Instituut
Fysieke
Veiligheid

Cyberrisico's en veiligheidsregio's

Hoe beoordelen veiligheidsregio's cyberrisico's?

Instituut Fysieke Veiligheid
Kennisontwikkeling en onderwijs
Postbus 7010
6801 HA Arnhem
Kemperbergerweg 783, Arnhem
www.ifv.nl
info@ifv.nl
026 355 24 00

Colofon

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

Opdrachtgever:	Raad Directeuren Veiligheidsregio (RDVR)
Contactpersoon:	Steven van de Looij, portefeuillehouder Digitale Ontwrichting en Cyber
Titel:	Cyberrisico's en veiligheidsregio's. Hoe beoordelen veiligheidsregio's cyberrisico's?
Datum:	28 februari 2020
Status:	Definitief
Versie:	1.0
Auteurs:	Jana Domrose MSc en Laurens van der Varst MSc
Projectleider:	Laurens van der Varst MSc
Review:	dr. Menno van Duin
Eindverantwoordelijk:	dr. Menno van Duin

Abstract

The research group Crisis Management of the Dutch Institute for Safety (IFV) has studied the mechanisms safety regions use assess cyber risks and how regions prepare themselves for this specific type of risks. The goal of this study is to find out whether the existing documents and methods concerning this matter are sufficient.
Based on desk research, an online questionnaire and an expert meeting, the following questions have been answered:

1. What can be found about cyber risks in the regional risk profiles and how are these risks assessed by safety regions?
2. How do safety regions make their risk assessment regarding cyber risks?
    a. Which partners and expertise do they use?
    b. How useful are existing methods for assessing cyber risks?
3. To what extent do safety regions think they are cyber vigilant and prepared for cyber crisis management?
    a. What are existing best practices and perspectives for action?
    b. What is needed?
4. How can safety regions strengthen their cyber vigilance and cyber crisis management?

This study has shown that safety regions use the Handreiking Regionaal Risicoprofiel, the Cybersecuritybeeld Nederland (considered most important) and the Nationaal Veiligheidsprofiel. Safety regions find it difficult to translate national cyber risks to regional risks. Besides, in the process of assessing cyber risks, regions do not make use of the knowledge and expertise of relevant stakeholders. They vary in their assessments considering the likelihood and impact of cyber risks. They assess their own preparations as (just) sufficient, and have taken various measures, although many safety regions are uncertain what steps to take.

In order to better anticipate cyber risks, safety regions want to make a risk assessment together with relevant stakeholders and be able to better translate national cyber risks to their own region. Furthermore, regions need to create clarity about the responsibilities and competencies of the stakeholders involved, develop (or create more clarity regarding) procedures concerning escalation and decision making and enlarge their own cyber crisis management capability by practicing cyber scenario’s and enriching their own knowledge position regarding cyber risks.

Concerning cyber vigilance, this study proposes to develop a method to systematically assess cyber risks, and to better involve and make use of the regional network of people and organisations. Concerning cyber crisis management, this study proposes the following measures: 1. Use a set of fixed questions in discussions with regional partners. 2. Use basic scenario’s for planning and practicing and come to agreements with partners concerning escalation and coordination during cyber crises or crises with a cyber component. 3. As safety region, take part in and organise regional cyber exercises and facilitate a network that collects the experiences with these exercises and make them available to safety regions.

Samenvatting

Het lectoraat Crisisbeheersing van het IFV heeft in opdracht van de RDVR-portefeuillehouder Digitale Ontwrichting en Cyber de wijze onderzocht waarop veiligheidsregio's cyberrisico's inventariseren en beoordelen en hoe veiligheidsregio's zich op cyberrisico's voorbereiden. Het doel is om in kaart te brengen of bestaande handreikingen en methodieken voldoende aanknopingspunten bieden voor zowel de inventarisatie en beoordeling van, als de voorbereiding op, cyberrisico's, en om – waar nodig – aanvullende handvatten te ontwikkelen. Hiervoor zijn de volgende onderzoeksvragen geformuleerd, die beantwoord zijn met behulp van deskresearch, een online enquête en een dialoogsessie:

1. Wat staat er momenteel in de regionale risicoprofielen over cyberrisico's en hoe worden deze risico's door veiligheidsregio's beoordeeld?
2. Hoe komen veiligheidsregio's tot hun cyberrisicobeoordeling?
    a. Welke partners en expertise benutten ze?
    b. Welke meerwaarde hebben bestaande methodieken bij het beoordelen van cyberrisico's?
3. In hoeverre denken veiligheidsregio's cyberwaakzaam te zijn en voorbereid op cybergevolgbestrijding?
    a. Wat zijn de 'best practices' en concrete handvatten?
    b. Welke behoeften zijn er?
4. Hoe kunnen veiligheidsregio's hun cyberwaakzaamheid en cybergevolgbestrijding verder versterken?

Het is gebleken dat voor het inventariseren en beoordelen van cyberrisico's de veiligheidsregio's de Handreiking Regionaal Risicoprofiel, het Cybersecuritybeeld Nederland en het Nationaal Veiligheidsprofiel gebruiken. Het Cybersecuritybeeld wordt door bijna alle gebruikers als belangrijke informatiebron voor cyberrisico's beschouwd. Veiligheidsregio's hebben moeite om landelijke risico's te vertalen naar regionale risico's. Bij de inventarisatie van cyberrisico's werkt minder dan de helft van de veiligheidsregio's samen met partners. Uit de analyse van de regionale risicoprofielen van de veiligheidsregio's blijkt dat de beoordelingen van waarschijnlijkheid en impact uiteenlopen.

Veiligheidsregio's beoordelen hun eigen preparatie op cyberwaakzaamheid en cybergevolgbestrijding met respectievelijk een 5 en 6. Zij ondernemen diverse activiteiten om zich voor te bereiden, zoals het opbouwen en onderhouden van regionale/landelijke netwerken, het opbouwen van cyberkennis en -expertise en het oefenen met cyberscenario's. Voor veel veiligheidsregio's is het nog zoeken hoe zich adequaat te prepareren op digitale verstoringen.

Om goed te kunnen anticiperen op cyberrisico's willen veiligheidsregio's: cyberrisico's in de omgeving in beeld brengen samen met partners; ontwikkelingen van het Cybersecuritybeeld Nederland vertalen naar de eigen regio; duidelijkheid krijgen over de rollen, taken en bevoegdheden van alle betrokken actoren (landelijk, regionaal, lokaal), inclusief hun eigen

rol en de benodigde expertise; procedures rond alarmering, opschaling en besluitvorming; de eigen expertise van cyberbronbestrijding en cybergevolgbestrijding vergroten; cyberscenario's uitwerken en (samen met partners) oefenen en een landelijk aanspreekpunt inrichten voor cyberrisico's en bij cyberincidenten.

In dit onderzoek worden de volgende aanbevelingen op het gebied van cyberwaakzaamheid gedaan: 1. Ontwikkel een methodiek om cyberrisico's systematisch te inventariseren en beoordelen. 2. Betrek bij de risicobeoordeling een regionaal netwerk van belanghebbenden en ga daarmee een dialoog aan over cyberrisico's. Aanbevelingen op het gebied van cybergevolgbestrijding zijn: 1. Gebruik vaste vragen in gesprekken met regionale partners. 2. Gebruik naar analogie van terrorismegevolgbestrijding basisscenario's voor planvorming en oefenen. Maak met de partners afspraken over alarmering, opschaling en onderlinge coördinatie bij digitale verstoringen. 3. Neem als veiligheidsregio deel aan en organiseer (boven-)regionale cyberoefeningen. Faciliteer als werkgroep Digitale ontwrichting en cyber een 'netwerk observatoren cyberoefeningen' dat opgedane ervaringen bundelt en beschikbaar stelt aan de veiligheidsregio's.

Inhoud

Inleiding

Aanleiding

Algemeen wordt aangenomen dat de samenleving te maken krijgt met nieuwe risico's onder invloed van ontwikkelingen op het gebied van technologie, demografie en klimaat (OECD, 2003). Hoewel risico's per definitie met onzekerheid zijn omgeven, is de onzekerheid rond nieuwe risico's nog groter, onder andere door het ontbreken van risicogegevens en door de veelheid aan factoren die van invloed zijn op het risico (OECD, 2003). In crisisliteratuur wordt voorspeld dat de nieuwe risico- en crisistypen duidelijk afwijken van de meer reguliere of routinematige crises, zoals branden en kleinere overstromingen (Comfort, Boin, & Demchak, 2010). Die nieuwe of ongekende crises zijn moeilijk kenbaar, beperken zich niet tot één bepaalde sector en kunnen razendsnel escaleren (Boin, 2017). Tevens leiden nieuwe, technologische risico's tot meer angst en onzekerheid, zo weten we uit de risicopsychologie (Slovic & Weber, 2002).

Diverse instanties zoals de Wetenschappelijke Raad voor het Regeringsbeleid pleiten recent voor meer investeringen in digitale weerbaarheid (2019). Ook veiligheidsregio's krijgen of hebben al te maken met nieuwe crisistypen, waaronder digitale ontwrichting. Dit roept de vraag op hoe de veiligheidsregio's zich hierop voorbereiden. Dat was voor de Raad van Directeuren Veiligheidsregio (RDVR) aanleiding voor het organiseren van een platform voor kennisdeling en het verder verkennen van de uitdagingen van digitale ontwrichting voor veiligheidsregio's. Dit heeft geresulteerd in het *Whitepaper digitale ontwrichting en cyber* (IFV, 2019). Hieruit blijkt dat veel digitale risico's in de omgeving 'verborgen' zitten: de omvang, aard en ernst van de cyberrisico's zijn niet duidelijk in beeld. Het in beeld brengen van die risico's, bijvoorbeeld in een 'cyber-omgevingsanalyse', is één van de genoemde uitdagingen. Daarnaast laten actuele ontwikkelingen zien dat hackers steeds meer actief op zoek zijn naar kwetsbare organisaties, bijvoorbeeld om systemen te gijzelen en losgeld te vragen. Omdat de soort organisatie hierbij vaak een ondergeschikte rol speelt, kunnen ook overheidsorganisaties mogelijke doelwitten zijn van cyberaanvallen.[1]

Opdracht

Naar aanleiding van deze eerste bevindingen heeft de RVDR-portefeuillehouder Digitale Ontwrichting en Cyber het lectoraat Crisisbeheersing gevraagd onderzoek te doen naar de wijze waarop veiligheidsregio's cyberrisico's momenteel inventariseren en beoordelen. Doelstelling is om in kaart te brengen of bestaande handreikingen en methodieken voldoende aanknopingspunten bieden voor zowel de inventarisatie en beoordeling van, als de voorbereiding op cyberrisico's, en om – waar nodig – aanvullende handvatten te ontwikkelen.

