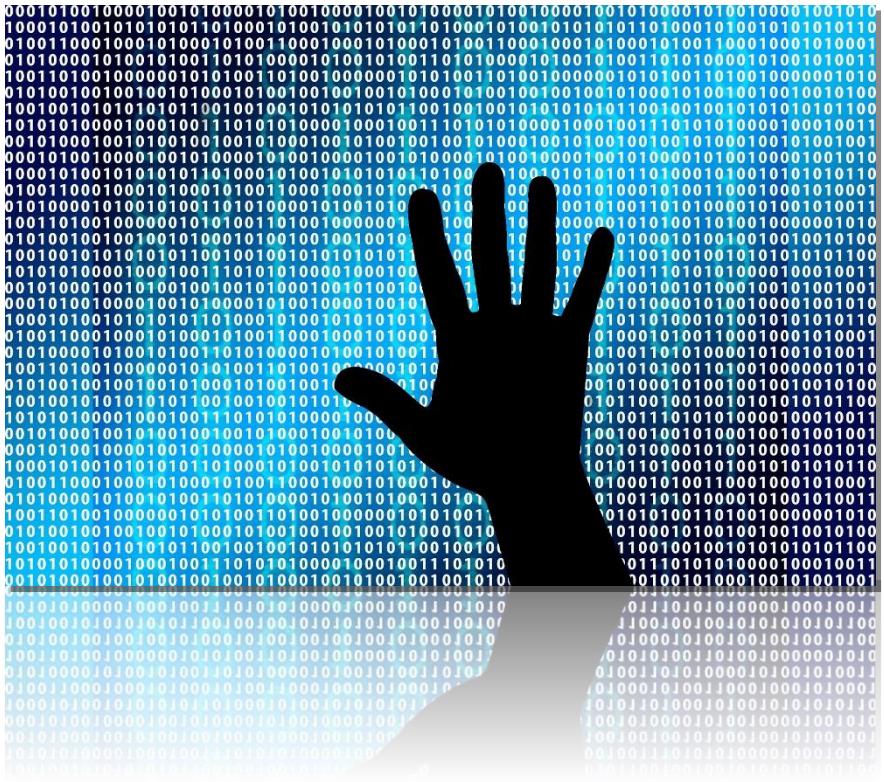
Uitvoeringsprogramma
Digitale Veiligheid
Regio Rotterdam

2025-2027



“Inwoners, ondernemers en organisaties weerbaar in een gedigitaliseerde wereld”

Inleiding

Onze samenleving digitaliseert steeds meer, wat grote voordelen biedt zoals efficiëntere processen en tijdsbesparing. Echter, deze digitalisering maakt ons ook afhankelijk van systemen en hun ontwikkelaars. De verwevenheid van systemen betekent dat een kwetsbaarheid in één onderdeel grote gevolgen kan hebben voor het hele systeem. Cyberincidenten en beïnvloeding vanuit andere landen kunnen ernstige effecten hebben op meerdere organisaties en groepen in de samenleving.

De toenemende digitalisering van de samenleving maakt het voor kwaadwillenden makkelijker om criminele delicten te plegen, zoal in de vorm van digitale criminaliteit en online norm-overschrijdend gedrag." Dit veroorzaakt aanzienlijke schade, variërend van economische verliezen tot bedreigingen voor de nationale veiligheid.

Slachtofferschap
In 2023 werden 2,3 miljoen Nederlanders getroffen door een vorm van online criminaliteit. De impact op slachtoffers is groot. Mensen en bedrijven lijden financiële schade, maar het tast ook het vertrouwen in elkaar aan. En het beïnvloedt het vertrouwen in de digitale infrastructuur.

De impact van slachtoffers van online fraude blijft niet beperkt tot financiële schade. Uit verschillende onderzoeken blijkt dat de impact van online criminaliteit niet onderdoet voor die van traditionele criminaliteit en in sommige opzichten zelfs groter is.

Slachtoffers zijn bovendien niet altijd bereid om aangifte te doen, bijvoorbeeld uit schaamte omdat ze het gevoel hebben dat ze er zelf in zijn getrapt. Als gevolg hiervan blijft de opsporing van online criminaliteit lastig vanwege een gebrekkige informatiepositie.

