincidenten gebleken dat er onvoldoende of beperkt tijd, geld, middelen en personeel beschikbaar is. Volgens de respondenten is dit een gevolg van de lage prioriteit die aan de voorbereiding op externe cyberincidenten wordt gegeven en de onduidelijkheid met betrekking tot de taakomschrijving van veiligheidsregio's bij externe cyberincidenten.

Daarnaast is er volgens de respondenten binnen veiligheidsregio's beperkt kennis voor het in beeld brengen van de noodzakelijke en relevante dreigingen bij niet-vitale organisaties binnen de regio en het inschatten van mogelijke cascade-effecten van een cyberincident in de regio. Ook de vaardigheden voor het vooraf inventariseren van mogelijke maatschappelijke effecten van een extern cyberincident zijn volgens de respondenten in mindere mate aanwezig.

Als laatste is ook de samenwerking die nodig is bij (de voorbereiding op) de gevolgbestrijding van externe cyberincidenten volgens de respondenten beperkt, aangezien 36% geen zicht heeft op interne deskundigen voor de gevolgbestrijding en 36% onvoldoende weet waar ze zelf en andere partijen verantwoordelijk voor zijn bij de gevolgbestrijding van externe cyberincidenten.

Onderzoeksvraag 4: "Welke gerichte interventies kunnen veiligheidsregio's helpen bij de voorbereiding op de bestrijding van interne cyberincidenten?"

Een van de grootste barrières bij (de voorbereiding op) de bestrijding van interne cyberincidenten betrof de beperkte motivatie. Deze is op basis van onderzoeksvraag 2 niet laag vanwege een gebrek aan bewustzijn van de dreiging, maar heeft mogelijk te maken met andere (achterliggende) factoren zoals gebrek aan bewustzijn van de effectiviteit van het aanbevolen/gewenste gedrag of gebrek aan bewustzijn van de eigen effectiviteit met betrekking tot de uitvoering van dit aanbevolen/gewenste gedrag. Om de motivatie te vergroten en gedragsveranderingsstrategieën te kunnen uitwerken en toepassen, moet daarom verdiepend onderzoek worden uitgevoerd, waarbij met behulp van het EPPM en de PMT wordt gekeken naar de achterliggende motieven voor de motivatie. Daarnaast kan de beperkte motivatie ook samenhangen met gebrek aan middelen en menskracht of kennis over verantwoordelijkheid en bevoegdheden. Nader statistisch onderzoek naar de samenhang tussen deze factoren kan hier meer duidelijkheid over geven. Zeker, aangezien de data al beschikbaar is.

Ook is het tekort aan middelen volgens de respondenten een van de prominentste barrières die moet worden aangepakt. Daarom moeten de mogelijkheden voor het ontwikkelen van hulpmiddelen (handreikingen, methodieken en protocollen) en opleidingen, trainingen en oefeningen in samenwerking met het NCSC, Private kennis-/adviesbureaus zoals Fox-IT en de VR-ISAC worden onderzocht. Hiervoor is extra onderzoek nodig wat betreft de specifieke aard van de hulpmiddelen waar behoefte aan is en de partijen die een rol kunnen spelen bij de ontwikkeling van deze middelen. Dit kan (gedeeltelijk) meteen worden toegepast in het lopende cyberkennis en -kunde onderzoek.

Tot slot kan de kennis en vaardigheden binnen veiligheidsregio's worden vergroot door de kennisaspecten en vaardigheden die zoals beschreven in onderzoeksvraag 2 beperkt aanwezig zijn, centraal te stellen bij het ontwikkelen en uitvoeren van hulpmiddelen, opleidingen, trainingen, oefeningen, netwerkdagen en Webinars.

Onderzoeksvraag 5: "Welke gerichte interventies kunnen veiligheidsregio's helpen bij de voorbereiding op de gevolgbestrijding van externe cyberincidenten?"

Het vergroten en verbeteren van nationale en regionale samenwerking is volgens de respondenten de belangrijkste factor voor het verbeteren van de voorbereiding op de gevolgbestrijding van externe cyberincidenten. Binnen deze netwerken moeten mensen met technische kennis en vaardigheden en mensen met kennis en vaardigheden van/voor crisismanagement worden gecombineerd. Op regionaal niveau kan hierbij worden gedacht aan ICT-medewerkers of CISO's en crisisfunctionarissen en op nationaal niveau kan worden gedacht aan het NCSC, de VR-ISAC, de 25 veiligheidsregio's en vitale partners. Het verbeteren van deze regionale en nationale samenwerking kan bijdragen aan het vergroten van kennis en vaardigheden, evenals de verduidelijking van de taakomschrijving.

Daarnaast is ook voor de cybergevolgbestrijding, om dezelfde reden als bij de cyberweerbaarheid, extra onderzoek nodig om de motivatie te vergroten en gedragsveranderingsstrategieën te kunnen uitwerken en toepassen. Ook voor de cybergevolgbestrijding kan met behulp van het EPPM en de PMT wordt gekeken naar de achterliggende motieven voor de motivatie en kan statistisch onderzoek naar de samenhang tussen invloedrijke factoren hier meer duidelijkheid over geven.

Tot slot kan de kennis en vaardigheden binnen veiligheidsregio's worden vergroot door de kennisaspecten en vaardigheden die zoals beschreven in onderzoeksvraag 3 beperkt aanwezig zijn, centraal te stellen bij het ontwikkelen en uitvoeren van hulpmiddelen, opleidingen, trainingen, oefeningen, netwerkdagen en Webinars.

Een combinatie van de interventies in onderzoeksvraag 4 en onderzoeksvraag 5 zal de voorbereiding op de (gevolg)bestrijding van interne en externe cyberincidenten verbeteren.

6 Aanbevelingen

Op basis van de conclusie uit Hoofdstuk 5, wordt in dit hoofdstuk een set aanbevelingen gegeven, die concreet advies geven over de manier waarop de voorbereiding van veiligheidsregio's op de (gevolg)bestrijding van interne en externe cyberincidenten kan worden verbeterd. De aanbevelingen zijn gericht aan het Instituut Fysieke Veiligheid, de opdrachtgever van dit onderzoek.

Aanbevelingen (hiërarchisch gestructureerd) voor de verbetering van de voorbereiding op de bestrijding van interne cyberincidenten:

1. Voer een verdiepend onderzoek uit naar de achterliggende oorzaken van de motivatie van veiligheidsregio's voor het al dan niet uitvoeren van voorbereidend gedrag, waarbij gebruik wordt gemaakt van het EPPM, de PMT en statistisch onderzoek zodat de samenhang tussen invloedrijke factoren duidelijk wordt. Adviseer op basis van de uitkomsten van dit verdiepende onderzoek over de toepassing van gedragsveranderingsstrategieën.
2. Onderzoek de mogelijkheden voor het ontwikkelen van hulpmiddelen (handreikingen, methodieken en protocollen) en opleidingen, trainingen en oefeningen in samenwerking met het NCSC, Private kennis-/adviesbureaus zoals Fox-IT en de VR-ISAC.
3. Stel bij het ontwikkelen en uitvoeren van de bovenstaande hulpmiddelen, opleidingen, trainingen en oefeningen of netwerkdagen en Webinars de volgende kennisaspecten en vaardigheden centraal:
    - Kennis voor het in beeld brengen van de keteneffecten
    - Kennis en vaardigheden voor het inschatten van de mogelijke oorzaak
    - Kennis voor het inventariseren van de schade op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie
    - Vaardigheden voor het vormen van een (technisch)oplossingsperspectief

Aanbevelingen (hiërarchisch gestructureerd) voor de verbetering van de voorbereiding op de gevolgbestrijding van externe cyberincidenten:

1. Adviseer veiligheidsregio's over het opzetten van regionale netwerken, waarin een combinatie wordt gemaakt van mensen met technische kennis en vaardigheden zoals ICT-medewerkers of CISO's en mensen met kennis en vaardigheden van/voor crisismanagement zoals de crisisfunctionarissen.
2. Adviseer en ondersteun (participeer eventueel) in het opzetten van een landelijk netwerk, waarin een combinatie wordt gemaakt van technische kennis en vaardigheden en 'crisiskennis en -vaardigheden'. Het NCSC, de VR-ISAC, de 25 veiligheidsregio's en vitale partners zijn hierin gewenste deelnemers.
3. Voer een verdiepend onderzoek uit naar de achterliggende oorzaken van de motivatie van veiligheidsregio's voor het al dan niet uitvoeren van voorbereidend gedrag, waarbij gebruik wordt gemaakt van het EPPM, de PMT en statistisch onderzoek zodat de samenhang tussen invloedrijke factoren duidelijk wordt. Adviseer op basis van de uitkomsten van dit verdiepende onderzoek over de toepassing van gedragsveranderingsstrategieën.
4. Stel bij het ontwikkelen en uitvoeren van toekomstige opleidingen, trainingen, oefeningen, netwerkdagen en Webinars de volgende kennisaspecten en vaardigheden centraal:
    - Kennis voor het inventariseren van relevante dreigingen bij niet-vitale organisaties
    - Kennis voor het inschatten van mogelijke cascade-effecten van een cyberincident binnen de regio
    - Vaardigheden voor het vooraf inventariseren van mogelijke maatschappelijke effecten van een extern cyberincident

Bibliografie

Berenschot. (2020a). *Handreiking Cybergevolgbestrijding (CGB) G4-gemeenten Deel 1.* Berenschot.

Berenschot. (2020b). *Handreiking Cybergevolgbestrijding (CGB) G4-gemeenten Deel 2.* Berenschot.

Bogaerts, S., & Poiesz, T. (2007). Gedragsverandering bij seksuele delinquenten. In *Maatwerk* (pp. 57-59). Springer.

Brouwer, E. (2021, maart 29). Toegepaste dataverzamelingsmethoden . Hengelo, Overijssel, Nederland.

COT. (z.d.). *Cyber. Van digitale weerbaarheid naar digitale kracht*. Opgehaald van Instituut voor Veiligheids- en Crisismanagement: https://cot.nl/crisismanagement/cyber/

Digital Trust Center. (z.d.). *Cyberbewustwording*. Opgehaald van digitaltrustcenter: https://www.digitaltrustcenter.nl/informatie-advies/cyberbewustwording#:~:text=De%20meeste%20cyberincidenten%20ontstaan%20door,voor%20het%20voorkomen%20van%20incidenten.

Evaluatiecommissie Wet veiligheidsregio's. (2020). *Evaluatie Wet veiligheidsregio's, naar toekomstbestendige crisisbeheersing en brandweerzorg.* Evaluatiecommissie Wet veiligheidsregio's.

Gemeente Hof van Twente. (2020, december 9). *Brief van burgemeester Ellen Nauta aan de inwoners van Hof van Twente over de cyberaanval*. Opgehaald van Gemeente Hof van Twente: https://www.hofvantwente.nl/actueel/nieuws-en-persberichten/nieuwsbericht/archief/2020/12/artikel/brief-van-burgemeester-ellen-nauta-aan-de-inwoners-van-hof-van-twente-over-de-cyberaanval-1778.html

IFV. (2019). *Whitepaper digitale ontwrichting en cyber.* Arnhem: IFV.

IFV. (2020a). *Cyberrisico's en veiligheidsregio's. Hoe beoordelen veiligheidsregio's cyberrisico's?* Arnhem: IFV.

IFV. (2020b). *Cybergevolgbestrijding: lessen uit cyberverstoringen in Nederland.* Arnhem: IFV.

IFV. (2020c). *Versterken van veerkracht. Naar een gezamenlijke aanpak van ongekende crises.* Arnhem: IFV.

IFV. (2020d, juni 29). *Nieuw cyber-inlichtingencentrum voor veiligheidsregio's*. Opgehaald van IFV: https://www.ifv.nl/nieuws/Paginas/Nieuw-cyber-inlichtingencentrum-voor-veiligheidsregios.aspx

IFV. (z.d.). *Over het IFV*. Opgehaald van IFV: https://www.ifv.nl/Paginas/Over-IFV.aspx#tab2

Kennis- en exploitatiecentrum Officiële Overheidspublicaties. (z.d.). *Wet veiligheidsregio's*. Opgehaald van Overheid wettenbank: https://wetten.overheid.nl/BWBR0027466/2021-01-01

Leeuw, A. (2021, februari 19). *Geen gemeente is echt voorbereid op een cybercrisis*. Opgehaald van Binnenlands Bestuur: https://www.binnenlandsbestuur.nl/digitaal/nieuws/geen-gemeente-is-echt-voorbereid-op-een.16121315.lynkx

Motivaction. (2021, februari 4). *Cybersecurity: hoe zorg je voor bewustwording en gedragsverandering?* Opgehaald van Motivaction:

https://www.motivaction.nl/kennisplatform/nieuws-en-persberichten/cybersecurity-hoe-zorg-je-voor-bewustwording-en-gedragsverandering

NCSC. (2021, mei 4). *Cybersecurity moet overal besproken worden.* Opgehaald van NCSC: https://magazines.ncsc.nl/ncscmagazine/2021/01/%E2%80%98cybersecurity-moet-overal-besproken-worden%E2%80%99

NCSC. (2021, februari). *Ontwikkelingen cybersecurity*. Opgehaald van NCSC: https://www.ncsc.nl/actueel/ontwikkelingen-cybersecurity

NCTV. (2018). *Nederlandse Cybersecurity Agenda.* NCTV.

NCTV. (2020a). *Cybersecuritybeeld Nederland.* NCTV.

NCTV. (2020b). *Nationaal Crisisplan Digitaal.* NCTV.

NCTV. (z.d.). *Vitale infrastructuur*. Opgehaald van NCTV: https://www.nctv.nl/onderwerpen/vitale-infrastructuur

Nederstigt, A. (2011). *Gelegenheid alleen maakt nog geen dief: Theoretische, methodologische en operationele suggesties voor een integrale benadering van winkeldiefstal.* Tilburg.

NOS. (2019, juni 24). *Storing KPN: 112 niet bereikbaar, landelijk noodnummer*. Opgehaald van NOS: https://nos.nl/artikel/2290486-storing-kpn-112-niet-bereikbaar-landelijk-noodnummer.html

Poiesz, T. (1999). *Gedragsmanagement. Waarom mensen zich (niet) gedragen.* Wormer: Inmerc BV.

Poiesz, T., & Robben, H. (1996). *Advertising Effects Under Different Combinations of Motivation, Capacity, and Opportunity to Process Information.*

Rijksoverheid. (2020, juni 29). *Grapperhaus: Ontwikkeling digitale dreiging Nederland is zorgwekkend*. Opgehaald van Rijksoverheid: https://www.rijksoverheid.nl/actueel/nieuws/2020/06/29/grapperhaus-ontwikkeling-digitale-dreiging-nederland-is-zorgwekkend

Rijksoverheid. (z.d.). *Landelijk Operationeel Coördinatiecentrum (LOCC)*. Opgehaald van Rijksoverheid: https://www.rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid/organisatie/organogram/directoraat-generaal-politie-en-veiligheidsregio%E2%80%99s-dgpenv/landelijk-operationeel-coordinatiecentrum-locc

Rogers, R. (1975). A protection motivation theory of fear appeals and attitude change. In *Journal of Psychology* (pp. 93-114).

Secura. (z.d.). *Theorie achter SAFE; "Gedrag stuur je door leren, motiveren en faciliteren"*. Opgehaald van Secura: https://www.secura.com/nl/services/mens/safe/theorie-achter-safe

Veiligheidsberaad. (2019). *Bestuurlijk routeboek digitale ontwrichting.*

Veiligheidsberaad. (2020, september 14). Samen slimmer met data, programma informatievoorziening veiligheidsregio's 2020-2025.

Veiligheidsregio Noord- en Oost-Gelderland. (2020, september 13). *Updates VNOG ten aanzien van gijzelsoftware*. Opgehaald van VNOG: https://www.vnog.nl/actueel/nieuws/2290-vnog-getroffen-door-gijzelsoftware

Verhoeven, N. (2011). *Wat is onderzoek? Praktijkboek methoden en technieken voor het hoger onderwijs.* Den Haag: Boom Lemma uitgevers.

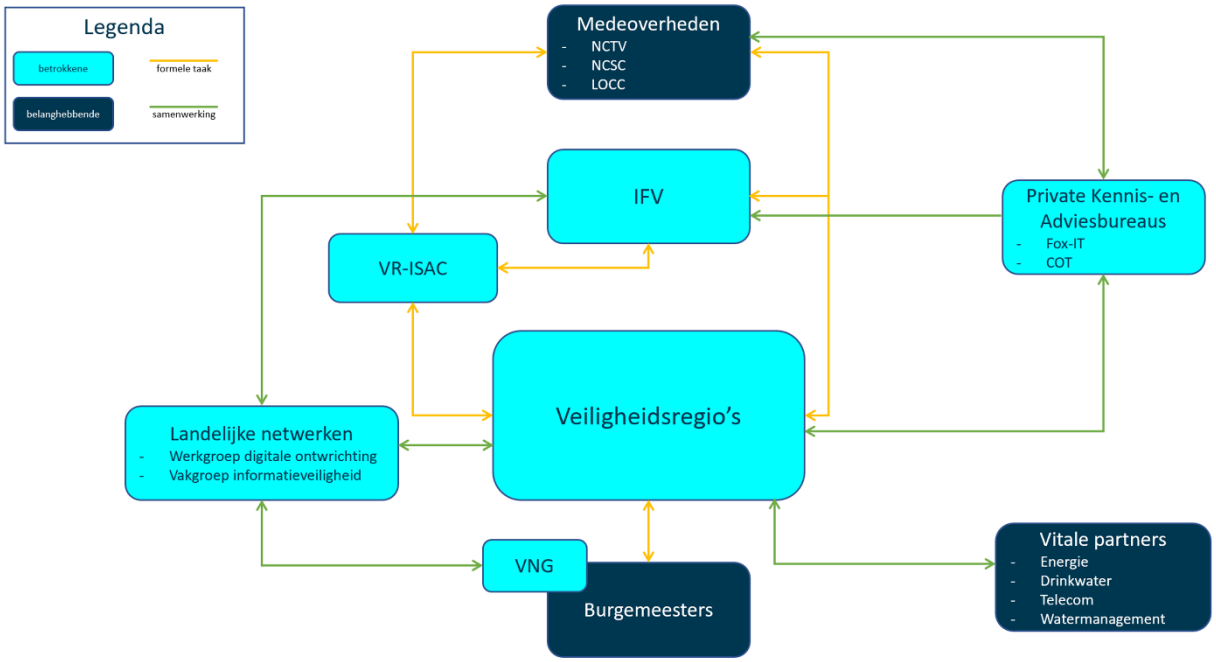
Werkgroep Digitale ontwrichting. (2019).

Wet veiligheidsregio's. (2010, februari 11). Opgehaald van https://wetten.overheid.nl/BWBR0027466/2021-01-01

Witte, K. (1992). Putting the Fear back in Fear Appeals: The Extended Parrales Process Model. In *Commuication Monographs* (pp. 329–349).

Bijlagen

Bijlage 1 Diagram betrokkenen en belanghebbenden



Bijlage 2 Topiclijst interviews

Algemeen:

- Korte introductie over functie
- Organisatie
- Kennis verdeling binnen de organisatie
- Hoe was het vroeger? Hoe heeft bijscholing plaats gevonden.