[1] NOS, 15 januari 2020. Nieuwsuur: Hack(poging) in ziekenhuis en gemeente: 'Urgentie lek leek niet duidelijk'. Op 24 januari 2020 ontleend aan https://nos.nl/nieuwsuur/artikel/2318812-hack-poging-in-ziekenhuis-en-gemeente-urgentie-lek-leek-niet-duidelijk.html.

Aanpak

Om in beeld te kunnen brengen of de bestaande instrumenten en informatiebronnen voldoende aanknopingspunten bieden voor de identificatie en beoordeling van, en de voorbereiding op cyberrisico's, zijn de volgende onderzoeksvragen geformuleerd:

1. Wat staat er momenteel in de regionale risicoprofielen over cyberrisico's en hoe worden deze risico's door veiligheidsregio's beoordeeld?
2. Hoe komen veiligheidsregio's tot hun cyberrisicobeoordeling?
    a. Welke partners en expertise benutten ze?
    b. Welke meerwaarde hebben bestaande methodieken bij het beoordelen van cyberrisico's?
3. In hoeverre denken veiligheidsregio's cyberwaakzaam te zijn en voorbereid op cybergevolgbestrijding?
    a. Wat zijn de 'best practices' en concrete handvatten?
    b. Welke behoeften zijn er?
4. Hoe kunnen veiligheidsregio's hun cyberwaakzaamheid en cybergevolgbestrijding verder versterken?

Om de onderzoekvragen te beantwoorden zijn drie methoden toegepast: het doen van deskresearch, het uitzetten van een online enquête en het houden van een dialoogsessie. Deze methoden worden hieronder nader toegelicht.

> Deskresearch:

In een eerste stap zijn 24 risicoprofielen[2] gescand op paragrafen over cyberrisico's. Hierbij is van ieder risicoprofiel de versie geraadpleegd die in september 2019 openbaar toegankelijk was, bijvoorbeeld via de website van de veiligheidsregio. Omdat niet alle veiligheidsregio's de term 'cyber' expliciet benoemen in hun risicoprofiel, zijn in het merendeel van de risicoprofielen paragrafen over uitval van ICT en telecommunicatie geanalyseerd. Hierbij is gekeken naar de inschaling van de kans op en impact van het risico, evenals naar de geïdentificeerde oorzaken en gevolgen. Daarnaast is uitgezocht of cyberrisico's als specifiek aandachtsgebied worden benoemd in de managementsamenvatting, inleiding of conclusie van het risicoprofiel. De bevindingen zijn gebundeld in een tabel (zie bijlage 1) en tevens samengevat in hoofdstuk 1 van dit rapport.

> Enquête:

Om in kaart te brengen hoe cyberrisico's in veiligheidsregio's worden gemonitord en beoordeeld, en in welke mate regio's denken voorbereid te zijn op cyberrisico's, is een digitale enquête uitgezet onder de Hoofden Veiligheidsbureau van alle 25 veiligheidsregio's (de enquête is beschikbaar op de IFV-website). De uitvraag liep van 14 oktober tot 8 november 2019 en werd op 18 september aangekondigd in de landelijke werkgroep 'Digitale ontwrichting en cyber'.

Na afstemming met de werkgroep is ervoor gekozen om in de enquête de volgende vijf thema's centraal te laten staan:

1. Organisatorische aandacht voor cybervraagstukken.
2. Mate van cyberwaakzaamheid in de veiligheidsregio's.

[2] Nb: Veiligheidsregio's Limburg-Noord en Zuid-Limburg hebben een gezamenlijk Provinciaal Risicoprofiel, waarnaar in dit rapport wordt verwezen.

3. Mate van voorbereiding op cybergevolgbestrijding in de veiligheidsregio's.
4. Gebruik van methodieken en informatiebronnen ter beoordeling van cyberrisico's.
5. Activiteiten ter voorbereiding op cyberrisico's.

In totaal hebben 21 veiligheidsregio's de enquête ingevuld. Na afloop van de deadline zijn de data van alle veiligheidsregio's samengevoegd en zijn er descriptieve analyses uitgevoerd om landelijke totalen en percentages in kaart te brengen.

> Expertsessie:

De bijeenkomst van de werkgroep Digitale ontwrichting en cyber op 27 november 2019 diende als dialoogsessie voor de vraag in hoeverre cyberrisico's geïdentificeerd en beoordeeld kunnen worden met behulp van bestaande hulpmiddelen, en welke best practices regio's op het gebied van risico-inventarisatie met elkaar kunnen delen. Daarnaast zijn concrete behoeften opgehaald voor het kunnen versterken van de cyberwaakzaamheid en (voorbereiding op) cybergevolgbestrijding. In totaal hebben circa 20 functionarissen van veiligheidsregio's deelgenomen aan de sessie, onder wie adviseurs risico- en crisisbeheersing. Daarnaast namen een adviseur van het LOCC (als vast lid van de werkgroep), TNO en de secretaris van het Analistennetwerk Nationale Veiligheid deel aan de discussie.

Leeswijzer

In hoofdstuk 1 worden de centrale begrippen toegelicht die in dit onderzoek aan de orde komen, evenals de bestaande methodieken voor risicobeoordeling. Hoofdstuk 2 bevat de bevindingen uit de 'quick-scan' van regionale risicoprofielen, en in hoofdstuk 3 staan de resultaten uit de enquête centraal. Hoofdstuk 4 bevat de bevindingen en in hoofdstuk 5 staan enkele aanbevelingen voor de veiligheidsregio's voor de voorbereiding op cyberwaakzaamheid en -gevolgbestrijding.

1 Achtergrond

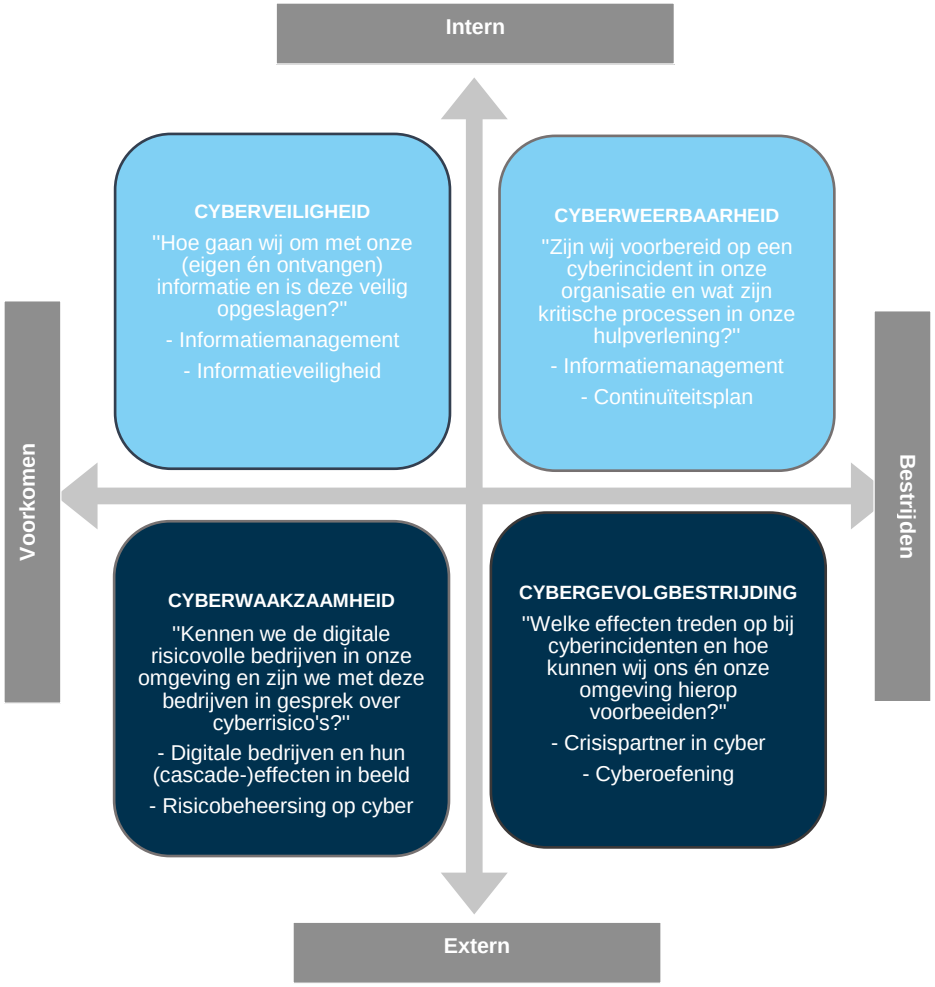
In dit hoofdstuk wordt aandacht besteed aan de centrale begrippen uit het onderzoek en worden de door de veiligheidsregio's gebruikte methoden voor risicobeoordeling toegelicht.

1.1 Centrale begrippen

In dit onderzoek is aangesloten bij de begrippen zoals gehanteerd in het *Whitepaper digitale ontwrichting en cyber*. Hierin wordt een cyberrisico gedefinieerd als: "Een risico waarvan de oorzaak en/of het gevolg in het digitale domein liggen en dat impact heeft op de samenleving, de (fysieke) veiligheid en/of openbare orde in een veiligheidsregio (IFV, 2019, p. 5)." Hierbij kan er sprake zijn van moedwilligheid of toeval en menselijke of technische fouten. Ook worden in het whitepaper vier componenten binnen het domein van 'cyber' onderscheiden, namelijk:

1. cyberveiligheid
2. cyberweerbaarheid
3. cyberwaakzaamheid
4. cybergevolgbestrijding.

De vier aandachtspunten zijn nader toegelicht in figuur 1.1.



Figuur 1.1 Het cyberkwadrant zoals uitgewerkt door Veiligheidsregio IJsselland

De centrale focus in dit onderzoek ligt op de twee externe componenten van het kwadrant: cyberwaakzaamheid en cybergevolgbestrijding. Cyberwaakzaamheid wordt gedefinieerd als het kennen van risico's met een digitale component in de samenleving. Deze risico's kunnen betrekking hebben op kwetsbare ICT-knooppunten, diensten, objecten en bevolkingsgroepen. 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/liggen. De voorbereiding op cybergevolgbestrijding kan betrekking hebben op de afstemming met crisispartners in de koude fase, of op de organisatie van (multidisciplinaire) cyberoefeningen.

Daarnaast kunnen cyberrisico's uiteraard ook invloed hebben op het functioneren van veiligheidsregio's en hulpdiensten. De inventarisatie van en voorbereiding op interne cyberrisico's staan niet centraal in het huidige onderzoek, ook al zal er in veel gevallen sprake zijn van een raakvlak met externe risico's.