Samenwerken bij de aanpak
Brede bestrijding van cybercrime draait om opsporing en vervolging, maar ook om het tegenhouden van criminaliteit (verstoring), het beperken van schade en het voorkomen van dader- en slachtofferschap (preventie). Er zijn veel publieke en private partijen actief op het thema digitale veiligheid. De verantwoordelijkheid voor de opsporing en vervolging van strafbare feiten ligt bij de Politie en het OM. De burgemeester is verantwoordelijk voor de openbare orde en veiligheid. De gemeenten hebben een rol bij bewustwording en preventie en nazorg van slachtoffers.

De afgelopen jaren werkten politie, Openbaar Ministerie, VeiligheidsAlliantie regio Rotterdam (VAR), gemeenten samen met publiek-private partijen aan een integrale aanpak veelvoorkomende gedigitaliseerde criminaliteit. In het uitvoeringsprogramma 2025-2027 zetten we in op een nog bredere aanpak op meerdere thema's.

Cyber vraagt pionieren

Als burgemeester in deze tijd kun je niet om cyber, de digitale wereld, heen. Een digitale wereld, die voortdurend nieuwe mogelijkheden en producten oplevert, waaraan niet te ontkomen is. In onze veeleisende rol als burgemeester van een gemeente, levert het heel veel efficiency en effectiviteit op, door daar gebruik van te maken. En het is vanuit de gezagsrol over politie en veiligheid een noodzaak geworden.
Het begint al met je agenda, je vergaderstukken en digitale meetings. Alles vergt digitale skills en tijd met digitale devices en media. Dat is soms stevig leren en proberen, want gewend zijn we er van vroeger uit niet aan. Het adagium "leven lang leren" doet hier zeker opgeld. Telkens zijn er nieuwe ontwikkelingen, die nieuwe vaardigheden vragen. Nieuwste loot aan de digitale stam is het gebruik van artificial intelligence, bijvoorbeeld via ChatGPT, op je smartphone of iPad. Een adequate en snelle naslag op alle mogelijke onderwerpen, is voor ons als burgemeesters daarmee supersnel en makkelijk beschikbaar. Hoe doe je dat in je dagelijks werk? En wat zijn naast mogelijkheden ook de risico's?
Communiceren op straat, in de raadzaal of via media is logisch en een belangrijk onderdeel van het burgemeesterswerk. Het doel is naast informeren vaak ook verbinding, vertrouwen en veiligheid creëren. Communicatie via social media heeft de mogelijkheden en het bereik enorm vergroot. Het levert vragen op als welke sociale media kies je, met welk doel op welk moment, en hoe combineer je beeld/geluid en tekst. Daar bestaan nog geen vaste patronen of regels. Ook de ambtenaren moeten dat leren en ervaren.
Daarnaast betekent veilig leven voor je bewoners ook veiligheid in de digitale activiteiten en plaatsen. Het grote aantal slachtoffers van digitale criminaliteit en de impact die het slachtofferschap heeft, maakt dat in steeds meer gemeenten digitale criminaliteit in de hoogste prioriteit is geplaatst in de veiligheidsplannen. Het betreft een divers samenstel van delicten als online-pesten, afpers-hackers, babbeltrucs-pincodes, sextortion, marktplaatsfraude, enzovoort. In de aanpak kiest menige burgemeester voor een pittige combinatie van preventieve maatregelen en repressieve aanpak. Wat doet de gemeente zelf, welke experts kunnen worden benut, welke inzet pleegt de politie in de aanpak, is er recherche capaciteit voor opsporing? Deze vragen komen meer en meer op tafel bij de burgemeester en de veiligheidsdriehoek.
In al die rollen en taken zijn er geen bestaande routines of instructies. Als die er waren, worden ze ook heel snel ingehaald door weer nieuwe toepassingen of aanpassingen. Daarom vraagt het zijn van burgemeester in cyber, wat we allemaal per definitie ook zijn, een pionierende instelling. Niet bevreesd iets te proberen, accepteren dat iets ook wel eens minder goed kan uitpakken, genieten van een geslaagde activiteit! Maar vooral het accepteren van cyber als onlosmakelijk onderdeel van onze taak.