Risicobesef:

- In hoeverre bestaat binnen veiligheidsregio's voldoende bewustzijn van de uit het digitale domein afkomstige dreigingen op de eigen organisatie? Top down/bottom up
- In hoeverre bestaat binnen veiligheidsregio's voldoende bewustzijn van de uit het digitale domein afkomstige dreigingen op de regio? Top down/bottom up
- In hoeverre zijn veiligheidsregio's voldoende voorbereid op een intern cyberincident? (denk aan gijzelsoftware en datalek)
- In hoeverre zijn veiligheidsregio's voldoende voorbereid op een extern cyberincident? (denk aan een cyberincident met invloed op de vitale infrastructuur)

Motivatie:

- In hoeverre zijn veiligheidsregio's voldoende gemotiveerd om zich voor te bereiden op interne en externe cyberincidenten?
- In hoeverre worden hierin belemmeringen ervaren?
- In hoeverre vinden veiligheidsregio's het belangrijk om zich voor te bereiden op interne en externe cyberincidenten?
- In hoeverre heeft de voorbereiding op interne en externe cyberincidenten prioriteit heeft in veiligheidsregio's?

Capaciteiten, kunde, vaardigheden :

- Welke kunde hebben veiligheidsregio's volgens u nodig voor een goede cyberweerbaarheid (intern)?
- Welke kunde hebben veiligheidsregio's volgens u nodig voor een goede cybergevolgbestrijding (extern)?
- In hoeverre bezitten/vergaren veiligheidsregio's voldoende instrumenten om zich voor te bereiden op de (gevolg)bestrijding van interne en externe cyberincidenten?
- In hoeverre stellen veiligheidsregio's voldoende financiële middelen beschikbaar om zich voor te bereiden op interne en externe cyberincidenten?
- In hoeverre stelt het management van veiligheidsregio's voldoende tijd/uren beschikbaar om voor te bereiden op interne en externe cyberincidenten?

Kennis:

- Welke kennis hebben veiligheidsregio's volgens u nodig voor een goede cyberweerbaarheid (intern)?
- In hoeverre beschikken veiligheidsregio's over deze kennis?
- Hoe kunnen ze deze kennis een plek geven in de reguliere crisisstructuur (COPIU/OT/BT)?
- Welke kennis hebben veiligheidsregio's volgens u nodig voor een goede cybergevolgbestrijding (extern)?
- In hoeverre beschikken veiligheidsregio's over deze kunde?
- Hoe kunnen ze deze kennis een plek geven in de reguliere crisisstructuur?

Algemeen:

- Wat zou veiligheidsregio's kunnen helpen bij het verbreden/vergroten van de kennis en kunde met betrekking tot de bestrijding van cyberincidenten?
    - Cyberoefeningen
    - Interne cyberfunctionaris
    - Cybernetwerken
    - Cyberscenario's
    - Leren van het verleden/ onderzoek naar voorgevallen cyberincidenten

Bijlage 2.1 Respondenten interviews

Organisatie	Naam respondent	Functie respondent
Veiligheidsregio Fryslân	Pim Wanders	Medewerker Vakbekwaamheid Crisisbeheersing
Veiligheidsregio Twente	Jeroen Brouwer	PrivacyOfficer, voorzitter VR-ISAC en voorzitter vakgroep Informatieveiligheid
Veiligheidsregio Utrecht	Puck de Ruijter	Beleidsadviseur Crisisbeheersing
COT Instituut voor Veiligheids- en Crisismanagement	Paul van Hoof	Senior adviseur onderzoeker
Vereniging van Nederlandse Gemeenten (VNG)	Peter van Dijk	Team informatiesamenleving

Bijlage 3 Benodigde factoren voor de voorbereiding op interne cyberincidenten

Cyberweerbaarheid

Motivatie voor (de voorbereiding op) de bestrijding van interne cyberincidenten:

- Het management vindt de voorbereiding op interne cyberincidenten belangrijk.
- Mensen op operationeel niveau vinden de voorbereiding op interne cyberincidenten belangrijk.
- De voorbereiding op interne cyberincidenten heeft hoge prioriteit.
- Cyberincidenten worden meegenomen in het continuïteitsplan.

Kennis voor de voorbereiding op de bestrijding van interne cyberincidenten:

- Het inventariseren van mogelijke cyberdreigingen op de eigen organisatie.
- Het vooraf inventariseren van mogelijke effecten van een intern cyberincident.
- Het in beeld brengen van de verbondenheid van/tussen verschillende interne systemen.
- Het inventariseren van vitale (bedrijfs)processen.

Kennis voor de bestrijding van interne cyberincidenten:

- Het identificeren van de geraakte systemen.
- Het in beeld brengen van de keteneffecten (verbondenheid van het geraakte systeem met andere systemen).
- Het inschatten van de mogelijke oorzaak (technische storing, menselijke fout of doelbewuste aanval).
- Het inventariseren van de schade op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie (zoals verlies van vertrouwelijke gegevens).
- Het inventariseren van de schade op ICT-systemen.
- Het inschatten van de impact op organisatieprocessen (bijvoorbeeld hulp- of dienstverlening).
- Het inschatten van de duur van de verstoring.
- Het vinden van een (technisch) oplossingsperspectief.
- Het bestrijden van de bron van de verstoring.
- Het bestrijden of verkleinen van de gevolgen/ effecten van het incident.
- Het herstellen van de schade aan de ICT-systemen.

Vaardigheden voor de voorbereiding op de bestrijding interne cyberincidenten:

- Het inventariseren van mogelijke cyberdreigingen op de eigen organisatie.
- Het vooraf inventariseren van de mogelijke effecten van een intern cyberincident.
- Het in beeld brengen van ketenrisico’s (verbondenheid van/tussen verschillende interne systemen).
- Het inventariseren van vitale (bedrijfs)processen.
- Het opstellen van scenario’s voor cyberoefeningen.

Vaardigheden voor de bestrijding van interne cyberincidenten:

- Het identificeren van de geraakte systemen.
- Het in beeld brengen van de keteneffecten (verbondenheid van het geraakte systeem met andere systemen).

- Het inschatten van de mogelijke oorzaak (technische storing, menselijke fout of doelbewuste aanval).
- Het inventariseren van de schade op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie (zoals verlies van vertrouwelijke gegevens).
- Het inventariseren van de schade op ICT-systemen.
- Het inschatten van de impact op organisatieprocessen (bijvoorbeeld hulp- of dienstverlening).
- Het inschatten van de duur van de verstoring.
- Het vormen van een (technisch) oplossingsperspectief.
- Het bestrijden van de bron van de verstoring.
- Het bestrijden of verkleinen van de gevolgen/effecten van het incident.
- Het herstellen van de schade aan ICT-systemen.
- Het nemen van beslissingen in grote onzekerheid en complexiteit.
- Het adequaat communiceren over het cyberincident richting het bestuur van de eigen organisatie.
- Het adequaat extern communiceren over het cyberincident.

Netwerken en samenwerking voor de bestrijding van interne cyberincidenten

- Het zicht hebben op interne deskundigen voor de incidentbestrijding van een intern cyberincident.
- Het kennen van overheidsorganisaties en private partijen, die kunnen helpen bij de voorbereiding op de bestrijding van interne cyberincidenten.
- Het kennen van overheidsorganisaties en private partijen, die kunnen helpen bij de bestrijding van interne cyberincidenten.
- Het in staat zijn om externe expertise in te zetten voor de voorbereiding op interne cyberrisico's (denk aan o.a. het NCSC/ private IT-dienstverleners).
- Het in staat zijn om externe expertise in te zetten voor de bestrijding van interne incidenten (denk aan o.a. het NCSC/ private IT-dienstverleners).

Middelen voor de bestrijding van interne cyberincidenten:

- Het bezitten van voldoende technische middelen (zoals systemen) om voor te bereiden op interne cyberincidenten.
- Het bezitten van voldoende hulpmiddelen (zoals handreikingen, methodieken en protocollen) om voor te bereiden op interne cyberincidenten.
- Het bezitten van voldoende personeel, toegerust om voor te bereiden op interne cyberincidenten.

Gelegenheid voor de bestrijding van interne cyberincidenten:

- Het reserveren van voldoende tijd om voor te bereiden op interne cyberincidenten.
- Het reserveren van voldoende financiële middelen om voor te bereiden op interne cyberincidenten.

Bijlage 4 Benodigde factoren voor de voorbereiding op externe cyberincidenten

Cybergevolgbestrijding

Motivatie voor (de voorbereiding op) de gevolgbestrijding van externe cyberincidenten:

- Het management vindt de voorbereiding op externe cyberincidenten belangrijk.
- Mensen op operationeel niveau vinden de voorbereiding op externe cyberincidenten belangrijk.
- De voorbereiding op externe cyberincidenten heeft hoge prioriteit.

Kennis voor de voorbereiding op de gevolgbestrijding van externe cyberincidenten:

- Het inventariseren van mogelijke cyberdreigingen op de regio.
- Het vooraf inventariseren van mogelijke maatschappelijk effecten van een extern cyberincident.
- Het inventariseren van maatschappelijk belangrijke externe processen en bedrijven (denk aan vitale infrastructuur zoals elektriciteit, internet, drinkwater of betalingsverkeer).

Kennis voor de gevolgbestrijding van externe cyberincidenten:

- Het inschatten van de mogelijke oorzaak (technische storing, menselijke fout of doelbewuste aanval).
- Het inschatten van de duur van de verstoring.
- Het inschatten van de impact op maatschappelijke processen (denk aan vitale infrastructuur zoals elektriciteit, internet, drinkwater of betalingsverkeer).
- Het bestrijden of verkleinen van de gevolgen/effecten van het incident.

Vaardigheden voor de voorbereiding op de gevolgbestrijding van externe cyberincidenten:

- Het inventariseren van mogelijke cyberdreigingen op de regio.
- Het vooraf inventariseren van mogelijke maatschappelijk effecten van een extern cyberincident.
- Het inventariseren van maatschappelijk belangrijke externe processen en bedrijven (denk aan vitale infrastructuur zoals elektriciteit, internet, drinkwater of betalingsverkeer).

Vaardigheden voor de gevolgbestrijding van externe cyberincidenten:

- Het inschatten van de mogelijke oorzaak (technische storing, menselijke fout of doelbewuste aanval).
- Het inschatten van de duur van de verstoring.
- Het inschatten van de impact op maatschappelijke processen (denk aan vitale infrastructuur zoals elektriciteit, internet, drinkwater of betalingsverkeer).
- Het bestrijden of verkleinen van de gevolgen/ effecten van het incident.
- Adequaat communiceren over het cyberincident richting het bestuur van de eigen organisatie.
- Adequaat extern communiceren over het cyberincident.

Bijlage 5 Enquête cyberweerbaarheid

Geachte respondent,

Cyberweerbaarheid is gezien de laatste ontwikkelingen en incidenten een actueel thema binnen veiligheidsregio's. Om deze reden doet het lectoraat Crisisbeheersing van het Instituut Fysieke Veiligheid (IFV) onderzoek naar benodigde cyberkennis en -kunde van veiligheidsregio's voor (de voorbereiding op) de bestrijding van interne cyberincidenten. Doel is het in beeld brengen van mogelijkheden voor het mobiliseren van cyberkennis en -kunde voor de crisisbeheersing.

Daarnaast wordt door een afstudeerster van het lectoraat Crisisbeheersing onderzocht, welke mogelijke barrières veiligheidsregio's ervaren bij de voorbereiding op cyberincidenten. Doel is het in beeld brengen van barrières en het aanreiken van gerichte interventies voor een versterking van de voorbereiding op de bestrijding van interne cyberincidenten.

De gegevens uit de enquête worden uitsluitend gebruikt voor een adviesrapport voor veiligheidsregio's en een afstudeerrapport voor het lectoraat Crisisbeheersing van het IFV en Hogeschool Saxion. We rapporteren daarbij niet op het niveau van een individuele veiligheidsregio.

U kunt de enquête te allen tijde pauzeren, uw gegevens worden automatisch opgeslagen. De enquête moet in dit geval wel vanuit dezelfde computer en binnen één week worden afgerond.

We zien uw reactie graag uiterlijk **9 april 2021** tegemoet.

Heeft u vragen over deze enquête of over het onderzoek, neem dan contact op met Jana Domrose via jana.domrose@ifv.nl.

Ik heb alle bovenstaande informatie gelezen en stem toe dat mijn antwoorden ten behoeve van dit onderzoek gebruikt mogen worden:

- ○ Ja
- ○ Nee

Begripsdefinities

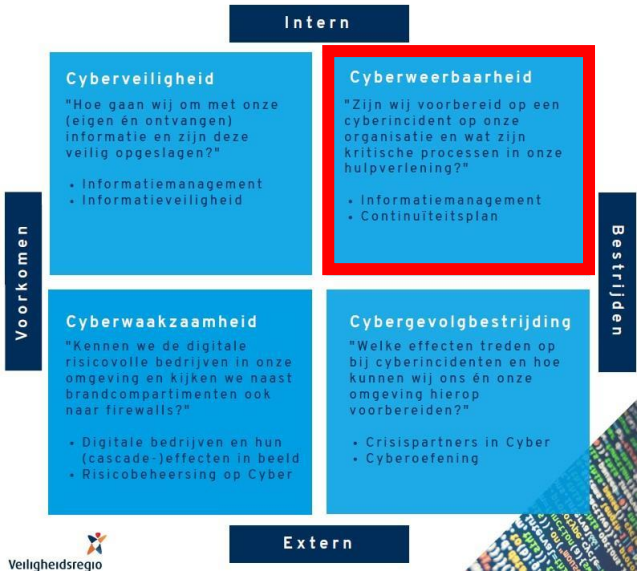
Hieronder vindt u belangrijke informatie over de focus van dit onderzoek en begripsdefinities. Wij willen u vragen om deze informatie goed door te nemen, voordat u verder gaat met de enquête.

Met deze enquête trachten wij te achterhalen hoe u zich als veiligheidsregio voorbereidt op de bestrijding van interne cyberincidenten. Onder een cyberincident verstaan wij:

Een gebeurtenis of activiteit die de beschikbaarheid, integriteit of vertrouwelijkheid van informatie- en procesbesturingssystemen aantast

Hierbij kunt u bijvoorbeeld denken aan:
- een aanval die processen, bestanden of systemen van de organisatie versleutelt,
- een technische storing, waardoor bepaalde systemen niet kunnen worden gebruikt.

Cyberincidenten kunnen zowel de eigen organisatie treffen, als een vitale sector binnen de veiligheidsregio. In deze enquête richten wij ons alleen op (de voorbereiding op) het **bestrijden van interne cyberincidenten**, de zogenoemde **cyberweerbaarheid**. Denk hierbij aan de reactie op een datalek of een DDoS aanval op de organisatie. In onderstaand cyberkwadrant van Veiligheidsregio IJsselland ligt cyberweerbaarheid rechts boven.



Hieronder volgen verschillende vragen over de voorbereiding op **cyberweerbaarheid** binnen uw veiligheidsregio. Wij zijn benieuwd naar uw professionele mening. Er bestaan geen goede of foute antwoorden.

Er wordt respectievelijk ingegaan op de urgentie, de kennis, de vaardigheden, de middelen & gelegenheid, de netwerken & samenwerking en de versterking van uw organisatie bij (de voorbereiding op) de bestrijding van interne cyberincidenten.

Urgentie:

1. In hoeverre bent u het eens met de volgende stellingen over urgentie in uw organisatie?

Binnen mijn organisatie….

	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens
…is het management bewust van de dreigingen uit het digitale domein voor de eigen organisatie.	○	○	○	○	○
…zijn mensen op operationeel niveau bewust van de dreigingen uit het digitale domein voor de eigen organisatie.	○	○	○	○	○
…vindt het management de voorbereiding op interne cyberincidenten belangrijk.	○	○	○	○	○
…vinden mensen op operationeel niveau de voorbereiding op interne cyberincidenten belangrijk.	○	○	○	○	○
…heeft de voorbereiding op interne cyberincidenten hoge prioriteit.	○	○	○	○	○
…worden cyberincidenten meegenomen in het continuïteitsplan.	○	○	○	○	○

Toelichting:

_____

_____

_____

Kennis bij de voorbereiding

2. In hoeverre bent u het eens met de volgende stellingen over kennis in uw organisatie? Geef ook aan of u de betreffende kennis idealiter binnen de eigen organisatie of bij een andere partij (buiten de organisatie) zou willen beleggen. U kunt ook beide opties aanvinken.

*Binnen mijn organisatie hebben we voldoende **kennis** om….*

	In hoeverre bent u het eens met de stelling?					Waar zou de betreffende kennis volgens u belegd moeten worden?	
	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens	Binnen de organisatie	Buiten de organisatie
…mogelijke cyberdreigingen op de eigen organisatie te inventariseren.	○	○	○	○	○	○	○
…mogelijke effecten van een intern cyberincident vooraf te inventariseren.	○	○	○	○	○	○	○
…verbondenheid van/tussen verschillende interne systemen in beeld te brengen.	○	○	○	○	○	○	○
…vitale (bedrijfs)processen te inventariseren.	○	○	○	○	○	○	○

3. Welke **kennis** is binnen uw organisatie nog (meer) nodig bij de **voorbereiding** op interne cyberincidenten?

_____

_____

_____

Kennis bij de bestrijding

4. In hoeverre bent u het eens met de volgende stellingen over kennis in uw organisatie? Geef ook aan of u de betreffende kennis idealiter binnen de eigen organisatie of bij een andere partij (buiten de organisatie) zou willen beleggen. U kunt ook beide opties aanvinken.

   *Binnen mijn organisatie hebben we bij een intern cyberincident voldoende **kennis** om….*

	In hoeverre bent u het eens met de stelling?					Waar zou de betreffende kennis volgens u belegd moeten worden?	
	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens	Binnen de organisatie	Buiten de organisatie
…de geraakte systemen te identificeren.	○	○	○	○	○	○	○
…de keteneffecten in beeld te brengen (verbondenheid van het geraakte systeem met andere systemen).	○	○	○	○	○	○	○
…de mogelijke oorzaak (technische storing, menselijke fout of doelbewuste aanval) in te schatten.	○	○	○	○	○	○	○
…de schade op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te inventariseren (zoals verlies van vertrouwelijke gegevens).	○	○	○	○	○	○	○
…de schade op ICT-systemen te inventariseren.	○	○	○	○	○	○	○

…de impact op organisatieprocessen (bijvoorbeeld hulp- of dienstverlening) in te schatten.	○	○	○	○	○	○	○
…de duur van de verstoring in te schatten.	○	○	○	○	○	○	○
…een (technisch) oplossingsperspectief te vinden.	○	○	○	○	○	○	○
…de bron van de verstoring te bestrijden.	○	○	○	○	○	○	○
…de gevolgen/ effecten van het incident te bestrijden of verkleinen.	○	○	○	○	○	○	○
…de schade aan de ICT-systemen te herstellen	○	○	○	○	○	○	○

5. Welke **kennis** is binnen uw organisatie nog (meer) nodig bij de **bestrijding** van interne cyberincidenten?

   _____

   _____

   _____

6. Waar zou uw organisatie de **kennis** over de bestrijding van interne incidenten idealiter willen beleggen? Er zijn meerdere antwoorden mogelijk.

   ☐ Binnen de organisatie bij een CISO (Chief Information Security Officer),

   ☐ Binnen de organisatie met medewerkers crisisbeheersing,

   ☐ Binnen de organisatie met ICT medewerkers,

   ☐ Overig, namelijk: _____

Toelichting:

_____

_____

_____

7. Welke externe partijen beschikken volgens u over relevante **kennis**, die u kunt raadplegen bij de bestrijding van interne cyberincidenten? Er zijn meerdere antwoorden mogelijk.