1.2 Inventariseren en beoordelen van risico's

In de op 1 oktober 2010 in werking getreden Wet veiligheidsregio's is vastgelegd dat de veiligheidsregio's moeten beschikken over een regionaal risicoprofiel dat samen met alle relevante partners is opgesteld (Ministerie van Veiligheid en Justitie, 2010). Het regionaal risicoprofiel is een inventarisatie en analyse van de aanwezige risicovolle situaties en de

soorten incidenten die zich daardoor kunnen voordoen, en wordt door veiligheidsregio's eens per vier jaar vastgesteld. Op basis van deze risicoanalyse maakt het bestuur van de veiligheidsregio strategische beleidskeuzes over de ambities voor de risico- en crisisbeheersing. Deze ambities worden vastgelegd in het beleidsplan van de veiligheidsregio's. Om veiligheidsregio's hierbij te ondersteunen, zijn de instrumenten en informatiebronnen beschikbaar die in de volgende paragrafen kort worden toegelicht.

1.2.1 Handreiking Regionaal Risicoprofiel

Voor het in beeld brengen en beoordelen van risico's beschikken veiligheidsregio's over de *Handreiking Regionaal Risicoprofiel* (HRR) uit 2009. Deze handreiking biedt een uniforme methodiek om een regionaal risicoprofiel op te stellen. De achterliggende gedachte is dat regionale profielen hierdoor onderling vergelijkbaar worden en profielen bovenregionaal op elkaar kunnen worden afgestemd. De handreiking bevat een uitwerking van verschillende crisis- en incidententypen, waaronder de verstoring van vitale infrastructuur en voorzieningen. Een scenario hierin is de verstoring van telecommunicatie en ICT door criminele activiteiten. Als belangrijkste algemene impactcriteria voor verstoring van telecommunicatie en ICT worden in de handreiking gezien:

1. Ernstig gewonden en chronisch zieken: de zorgsector (zoals thuiszorg) is voor zijn gezondheidshulp afhankelijk van telecommunicatie; alarmcentrales zijn niet meer bereikbaar.
2. Kosten: indirecte kosten. Veel bedrijven komen stil te liggen en lopen opdracht mis. Automatische bewaking en beveiliging vallen weg.
3. Verstoring van het dagelijks leven: de directe hulpvraag aan overheid wordt sterk beperkt; denk ook aan verkeersregeling. De aansturing van de hulpverlening is afhankelijk van C2000.
4. Aantasting van de positie van het lokale en regionale bestuur: de schuldvraag is complex vanwege meerdere partijen met een taak en verantwoordelijkheid.
5. Sociaalpsychologische impact: onrust

Risico's door 'moedwillig handelen', waaronder ook cybercriminaliteit, worden niet apart genoemd in de handreiking. Dergelijke handelingen worden als trigger beschouwd voor de uitval van ICT en telecommunicatie.

1.2.2 Nationale risicobeoordeling

Voor het beoordelen van de risico's voor de nationale veiligheid maakt het Analistennetwerk Nationale Veiligheid gebruik van de Leidraad Risicobeoordeling (2019b). Uitgangspunt zijn zes nationale veiligheidsbelangen, waaronder fysieke en economische veiligheid en sociale en politieke stabiliteit. De beoordeling van risico's vindt plaats op basis van de criteria impact en waarschijnlijkheid. De impact en waarschijnlijkheid worden 'gescoord' op klassen variërend van respectievelijk beperkt tot catastrofaal (voor impact) en zeer onwaarschijnlijk tot zeer waarschijnlijk (voor waarschijnlijkheid van optreden). De beoordeling vindt plaats binnen een netwerk van inhoudelijke kennisinstellingen. Daarbinnen worden scenario's eerst uitgewerkt en daarna in multidisciplinair verband besproken en beoordeeld.

Deze benadering resulteert in de geïntegreerde risicoanalyse (Analistennetwerk Nationale Veiligheid, 2019a). Dat rapport bevat een beschrijvende beschouwing en duiding van risico's én een beoordeling van scenario's op de genoemde veiligheidsbelangen.

Digitale sabotage (verstoring met ‘collateral damage’) en cyberspionage worden gezien als risico’s met een hoge mate van waarschijnlijkheid. De kans dat deze risico’s zich voordoen is zeer waarschijnlijk tot hoog.

Naast de genoemde scenario’s die binnen het thema cyberdreigingen zijn ontwikkeld, is in de uitwerking van de zes nationale veiligheidsbelangen een nieuw criterium opgenomen met betrekking tot ‘cyber’. Dit is het criterium ‘aantasting van de integriteit van de digitale ruimte’ (criterium 1.3.) De digitale ruimte is hierbij gedefinieerd als “het conglomeraat van ICT-middelen en -diensten en bevat alle entiteiten die digitaal verbonden (kunnen) zijn”. Het domein omvat zowel permanente als tijdelijke of plaatselijke verbindingen, evenals de gegevens (o.a. data, programmacode, informatie) die zich in dit domein bevinden, waarbij geen geografische beperkingen zijn gesteld.” (Analistennetwerk Nationale Veiligheid, 2019b, p. 14)

1.2.3 Cybersecuritybeeld Nederland

Het ‘Cybersecuritybeeld Nederland’ (CSBN) biedt inzicht in dreigingen, belangen en weerbaarheid op het gebied van cybersecurity in relatie tot de nationale veiligheid. Opvallende ontwikkelingen op het gebied van cybersecurity worden in een kwalitatieve vorm beschreven en kunnen door alle overheidsinstanties worden geraadpleegd. Zo wordt er in het CSBN 2019 gewezen op een toenemende digitale dreiging door statelijke actoren, die een hoge impact kan hebben op de nationale veiligheid (NCTV, 2019). Vrijwel alle vitale processen en systemen in Nederland zijn deels of volledig gedigitaliseerd, waarbij er nauwelijks terugvalopties of analoge alternatieven zijn, constateert de NCTV. De toenemende digitale dreiging en grote afhankelijkheid van het ongestoord functioneren van ICT-voorzieningen, maken Nederland kwetsbaar voor digitale aanvallen.

2 Cyber in regionale risicoprofielen

In dit hoofdstuk wordt toegelicht hoe cyber als onderwerp terugkomt in de regionale (en het provinciale) risicoprofielen. Hiertoe is een quick-scan van alle risicoprofielen uitgevoerd.

2.1 Hoe komen cyberrisico's terug in regionale risicoprofielen?

Uit de scan van alle risicoprofielen blijkt dat cyberrisico's veelal onder 'verstoring ICT en telecommunicatie' en 'uitval spraak- en datacommunicatie' worden opgevoerd en geanalyseerd. In vier risicoprofielen is de risiconaam vervangen door (of aangevuld met) de termen 'cyber', 'cyberincidenten', 'cyberverstoring' of 'digitale verstoring'.
Wederom vier veiligheidsregio's analyseren in hun risicoprofielen specifiek moedwillige 'cybercrime', 'cyberspionage' of 'aantasting van de cybersecurity' als risicotypen, waarvan drie apart naast het incidenttype 'uitval van ICT en telecommunicatie'. In vrijwel alle risicoprofielen wordt bewust menselijk handelen, zoals cybercrime, cyberterrorisme en vandalisme, als mogelijke oorzaak voor een uitval van spraak- en datacommunicatie genoemd.

Daarnaast zijn cybergerelateerde ontwikkelingen in 22 risicoprofielen als specifiek aandachtspunt benoemd in de managementsamenvatting, inleiding of conclusie. Veelal wordt hierbij gerefereerd aan de groeiende maatschappelijke afhankelijkheid en verwevenheid van digitale systemen en informatie.

Veiligheidsregio Brabant Zuidoost (2019, p. 120) identificeert in haar risicoprofiel de volgende vier maatschappelijke risico's op het gebied van cyber en ICT:

1. De afhankelijkheid van ICT is groot en neemt nog altijd toe. De potentiële impact van incidenten wordt daardoor groter.
2. Cybercriminelen hebben een kennisvoorsprong. Cybercrime is daarmee nog relatief ongrijpbaar.
3. ICT-gebruikers krijgen een grote verantwoordelijkheid toegedicht voor beveiliging, maar worden steeds vaker geconfronteerd met kwetsbaarheden in apparaten en diensten waar ze beperkte invloed op, of kennis van hebben.
4. Een brede groep organisaties heeft belangrijke (technische) basismaatregelen nog niet op orde, zoals het patchen en updaten van systemen of het wachtwoordbeleid.

Ook de afhankelijkheid en kwetsbaarheid van de veiligheidsregio zelf wordt in meerdere risicoprofielen als aandachtspunt benoemd. Om in te kunnen spelen op ontwikkelingen en nieuwe risico's benadrukken meerdere veiligheidsregio's de noodzaak van nieuwe samenwerkingsverbanden. Zo geeft Veiligheidsregio Twente aan:

“Bij cyber-gerelateerde incidenten zijn, behalve de bekende inzet van brandweer, politie en geneeskundige hulpverlening, ook andere partners betrokken. Specialistische kennis van ICT en AI is noodzakelijk voor oplossingen. De veiligheidsregio moet dan ook veerkrachtig zijn, kunnen samenwerken met ‘nieuwe’ partners en heeft wellicht meer specialistische kennis nodig (2018, p.19).”

2.2 Hoe worden cyberrisico’s beoordeeld?

In alle risicoprofielen zijn cybergerelateerde risico’s gepositioneerd in een risicodiagram. [3] De beoordeling van waarschijnlijkheid en impact lopen hierbij uiteen. De incidenttypen ‘uitval ICT en telecommunicatie’ en ‘uitval spraak- en datacommunicatie’ zijn in 23 (waaronder één provinciaal) risicoprofielen als volgt beoordeeld: [4]

> 3 x onwaarschijnlijk en ernstig
> 3 x mogelijk en aanzienlijk
> 8 x mogelijk en ernstig
> 3 x mogelijk en zeer ernstig
> 4 x waarschijnlijk en ernstig
> 2 x waarschijnlijk en zeer ernstig/catastrofaal

Tabel 2.1 Risicobeoordeling van uitval ICT en telecommunicatie/ spraak- en datacommunicatie in de veiligheidsregio’s

Risicodiagram: Impact/ waarschijnlijkheid					
Catastrofaal				2 VR	
Zeer ernstig			3 VR		
Ernstig		3 VR	8 VR	4 VR	
Aanzienlijk			3 VR		
Beperkt					
	Zeer onwaarschijnlijk	Onwaarschijnlijk	Mogelijk	Waarschijnlijk	Zeer waarschijnlijk

De inschaling van moedwillige cybercrime (inclusief cyberspionage en aantasting van de cybersecurity) loopt eveneens uiteen in die risicoprofielen waar deze meegenomen wordt als (apart) incidenttype:

> 1 x mogelijk en aanzienlijk
> 2 x mogelijk en zeer ernstig
> 1 x waarschijnlijk en aanzienlijk

[3] Een risicodiagram is een versimpelde weergave van risico’s; de achterliggende overwegingen waarop de beoordeling is gebaseerd en wat er onder het risico wordt geschaard, blijven buiten beeld.
[4] In één geanalyseerd regionaal risicoprofiel wordt enkel verwezen naar het incidenttype cybercrime, en niet naar ‘uitval ICT en telecommunicatie’ of ‘uitval spraak- en datacommunicatie’. Deze risicobeoordeling is niet meegenomen in de tabel.

