Veiligheidscoalitie
Midden-Nederland

Programma Digitale Veiligheid

2020-2022

'De mens als ~~zwakste~~ sterkste schakel'

Door: Taskforce Digitale Veiligheid
In opdracht van: Regionaal Veiligheidscollege Midden-Nederland
Datum: juli 2020

Kroonstraat 25 – Postbus 8300 – 3503 RH – Utrecht – 06 148 73 690 – secretariaat@rvs-mn.nl – www.veiligheidscoalitie.nl

Veiligheidscoalitie
Midden-Nederland

Samenvatting

WAAROM

Werkzame principes & uitgangspunten
- Zelf het goede voorbeeld geven
- Publieke waarden centraal
- Publiek-private coalities
- Toegankelijke aanpak
- Verbinding tussen domeinen
- Rekening houden met elkaars opgaven
- Zoeken naar 'wat werkt'
- Kansen van digitalisering benutten

Urgentie
- Afhankelijkheid en impact van digitalisering op veiligheid en privacy wordt groter
- Beschermende maatregelen blijven achter bij de digitale dreigingen en risico's
- Toename in slachtofferschap met grote impact en schade
- Emotionele impact

Context
- Probleem wordt niet gevoeld
- Opsporing complex
- Impact relatief groot
- (Lokale) overheid zoekt naar rol
- Snel wisselende verschijningsvormen
- Weinig verbinding tussen veiligheid, informatiebeveiliging en privacy
- Standaard interventies leiden niet tot gedragsverandering

HOE

Wat doen we / gaan we doen
1. We duiden het vraagstuk: (onderzoek, masterclasses, verbinden domeinen oov/informatiebeveiliging)
2. We gaan concreet aan de slag: interventies weerbare jongeren, weerbare ondernemers, weerbare medewerkers
3. We bieden ruimte voor experimenten: privacy by design, toepassing big data veiligheidsdomein, stadspanel big data

Wat zien we gebeuren (positief & negatief)
- Aandacht voor digitale veiligheid neemt toe
- Nieuwe netwerken
- Samenhang tussen interventies ontbreekt
- Geen structurele financiele middelen. Enkel innovatiesubsidies.

WAT

Wie willen we beïnvloeden?
- Jongeren
- MKB'ers
- Eigen medewerkers
- Colleges/gemeenteraden/ burgemeesters
- Bestuur en leiding OM en Politie
- Kennisinstellingen
- VNG / Ministeries
- Bedrijven en brancheorganisaties

Wat willen we bereiken
- In 2022 zijn we beter beschermd tegen digitale indringers en criminelen
- We vinden de aanpak van digitale onveiligheid net zo normaal als de aanpak van bijvoorbeeld high-impact-crimes

Wat willen we onderzoeken?
- Wat zijn effectieve interventies om menselijk gedrag te veranderen
- Kansen digitalisering voor de aanpak van sociale veiligheidsvraagstukken
- Rol lokale overheid in relatie tot publieke en private partijen
- Op welke manier kan de overheid recht doen aan de behoeften van slachtoffers en daders van digitale criminaliteit

Cijfers
Cyberbeeld Midden Nederland, 6 en 12mnds rapportage, Rapporten CBS, CPB

Letters
Weten-schappelijke onderzoeken, trendrapporta-ges, inciden-tanalyses

Dialoog
Zie beïnvloeding.
Over rollen, verantwoordelijkheden en slim samenwerken. Over 'wat werkt' en de uitgangspunten van het programma.

Hulpmiddel: nieuwe tool leefstijlgericht communiceren

Beeld & Verhaal
Nieuwsbrief RVS met verhalen uit de praktijk, podcasts, persberichten digitale criminaliteit, volgen strafzaken digitale criminaliteit, Filmpjes / Games website RVS

Samen effectief voor een veilig Midden-Nederland

Kroonstraat 25 – Postbus 8300 – 3503 RH – Utrecht – 06 148 73 690 – secretariaat@rvs-mn.nl – www.veiligheidscoalitie.nl

Inhoudsopgave

Samenvatting 2

Inhoudsopgave 3

1 Naar een betere bescherming tegen digitale indringers 4

2 Doel en aanpak 5
2.1 Doel programma Digitale Veiligheid 5
2.2 Uitgangspunten van het programma 5
2.3 Wat gaan we doen? 7
2.4 Organisatie 12
2.5 Monitoren en verantwoorden 13

3 De complexe context van digitale veiligheid 16
3.1 Verschuiving van criminaliteit 16
3.2 Toenemende digitale afhankelijkheid 16
3.3 Kwetsbaarheden en risico's: over het Internet of Things en de menselijke factor 16
3.4 Wie worden slachtoffer en wat weten we over interventies? 18
3.5 Rol van de partners 20

4 Communicatie 23
4.1 Kernboodschappen voor partners, jongeren, ondernemers en medewerkers 23
4.2 Interne en externe communicatie 24

5 Randvoorwaarden en risico's 25
5.1 Randvoorwaarden 25
5.2 Risico's 25

Bijlage 1 Definities 26

Bijlage 2 Actoren 28

Bijlage 3 Impact Digitalisering 31

Bijlage 4 Begroting 2020 34

Bijlage 5 Mindmap Eigen Huis op Orde VNG 35

1 Een betere bescherming tegen digitale indringers

Stel je voor, je klikt op een verkeerde link en geeft hackers daarmee toegang om gijzelsoftware te plaatsen. Alle bestanden en systemen zijn vanaf dat moment vergrendeld. En het enige wat je kunt doen om alles terug te krijgen, is betalen. Het gebeurde Frank Landhuis die in 2017 werd gegijzeld door een hacker. Orders konden niet meer worden aangemaakt, facturen niet meer betaald of e-mails worden verstuurd. In januari 2020 gebeurde hetzelfde bij de Universiteit Maastricht. De schade bedraagt meer dan tonnen.

Steeds meer mensen worden slachtoffer van een vorm van digitale criminaliteit. In 2018 waren dat 1,2 miljoen mensen en dit aantal neemt jaarlijks toe. Het aantal fraudegevallen met onlinehandel steeg het afgelopen jaar met 31% en het aantal online betaalfraude, zoals phishing of skimming, steeg met 67%. Dit is een gevolg van de steeds verdergaande digitalisering. Deze biedt ons veel voordelen, maar we denken onvoldoende na over de risico's en kwetsbaarheden en het nemen van beschermende maatregelen. We weten ons fysieke huis goed te beveiligen, maar de ramen en deuren van ons digitale huis laten we open.

Digitale Veiligheid is daarom één van de prioriteiten uit de Regionale Veiligheidsstrategie Midden-Nederland 2019-2022. Het doel van het programma is om in 2022 beter beschermd te zijn tegen digitale indringers en criminelen. Ook willen we als veiligheidscoalitie de aanpak van digitale criminaliteit net zo normaal maken als de aanpak van bijvoorbeeld woninginbraken en veelvoorkomende criminaliteit. Dat begint volgens ons met duiding van het vraagstuk, samen concreet aan de slag gaan en onderzoeken wat werkt. Dit zijn dan ook de rode draden in het programma.

De focus in dit programma ligt vooral op digitale criminaliteit. Om digitale criminaliteit te voorkomen en te bestrijden is voortdurend reflectie en actie nodig op de manier waarop we als mens met onze digitale veiligheid omgaan. Daarom heet dit programma 'Digitale Veiligheid' en staat de mens daarin als 'zwakste en tevens sterkste schakel' centraal.

Leeswijzer

Dit programmaplan beschrijft op welke manier we als regio de komende jaren toewerken naar ons doel. We beginnen met de concrete aanpak in hoofdstuk 2 en geven achtergronden en duiding in hoofdstuk 3. In de hoofdstukken 4 en 5 wordt stilgestaan bij de communicatie over en de risico's binnen het programma. In de bijlagen wordt een overzicht geschetst van definities, actoren, de impact van digitalisering en een begroting.

Dit programmaplan is gericht aan de veiligheidsprofessionals van politie, OM en gemeenten in Midden-Nederland.

2 Doel en aanpak

2.1 Doel programma Digitale Veiligheid

In 2022 zijn we[1] beter beschermd te zijn tegen digitale indringers en criminelen.

- We zijn en blijven wakker op digitale dreigingen en risico's;
- We weten wat we willen beschermen en doen dat ook in toenemende mate;
- We hebben nieuwe coalities (publiek en privaat) gevormd om weerbaar te zijn;
- We vinden de aanpak van digitale onveiligheid en criminaliteit net zo normaal als de aanpak van bijvoorbeeld high impact crimes en veelvoorkomende criminaliteit.

Elk jaar wordt het programma voorzien van een actieagenda waarin de activiteiten beschreven staan voor de uitvoering van het programma.

2.2 Uitgangspunten van het programma

1. <u>We geven zelf het goede voorbeeld</u>
   De informatiebeveiliging van onze eigen organisaties is op orde. De overheid beschikt over een groot aantal persoonlijke gegevens van burgers en heeft de verantwoordelijkheid deze te beschermen. Gegeven de mens als zwakte schakel in deze informatiebeveiliging dient het eigen personeel goed getraind te worden om deze gegevens te beschermen.

2. <u>We stellen publieke waarden centraal</u>
   Binnen de aanpak van digitale onveiligheid worden nieuwe coalities gevormd met publieke en private partijen. Daarbij staan we als overheid wel voor onze publieke waarden zoals privacy, autonomie en veiligheid. Zie ook bijlage 3 'impact digitalisering'.

3. <u>We staan voor een toegankelijke aanpak</u>
   De interventies binnen het programma zijn laagdrempelig (bijvoorbeeld via subsidies) en niet complex zodat ze in de lokale veiligheidsaanpak te borgen zijn. Daarnaast maken we het taalveld niet onnodig ingewikkeld voor onszelf en de doelgroepen waar we ons op richten.

4. <u>We zoeken verbinding en samenhang tussen de domeinen openbare orde en informatiebeveiliging</u>
   Dit uitgangspunt hangt samen met het eerste uitgangspunt. Dat betekent automatisch dat het vraagstuk een goede verbinding vraagt tussen openbare orde en veiligheid en informatiebeveiliging.

[1] Veiligheidscoalitie en risicogroepen (vooral jongeren, ondernemers, eigen medewerkers).

5. We houden rekening met elkaars interne opgaven
   Partners hebben te maken met verschillende opgaven. In de landelijke veiligheidsagenda zijn bijvoorbeeld afspraken gemaakt over het aantal verdachten cybercrime. En tussen de arrondissementsparketten zijn verschillende cybercrimefenomenen verdeeld. Zo werkt de eenheid Midden Nederland de aanpak van DDOS-aanvallen uit.

6. We hebben oog voor slachtoffers en daders en gaan op zoek naar wat werkt
   We werken aan een steeds duidelijker beeld over slachtofferschap, daderschap en werkzame interventies. Daarom werken we mee aan wetenschappelijk onderzoek. Niemand zit te wachten op een programma dat een hoog 'schieten-met-hagel-gehalte' heeft. Daarom ligt de focus op de lange termijn. Ook delen en bespreken we de uitkomsten van landelijke onderzoeksprogramma's in en met het netwerk.