☐ Nationaal Cyber Security Center (NCSC)

☐ Andere veiligheidsregio's

☐ Publieke kennisinstellingen zoals hogescholen en universiteiten

☐ Private kennis-/adviesbureaus zoals Fox-IT

☐ Instituut Fysieke Veiligheid (IFV)

☐ Landelijk voorziening Veiligheidsregio Information Sharing and Analysis Center (VR-ISAC)

☐ Landelijke netwerken zoals werkgroep Digitale ontwrichting en cyber & vakgroep Informatieveiligheid

☐ Overig, namelijk: _____

Toelichting:

_____

_____

_____

Vaardigheden bij de voorbereiding

8. In hoeverre bent u het eens met de volgende stellingen over vaardigheden in uw organisatie? Geef ook aan of u de betreffende vaardigheden idealiter binnen de eigen organisatie of bij een andere partij (buiten de organisatie) zou willen beleggen. U kunt ook beide opties aanvinken.

   *Binnen mijn organisatie hebben we voldoende **vaardigheden** om…*

	In hoeverre bent u het eens met de stelling?					Waar zou de betreffende kennis volgens u belegd moeten worden?	
	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens	Binnen de organisatie	Buiten de organisatie
…mogelijke cyberdreigingen op de eigen organisatie te inventariseren.	○	○	○	○	○	○	○
…mogelijke effecten van een intern cyberincident vooraf te inventariseren.	○	○	○	○	○	○	○
…ketenrisico's in beeld te brengen (verbondenheid van/tussen verschillende interne systemen).	○	○	○	○	○	○	○
… vitale (bedrijfs)processen te inventariseren.	○	○	○	○	○	○	○
…scenario's voor cyberoefeningen op te stellen.	○	○	○	○	○	○	○

9. Welke **vaardigheden** zijn binnen uw organisatie nog (meer) nodig bij de **voorbereiding** op interne cyberincidenten?

   _____

   _____

   _____

Vaardigheden bij de bestrijding

10. In hoeverre bent u het eens met de volgende stellingen over vaardigheden in uw organisatie? Geef ook aan of u de betreffende vaardigheden idealiter binnen de eigen organisatie of bij een andere partij (buiten de organisatie) zou willen beleggen. U kunt ook beide opties aanvinken.

    *Binnen mijn organisatie hebben we bij een intern cyberincident voldoende **vaardigheden** om…*

	In hoeverre bent u het eens met de stelling?					Waar zou de betreffende kennis volgens u belegd moeten worden?	
	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens	Binnen de organisatie	Buiten de organisatie
…de geraakte systemen te identificeren.	○	○	○	○	○	○	○
…de keteneffecten in beeld te brengen (verbondenheid van het geraakte systeem met andere systemen).	○	○	○	○	○	○	○
…de mogelijke oorzaak (technische storing, menselijke fout of doelbewuste aanval) in te schatten.	○	○	○	○	○	○	○
…de schade op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te inventariseren (zoals verlies van vertrouwelijke gegevens).	○	○	○	○	○	○	○
…de schade op ICT-systemen te inventariseren.	○	○	○	○	○	○	○

…de impact op organisatieprocessen (bijvoorbeeld hulp- of dienstverlening) in te schatten.	○	○	○	○	○	○	○
…de duur van de verstoring in te schatten.	○	○	○	○	○	○	○
…een (technisch) oplossingsperspectief te vormen.	○	○	○	○	○	○	○
…de bron van de verstoring te bestrijden.	○	○	○	○	○	○	○
…de gevolgen/effecten van het incident te bestrijden of verkleinen.	○	○	○	○	○	○	○
…de schade aan ICT-systemen te herstellen.	○	○	○	○	○	○	○
…beslissingen te nemen in grote onzekerheid en complexiteit.	○	○	○	○	○	○	○
…adequaat richting het bestuur van de eigen organisatie te communiceren over het cyberincident.	○	○	○	○	○	○	○
…adequaat extern te communiceren over het cyberincident.	○	○	○	○	○	○	○

11. Welke **vaardigheden** zijn binnen uw organisatie nog (meer) nodig bij de **bestrijding** van interne cyberincidenten?

_____

_____

_____

12. Waar zou uw organisatie **vaardigheden** met betrekking tot de bestrijding van interne incidenten idealiter willen beleggen? Er zijn meerdere antwoorden mogelijk.

- ☐ Binnen de organisatie bij een CISO (Chief Information Security Officer),
- ☐ Binnen de organisatie met medewerkers crisisbeheersing,
- ☐ Binnen de organisatie met ICT medewerkers,
- ☐ Overig, namelijk: _____

Toelichting:

_____

_____

_____

13. Welke externe partijen beschikken volgens u over relevante **vaardigheden**, die u kunt raadplegen bij de bestrijding van interne cyberincidenten? Er zijn meerdere antwoorden mogelijk.

- ☐ Nationaal Cyber Security Center (NCSC)
- ☐ Andere veiligheidsregio's
- ☐ Publieke kennisinstellingen zoals hogescholen en universiteiten
- ☐ Private kennis-/adviesbureaus zoals Fox-IT
- ☐ Instituut Fysieke Veiligheid (IFV)
- ☐ Landelijke voorziening Veiligheidsregio Information SHaring and Analysis Center (VR-ISAC)
- ☐ Landelijke netwerken zoals werkgroep Digitale ontwrichting en cyber & vakgroep Informatieveiligheid
- ☐ Overig, namelijk: _____

Toelichting:

_____

_____

_____

Middelen en gelegenheid

14. In hoeverre bent u het eens met de volgende stellingen over middelen en gelegenheid in uw organisatie?

Onze organisatie…

	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens
…bezit voldoende technische middelen (zoals systemen) om zich voor te bereiden op interne cyberincidenten.	○	○	○	○	○
…bezit voldoende hulpmiddelen (zoals handreikingen, methodieken en protocollen) om zich voor te bereiden op interne cyberincidenten.	○	○	○	○	○
…bezit voldoende personeel, toegerust om zich voor te bereiden op interne cyberincidenten.	○	○	○	○	○
…reserveert voldoende tijd om zich voor te bereiden op interne cyberincidenten.	○	○	○	○	○
…reserveert voldoende financiële middelen om zich voor te bereiden op interne cyberincidenten.	○	○	○	○	○

Toelichting:

_____

_____

_____

Netwerken & samenwerking

15. In hoeverre bent u het eens met de volgende stellingen over netwerken en samenwerking in uw organisatie?

Binnen mijn organisatie…

	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens
… hebben wij zicht op interne deskundigen voor de incidentbestrijding van een intern cyberincident.	○	○	○	○	○
…kennen wij overheidsorganisaties en private partijen, die ons kunnen helpen bij de **voorbereiding** op de bestrijding van interne cyberincidenten.	○	○	○	○	○
…kennen wij overheidsorganisaties en private partijen, die ons kunnen helpen bij de **bestrijding** van interne cyberincidenten.	○	○	○	○	○
…zijn wij in staat om externe expertise in te zetten voor de **voorbereiding** op interne cyberrisico's (denk aan o.a. het NCSC/ private IT-dienstverleners).	○	○	○	○	○
… zijn wij in staat om externe expertise in te zetten voor de **bestrijding** van interne incidenten (denk aan o.a. het NCSC/ private IT-dienstverleners).	○	○	○	○	○

Toelichting:

_____

_____

_____

Versterking van de cyberweerbaarheid

16. Op welke factoren zou uw organisatie zich moeten richten om de voorbereiding op interne cyberincidenten te versterken? Rangschik de factoren door de antwoordopties naar boven/beneden te schuiven, waarbij **nummer 1 belangrijkste factor is**.

- ☐ Motivatie/urgentiebesef
- ☐ Kennis
- ☐ Kunde/vaardigheden
- ☐ Middelen (mensen, systemen, handreikingen etc.)
- ☐ Netwerken en samenwerking
- ☐ Tijd
- ☐ Geld
- ☐ Overig, namelijk: _____

Toelichting:

_____

_____

_____

17. Mogelijk heeft u nog concrete behoeften om u effectief voor te kunnen bereiden op de bestrijding van cyberincidenten in uw organisatie. Deze kunt u hieronder noemen en toelichten:

_____

_____

_____

_____

_____

18. Bent u eventueel bereid om in een interview meer informatie te verstrekken over uw best practices of aanbevelingen?

Ja, u kunt contact opnemen via: _____
Nee

U heeft het einde van deze enquête bereikt. Wij danken u hartelijk voor uw deelname!

Wanneer u op **'Volgende'** klikt, worden uw antwoorden opgeslagen en geregistreerd. U krijgt vervolgens een overzicht van uw antwoorden te zien. Dit kunt u indien gewenst downloaden als pdf.

Bijlage 6 Enquête cybergevolgbestrijding

Geachte respondent,

Cybergevolgbestrijding is een actueel thema binnen veiligheidsregio's. Op verzoek van de portefeuillehouder Digitale ontwrichting en cyber, doet het lectoraat Crisisbeheersing van het Instituut Fysieke Veiligheid (IFV) onderzoek naar benodigde cyberkennis en -kunde van veiligheidsregio's voor de gevolgbestrijding van externe cyberincidenten. Doel is het in beeld brengen van mogelijkheden voor het mobiliseren van cyberkennis en -kunde voor de crisisbeheersing.

Daarnaast wordt door een afstudeerster van het lectoraat Crisisbeheersing onderzocht, welke mogelijke barrières veiligheidsregio's ervaren bij de voorbereiding op cyberincidenten. Doel is het in beeld brengen van barrières en het aanreiken van gerichte interventies voor een versterking van de voorbereiding op de gevolgbestrijding van externe cyberincidenten.

De gegevens uit de enquête worden uitsluitend gebruikt voor een adviesrapport voor veiligheidsregio's en een afstudeerrapport voor het lectoraat Crisisbeheersing van het IFV en Hogeschool Saxion. We rapporteren daarbij niet op het niveau van een individuele veiligheidsregio.

U kunt de enquête te allen tijde pauzeren, uw gegevens worden automatisch opgeslagen. De enquête moet in dit geval wel vanuit dezelfde computer en binnen één week worden afgerond.

We zien uw reactie graag uiterlijk **9 april 2021** tegemoet.

Heeft u vragen over deze enquête of over het onderzoek, neem dan contact op met Jana Domrose via jana.domrose@ifv.nl.

Ik heb alle bovenstaande informatie gelezen en stem toe dat mijn antwoorden ten behoeve van dit onderzoek gebruikt mogen worden:

- ○ Ja
- ○ Nee

Begripsdefinities

Hieronder vindt u belangrijke informatie over de focus van dit onderzoek en begripsdefinities. Wij willen u vragen om deze informatie goed door te nemen, voordat u verder gaat met de enquête.

Met deze enquête trachten wij te achterhalen hoe u zich als veiligheidsregio voorbereidt op de gevolgbestrijding van externe cyberincidenten. Onder een cyberincident verstaan wij:

Een gebeurtenis of activiteit die de beschikbaarheid, integriteit of vertrouwelijkheid van informatie- en procesbesturingssystemen aantast

Hierbij kunt u bijvoorbeeld denken aan:

- een hack die het betalingsverkeer platlegt,
- een aanval die processen, bestanden of systemen van een vitale organisatie versleutelt,
- een brand die de elektriciteit platlegt.

Cyberincidenten kunnen zowel de eigen organisatie treffen, als een vitale sector binnen de veiligheidsregio. In deze enquête richten wij ons alleen op (de voorbereiding op) de **gevolgbestrijding van externe cyberincidenten**, de zogenoemde **cybergevolgbestrijding**. Cybergevolgbestrijding behelst alle activiteiten in het kader van het beperken van de effecten van een incident waarvan de oorzaak en/of het gevolg in het digitale domein ligt. Denk hierbij aan de reactie op een verstoring van vitale infrastructuur zoals elektriciteit, internet, drinkwater of betalingsverkeer binnen de regio. In het vervolg van de enquête wordt omwille van de leesbaarheid gerefereerd aan 'externe incidenten'. In onderstaand cyberkwadrant van Veiligheidsregio IJsselland ligt cybergevolgbestrijding rechts onder.

Hieronder volgen verschillende vragen over de voorbereiding op **cybergevolgbestrijding** binnen uw veiligheidsregio. Wij zijn benieuwd naar uw professionele mening. Er bestaan geen goede of foute antwoorden.

Er wordt respectievelijk ingegaan op de urgentie, de kennis, de vaardigheden, de middelen & gelegenheid, de netwerken & samenwerking en de versterking van uw organisatie bij (de voorbereiding op) de gevolgbestrijding van externe cyberincidenten.

Urgentie

19. In hoeverre bent u het eens met de volgende stellingen over urgentie in uw organisatie?

Binnen mijn organisatie….

	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens
…is het management bewust van de dreigingen uit het digitale domein voor de regio.	○	○	○	○	○
…zijn mensen op operationeel niveau bewust van de dreigingen uit het digitale domein voor de regio.	○	○	○	○	○
…vindt het management de voorbereiding op externe cyberincidenten belangrijk.	○	○	○	○	○
…vinden mensen op operationeel niveau de voorbereiding op externe cyberincidenten belangrijk.	○	○	○	○	○
…heeft de voorbereiding op externe cyberincidenten hoge prioriteit.	○	○	○	○	○

Toelichting:

_____

_____

_____

Kennis bij de voorbereiding

20. In hoeverre bent u het eens met de volgende stellingen over kennis in uw organisatie? Geef ook aan of u de betreffende kennis idealiter binnen de eigen organisatie of bij een andere partij (buiten de organisatie) zou willen beleggen. U kunt ook beide opties aanvinken.

*Binnen mijn organisatie hebben we voldoende **kennis** om...*

	In hoeverre bent u het eens met de stelling?					Waar zou de betreffende kennis volgens u belegd moeten worden?	
	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens	Binnen de organisatie	Buiten de organisatie
…mogelijke cyberdreigingen op de regio te inventariseren.	○	○	○	○	○	○	○
…mogelijke maatschappelijke effecten van een extern cyberincident vooraf te inventariseren.	○	○	○	○	○	○	○
…maatschappelijk belangrijke externe processen en bedrijven te inventariseren(denk aan vitale infrastructuur zoals elektriciteit, internet, drinkwater of betalingsverkeer).	○	○	○	○	○	○	○

21. Welke **kennis** is binnen uw organisatie nog (meer) nodig bij de **voorbereiding** op externe cyberincidenten?

_____

_____

_____

Kennis bij de gevolgbestrijding

22. In hoeverre bent u het eens met de volgende stellingen over kennis in uw organisatie? Geef ook aan of u de betreffende kennis idealiter binnen de eigen organisatie of bij een andere partij (buiten de organisatie) zou willen beleggen. U kunt ook beide opties aanvinken.

    *Binnen mijn organisatie hebben we bij een extern cyberincident voldoende **kennis** om…*

	In hoeverre bent u het eens met de stelling?					Waar zou de betreffende kennis volgens u belegd moeten worden?	
	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens	Binnen de organisatie	Buiten de organisatie
…de mogelijke oorzaak (technische storing, menselijke fout of doelbewuste aanval) in te schatten.	○	○	○	○	○	○	○
…de duur van de verstoring in te schatten.	○	○	○	○	○	○	○
…de impact op maatschappelijke processen in te schatten (denk aan vitale infrastructuur zoals elektriciteit, internet, drinkwater of betalingsverkeer).	○	○	○	○	○	○	○
…de gevolgen/effecten van het incident te bestrijden of verkleinen.	○	○	○	○	○	○	○

23. Welke **kennis** is binnen uw organisatie nog (meer) nodig bij de **gevolgbestrijding** van externe cyberincidenten?

    _____

    _____

    _____

24. Waar zou uw organisatie de **kennis** over de gevolgbestrijding van externe incidenten idealiter willen beleggen? Er zijn meerdere antwoorden mogelijk.

- ☐ Binnen de organisatie bij een CISO (Chief Information Security Officer),
- ☐ Binnen de organisatie met medewerkers crisisbeheersing,
- ☐ Binnen de organisatie met ICT medewerkers,
- ☐ Overig, namelijk: _____

Toelichting:

_____

_____

_____

25. Welke externe partijen beschikken volgens u over relevante **kennis**, die u kunt raadplegen bij de gevolgbestrijding van externe cyberincidenten? Er zijn meerdere antwoorden mogelijk.

- ☐ Nationaal Cyber Security Center (NCSC)
- ☐ Andere veiligheidsregio's
- ☐ Publieke kennisinstellingen zoals hogescholen en universiteiten
- ☐ Private kennis-/adviesbureaus zoals Fox-IT
- ☐ Instituut Fysieke Veiligheid (IFV)
- ☐ Landelijke voorziening Veiligheidsregio Information Sharing and Analysis Center (VR-ISAC)
- ☐ Landelijke netwerken zoals werkgroep Digitale ontwrichting en cyber & vakgroep Informatieveiligheid
- ☐ Overig, namelijk: _____

Toelichting:

_____

_____

_____

Vaardigheden bij de voorbereiding

26. In hoeverre bent u het eens met de volgende stellingen over vaardigheden in uw organisatie? Geef ook aan of u de betreffende kennis idealiter binnen de eigen organisatie of bij een andere partij (buiten de organisatie) zou willen beleggen. U kunt ook beide opties aanvinken.

*Binnen mijn organisatie hebben we voldoende **vaardigheden** om…*

	In hoeverre bent u het eens met de stelling?					Waar zou de betreffende kennis volgens u belegd moeten worden?	
	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens	Binnen de organisatie	Buiten de organisatie
…mogelijke cyberdreigingen op de regio te inventariseren.	○	○	○	○	○	○	○
…mogelijke maatschappelijke effecten van een extern cyberincident vooraf te inventariseren.	○	○	○	○	○	○	○
…maatschappelijk belangrijke externe processen en bedrijven te inventariseren (denk aan vitale infrastructuur zoals elektriciteit, internet, drinkwater of betalingsverkeer).	○	○	○	○	○	○	○

27. Welke **vaardigheden** zijn binnen uw organisatie nog (meer) nodig bij de **voorbereiding** op externe cyberincidenten?

_____

_____

_____

Vaardigheden bij de gevolgbestrijding

28. In hoeverre bent u het eens met de volgende stellingen over vaardigheden in uw organisatie? Geef ook aan of u de betreffende kennis idealiter binnen de eigen organisatie of bij een andere partij (buiten de organisatie) zou willen beleggen. U kunt ook beide opties aanvinken.

*Binnen mijn organisatie hebben we bij een extern cyberincident voldoende **vaardigheden** om…*

	In hoeverre bent u het eens met de stelling?					Waar zou de betreffende kennis volgens u belegd moeten worden?	
	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens	Binnen de organisatie	Buiten de organisatie
…de mogelijke oorzaak (technische storing, menselijke fout of doelbewuste aanval) in te schatten.	○	○	○	○	○	○	○
…de duur van de verstoring in te schatten.	○	○	○	○	○	○	○
…de impact op maatschappelijke processen in te schatten (denk aan vitale infrastructuur zoals elektriciteit, internet, drinkwater of betalingsverkeer).	○	○	○	○	○	○	○
…de gevolgen/ effecten van het incident te bestrijden of verkleinen.	○	○	○	○	○	○	○
	○	○	○	○	○	○	○

…adequaat richting het bestuur van de eigen organisatie te communiceren over het cyberincident.	○	○	○	○	○	○	○
…adequaat extern te communiceren over het cyberincident.							

29. Welke **vaardigheden** zijn binnen uw organisatie nog (meer) nodig bij de **gevolgbestrijding** van externe cyberincidenten?

_____

_____

_____

30. Waar zou uw organisatie **vaardigheden** met betrekking tot de gevolgbestrijding van externe incidenten idealiter willen beleggen? Er zijn meerdere antwoorden mogelijk.

☐ Binnen de organisatie bij een CISO (Chief Information Security Officer),

☐ Binnen de organisatie met medewerkers crisisbeheersing,

☐ Binnen de organisatie met ICT medewerkers,

☐ Overig, namelijk: _____

Toelichting:

_____

_____

_____

31. Welke externe partijen beschikken volgens u over relevante **vaardigheden**, die u kunt raadplegen bij de gevolgbestrijding van externe cyberincidenten? Er zijn meerdere antwoorden mogelijk.