Hoe de beoordeling van cybergerelateerde risico's tot stand komt, blijkt niet uit alle risicoprofielen. De kans bestaat dat veiligheidsregio's (cyber)risico's niet op uniforme wijze inschatten, waardoor het onderling vergelijken van risico's lastig is.[5] Slechts twaalf veiligheidsregio's hebben hun risico's kenbaar[6] geanalyseerd aan de hand van de impactcriteria uit de HRR. Als belangrijkste impactgebieden voor het risicotype 'uitval ICT en telecommunicatie' worden gezien:

> doden
> ernstig gewonden en chronische zieken
> kosten
> verstoring van het dagelijkse leven
> sociaalpsychologische impact

Hierbij worden de laatste twee criteria doorgaans als ernstig tot zeer ernstig ingeschaald. In een aantal risicoprofielen wordt daarnaast gerefereerd aan een 'mogelijke aantasting van de positie van het lokale en regionale openbaar bestuur', waarbij de impactbeoordeling uiteenloopt van aanzienlijk tot zeer ernstig.

In enkele risicoprofielen wordt uitgegaan van een (beperkt tot ernstig) risico op de aantasting van de integriteit van het grondgebied en in één risicoprofiel is de 'langdurige aantasting van milieu en natuur (flora en fauna)' geïdentificeerd als ernstig risico bij uitval van telecommunicatie en ICT: "Wanneer door het niet bereikbaar zijn van de alarmcentrale een natuurbrand in het beginstadium niet gemeld kan worden, zal deze zich razendsnel ontwikkelen. Ervaringen met natuurbranden leren dat het op deze wijze verloren gaan van 350 ha natuurgebied geen uitzondering is (Veiligheidsregio Brabant-Noord, 2018, p. 80)."

Vrijwel alle veiligheidsregio's benadrukken bij uitval van ICT en telecommunicatie het gevaar van cascade- of keteneffecten. Zo wordt er rekening gehouden met een verstoring van het openbare en bedrijfsleven door onder andere de uitval van het betalingsverkeer, het stilvallen van verkeersregelinstallaties, de verstoring van de ziekenhuiszorg en het wegvallen van communicatie tussen personen. Ook wordt in een aantal risicoprofielen specifiek rekening gehouden met een verstoring van de hulpverlenings- en crisisbeheersingsprocessen van de veiligheidsregio zelf, bijvoorbeeld door de uitval van communicatiesystemen zoals C2000 en het alarmnummer 112.

Belangrijke criteria waar rekening mee moet worden gehouden vanuit het oogpunt van continuïteit zijn:

1. De verwevenheid van de voorzieningen/netwerken (ook met andere vitale voorzieningen).
2. De veelheid van aanbieders in de keten en de onderlinge afhankelijkheid/gelaagdheid (en daarmee een moeilijk inzicht in gevolgen).
3. De keteneffecten die mogelijke verstoringen te weeg zullen brengen (en het gebrek aan 'awareness' hieromtrent).
4. Afnemende maatschappelijke acceptatie van verstoringen.

(Veiligheidsregio Gooi en Vechtstreek, 2015, p. 35)

Enkele veiligheidsregio's identificeren in hun risicoprofiel specifieke risico-objecten, zoals datacentra of ICT-knooppunten.

[5] Zie ook: Inspectie Justitie en Veiligheid, 2019; IFV, 2017.

[6] Niet alle veiligheidsregio's hebben een achtergronddocument van hun risicoprofiel gepubliceerd. Er bestaat derhalve de mogelijkheid dat ook voor het opstellen van de overige risicoprofielen gebruik is gemaakt van de impactcriteria uit de handreiking.

3 Voorbereiding op cyberrisico's in de veiligheidsregio's

Dit hoofdstuk bevat de resultaten van de uitvraag onder de hoofden Veiligheidsbureau van de veiligheidsregio's. Omwille van de leesbaarheid wordt in het vervolg steeds gerefereerd aan 'de veiligheidsregio's'. Daarnaast hebben de resultaten alleen betrekking op de 21 veiligheidsregio's die de enquête hebben ingevuld.

De enquêteresultaten zijn landelijk weergegeven en opgesplitst in de volgende onderdelen, die elk in een paragraaf behandeld worden:

> aandacht voor cyberrisico's in de veiligheidsregio's
> inventarisatie en beoordeling van cyberrisico's
> actuele ontwikkelingen en prioriteiten, zoals activiteiten, behoeften en aanbevelingen op het gebied van cyberwaakzaamheid en -gevolgbestrijding.

Daarnaast bevat dit hoofdstuk aandachtspunten en behoeften die uit de expertsessie naar voren kwamen. Deze zijn weergegeven in blauwe kaders.

3.1 Aandacht voor cyberrisico's

3.1.1 Organisatie

In veertien veiligheidsregio's zijn de onderwerpen cyberwaakzaamheid en cybergevolgbestrijding neergelegd bij individuele functionarissen en in vier regio's (aanvullend) bij een ambtelijke interne werkgroep. In drie regio's bestaat een (deels aanvullende) regionale werkgroep met vertegenwoordigers van diverse kolommen en organisaties. Drie regio's geven aan dat het thema cyber (nog) niet specifiek is uitgezet binnen de eigen organisatie.

Gemiddeld zijn er per veiligheidsregio vier medewerkers werkzaam op het gebied van cyberwaakzaamheid en cybergevolgbestrijding. In de meeste regio's is het onderwerp belegd bij adviseurs crisisbeheersing, ICT-medewerkers, beleidsmedewerkers en CISO's ('chief information security officers'). In een aantal veiligheidsregio's houden zich programmaleiders informatie en/of netwerkorganisaties bezig met vraagstukken rondom cyber, terwijl dit in wederom andere regio's voornamelijk adviseurs zijn op het gebied van opleiden, trainen en oefenen.

3.1.2 Belangrijkste cyberrisico's

De cyberrisico's, die door veiligheidsregio's als meest belangrijk en impactvol worden beschouwd zijn:

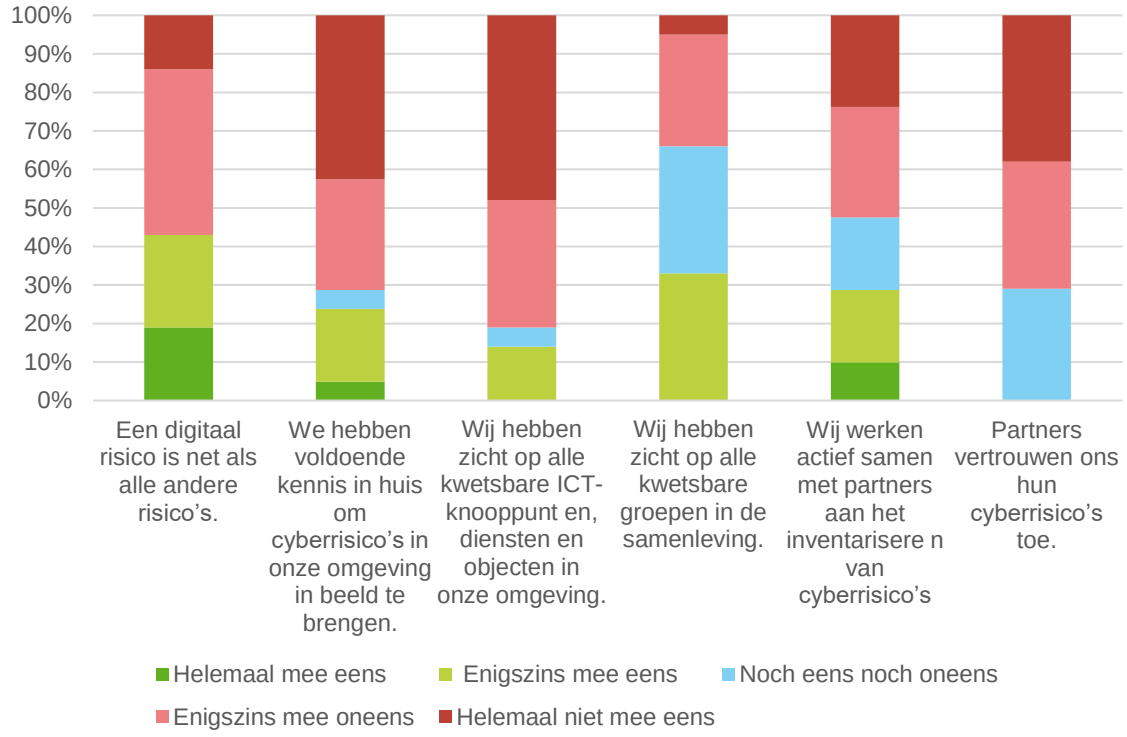
1. Uitval van vitale voorzieningen, zoals drinkwater-, energie-, ICT- en telecombedrijven.

2. Verstoring van de continuïteit van de eigen crisisorganisatie of hulpverlening, bijvoorbeeld door de uitval van communicatiemiddelen.
3. Verstoring van BRZO-bedrijven[7], met als gevolg fysieke veiligheidsrisico's en/of gezondheidsrisico's voor de omgeving.
4. Hack of uitval van datacentra, waardoor gevoelige data kunnen lekken en de privacy van bedrijven of particulieren in het geding komt.

Ook storingen binnen ziekenhuizen en zogenoemde cascade-effecten, waarbij een (cyber)incident tot andere fysieke en/of digitale verstoringen kan leiden, worden door meerdere regio's als toprisico's geïdentificeerd.

3.1.3 Cyberwaakzaamheid en cybergevolgbestrijding

Op een schaal van nul tot tien geven veiligheidsregio's gemiddeld een vijf aan hun cyberwaakzaamheid. Figuur 3.1 laat zien dat de meeste regio's beseffen dat een digitaal risico afwijkt van meer alledaagse, fysieke risico's zoals grootschalige branden. 81% geeft echter aan niet volledig zicht te hebben op alle kwetsbare ICT-knooppunten, diensten en objecten in de eigen regio. Daarnaast denkt 72% niet voldoende kennis te hebben binnen de organisatie om cyberrisico's in de omgeving in beeld te brengen. Minder dan de helft werkt actief samen met partners om cyberrisico's te inventariseren, meer dan twee derde geeft aan dat partners hun cyberrisico's niet toevertrouwen aan de regio 34% van de veiligheidsregio's gelooft alle kwetsbare groepen in de samenleving in beeld te hebben, terwijl 32% aangeeft dat dit nog niet het geval is.