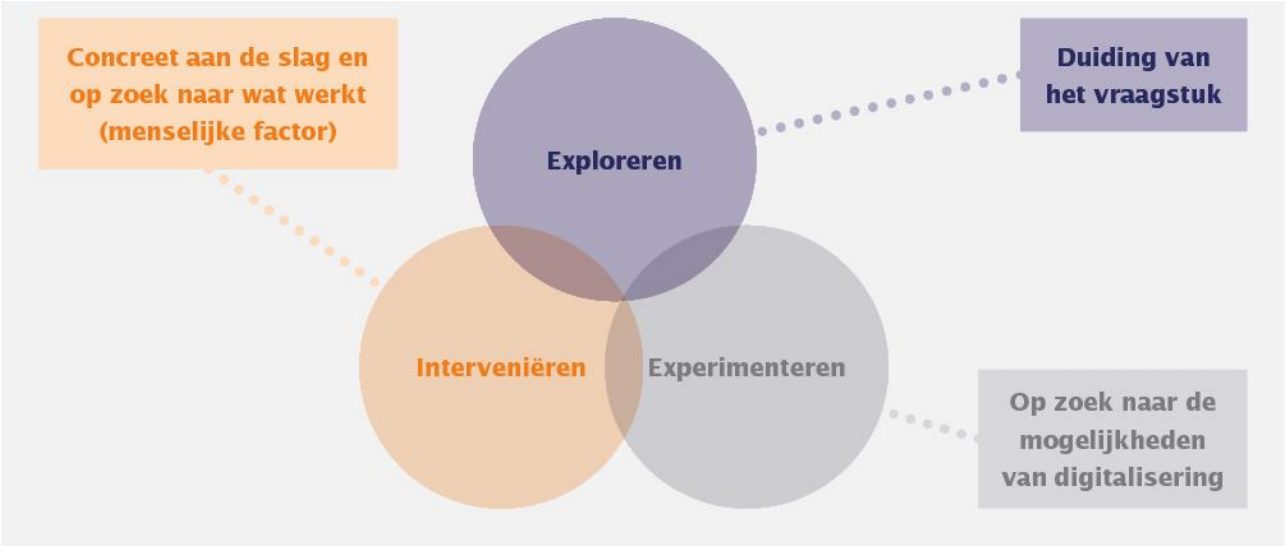
7. We hebben oog voor de mogelijkheden van digitalisering
   We staan niet alleen stil bij de risico's en gevaren van digitalisering, maar ook bij de mogelijkheden ervan om sociale veiligheidsvraagstukken op te lossen. We bieden daarom een platform voor nieuwe experimenten, concepten en technieken op het snijvlak van veiligheid, informatiebeveiliging en privacy.

2.3 Wat gaan we doen?

We richten het programma in langs drie programmalijnen: exploreren, interveniëren en experimenteren. We richten ons daarbij voornamelijk op het voorkomen van digitale criminaliteit door de mens als zwakste en tevens sterkste schakel in de informatiebeveiliging centraal te stellen. Ieder jaar werken we deze programmalijnen uit in de zogenoemde actie-agenda conform de overzichten op de volgende pagina.

De focus van het programma ligt nadrukkelijk niet op cybergevolgbestrijding. In de eerste plaats omdat er op verschillende niveau's al plannen voor cybergevolgbestrijding worden ontwikkeld. Op landelijk niveau wordt onder beheer van de Nationaal Coördinator Terrorismebestrijding gewerkt aan het Nationaal Crisisplan ICT. Voor het bovenlokale en regionale niveau is onder regie van het Veiligheidsberaad een bestuurlijk routeboek cybergevolgbestrijding ontwikkeld. En bureau Berenschot heeft in opdracht van de G4 de handreiking cybergevolgbestrijding gemaakt. In de tweede plaats omdat de primaire taak van de veiligheidscoalitie vooral bestaat uit de gezamenlijke (preventieve) aanpak van criminaliteit.

Overigens valt cybergevolgbestrijding niet los te koppelen van digitale criminaliteit.
Te denken valt aan het gebruik van malware en DDOS-aanvallen waarmee opzettelijk de beschikbaarheid, integriteit of vertrouwelijkheid van gedigitaliseerde processen of systemen wordt aangetast waardoor maatschappelijk ontwrichting optreedt. Voor zover mogelijk werken we met de veiligheidsregio's samen om de ontwikkelingen en nieuwste inzichten ten aanzien van digitale veiligheid, digitale criminaliteit en cybergevolgbestrijding in gezamenlijke netwerkbijeenkomsten en masterclasses aan te bieden binnen de veiligheidscoalitie.



1. Exploreren [2]

Eindproduct / dienstverlening	Acties	Doel	Looptijd
Platform professionals Digitale Veiligheid	1ste Netwerkbijeenkomst CISO's OOV'ers en privacyfunctionarissen	Verbinding tussen OOV'ers, Ciso's en privacyfunctionarissen versterken rondom thema digitale veiligheid	2020-2022
Masterclasses Digitale Veiligheid (Online)	Programma ontwikkelen met o.a. cyberteam Politie en externe sprekers	Als veiligheidscoalitie up-to-date zijn op digitale veiligheid	2020-2022
Bestuursconferentie MN	Opstellen interactief programma met workshops	Urgentiebesef en bewustzijn vergroten bij partners. Vaststellen van het programma Digitale Veiligheid.	2020-2022
Zitting / Presentatie Digitale Criminaliteit	Jaarlijks media en professionals uitnodigen voor zitting en/of een presentatie over een zaak houden tijdens een masterclass of netwerkbijeenkomst	Kennisbevordering veiligheidsnetwerk en extra maatschappelijke en aandacht voor digitale veiligheid.	2020-2022
Factsheet bestuursrechtelijk handhaven cybercrime	Uitkomsten onderzoeksprogramma's zoals NCSR en Politie en Wetenschap volgen en vertalen naar praktijk	Inzicht in de mogelijkheden van bestuursrechtelijke handhaving van digitale faciliteerders van o.a. georganiseerde misdaad (denk bijv. aan hostingbedrijven)	2021-2022
Digitaal District Midden Nederland (Politie)	Bewustwording, kennis, expertise en samenwerking vergroten.	Legitimiteit politie behouden. De politie is ook waakzaam en dienstbaar is in de online-omgeving. Goede voorbeelden (o.a. digitale wijkagent, webcare, knock and talk-gesprekken) vinden navolging in steeds meer basisteams.	2020-2022
Cyberbeeld	Ontwikkelen cyberbeeld (kwartaal)	Partners inzicht bieden in het verloop van digitale criminaliteit in Midden Nederland via een kwartaaloverzicht en via aangepaste veiligheidsbeelden vanuit bureau RVS	2020-2022

2. Interveniëren

Eindproduct / dienstverlening	Acties	Doel	Looptijd
Pilot Hackshield Midden Nederland	Start pilot met lokale users (scholen, verenigingen). Startbijeenkomst voor gemeenten Film	Weerbaarheid kinderen 8-12 jaar vergroten via gamification en storytelling. Zie www.joinhackshield. nl. Bedrijfsleven financiert stichting. Lokale overheid vervult makelaarsrol tussen stichting en scholen, verenigingen etc.	2020-2022
MKB-bijeenkomsten Digitale Veiligheid	Faciliteren van bijeenkomsten in samenwerking met Het CCV	Bewustzijn en handelingsperspectief vergroten.	2019-2022
Cyberchef Amersfoort	ICT-studenten aan ondernemers koppelen.	Van bewustzijn naar gedragsverandering. Interventie in periode 2020-2022 schaalbaar maken voor de regio. Bewustwording direct koppelen aan een concrete handeling (bijv. quiz, installeren password manager, scan MKB, beveiligingsaanpassingen etc.)	2020-2022
Regionale doe-bijeenkomst voor ondernemers (locatie Utrecht)	Programma en workshops (menukaart digitale veiligheid) opzetten	Bewustzijn vergroten en concreet aan de slag met gedragsverandering. Ondernemers gaan met experts aan de slag met de kwetsbaarheden in hun bedrijfsvoering en devices.	2021-2022
Podcastserie digitale criminaliteit	In samenwerking met cyberteam en radio een podcastserie maken (afhankelijk van subsidie)	Langs de as van spannende verhalen (gebaseerd op cases uit de regio) de bewustwording bij een groot publiek vergroten. Vertellen werkt beter dan instructie.	2020-2021
Factsheet Uitrol Cyber24-escapekoffer	Ophalen van leerervaringen in regio (Halt+ Voorhoedegemeenten: Almere, Amersfoort, Utrecht, Utrechtse Heuvelrug, Hilversum)	Vergroten weerbaarheid jongeren (12 tot 18 jaar). De cyber24-escapekoffer bestaat uit zes verschillende korte verhaallijnen voor en over jongeren. Jongeren tussen de 12 en 21 jaar krijgen opdrachten die passen in hun online leven. Zij zullen zowel 'daderschap' als 'slachtofferschap' ervaren.	2020-2022
Onderzoeksproject 'Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime'.	Deelname (uren) bureau RVS. Faciliteren onderzoekscons ortium Hogescholen en NCSR.	Ontwikkelen van effectieve interventies die daadwerkelijk tot gedragsverandering bij doelgroepen leiden.	2020-2022

Eindproduct / dienstverlening	Acties	Doel	Looptijd
Hackright en Hacklight	Hackright toepassen als alternatieve interventie (OM). Hacklight als niet strafrechtelijke interventie bij risicovol gedrag	Voorkomen van (herhaald) dader- en slachtofferschap van digitale criminaliteit onder jongeren tot en met 21 jaar.	2021-2022
Digitale buurtpreventie	Regionale randvoorwaard en (opleiding/instructie) ten behoeve van lokale teams borgen	Een digitaal weerbaar dorp of wijk door de inzet van digitale buurtambassadeurs. Gemeenten die beschikken over een goede infrastructuur en goed functionerende buurtpreventieteams faciliteren we (als buurtpreventieteams dat zelf willen) met basisopleiding/training/ advies.	2021-2022

3. Experimenteren

Eindproduct / dienstverlening	Acties	Doel	Looptijd
Testen weerbaarheid social engineering	Voorstel/aanbod ontwikkelen voor goede tests medewerkers	Weerbaarheid medewerkers vergroten ten behoeve van de informatiebeveiliging binnen de eigen organisatie en ter voorkoming slachtofferschap burgers en bedrijven	2020-2022
Factsheet: "Hoe ga je in gesprek met burgers over opensource, big data, toepassing sensoren"	Monitoren 'Stadspanel Smart City'.	Inzicht in op welke manier publieke waarden gewaarborgd kunnen blijven binnen toepassingen van opensource- en big data door lokale overheid.	2021-2022
Kennisdeling Privacy by design innovaties	Monitoren toepassingen privacy by design en pilots daarmee in Amsterdam, Nijmegen, Amersfoort, Almere etc.	Overheden en bedrijven die toepassingen mogelijk maken waardoor mensen meer grip op hun gegevens krijgen en daardoor minder risico lopen op bijvoorbeeld gegevensdiefstal en identiteitsfraude.	2021-2022
Handreiking en training inzet Opensource en Big Data bij veiligheidsproblematiek	Start samenwerking met lectoraat kennisanalyse en sociale veiligheid (promotieonderzoek) vanaf september 2020 Casuïstiek selecteren Gaandeweg het onderzoek leersessies voor het netwerk aanbieden	Inzicht verkrijgen in hoe veiligheidsprofessionals voorbereid kunnen worden op hun rol bij de inzet van data/datasystemen voor de aanpak van sociale veiligheidsproblemen. Rekening houdend met publieke waarden als privacy, autonomie, inclusie en rechtvaardigheid.	2020-2022

2.4 Organisatie

Regionale veiligheidsstrategie 2019-2022

Opdrachtgever / Regionaal Veiligheidscollege MN

Digitale Veiligheid is één van de drie prioriteiten in de gezamenlijke regionale veiligheidsstrategie 2019-2022 die door het Regionaal Veiligheidscollege (RVC) is vastgesteld. Daarmee is het RVC de opdrachtgever voor dit programma.