- ☐ Nationaal Cyber Security Center (NCSC)
- ☐ Andere veiligheidsregio's
- ☐ Publieke kennisinstellingen zoals hogescholen en universiteiten
- ☐ Private kennis-/adviesbureaus zoals Fox-IT
- ☐ Instituut Fysieke Veiligheid (IFV)
- ☐ Landelijke voorziening Veiligheidsregio Information Sharing and Analysis Center (VR-ISAC)
- ☐ Landelijke netwerken zoals werkgroep Digitale ontwrichting en cyber & vakgroep Informatieveiligheid
- ☐ Overig, namelijk: _____

Toelichting:

_____

_____

_____

Middelen en gelegenheid

32. In hoeverre bent u het eens met de volgende stellingen over middelen en gelegenheid in uw organisatie?

Onze organisatie…

	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens
…bezit voldoende technische middelen (zoals systemen) om zich voor te bereiden op externe cyberincidenten.	○	○	○	○	○
…bezit voldoende hulpmiddelen (zoals handreikingen, methodieken en protocollen) om zich voor te bereiden op externe cyberincidenten.	○	○	○	○	○
…bezit voldoende personeel, toegerust om zich voor te bereiden op externe cyberincidenten.	○	○	○	○	○
…reserveert voldoende tijd om zich voor te bereiden op externe cyberincidenten.	○	○	○	○	○
…reserveert voldoende financiële middelen om zich voor te bereiden op externe cyberincidenten.	○	○	○	○	○

Toelichting:

_____

_____

_____

Netwerken & samenwerking

33. In hoeverre bent u het eens met de volgende stellingen over netwerken en samenwerking in uw organisatie?

Binnen mijn organisatie…

	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens
… hebben wij zicht op interne deskundigen voor de gevolgbestrijding van een extern cyberincident.	○	○	○	○	○
…kennen wij overheidsorganisaties en private partijen, die ons kunnen helpen bij de **voorbereiding** op de gevolgbestrijding van externe cyberincidenten.	○	○	○	○	○
…kennen wij overheidsorganisaties en private partijen, die ons kunnen helpen bij de **gevolgbestrijding** van externe cyberincidenten.	○	○	○	○	○
…zijn wij in staat om externe expertise in te zetten voor de **voorbereiding** op externe cyberrisico's (denk aan o.a. het NCSC/ private IT-dienstverleners).	○	○	○	○	○
… zijn wij in staat om externe expertise in te zetten voor de **gevolgbestrijding** van externe incidenten (denk aan o.a. het NCSC/ private IT-dienstverleners).	○	○	○	○	○
…weten wij waar we verantwoordelijk voor zijn bij de gevolgbestrijding van externe cyberincidenten.	○	○	○	○	○
…weten wij welke verantwoordelijkheden de andere betrokken teams hebben bij de gevolgbestrijding van externe cyberincidenten.	○	○	○	○	○
…zijn wij in staat om tijdens de gevolgbestrijding van een extern cyberincident samen te werken met de andere betrokken teams.	○	○	○	○	○

Toelichting:

_____

_____

_____

Versterking van de voorbereiding op cybergevolgbestrijding

34. Op welke factoren zou uw organisatie zich moeten richten om de voorbereiding op externe cyberincidenten te versterken? Rangschik de factoren door de antwoordopties naar boven/beneden te schuiven, waarbij **nummer 1 belangrijkste factor is**.

- ☐ Motivatie/urgentiebesef
- ☐ Kennis
- ☐ Kunde/vaardigheden
- ☐ Middelen (mensen, systemen, handreikingen etc.)
- ☐ Netwerken en samenwerking
- ☐ Tijd
- ☐ Geld
- ☐ Overig, namelijk: _____

Toelichting:

_____

_____

_____

35. Mogelijk heeft u nog concrete behoeften om u effectief voor te kunnen bereiden op de gevolgbestrijding van cyberincidenten in uw regio. Deze kunt u hieronder noemen en toelichten:

_____

_____

_____

_____

_____

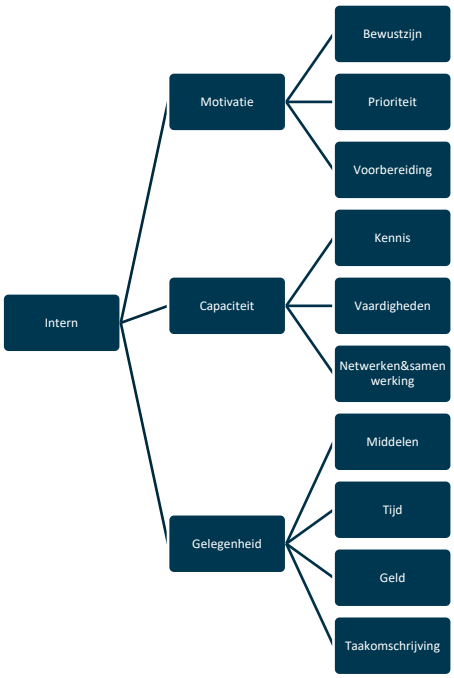
36. Bent u eventueel bereid om in een interview meer informatie te verstrekken over uw best practices of aanbevelingen?

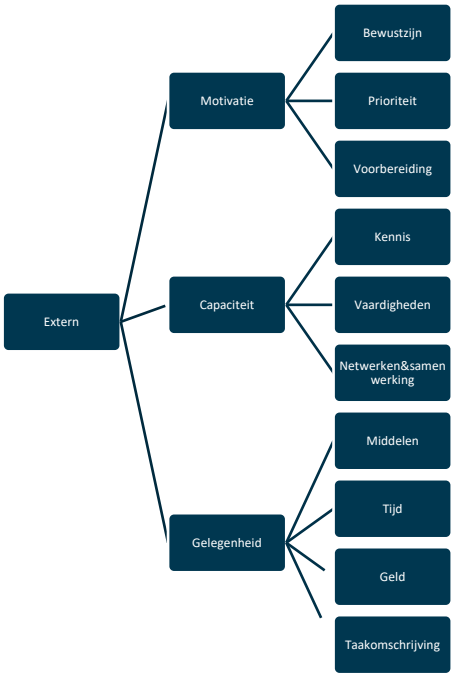
Ja, u kunt contact opnemen via: _____
Nee

U heeft het einde van deze enquête bereikt. Wij danken u hartelijk voor uw deelname!

Wanneer u op **'Volgende'** klikt, worden uw antwoorden opgeslagen en geregistreerd. U krijgt vervolgens een overzicht van uw antwoorden te zien. Dit kunt u indien gewenst downloaden als pdf.

Bijlage 7 Axiale codeerschema's





Bijlage 8 Resultaten enquête cyberweerbaarheid

Uitwerking resultaten enquête cyberweerbaarheid
Respondenten: VR-ISAC (12)

Motivatie en urgentiebesef

- De respondenten geven aan dat het management van de veiligheidsregio over het algemeen bewust is van de dreigingen uit het digitale domein voor de eigen organisatie. 58% van de respondenten is het enigszins of helemaal eens met de stelling. Opvallend is dat het grootste deel van deze respondenten (42%) het helemaal eens is met de stelling. 25% is het niet eens of oneens met de stelling en 17% van de respondenten is het enigszins oneens met de stelling.
- De mensen op operationeel niveau lijken ook bewust te zijn van de dreigingen uit het digitale domein voor de eigen organisatie. 67% van de respondenten is het enigszins of helemaal eens met de stelling. Wel is het hierbij opvallend dat maar 8% hiervan het helemaal eens is met de stelling en dus de overige respondenten het enigszins met de stelling eens zijn. 25% van de respondenten is het niet eens of oneens met de stelling en 8% is het enigszins oneens met de stelling.
- Daarnaast lijkt de stelling over de mate waarin het management de voorbereiding op interne cyberincidenten belangrijk vindt, voor verdeeldheid te zorgen. Zo is 17% het helemaal met de stelling eens en vindt dus dat het management de voorbereiding belangrijk vindt. 33% is het enigszins met de stelling eens, 33% is het niet eens of oneens en 17% is het enigszins oneens met de stelling.
- De respons op de stelling over de mate waarin mensen op operationeel niveau de voorbereiding op interne cyberincidenten belangrijk vindt, is identiek aan de bovenstaande respons. Ook hierbij is 17% het helemaal met de stelling eens en vindt dus dat mensen op operationeel niveau de voorbereiding belangrijk vindt. 33% is het enigszins met de stelling eens, 33% is het niet eens of oneens en 17% is het enigszins oneens met de stelling.
- De stelling over de mate waarin de voorbereiding op interne cyberincidenten hoge prioriteit krijgt binnen de veiligheidsregio, zorgt ook weer voor veel verschillende reacties. 33% van de respondenten is het enigszins oneens met de stelling, 33% is het niet eens of oneens, 25% is het enigszins oneens met de stelling en 9% is het helemaal oneens met de stelling.
- Tot slot worden cyberincidenten volgens de respondenten maar door een klein deel van de meegenomen in het continuïteitsplan. Zo is 42% van de respondenten het helemaal of enigszins eens met de stelling. 25% is het niet eens of oneens. De laatste 33% van de respondenten is het enigszins oneens met de stelling, wat inhoudt dat cyberincidenten volgens deze respondenten niet door veiligheidsregio's worden meegenomen in het continuïteitsplan.

Binnen mijn organisatie…	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens
…is het management bewust van de dreigingen uit het digitale domein voor de eigen organisatie.	5	2	3	2	0
…zijn mensen op operationeel niveau bewust van de dreigingen uit het digitale domein voor de eigen organisatie.	1	7	3	1	0
…vindt het management de voorbereiding op interne cyberincidenten belangrijk.	2	4	4	2	0
…vinden mensen op operationeel niveau de voorbereiding op interne cyberincidenten belangrijk.	2	4	4	2	0
…heeft de voorbereiding op interne cyberincidenten hoge prioriteit.	0	4	4	3	1
…worden cyberincidenten meegenomen in het continuïteitsplan.	1	4	3	4	0

Toelichtingen:

- "Het bewustwordingsniveau is wel aan het groeien. Cyberveiligheid is steeds meer een onderwerp in de media."
- "Mijn persoonlijke mening is dat we er nog te weinig aan doen, ook na onze hack."
- "Er is geen continuïteitsplan."
- "O.a. beleid en draaiboek Ransomware in wording, onderdeel continuïteitsplan."

Kennis bij de voorbereiding:

- De kennis voor het inventariseren van mogelijke dreigingen op de eigen organisatie blijkt volgens de respondenten binnen het merendeel van de veiligheidsregio's aanwezig te zijn. Zo is 58% van de respondenten het enigszins of helemaal niet eens met de stelling. 33% van de respondenten is het niet eens of oneens en 9% is het enigszins oneens met de stelling. Echter zouden alle respondenten deze kennis idealiter intern/binnen de organisatie beleggen. 50% van de respondenten zou deze kennis daarnaast ook extern willen beleggen.
- De kennis voor het inventariseren van mogelijke effecten van een intern cyberincident is volgens de meeste respondenten wel binnen veiligheidsregio's te vinden. Zo is 50% van de respondenten het enigszins of helemaal eens met de stelling. Toch lijkt er nog wel ruimte voor verbetering, aangezien 33% van de respondenten het niet eens of oneens is en 17% van de respondenten het enigszins of helemaal oneens is. Zeker, aangezien door alle respondenten is aangegeven dat deze kennis idealiter binnen de organisatie wordt belegd. Daarnaast zou 17% van de respondenten deze kennis daarnaast ook extern willen beleggen.
- De stelling over de kennis voor het in beeld brengen van de verbondenheid tussen verschillende interne systemen, zorgt voor een perfecte verdeling van antwoorden van de

respondenten. Het grootste deel van de respondenten is het niet eens of oneens met de stelling (34%). 25% is het enigszins eens met de stelling en 25% is het enigszins oneens met de stelling. Daarnaast is 8% het helemaal eens en is de overige 8% het helemaal niet met de stelling eens. Ook hier is volgens de respondenten dus nog ruimte voor verbetering. Bij de vraag of deze kennis intern of extern moet worden belegd, is de groep respondenten minder verdeeld. Alle respondenten, op één na, zouden de kennis intern beleggen. 33% van de respondenten zou de kennis (daarnaast/ook) extern willen beleggen.

- De kennis voor het inventariseren van de vitale bedrijfsprocessen is volgens de respondenten zeker binnen de veiligheidsregio's aanwezig. 33% is het helemaal met de stelling eens, 42% is het enigszins met de stelling eens, 8% is het niet eens of oneens en 17% is het enigszins oneens met de stelling. Daarnaast zijn alle respondenten het met elkaar eens dat deze kennis intern moet worden belegd.

Binnen mijn organisatie hebben we voldoende kennis om...	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens	Intern	Extern
…mogelijke cyberdreigingen op de eigen organisatie te inventariseren.	1	6	4	1	0	12	6
…mogelijke effecten van een intern cyberincident vooraf te inventariseren.	1	5	4	2	0	12	2
…verbondenheid van/tussen verschillende interne systemen in beeld te brengen.	1	3	4	3	1	11	4
…vitale (bedrijfs)processen te inventariseren.	4	5	1	2	0	12	0

Toelichtingen over welke kennis (nog meer) nodig is bij de voorbereiding:

- "Kennis van afhankelijkheden en bedrijfskritisch-heid."
- "Communicatie en Crisismanagement."
- "Specialistische (technische) kennis."
- "Het identificeren en kwalificeren van potentiële IOC's."
- "Kennis hebben van (cyber)risicomanagement (signaleren en proces van beoordelen, en evt. maatregelen treffen)."
- "Forensisch (beeld van inzet), meldingenstructuur."
- "Monitoring en duiding van signalen."
- "Kennis van de effecten en hoe deze doorwerken in de processen."
- "Kennis van de prioriteiten/volgordelijkheid t.b.v. het continuïteitsplan."
- "Vooral het in de gaten houden van de informatiestromen, zodra er een uitbraak is dat je daar dan acties op kunt nemen."

Kennis bij de bestrijding:

- De kennis om de geraakte systemen te identificeren is volgens de meerderheid van de respondenten aanwezig binnen de veiligheidsregio's. 67% van de respondenten is het enigszins eens met de stelling. Daarnaast vinden alle respondenten, op één na, dat deze kennis intern moet worden belegd. 50% van de respondenten zou deze kennis daarnaast ook extern beleggen.
- De stelling over de kennis die nodig is voor het in beeld brengen van de keteneffecten zorgt voor verdeeldheid. De meerderheid van de respondenten is het niet eens of oneens met de stelling (42%). 33% is het enigszins oneens met de stelling, 8% is het helemaal oneens met de stelling en 17% is het juist enigszins eens met de stelling. Hierbij is dus mogelijkheid tot verbetering. Zeker aangezien 83% van de respondenten vindt dat deze kennis intern moet worden belegd. 50% van de respondenten vindt dat de kennis (daarnaast/ook) extern moet worden belegd.
- De kennis voor het inschatten van de mogelijke oorzaak is volgens de meeste respondenten niet aanwezig binnen de veiligheidsregio's. Zo is 50% van de respondenten het enigszins oneens met de stelling. Daarnaast is 25% het niet eens of oneens, maar is ook 25% het juist wel enigszins eens met de stelling. Over de mate waarin deze kennis binnen veiligheidsregio's aanwezig is heerst dus nog verdeeldheid. De reacties op de vraag of deze kennis intern of extern moet worden belegd zijn ook verdeeld. Zo vindt 75% van de respondenten dat de kennis extern of zowel intern als extern moet worden belegd, maar vindt 67% dat de kennis intern of zowel intern als extern moet worden belegd.
- De kennis voor het inschatten van de schade op de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie is volgens de respondenten in mindere mate aanwezig binnen de veiligheidsregio's. 50% van de respondenten is het niet eens of oneens, 17% is het enigszins eens, maar 17% is het enigszins oneens en de overige 16% is het helemaal oneens met de stelling. De reacties op de vraag of deze kennis intern of extern moet worden belegd zijn verdeeld. Zo vindt 75% van de respondenten dat de kennis intern of zowel intern als extern moet worden belegd, maar vindt 67% dat de kennis extern of zowel intern als extern moet worden belegd.
- De kennis voor het inschatten van de schade op de ICT-systemen is volgens de respondenten wel grotendeels aanwezig binnen de veiligheidsregio's. Zo is 50% het enigszins met de stelling eens, is 17% het niet eens of oneens, is 8% het enigszins oneens en is 25% het helemaal niet eens met de stelling. Ook hier verbetering mogelijk. Toch geven alle respondenten, op één na, aan dat deze kennis idealiter extern wordt belegd. Daarnaast geeft 67% van de respondenten aan dat de kennis idealiter (daarnaast/ook) intern wordt belegd.
- De kennis om de impact op organisatieprocessen in te schatten is volgens de respondenten aanwezig binnen de veiligheidsregio's. 67% is het enigszins eens met de stelling, 25% is het niet eens of oneens en opvallend genoeg is 8% het helemaal oneens met de stelling. Alle respondenten, op één na, geven hierbij aan dat de kennis intern moet worden belegd (92%). De andere respondent zou de kennis idealiter extern willen beleggen (8%).
- De kennis om de duur van de verstoring in te schatten is volgens de respondenten in mindere mate aanwezig binnen de veiligheidsregio's. Zo is 42% van de respondenten het helemaal oneens met de stelling, is 17% het enigszins oneens, is 33% het niet eens of oneens en is de overige 8% het enigszins eens met de stelling. De reacties op de vraag of de kennis intern of extern belegd moet worden heerst verdeeldheid. 67% van de respondenten zou de kennis idealiter intern of zowel intern als extern beleggen, maar ook 67% zou de kennis idealiter extern of zowel intern als extern beleggen.

- De kennis om een (technisch)oplossingsperspectief te vinden is volgens de respondenten ook niet aanwezig binnen de veiligheidsregio's. 42% is het niet eens of oneens met de stelling, 33% is het enigszins oneens, 17% is het helemaal oneens en 8% is het enigszins eens. Echter gaven alle respondenten, op één na, aan dat deze kennis idealiter extern wordt belegd (92%). Daarnaast gaf 67% aan dat de kennis idealiter (daarnaast/ook) intern wordt belegd.
- De kennis om de bron van de verstoring te bestrijden is volgens de respondenten ook in mindere mate aanwezig binnen de veiligheidsregio's. Zo is 42% van de respondenten het helemaal oneens met de stelling, is 33% het enigszins oneens, is 8% het niet eens of oneens en is 17% het enigszins eens met de stelling. Daarnaast zou 75% van de respondenten de kennis idealiter extern of zowel intern als extern beleggen, maar zou 50% de kennis idealiter intern of zowel intern als extern beleggen.
- De stelling over de kennis om de gevolgen en effecten van een incident te verkleinen of bestrijden zorgt bij verdeeldheid onder de respondenten. Zo is het grootste deel van de respondenten het niet eens of oneens met de stelling (42%). 33% van de respondenten is het enigszins eens met de stelling, maar 17% is het enigszins oneens en 8% is het helemaal oneens. De reacties op de vraag of deze kennis intern of extern moet worden belegd zijn verdeeld. Zo vindt 75% van de respondenten dat de kennis intern of zowel intern als extern moet worden belegd, maar vindt 67% dat de kennis extern of zowel intern als extern moet worden belegd.
- Tot slot zorgt ook de stelling over de kennis om de schade aan ICT-systemen te herstellen voor verdeeldheid onder de respondenten. Zo is 41% van de respondenten het enigszins eens met de stelling, is 17% het niet eens of oneens, is 17% het enigszins oneens en is 25% het helemaal oneens. Daarnaast zou 83% van de respondenten deze kennis idealiter extern of zowel intern als extern willen beleggen. 67% van de respondenten zou de kennis idealiter intern of zowel intern als extern willen beleggen.