Figuur 3.1 Zes schaalvragen (helemaal mee eens – helemaal niet mee eens) over de mate van cyberwaakzaamheid in de veiligheidsregio's

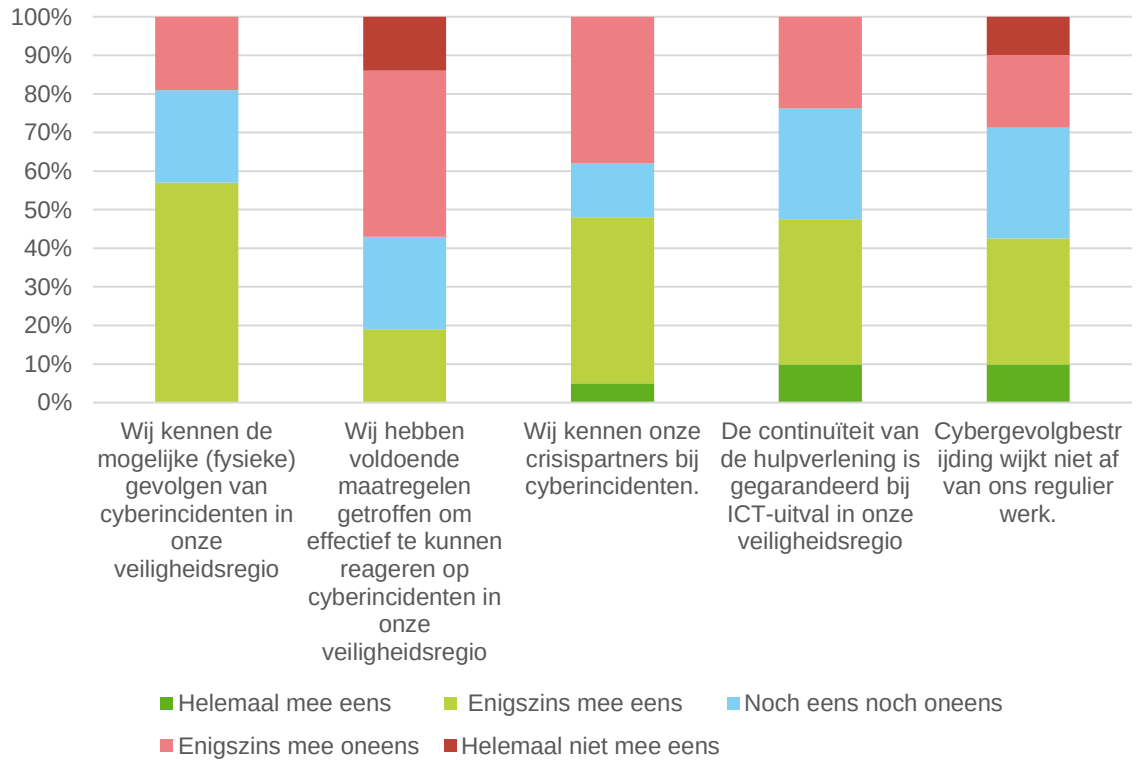
[7] BRZO staat voor Besluit risico's zware ongevallen en betreft bedrijven die met veel gevaarlijke stoffen werken. De stoffen kunnen giftig, ontvlambaar of explosief zijn.

Aanvullend op de schaalvragen gaven meerdere respondenten aan dat de veiligheidsregio's zich nog in een fase van 'bewustwording' bevinden op het gebied van digitale ontwrichting en cyber. Ook is erop gewezen dat er wel degelijk kennis aanwezig is in de verschillende regio's en bij externe partners, maar dat deze nog niet voldoende gebundeld is.

Hoe onderscheidt digitale ontwrichting zich van reguliere crises? – Input uit de expertsessie

1. Cyberincidenten zijn vaak niet (of minder direct) zicht- en tastbaar dan klassieke, fysieke incidenten en crises. Bij fysieke incidenten met een digitale oorzaak is de bron vaak moeilijk te identificeren.
2. Het verloop van een cyberincident is aan de voorkant nagenoeg onvoorspelbaar.
3. Cyberincidenten houden zich niet aan grenzen en kunnen meerdere domeinen betreffen.
4. Dit heeft tot gevolg dat men met andere partners moet afstemmen en samenwerken dan bij klassieke incidenten.
5. Er spelen veelal andere dilemma's. Zo kan het herstel van ICT-voorzieningen van getroffen bedrijven of organisaties op gespannen voet staan met opsporingsbelangen van de politie.
6. Een cyberincident kan daardoor een langer herstel- en nazorgtraject tot gevolg hebben.
7. Al met al vergen cyberincidenten meer flexibiliteit en improvisatievermogen van een crisisorganisatie dan klassieke incidenten.

De gemiddelde score voor de voorbereiding op cybergevolgbestrijding is met een zes iets hoger dan het cijfer voor cyberwaakzaamheid. Een factor die hieraan ten grondslag kan liggen is de bekendheid met mogelijke gevolgen van cyberincidenten (bij 57% van de regio's) en crisispartners (bij 48%). Daarnaast geeft ongeveer de helft van de regio's aan reguliere procedures te kunnen toepassen op cybergevolgbestrijding en vertrouwen te hebben in de continuïteit van de eigen hulpverleningsorganisatie bij ICT-uitval (zie ook figuur 3.2).



Figuur 3.2 Vijf vragen over de mate van voorbereiding op cybergevolgbestrijding in de veiligheidsregio's

Respondenten lichten toe dat de fysieke effecten van een cyberincident vergelijkbaar kunnen zijn met die van reguliere incidenten. Op (de bestrijding van) digitale gevolgen is binnen de veiligheidsregio's daarentegen nog weinig zicht. Ook is nog niet overal bekend hoe de verantwoordelijkheden verdeeld zijn bij een cyberincident, waardoor er volgens de respondenten meer zou moeten worden ingezet op kennis en bewustwording.[8]

3.2 Inventarisatie van cyberrisico's

3.2.1 Bestaande methodieken

83% van de veiligheidsregio's geeft aan gebruik te maken van de HRR voor het inventariseren en beoordelen van cyberrisico's. 57% raadpleegt (daarnaast) het *Cybersecuritybeeld Nederland*, en 29% het NVP.

De HRR en het NVP worden door respectievelijk 23% en 33% van de veiligheidsregio's die deze documenten raadplegen, als waardevolle tools beschouwd voor de inventarisatie en beoordeling van cyberrisico's. Daarnaast vindt de helft van de gebruikers dat het NVP belangrijke informatie bevat over cyberrisico's; 22% van de gebruikers zegt dit over de HRR. Uit de toelichtingen blijkt dat de HRR en NVP vooral als statische, procesmatige documenten worden beschouwd voor de risico-inventarisatie, maar niet als specifieke informatiebronnen over cyberrisico's. Zo zijn cyberrisico's bijvoorbeeld niet expliciet benoemd in de laatste versie van de handreiking uit 2009 (zie ook paragraaf 1.2.1).

Regionale risicoprofielen
Het inventariseren en beoordelen van nieuwe risico's zoals cyber is niet eenvoudig: risico-informatie is beperkt beschikbaar en versnipperd en veiligheidsregio's hebben veel partijen nodig voor een gefundeerde risicodialoog. Het roept bij veiligheidsregio's ook de vraag op welke informatie nodig is en waar die informatie te vinden is. Andere vragen zijn:

> In hoeverre moeten regio's afzonderlijk van elkaar dit soort nieuwe grensoverschrijdende risico's beoordelen en zou dit niet meer in samenhang met landelijke risicobeoordeling moeten, zoals eerder voorgesteld in het rapport *Risico's in samenhang* (IFV, 2018)?
> Is de bestaande methodiek, zoals opgenomen in de handreiking uit 2009 nog wel actueel en passend bij het huidige risicolandschap?
> Welke methodiek kunnen veiligheidsregio's hanteren voor de risicodialoog met vitale/niet vitale partijen in hun omgeving?

Ons advies is om deze vragen als input te gebruiken binnen het landelijk netwerk regionaal risicoprofiel en met relevante actoren zoals het analistennetwerk Nationale Veiligheid de bestaande methodiek te herijken.

Het Cyber Security Beeld Nederland daarentegen wordt door bijna alle gebruikers (92%) als belangrijke informatiebron voor cyberrisico's beschouwd. De helft van de gebruikers geeft aan dat het CSBN ze ondersteunt bij de inventarisatie van cyberrisico's in de eigen regio. Uit enkele opmerkingen blijkt echter dat veiligheidsregio's nogal moeite hebben bij het vertalen van landelijke risico's naar regionale risico's: "Het CSBN is te algemeen om conclusies te trekken voor onze regio. Algemeen is het wel een duidelijk beeld."

[8] Zie in dat kader ook de TNO Factsheet Challenge Regionale Cybergevolgbestrijding Veiligheidsregio Zuid-Holland-Zuid (TNO, 2019)

3.2.2 Organisaties en instanties

Circa driekwart van de veiligheidsregio's wint bij het opstellen van een risicoprofiel voor cyberincidenten advies in bij vitale partners en andere regio's. Ruim de helft verwerkt informatie van het NCSC, en iets minder dan de helft staat in contact met gemeenten. NCTV, LOCC, NCC en private kennisinstellingen worden in de voorbereidende fase door ongeveer een kwart van de veiligheidsregio's geraadpleegd. Daarnaast geeft een aantal respondenten aan contact te zoeken met ziekenhuizen, de politie, het Openbaar Ministerie, Agentschap Telecom en ministeries als Justitie en Veiligheid en Defensie evenals ketenpartners. Ook openbare informatie van het internet wordt door enkele regio's benut.

Het inventariseren en beoordelen van cyberrisico's – adviezen en aandachtspunten uit de expertsessie:

1. Maak een brede partner-/stakeholderanalyse.
2. Ga met bestaande partners in gesprek over cyberrisico's.
3. Doorloop – samen met deze partners – de cyberscenario's.
4. Focus niet alleen op vitale infrastructuur, maar ook op BRZO-bedrijven en maatschappelijke organisaties zoals ziekenhuizen, hogescholen en universiteiten.
5. Bevorder bewustwording onder bekende hoogrisicobedrijven in de regio en inventariseer informatiebehoeften.

Verder geven deelnemers aan behoefte te hebben aan een checklist met te stellen vragen over cyberrisico's.

3.3 Ontwikkelingen en prioriteiten

3.3.1 Aanvullende activiteiten

Ter voorbereiding op mogelijke cyberincidenten neemt de grote meerderheid (86%) van de veiligheidsregio's deel aan landelijke, bovenregionale en/of regionale netwerken op het gebied van digitale ontwrichting en cyber, en werkt actief aan de opbouw van cyberkennis en expertise (82%). Daarnaast oefent meer dan de helft (67%) van de regio's met cyberscenario's, bijvoorbeeld in een GBT- of ROT-setting. Voor het opleiden en trainen van cyberfunctionarissen is in 43% van de regio's aandacht. 38% heeft cyberscenario's reeds uitgewerkt in de eigen planvorming. Daarnaast zijn enkele veiligheidsregio's bezig met (de voorbereiding van) beïnvloedingsanalysen.