Opdrachtnemer / Taskforce Digitale Veiligheid

De Taskforce bestaat uit de bestuurlijk vertegenwoordigers van de vijf districten, de portefeuillehouder cybercrime van de politie en de (cyber)(officier van justitie. De Taskforce is opdrachtnemer van het programma en zorgt ervoor dat het programma kan worden uitgevoerd, onder meer door ervoor te zorgen dat de noodzakelijke beslissingen worden genomen. Iedere bestuurlijke vertegenwoordiger presenteert in zijn of districtelijk veiligheidscollege de stand van zaken van het programma en eventuele voorstellen (informeren, opiniërend of besluitvormend). De Taskforce komt minimaal 5 keer per jaar bij elkaar. Ieder Taskforcelid adopteert een specifiek onderwerp en is daarvoor eerste aanspreekpunt voor de programmamanager.

Programmamanager en projectleider

Iedere programma wordt operationeel bestuurd door een programmamanager, projectleider en een werkgroep. De programmamanager geeft het programma vorm, stuurt het aan en brengt het tot een goed einde. Hij zorgt ervoor dat het programma wordt uitgevoerd en de doelen steeds dichterbij komen en rapporteert aan de Taskforce. Hij bereidt de besluitvorming voor ten behoeve van de Taskforce en de districtelijke veiligheidscolleges en stuurt samen met de projectleider digitale veiligheid de werkgroep(en) aan. De projectleider zorgt ervoor dat een inspanning - bijvoorbeeld een project - binnen het programma wordt gerealiseerd en het afgesproken resultaat of de afgesproken uitkomst tot stand komt in nauwe samenwerking met de ambtelijke werkgroep en de programmamanager.

Werkgroep

De werkgroep digitale veiligheid bestaat uit ambtelijk vertegenwoordigers van de vijf districten. De werkgroep bereidt de vergaderingen voor de Taskforce voor en geeft in het ambtelijke vooroverleg voor de districtelijke veiligheidscolleges een toelichting op de stand van zaken van het programma en eventuele voorstellen (informeren, opiniërend of besluitvormend). Binnen de werkgroep worden de activiteiten/inspanningen van het programma verdeeld onder de subwerkgroep exploreren en experimenteren en een subwerkgroep interventies. Werkgroepleden motiveren collega's uit andere gemeenten of teams om bij te dragen aan de uitvoering van activiteiten/inspanningen. Bijvoorbeeld door een nieuw initiatief lokaal te faciliteren. De werkgroep komt minimaal 5 keer per jaar plenair samen.

Communicatie-advies en ondersteuning bureau RVS en werkgroep communicatie,

2.5 Monitoren en verantwoorden

Het monitoren en verantwoorden is gekoppeld aan het hoofddoel en de afgeleide doelen. Hiervoor hebben we de volgende indicatoren opgesteld[3]. Het betreft vooral indicatoren die iets zeggen over onze inspanningen. Effectindicatoren zijn lastig op te stellen omdat een causaal verband tussen veiligheidsinterventies en maatschappelijk effect moeilijk aantoonbaar is gezien de vele variabelen die een rol kunnen spelen. Via praktijkgericht onderzoek wordt wel een poging gedaan (zie indicator 1.9).

1	**Hoofddoel: In 2022 zijn we beter beschermd tegen digitale indringers en criminelen**
1.1	Aantal gemeentelijke interventies per doelgroep (jongeren/ondernemers/medewerkers) en het geschatte bereik ervan
1.2	Aantal aangiften politie
1.3	Aantal onderzoeken politie
1.4	Aantal haalzaken politie (zaken zonder aangifte die toch opgepakt worden)
1.5	Aantal verdachten OM
1.6	Aantal alternatieve interventies OM (o.a. Hackright)
1.7	Aantal dadergerichte interventies politie (waaronder ook verstoren)
1.8	Aantal slachtoffergerichte interventies politie (bijv, adviesgesprekken slachtoffers)
1.9	Mate waarin risicodoelgroepen aangeven te weten hoe ze hun gedrag kunnen veranderen, dat ook daadwerkelijk doen of voornemens zijn dat te doen (effect)

2	**Subdoel 1: We zijn en blijven wakker op digitale dreigingen en risico's.**
2.1	Aantal kennisbijeenkomsten en trainingen en het aantal bestuurders en veiligheidsadviseurs van gemeenten, politie en OM deze kennisbijeenkomsten of trainingen bijwoont.
2.2	Aantal onderzoeken/publicaties/ervaringsverhalen over digitale onveiligheid en criminaliteit waar het netwerk kennis van heeft kunnen nemen.

3	**Subdoel 2-4:** • **De aanpak van digitale veiligheid is net zo vanzelfsprekend als de aanpak van bijvoorbeeld high-impact-crimes of veelvoorkomende criminaliteit** • **We weten wat we willen beschermen en doen dat ook in toenemende mate;** • **We hebben nieuwe coalities (publiek en privaat) gevormd**
3.1	Aantal gemeenten dat in hun jaarplan of integrale veiligheidsplan de aanpak van digitale onveiligheid en criminaliteit heeft opgenomen en erover rapporteert
3.2	Aantal pilots politie geborgd in andere teams (bijv digitale wijkagent, knock and talk, etc)
3.3	Aantal lokale integrale interventies met Politie, OM, Gemeenten en andere partners
3.4	Mate waarin veiligheidsprofessionals aangeven zich de materie voldoende eigen gemaakt te hebben om er in hun werk mee uit de voeten te kunnen

[3] Vanuit het programma 'Digitaal District Politie Midden Nederland' zijn een aantal relevante indicatoren opgenomen in dit programma. De volledige monitoring en verantwoording wordt apart door de Politie opgesteld.

Meer dan alleen cijfers
Veel digitale criminaliteit en onveiligheid blijft buiten beeld bij de criminaliteitscijfers. Zoals benoemd in de Veiligheidsstrategie 2019-2022 willen we bij ons streven naar een veiliger Midden-Nederland daarom niet uitsluitend meer uitgaan van cijfers. We willen naar een rijkere en meer kwalitatieve vorm van kiezen, monitoren en verantwoorden.

Daarom maken we ook in dit programma meer gebruik van een combinatie tussen cijfers, beelden, onderzoeken en verhalen vanuit samenleving en professionals. Op basis daarvan voeren we het gesprek met elkaar in werkgroep, Taskforce, DVC en RVC.

Vorm	Activiteiten
Cijfers	6 en 12 mnds rapportage aanvullen met delicten digitale criminaliteit. Nu wordt alleen online fraude vermeld. Kwartaalbeeld cybercrime Politie Midden Nederland inclusief duiding. Zie verder: indicatoren.
Onderzoeken	Bijdrage leveren aan periodieke trendanalyse (jaarlijks) die vanuit RVS wordt opgemaakt. Hier betrekken we de inzichten uit recente wetenschappelijke onderzoeken bij. Meerjarig praktijkgericht onderzoek Saxion/ Haagse Hogeschool naar effectieve interventies. Taskforce en DVC's worden in de periode 2020-2022 minimaal 1 keer op de hoogte gebracht van de resultaten.
Beelden en verhalen	Jaarlijks brengen we een zittingsdag met cyberzaken in beeld. Politie, OM en burgemeesters vragen op die dag extra maatschappelijke aandacht voor het onderwerp digitale veiligheid. Indien ze daarvoor toestemming geven brengen we ook de verhalen van slachtoffers en daders in beeld. We tekenen verhalen op van de doelgroepen (jongeren/ondernemers/medewerkers).

Het meten van deze indicatoren gebeurt voornamelijk aan de hand van vragenlijsten, data van Politie en OM, kwalitatief onderzoek (waaronder meerjarig praktijkgericht wetenschappelijk onderzoek naar interventies binnen de regio). Voor het digitaal district wordt een aparte effectmonitoring opgesteld.

De resultaten en effecten van het programma worden tussentijds en na afloop van de programmaperiode geëvalueerd. Tussentijds in juli 2021. De eindevaluatie volgt eind 2022.
In dit programma zijn voorlopige indicatoren benoemd. Indien nodig worden deze tussentijds gewijzigd/aangevuld.

Voor de besturing van het programma maken we gebruik van het onderstaande schema (https://www.werkenaanprogrammas.nl/). Twee keer per jaar wordt dit schema in de werkgroep en Taskforce benut om te sturen op de voortgang van het programma.

	Tempo	**Haalbaarheid**	**Efficiëntie**	**Flexibiliteit**	**Doeltreffendheid**
Overall	Zijn we op tijd klaar met het programma	Gaan we de ambitie realiseren	Is het programma voldoende rendabel	Kan het programma nog anders	Heeft het programma voldoende impact
Doelen Indicatoren	Komen de doelen voldoende snel dichterbij	Zijn de doelen voldoende haalbaar	Wegen de financiële baten voldoende op tegen de kosten	Zijn de doelen voldoende bij te stellen	Halen we voldoende baten uit het programma
Inspanningen	Worden de inspanningen voldoende snel uitgevoerd	Zijn de inspanningen voldoende realiseerbaar	Voeren we de inspanningen voldoende efficiënt uit	Zijn de inspanningen in voldoende mate aan te passen	Dragen de inspanningen voldoende bij aan de doelen
Middelen	Komen de middelen voldoende snel ter beschikking	Zijn de middelen voldoende beschikbaar en bruikbaar	Zetten we de middelen voldoende rendabel in	Zijn de middelen in voldoende mate anders in te zetten	Dragen de middelen voldoende bij aan de inspanningen

3 De complexe context van digitale veiligheid

3.1 Verschuiving van criminaliteit

In 2018 waren 1,2 miljoen mensen slachtoffer van digitale criminaliteit. Dit betekent dat 1 op de 10 Nederlanders slachtoffer is geweest van digitale criminaliteit. De maatschappelijke schade werd in 2018 geschat op 10 miljard. Verder zien we binnen de 'traditionele' criminaliteit al jaren een daling, de zogenaamde 'crime-drop'. Er vindt een verschuiving plaats van fysieke criminaliteit naar digitale criminaliteit.