Binnen mijn organisatie hebben we bij een extern cyberincident voldoende kennis om…	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens	Intern	Extern
…de geraakte systemen te identificeren.	0	8	1	2	1	11	6
…de keteneffecten in beeld te brengen (verbondenheid van het geraakte systeem met andere systemen).	0	2	5	4	1	10	6
…de mogelijke oorzaak (technische storing, menselijke fout of doelbewuste aanval) in te schatten.	0	3	3	6	0	8	9
…de schade op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te inventariseren (zoals verlies van vertrouwelijke gegevens).	0	2	6	2	2	9	8

…de schade op ICT-systemen te inventariseren.	0	6	2	1	3	8	11
…de impact op organisatieprocessen (bijvoorbeeld hulp- of dienstverlening) in te schatten.	0	8	3	0	1	11	1
…de duur van de verstoring in te schatten.	0	1	4	2	5	8	8
…een (technisch) oplossingsperspectief te vinden.	0	1	5	4	2	8	11
…de bron van de verstoring te bestrijden.	0	2	1	4	5	6	9
…de gevolgen/ effecten van het incident te bestrijden of verkleinen.	0	4	5	2	1	9	8
…de schade aan de ICT-systemen te herstellen	0	5	2	2	3	8	10

Toelichtingen over welke kennis (nog meer) nodig is bij de bestrijding van interne cyberincidenten:

- “Diepgaande technische kennis.”
- “Specifieke juridische kennis (bijvoorbeeld op het gebied van verzekeringen en schade).”
- “Voor bijna alle bovengenoemde kennis heb je externe expertise nodig, al is het alleen maar om een sparringspartner te hebben.”
- “Bijna alles is uitbesteed, de regie moet bij ons liggen, de technische oplossing zal vaak bij de externe leverancier liggen. Kennis nodig van goed leverancier management. En kennis nodig van goed regie hebben (uitbesteden is niet gelijk aan, niets meer hoeven doen of weten).”
- “De kennis zal hybride zijn; een deel in de eigen organisatie + een deel externe expertise.”
- “Forensisch, veilige data restore, beoordeling gedrag van incident.”
- “Omgaan met ethische en/of juridische kwesties.”
- “Kennis voor bijv. forensisch onderzoek ontbreekt, maar wordt ingehuurd indien nodig.”
- “Wij zijn nu bezig met het inrichten van EDR zodat er extern gemonitord (24/7) wordt.”

Het intern beleggen van de kennis over de bestrijding van interne cyberincidenten:

De meeste respondenten zouden de kennis over de bestrijding van interne cyberincidenten idealiter binnen de organisatie bij ICT medewerkers beleggen (36%). Daarnaast had 32% van de respondenten de voorkeur om de kennis binnen de organisatie bij een CISO (Chief Information Security Officer) te beleggen en zou 16% het idealiter bij medewerkers crisisbeheersing beleggen. De overige respondenten (16%) brachten zelf ideeën voor het beleggen van de kennis binnen de organisatie:

- "(Technical) Information Security Officer."
- "Externe specialisten."
- "Toekomstig VR-CERT."
- "Contractueel externe partij."
- "Directie."

Opmerking: er konden meerdere antwoorden worden aangekruist, waardoor de percentages zijn gebaseerd op alle aangekruiste antwoorden. 'ICT-medewerker' is door 11 van de 12 respondenten gekozen en 'CISO' door 10 van de 12. 'Medewerker crisisbeheersing' werd door 5 van de 12 respondenten gekozen.

Daarnaast werden veel antwoorden voorzien van een toelichting:

- "Ieder met een eigen focus, maar wel met overlapping."
- "Nu nog geen CISO."
- "Bijna altijd is het noodzakelijk om externe expertise in te schakelen."
- "Bovenstaande als we uitgaan van een Cyberincident, met de 3 antwoorden als gemêleerd gezelschap."
- "Iedereen heeft kennis nodig, alleen op een ander vlak of van een ander moment in de incidentbestrijding. De ICT medewerkers moeten kennis hebben om te kunnen herkennen en in actie te komen of om alarm te kunnen slaan. De medewerkers crisisbeheersing zouden bijv. een draaiboek kunnen klaar hebben en de organisatie kunnen laten oefen met een interne crisis en op die manier kennis hebben van de bestrijding van interne incidenten. De CISO heeft een overkoepelende rol en zal zeker ook kennis moeten hebben van bestrijding interne incidenten. Vooral ook in het voorkomen van incidenten, maar zeker ook (extern) kennis verzamelen en (intern) kennis delen in het handelingsperspectief bij een incident."
- "Verschil tussen incident en crisis; incident handelt de ICT-afdeling zelf af, crisis vergt aanvullende inzet van de crisisorganisatie(structuur)."
- "Ontwikkelingen gaan te snel om alles zelf blijvend te ondersteunen, kennis- en uitvoerende partij achter de hand houden."
- "Bij ons zou dat echt een samenspel zijn van afdeling automatisering en CISO."

Het extern beleggen van de kennis over de bestrijding van interne cyberincidenten:

De meeste respondenten zouden de kennis over de bestrijding van interne cyberincidenten idealiter buiten de organisatie bij het Nationaal Cyber Security Center (19%), Private kennis-/adviesbureaus zoals Fox-IT (19%) en landelijke voorziening Veiligheidsregio Information Sharing and Analysis Center (19%), beleggen. Ook andere veiligheidsregio's (17%) is vaak genoemd als plek waar de kennis vandaan kan worden gehaald.

Landelijke netwerken zoals werkgroep Digitale ontwrichting en cyber & vakgroep Informatieveiligheid (10%), overige (8%), Het Instituut Fysieke Veiligheid (8%) en publieke kennisinstellingen zoals hogescholen en universiteiten (3%), zijn minder vaak genoemd. Daarnaast brachten de respondenten die overige hadden gekozen zelf aanvullende ideeën voor het beleggen van de kennis buiten de organisatie:

- "KPN -Security-CERT, Deloitte-CERT."
- "Vakgroep informatieveiligheid."
- "Het internet in algemene zin."
- "IBD."
- "Politie (Team digitale opsporing)."

Opmerking: er konden meerdere antwoorden worden aangekruist, waardoor de percentages zijn gebaseerd op alle aangekruiste antwoorden. Nationaal Cyber Security Center, Private kennis-/adviesbureaus zoals Fox-IT en landelijke voorziening Veiligheidsregio Information Sharing and Analysis Center heeft geen hoog percentage, maar is wel door alle respondenten gekozen. Daarnaast is 'andere veiligheidsregio's' door 11 van de 12 respondenten gekozen, is 'Landelijke netwerken zoals werkgroep Digitale ontwrichting en cyber & vakgroep Informatieveiligheid' door 6 van de 12 gekozen, is 'Instituut Fysieke Veiligheid' door 3 van de 12 gekozen en is 'publieke kennisinstellingen zoals hogescholen en universiteiten' door 2 van de 12 gekozen.

Ook werden een aantal antwoorden voorzien van een toelichting:

- "Ik denk dat er ondertussen redelijk wat kennis is opgedaan door de andere veiligheidsregio's."
- "Elke organisatie heeft te maken met cyberweerbaarheid, en je kunt van iedereen leren. Ik denk dat je het meest leert van organisaties die al verder zijn in hun plannen en uitvoering, of van organisaties die een cyber incident hebben meegemaakt. Zodat je van hun lessons learned kan leren."
- "Interne cyberincidenten zijn per definitie technisch van aard. Geen vinkje bij werkgroep Digitale ontwrichting & cyber en vakgroep informatieveiligheid omdat de werkgroep geen technische kennis heeft."
- "Eea vraagt om specialisatie die voor een 'gewoon bedrijf' niet vast te houden zijn."

Vaardigheden bij de voorbereiding:

- De vaardigheden voor het inventariseren van mogelijke dreigingen op de eigen organisatie blijkt binnen veiligheidsregio's grotendeels aanwezig te zijn. Zo is 50% van de respondenten het enigszins eens met de stelling. 25% van de respondenten is het niet eens of oneens en de andere 25% is het enigszins oneens met de stelling. Daarnaast vinden alle respondenten, op één na, dat deze vaardigheden intern moeten worden belegd (92%). 50% van de respondenten zou de vaardigheden (daarnaast/ook) extern beleggen.
- De stelling over de vaardigheden voor het inventariseren van mogelijke effecten van een intern cyberincident zorgt voor verdeeldheid. Zo is 50% van de respondenten het niet eens of oneens met de stelling. 33% is het enigszins met de stelling eens en 17% is het enigszins met de stelling oneens. Ook hier is door alle respondenten, op één na, aangegeven dat deze vaardigheden idealiter binnen de organisatie wordt belegd. Daarnaast zou 58% van de respondenten deze vaardigheden (daarnaast/ook) extern willen beleggen.
- De stelling over de vaardigheden voor het in beeld brengen van de verbondenheid tussen verschillende interne systemen, zorgt ook voor een verdeling van antwoorden van de respondenten. Het grootste deel van de respondenten is het niet eens of oneens met de stelling (58%). 25% is het enigszins eens met de stelling en 17 % is het enigszins oneens met de stelling. Bij de vraag of deze vaardigheden intern of extern moeten worden belegd, is de groep respondenten minder verdeeld. Alle respondenten, op één na, zouden de vaardigheden intern beleggen. 42% van de respondenten zou de vaardigheden (daarnaast/ook) extern willen beleggen.
- De vaardigheden voor het inventariseren van de vitale bedrijfsprocessen is volgens de respondenten zeker binnen de veiligheidsregio's aanwezig. 8% is het helemaal met de stelling eens, 67% is het enigszins met de stelling eens, 17% is het niet eens of oneens en 8% is het enigszins oneens. Daarnaast hebben alle respondenten aangegeven deze vaardigheden idealiter intern te willen beleggen.
- De vaardigheden om scenario's voor cyberoefeningen op te stellen is volgens de respondenten niet binnen alle veiligheidsregio's aanwezig. Het grootste deel van de respondenten is het niet eens of oneens met de stelling (42%). 25% is het enigszins eens met de stelling, 25% is het enigszins oneens met de stelling en 8% is het helemaal niet eens met de stelling. Daarnaast zou de meerderheid van de respondenten deze vaardigheden intern of zowel intern als extern willen beleggen (83%). 67% van de respondenten zou de vaardigheden idealiter extern of zowel intern als extern willen beleggen,

Binnen mijn organisatie hebben we voldoende vaardigheden om...	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens	Intern	Extern
…mogelijke cyberdreigingen op de eigen organisatie te inventariseren.	0	6	3	3	0	11	6
…mogelijke effecten van een intern cyberincident vooraf te inventariseren.	0	4	6	2	0	11	7
…ketenrisico's in beeld te brengen (verbondenheid van/tussen verschillende interne systemen).	0	3	7	2	0	11	5
… vitale (bedrijfs)processen te inventariseren.	1	8	2	1	0	12	0
…scenario's voor cyberoefeningen op te stellen.	0	3	5	3	1	10	8

Toelichtingen over welke vaardigheden (nog meer) nodig zijn bij de voorbereiding:

- "Auditing."
- "Bereidheid/Bewustwording."
- "Digitaal leiderschap."
- "Improvisatievermogen."
- "Een lerend vermogen, interesse in bitjes en bytjes, en de kunst om een voor veel mensen inhoudelijk moeilijk onderwerp begrijpelijk te maken. Als je snapt wat er speelt, of wat je aan het doen bent, en waarom, dan is het m.i. makkelijker om te handelen als er een incident plaatsvindt."
- "Een gecentraliseerde nog op te richten SOC en CERT kunnen ondersteunen in de (ontwikkeling van) interne vaardigheden."
- "Crisis organisatie, het opschalen naar passende niveaus."
  "Omgaan met ethisch en juridische kwesties."
- "Wij willen heel graag gaan oefenen met cyber incidenten."

Vaardigheden bij de bestrijding:

- De vaardigheden om de geraakte systemen te identificeren is volgens de meerderheid van de respondenten aanwezig binnen de veiligheidsregio's. 50% van de respondenten is het enigszins eens met de stelling, 25% is het niet eens of oneens en 25% is het enigszins oneens met de stelling. Daarnaast vindt de meerderheid van de respondenten dat deze vaardigheden intern of zowel intern als extern moeten worden belegd (83%). 50% van de respondenten zou deze vaardigheden extern of zowel intern als extern beleggen.
- De stelling over de vaardigheden die nodig zijn voor het in beeld brengen van de keteneffecten zorgt voor verdeeldheid. De meerderheid van de respondenten is het niet eens of oneens met de stelling (50%). 25% is het enigszins eens met de stelling en 25% is het enigszins oneens met de stelling. Daarnaast vindt de meerderheid van de respondenten dat deze vaardigheden intern of zowel intern als extern moeten worden belegd (83%). 67% van de respondenten zou deze vaardigheden extern of zowel intern als extern beleggen.
- De vaardigheden voor het inschatten van de mogelijke oorzaak is volgens de meeste respondenten niet aanwezig binnen de veiligheidsregio's. Zo is 42% van de respondenten het enigszins oneens met de stelling en is 8% het helemaal oneens met de stelling. Daarnaast is 33% het niet eens of oneens, maar is 17% het juist wel enigszins eens met de stelling. De reacties op de vraag of deze vaardigheden intern of extern moeten worden belegd zijn ook verdeeld. Zo vindt 75% van de respondenten dat de vaardigheden intern of zowel intern als extern moeten worden belegd, maar vindt 50% dat de vaardigheden extern of zowel intern als extern moeten worden belegd.
- De vaardigheden voor het inschatten van de schade op de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie is volgens de respondenten niet in alle veiligheidsregio's aanwezig. 33% van de respondenten is het enigszins eens met de stelling, 33% is het niet eens of oneens, 17% is het enigszins oneens en 17% is het helemaal oneens. De reacties op de vraag of deze vaardigheden intern of extern moeten worden belegd zijn verdeeld. Zo vindt 75% van de respondenten dat de vaardigheden intern of zowel intern als extern moeten worden belegd, maar vindt 67% dat de vaardigheden extern of zowel intern als extern moeten worden belegd.
- De vaardigheden voor het inschatten van de schade op de ICT-systemen is volgens de respondenten in mindere mate aanwezig binnen de veiligheidsregio's. Zo is 42% het enigszins oneens, is 42% het niet eens of oneens en is 16% het enigszins eens met de stelling. , is 8% het enigszins oneens en is 25% het helemaal niet eens met de stelling. Alle respondenten, op één na, beleggen deze vaardigheden idealiter extern of zowel intern als extern (92%). Daarnaast geeft 75% van de respondenten aan dat de vaardigheden idealiter (daarnaast/ook) intern worden belegd.
- De vaardigheden om de impact op organisatieprocessen in te schatten is volgens de respondenten aanwezig binnen de veiligheidsregio's. 58% is het enigszins eens met de stelling, 25% is het niet eens of oneens en 17% is het enigszins oneens met de stelling. Alle respondenten geven hierbij aan dat de vaardigheden intern moeten worden belegd (100%). Daarnaast zou 17% van de respondenten de vaardigheden daarnaast ook extern willen beleggen.
- De vaardigheden om de duur van de verstoring in te schatten is volgens de respondenten in mindere mate aanwezig binnen de veiligheidsregio's. Zo is 17% van de respondenten het helemaal oneens met de stelling, is 42% het enigszins oneens, is 33% het niet eens of oneens en is de overige 8% het enigszins eens met de stelling. Daarnaast zouden alle respondenten,

op één na, deze vaardigheden idealiter extern willen beleggen. 67% van de respondenten zou de vaardigheden (daarnaast/ook) intern willen beleggen.

- De vaardigheden om een (technisch)oplossingsperspectief te vinden is volgens de respondenten ook niet aanwezig binnen de veiligheidsregio's. 50% is het enigszins oneens met de stelling, 25% is het niet eens of oneens en 25% is het enigszins eens. Echter gaven alle respondenten, op één na, aan dat deze vaardigheden idealiter intern worden belegd (92%). Daarnaast gaf 67% aan dat de vaardigheden idealiter (daarnaast/ook) extern worden belegd.
- De vaardigheden om de bron van de verstoring te bestrijden is volgens de respondenten ook in mindere mate aanwezig binnen de veiligheidsregio's. Zo is 17% van de respondenten het helemaal oneens met de stelling, is 50% het enigszins oneens, is 17% het niet eens of oneens en is 16% het enigszins eens met de stelling. Daarnaast zou 83% van de respondenten de vaardigheden idealiter extern of zowel intern als extern beleggen, maar zou 67% de vaardigheden idealiter intern of zowel intern als extern beleggen.
- De vaardigheden om de gevolgen en effecten van een incident te verkleinen of bestrijden zorgt bij verdeeldheid onder de respondenten. Zo is het grootste deel van de respondenten het niet eens of oneens met de stelling (67%). 17% van de respondenten is het enigszins eens met de stelling, maar 17% is het enigszins oneens. De reacties op de vraag of deze vaardigheden intern of extern moeten worden belegd zijn minder verdeeld. Zo vinden alle respondenten, op één na, dat de vaardigheden intern of zowel intern als extern moete worden belegd. Daarnaast vindt 50% van de respondenten dat de vaardigheden idealiter (daarnaast/ook) extern worden belegd.
- De stelling over de vaardigheden om de schade aan ICT-systemen te herstellen voor verdeeldheid onder de respondenten. Zo is 33% van de respondenten het enigszins eens met de stelling, is 33% het niet eens of oneens, is 25% het enigszins oneens en is 9% het helemaal oneens. Daarnaast zou 83% van de respondenten deze vaardigheden idealiter extern of zowel intern als extern willen beleggen. 75% van de respondenten zou de vaardigheden idealiter intern of zowel intern als extern willen beleggen.
- De vaardigheden om beslissingen te nemen in grote onzekerheid en complexiteit is volgens de respondenten aanwezig binnen de veiligheidsregio's. Zo is 8% het helemaal eens met de stelling. Is 42% het enigszins eens met de stelling, is 25% het niet eens of oneens, is 17% het enigszins oneens en is 8% het helemaal oneens met de stelling. Daarnaast hebben alle respondenten aangegeven dat ze deze vaardigheden idealiter intern beleggen. 50% zou de vaardigheden daarnaast ook extern willen beleggen.
- De vaardigheden om adequaat richting het bestuur van de eigen organisatie te communiceren is volgens de respondenten ook aanwezig binnen de veiligheidsregio's. Zo is 17% het helemaal eens met de stelling, is 42% het enigszins eens met de stelling, is 25% het niet eens of oneens en is 17% het enigszins oneens met de stelling. Ook hier hebben alle respondenten aangegeven deze vaardigheden idealiter intern te beleggen. Daarnaast zou 17% van de respondenten deze vaardigheden ook extern beleggen.
- De vaardigheden om adequaat extern te communiceren is volgens de respondenten aanwezig binnen de veiligheidsregio's. 8% is het helemaal eens met de stelling, 58% is het enigszins eens met de stelling, 25% is het niet eens of oneens en 8% is het enigszins oneens. Ook hier hebben alle respondenten aangegeven deze vaardigheden idealiter intern te beleggen. 25% van de respondenten zou de vaardigheden daarnaast ook nog extern willen beleggen.

