1. Samenvatting

Digitale afhankelijkheid is opgenomen als één van de aanjagers in het Regionaal Risicoprofiel. Door de maatschappelijk ontwrichtende schade die het uitvallen van digitale systemen kan hebben, is het belangrijk in de gaten te houden welke ontwikkelingen er plaats vinden op het gebied van cyberrisico's. Zeker gezien de snelheid waarmee deze ontwikkelingen plaats kunnen vinden. Daarom is in dit document opnieuw gekeken welke cyberrisico's te onderscheiden zijn en op welke wijze VRHM op deze risico's in blijft spelen. Hoewel de digitale afhankelijkheid in Nederland nog steeds groeit, kan geconcludeerd worden dat het huidige beeld van nationale veiligheidsbelangen, de dreigingen tegen deze belangen en de digitale weerbaarheid in Nederland ten opzichte van 2021 niet fundamenteel gewijzigd zijn. Wel is het cyberdreigingsbeeld verder ontwikkeld. VRHM blijft zich daarom investeren in de interne cyberveiligheid en gevolgbestrijding.

2. Algemeen

Onderwerp:	Cyber	**Opgesteld door:**	VRHM Risicoduiding Roos Vegter
Voorstel t.b.v. vergadering:	Algemeen Bestuur	**Datum:**	20 april 2023
Agendapunt:	14.	**Bijlage(n):**	
Portefeuille:	A. Heijstee (DB) L. Weber (VD)	**Status:**	Informatief
Vervolgtraject besluitvorming:	N.v.t.	**Datum:**	N.v.t.

3. Toelichting

Aanleiding

Het belang van digitale systemen wordt in onze samenleving steeds groter. Veel aspecten van het dagelijks leven zijn gebaseerd op deze digitale systemen, en zijn hier inmiddels onlosmakelijk aan verbonden. Dit biedt enorm veel mogelijkheden, maar er kleven ook risico's aan. Wanneer deze digitale systemen (gedeeltelijk) uitvallen, heeft dit impact op het functioneren van onze samenleving. Het uitvallen van digitale systemen kan voortkomen uit technisch of menselijk falen, maar kan ook voortkomen uit cyberaanvallen en -incidenten.

Digitale afhankelijkheid is opgenomen als één van de aanjagers in het Regionaal Risicoprofiel. De toenemende digitale afhankelijkheid kan namelijk de risico's voor de fysieke veiligheid van de regio vergroten. Hoewel de hulpdiensten bij een digitale verstoring niet de eerste aangewezen partij zijn om het probleem op te lossen, heeft de veiligheidsregio wel een rol in de gevolgbestrijding hiervan. Daarnaast moet VRHM ook de eigen cyberveiligheid op orde hebben. Door de maatschappelijk ontwrichtende schade die het uitvallen van digitale systemen kan hebben, is het belangrijk inzicht te hebben in de factoren die dit uitvallen kunnen veroorzaken, en welke ontwikkelingen hierin te detecteren zijn. Inzicht in deze cyberrisico's is namelijk relevant voor de voorbereiding op digitale verstoringen, en voor de mogelijke gevolgen van digitale verstoringen.

Medio 2021 is een overzicht gemaakt welke cyberrisico's voor VRHM bestaan. Hoewel de dreigingen in deze lijst op dit moment nog steeds relevant zijn, is de mate waarin deze dreigingen relevant zijn

veranderd. Dit komt mede omdat de ontwikkelingen in digitale systemen enorm snel gaan. Daarom is regelmatige update van deze cyberrisico's essentieel. Niet enkel voor het inzicht in deze cyberrisico's, maar ook voor de preparatie daarop, zoals de planvorming en oefeningen die op deze cyberrisico's gebaseerd zijn.

Binnen de cyberrisico's is onderscheid gemaakt tussen ontwikkelingen in Europa en ontwikkelingen in Nederland. Dit is gebaseerd op twee verschillende bronnen. De eerste bron is afkomstig van het Europees Agentschap voor Cyberbeveiliging (ENISA). ENISA brengt elk jaar een rapport uit over de status van cybersecurity, de voornaamste dreigingen en relevante trends. Dit rapport wordt gemaakt op Europees niveau. Het meest recente ENISA rapport komt uit juli 2022[1]. Daarnaast is gebruik gemaakt van het Cybersecuritybeeld Nederland (CSBN). Het CSBN biedt op nationaal niveau inzicht in de digitale dreigingen in Nederland, belangen die daardoor aangetast kunnen worden, de weerbaarheid tegen deze dreigingen en tot slot de risico's. Het CSBN wordt jaarlijks vastgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)[2].