Wanneer we kijken naar individueel slachtofferschap zien we vier soorten delicten in de top staan. Hacken, e-fraude, kinderporno en de inbreuk op privacy (Tijdschrift voor Veiligheid, 2018). Verschillende vormen van digitale criminaliteit worden vaak tegelijk gebruikt. Zo hoeft hacken op zichzelf geen einddoel te zijn, het kan ook een stap zijn om data te stelen of een bankrekening te plunderen. In Midden-Nederland komen e-fraude, account-take over, techsupport scam en factuurfraude het vaakst voor.

3.2 Toenemende digitale afhankelijkheid

Ons leven is in toenemende mate afhankelijk geworden van digitale technologieën (Rathenau Instituut, 2017). De fysieke en online wereld raakt steeds meer met elkaar verweven. We bankieren online, leren online, en hebben online contact met anderen. Digitalisering stuurt en beïnvloedt steeds meer ons leven. Bijvoorbeeld door het gebruik maken van slimme apparaten (Internet of Things) of sensoren in openbare ruimtes. We maken daar volop gebruik van, maar denken nauwelijks na over de risico's en kwetsbaarheden voor onze veiligheid en privacy. Daarnaast kunnen digitale incidenten resulteren in maatschappelijke ontwrichting (CSBN, 2019, WODC, 2019). In veel gevallen kunnen deze incidenten ontstaan als van gevolg van menselijk falen. Voorbeelden hiervan zijn het niet installeren van updates, het klikken op verdachte linkjes of het simpelweg niet even fysiek checken of de berichtgever degene is die hij zegt te zijn. In bijlage 3 wordt de afhankelijkheid en impact van digitalisering uitgebreider omschreven.

3.3 Kwetsbaarheden en risico's: over het Internet of Things en de menselijke factor

Internet of Things

De digitale transformatie gaat in een rap tempo. Maar antwoorden op belangrijke vragen over de veiligheid, risico's en privacy groeien niet in ditzelfde tempo mee. Volgens Sandro Etalle (hoogleraar cybersecurity TU Eindhoven) staan we op een keerpunt van de geschiedenis. 'Als we nu niets doen, lopen we het risico overrompeld te worden door een technologie die we nu niet overzien of controleren en die onze privacy en veiligheid geheel ondermijnt'. Etalle spreekt over de ontwikkeling van het Internet of Things (IoT). Dit is een internet dat enkel bestaat uit met elkaar verbonden computers. Het aantal apparaten dat gekoppeld is groeit in een sneltreinvaart. Denk aan zelfrijdende auto's, intelligente thermostaten, sensoren, koelkasten, slimme huissystemen en complete energiecentrales.

Naar verwachting bevat het IoT in 2030, 75 miljard aangesloten apparaten wereldwijd. Het probleem dat Etalle schetst, is het gebrek aan controle op de ontwikkeling van dit soort technieken. Door de omvang van de technologie brengt dit een groot risico met zich mee. Denk bijvoorbeeld aan cryptojacken en DDOS aanvallen waarmee vitale websites en systemen worden platgelegd. Dit soort aanvallen wordt vaak al voor tientallen euro's als service aangeboden. Huidige veiligheidsmethodes zoals virusscanners of firewals voldoen niet meer als oplossing om jezelf hiertegen te wapenen.

Het probleem wordt echter niet direct door consumenten en fabrikanten gevoeld. Dit weerhoudt hen ervan hun apparaten beter te beveiligen. Zij ondervinden namelijk niet direct een nadeel van DDOS-aanvallen die gepleegd worden via hun apparaten die door consumenten slecht beveiligd worden. Hierdoor is er geen economische prikkel om het probleem op te lossen. Dit wordt ook wel het 'falen van de markt' genoemd (CBS, 2019). Bijvoorbeeld door productregulering op Europees niveau kan dit opgelost worden.

Omdat dit nog een te grote stap is, is voornamelijk winst te behalen in bewustwording en alternatieve interventies bij deze vorm van criminaliteit. Onderzoek laat ook zien dat tegenmaatregelen bij eindgebruikers van IOT-apparaten zeer effectief kunnen zijn. Het gaat om interventies als in quarantaine plaatsingen en het notificeren en instrueren waardoor het merendeel van de infecties wordt weggehaald en het percentage re-infectie zeer laag is (Cleaning Up The Internet Of Evil Things, 2019). Ook is bewustwording bij consumenten nodig dat hun slecht beveiligde IoT-apparaten rekenkracht leveren voor schadelijk DDOS-aanvallen.

> "Criminelen kunnen de besturing van slimme apparaten overnemen. Daarmee krijgt het vraagstuk van veiligheid ook een fysieke dimensie. Zo liet een beveiligingsonderzoeker zien hoe eenvoudig de speelgoedpop Cayla is te hacken en hij liet daartoe de pop passages uit de erotische roman Fifty Shades of Grey en quotes van de fictieve psychopaat Hannibal Lecter uit het boek The Silence of the Lambs citeren. Het hacken van de pop is een relatief onschuldig voorbeeld, maar de Nieuw- Zeelandse hacker Barnaby Jack liet tijdens een conferentie in 2011 zien dat hij de insulinepomp van een vriend te kon hacken. Hij kon de complete bediening overnemen en was in staat een fatale hoeveelheid insuline toe te dienen. Andere hackers lieten ook al zien dat ze de besturing van een via wifi bestuurde pacemaker konden overnemen en het apparaat een fatale schok af konden laten leveren (Greenberg & Zetter 2015)". Het vraagstuk van beveiliging wordt extra complex doordat in het IoT apparaten in verbinding met elkaar staan, waardoor een succesvolle hack van een koffiezetapparaat bijvoorbeeld toegang kan verschaffen tot de auto of toegang geven tot de voordeur" (Rathenau-Instituut, 2017, p.52).

Menselijke factor
De mens is de zwakste schakel in informatiebeveiliging (Van Eeten et al., 2019). Bij digitale criminaliteitsvormen zoals CEO-fraude, whatsappfraude, phising of spoofing wordt hier goed op ingespeeld. Deze aanvalstechniek wordt 'social engineering' genoemd en is een aanvalstechniek waarin misleiding en bedrog worden gebruikt om doelwitten actief te laten meewerken aan hun eigen slachtofferschap. Dit betekent dat met bewustwordingscampagnes en interventies gericht op die menselijke factor veel winst te behalen valt (Bullée, Montoya, Junger & Hartel, 2018).

Persoonsgegevens en het gebruik van data
Er zijn landelijke afspraken nodig over het delen van data. Er komen steeds meer vragen over hoe bedrijven omgaan met de data die zij verzamelen. Denk bijvoorbeeld aan Facebook. Binnen landelijke afspraken is het van belang dat gebruikers controle behouden over hun eigen data en ook de digitale instrumenten krijgen om dit op een makkelijke manier te doen.

In Nederland werkt de stichting Privacy by Design aan een dergelijk instrument. Deze app heet IRMA, 'I reveal my attributes. Deze digitale vertrouwensinfrastructuur lost kwetsbaarheden op en focust op twee elementen, data en vertrouwen. Privacy by Design beoogt met IRMA die grip, en daarmee vertrouwen en veiligheid in de samenleving, terug te geven. De stichting heeft hiervoor in 2018 de Brouwerprijs voor Wetenschap en Samenleving en in 2019 de internet innovatie award ontvangen. Met het IRMA-project richt de stichting zich volgens de jury 'op een groot en groeiend maatschappelijk probleem: de bescherming van persoonsgegevens in een samenleving waarin mensen zich steeds vaker moeten identificeren, waarbij de zorg groeit dat men de grip kwijtraakt over de eigen persoonsgegevens met identiteitsfraude als *worst case scenario*. Veertig gemeenten in Nederland ondersteunen IRMA al vanuit de Basisregistratie Personen met het aanleveren van attributen. Vanuit Midden-Nederland zijn dat De Bilt, Almere, Utrecht en Amersfoort. Ook de Nationale Politie is betrokken.

Daarnaast kan IRMA in toekomst helpen bij het voorkomen van verschillende vormen van digitale criminaliteit zoals account –takeover of identiteitsfraude. Mensen gebruiken nu vaak hetzelfde wachtwoord voor verschillende accounts. Dit maakt het systeem kwetsbaar en vormt een risico voor de veiligheid van gegevens. Zo werd in januari 2020 in Arnhem een 22-jarige verdachte opgepakt omdat hij 12 miljard emailadressen, gebruikersnamen en wachtwoorden te koop aanbood. Alleen al in Nederland kunnen 3,1 miljoen accounts gebruikt worden voor identiteitsfraude. Dit betekent dat 1 op 5 internetgebruikers gehackt is. Zelfs jaren nadat het account is gehackt, kan het wachtwoord nog gebruikt worden voor identiteitsfraude.

3.4 Wie worden slachtoffer en wat weten we over interventies?

Risicogroepen; jongeren, ondernemers en medewerkers
Jongeren zijn het vaakst slachtoffer van digitale criminaliteit. Hoewel vaak wordt gedacht aan ouderen als risicodoelgroep, was 12% van de jongeren tussen de 12 en 25 jaar in 2019 slachtoffer. Dit komt voornamelijk omdat jongeren het vaakst online zijn en daardoor het meeste risico lopen en ook meer risico's nemen. De online wereld voelt voor jongeren anoniem en dit heeft impact op hun gedrag en de mate waarin zij de schade van hun acties overzien. Vooral bij cyberpesten is dit een bekend fenomeen.

Daarnaast is het MKB één van de belangrijkste doelgroepen (Centraal Planbureau, 2019). Ondernemers van middelkleine bedrijven hebben 20% meer kans om slachtoffer te worden. Ze maken relatief weinig gebruik van eenvoudige beveiligingsmaatregelen als VPN, sterke wachtwoorden, tokenauthenticatie en middels encryptie verstuurde data. Beveiligings-onderzoekers, verzekeraars en branche-organisatie MKB-Nederland bevestigen dit. Bedrijven lopen hierdoor veel schade op en kunnen als gevolg daarvan zelfs failliet gaan.

Tot slot vormen ook de eigen medewerkers een belangrijke doelgroep. Zo is bijvoorbeeld voor gemeenten 'informatie de brandstof van een gemeentelijke organisatie. Van keukentafelgesprek tot parkeerbeheer. Bestuurders en ambtenaren hebben informatie nodig om hun werk goed te kunnen doen.

De informatie is ook steeds vaker vertrouwelijk van aard (gegevens cliënten, gegevens in de aanpak van ondermijning etc). Het is van groot belang dat deze gegevens goed beveiligd zijn' Stol en Bantema (2019). Wanneer dergelijke informatie wordt buitgemaakt, lopen inwoners, bedrijven en overheden grotere kans om vroeg of laat slachtoffer te worden van criminaliteit. Ook het vertrouwen in de overheid kan er enorm door geschaad worden. Medewerkers vormen dus een risicodoelgroep en moeten voortdurend gewapend worden tegen criminelen die via allerlei misleidingstactieken uit zijn op het platleggen van de dienstverlening en/of het stelen van persoons- en bedrijfsgevoelige data.