3.3.2 Behoeften en aanbevelingen vanuit de regio's

Respondenten geven aan dat het binnen veiligheidsregio's momenteel nog ontbreekt aan kennis en bewustwording op het gebied van cyber. Een overzicht van regionale en landelijke partners en hun verantwoordelijkheden tijdens verschillende soorten cyberincidenten, zou volgens een aantal regio's kunnen helpen effectief te reageren op digitale crises: "Help de VR'en bij inzicht in het netwerk van partners die hierin iets moeten betekenen," suggereert een respondent. Een andere respondent stelt voor een landelijk kenniscentrum voor cyberrisico's in te richten voor alle veiligheidsregio's, terwijl een andere pleit voor een "Landelijke expertisepool cyber", die als liaison kan plaatsnemen in een regionaal crisisteam. Andere respondenten geven aan baat te hebben bij een sectoraal Computer Emergency Response Team (CERT) dat de eigen crisisorganisatie kan ondersteunen bij cyberscenario's. Ook een samenvatting van alle beschikbare informatie op het gebied van

cyber en een concrete handreiking met handelingsperspectieven kan volgens sommige respondenten bijdragen aan een bekwaam optreden tijdens of na een digitale verstoring.

Behoeften op het gebied van cyberwaakzaamheid en -gevolgbestrijding – input uit de expertsessie:

Cyberwaakzaamheid:
De rol van de veiligheidsregio in de risicobeheersing identificeren en hier vervolgens een concreet stappenplan voor maken. Onderdelen kunnen zijn:

1. Kennis opbouwen op het gebied van digitale verstoring en cyber. Hiervoor moet eerst geanalyseerd worden welke kennis en vaardigheden een veiligheidsregio daadwerkelijk zelf in huis moet hebben.
2. Een netwerkanalyse maken om partners en risico-objecten in de digitale wereld in beeld te brengen.
3. Bewustwording verhogen door risicocommunicatie in de koude fase, bijvoorbeeld bij risicobedrijven in de eigen regio.

Voorbereiding op cybergevolgbestrijding:

1. Inzicht vergroten in de benodigde deskundigheid voor de omgang met een digitale verstoring en hierbij ook nadenken over de benodigde crisisorganisatie. De huidige structuren en procedures zijn volgens deelnemers vooral gericht op klassieke crises.
2. Aandacht voor continuïteit van vitale processen voor hulpverlening en crisisbeheersing.
3. Voorbereiden op scenario's met veel onzekerheid over de effectiviteit van de bronbestrijding en met lange doorlooptijden om tot een oplossing te komen.
4. Mogelijke cyberscenario's uitwerken en (samen met partners) doorlopen. Oefenervaringen vervolgens delen met andere regio's. Ook kan het leerzaam zijn om eens mee te kijken met een oefening van een andere regio.
5. In de warme fase: deskundigheid (waaronder Nationaal CrisisCentrum (NCC), Nationaal Cyber Security Centrum (NCSC), Computer Emergency Respons Team (CERT, Information Sharing & Analysis Center (ISAC) zo veel mogelijk 'aan tafel' halen voor een adequate duiding van het incident.

Naast behoeften heeft een aantal respondenten concrete aanbevelingen geformuleerd om de cyberwaakzaamheid en (voorbereiding op) cybergevolgbestrijding te kunnen versterken binnen de regio's. Een vaak genoemde tip is om al aan de voorkant contact te leggen met partners: "Zorg zichtbaar te zijn op de vele bijeenkomsten in dit veld," geeft een regio aan; "Nodig jezelf uit bij anderen om over dit onderwerp te praten," stelt een andere voor. Ook wordt er geadviseerd om bij een cyberincident waarbij meerdere veiligheidsregio's getroffen zijn door een digitale verstoring, beroep te doen op het LOCC-Bovenregionaal.

Risicobeheersing rond digitale weerbaarheid: rol en mogelijkheden van veiligheidsregio's
Een actuele discussie onder vertegenwoordigers van de veiligheidsregio's richt zich op de rol van de veiligheidsregio op het gebied van cyberveiligheid/weerbaarheid in relatie tot bedrijven en maatschappelijke organisaties. Is er, naar analogie van klassieke brandveiligheidsinspecties, een rol weggelegd voor veiligheidsregio's ten aanzien van inspectie, toezicht en advisering bij bedrijven? En zo ja, welke bevoegdheden en expertise op het gebied van cyberveiligheid zijn vereist om die rol in te vullen?
Voor veiligheidsregio's is het in elk geval raadzaam om actief de dialoog met betreffende bedrijven en organisaties in de regio op te zoeken en deze:

> te bevragen over hun digitale risico's en weerbaarheid
> op de hoogte te brengen van mogelijke gevolgen van een ICT-verstoring voor de veiligheidsregio (en de noodzaak van onderlinge informatiedeling en samenwerking)

> te betrekken in regionale samenwerkingsnetwerken voor risicoanalyse en -beheersing.

Een dergelijke risicodialoog draagt bij aan het bevorderen van risicobewustzijn bij partners (voor zover nog niet aanwezig) en versterkt onderlinge relaties tussen de veiligheidsregio en vitale/niet vitale partijen – relaties waarvan beide partijen baat hebben bij daadwerkelijke verstoringen.

4 Conclusies

In dit hoofdstuk worden de conclusies besproken die uit het voorliggende onderzoek naar voren zijn gekomen. In het volgende hoofdstuk zullen enkele aanbevelingen worden gedaan die kunnen bijdragen aan een betere voorbereiding op en omgang met cyberrisico's door veiligheidsregio's.

4.1.1 Wat staat er in de regionale risicoprofielen over cyberrisico's en hoe worden deze risico's door veiligheidsregio's beoordeeld?

1. 'Cyber' komt als thema terug in vrijwel alle regionale risicoprofielen. Als benaming gebruiken de veiligheidsregio's vaak klassieke begrippen als 'uitval telecommunicatie en ICT' en 'uitval vitale voorzieningen'. De diepte waarmee cyberrisico's in beeld worden gebracht, varieert. Sommige regio's identificeren digitale ontwikkelingen als algemeen aandachtspunt en trend voor de komende jaren – een trend met potentiele impact op verschillende veiligheidsdomeinen. Andere berekenen kans en impact van specifieke (moedwillige) cyberscenario's.
2. In de meeste risicoprofielen wordt 'cyber' beschouwd als mogelijke oorzaak van een fysiek incident. De meeste risicoprofielen richten zich hierbij op de uitval van nutsvoorzieningen (vooral ICT en telecommunicatie), storingen bij ziekenhuizen en BRZO-bedrijven en cascade-effecten. Uit de enquête komt de volgende top-4 van risico's naar voren:
   – uitval van vitale infrastructuur
   – verstoring van de continuïteit van de eigen hulpverlening
   – verstoring van BRZO-bedrijven
   – hack van datacenters
3. Over digitale risico-objecten zoals datacentra of ICT-knooppunten, lijkt nog weinig bekend te zijn binnen de regio's, mogelijk omdat datacenters over het algemeen geen direct risico vormen voor de openbare veiligheid. De meeste regio's beseffen wel dat een digitaal risico afwijkt van meer alledaagse, fysieke risico's zoals grootschalige branden. 81% geeft echter aan niet volledig zicht te hebben op alle kwetsbare ICT-knooppunten, diensten en objecten in de eigen regio. Daarnaast denkt 72% niet voldoende kennis te hebben binnen de organisatie om cyberrisico's in de omgeving in beeld te brengen. Minder dan de helft werkt actief samen met partners om cyberrisico's te inventariseren.

4.1.2 Hoe komen veiligheidsregio's tot een beoordeling van cyberrisico's?

1. Methodieken als de *Handreiking Regionaal Risicoprofiel* bieden weinig inhoudelijk houvast en vooral procesinformatie voor de inventarisatie van (cyber)risico's binnen de eigen regio. Daarbij is niet altijd even transparant hoe veiligheidsregio's risico's inschatten, waardoor het onderling vergelijken van de gehanteerde werkwijzen en uitkomsten lastig blijft. Het Cyber Security Beeld Nederland (CSBN) daarentegen bevat voor veiligheidsregio's belangrijke informatie over ontwikkelingen op het gebied van

cyber. Uitdaging voor veel veiligheidsregio's is vooral het vertalen van die ontwikkelingen naar de eigen regio.

2. Op dit moment werkt minder dan de helft van de veiligheidsregio's actief samen met partners bij de inventarisatie van cyberrisico's. Waar uitwisseling plaatsvindt, worden vooral vitale partners en andere veiligheidsregio's geraadpleegd. Het onderling delen van 'risico-informatie' tussen veiligheidsregio's en hun partners is niet altijd vanzelfsprekend.

4.1.3 In hoeverre denken veiligheidsregio's voorbereid te zijn op cyberwaakzaamheid en -gevolgbestrijding?

1. De veiligheidsregio's beoordelen hun eigen preparatie op cyberwaakzaamheid en cybergevolgbestrijding met respectievelijk een 5 en 6. Gemiddeld zijn er per veiligheidsregio vier medewerkers werkzaam op het gebied van cyberwaakzaamheid en cybergevolgbestrijding.
2. De meerderheid van de veiligheidsregio's bereidt zich al voor op mogelijke cyberscenario's. Door de veiligheidsregio's worden diverse activiteiten genomen om zich voor te bereiden. Als belangrijkste activiteiten worden genoemd:
   – het opbouwen en onderhouden van regionale/landelijke netwerken (86%)
   – het opbouwen van cyberkennis en -expertise (81%)
   – oefenen met cyberscenario's (67%).
3. Voor veel veiligheidsregio's is het nog zoeken hoe zich adequaat te prepareren op digitale verstoringen. De nodige onduidelijkheid en onbekendheid bestaat onder meer over:
   – rollen, taken en bevoegdheden van betrokken actoren
   – procedures rond alarmering, opschaling en besluitvorming
   – benodigde eigen expertise op het vlak van cybergevolgbestrijding.
4. Over de bestrijding van de fysieke effecten van een cyberincident maakt men zich over het algemeen weinig zorgen binnen de veiligheidsregio's. De reguliere crisisbeheersingsstructuren en procedures zijn naar verwachting ook voor digitale verstoringen behulpzaam. Minder zicht hebben veiligheidsregio's op de bestrijding van de oorzaken van digitale verstoringen (bronbestrijding) en op de taken en bevoegdheden van landelijke, regionale en lokale actoren bij een cyberincident. Er is binnen de veiligheidsregio's behoefte om deze netwerken beter in beeld te brengen. Tevens is er behoefte aan een landelijk aanspreekpunt voor cyberrisico's en -incidenten; een aanspreekpunt dat in de koude en warme fase kan worden benaderd.