Bert Wijbenga – van Nieuwenhuizen,
Burgemeester van Vlaardingen en voorzitter Cyberburgemeesters Nederland

'In al die rollen en taken zijn er **geen bestaande routines of instructies'**

Column Burgemeestersblad, december 2024

Regionale ambitie

Het regionaal uitvoeringsprogramma is ingericht op de onderstaande vier thema's. Het programma heeft zowel een duurzaam als een dynamisch karakter. Er is een koers die tussentijds kan worden aangescherpt en/of bijgesteld. Voor deze aanscherping is het zaak om voortdurend de voortgang te monitoren en periodiek te besluiten over bijstelling van het actieplan en daarmee de inzet van de partners voor de verschillende maatregelen. Daarmee behouden we ruimte om mee te bewegen met landelijke en regionale ontwikkelingen en waar gewenst lokaal maatwerk toe te passen. Daarnaast gaan ontwikkelingen rondom digitale criminaliteit enorm snel. Om hierop in te spelen, zullen wij jaarlijks kijken welke thema's prioriteit moeten krijgen.

Het is tenslotte belangrijk om aandacht te hebben voor de samenhang met overlappende aanpakken, programma's en beleidsterreinen en daar waar mogelijk de krachten regionaal en landelijk te bundelen. Denk daarbij aan het programma Preventie met Gezag en Mensenhandel (criminele uitbuiting) en Maatschappelijk Ongenoegen.

In dit uitvoeringsprogramma staat hoe we in de periode 2025 – 2027, samen met 23 gemeenten, politie en Openbaar Ministerie, VAR, PVO en andere ketenpartners in de regio Rotterdam, aan digitale veiligheid willen werken, met als ambitie:

Digitale criminaliteit:
- Het voorkomen, verstoren en bestrijden van digitale criminaliteit.
- Het versterken van de digitale weerbaarheid van inwoners en ondernemers.
- (Potentiële) plegers bewust maken van de risico's en gevolgen van hun onlinegedrag voor zichzelf en de maatschappelijke impact die dat online gedrag kan hebben.
- Daders aanpakken en duurzame barrières opwerpen.

Cybercrisis en -incidentbeheersing:
- Voorbereid zijn op digitale ontwrichting.

Eigen huis op orde:
- Eigen organisatie en digitale infrastructuur beschermen tegen bedreigingen.

Digitaal weerbare democratie:
- Handelingsperspectief bij online aangejaagde ordeverstoringen
- Voorbereid zijn op ongewenste buitenlandse beïnvloeding in de digitale wereld/statelijke dreigingen
- Betrouwbare en transparante informatiebron zijn voor inwoners.
- Desinformatie actief bestrijden door middel van educatie, samenwerking met lokale en nationale partners, en het bevorderen van mediawijsheid.

Organisatie

RVO

- Opdrachtgever met regionaal portefeuillehouder Digitale Veiligheid: burgemeester Wijbenga- van Nieuwenhuizen.

Stuurgroep Digitale Veiligheid

- De stuurgroep onder voorzitterschap van de regionaal portefeuillehouder bestaat uit: Programma-managers digitale transformatie OM en Politie, Adjunct directeur directie veilig gemeente Rotterdam, hoofd VAR en adviseur regioburgemeester.

Projectteam Digitale Veiligheid

- Vertegenwoordigers vanuit Politie, OM, VAR, PVO en gemeente Rotterdam.

Werkgroepen thematisch

- Thematische werkgroepen met deelnemers vanuit het publiek-private netwerk.

Netwerk Digitale Veiligheid

- Netwerk van aandachtsfunctionarissen Digitale Veiligheid.
- Optioneel sluiten de digitale wijkagenten aan

Financiën

De politie, OM, VAR, PVO en gemeente Rotterdam leveren capaciteit voor het projectteam en de thematische werkgroepen.

Vanuit de VAR wordt met financiering vanuit de Citydeal Cyberweerbaarheid 0,5 fte ingezet met een regionale projectleider, die een aanjaag- en ondersteunende rol heeft richting de gemeenten. Deze financiering loopt vooralsnog tot 1-1-2026. Er wordt samen met het Platform Cyberburgemeesters een lobby ingezet voor continuering van deze middelen.

Binnen de reguliere begrotingen zijn middelen opgenomen voor de uitvoering van projecten. Ook wordt gebruik gemaakt van incidentele subsidies.

Monitoring en evaluatie

We zetten veelal preventieve interventies in. Preventie leidt tot meer bewustwording en dat zorgt ervoor dat inwoners en ondernemers sneller en vaker (digitale) incidenten melden. De meldingsbereidheid is o.a. door schaamte erg laag, waardoor er sprake is van een groot ‘dark number’. We zetten in op de verhoging van de meldingsbereidheid.