Binnen mijn organisatie hebben we bij een intern cyberincident voldoende vaardigheden om...	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens	Intern	Extern
…de geraakte systemen te identificeren.	0	6	3	3	0	10	6
…de keteneffecten in beeld te brengen (verbondenheid van het geraakte systeem met andere systemen).	0	3	6	3	0	10	8
…de mogelijke oorzaak (technische storing, menselijke fout of doelbewuste aanval) in te schatten.	0	2	4	5	1	9	6
…de schade op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te inventariseren (zoals verlies van vertrouwelijke gegevens).	0	4	4	2	2	9	8
…de schade op ICT-systemen te inventariseren.	0	2	5	5	0	9	11
…de impact op organisatieprocessen (bijvoorbeeld hulp- of dienstverlening) in te schatten.	0	7	3	2	0	12	2
…de duur van de verstoring in te schatten.	0	1	4	5	2	8	11
…een (technisch) oplossingsperspectief te vormen.	0	3	3	6	0	11	8
…de bron van de verstoring te bestrijden.	0	2	2	6	2	8	10
…de gevolgen/effecten van het incident te bestrijden of verkleinen.	0	2	8	2	0	11	6
…de schade aan ICT-systemen te herstellen.	0	4	4	3	1	9	10

…beslissingen te nemen in grote onzekerheid en complexiteit.	1	5	3	2	1	12	6
…adequaat richting het bestuur van de eigen organisatie te communiceren over het cyberincident.	2	5	3	2	0	12	2
…adequaat extern te communiceren over het cyberincident.	1	7	3	1	0	12	3

Toelichtingen over welke vaardigheden (nog meer) nodig zijn bij de bestrijding:

- “Forensische vaardigheden vooral uit externe expertise halen.”
- “Ervaring met de coördinatie van het bestrijden van cyberincidenten.”
- “Denk dat de communicatie een samenspel is van de externe en wijzelf, wij vertalen het dan richting management.”
- “Alle ICT is uitbesteed, vaardigheid om snel te schakelen en goeden afspraken en relatiemanagement met externe leverancier is wel handig.”.
- “Afhankelijk van keuzes uit directie en management.”

Het intern beleggen van de vaardigheden voor de bestrijding van interne cyberincidenten:

De meeste respondenten zouden de vaardigheden van de bestrijding van interne cyberincidenten binnen de organisatie idealiter bij een CISO (Chief Information Security Officer) beleggen (28%) en/of bij ICT medewerkers beleggen (28%). Daarnaast zouden respondenten het ook bij medewerkers crisisbeheersing beleggen (22%).De overige respondenten (22%) brachten zelf ideeën voor het beleggen van de kennis binnen de organisatie:

- “(Technical) Information Security Officer.”
- “Security-Board (CISO, FG, Business Controller, Jurist.”
- “Heel de organisatie.”
- “Externe forensische expertise.”
- “Externe partner.”
- “Directie.”
- “Betrokkenheid van andere afdelingen.”

Daarnaast werden een aantal antwoorden voorzien van een toelichting:

- “Geen CISO.”
- “Met deze vraag kan ik even niets sorry. Ik weet niet waar je op doelt. Idealiter worden vaardigheden mbt cyberweerbaarheid in verschillende vormen/niveau's van alle medewerkers gevraagd. Iedereen maakt gebruik van informatie en iedereen kan een melder moeten zijn, en iedereen mag op zijn hoede zijn bij verdachte zaken. Er zal een hele matrix zijn aan wat iemand moet weten per type rol (gebruiker, functioneel beheerder, teamleider, CISO, etc). Idealiter borg je alle typen vaardigheden (dus ook andere dan cyberweerbaarheid)

in een brede P&O structuur. Maar als je bedoelt, wie heeft de regie over het inbedden van deze vaardigheden binnen de organisatie, dan kom ik bij de CISO uit."

- "Uitgaande dat hier een crisis wordt bedoeld i.p.v. incident - Idealiter is de CISO en de ICT-afdeling vaardig op technisch vlak en komt er ondersteuning van de crisisorganisatie op het vlak van het inrichten van een crisisorganisatie en crisiscommunicatie."
- "Diverse schakels nodig voor escalatie."

Het extern beleggen van de vaardigheden voor de bestrijding van interne cyberincidenten:

Alle twaalf respondenten zouden de vaardigheden voor de bestrijding van interne cyberincidenten buiten de organisatie idealiter bij Private kennis-/adviesbureaus zoals Fox-IT beleggen (22%). Daarnaast zouden elf respondenten de vaardigheden bij landelijke voorziening Veiligheidsregio Information Sharing and Analysis Center (20%) en zouden tien respondenten het bij het Nationaal Cyber Security Center (19%) beleggen. Negen respondenten noemden andere veiligheidsregio's (17%) en zes respondenten kozen voor landelijke netwerken zoals werkgroep Digitale ontwrichting en cyber & vakgroep Informatieveiligheid (11%). Publieke kennisinstellingen zoals hogescholen en universiteiten werd door drie respondenten gekozen (6%), Het Instituut Fysieke Veiligheid is door twee respondenten gekozen (4%) en de laatste respondent (2%) brachten zelf aanvullende ideeën voor het beleggen van de kennis buiten de organisatie:

- "Vakgroep informatieveiligheid."

Ook werden een aantal antwoord voorzien van een toelichting:

- "Ik denk dat bedoeld wordt met de vraag, waar is er ervaring of vaardigheid met hoe om te gaan met incidenten? Vooraf of als er een incident gaande is? of allebei? Afhankelijk van waarin je verkeert, zou ik bij een gaand incident eerst ISAC raadplegen, die zullen me adviseren om zo snel mogelijk te schakelen met extern bureau omdat we geen ICT kennis in huis hebben. Parallel ook het NCSC te informeren. Maar bij het maken van een goed plan (van aanpak), kan ik de vaardigheden van alle partijen aanspreken."
- "Regio's maken voor een deel gebruik van vergelijkbare systemen, deze kennis en vaardigheden kun je delen wanneer nodig."

Middelen en gelegenheid:

- De technische middelen om voor te bereiden op interne cyberincidenten zijn volgens de respondenten niet voldoende aanwezig. Het grootste deel van de respondenten (50%) is het enigszins oneens met de stelling en 17% is het zelf helemaal oneens. De overige 33% van de respondenten is het niet eens of oneens.
- De hulpmiddelen om voor te bereiden op interne cyberincidenten zijn volgens de respondenten ook niet voldoende aanwezig. Zo is 33% het enigszins oneens met de stelling en is 33% het helemaal niet eens met de stelling. De overige respondenten (33%) zijn het niet eens en niet oneens met de stelling.
- De hoeveelheid personeel dat is toegerust om zich voor te bereiden op interne cyberincidenten is volgens de respondenten ook niet voldoende aanwezig. Zo is 50% van de respondenten het helemaal niet eens met de stelling en is 42% het enigszins oneens. Daarnaast is 8% het niet eens of oneens.
- Ook de hoeveelheid beschikbare tijd is volgens de respondenten niet voldoende. Zo is 66% het helemaal oneens met de stelling en is 33% het enigszins oneens.

- Ook de hoeveelheid beschikbare financiële middelen is volgens de respondenten niet voldoende voor de voorbereiding op interne cyberincidenten. Zo is 50% van de respondenten het helemaal oneens met de stelling en is 33% het enigszins oneens. De overige respondenten zijn het niet eens of oneens (8%) of zijn het opvallend genoeg helemaal eens met de stelling (8%).

Onze organisatie…	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens
…bezit voldoende technische middelen (zoals systemen) om zich voor te bereiden op interne cyberincidenten.	0	X	4	6	2
…bezit voldoende hulpmiddelen (zoals handreikingen, methodieken en protocollen) om zich voor te bereiden op interne cyberincidenten.	0	X	4	4	4
…bezit voldoende personeel, toegerust om zich voor te bereiden op interne cyberincidenten.	0	X	1	5	6
…reserveert voldoende tijd om zich voor te bereiden op interne cyberincidenten.	0	X	0	4	8
…reserveert voldoende financiële middelen om zich voor te bereiden op interne cyberincidenten.	1	X	1	4	6

Toelichtingen:

- "Ik denk dat menigeen zich overschat in de beschikbare kennis en kunde die nodig is voor een cyberincident. Evenals de benodigde middelen."
- "Het onderwerp is de afgelopen jaren onderbelicht geweest. Er is nu wel aandacht, maar we staan 5-0 achter."
- "Eea is in wording, huidige situatie onvoldoende."
- "De urgentie wordt wel opgemerkt, maar de dagelijkse operatie vraagt al (te)veel tijd."

Netwerken en samenwerking:

- Het zicht van veiligheidsregio's op interne deskundigen voor de incidentbestrijding van een intern cyberincident is volgens de meeste de respondenten goed. Zo is 58% het enigszins met de stelling eens. Echter is 25% van de respondenten is het enigszins oneens met de stelling, wat inhoudt dat veiligheidsregio's volgens hen geen zicht hebben op de interne deskundigen. De overige respondenten (17%) zijn het niet eens of oneens.
- Over de vraag of veiligheidsregio's de partijen kennen die kunnen helpen in de voorbereiding van de bestrijding heerst minder verdeeldheid. Met 83% die het enigszins eens is met de stelling en 8% die het helemaal eens is met de stelling, blijkt dat veiligheidsregio's de partijen

kennen die kunnen helpen bij de voorbereiding. De overige 8% is het niet eens of oneens met de stelling.

- Ook kennen veiligheidsregio's volgens de respondenten de partijen die kunnen helpen bij de bestrijding. Het grootste deel van de respondenten (50%) is het enigszins eens met de stelling en 25% van de respondenten is het helemaal eens met de stelling. 25% van de respondenten is het niet eens of oneens met de stelling.
- Het inzetten van externe expertise voor de voorbereiding op de bestrijding kan volgens 67% van de respondenten door de veiligheidsregio's worden gedaan, aangezien zij het helemaal of enigszins eens zijn met de stelling. 33% geeft aan het niet eens of oneens te zijn met de stelling.
- Het inzetten van externe expertise voor de bestrijding kan volgens 58% van de respondenten door de veiligheidsregio's worden gedaan, aangezien zij het helemaal of enigszins eens zijn met de stelling. Daarnaast is 25% het niet eens of oneens, is 8% het enigszins oneens en is 8% het helemaal oneens met de stelling.

Binnen mijn organisatie…	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens
… hebben wij zicht op interne deskundigen voor de incidentbestrijding van een intern cyberincident.	0	7	2	3	0
…kennen wij overheidsorganisaties en private partijen, die ons kunnen helpen bij de **voorbereiding** op de bestrijding van interne cyberincidenten.	1	10	1	0	0
…kennen wij overheidsorganisaties en private partijen, die ons kunnen helpen bij de **bestrijding** van interne cyberincidenten.	3	6	3	0	0
…zijn wij in staat om externe expertise in te zetten voor de **voorbereiding** op interne cyberrisico's (denk aan o.a. het NCSC/ private IT-dienstverleners).	1	7	4	0	0
… zijn wij in staat om externe expertise in te zetten voor de **bestrijding** van interne incidenten (denk aan o.a. het NCSC/ private IT-dienstverleners).	1	6	3	1	1

Toelichtingen:

- “We zijn wel in staat om de externe expertise in te zetten, echter ontbreekt het nog aan de juiste SLA's voor acute inzet.”
- “Ik denk dat al er echt iets gebeurd, er opeens veel mogelijk is. Wel een persoonlijke mening/inschatting.”
- “VR-ISAC is al ingezet geweest bij de crisis in VNOG en zou ook door andere VR's als externe expertise kunnen worden ingeschakeld.”
- “Staat en valt bij keuzes vanuit het management.”
- “Indien een intern incident zicht voordoet, zijn de benodigde contacten beschikbaar.”

Interventies en verbeteringen:

- De respondenten zijn verdeeld als wordt gekeken naar de belangrijkste factoren waarop veiligheidsregio’s zich moeten richten om de voorbereiding op interne cyberincidenten te versterken. Met een gemiddelde van 2.75 is motivatie/urgentiebesef volgens de respondenten de belangrijkste factor. Daarna volgen tijd (gem. 3.42) en middelen (gem. 3.50). Geld, kennis en kunde/vaardigheden zijn iets minder vaak gekozen met respectievelijk gemiddelden van 4.50, 4.58 en 5.08. Netwerken en samenwerking staat onderaan met een gemiddelde van 5.33 en ‘overige’ met een gemiddelde van 6.83. Hierbij zijn twee extra factoren genoemd: “Je zou ze allemaal op 1 willen zetten...” & “Ik heb tijd hoog gezet omdat je met meer tijd, ook kennis en kunde kunt gaan opdoen. Bijv. door netwerken en samenwerken. Dan weet je wat er nodig is, en vraag je geld om daartoe de middelen voor te kunnen regelen.”.

	1	2	3	4	5	6	7	8
Motivatie/urgentiebesef	4	2	2	2	1	1	0	0
Kennis	2	0	1	0	5	3	1	0
Kunde/vaardigheden	1	1	1	1	1	3	4	0
Middelen (mensen, systemen, handreikingen etc.)	2	2	2	3	1	1	1	0
Netwerken en samenwerking	1	1	0	1	3	2	2	2
Tijd	0	3	4	4	0	0	1	0
Geld	0	3	2	1	1	2	3	0
Overig	2	0	0	0	0	0	0	10

	Gemiddelde	Standaardafwijking
Motivatie/urgentiebesef	2.75	1.64
Kennis	4.58	1.85
Kunde/vaardigheden	5.08	2.02
Middelen (mensen, systemen, handreikingen etc.)	3.50	1.80
Netwerken en samenwerking	5.33	2.09
Tijd	3.42	1.32
Geld	4.50	1.98
Overig	6.83	2.61

Overige behoeften voor een verbetering van de voorbereiding op de bestrijding:

- “Ik kan nu even niets bedenken.”
- “Allemaal snel aan de slag met het versnellingsprogramma informatieveiligheid.”
- “M.i. moet je het voorbereiden op Cyberincidenten niet regionaal laten organiseren, maar vanuit bijvoorbeeld het IFV die met een team de regio's jaarlijks bezoekt, zo ervaring opbouwt, goed kan vergelijken tussen de regio's onderling en kan worden ingezet bij een regio indien de situatie hierom vraagt.”

Bijlage 9 Resultaten enquête cybergevolgbestrijding

Uitwerking resultaten enquête cybergevolgbestrijding
Respondenten: werkgroep Digitale ontwrichting en cyber (14)

Motivatie en urgentiebesef

- De respondenten geven aan dat het management van de veiligheidsregio over het algemeen bewust is van de dreigingen uit het digitale domein voor de regio. 93% van de respondenten is het enigszins of helemaal eens met de stelling. De overige respondenten zijn het niet eens of oneens.
- De mensen op operationeel niveau lijken iets minder bewust te zijn van de dreigingen uit het digitale domein voor de regio. 50% van de respondenten is het enigszins of helemaal eens met de stelling. 21% van de respondenten is het enigszins of helemaal oneens met de stelling. De overige respondenten (29%) zijn het niet eens of oneens.
- Daarnaast lijkt het management de voorbereiding op externe cyberincidenten belangrijk te vinden, aangezien 93% van de respondenten het enigszins of helemaal eens is met de stelling. De overige respondenten (7%) zijn het niet eens of oneens.
- Ook hierbij geven de respondenten aan dat de voorbereiding op externe cyberincidenten minder belangrijk wordt gevonden door mensen op operationeel niveau. Hierbij is 57% van de respondenten het enigszins of helemaal eens met de stelling (in tegenstelling tot 93% bij het management). Daarnaast is 21% van de respondenten het enigszins oneens.
- De helft van de respondenten (50%) vindt dat de voorbereiding op externe cyberincidenten hoge prioriteit krijgt binnen de veiligheidsregio en is het daarom helemaal of enigszins eens met de stelling. 29% van de respondenten is het niet eens of oneens en 21% van de respondenten is het enigszins oneens met de stelling.

Binnen mijn organisatie…	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens
…is het management bewust van de dreigingen uit het digitale domein voor de regio.	5	8	1	0	0
…zijn mensen op operationeel niveau bewust van de dreigingen uit het digitale domein voor de regio.	1	6	4	2	1
…vindt het management de voorbereiding op externe cyberincidenten belangrijk.	6	7	1	0	0
…vinden mensen op operationeel niveau de voorbereiding op externe cyberincidenten belangrijk.	2	6	5	0	1
…heeft de voorbereiding op externe cyberincidenten hoge prioriteit.	2	5	4	3	0

Toelichtingen:

- "Cyberincidenten worden momenteel een beetje weggedrukt door Corona crisis zoals zoveel andere zaken."
- "Volgens mij zien medewerkers VR een cyberincident vooral als iets waar zij alleen de gevolgen moeten aanpakken. Dus langdurige uitval van drinkwater, elektra logistieke ketens."
- "Op papier wel, tot het geld of capaciteit kost."

Kennis bij de voorbereiding:

- De kennis voor het inventariseren van mogelijke dreigingen op de regio blijkt binnen veiligheidsregio's gering aanwezig te zijn. Zo is 79% van de respondenten het enigszins of helemaal niet eens met de stelling. Echter zou 86% van de respondenten deze kennis idealiter extern/buiten de organisatie beleggen. 43% van de respondenten zou deze kennis (daarnaast/ook) intern willen beleggen.
- De kennis voor het inventariseren van mogelijke maatschappelijke effecten van een extern cyberincident is volgens de respondenten wel binnen veiligheidsregio's te vinden. Zo is 57% van de respondenten het enigszins of helemaal eens met de stelling. Toch lijkt er nog wel ruimte voor verbetering, aangezien 29% van de respondenten het niet eens of oneens is en 14% van de respondenten het enigszins of helemaal oneens is. Zeker, aangezien door alle respondenten is aangegeven dat deze kennis idealiter binnen de organisatie wordt belegd. Daarnaast zou 36% van de respondenten deze kennis daarnaast ook extern willen beleggen.
- De kennis voor het inventariseren van de maatschappelijk belangrijke externe processen en bedrijven binnen de regio, is met een percentage van 57% ook binnen de veiligheidsregio aanwezig. De overige respondenten (43%) zijn het niet eens en niet oneens met de stelling. Ook hier is volgens de respondenten dus nog ruimte voor verbetering. Bij de vraag of deze kennis intern of extern moet worden belegd, is de groep respondenten verdeeld. 71% van de respondenten zou de kennis intern of zowel intern als extern willen beleggen. 64% van de respondenten zou de kennis extern of zowel intern als extern willen beleggen.