5 Aanbevelingen

In dit hoofdstuk worden enkele aanbevelingen gedaan die kunnen bijdragen aan een verdere preparatie op cyberwaakzaamheid en gevolgbestrijding door veiligheidsregio's. Voor iedere aanbeveling zijn mogelijke actiehouders benoemd.

5.1.1 Cyberwaakzaamheid

1. Ontwikkel een methodiek om cyberrisico's gefundeerd en systematisch te inventariseren en beoordelen. Denk bijvoorbeeld aan een opleidingsmodule of systematiek voor het vertalen van het Cyber Security Beeld Nederland naar de veiligheidsregio's en het voeren van een gedegen risicodialoog. Ook kan er verkend worden of een 'cybercrisisfunctionaris', met deskundigheid op het gebied van digitale risico's en een relevant expertisenetwerk, van meerwaarde is voor de eigen organisatie (actie: werkgroep Digitale Ontwrichting en Cyber).[9]
2. Gezien de voortdurende ontwikkelingen binnen de digitale wereld lijkt het niet reëel om alle cyberrisico's in beeld te hebben. Wel valt er winst te halen uit een bredere risicodialoog met vitale en niet vitale partners. Betrek bij de risicobeoordeling een regionaal netwerk van belanghebbenden. Denk hierbij juist ook aan partijen van buiten de eigen, vertrouwde kaders, zoals:
    a. vitale sectoren (zoals water, energie, openbaar vervoer)
    b. maatschappelijke organisaties zoals ziekenhuizen
    c. BRZO-bedrijven.

    Organiseer met dit regionale netwerk een open en inclusieve dialoog over cyberrisico's, waarbij diverse disciplines en perspectieven worden benut. Verder kan het nuttig blijken in risicodialogen niet eenzijdig te focussen op risico's, maar juist ook op onderliggende zorgen en angsten van bestuurders en beleidsmakers. Door zorgen rond nieuwe risico's met elkaar te delen ontstaat er een gevarieerder en meer gedeeld perspectief op risico's bij alle partners, en kunnen zorgen mogelijk (deels) worden weggenomen. (actie: veiligheidsregio's).

5.1.2 Cybergevolgbestrijding

3. Bedenk enkele concrete vragen over cyberrisico's, die met iedere regionale partner besproken zouden kunnen worden (actie: werkgroep Digitale Ontwrichting en Cyber). Hierbij kan gedacht worden aan vragen als:
    a. Wat zijn de belangrijkste cyberrisico's in de regio? Hoe bereidt men zich daarop voor?
    b. Wat verwachten regionale partners van de veiligheidsregio bij cyberverstoringen (en wat kunnen veiligheidsregio's van de betreffende partners verwachten)?

[9] In het opbouwen en uitwisselen van expertise over het inventariseren en beoordelen van (cyber)risico's zou het landelijke netwerk risicobeoordeling een betekenisvolle rol kunnen spelen.

c. Wat kunnen veiligheidsregio's en regionale partners voor elkaar betekenen in de koude en warme fase van een cyberincident?

4. Werk in de regionale preparatie op cybergevolgbestrijding naar analogie van terrorismegevolgbestrijding (TGB): gebruik enkele basisscenario's voor planvorming en oefenen. Mogelijke scenario's zijn:
   a. een cyberverstoring door 'collateral damage' (gebaseerd op de scenario's van het analistennetwerk nationale veiligheid);
   b. een verstoring in vitale ICT-voorzieningen van hulpdiensten zoals C2000 en LCMS;
   c. een digitale verstoring van vitale, maatschappelijke voorzieningen zoals water en energie.

   Deze benadering biedt houvast, is voorspelbaar richting de partners en biedt stap-voor-stap beter zicht op sterke en zwakke punten in de gezamenlijke preparatie, waaronder de samenwerking met 'nieuwe actoren' als het NCSC en cyberexperts. Maak waar nodig en gewenst met de partners concrete afspraken over alarmering, opschaling en onderlinge coördinatie bij digitale verstoringen (actie: veiligheidsregio's i.s.m. IFV/NCSC/NCTV).

5. Neem als veiligheidsregio – waar mogelijk – deel aan cyberoefeningen van andere veiligheidsregio's, of organiseer een bovenregionale cyberoefening. Faciliteer als Werkgroep Digitale Ontwrichting en Cyber een 'netwerk observatoren cyberoefeningen' die opgedane ervaringen bundelt en beschikbaar stelt aan de veiligheidsregio's (actie: werkgroep digitale ontwrichting).

Literatuur

Analistennetwerk Nationale Veiligheid (2019a), *Geïntegreerde risicoanalyse Nationale Veiligheid*, Bilthoven: RIVM.

Analistennetwerk Nationale Veiligheid (2019b), *Leidraad risicobeoordeling*, Bilthoven: RIVM.

Boin, A. (2017). *De Grenzeloze Crisis: Uitdagingen voor Politiek en Bestuur*. Oratie. Leiden: Universiteit Leiden.

Comfort, L. K., Boin, A., & Demchak, C. C. (eds.) (2010). *Designing Resilience: Preparing for Extreme Events*. Pittsburgh: University of Pittsburgh Press.

Expertgroep Regionaal Risicoprofiel (2019). *Achtergronddocument Regionaal Risicoprofiel 2019: Methodiek en onderbouwing*.

GHOR Nederland, Landelijk Overleg van Coördinerend Gemeentesecretarissen, Nederlandse Vereniging voor Brandweerzorg en Rampenbestrijding & Raad van Hoofdcommissarissen (2009). *Handreiking Regionaal Risicoprofiel*.

Inspectie Justitie en Veiligheid (2019), *De voorbereiding op hulpverlening na een terroristische aanslag*, Den Haag: Ministerie van Justitie en Veiligheid

Instituut Fysieke Veiligheid (2017). *Risico's in samenhang. Een verkennende studie naar de aansluiting tussen regio's en Rijk*. Arnhem: IFV.

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

Lagadec, P. (2007). Crisis Management in the Twenty-First Century: "Unthinkable" Events in "Inconceivable"Contexts. In Rodriguez, H., Quarantelli, E. L., en Dynes, R.R. (eds.), *Handbook of Disaster Research* (pp. 489–507). New York: Springer Science + Business Media.

Ministerie van Veiligheid en Justitie (2010). *Brochure: Wet veiligheidsregio's*. Den Haag: Ministerie van Veiligheid en Justitie.

NCTV (2019). *Cybersecuritybeeld Nederland: CSBN 2019*. Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

OECD (2003). *Emerging Risks in the 21st Century. An Agenda for Action*. Paris: OECD.

Slovic, P., & Weber, E. U. (2002). Perception of risk posed by extreme events. Paper voor conferentie *Risk Management Strategies in an Uncertain World*, April 12-13, New York, 1–21:https://www.ldeo.columbia.edu/chrr/documents/meetings/roundtable/white_papers/slovic_wp.pdf

TNO, *Factsheet Challenge Regionale Cybergevolgbestrijding Veiligheidsregio Zuid-Holland-Zuid*, 2019.

Veiligheidsregio Brabant-Noord (2018). *Samenvatting actualisatie risicoprofiel 2018: Veiligheidsrisico's in Brabant-Noord*.

Veiligheidsregio Gooi en Vechtstreek (2015). *Regionaal Risicoprofiel. Rapport*.

Veiligheidsregio Twente (2018). *Regionaal Risicoprofiel Twente*. Enschede: Veiligheidsregio Twente.

Bijlage 1 Analyse risicoprofiel per veiligheidsregio

	Veiligheids-regio	Laatste versie regio-naal risico-profiel	Cyberri-sico's als specifiek aan-dachts-gebied	Risiconaam / risiconamen	Risicobeoordeling			Genoemde risico's
					Kans	Impact	Aanleiding	Effect
1	Groningen	2016-2019	Ja	Uitval telecommunicatie & ICT	Mogelijk	Ernstig		> Verstoring openbare leven (uitval betalingsverkeer, stilvallen verkeersregelinstallaties, wegvallen van communicatie tussen personen en door hulpbehoevenden) > Verstoring bedrijfsleven > Uitval van belangrijke internetvoorziening in de Eemshaven (landelijke impact)
2	Fryslân	2018-2021	Ja	Uitval voorzieningen voor spraak- en data-communicatie (cyber)	Mogelijk	Aanzienlijk		> Effecten op openbare leven > Effecten op bedrijfsleven > Verstoring van dataverkeer (lek van vertrouwelijke informatie) > Cybercrime als aanleiding van uitval ICT

3	Drenthe	2015	Twijfel[10]	Verstoring telecommunicatie en ICT	Onwaar-schijnlijk	Ernstig	Impacttypen Handreiking Regionaal Risicoprofiel: > Doden: ernstig gevolg > Ernstig gewonden: ernstig gevolg > Kosten: ernstig gevolg > Verstoring dagelijks leven: ernstig gevolg > Sociaalpsychologische impact: woede en angst: ernstig gevolg
4	IJsselland	2018	Ja	Verstoring telecom/ICT	Mogelijk	Ernstig	Impacttypen Handreiking Regionaal Risicoprofiel: > Aantasting van de integriteit van het grondgebied (eventueel bij buitenlandse inmenging): beperkt gevolg > Doden: ernstig gevolg > Ernstig gewonden en chronisch zieken: ernstig gevolg > Lichamelijk lijden (gebrek aan primaire levensbehoeften): beperkt gevolg > Kosten: ernstig gevolg > Verstoring dagelijks leven: zeer ernstig gevolg > Aantasting van positie van het lokale en regionale openbaar bestuur: beperkt gevolg > Sociaalpsychologische impact: zeer ernstig gevolg
5	Twente	2018	Ja	Verstoring telecommunicatie/ ICT	Mogelijk	Ernstig	Gevolgen cyberincidenten: > Verlies van gegevens of informatiediefstal

[10] De projectgroep is van mening dat er inzicht ontbreekt over de (keten)effecten van verstoring in telecommunicatie en ICT. Naar aanleiding van het beschreven scenario in de bijlage heeft de projectgroep ervoor gekozen de weging van doden en kosten zwaarder in te schatten. Er is gesproken over het scenario zoals in het bijlagenrapport *Drents risicoprofiel 2011* staat beschreven, waarbij het aantal doden en economische schade hoger wordt verondersteld.