We evalueren het uitvoeringsprogramma digitale veiligheid op proces en effect. We kijken tijdens de procesevaluatie naar de uitgevoerde acties en de planning. Daarnaast wordt met gemeenten (CISO en OOV-adviseur) jaarlijks een thermometer-gesprek gevoerd, waarbij op de verschillende thema’s de aanpak door de gemeenten wordt geëvalueerd.

Bij de effectevaluatie kijken we naar de bereikte effecten. Hebben we met de ingezette interventies bereikt wat we wilden bereiken? En wat zijn de resultaten van landelijke monitoren op het thema?

Met ondersteuning van het kenniscentrum van de gemeente Rotterdam wordt de vorm van monitoring en evalueren nog verder uitgewerkt.

Algemeen

Er zijn een aantal activiteiten die alle thema's betreffen die verderop in dit uitvoeringsprogramma staan. Hieronder een overzicht. Daarna volgt een overzicht per thema.

	Actie	Planning	Wie
1	Faciliteren/aanjagen regionaal netwerk digitale veiligheid	Doorlopend	VAR
2	Uitvoering programmaplan digitale transformatie interne organisatie	Doorlopend	Politie/OM
3	Faciliteren netwerk digitaal wijkagenten	Doorlopend	Politie/VAR
4	Voorzitterschap/secretariaat landelijk platform cyberburgemeesters	Doorlopend	Portefeuillehouder/VAR
5	Delen (landelijke) relevante onderzoeken/ rapporten via kennisbank van de VAR.	Doorlopend	VAR
6	Agenderen trends en ontwikkelingen via leerhuizen en kennisbijeenkomsten (3x per jaar een netwerkbijeenkomst)	Doorlopend	VAR
7	Faciliteren digitale community thema Digitale Veiligheid via website VAR	Doorlopend	VAR
8	Delen goede voorbeelden lokaal uitvoeringsplan digitale veiligheid	2025	VAR
9	Opstellen lokaal uitvoeringsplan digitale veiligheid	2026 (uiterlijk)	Gemeenten
10	Onderzoek naar verbeteren online nabijheid politie: Actieonderzoek op een basisteam en daarmee een bijdrage leveren aan de vraag wat precies de rol van de politie is op het internet/in de internetsamenleving en hoe die wordt vormgegeven.	2025	Politie

Digitale criminaliteit

Weerbare inwoners en ondernemers

Inwoners, ondernemers en organisaties worden beter geïnformeerd door gemeenten, Politie en andere partijen op de gevaren van gedigitaliseerde criminaliteit, maar we zijn er nog niet. Daarnaast zien wij ook dat er nieuwe criminaliteitsvormen ontstaan zijn waar burgers en bedrijven alert op moeten zijn. Niet iedereen past de basismaatregelen toe, zoals het gebruik van unieke wachtwoorden en multifactor-authenticatie (twee of meer methodes gebruiken om toegang te krijgen tot een onlineapplicatie). Het is van belang dat inwoners en ondernemers beter weten waarop ze moeten letten en wat ze wel of juist niet moeten doen.

De regionale aanpak richt zich op het bewuster en weerbaarder maken van burgers en bedrijven om de werkwijzen die leiden tot gedigitaliseerde criminaliteit tijdig te herkennen en (herhaald) slachtofferschap te voorkomen. Daarnaast richten we de aanpak ook op daderpreventie. Dit wordt bereikt door het breder inzetten van kansrijke bestaande initiatieven, bredere uitrol van ´best practices´ en daar waar nodig ontwikkelen van nieuwe campagnes en initiatieven.

(Jonge) plegers

De regionale aanpak richt zich verder op het bewust maken van jongeren van de risico's en gevolgen van hun onlinegedrag. Met als doel hen veerkrachtig te maken en een handreiking te geven, wanneer zij (onbewust/onbedoeld) dader dreigen te worden van een onlinedelict of ander schadelijk onlinegedrag. Jongeren kunnen via uitbuiting verzeild raken in digitale criminaliteit zoals sextortion of geldezel zijn, waardoor ze dader, maar tegelijkertijd ook slachtoffer zijn. Er wordt ingezet om (herhaald) daderschap tot een minimum te beperken, bijvoorbeeld binnen het programma Preventie met Gezag.