Binnen mijn organisatie hebben we voldoende kennis om...	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens	Intern	Extern
…mogelijke cyberdreigingen op de regio te inventariseren.	0	1	2	7	4	6	12
…mogelijke maatschappelijke effecten van een extern cyberincident vooraf te inventariseren.	1	7	4	1	1	14	5
…maatschappelijk belangrijke externe processen en bedrijven te inventariseren(denk aan vitale infrastructuur zoals elektriciteit, internet, drinkwater of betalingsverkeer).	0	8	6	0	0	10	9

Toelichtingen over welke kennis (nog meer) nodig is bij de voorbereiding:

- “Het netwerk goed kennen dus weten wie je waarvoor moet hebben in een digitale crisissituatie of dreiging, er echt mee oefenen.”
- “Taken, verantwoordelijkheden en bevoegdheden van betrokken partijen, verhouding partners in het cyberdomein, wie kan ons waarmee helpen?”
- “Het gaat bij ons meer om capaciteit, zodat we meer kunnen doen om ons op dit thema verder te verdiepen en bekwamen.”
- “Het speelveld welke partijen spelen welke rol bij een digitale verstoring.”
- “Informatie over de operationele aanpak van de bestrijding door externe partij. Hoe groot is de kans dat vitale sectoren uitvallen?”
- “Wat de effecten van een cyberaanval zijn op een bedrijf in de regio wat maatschappelijke ontwrichting tot gevolg kan hebben, buiten de vitale infrastructuren en RBP bedrijven waar wij als eerste aan denken. Ik denk dat we ons onvoldoende bewust zijn van mogelijke andere gevaren die schuilen bij andere (externe) bedrijven als gevolg van een cyberaanval. Daarnaast is het lastig te bepalen in hoeverre de veiligheidsregio daarvoor aan de lat staat en wat wij daarin zouden kunnen betekenen.”
- “Kennis over de 'domino-effecten'; als er ergens iets gebeurt, waar kan dat dan mogelijk nog meer effect op hebben?”
- “Binnen de directie Risicobeheersing is het nog zoeken welke digitale dreigingen/risico's noodzakelijk zijn om te zoeken, het gaat namelijk vooral om de impact die iets kan hebben. Onze primaire focus gaat uit naar vitale bedrijven, BRZO bedrijven etc. Bij verstoring zal de maatschappelijke impact groot zijn. Daarnaast moeten we de functionarissen van de regionale crisisorganisatie 'cyberbekwaam' maken, met daarbij in achtneming dat de verantwoordelijkheid ligt bij de effectbestrijding.”
- “Partners die bij de bestrijding van dit soort incidenten belangrijk zijn.”
- “Realistische scenariobeschrijvingen met voorstelbare cascade-effecten.”
- “De concrete uitwerking van onze rol bij het bestrijden van effecten als gevolg van een cyberincident. Dan met name onze rol ten opzichte van alle andere betrokken partijen.”
- “Basiskennis van veelgebruikte begrippen en de dynamiek van een cybercrisis.”
- “Als ik puur naar gevolgbestrijding kijk dan denk ik dat wij nog onvoldoende externe expertise inschakelen. Als regio is het moeilijk om deze kennis binnen huis te krijgen. We hebben ontzettend goede contacten met onze partners, maar er is geen verbinding op bijv. ICT niveau. Operationele voorbereiding op andere thema's hebben we wel geborgd, maar het is raar dat wij ICT specialisten van onze organisatie niet koppelen aan ICT specialisten van onze partners. Doe je dit wel, dan kan je volgens mij heel snel inzichtelijk maken waar de kwetsbaarheden in onze regio zit.”
- “Netwerken en kennis van cyber.”

Kennis bij de bestrijding:

- De kennis om de mogelijke oorzaak van een extern cyberincident in te schatten is volgens de respondenten niet aanwezig binnen de veiligheidsregio’s. 86% van de respondenten is het enigszins of helemaal oneens met de stelling. Daarnaast vinden alle respondenten dat deze kennis extern moet worden belegd. 21% van de respondenten zou deze kennis daarnaast ook intern beleggen.
- De kennis die nodig is voor het inschatten van de duur van een verstoring is volgens de respondenten ook niet aanwezig binnen de veiligheidsregio’s. 93% van de respondenten is het enigszins of helemaal oneens met de stelling. Daarnaast vinden alle respondenten, op

één na, dat deze kennis extern moet worden belegd. 36% van de respondenten vinden dat de kennis (daarnaast/ook) intern moet worden belegd.

- De kennis voor het inschatten van de impact op maatschappelijke processen is volgens de meeste respondenten echter wel aanwezig binnen de veiligheidsregio's. Zo is 50% van de respondenten het enigszins eens, is 36% van de respondenten het niet eens of oneens en is 14% van de respondenten het enigszins oneens met de stelling. Over de mate waarin deze kennis binnen veiligheidsregio's aanwezig is heerst dus nog verdeeldheid. De reacties op de vraag of deze kennis intern of extern moet worden belegd zijn minder verdeeld. Zo vinden alle respondenten dat deze kennis intern moet worden belegd, maar vindt 50% dat deze kennis daarnaast ook extern moet worden belegd.
- De kennis voor het bestrijden of verkleinen van de gevolgen is volgens de respondenten wel binnen de veiligheidsregio's aanwezig. 64% van de respondenten is het helemaal of enigszins eens met de stelling. De overige 36% van de respondenten is het niet eens en niet oneens met de stelling. De reacties op de vraag of deze kennis intern of extern moet worden belegd zijn minder verdeeld. Zo vinden alle respondenten dat deze kennis intern moet worden belegd, maar vindt 50% dat deze kennis daarnaast ook extern moet worden belegd.

Binnen mijn organisatie hebben we bij een extern cyberincident voldoende kennis om…	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens	Intern	Extern
…de mogelijke oorzaak (technische storing, menselijke fout of doelbewuste aanval) in te schatten.	0	0	2	4	8	3	14
…de duur van de verstoring in te schatten.	0	0	1	4	9	5	13
…de impact op maatschappelijke processen in te schatten (denk aan vitale infrastructuur zoals elektriciteit, internet, drinkwater of betalingsverkeer).	0	7	5	2	0	14	7
…de gevolgen/effecten van het incident te bestrijden of verkleinen.	1	8	5	0	0	14	7

Toelichtingen over welke kennis (nog meer) nodig is bij de gevolgbestrijding:

- "Taken, verantwoordelijkheden en bevoegdheden van betrokken partijen, verhouding partners in het cyberdomein, wie kan ons waarmee helpen?"
- "Kennis van relevante netwerkpartners (wie heb je nodig, hoe bereik je ze ten tijde van cybercrises, etc))"

- “Kennissen in het digitale domein is misschien nog wel belangrijker dan eigen kennis.”
- “Idem: kennis over 'domino-effecten'; als er ergens iets gebeurt, wat voor effect op andere sectoren/vitale processen kan dat hebben?”
- “Belangrijkste is enige vorm van 'cyberbekwaamheid', maar de getroffen organisatie is primair verantwoordelijk voor het geven van duiding. Het is dus vooral belangrijk om een goed netwerk te hebben én goede werkafspraken. Het inschatten van de impact op maatschappij is een taak van de veiligheidsregio, een integraal beeld opmaken, hiervoor is bepaalde kennis nodig.”
- “Meer inzicht in de duur en oplossingsperspectieven.”
- “Kennis van netwerken, sturingslijnen.”
- “Bij een incident zoals deze is de technische duiding en de vertaalslag naar crisisbeheersing niet geborgd.”
- “Kennis van de landelijke crisisstructuur bij cyberincidenten en kennis van partners die van belang zijn tijdens een cybercrisis.”
- “Je moet als het ware een liaison Cyber kunnen oproepen. Ik geloof dat onze crisisorganisatie prima in staat is om de effecten te gaan aanpakken of te verkleinen, maar dan heb je wel kennis nodig op het thema. Nu hebben we dit geborgd met het cybercrimeteam van onze politie-eenheid. Je hebt duiding nodig op het thema en inschatting van hoe lang dit gaat duren. Wij gaan zelf 'de brand niet blussen'.”
- “Cyber inhoudelijk.”
-

Het intern beleggen van de kennis over de gevolgbestrijding van externe cyberincidenten:

De meeste respondenten zouden de kennis over de gevolgbestrijding van externe cyberincidenten idealiter binnen de organisatie bij medewerkers crisisbeheersing beleggen (48%). 24% van de respondenten had de voorkeur om de kennis binnen de organisatie bij een CISO (Chief Information Security Officer) te beleggen en 11% zou het idealiter bij ICT medewerkers beleggen. De overige respondenten (17%) brachten zelf ideeën voor het beleggen van de kennis binnen de organisatie:

- “Regiogrensoverschrijdend, dus bij een SOC op CERT bovenregionaal”
- “Landelijk expert team”
- “Getroffen organisatie(s), netwerk in de regio, politie (team cybercrime), gemeenten, NCSC, NCTV.”
- “Crisisfunctionarissen”
- “Je kan het ook borgen door slimme pps-constructies. De echte vakkundige mensen werken vaak in de private sector, niet in de publieke.”

Daarnaast werden veel antwoorden voorzien van een toelichting:

- “Mix / samenwerking van de getroffen organisatie(s) en de crisisorganisatie.”
- “Gevolgbestrijding 'hoort' in algemene zin bij de crisisorganisatie.”
- “Lijkt mij niet zinvol om 25 maal veel moeite te moeten doen om bij te blijven. Liever een kleiner landelijk expert team wat je kan helpen.”
- “Doe wat je normaal ook doet bij de voorbereiding op andere incidenten.”
- “Een combinatie. We hebben denk ik ICT kennis nodig om volledig in kaart te hebben waar een verstoring allemaal impact kan gaan hebben en hoe groot de afhankelijkheden zijn. Vervolgens hoe wij in geval van crisis zo goed mogelijk als crisisorganisatie kunnen acteren, wat echt wel anders is dan bij de 'bekende' incidenten.”

- “Onze maatschappij zit dermate ingewikkeld in elkaar, en is der mate verweven met elkaar, dat er een integraal beeld opgemaakt moet worden.”
- “Ik denk dat alle die categorieën hun eigen rol hebben. Zowel in de koude als warme fase.”
- “Dit moet primair liggen bij de medewerkers van crisisbeheersing. Bij een cyberincident zou er bij de CISO geïnformeerd kunnen worden voor een eerste duiding omdat technische kennis op dat moment nog niet aanwezig is binnen de crisisorganisatie.”
- “Ik denk dat onze eigen ICT afdeling ons al van veel duiding kan voorzien. Een slimme wisselwerking tussen de afdeling crisisbeheersing en ICT zou dus voor de hand liggen, maar is nog niet vanzelfsprekend. Al moet ik zeggen dat de lijnen tussen CISO en wij als medewerkers van de afdeling Crisisbeheersing kort zijn.”
- “Eigen organisatie of gevolgbestrijding is zo n verschil dat dit bij de crisisorganisatie moet liggen.”

Het extern beleggen van de kennis over de gevolgbestrijding van externe cyberincidenten:

De meeste respondenten zouden de kennis over de gevolgbestrijding van externe cyberincidenten idealiter buiten de organisatie bij het Nationaal Cyber Security Center (17%) en Private kennis-/adviesbureaus zoals Fox-IT (17%) beleggen. Ook publieke kennisinstellingen zoals hogescholen en universiteiten (16%), landelijke voorziening Veiligheidsregio Information Sharing and Analysis Center (14%), landelijke netwerken zoals werkgroep Digitale ontwrichting en cyber & vakgroep Informatieveiligheid (12%) en andere veiligheidsregio’s (12%) zijn vaak genoemd als organisaties waar de kennis extern zou kunnen worden belegd. Het Instituut Fysieke Veiligheid is met 7% opvallend weinig genoemd. De overige respondenten (4%) brachten zelf aanvullende ideeën voor het beleggen van de kennis buiten de organisatie:

- IBD, Digital Trust Center (DTC), getroffen organisatie(s), HTC politie
- Politie
- Ministeries en de partijen waar het om gaat als RWS, drinkwater bedrijven etc.

Ook werden een aantal antwoorden voorzien van een toelichting:

- “Allen in de koude fase, maar in warme fase denk ik alleen NCSC, andere regio's (die ervaring hebben met cybercrises), VR-ISAC.”
- “Voor bv. de scholen en kennisinstellingen geldt dat we ze kunnen benaderen, maar we de eerste stap vaak nog moeten zetten. Dat kan beter in 'vredestijd' dan in crisistijd. Door Corona loopt deze oriëntatie vertraging op.”
- “Bij een externe cyberverstoring is het zeer de vraag in hoeverre de veiligheidsregio betrokken/verantwoordelijk is en of zij één van deze partijen moeten betrekken.”

Vaardigheden bij de voorbereiding:

- De vaardigheden voor het inventariseren van mogelijke dreigingen op de regio blijkt binnen veiligheidsregio's gering aanwezig te zijn. Zo is 79% van de respondenten het enigszins of helemaal niet eens met de stelling. Daarnaast heerst er verdeeldheid over de vraag of deze vaardigheden intern of extern moeten worden belegd. Zo zou 57% van de respondenten de vaardigheden intern of zowel intern als extern beleggen en zou 79% van de respondenten de vaardigheden extern of zowel intern als extern beleggen. De meerderheid zou dus in ieder geval de vaardigheden extern beleggen.
- De stelling over de vaardigheden voor het vooraf inventariseren van de mogelijke maatschappelijke effecten van een cyberincident zorgt voor verdeeldheid onder de respondenten. Zo is 14% het helemaal eens met de stelling, is 36% het eens met de stelling, is 21% het niet eens of oneens en is 29% van de respondenten het enigszins oneens met de stelling. Wel wordt door alle respondenten, op één na, aangegeven dat deze vaardigheden intern moeten worden belegd. 50% van de respondenten zou deze vaardigheden (daarnaast/ook) extern beleggen.
- De vaardigheden voor het inventariseren van maatschappelijk belangrijke externe processen en bedrijven, blijkt door een overgrote meerderheid van de respondenten binnen de veiligheidsregio's aanwezig te zijn. 79% van de respondenten zijn het helemaal of enigszins met de stelling eens en geven daarmee aan dat de vaardigheden aanwezig zijn. Daarnaast is door alle respondenten aangegeven dat deze vaardigheden idealiter binnen de organisatie worden belegd. 57% zou deze vaardigheden daarnaast ook extern beleggen.

Binnen mijn organisatie hebben we voldoende vaardigheden om…	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens	Intern	Extern
…mogelijke cyberdreigingen op de regio te inventariseren.	0	1	2	7	4	8	11
…mogelijke maatschappelijke effecten van een extern cyberincident vooraf te inventariseren.	2	5	3	4	0	13	7
…maatschappelijk belangrijke externe processen en bedrijven te inventariseren (denk aan vitale infrastructuur zoals elektriciteit, internet, drinkwater of betalingsverkeer).	1	10	2	1	0	14	8

Toelichtingen over welke vaardigheden (nog meer) nodig zijn bij de voorbereiding:

- "VR is niet de kennispartij om cyberdreiging te kunnen inventariseren in het algemeen, maar wel voor haar eigen organisatie specifiek."
- "Vaardigheden met atypische en langdurige maatschappij ontwrichtende incidenten. We zijn nu veelal van de korte klap."
- "Ik denk dat vooral externe bedrijven (als in; niet voor ons bekend als vitaal) onvoldoende in beeld zijn. Zij hebben ongetwijfeld een heel ICT team en netwerken gericht op cybersecurity, waar wij als VR onvoldoende op aangehaakt zijn. De vraag is ook wat voor ontwrichting bij een aanval op bedrijf X teweeg zou brengen en wat de VR hier vervolgens mee kan."
- "Juiste ontsluiting met het netwerk."
- "Eerlijkheidsgebied zou ik het niet weten. De focus moet wel liggen op de potentiële maatschappelijke impact, en niet zozeer op digitale verstoringen an sich."
- "Risicoanalyses, snel opbouwen van ad hoc samenwerkingsverbanden."
- "Mogelijk nieuwe ontwikkelingen op het gebied van cyber te integreren."
- "Wij zijn nu met twee collega's bezig vanuit de afdeling CB op het gebied van Cybergevolgbestrijding. Je ziet dat het ontzettend moeilijk is om de kwetsbaarheden in kaart te kunnen brengen. Je weet grofweg niet waar je moet beginnen. Daar staat wel tegenover dat wij een concept Multidisciplinaire Informatiekaart Digitale Ontwrichting & Cybergevolgbestrijding hebben ontwikkeld die een beeldvormend karakter kent voor het ROT. Deze beschrijft voornamelijk het netwerk en geeft duiding op het thema."
- "Cyber kennis"

Vaardigheden bij de gevolgbestrijding:

- De vaardigheden voor het inschatten van de mogelijke oorzaak tijdens een extern cyberincident is volgens de respondenten niet aanwezig binnen de veiligheidsregio's. Zo is 71% van de respondenten het enigszins of helemaal oneens met de stelling, waarmee ze aangeven dat deze vaardigheden niet binnen veiligheidsregio's aanwezig zijn. Daarnaast geven alle respondenten, op één na, aan dat deze vaardigheden idealiter buiten de organisatie worden belegd. 29% van de respondenten zou de vaardigeden (daarnaast/ook) intern beleggen.
- De vaardigheden voor het inschatten van de duur van de verstoring tijdens een extern cyberincident is volgens de respondenten ook niet aanwezig binnen de veiligheidsregio's. Ook hier geeft 71% van de respondenten aan, het enigszins of helemaal oneens te zijn met de stelling, waarmee ze aangeven dat deze vaardigheden niet binnen veiligheidsregio's aanwezig zijn. Daarnaast geven alle respondenten, op één na, de voorkeur voor het extern beleggen van de vaardigheden. 42% van de respondenten zou de vaardigheden (daarnaast/ook) intern beleggen.
- De vaardigheden voor het inschatten van de maatschappelijke impact tijdens een extern cyberincident is volgens een grote meerderheid van de respondenten wel aanwezig binnen veiligheidsregio's. Zo is 57% van de respondenten het met de stelling eens en is 36% van de respondenten het niet eens of oneens. Daarnaast geven alle respondenten aan dat deze vaardigheden in ieder geval binnen de organisatie moet worden belegd (100%), waarbij een groot deel ook aangaf dat deze vaardigheden daarnaast ook extern zou kunnen worden belegd (57%).
- De vaardigheden voor het bestrijden of verkleinen van de gevolgen van een extern cyberincident zijn volgens de respondenten ook aanwezig binnen de veiligheidsregio's. Zo is

14% het helemaal met de stelling eens, is 50% het met de stelling eens en is 36% het niet eens of oneens. Geen enkele respondent was het dus oneens met deze stelling. Ook hier geven alle respondenten aan dat deze vaardigheden in ieder geval binnen de organisatie moet worden belegd (100%), waarbij de helft aangaf dat deze vaardigheden daarnaast ook extern zou kunnen worden belegd (50%).

- De vaardigheden voor het adequaat communiceren richting het bestuur van de eigen organisatie is volgens de meerderheid van de respondenten binnen veiligheidsregio's aanwezig. 50% is het enigszins of helemaal eens met de stelling, 36% is het niet eens of oneens en de overige 14% is het enigszins oneens met de stelling. Ook hier geven alle respondenten aan dat deze vaardigheden in ieder geval binnen de organisatie moet worden belegd (100%), waarbij een enkeling aangaf dat deze vaardigheden daarnaast ook extern zou kunnen worden belegd.
- De stelling over de vaardigheden voor het adequaat extern communiceren, zorgt voor een bijna perfecte verdeling van de antwoorden. Het grootste deel van de respondenten (50%) zijn het niet eens of oneens met de telling. Daarnaast is 14% het helemaal met de stelling eens, is 14% het enigszins met de stelling eens, is 14% het enigszins met de stelling oneens en is 8% het helemaal oneens met de stelling. Wel geven alle respondenten aan dat deze vaardigheden in ieder geval binnen de organisatie moet worden belegd (100%), waarbij een groot deel aangeeft dat deze vaardigheden daarnaast ook extern zou kunnen worden belegd (64%).