								> Fysieke gevolgen door uitval vitale sectoren of systemen > Cyberincidenten kunnen aan de basis staan van meerdere scenario's, zoals uitval van de elektriciteitsvoorziening, verstoring van ICT en uitval van de drinkwatervoorziening.
6	Noord- en Oost-Gelderland	2017-2020	Ja	Uitval ICT	Mogelijk / waarschijn-lijk	Zeer ernstig	Scenario niet uitgewerkt / toegelicht	Scenario niet uitgewerkt / toegelicht
7	Gelderland Midden	2016-2019	Ja	Cybercrime	Mogelijk	Zeer ernstig		Impacttypen Handreiking Regionaal Risicoprofiel: > Kosten: ernstige gevolgen > Verstoring van het dagelijkse leven: catastrofale gevolgen > Aantasting van de lokale en regionale positie van bestuur: zeer ernstige gevolgen > Sociaalpsychologische impact: zeer ernstige gevolgen
8	Gelderland-Zuid	2016-2019	Twijfel[11]	Verstoring telecommunicati e en ICT	Onwaar-schijnlijk	Ernstig		> Impact op het maatschappelijk functioneren (ziekenhuiszorg, vitale infrastructuur, pinverkeer en verkeersmanagement) en bedrijfsleven. > Uitval communicatiesysteem C2000 en alarmnummer 112 Impacttypen Handreiking Regionaal Risicoprofiel: > Doden: aanzienlijk gevolg > Ernstig gewonden en chronische zieken: ernstig gevolg

[11] "Het scenario 'Verstoring telecommunicatie en ICT' is ongewijzigd, maar gezien de toenemende afhankelijkheid van ICT opnieuw beoordeeld."

									> Kosten: ernstig gevolg > Verstoring van het dagelijkse leven: ernstig gevolg > Sociaalpsychologische impact: ernstig gevolg
9	Utrecht	2019	Ja	Cyberverstoring vitale sector / verstoring satellietsysteme n / aantasting internetfundame nt	Mogelijk	Aanzienlijk / ernstig			ICT & telecommunicatie: > Uitval van internet, datadiensten, spraakdiensten en satelliet tijd- en plaatsbepaling met risico voor betalings- en effectenverkeer met zelfs Europese uitstraling Cyberdreigingen: > Op alle vlakken dreigingen: communicatie, betalingsverkeer, fysieke verstoringen, het niet meer werken van eigen systemen
				Cyberspionage overheid	Waarschijn-lijk	Aanzienlijk			
10	Noord-Holland-Noord	2015-2018	Nee	Verstoring ICT	Mogelijk	Beperkt / ernstig			> Tijdelijke problemen in / uitval van bedrijfsvoering van zorginstellingen, overheid en particulieren > Uitval van het telefoonnetwerk kan leiden tot maatschappelijke onrust
11	Zaanstreek-Waterland	2019-2020	Ja	Uitval vitale voorzieningen	Waarschijn-lijk	Zeer ernstig / catastrofaal			> Uitval van de vitale voorzieningen raakt alle sectoren van de samenleving: burgers, bedrijven, organisaties, hulpverlening en de overheid
12	Kennemerland	2019-2022	Ja	Uitval ICT (cyberincident)	Waarschijn-lijk	Ernstig	>	Onbedoeld	> Impact op samenleving als geheel (burgers, dataverkeer en veel bedrijfsprocessen)

							> Technische oorzaken > Opzet door kwaad-willenden (malware, hacks, DDoS)	> Hulpverlenings- en crisisbeheersingsprocessen van de veiligheidsregio	
13	Amsterdam-Amstelland	2017	Ja	Verstoring telecommunicatie en ICT	Waarschijn-lijk	Ernstig/ zeer ernstig	cyber crime)	Impacttypen Handreiking Regionaal Risicoprofiel: > Doden: beperkt gevolg > Ernstig gewonden en chronisch zieken: aanzienlijk gevolg > Kosten: ernstig gevolg > Verstoring van het dagelijks leven: ernstig gevolg > Aantasting van positie van lokale en regionaal openbaar bestuur: ernstig gevolg > Sociaalpsychologische impact: aanzienlijk gevolg	
14	Gooi en Vechtstreek	2015	Ja	Verstoring telecommunicatie en ICT	Mogelijk	Zeer ernstig	> Technische storingen, > Graafwerkzaamheden > Brand > Invloeden van buitenaf (zoals terrorisme)	> Brede impact op maatschappelijk functioneren, zoals ziekenhuiszorg, vitale infrastructuur, pinverkeer en verkeersmanagement > Verstoring calamiteitenorganisatie door uitval communicatiesysteem C2000 en het alarmnummer 112	

15	Haaglanden	2019	Ja	Verstoring ICT - telecommunicatie	Mogelijk	Aanzienlijk	Impact op: > Sociale en politieke stabiliteit > Ecologische veiligheid > Economische veiligheid Door verweving van verschillende netwerken zullen keteneffecten optreden
16	Hollands Midden	2018	Ja	Verstoring telecommunicatie & ICT	Mogelijk	Aanzienlijk	> Verstrekkende gevolgen voor het zakelijke en het sociaal-maatschappelijke leven (geen telefonie, internet, verstoring betalingsverkeer) > Uitval belangrijke/vitale infrastructuur (ziekenhuizen/ verkeersregelinstallaties) > Maatschappelijke onrust, samen met grote economische schade
				Cybercrime[12]	Mogelijk/ waarschijn-lijk	Zeer ernstig	> Uitval van vitale infrastructuur > Secundaire effecten kunnen invloed hebben op het welzijn van mensen of de ecologie > Sociaalpsychologische impact: onrust en onzekerheid > Hulpverlening komt niet op gang (aantasting bedrijfscontinuïteit VRHM) > Gevolgen voor het openbaar bestuur en de politieke stabiliteit

[12] Opgevoerd onder hoofdcategorie ‘publieke veiligheid’.

17	Rotterdam-Rijnmond	2017-2020	Ja	Uitval spraak- en datacommunicatie	Mogelijk	Ernstig	Impacttypen Handreiking Regionaal Risicoprofiel: > Doden: aanzienlijk gevolg > Ernstig gewonden en chronische zieken: ernstig gevolg > Kosten: ernstig gevolg > Verstoring van het dagelijkse leven: zeer ernstig gevolg > Sociaalpsychologische impact: zeer ernstig gevolg
18	Zuid-Holland-Zuid	2019	Ja	Digitale verstoring	Waarschijn-lijk	Zeer ernstig	Impacttypen Handreiking Regionaal Risicoprofiel: > Aantasting van de integriteit van het grondgebied: beperkt gevolg > Doden: aanzienlijk gevolg > Ernstig gewonden en chronische zieken: aanzienlijk gevolg > Lichamelijk lijden (gebrek aan primaire levensbehoefte): aanzienlijk gevolg > Kosten: zeer ernstig gevolg > Verstoring van het dagelijkse leven: catastrofaal gevolg > Aantasting van de positie van het lokale en regionale openbaar bestuur: aanzienlijk tot ernstig gevolg > Sociaalpsychologische impact: ernstig gevolg
19	Zeeland	2019-2023	Ja	Uitval voorziening voor spraak- en datacommunicatie	Mogelijk	Ernstig	> Groot effect op het openbare leven en het bedrijfsleven (incl. dataverkeer); veel processen zullen bij een uitval tot stilstand komen

							> Invloed op alarmerings- en communicatiesystemen (P2000/C2000) en datasystemen van de hulpdiensten > Ontwrichting van de samenleving > Lek van vertrouwelijke informatie
20	Midden en West-Brabant	2015-2019	Ja	Verstoring telecommunicatie en ICT	Mogelijk	Ernstig	Impacttypen Handreiking Regionaal Risicoprofiel: > Aantasting van de integriteit van het grondgebied: ernstig gevolg > Doden: aanzienlijk gevolg > Ernstig gewonden en chronische zieken: ernstig gevolg > Kosten: ernstig gevolg > Verstoring van het dagelijkse leven: zeer ernstig gevolg > Aantasting van de positie van het lokale en regionale openbaar bestuur: aanzienlijk gevolg > Sociaalpsychologische impact: zeer ernstig gevolg
21	Brabant-Noord	2018	Ja	Verstoring van telecom / ICT	Waarschijnlijk	Ernstig	Meest kwetsbare bronnen zijn de datacenters en de POP's[13] van het vaste telecommunicatienetwerk. Impacttypen Handreiking Regionaal Risicoprofiel: > Doden: aanzienlijk gevolg > Ernstig gewonden en chronische zieken: aanzienlijk gevolg

[13] POP: 'Point Of Presence': locatie van een (lange afstand) telefooncentrale die een lokaal telefoonnetwerk bedient.

							> Kosten: aanzienlijk gevolg > Langdurige aantasting van milieu en natuur (flora en fauna): ernstig gevolg > Verstoring van het dagelijkse leven: ernstig gevolg > Aantasting van de positie van het lokale en regionale openbaar bestuur: beperkt gevolg > Sociaalpsychologische impact: ernstig tot zeer ernstig gevolg
22	Brabant-Zuidoost	2019	Ja	Verstoring telecommunicatie en ICT	Waarschijnlijk	Ernstig	Meest kwetsbare bronnen zijn de datacenters en de POP's[14] van het vaste telecommunicatienetwerk. Impacttypen Handreiking Regionaal Risicoprofiel: > Doden: aanzienlijk gevolg > Ernstig gewonden en chronische zieken: ernstig gevolg > Kosten: aanzienlijk gevolg > Verstoring van het dagelijkse leven: aanzienlijk gevolg > Aantasting van de positie van het lokale en regionale openbaar bestuur (m.n. indicator aantasting openbare orde en veiligheid): beperkt gevolg > Sociaalpsychologische impact: zeer ernstig gevolg

[14] POP: 'Point Of Presence': locatie van een (lange afstand) telefooncentrale die een lokaal telefoonnetwerk bedient.

				Aantasting cybersecurity	Mogelijk	Aanzienlijk	Impacttypen Handreiking Regionaal Risicoprofiel: > Doden: aanzienlijk gevolg > Ernstig gewonden en chronische zieken: aanzienlijk gevolg > Kosten: aanzienlijk gevolg > Verstoring van het dagelijkse leven: aanzienlijk gevolg > Sociaalpsychologische impact: ernstig gevolg
23/24	Limburg-Noord & Zuid-Limburg[15]	2020-2023	Ja	Uitval spraak- en datacommunicatie	Mogelijk	Zeer ernstig	Impacttypen Handreiking Regionaal Risicoprofiel: > Aantasting integriteit grondgebied: ernstig gevolg > Doden: ernstig gevolg > Ernstig gewonden en chronische zieken: ernstig gevolg > Kosten: ernstig gevolg > Verstoring van het dagelijkse leven: ernstig gevolg > Aantasting positie lokaal en regionaal openbaar bestuur: ernstig gevolg > Sociaalpsychologische impact: ernstig gevolg

[15] Veiligheidsregio's Limburg-Noord en Zuid-Limburg hebben de noodzaak tot samenwerking vertaald naar het eerste Provinciaal Risicoprofiel dat door twee veiligheidsregio's – samen met andere partners – is opgesteld.