Georganiseerde misdaad

Criminelen stappen steeds vaker in de digitale criminaliteit. Het criminele verdienmodel ligt meer en meer in digitale criminaliteit en de pakkans is klein. Volgens het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) en het Openbaar Ministerie wordt het merendeel van digitale criminaliteit veroorzaakt door ondermijnende, georganiseerde misdaad. Digitale criminaliteit is een belangrijk werkterrein van traditionele criminele organisaties geworden, die digitaal afpersen of gestolen informatie verkopen en misbruiken. Er zijn nieuwe netwerken van online daders bijgekomen die een technische specialisatie hebben. Deze specialisatie verkopen ze, waardoor voor andere criminelen slechts een basis technische kennis voldoende is. Onderling kopen en verkopen ze cybercrimediensten en -toolkits via illegale marktplaatsen op het darkweb (het zogenaamde Cybercrime-as-a-service). Ook delen criminelen bijvoorbeeld op fora en Telegramkanalen werkzame aanpakken. Daarnaast zien we dat drugs-gerelateerde criminaliteit en digitale criminaliteit meer en meer met elkaar verweven zijn geraakt. Criminelen plegen cyberdelicten, vaak in combinatie met drugsdelicten en/of wapenbezit. Verdachten worden opgespoord en zo mogelijk vervolgd.

	Actie	Planning	Wie
1.	Delen en ondersteunen bij inzet van interventies voor de verschillende doelgroepen (zie bijlage 2)	Doorlopend	VAR/PVO
2.	Delen (landelijke) relevante onderzoeken/ rapporten via kennisbank van de VAR.	Doorlopend	VAR
3.	Landelijke voorlichtingscampagnes vanuit het programma Online Fraude worden met handelingsperspectief gedeeld met gemeente, politie en andere partners in het regionale netwerk.	Doorlopend	VAR
4.	Vroegtijdig signaleren en uitwisseling informatie over modus operandi en trends.	Doorlopend	Politie/OM/NVB/CION
5.	Zicht op aard en omvang via dashboard “Zicht op cyber”.	Doorlopend	Landelijke kerngroep Online Fraude/CBS
6.	Onderzoek schaalvergroting project Rotterdam_Protected naar andere gemeenten		VAR/Politie/Eset/Sparta/Gemeenten
7.	Bespreken cyberbeelden in lokale driehoek en Districtelijk Veiligheidsoverleg.	Jaarlijks	Politie/OM/gemeenten
8.	Online platform voor regionale kennisuitwisseling en samenwerking (community via website VAR)	Doorlopend	VAR/regionaal netwerk digitale veiligheid
9.	Inzicht in mogelijke barrières en technische interventies om fraude te voorkomen.	Doorlopend	Politie/OM/samenwerkingsvormen passend bij fraudevorm
10.	Periodieke informatie/rapportage over ontwikkelingen en resultaten op het gebied van opsporing en vervolging.	Jaarlijks	Politie/OM
11.	Vergroten meldings- en aangiftebereidheid: Online aangifte mogelijk voor burgers voor alle fraudevormen. Gemeenten ondersteunen daarbij met communicatie en campagnes.	2025/2026	Politie/gemeenten
12.	Vergroten meldingsbereidheid: Inrichting online aangifteloket voor gemeenten en ondernemers.	2025/2026	Politie (landelijk met regionale afspraken)
13.	Bevorderen alternatieve afdoening via o.a. het project Cease and desist.	Doorlopend	Politie/OM
14.	Verbetering ondersteuning slachtoffers: inzet Digitale Meldkamer.		Politie/slachtofferhulp
15.	Organiseren actiedag “Echt niet vandaag”	Jaarlijks	Regionale projectgroep/publiek-private partners
16.	Lancering van de vernieuwde film Echt of Nép met toegevoegde digitale criminaliteitsvormen (Aan- en verkoopfraude, Relationele beleggingsfraude en Stem nabootsing)	2025	CCV/VAR
17.	Implementatie en bekendheid online-aangiftemogelijkheid voor bedrijven, de zogeheten ‘mijnpolitiezakelijk’-omgeving.	2025	Politie/PVO
18.	Organiseren netwerkbijeenkomst Geldezels	2025	VAR
19.	De mogelijkheid onderzoeken van een campagne via Meld Misdaad Anoniem (MMA)	2026	Politie
20.	Betrekken scholen bij de aanpak: er worden goede voorbeelden van lespakketten gedeeld.	2025/2026	VAR/gemeenten
21.	Onderzoeken inzet interventie storytelling slachtoffers: slachtoffer spreekt.	2025/206	Politie/OM/VAR/gemeenten
21.	Jaarlijks een actueel thema kiezen waarvoor extra aandacht zal zijn binnen de aanpak, zoals: geldezels, cryptovalutascam, jonge aanwas in digitale criminaliteit, sextortion.	Jaarlijks	Projectgroep i.s.m. publiek-private partners