Impact
Veel delicten die van oudsher in de fysieke omgeving werden gepleegd, hebben nu een online component. Door het grenzeloze karakter ervan is de schade van het delict groot. Denk bijvoorbeeld aan afpersing, identiteitsfraude, smaad en laster. De impact is niet alleen groot in termen van schade, maar ook in termen van psychische impact. Je weet nooit wanneer het slachtofferschap ophoudt.

Zo kan een slachtoffer van sextortion telkens opnieuw geconfronteerd worden met beelden die opduiken. De *exposure is dus* enorm en dat geldt niet alleen voor individuen, maar ook voor organisaties. Tot slot wijzigt de handelswijze van criminelen zeer snel. Dit maakt het voor mensen en organisaties lastig om zichzelf voortdurend goed te beschermen.

Interventies
Voor cybercrime[4] is een ander soort interventies nodig dan voor traditionele criminaliteit (Kranenbarg, 2018). Onderzoek laat zien dat er verschillen zijn tussen de daderprofielen van cybercrime en traditionele criminaliteit. Dit houdt in dat beschermende factoren bij beiden ook op een andere manier werken. Bijvoorbeeld, het hebben van werk. Dit is voor traditionele criminaliteit een beschermende factor maar werkt op een andere manier bij cybercrime. Opvallend is dat mensen met een opleiding of die binnen de IT-sector werken vaak uit nieuwsgierigheid een cyberdelict plegen. Om te kijken hoever ze kunnen gaan. Daar komt bij dat cybercrime anoniem is En de pakkans laag. Dus de drempel ligt heel laag. Men heeft gevoel dat er weinig gevolgen zijn. Dit speelt ook een rol bij jongeren die cybercrime vaak bagatelliseren (Kersten & Stol, 2017). Ook bij jongeren is er verschil in daderprofielen en beschermende factoren. Bij cybercrime zijn er meer beschermende factoren aanwezig. Zo zijn jongeren opener naar hun ouders en hebben ze minder criminele vrienden. Daarnaast is het bij cybercrime voor veel jongeren onduidelijk waar de grenzen liggen (Kranenbarg, 2018). Bij traditionele criminaliteit zijn deze grenzen veel helderder. Daarom is het belangrijk om aan te geven waar de grenzen liggen en te focussen op de gevolgen. Hier ligt een belangrijke rol voor de politie en het Openbaar Ministerie om, als het gaat om cybercrime, actiever naar buiten te treden in communicatie over de opsporing en vervolging van delicten (Kranenbarg, 2018). De meeste onderzochte interventies voor cybercrime blijken niet bewezen effectief. Interventies zijn vaak niet theoretisch onderbouwd en het toepassen van standaard interventies bij deze vorm van criminaliteit werkt vaak averechts (WODC, 2017).

[4] Omdat in het onderzoek cybercrime in enge zin is bedoeld, gebruiken we in deze paragraaf bewust niet de term digitale criminaliteit.

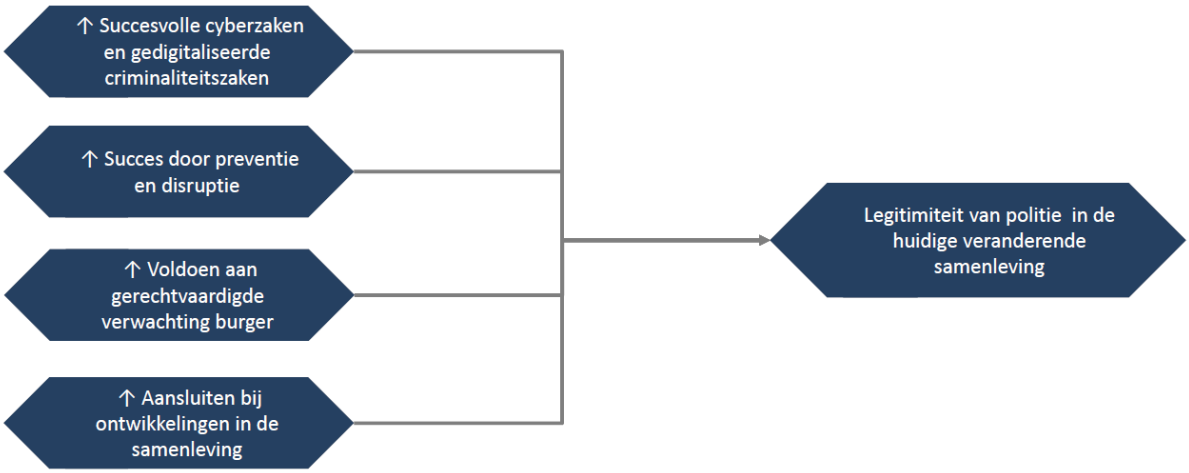
Onderzoekers verwachten dat interventies gericht op het beïnvloeden van peergroups, geautomatiseerde vormen van reageren, zoals digigeren, en technische preventie in combinatie met gedragsveranderende maatregelen wel effect hebben. Van interventies die enkel en hoofdzakelijk inzetten op voorlichting of afschrikking kan weinig verwacht worden.

Aangiftes
Het aantal aangiftes van digitale criminaliteit is laag en daarom geen afspiegeling van wat er daadwerkelijk aan digitale criminaliteit plaatsvindt. Bijvoorbeeld bij hacken wordt slechts in 7% van de gevallen gemeld. Bij andere vormen van criminaliteit is dit 37,5%. Dit heeft onder andere te maken met het feit dat slachtoffers zich schamen. Daarnaast heerst het idee dat er weinig met hun aangifte wordt gedaan. De pakkans is namelijk laag. Ook speelt mee dat burgers de politie en het Openbaar Ministerie niet per definitie als eerste aanspreekpunt zien. Afhankelijk van het delict wordt in eerst contact gezocht met bijvoorbeeld een bank (Leukfeld, Notté & Mash, 2018).

Het is belangrijk om meer aangiftes en meldingen te registreren om beter inzicht te krijgen in het soort delicten dat wordt gepleegd, door wie en op welke wijze. Dit kan de pakkans vergroten. Dit vereist wel dat de politie deze aangiftes op de juiste manier verwerkt. Hier ontstaat een spanningsveld tussen het stimuleren van de aangiftebereidheid en de mate waarin de politie deze kan oppakken. Het thema digitale criminaliteit is namelijk ook voor de politie een ontwikkelopgave.

3.5 Rol van de partners

Digitaal district Midden Nederland (Politie)
In Midden Nederland wordt door de politie hard aan gewerkt aan het ‘normaal maken’ van het onderwerp digitale criminaliteit binnen de hele organisatie. Daarom wordt in deze programmaperiode het digitaal district gelanceerd. Het grote doel van het digitaal district is de legitimiteit van de politie behouden.



In 2020 wordt het digitaal district gelanceerd. De inspanningen in het kader van het digitaal district worden onderzocht op hun effecten. Zie verder de paragraaf monitoren en verantwoorden in het voorgaande hoofdstuk

Operationalisatie	Succes in zaken (cyber en gedigitaliseerde criminaliteit)	Succes door preventie en disruptie	Voldoen aan gerechtvaardigde verwachting burger	Aansluiting bij digitale ontwikkelingen
	Het succes in brengzaken wordt behaald door: ▪ Aangiftes van goede kwaliteit ▪ Toewijzing/sturing op het draaien van zaken ▪ Capaciteit met kunde ▪ Inzet van opsporingsmiddelen digitaal ***Cyber specifiek:*** Succes in haalzaken wordt behaald door inzicht te hebben in fenomenen	Het succes door preventie en disruptie wordt behaald door: ***preventie*** ▪ Daderpreventie en slachtofferpreventie voor cyber en gedigitaliseerde criminaliteit ***disruptie*** ▪ Het verstoren van fenomenen ▪ Het verstoren op individueel of groepsniveau	Aan de verwachting wordt voldaan door: ▪ Te sturen op een realistische verwachting ▪ Te zorgen dat de burger zich begrepen voelt ▪ Deskundigheid te laten zien, zowel reactief in contact met de burger als proactief in de vorm van reclame	Er wordt aangesloten bij digitale ontwikkelingen door: ▪ Inzicht te hebben in digitale ontwikkelingen ▪ Manier van organiseren die mogelijk maakt om snel kunnen inspelen op ontwikkelingen buiten

Openbaar Ministerie
Het Openbaar Ministerie voert het gezag over de opsporing van cybercrime door de politie en bijzondere opsporingsdiensten en beslist over strafrechtelijke vervolging. In de meerjarenstrategie computercriminaliteit wordt ook grote waarde toegekend aan publiek-private samenwerking, het verstoren van criminele activiteiten en netwerken en inzetten op innovatie en alternatieve interventies. Ieder parket heeft een specifiek ‘cyberontwikkelthema’. Midden-Nederland richt zich op het fenomeen DDOS-aanvallen.

Het OM en de Politie kunnen verder een grote rol spelen in het genereren van maatschappelijke aandacht rond specifieke cyberzaken (generale preventie) en de inzet van expertise om zogenaamde barrièremodellen te ontwikkelen.

Rol lokale overheid
Gemeenten worden op drie manieren geconfronteerd met digitale veiligheid (VNG agenda digitale veiligheid, 2020). Op het vlak van informatiebeveiliging, digitale incidenten- en crises en digitale criminaliteit. Zie voor een uitgebreid overzicht bijlage 4 ‘Mindmap Eigen Huis Op Orde VNG’.

In dit programma is vooral de informatiebeveiliging in relatie tot digitale criminaliteit relevant. Volgens de VNG is er voor gemeenten een belangrijke rol weggelegd in het ‘eigen huis op orde’ brengen en houden. De digitale infrastructuur moet goed beveiligd zijn. Maar ook de eigen medewerkers mogen niet vergeten worden. Zie de vorige paragraaf over eigen medewerkers als belangrijke risicogroep en het belang om voortdurend gewapend te worden tegen digitale indringers en criminelen die via allerlei misleidingstactieken uit zijn op het platleggen van de dienstverlening en/of het stelen van persoons- en bedrijfsgevoelige data.

Lokale overheden doen er ook goed aan na te denken over de toepassing van big data in het veiligheidsdomein. Hoe willen we als overheid met onze burgers omgaan? Hoe maken we als professionals de juiste afweging tussen maatschappelijke veiligheid enerzijds en grondrechten van burgers anderzijds? Is het subsidiëren van een digitale deurbellen met camera in de strijd tegen woninginbraken nog steeds een goed idee als we niet weten wat er met de data van mensen gebeurt of wanneer de beveiliging ervan te wensen overlaat? En hoe voorkomen we dat het gebruik van algoritmes leidt tot risicoprofilering waardoor de minst bedeelden en de meest kwetsbaren uit bepaalde wijken en buurten al bij voorbaat als verdacht worden aangemerkt?