Europees niveau

- De hoeveelheid cybersecurity aanvallen zijn in 2022 toegenomen ten opzichte van 2021. Naast de hoeveelheid aanvallen, is ook de impact hiervan toegenomen.
- DDoS-aanvallen en ransomware zijn nog altijd de meest voorkomende dreigingen. Sinds 2021 is hier zelfs een toename in te zien. Er is sprake van een DDoS-aanval (Distributed Denial of Service-aanval) wanneer cybercriminelen meervoudige verzoeken om een website te bezoeken verzenden, waardoor deze website onbereikbaar wordt. Bij ransomware (gijzelsoftware) worden bestanden op de computer geblokkeerd, waardoor deze bestanden, of zelfs de gehele computer, onbereikbaar worden. Deze worden pas weer beschikbaar wanneer een bedrag betaald wordt.
- Er is bovendien een toename zichtbaar in cyberoorlog en hacktivisme. Er is sprake van cyberoorlog wanneer gepoogd wordt een land of samenleving te ontregelen door gebruik te maken van digitale verstoringen. Polarisatie en internationale conflicten kunnen daarbij een voedingsbodem vormen. Vooral de Rusland-Oekraïne crisis heeft een nieuwe periode van cyberoorlog ingeluid. Een vorm van cyberoorlog is hacktivisme. Hierbij worden digitale verstoringen gebruikt om een politieke boodschap over te brengen, bijvoorbeeld door het stelselmatig digitaal intimideren van personen en organisaties.