Crisis- en incidentenbeheersing

Cyberincidenten en cybercrisis die ontstaan bij bedrijven, instellingen en belangrijke voorzieningen binnen de gemeentegrenzen, kunnen een impact hebben op de samenleving. Vaak kan het bedrijf of instelling het incident zelf oplossen, maar soms kan het ook zijn weerslag hebben op de lokale samenleving waardoor de gemeente betrokken raakt.

Met name als het om semipublieke voorzieningen (wegen, bruggen, sluizen, scholen, ziekenhuizen, culturele instellingen, verzorgingshuizen, etc.) gaat, zal de bevolking naar de gemeente en specifiek naar de burgemeester kijken. Goed voorbereide gemeenten weten hoe zij zelf (in de lokale driehoek) of samen met andere gemeenten en/of de Veiligheidsregio kunnen handelen om de cyberincidenten en -crisis beheersbaar te maken en af te wikkelen.

	Actie	Planning	Wie
1	Organiseren Regionale oefening in de driehoek en lokale crisisorganisatie	2025	VAR/Gemeenten/IBD/VR-RR en VR-ZHZ
2	Delen goede voorbeelden van oefenmodules incl. rol bestuurder	Doorlopend	VAR/VR-RR/VR-ZHZ
3	Delen format lokaal communicatieplan cybercrisis	2026	VAR
4	Delen format lokaal crisisplan cybercrisis	2025	VAR
5	Delen handelingsperspectief digitale veiligheid bij vergunningverlening bedrijven.	2025	VAR
6	Stimuleren deelname aan landelijke cybercrisisoefening ISIDOOR	Jaarlijks	VAR/VR-RR/VR-ZHZ
7	Stimuleren ketenafhankelijkheid/bewustwording in de haven en andere watergebonden locaties.	2025/2026	Gemeente Rotterdam/FERM/PVO
8	Volgen (landelijke) trainingen door de SGBO's.	Doorlopend	Politie

Eigen huis op orde

Gemeenten zijn verantwoordelijk voor het goed functioneren van de eigen digitale systemen (hardware en software) en digitale informatievoorzieningen, zodat de dienstverlening en bedrijfsvoering in goede orde verloopt en de beschikbare informatie bij de gemeente goed beveiligd is.

De Informatiebeveiligingsdienst (IBD) is een belangrijke partner in het op orde brengen van het eigen huis. Zij heeft op haar website een hele reeks documenten ter beschikking gesteld die ondersteuning kunnen bieden in het beveiligen van de eigen informatiehuishouding.

	Actie	Planning	Wie
1	Faciliteren CISO-netwerk en zorgen voor verbinding met OOV netwerk	Doorlopend	VAR/CISO's gemeenten en veiligheidsregio's
2	Verbeteren meldingsbereidheid gemeenten > politie	2025	Politie/CISO's gemeenten
3	Formats en standaardisatie van documentatie	2025	VAR/CISO's gemeenten
4	Ondersteunen van CISO's bij creëren van bestuurlijke aandacht voor informatieveiligheid.	2025	VAR/CISO's gemeenten en veiligheidsregio's
5	Delen goede voorbeelden/aandacht vragen voor dilemma's rond implementatie Cyberbeveiligingswet (NIS2 richtlijn).	2025-2026	VAR/CISO's gemeenten/IBD
6	Aandacht voor 'knaken bij taken': implementatie van (europese) wetgeving rond informatieveiligheid kost gemeenten capaciteit en middelen. Hiervoor via de VNG tot compensatie komen.	Doorlopend	VNG/Landelijk Platform Cyberburgemeesters (ondersteuning door VAR)

Digitaal weerbare democratie

Onze democratie is steeds meer afhankelijk van wat er in de digitale wereld gebeurt. Wanneer staten pogen democratische processen te ondermijnen, komt onze samenleving onder druk te staan. Dit gebeurt als de legitimiteit van de overheid in twijfel wordt getrokken, er een gebrek aan solidariteit is of er sprake is van polarisatie of enclavevorming. Door onder andere desinformatie kan de politieke en bestuurlijke integriteit van de volksvertegenwoordiging en de rechtspraak in twijfel worden getrokken. Of kan er twijfel over de vrijheid, eerlijkheid of anonimiteit van verkiezingen gezaaid worden.