Op het gebied van openbare orde en cyberspace is de rol van de gemeente en vooral die van de burgemeester nog zeer beperkt. Dit vanwege het wettelijk vereiste dat maatregelen aangesloten moeten zijn op territoriale begrenzing van gemeentelijke bevoegdheden. Het probleem van deze beperking is dat de offline verstoring territoriaal bepaald kan zijn, maar dat dit niet hoeft te gelden voor de online aanleiding. Conclusie is dan ook dat op dit punt allereerst de wetgever aan zet is. Bestuurlijk blijven dan de volgende opties over: 1- online in gesprek gaan met de personen achter de uitingen die mogelijk verstorend zijn. 2- op basis van de Notice and Take Down procedure contact opnemen met digitale dienstverleners om uitingen die in strijd zijn met de gebruikersvoorwaarden van het betreffende platform te laten verwijderen. 3-Het online verspreiden van uitingen die de gewraakte uitingen tegenspreken of nuanceren. 4- Het opleggen van een dwangsom om bijvoorbeeld een illegaal onaangekondigd illegaal offline feest te voorkomen.

Publiek-private samenwerking
Veel vormen van digitale criminaliteit zijn te relateren aan online dienstverlening door financiële instellingen en bedrijven en risicovol gedrag van internetgebruikers. In het voorkomen en bestrijden van digitale criminaliteit moet samen opgetrokken worden. Dit gebeurt ook in toenemende mate. De uitdaging is om met elkaar een integrale aanpak te realiseren waarbij ingezet wordt op bestaande kansrijke initiatieven en nieuwe experimenten.

Link met het programma ondermijning
De mogelijkheden die ICT en het internet bieden, zorgen niet alleen voor nieuwe vormen van criminaliteit, maar ook voor een transformatie van de georganiseerde criminaliteit. Door het internet wordt de schaal daarvan steeds groter. Dit fenomeen wordt ook wel de cyberlift genoemd (WODC, 2018). Denk hierbij aan het gebruik cryptovaluta's of geldoverdrachten via webaccounts die als bankrekening dienen. Hierdoor is het relatief eenvoudig om wereldwijd afgeschermde geldoverdrachten uit te voeren en geld wit te wassen. Daar komt bij dat cybercrime simpel kan ingekocht kan worden. Criminelen huren specialistische kennis in of kopen doe-het-zelf-pakketten online. Hierdoor wordt cybercrime voor een breed publiek toegankelijk en inzetbaar (WODC, 2018). Dit wordt ook wel de democratisering van cybercrime genoemd.

Binnen het programma ondermijning is ook aandacht voor 'bestuurlijke weerbaarheid' en de integriteit van het personeel. Dit raakt aan onze constatering dat medewerkers ook ten aanzien van digitale criminaliteit een risicodoelgroep zijn.

4 Communicatie

Een goed communicatie draagt bij aan het bereiken van de doelen van het programmaplan. Het helpt bij het creëren van urgentiebesef en handelingsperspectief binnen de veiligheidscoalitie en bij de doelgroepen we in het programma voor ogen hebben.

Communicatie vanuit het programma is tevens gericht op het doorbreken van de schaamte die met slachtofferschap gepaard gaat, het vergroten van de meldingsbereidheid en het toegankelijk en normaal maken van het onderwerp (ook qua taalgebruik en jargon).

4.1 Kernboodschappen voor partners, jongeren, ondernemers en medewerkers

Partners
Iedereen kan elke dag slachtoffer worden van digitale criminaliteit. In 2018 hadden 1,2 miljoen mensen hier mee te maken en dit aantal stijgt. Wij, Veiligheidscoalitie Midden-Nederland, willen dat onze inwoners, eigen medewerkers en bedrijven in 2022 beter beschermd zijn tegen digitale indringers en criminelen. Alle partners in Midden-Nederland zijn daarvoor nodig. Wil jij je expertise en organisatie hiervoor inzetten? Doe mee en samen gaan we op zoek naar wat werkt!

Jongeren
Jij zit veel online. Logisch. Want (ook) daar heb je contact met je vrienden, ontmoet je nieuwe mensen, werk je aan je school of studie, verdien je wat geld of maak je plezier. Maar je bent niet de enige online. En ook minder anoniem dan je denkt. Criminelen slaan vaak online toe. Ruim 1 op de 10 jongeren wordt slachtoffer van cybercriminaliteit. Dat kan je veel geld kosten, maar ook al je privédata en zelfs je identiteit kan op straat komen te liggen. Wees je dus bewust van de risico's! Jij kan jezelf het beste beschermen online. Doe dat. Kijk op www.xxxxx welke maatregelen jij kan nemen om geen slachtoffer te worden van internetcriminelen.

Ondernemers
Als ondernemer kan je (bijna) niet zonder internet. Online factureren, de opslag en het beheer van je klantadministratie, het bestellen en verzenden van je producten. Juist als bedrijf loop je extra risico. Je bent interessanter dan een particulier. Internetcriminelen zijn uit op jouw data en/of je geld. Gelukkig kun je je hier zelf, samen met je medewerkers, goed tegen wapenen. Kijk op xxxxx welke simpele maatregelen je kunt nemen om geen slachtoffer te worden van internetcriminelen.

Medewerkers
Je krijgt als medewerker veel informatie over personen en bedrijven in handen. Vaak gaat het om gevoelige informatie die iets zegt over de persoonlijke omstandigheden van mensen. Deze data is voor internetcriminelen geld waard. Ze gebruiken het voor phishingmail, telefonische misleiding en zelfs afpersing. Of ze verkopen het gewoon. Internetcriminelen worden steeds slimmer en innovatiever om je informatie afhandig te maken. Gelukkig weten we ook steeds beter hoe ze werken. En wat je kunt doen om niet in hun vallen te trappen. Meer weten? Neem dan contact op met xxxxx en meldt je aan voor de trainingen/masterclass op …/…/…

4.2 Interne en externe communicatie

- We communiceren maandelijks met ons samenwerkingspartners via onze nieuwsbrief RVS en via sociale media (o.a. een speciaal LinkedIn-account van het programma digitale veiligheid).
- Op de website van bureau RVS publiceren we per onderwerp relevante onderzoeken interventies en campagnematerialen in de apothekerskast digitale veiligheid.
- Een communicatiewerkgroep bestaande uit communicatieadviseurs van gemeenten, politie en OM adviseren ons op aanvraag over de communicatie bij interventies richting risicodoelgroepen, het organiseren van (pers)bijeenkomsten en interviews, het indienen van subsidievoorstellen etc.
- De Taskforceleden zijn binnen hun district het bestuurlijk aanspreekpunt voor collega bestuurders. Wie de media-woordvoering doet wordt per onderwerp besproken binnen de Taskforce en waar nodig afgestemd met collega's buiten de Taskforce, zoals (regio) burgemeester, politiechefs, (hoofd)officier van justitie etc. Dat geldt eveneens voor de benadering van politici en bestuurders op landelijk niveau.
- We halen persoonlijke verhalen op bij professionals en risicodoelgroepen via interviews, video's, podcasts.
- Om effectief te communiceren is het belangrijk dat we onze doelgroepen goed kennen. Iedere gemeente krijgt in 2020 opnieuw de handreiking leefstijlgericht communiceren aangeboden met praktische tips over burgerparticipatie bij o.a. (digitale) veiligheid, veiligheid en zorg en ondermijning. De handreiking is tot op wijk en buurtniveau gespecificeerd.
- We gaan actief naar doelgroepen toe
- We brengen het landschap rond digitale veiligheid steeds beter in kaart.

5 Randvoorwaarden en risico's

5.1 Randvoorwaarden

Het gaat bij randvoorwaarden niet om onderwerpen die geregeld moeten worden om het programma te laten slagen. Randvoorwaarden hebben betrekking op afspraken waar we ons aan geconformeerd hebben en specifieke wet- en regelgeving.

- Regionale Veiligheidsstrategie 2019-2022

- De afspraken uit de landelijke veiligheidsagenda met betrekking tot cybercrime https://www.regioburgemeesters.nl/thema/sturing-op-politie/landelijke-beleidsdoelstellingen/veiligheidsagenda-2019-2022/. Voor Midden Nederland geldt in 2019 en 2020 een aantal van 33 reguliere onderzoeken waarvan 25% alternatieve (bijvoorbeeld Halt-afdoening) of aanvullende interventies.

- Wet- en regelgeving, in het bijzonder de Wet Computercriminaliteit III / Richtlijnen OM / Wet Digitale Overheid (in behandeling) / AVG / BIG)

5.2 Risico's

Bij risico's gaat het om onzekere gebeurtenissen die negatieve invloed hebben op het programma. Bijvoorbeeld omdat ze ervoor zorgen dat interventies niet uitgevoerd kunnen worden, langer duren en doelen niet gehaald worden.

- Het programma is voor een groot deel afhankelijk van subsidies. Indien er geen of onvoldoende subsidies beschikbaar zijn, kunnen sommige interventies niet starten. Via de Taskforce wordt regionaal en landelijk ingezet op het belang van aanjaagsubsidies.

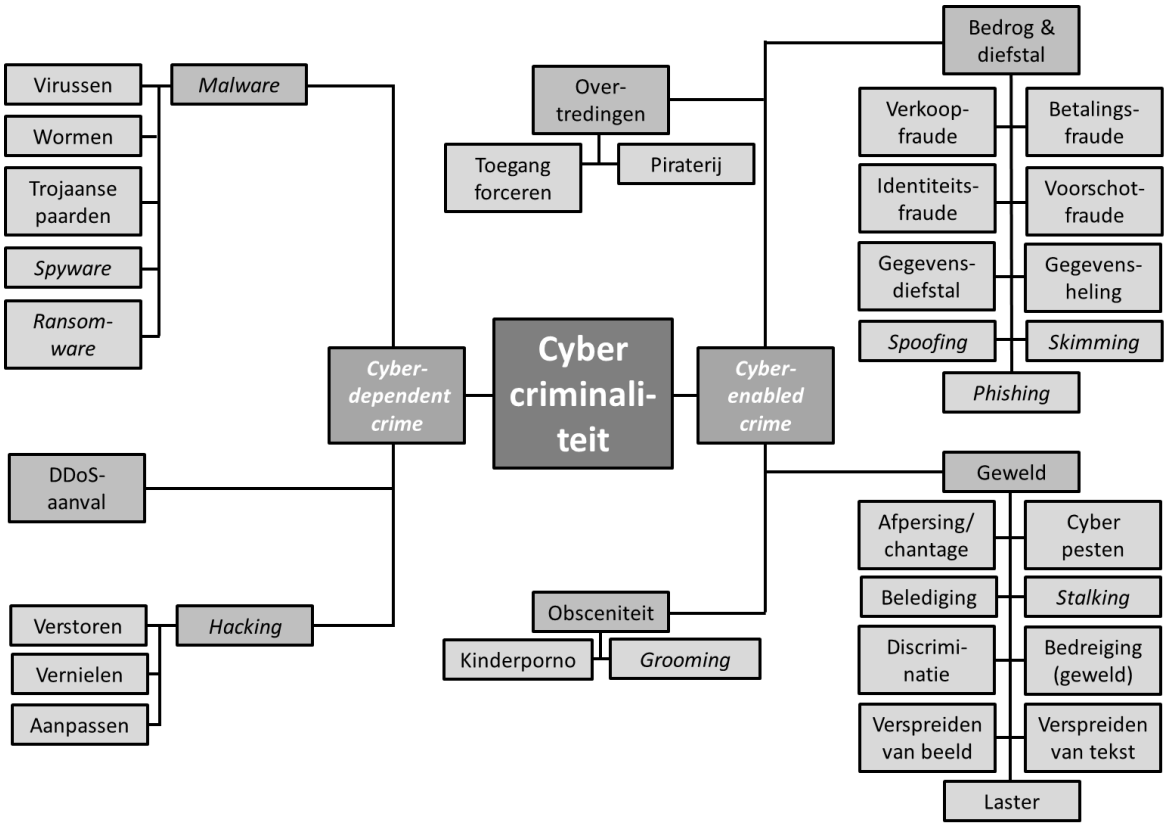
- Het programma heeft voortdurend koplopers nodig voor het omarmen van initiatieven of het bemiddelen daarin naar lokale maatschappelijke partners (scholen, verenigingen, bedrijven). Wanneer lokaal urgentiebesef ontbreekt, stokt de uitvoering van het programma. Om die reden geven we bij het begin van het programma prioriteit aan explorerende activiteiten en werken we met een aanjaagbudget.