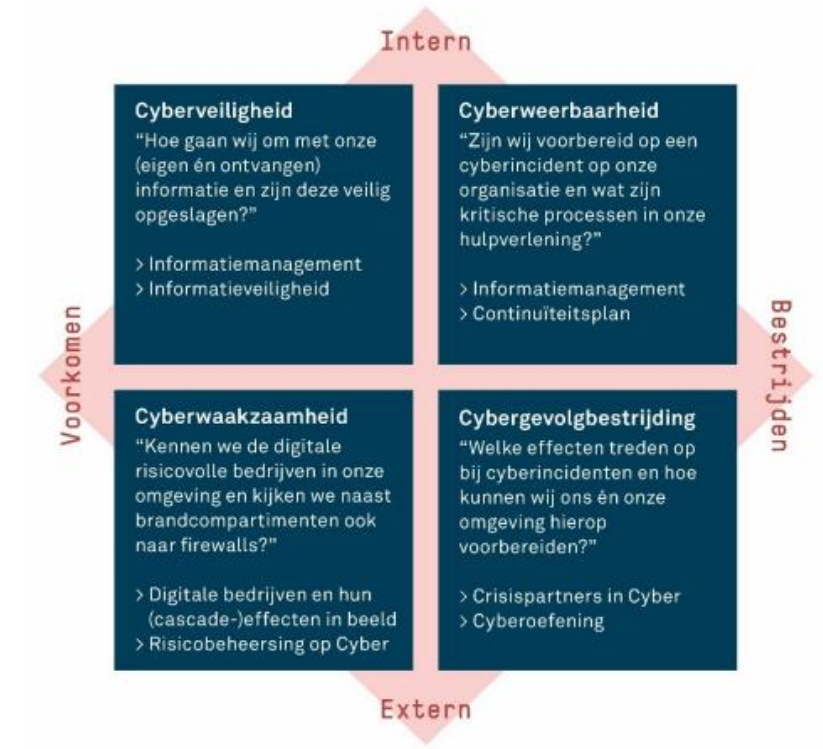
Nationaal niveau

- Het huidige beeld van nationaal veiligheidsbelangen, de dreigingen daartegen en onze digitale weerbaarheid is ten opzichte van 2021 niet fundamenteel gewijzigd. Wel is het dreigingsbeeld verder ontwikkeld.
- Er is een toename te detecteren in cyberaanvallen door statelijke actoren. Dit heeft ook gevolgen op nationaal niveau.
- Cyberaanvallen op leveranciersketens door criminelen zijn een groeiend probleem. Dit heeft namelijk niet alleen impact op de directe slachtoffers, maar ook op ketens van leveranciers, klanten en burgers. Cybercriminelen vallen hierbij hun einddoelwit aan door gebruik te maken van leveranciers en zakenpartners. Als methode wordt nog steeds veelvoudig ransomware gebruikt.
- In 2022 werd meer gebruik gemaakt van zero-day kwetsbaarheden. Er is sprake van een zero-day kwetsbaarheid wanneer een kwetsbaarheid in een nieuwe hardware- of software-systeem nog niet bekend is, waardoor deze kwetsbaarheid nog niet is opgelost. Hier kunnen criminelen vervolgens misbruik van maken.
- In Nederland is de directe dreiging die van hacktivisten uitgaat klein. Er bestaat echter wel afgeleide dreiging vanuit deze groeperingen.

[1] ENISA Threat Landscape (ETL) 2022.
[2] NCTV. Cybersecuritybeeld Nederland (CSBN) 2022.

- In 2021 werd geconstateerd dat de digitale weerbaarheid in Nederland nog niet voldoende is. Dit beeld is in 2022 helaas ongewijzigd. De omvang van de dreiging en de digitale afhankelijkheid groeit enerzijds, maar anderzijds groeit de weerbaarheid van de samenleving. De weerbaarheid blijft echter achter op wat er nodig is.

Cyberkwadrant
Wij werken binnen VRHM net als andere veiligheidsregio's met het cyberkwadrant (afbeelding 1). Middels een cyberkwadrant kan geïllustreerd worden op welke manieren een veiligheidsregio met cyberrisico's geconfronteerd kan worden. Deze cyberkwadrant zal gebruikt worden om de stand van zaken rondom het thema cyber bij VRHM uiteen te zetten.



Afbeelding 1: het cyberkwadrant zoals uitgewerkt door Veiligheidsregio IJsselland

Cyberveiligheid

'Hoe gaan wij om met onze (eigen én ontvangen) informatie en zijn deze veilig opgeslagen?'

Het garanderen van cyberveiligheid houdt in dat de interne systemen goed op orde zijn, en dat informatie veilig is opgeslagen. Voor een goed functionerende crisisorganisatie is deze interne cyberveiligheid essentieel. Dit betekent dat VRHM inzicht heeft in eigen processen en (mogelijke) kwetsbaarheden op digitaal vlak. Naast inzicht moet er actief gewerkt worden aan minimalisering van deze kwetsbaarheden. De afdeling informatiemanagement (IM) is verantwoordelijk voor de informatieveiligheid van onze interne infrastructuur. In het afgelopen jaar is binnen het 'Versnellingsprogramma Informatieveiligheid'[3] ook binnen VRHM gewerkt aan implementatie van de Baseline Informatiebeveiliging Overheid (BIO). Denk hierbij aan doorvoeren van technische beveiligingsmaatregelen, tabletop oefeningen rondom cyberweerbaarheid en bewustwording door middel van e-learning en publicaties.
Cyberweerbaarheid

[3] Versnellingsplan Informatieveiligheid - Nederlands Instituut Publieke Veiligheid.

'Zijn wij voorbereid op een cyberincident op onze organisatie en wat zijn kritische processen in onze hulpverlening?'

Voor de interne cyberveiligheid bestaat de vakgroep Informatieveiligheid om kennis uit te wisselen met andere veiligheidsregio's. Daarnaast is het VR-ISAC (Veiligheidsregio – Information Sharing and Analysis Center) ingericht ter ondersteuning van de cyberweerbaarheid van de eigen ICT-omgeving van de veiligheidsregio's. Op die manier zijn de veiligheidsregio's formeel aangesloten op vertrouwelijke informatie-uitwisseling met het Nationaal Cyber Security Centrum (NCSC).

Cyberwaakzaamheid

'Kennen we de digitale risicovolle bedrijven in onze omgeving en kijken we naast brandcompartimenten ook naar firewalls?'

Naast de voorbereiding op interne cyberincidenten, heeft VRHM ook een rol in het verkleinen van de risico's op fysieke gevolgen door externe cyberincidenten. Vooropgesteld dat de eigen organisatie verantwoordelijk blijft voor de eigen cyberveiligheid. VRHM kan echter wel een rol spelen in het aankaarten van bepaalde cyberonderwerpen, en het uitwisselen van informatie tussen verschillende partners. Op deze manier wordt het cyberbewustzijn verhoogd en worden partners gestimuleerd om de eigen cyberveiligheid op peil te houden. Dit doen we onder andere door cyber op de (bestuurlijke) agenda te houden. Maar ook door gesprekken die we met onze partners binnen crisisbeheersing gaan voeren en waarin we gezamenlijk gaan onderzoeken of de keten goed is voorbereid en op elkaar is aangesloten.