Online aangejaagde ordeverstoring

Gemeenten worden steeds vaker geconfronteerd met fysieke ordeverstoringen die online beginnen of online versterkt worden. Het gaat dan bijvoorbeeld om onrust rondom politieke besluiten, overlast door groepen en individuen, oproepen tot demonstraties en illegale evenementen.

Statelijke dreigingen/ongewenste buitenlandse inmenging (OBI)

Statelijke actoren bedreigen in toenemende mate en op verschillende manieren de nationale veiligheidsbelangen. Dit komt onder meer door belangrijke geopolitieke ontwikkelingen. Meerdere statelijke actoren intensiveren daarbij ook hun cyberactiviteiten. In een recente kamerbrief wordt vermeld dat Nederland doelwit is van hybride aanvallen, zoals cyberoperaties, spionage en sabotage en aangegeven wat nodig is voor het weerbaar maken van de samenleving.

Statelijke dreigingen zijn dwingende, ondermijnende, misleidende of heimelijke activiteiten van of namens statelijke actoren, onder de drempel van gewapend conflict, die de nationale veiligheidsbelangen van Nederland kunnen schaden door een combinatie van nagestreefde doelen, gebruikte middelen en ressorterende effecten (bron AIVD).

Desinformatie

Het verspreiden van nepnieuws of oproepen die kunnen leiden tot openbare ordeverstoringen worden, zeker als het niet strafbaar is, niet geregistreerd als (digitale) criminaliteit. De kans dat plegers worden opgepakt of uitgeleverd voor hun daden is klein. Ze verschuilen zich achter anonieme accounts, versleutelde internetverbindingen en bevinden zich vaak buiten de geografische grenzen van het lokaal bevoegd gezag. Kennis over desinformatie is essentieel om de weerbaarheid te vergroten. Dit is nodig om onze democratische rechtsorde te beschermen en openbare orde incidenten te voorkomen.

Bij de hieronder genoemde acties is een raakvlak met het regionale thema maatschappelijk ongenoegen. Het wordt vanuit dit programma opgepakt, wanneer er een duidelijk cybercomponent is.

	Actie	Planning	Wie
1	Het bieden van handelingsperspectief op statelijke dreigingen op lokaal niveau via een handreiking.	2025	VAR
2	Mede-organiseren landelijke kennisbijeenkomst voor burgemeesters over het thema Statelijke dreigingen/OBI	2025	VAR/Bureau regio burgemeesters/NGB
3	Ontwikkelen E-learning gebruik barrièremiddel online aangejaagde ordeverstoring (subsidieproject)	2025	VAR
4	Scholen stimuleren leerlingen te leren hoe ze veilig omgaan met het internet (mediawijsheid). Bijvoorbeeld met speciale lespakketten: daarmee leren ze bijvoorbeeld beter met sociale media omgaan. En slim informatie zoeken en beoordelen. Een voorbeeld van een lesmethode is de nepnieuws-game Bad News.	Doorlopend	Gemeenten
5	De online, digitaal wijkagent volgt wat mensen bezighoudt op social media, in de lokale en regionale online media, en op internetfora. De digitaal wijkagent weet wat er online speelt, heeft contact met de lokale OOV'er en kan signalen van mogelijke ordeverstoringen monitoren en delen.	Doorlopend	Politie
6	Het opstellen van regionale samenwerkingsafspraken tussen gemeenten en politie over rol, informatiedeling en interventies bij OAOV.	2025	VAR/gemeenten/politie
7	Het vormen van een netwerk op statelijke dreigingen.	Doorlopend	VAR/gemeenten
8	Het organiseren van een regionale netwerkbijeenkomst op statelijke dreigingen.	Juni 2025	VAR