Bijlage 1 Definities

Definitie cybercriminaliteit / digitale criminaliteit
Het gebruiken van het internet of andere computertechnologie ten behoeve van het faciliteren van criminaliteit of ander normoverschrijdend gedrag. Onder (I) *cyber-enabled criminaliteit* worden klassieke vormen van criminaliteit verstaan, die door middel van ICT op een grotere schaal kunnen worden uitgevoerd, zoals oplichting, identiteitsfraude en *phishing*. Onder (II) *cyber-dependent criminaliteit* wordt criminaliteit verstaan die wordt gepleegd door middel van ICT met ICT als doelwit, zoals hacks, DDoS-aanvallen, virussen, ransomware en andere malware. (Spithoven 2020, op basis van Kleve, De Mulder & Van Noortwijk, 2010; Holt & Bossler, 2013; Leukfeldt, 2016, 2018; Holt, Bossler & Seigfried-Spellar, 2018).

In dit programma gebruiken we in plaats van cybercrime de term 'digitale criminaliteit'. Dat sluit aan bij ons doel om het onderwerp 'normaler en toegankelijker' te maken.

Taxonomie cybercriminaliteit / digitale criminaliteit (Spithoven 2020, p. 49)



Definitie cyberweerbaarheid (Spithoven, 2020; Misana-ter Huurne et al., 2020)
De combinatie van een voldoende hoge mate van risicobewustzijn en zelfbeschermend gedrag onder burgers en ondernemers om slachtofferschap van cybercriminaliteit te voorkomen.

Overige definities [5]

Cyberspace ofwel onze digitale ruimte/omgeving	Onze digitale ruimte bestaat enerzijds uit een technologische grondlaag die randvoorwaardelijk is voor de interactie waardoor de sociale realiteit ontstaat die 'cyberspace' ofwel digitale ruimte wordt genoemd. Verder heeft cyberspace de volgende kenmerken: 1. Het heeft een sociale structuur die nauw is verweven met die van de offline wereld en is daarvan wel te onderscheiden maar niet te scheiden; 2. Ze beïnvloeden elkaar voortdurend en wederkerig. Mensen kunnen 'in cyberspace zijn' door handelingen te verrichten waarmee iets in cyberspace wordt vastgelegd, gebruikt, gewijzigd of geraadpleegd'.
Digitale veiligheid	Digitale veiligheid gaat over het beschermen van mensen en organisaties tegen iedere dreiging die voorkomt uit een digitale omgeving. Dat kan de dreiging zijn die uitgaat van cybercrime/ digitale criminaliteit, maar ook van de dreiging die uitgaat van een ontoereikende beveiliging van genetwerkte systemen (hardware en softwaredata)
Cybersecurity	Cybersecurity gaat over het beveiligen van genetwerkte systemen (hardware, softwaredata)

[5] Op basis van de definities van Stol en Litska Strikwerda (2017) en Het CCV.

Bijlage 2 Actoren

In deze bijlage worden de belangrijkste actoren in relatie tot digitale veiligheid genoemd. Het is geen uitputtend overzicht. Bij iedere actor wordt aangegeven welke benadering we voorstaan. Aan deze bijlage wordt eind 2020 een zogenaamd 'cyberlandschap' toegevoegd waarin het geheel van actoren en hun rollen en verantwoordelijkheden wordt omschreven.

Gemeenten, Politie en OM	De partners van de regionale veiligheidsstrategie hebben zich gecommitteerd aan de strategie 2019-2022 waarin de aanpak van digitale criminaliteit en onveiligheid als prioriteit is benoemd.
Benadering: iedere partner binnen de veiligheidsstrategie wordt ambtelijk en bestuurlijk meegenomen in de plannen en interventies met betrekking tot digitale veiligheid. Partners worden actief bevraagd regionaal of lokaal mee te werken aan interventies en experimenten of aan te geven waar men advies en ondersteuning nodig heeft. Hiervoor wordt een aanjaagbudget beschikbaar gesteld.	

Nationaal Cyber Security Center (onderdeel J&V). Wettelijke taak op grond van de wet beveiliging netwerk- en informatiesystemen (Wbni).	Duiden van (internationale) dreigingen en kwetsbaarheden in digitale domein / verbinden partijen, kennis en informatie tussen nationale en internationale partners / advisering en handelingsperspectief. Bekend van o.a. de campagne Alert Online of via de website veiligeinternetten.nl en het Digital Trust Center (DTC) dat ondernemers helpt met veilig digitaal ondernemen. Op landelijk niveau heeft het NSCS de IRB die adviseert aan de nationale crisisteams. Voor de gemeenten is ook de IBD een belangrijke schakel. Op het moment dat een andere partij dan de gemeente is getroffen door een cyberverstoring, dan is deze partij zelf verantwoordelijk voor de melding aan nationaal niveau. In het geval van een vitale sector geldt een meldplicht richting het NCSC. In andere gevallen kan de verstoring gemeld worden bij de CERT (Computer Emergency Response Teamvan deze sector (bijvoorbeeld de Z-CERT voor ziekenhuizen). Dit CERT zal dit vervolgens doormelden aan het NCSC. Het NCSC is ook betrokken bij het Nationaal Crisisplan ICT.
Benadering: betrekken in interventies gericht op doelgroep ondernemers. Materiaal gebruiken we voor lokale campagnes. Het cybersecuritybeeld dat jaarlijks verschijnt, betrekken we binnen de programmalijn 'exploreren'.	

Informatie Beveiligingsdienst (IBD)	De IBD is de partij die voor de gemeente een goed overzicht heeft van het betrokken netwerk en die kan ontsluiten, de gemeente kan adviseren, etc. De rol die het NCSC heeft voor de Vitale infrastructuur heeft de IBD voor gemeenten. De IBD monitort op algemene dreigingen die relevant zijn voor gemeenten en informeert gemeenten wanneer nodig met gericht advies om deze dreigingen tegen te gaan. Op basis van informatie van gemeenten stuurt de IBD dagelijks actuele kwetsbaarheidswaarschuwingen over de hardware, software en systemen die de gemeente in gebruik heeft. De gemeente kan in geval van een cyberincident contact opnemen met de CERT (Computer Emergency Response Team) van de IBD. De IBD is het aanspreekpunt voor gemeenten in geval van een incident dat te maken heeft met informatiebeveiliging. De IBD zou kunnen worden gezien als de CERT van de gemeente.
Benadering: betrekken in netwerkbijeenkomsten ciso's en adviseurs openbare orde en veiligheid.	

Veiligheidsberaad/ Veiligheidsregio's	Het Veiligheidsberaad bestaat uit de voorzitters van de 25 veiligheidsregio's die met elkaar van gedachten wisselen over strategische en integrale veiligheidsvraagstukken en -ontwikkelingen van nu en in de toekomst. Van de evaluatie van de Wet veiligheidsregio's tot aan cyber security en de rol van de veiligheidsregio's. Begin 2020 wordt het bestuurlijk routeboek digitale ontwrichting verwacht ten behoeve van de crisisorganisatie. In de handreiking worden meerdere scenario's uitgewerkt waarin cyberincidenten leiden tot ontwrichting op lokaal, regionaal en landelijk niveau. Tevens worden er netwerkkaarten in opgenomen.
Benadering: betrekken in netwerk ciso's en adviseurs openbare orde en veiligheid. Bespreken bestuurlijk routeboek cybergevolgbestrijding op netwerkbijeenkomsten waar we ook de veiligheidsregio's in betrekken.	

De Cybersecuriy Alliantie (publiek-privaat)	De CS Alliantie biedt een onafhankelijk netwerk en platform voor publiek-private samenwerking op het gebied van cybersecurity. Dat betekent dat de uitvoering van de projecten niet afhankelijk is van één partij. Iedereen kan zich verbinden aan de CS Alliantie en een project aanmelden. De CS Alliantie faciliteert concrete kortlopende projecten die maximaal negen maanden duren. Daarnaast geeft de CS Alliantie inzicht in lopende projecten in het Nederlandse cybersecuritylandschap.
Benadering: De alliantie schetst het cybersecuritylandschap wat op zich waardevolle inzichten geeft. Zoals informatie over het Nederlands Cyber Collectief met veel initiatieven en verhalen die gedeeld kunnen worden (zoals het cyberwoordenboek en het dagboek van een hacker). De alliantie houden we in het achterhoofd i.v.m. publiek-private interventies die niet voor reguliere subsidies in aanmerking komen.	

Defensie (DEFCERT)	Digitale systemen spelen een steeds grotere rol bij inlichtingen en veiligheid. Daarom gaat de krijgsmacht ook dreigingen in de digitale omgeving (cyberspace) aanpakken. Naast de zee, het land, de lucht en de ruimte is cyberspace daarmee het 5e werkgebied van de krijgsmacht. Het ministerie van Defensie zet hiervoor onder meer het Computer Emergency Response Team (DefCERT) dat ook civiele autoriteiten kan ondersteunen bij de coördinatie van cyberdreigingen. Er is nauwe samenwerking met o.a. het NCSC.
Benadering: zie NSCS	

VNG (commissie digitalisering)	De commissie digitalisering en informatiebeleid richt zich op een goede informatievoorziening en een goede informatiestructuur waardoor gemeenten de dienstverlening aan inwoners en bedrijven kunnen optimaliseren. Informatieveiligheid en innovatie hebben daarin een belangrijke plaats. Ook in relatie tot openbare orde en veiligheid. Recentelijk is bijvoorbeeld de cybergame openbare orde en informatieveiligheid gelanceerd die in principe door alle gemeenten gespeeld kan worden. Op dit moment wordt ook gewerkt aan een agenda digitale veiligheid 2020 gericht op informatiebeveiliging, digitale criminaliteit en de omgang met cyberincidenten
Benadering: we informeren de VNG over de programma's en activiteiten en de knelpunten die we ervaren in de regionale en lokale aanpak van digitale onveiligheid	

NSCR en Cybersciencecenter	NSCR: Onderzoeksproject INTERSECT. Consortium van private en publieke partijen dat onder leiding van de TU Eindhoven onderzoek doet naar het veiliger maken van het Internet of Things. Cybersciencecenter: Het cyber science-center biedt een overzicht van lopende en reeds afgeronde wetenschappelijke onderzoeken. https://cybersciencecenter.nl/ Ook het Centraal Planbureau, TNO, de WRR, het CBS, het WODC en Politie en Wetenschap publiceren regelmatig over digitale veiligheid.
Benadering: onderzoek vormt de legitimiteit voor ons programma en de interventies. We stellen ons van onderzoeken op de hoogte en vragen onderzoekers een bijdrage te leveren voor netwerkbijeenkomsten, conferenties etc.	