Ook het Nederlands Instituut Publieke Veiligheid (NIPV) heeft een bijdrage door onderzoek binnen het thema cyber. Zo is in het tweede deel van 2022 door het NIPV de verkenning 'Bestuurlijke bevoegdheden bij (dreigende) digitale incidenten'[4] uitgebracht. Hierin wordt een overzicht geschetst van de huidige bevoegdheden en overige interventiemogelijkheden van burgemeesters en/of voorzitters veiligheidsregio's bij (dreigende) digitale incidenten.

Cybergevolgbestrijding

'Welke effecten treden op bij cyberincidenten en hoe kunnen wij ons én onze omgeving hierop voorbereiden?'

<u>Planvorming</u>
Een belangrijke rol van de warme fase is cybergevolgbestrijding. Ondanks de bovengeschetste ontwikkelingen in cyberrisico's, veranderen deze processen voor VRHM niet fundamenteel. De belangrijke aspecten van cybergevolgbestrijding zijn verwerkt in de multidisciplinaire Informatiekaart cybergevolgbestrijding (zie bijlage 1). De informatiekaart is eind juli 2022 voor het laatst bijgewerkt. Met name de vraagstukken die kunnen opspelen in het kader van cybergevolgbestrijding zijn in de laatste versie van de informatiekaart aangescherpt.

Daarnaast is eind 2022 de Landelijk Crisisplan Digitaal-Publicatie (LCD-P) uitgebracht. Hierin staat een overzicht van de actoren en bijbehorende verantwoordelijkheden, een overzicht van crisisprocessen en dilemma's, en sleutelbesluiten. Het LCD-P geeft zo kaders aan veiligheidsregio's voor de aanpak bij een digitale crisis. Dit plan zal ook in VRHM geïmplementeerd worden. Deze implementatie zal in 2023 worden opgepakt.

[4] NIPV (2022). Bestuurlijke bevoegdheden cyber.

Opleiden, trainen, oefenen (OTO)
Naast kennis over de cyberrisico's en (mogelijke) bijbehorende gevolgen, is het belangrijk dat crisisfunctionarissen goed voorbereid zijn op deze digitale incidenten. Daarom wordt er ten behoeve van OTO een e-learning cyberbestrijding ontwikkeld. Hierin zal aandacht zijn voor de impact die de cyberrisico's met zich meebrengen. Het vergroten van 'cyber' bewustzijn, is een continu proces, welke dus terug moet blijven komen binnen het OTO programma.

Naast crisisfunctionarissen moeten ook gemeenten op de hoogte blijven van de risico's van digitale verstoringen. Om deze reden organiseert Bureau Gemeentelijke Crisisbeheersing (BGC) cybergames voor colleges van gemeenten. Op deze manier wordt binnen gemeenten bewustwording gecreëerd over de risico's. Deze cybergames vinden in 2023 weer plaats.

Tot slot wordt ook gekeken naar het organiseren van een themabijeenkomst over cyber voor het Algemeen Bestuur. Dit kan mogelijk in de vorm van het bespreken van dilemma's. Op dit moment is het streven om deze themabijeenkomst in het najaar van 2023 te organiseren.

Netwerk
VRHM sluit aan bij landelijke en regionale netwerken. Binnen de landelijke werkgroep digitale ontwrichting worden bijvoorbeeld ontwikkelingen besproken, scenario's doorgenomen en onderzoeken gepresenteerd. Daarnaast sluit VRHM aan bij het regionale CISO overleg, waarbij de CISO's van de gemeenten in Hollands Midden periodiek bij elkaar komen. In dit overleg worden ontwikkelingen gedeeld en ervaringen uitgewisseld.

4. Implementatie en communicatie
Cyberveiligheid is onderdeel van het VRHM jaarplan 2023.

5. Bijlagen
Vanwege de vertrouwelijkheid van de informatie worden informatiekaarten niet meegezonden met de vergaderstukken van het Algemeen Bestuur. De informatie is te vinden in de DB stukken van 6 april 2023.