Binnen mijn organisatie hebben we bij een extern cyberincident voldoende vaardigheden om…	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens	Intern	Extern
…de mogelijke oorzaak (technische storing, menselijke fout of doelbewuste aanval) in te schatten.	0	1	3	3	7	4	13

…de duur van de verstoring in te schatten.	0	0	4	4	6	6	13
…de impact op maatschappelijke processen in te schatten (denk aan vitale infrastructuur zoals elektriciteit, internet, drinkwater of betalingsverkeer).	0	8	5	1	0	14	8
…de gevolgen/ effecten van het incident te bestrijden of verkleinen.	2	7	5	0	0	14	7
…adequaat richting het bestuur van de eigen organisatie te communiceren over het cyberincident.	2	5	5	2	0	14	2
…adequaat extern te communiceren over het cyberincident.	2	2	7	2	1	14	9

Toelichtingen over welke vaardigheden (nog meer) nodig zijn bij de gevolgbestrijding:

- “Kunnen duiden van de situatie, alle partijen goed begrijpen (technisch, impact, maatschappelijk en bestuurlijk)”
- “Onze ICT afdeling heeft ontzettend veel kennis, ik durf vanuit crisisbeheersing niet de inschatting te maken hoe snel wij een de oorzaak en duur van een mogelijke aanval ingeschat hebben.”
- “Communicatie naar de samenleving zal ook verlopen via getroffen organisatie. Communicatie over hulpverlening en breder maatschappelijke impact via gemeenten/veiligheidsregio, dit is niet anders dan anders.”
- “Meer kennis over (ontwrichting van) de digitale samenleving; welke relaties, keteneffecten etc.”
- “De betrokken partijen met elkaar te verbinden.”
- “Een goed landelijk netwerk ontbreekt nog. Het NCP is nu nog onvolledig. Wij hopen dat deze snel geüpdatet wordt en dat de positie van bijv. een VR-ISAC hierin ook wordt opgenomen.”

Het intern beleggen van de vaardigheden voor de gevolgbestrijding van externe cyberincidenten:

De meeste respondenten zouden de vaardigheden van de gevolgbestrijding van externe cyberincidenten idealiter binnen de organisatie bij medewerkers crisisbeheersing beleggen (52%). 19% van de respondenten heeft de voorkeur om de vaardigheden binnen de organisatie bij een CISO (Chief Information Security Officer) te beleggen en 11% zou het idealiter bij ICT medewerkers beleggen. De overige respondenten (18%) brachten zelf ideeën voor het beleggen van de vaardigheden binnen de organisatie:

- Communicatie, crisisorganisatie
- Landelijk expert team
- Partnerorganisaties
- Piketfunctionarissen
- Ook hier geldt weer PPS constructies. Wij hoeven niet alles zelf te doen, maar het inschakelen van private instelling is soms wel nog een taboe of heerst een taboe op. Ik zeg juist doen! Zeker wanneer jij de kennis of vaardigheden niet hebt.

Daarnaast werden een aantal antwoorden voorzien van een toelichting:

- “Digitale verstoringen met een maatschappelijk ontwrichtend karakter zijn per definitie regio overschrijdend.”
- “Niet anders dan wat we normaal doen.”
- “Gevolgbestrijding dan toch hoofdzakelijk bij CB, maar gebaseerd op kennis van externen/ICT experts over de mogelijke scenario's.”

Het extern beleggen van de vaardigheden voor de gevolgbestrijding van externe cyberincidenten:

Alle respondenten zouden de vaardigheden voor de gevolgbestrijding van externe cyberincidenten idealiter buiten de organisatie bij het Nationaal Cyber Security Center (19%) beleggen. Daarnaast zouden veel respondenten het bij Private kennis-/adviesbureaus zoals Fox-IT (15%), andere veiligheidsregio’s (15%) of landelijke voorziening Veiligheidsregio Information Sharing and Analysis Center (15%). Publieke kennisinstellingen zoals hogescholen en universiteiten (13%) en landelijke netwerken zoals werkgroep Digitale ontwrichting en cyber & vakgroep Informatieveiligheid (13%) zijn door de respondenten minder vaak gekozen. Het Instituut Fysieke Veiligheid is met 8% opvallend weinig genoemd. De overige respondenten (2%) brachten zelf aanvullende ideeën voor het beleggen van de vaardigheden buiten de organisatie:

- HTC Politie, IBD, DTC
- Politie (team cyber)

Ook werden een aantal antwoord voorzien van een toelichting:

- “Netwerken en vakgroepen leveren een bijdrage aan deze vaardigheden maar bezitten ze ons inziens niet. De organisaties waar ze voor werken wel.”

Middelen en gelegenheid:

- De technische middelen om voor te bereiden op externe cyberincidenten zijn volgens de respondenten niet voldoende aanwezig. Het grootste deel van de respondenten (43%) is het enigszins oneens met de stelling, 36% van de respondenten is het niet eens of oneens, 14% is het juist wel eens met de stelling en 7% is het helemaal niet eens met de stelling.
- De hulpmiddelen om voor te bereiden op externe cyberincidenten zijn volgens de respondenten ook niet voldoende aanwezig. Zo is 50% het enigszins oneens met de stelling en is 14% het helemaal niet eens met de stelling. De overige respondenten (36%) zijn het niet eens en niet oneens met de stelling.
- De hoeveelheid personeel dat is toegerust om zich voor te bereiden op externe cyberincidenten is volgens de respondenten ook niet voldoende aanwezig. Zo is 79% van de respondenten het enigszins of helemaal niet eens met de stelling. Daarnaast is 14% het niet eens of oneens en is 7% het juist wel eens met de stelling.
- Ook de hoeveelheid beschikbare tijd is volgens de respondenten niet voldoende. Zo is 43% het oneens met de stelling en is zelfs 36% het helemaal oneens met de stelling. De overige respondenten (21%) zijn het niet eens of oneens.
- Ook de hoeveelheid beschikbare financiële middelen is volgens de respondenten niet voldoende voor de voorbereiding op externe cyberincidenten. Zo is 86% van de respondenten het enigszins of helemaal oneens met de stelling. De overige respondenten (14%) zijn het niet eens of oneens.

Onze organisatie…	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens
…bezit voldoende technische middelen (zoals systemen) om zich voor te bereiden op externe cyberincidenten.	2	X	5	6	1
…bezit voldoende hulpmiddelen (zoals handreikingen, methodieken en protocollen) om zich voor te bereiden op externe cyberincidenten.	0	X	5	7	2
…bezit voldoende personeel, toegerust om zich voor te bereiden op externe cyberincidenten.	1	X	2	10	1
…reserveert voldoende tijd om zich voor te bereiden op externe cyberincidenten.	0	X	3	6	5
…reserveert voldoende financiële middelen om zich voor te bereiden op externe cyberincidenten.	0	X	2	10	2

Toelichtingen:

- “Crisisvaardigheden van een regio komen ook van pas bij bestrijding digitale verstoringen. ICT kennis zit extern, maar besluiten onder tijdsdruk en met weinig informatie wel. Belangrijk is ook om het eigen ICT en continuïteit van de regio op orde te hebben anders wordt het wel een heel lastig verhaal.”
- “We beginnen wakker te worden.”
- “Technische middelen zijn er voldoende, het gaat vooral om het kennisniveau van de crisisfunctionarissen. En wellicht een specifieke rol/functie (cyber), overigens kan dit naar mijn inziens een landelijke pool zijn. Maar hier wil ik nog wel eens verder over discussiëren (Puck de Ruijter, VRU).”
- “Dat blijft altijd een afweging. Ieder risico is belangrijk. Cyber is voor mij persoonlijk wel erg belangrijk.”
- “Ik mis hier een keuzemogelijkheid: Enigszins mee eens. Mijn antwoorden die ik heb opgegeven onder noch eens/noch oneens vallen in deze categorie.”

Netwerken en samenwerking:

- Over het zicht van veiligheidsregio’s op interne deskundigen voor de gevolgbestrijding van een extern cyberincident heerst verdeeldheid onder de respondenten. 43% van de respondenten is het enigszins met de stelling een, wat inhoudt dat veiligheidsregio’s zicht hebben op de interne deskundigen. 36% van de respondenten is het daarentegen enigszins oneens met de stelling, wat inhoudt dat veiligheidsregio’s geen zicht hebben op de interne deskundigen. De overige respondenten (21%) zijn het niet eens of oneens.
- Over de vraag of veiligheidsregio’s de partijen kennen die kunnen helpen in de voorbereiding van de gevolgbestrijding heerst minder verdeeldheid. Met 71% die het helemaal of enigszins eens is met de stelling, blijkt dat veiligheidsregio’s de partijen kennen die kunnen helpen bij de voorbereiding. De overige respondenten (21%) zijn het niet eens of oneens of zijn het enigszins oneens met de stelling.
- Over de vraag of veiligheidsregio’s de partijen kennen die kunnen helpen bij de gevolgbestrijding heerst meer verdeeldheid. Het grootste deel van de respondenten (36%) is het niet eens of oneens met de stelling. 43% van de respondenten is het helemaal of enigszins eens met de stelling. 21% van de respondenten is het daarentegen enigszins oneens met de stelling.
- Het inzetten van externe expertise voor de voorbereiding op de cybergevolgbestrijding kan volgens 43% van de respondenten door de veiligheidsregio’s worden gedaan, aangezien zij het helemaal of enigszins eens zijn met de stelling. 50% geeft aan het niet eens of oneens te zijn met de stelling en 7% geeft aan het helemaal niet eens te zijn met de stelling.
- Het inzetten van externe expertise voor de cybergevolgbestrijding kan volgens 57% van de respondenten door de veiligheidsregio’s worden gedaan, aangezien zij het helemaal of enigszins eens zijn met de stelling. Daarnaast is 29% het niet eens of oneens en is 14% het helemaal niet eens met de stelling.
- Over de mate waarin veiligheidsregio’s weten waar ze verantwoordelijk voor zijn bij de gevolgbestrijding van externe cyberincidenten heerst verdeeldheid. 50% van de respondenten is van mening dat zijn veiligheidsregio weet wat zijn verantwoordelijkheden zijn, aangezien zij het helemaal of enigszins eens zijn met de stelling. 14% van de respondenten is het niet eens of oneens en 36% is het enigszins oneens met de stelling.

- Ook ever de mate waarin veiligheidsregio's weten waar anderen verantwoordelijk voor zijn bij de gevolgbestrijding van externe cyberincidenten heerst verdeeldheid. 36% van de respondenten is het enigszins met de stelling eens, 36% van de respondenten is het niet eens of oneens met de stelling en 28% van de respondenten is het enigszins oneens met de stelling.
- De mate waarin veiligheidsregio's in staat zijn om tijdens de gevolgbestrijding van een extern cyberincident samen te werken met de andere betrokken teams is volgens de respondenten wel groot. Zo is 64% het helemaal of enigszins eens met de stelling. Daarnaast is 29% het niet eens of oneens en is 7% het enigszins oneens met de stelling.

Binnen mijn organisatie…	Helemaal mee eens	Enigszins mee eens	Noch eens noch oneens	Enigszins mee oneens	Helemaal niet mee eens
… hebben wij zicht op interne deskundigen voor de gevolgbestrijding van een extern cyberincident.	0	6	3	5	0
…kennen wij overheidsorganisaties en private partijen, die ons kunnen helpen bij de **voorbereiding** op de gevolgbestrijding van externe cyberincidenten.	2	8	2	2	0
…kennen wij overheidsorganisaties en private partijen, die ons kunnen helpen bij de **gevolgbestrijding** van externe cyberincidenten.	2	4	5	3	0
…zijn wij in staat om externe expertise in te zetten voor de **voorbereiding** op externe cyberrisico's (denk aan o.a. het NCSC/ private IT-dienstverleners).	2	4	7	0	1

… zijn wij in staat om externe expertise in te zetten voor de **gevolgbestrijding** van externe incidenten (denk aan o.a. het NCSC/ private IT-dienstverleners).	2	6	4	0	2
…weten wij waar we verantwoordelijk voor zijn bij de gevolgbestrijding van externe cyberincidenten.	2	5	2	5	0
…weten wij welke verantwoordelijkheden de andere betrokken teams hebben bij de gevolgbestrijding van externe cyberincidenten.	0	5	5	4	0
…zijn wij in staat om tijdens de gevolgbestrijding van een extern cyberincident samen te werken met de andere betrokken teams.	4	5	4	1	0

Toelichtingen:

- “Met name het contact tussen regio en rijk wordt wel een lastig punt. Hoe weten die twee elkaar te vinden tijdens digitale verstoring?”
- “We hebben tot op heden vooral informatie verzameld en het netwerk proberen te versterken, maar nog niet voldoende om te kunnen zeggen dat wij ons goed voorbereid hebben. We hebben nog geen planvorming voor cyber, staat wel op korte termijn op de planning.”
- “De partijen die betrokken zijn bij de gevolgbestrijding zijn de bekende organisaties in de crisisorganisatie, echter zijn de getroffen organisaties ook betrokken. De regionale crisisorganisatie is niet bekend met alle organisaties in haar verzorgingsgebied, en dit hoeft naar mijn weten ook niet.”
- “Het inschakelen van bepaalde expertise zal in de praktijk vaak buiten de veiligheidsregio om gebeuren, maar eerder vanuit de verantwoordelijkheid van de getroffen organisatie zelf (en eigen afspraken).”
- “Het moet een keer gebeuren en dan weet je hoe je ervoor staat. Ik denk dat wij al een heel eind zijn, maar nog niet volledig. In april/mei hebben wij een netwerkdag met onze partners om dieper in dit onderwerp te duiken met ons netwerk. Ik geloof aan de ander kant wel dat onze operationele functionarissen in staat zijn om kennis/vaardigheden die zij niet hebben ten tijde van een crisis op een andere plaats te gaan zoeken.”

Interventies en verbeteringen:

- De respondenten zijn verdeeld als wordt gekeken naar de belangrijkste factoren waarop veiligheidsregio's zich moeten richten om de voorbereiding op externe cyberincidenten te versterken. Met een gemiddelde van 2.14 is netwerken en samenwerking volgens de respondenten de belangrijkste factor. Daarna volgen motivatie/urgentiebesef (gem. 3.00) en kennis (gem. 3.71). Middelen, tijd en kunde/vaardigheden zijn iets minder vaak gekozen met respectievelijk gemiddelden van 4.29, 4.50 en 4.71. Geld staat onderaan met een gemiddelde van 6.14 en 'overige' met een gemiddelde van 7.50. Hierbij zijn twee extra factoren genoemd: "Kennisniveau is het belangrijkste. de rol van de regionale crisisorganisatie staat vast (zie NCP D)." & "Ik denk dat er een natuurlijke volgorde zit in al deze factoren.".

	1	2	3	4	5	6	7	8
Motivatie/urgentiebesef	6	1	0	4	1	1	1	0
Kennis	3	1	1	5	1	2	1	0
Kunde/vaardigheden	0	0	3	1	8	1	1	0
Middelen (mensen, systemen, handreikingen etc.)	0	3	3	2	2	1	3	0
Netwerken en samenwerking	3	6	5	0	0	0	0	0
Tijd	1	2	2	1	1	6	1	0
Geld	0	1	0	1	1	3	7	1
Overig	1	0	0	0	0	0	0	13

	Gemiddelde	Standaardafwijking
Motivatie/urgentiebesef	3.00	2.04
Kennis	3.71	1.87
Kunde/vaardigheden	4.71	1.10
Middelen (mensen, systemen, handreikingen etc.)	4.29	1.83
Netwerken en samenwerking	2.14	0.74
Tijd	4.50	1.88
Geld	6.14	1.51
Overig	7.50	1.80

Overige behoeften voor een verbetering van de voorbereiding op de gevolgbestrijding:

- "Primair gaat het om het kennisniveau van de regionale crisisorganisatie, en de rolvastheid die geboden is. De wettelijke taak is namelijk niet veranderd. Daarnaast ben ik een groot voorstander om een landelijke pool op te richten met crisisfunctionarissen uit het land die alle processen rondom cybergevolgbestrijding goed kennen. Zo hoeft niet elke veiligheidsregio een eigen pool op te richten, wat niet realistisch en niet noodzakelijk is."
- "Meer samenwerking in operationele voorbereiding. Landelijk de toon zetten met aantal trekkers en belangrijke stakeholders, dit regionaal uitzetten en verrijken."

- “Naar mate onze rol in dit thema meer en meer duidelijk wordt, zou het fijn zijn om beginnende crisisfunctionarissen (of men die onbekend is op dit thema) meer te leren over dit thema. Bijvoorbeeld als een hoofdstuk in een handboek of een presentatie.”
- “Planvorming. Overzicht van private dienstverleners en hun expertise.”
- “Ik ben erg nieuwsgierig naar het nieuwe NCP. Deze hebben wij nu als onderliggend document gebruikt voor het eerste concept van de MIK digitale ontwrichting en cybergevolgbestrijding. Ik hoop dat het NCP gaat voorzien in een duidelijk netwerk met taken/verantwoordelijkheden voor een VR. Ik denk dat dat het allerbelangrijkste is. Met een goed netwerk weet ik zeker dat wij een cyberincident (extern) kunnen bestrijden. Een bepaalde vorm van basis kennis/vaardigheden en operationele voorbereiding/training is ook vereist.”

Bijlage 10 Overzicht barrières cyberweerbaarheid en cybergevolgbestrijding

Barrières	Cyberweerbaarheid	Cybergevolgbestrijding
Motivatie	De mate waarin de voorbereiding op interne cyberincidenten prioriteit krijgt binnen de veiligheidsregio's is beperkt.	De mate waarin de voorbereiding op externe cyberincidenten prioriteit krijgt binnen de veiligheidsregio's is beperkt.
Kennis	Onvoldoende/beperkt kennis voor: • Het in beeld brengen van de keteneffecten (verbondenheid van het geraakte systeem met andere systemen). • Het inschatten van de mogelijke oorzaak (technische storing, menselijke fout of doelbewuste aanval). • Het inventariseren van de schade op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie (zoals verlies van vertrouwelijke gegevens).	Onvoldoende/beperkt kennis voor: • Het in beeld brengen van de noodzakelijke en relevante dreigingen bij niet-vitale organisaties binnen de regio. • Het inschatten van mogelijke cascade-effecten van een cyberincident in de regio.
Vaardigheden	Onvoldoende/beperkte vaardigheden voor: • Het opstellen van scenario's voor cyberoefeningen. • Het inschatten van de mogelijke oorzaak (technische storing, menselijke fout of doelbewuste aanval). • Het vormen van een (technisch)oplossingsperspectief. • Het in beeld brengen van de keteneffecten (verbondenheid van het geraakte systeem met andere systemen). • Het inventariseren van de schade op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie (zoals verlies van vertrouwelijke gegevens). • Het bestrijden of verkleinen van de gevolgen/effecten.	Onvoldoende/beperkte vaardigheden voor: • Het vooraf inventariseren van mogelijke maatschappelijke effecten van een extern cyberincident.
Samenwerking	-	Onvoldoende/beperkt zicht op interne deskundigen voor de gevolgbestrijding. Onvoldoende/beperkt zicht op eigen verantwoordelijkheden bij de gevolgbestrijding van externe cyberincidenten Onvoldoende/beperkt zicht op verantwoordelijkheden van andere betrokken teams bij de gevolgbestrijding van externe cyberincidenten.

		Onvoldoende/beperkt inschakelen van externe expertise op zowel regionaal als nationaal niveau.
Middelen	Onvoldoende/beperkt technische middelen (zoals systemen) om voor te bereiden op interne cyberincidenten. Onvoldoende/beperkt hulpmiddelen (zoals handreikingen, methodieken en protocollen) om voor te bereiden op interne cyberincidenten. Onvoldoende/beperkt personeel, dat is toegerust om voor te bereiden op interne cyberincidenten.	Onvoldoende/beperkt technische middelen (zoals systemen) om voor te bereiden op externe cyberincidenten. Onvoldoende/beperkt hulpmiddelen (zoals handreikingen, methodieken en protocollen) om voor te bereiden op externe cyberincidenten. Onvoldoende/beperkt personeel, dat is toegerust om voor te bereiden op externe cyberincidenten.
Tijd	Onvoldoende/beperkt tijd voor de voorbereiding op interne cyberincidenten	Onvoldoende/beperkt tijd voor de voorbereiding op externe cyberincidenten.
Geld	Onvoldoende/beperkt financiële middelen voor de voorbereiding op interne cyberincidenten	Onvoldoende/beperkt financiële middelen voor de voorbereiding op externe cyberincidenten.