Hogescholen	De Haagse Hogeschool en Saxion Hogescholen gaan met diverse gemeenten en regionale veiligheidsverbanden praktijkgericht onderzoek doen naar de risicoperceptie van cybercrime en het ontwerpen van werkzame interventies. Een subsidie hiervoor is toegekend (Raak-publiek) Met de Hogeschool Utrecht wordt samengewerkt in het kader van een promotieonderzoek naar: het gebruik van big data door professionals in het sociaal veiligheidsdomein en hoe publieke waarden daarin te wegen (proefschrift periode 2020-2024)
Benadering: actieve samenwerking. Gemeenten in de regio benaderen om interventies voor het onderzoek aan te melden (via oov en burgemeesters).	

Ministerie (J&V) en (BZK)	Er is 1 miljoen euro beschikbaar gesteld voor projecten van digitale veiligheid voor zowel de G4 als de G40-steden. Er zijn daarnaast incidenteel subsidies (citydeal) beschikbaar voor innovatieve interventies gericht op diverse doelgroepen. Verder heeft het Ministerie van Justitie en Veiligheid via het CCV subsidies verstrekt aan het platform veilig ondernemen (dat onder de paraplu van bureau RVS werkt) om op lokaal niveau de weerbaarheid van het MKB een impuls te geven.
Benadering: Ministeries op diverse niveau's informeren over het programma digitale veiligheid, o.a. via Taskforceleden. Tevens het Ministerie op de hoogte brengen van de regionale en lokale ervaringen/knelpunten in de aanpak en de noodzaak van aanjaagsubsidies in plaats van alleen innovatiesubsidies om de lokale aanpak van digitale onveiligheid en criminaliteit te borgen. Verder doen we mee met subsidieaanvragen en leggen we in het kader van 'weerbare medewerkers en informatiebeveiliging' meer dan nu de verbinding met BZK.	

Het CCV.	Het CCV biedt kennisproducten en ondersteuning ten aanzien van diverse veiligheidsvraagstukken, waaronder ook digitale veiligheid (connected cyber cities).
Benadering: samenwerking en afstemming van activiteiten en aanbod richting gemeenten.	

Halt	Halt houdt zich bezig met beginnende jeugdcriminaliteit. Steeds vaker vindt deze jeugdcriminaliteit online plaats, zoals ongewenste sexting, online pesten en cybercrime
Benadering: betrekken bij interventies. Inzetten op aandacht voor digitale criminaliteit in de preventiecontracten bij gemeenten en bij alternatieve interventies (Hacklight en Hackright).	

Bijlage 3 Impact Digitalisering

Werken aan digitale veiligheid vraagt inzicht in de werking en invloed van digitalisering. Het Rathenau-Instituut schetst hoe digitalisering onze wereld beïnvloedt op zowel materieel, biologisch en sociaal-cultureel gebied. Dit is al tientallen jaren aan de gang, maar het is recent wel makkelijker geworden 'om op steeds gedetailleerder niveau, real-time te interveniëren in de fysieke wereld'. Dat betekent dat processen in de fysieke wereld worden gemeten, dat de hieruit voortkomende data wordt geanalyseerd, en dat er vervolgens real-time op gedetailleerd niveau wordt ingegrepen. Het effect van de interventie kan vervolgens weer worden gemeten, geanalyseerd en worden bijgesteld'. In deze bijlage zien we hoe dat ons leven beïnvloedt, of beter gezegd, stuurt (Rathenau, 2019, p.33-43) en welke vraagstukken dat oplevert.

Onze openbare ruimte. 'De slimme stad'. Via allerlei sensoren kunnen overheden, bedrijven en bewoners gedetailleerd inzicht krijgen in processen in de stad. De slimme stad belooft een duurzame en comfortabele leefomgeving zonder files, energieverspilling of ongure steegjes. 'Slim' in deze context betekent dat ICT – software, sensoren en het internet – een digitale laag over de stad heen legt. Deze laag zorgt voor continue gegevensstromen, waarmee gemeenten gedrag van bewoners, verkeersdeelnemers of inbrekers kunnen monitoren of (bij)sturen. Een mogelijke toepassing is bijvoorbeeld een slimme lantaarnpaal die zelf bepaalt wanneer hij aan gaat, met lichtkleuren de gemoedstoestand van voorbijgangers kan beïnvloeden en mogelijk agressie kan voorkomen, en met camera's voorbijkomend verkeer monitort.

Ons huis. Via het Internet of Things (IoT) krijgen allerlei huishoudelijke apparaten een internetadres. Ze worden 'aan het net' gehangen en krijgen sensoren, rekenkracht en communicatiemogelijkheden. Voorbeelden hiervan zijn slimme thermostaten die verbonden zijn met de energieleverancier en digitaal inzicht bieden in ons energieverbruik ten opzichte van anderen, of een slimme TV die ons kijkgedrag analyseert en ons op basis daarvan tips voor andere programma's geeft. Ook Barbie heeft inmiddels een microfoon en een internetverbinding.

Ons lichaam en ons gedrag. De huidige generatie smartphones en apps bieden hulp aan mensen om zelf hun bloeddruk, glucose, hartslagvariabiliteit en stressreacties te monitoren. Van toekomstige generatie digitale coachingsapparaten wordt verwacht dat ze met behulp van kleinere en betere sensoren de psychofysiologische staat van gebruikers voortdurend kunnen monitoren. Wetenschappers en bedrijven weten dat er allerlei informatie uit ons digitale surfgedrag valt af te leiden. Dit komt door de combinatie van de aanwezigheid van grote hoeveelheden digitale, gegevens te analyseren. Facebookprofielen geven bijvoorbeeld informatie over seksuele geaardheid of politieke voorkeuren. Watson van IBM heeft genoeg aan een A4'tje tekst om een persoonlijkheidsanalyse van de auteur te maken.

Onze sociaal-culturele omgeving. Digitalisering dringt door in ons sociale en culturele leven: shoppen, muziek luisteren, contact met vrienden, actie voeren, het vinden van dates doen we in toenemende mate online. We vergroeien met onze smartphone, die dé verbinding vormt tussen het fysieke en virtuele leven. Floridi et al. (2014) kenmerken dit als onlife: het onderscheid tussen offline en online leven is niet meer te maken; ze zijn één geworden. Recente ontwikkelingen in *virtual reality* en *augmented reality* dragen ook bij aan deze versmelting. Via *virtual reality* (VR) kunnen gebruikers virtuele ervaringen 'echter' of beter voelen. Gamemakers passen de techniek toe om gamers meer op te laten gaan in hun spel. Ook andere domeinen maken gebruik van VR, zoals de zorg voor het revalideren van een lichamelijke handicap of in het leger om militairen te trainen. Via *augmented reality* (AR) kunnen gebruikers real-time extra informatie krijgen. Vanaf 2010 ontstaan er radicale nieuwe organisatievormen door digitale platformen. Voorbeelden zijn Airbnb en Uber. Het gaat om exponentiële organisaties die zo min mogelijk vaste medewerkers en zo veel mogelijk personeel op afroep willen hebben, optimaal gebruikmaken van de gratis diensten van een digitale gemeenschap, maximaal gebruikmaken van geautomatiseerde algoritmen en zo min mogelijk kapitaalgoederen in eigen bezit hebben. En blockchaintechnologie maak het mogelijk autonome organisaties te ontwikkelen: organisaties die volledig uit bits en bytes bestaan. De technologie kan een set van afspraken en taken automatiseren en zo de functie van een bepaalde organisatie overnemen. O.a. cryptomunten zijn op deze technologie gebaseerd.

Onze digitale omgeving. De omvang van de digitale wereld is exponentieel gegroeid en lijkt zijn eigen 'wet van Moore' te kennen: elke twee tot drie jaar verdubbelt de hoeveelheid data (Mayer-Schonberger & Cukier 2013b; IDC 2014); een fenomeen dat inmiddels bekend staat als 'big data'. De data zijn bijvoorbeeld afkomstig van camera's, smartphones, tablets en andere draagbare apparaten, of van browsers en sociale netwerken. Die almaar uitdijende digitale wereld betekent ook dat we steeds afhankelijker zijn van slimme algoritmen (software) om informatie te halen uit alle bits en bytes. Dataverzamelingen en data-analyses worden steeds complexer van aard. Bedrijven en overheden zetten (zelflerende) software vaker in om processen efficiënter te laten verlopen, bijvoorbeeld op de beurs, bij het verstrekken van krediet, bij het opsporen van fraude, of bij het reguleren van content op sociale media. En naarmate software vaker automatisch beslissingen neemt, neemt het belang van controle op die systemen toe.

Thema	Vraagstukken
Privacy	Gegevensbescherming, privacy, digitaal huisrecht, mentale privacy, surveillance, doelverschuiving
Autonomie	Keuzevrijheid, vrijheid van meningsuiting, manipulatie, paternalisme
Veiligheid	Informatieveiligheid, identiteitsfraude, fysieke veiligheid
Controle over technologie	Controle en inzicht in algoritmen, verantwoordelijkheid, onvoorspelbaarheid
Menselijke waardigheid	Dehumanisatie, instrumentalisering, *de-skilling*, de-socialisatie, werkeloosheid
Rechtvaardigheid	Discriminatie, uitsluiting, gelijke behandeling, stigmatisering
Machtsverhoudingen	Oneerlijke concurrentie, uitbuiting, relatie consument-bedrijf

Rathenau Instituut

Bijlage 4 Begroting 2020

Personeel

Programmamanager Digitale Veiligheid	Personeelsbudget RVS
Projectleider Digitale Veiligheid	Personeelsbudget RVS

Programma

Netwerkbijeenkomsten / Masterclasses (exclusief bestuursconferenties)	€5000,-	Projecten RVS
Aanjaagbudget lokale initiatieven (o.a. voor promotie en faciliteren bijeenkomsten/campagne en promotiematerialen)	€10.000,-	Projecten RVS
Interventies Ondernemers	€11.000 -€50.000	Afhankelijke van subsidie lokale weerbaarheid digitale criminaliteit
Interventies Medewerkers	pm	Afhankelijk van subsidie[6]
Podcastserie Digitale Veiligheid	€35.000	Subsidie J&V
Onderzoek cyberweerbaarheid gemeenten door onderzoeksconsortium Saxion/Haagse Hogeschool, NSCR, gemeenten en regio's	€300.000 €300.000 →	Subsidie Raak-publiek Uren partners consortium

[6] In deze programmaperiode onderzoeken we met o.a. het ministerie van BZK de mogelijkheden hiervoor.

Bijlage 5 Mindmap Eigen Huis op Orde VNG