Bijlagen

1. Begrippen

Gedigitaliseerde criminaliteit	Misdrijven waarbij criminelen ICT als middel inzetten om traditionele vormen van criminaliteit te plegen. Zoals bijvoorbeeld hulpvraag-fraude, aan- en verkoopfraude.
Cybercriminaliteit	Computercriminaliteit, cybercriminaliteit of cybercrime is criminaliteit met ICT als middel én doelwit. Zoals hacking, DDoS-aanvallen, en ransomware
Digitale criminaliteit	Cybercrime en gedigitaliseerde criminaliteit tezamen wordt ook wel 'digitale criminaliteit' genoemd.
Aan- en verkoopfraude	Aan- en verkoopfraude is het opzettelijk kopen of het verkopen van goederen of diensten op internet zonder die te leveren of te betalen.
Helpdeskfraude	Bij deze vorm van fraude doet een fraudeur zich bijvoorbeeld telefonisch voor als een medewerker van de overheid of een bedrijf (e.g. "Dutch Supreme Court", bank, softwarebedrijf). In de meeste gevallen wordt het slachtoffer door de fraudeur benaderd, maar het kan ook voorkomen dat het slachtoffer zelf op zoek gaat naar een helpdesk van een organisatie (e.g. via Google, Bing) en per ongeluk uitkomt bij een frauduleuze helpdesk. De fraudeur heeft interactie met het slachtoffer en zet het slachtoffer aan tot het doen van een overboeking, tot het afgeven van betaalmiddelen (e.g. bankpas, telefoon) of eventueel tot het installeren van Remote Access Tooling (e.g. AnyDesk, Teamviewer, Quick Assist) waarna er frauduleuze transacties plaatsvinden.
Hulpvraagfraude	Bij deze vorm van fraude worden personen via Direct Messaging (iMessage, sms of WhatsApp) benaderd door: 1) een onbekende die zich voordoet als een familielid, vriend, bekende o.i.d., of 2) door een bekende afzender die overgenomen is door een cybercrimineel. Nadat vertrouwen is opgebouwd via enkele sociale interacties volgt een dringend verzoek om financiële hulp. Er wordt gebruik gemaakt van (psychologische) manipulatie om personen te verleiden tot het doen van een storting op het rekeningnummer van een derde, door bijvoorbeeld haast en urgentie te suggereren.
Identiteitsfraude	Identiteitsfraude is het opzettelijk gebruik maken van andermans identiteit, manipuleren van je eigen identiteit (bijvoorbeeld leeftijd) of het creëren van een fictieve identiteit, waardoor uit dat gebruik enig nadeel kan ontstaan. De verkregen (valse) identiteit wordt bijvoorbeeld gebruikt om iemand mee op te lichten, een bankrekening te openen, online bestellingen te plaatsen, leningen af te sluiten, zaken met de overheid te regelen, (cyber)pesten, het passeren van een landsgrens of om toegang te krijgen tot een horecagelegenheid
Phishing	Phishing (password harvesting fishing) is een verzamelnaam voor alle digitale activiteiten waarmee criminelen door middel van deceptie en imitatie onrechtmatig proberen persoonlijke gegevens van iemand te verkrijgen en/of binnen te dringen op een apparaat of account van die persoon. Het hoeft niet een op zichzelf staand cybercrime fenomeen te zijn. Een phishing aanval kan namelijk voor meerdere doeleinde worden ingezet:

	• Het verkrijgen van inloggegevens om toegang te verkrijgen tot bijvoorbeeld een account, een server, een netwerk of iets soortgelijks. • Het verkrijgen van andere gevoelige informatie, zoals financiële gegevens of persoonlijke informatie. • Het versturen van malware, zoals ransomware, een keylogger of een RAT. • Het overtuigen van een slachtoffer om een andere activiteit uit te voeren die tegen het eigenbelang ingaat, zoals het overmaken van geld of het delen van persoonlijke data.
Pig Butchering (relationele beleggingsfraude)	Een vorm van 'financial grooming' en oplichting waarbij eerst een relatie wordt opgebouwd met het slachtoffer. Pig butchering betekent in het Nederlands het slachten van het vetgemeste varken.
AI voice cloning	Cybercriminelen gebruiken AI (kunstmatige intelligentie) om mensen telefonisch op te lichten. Met zogenaamde 'voice cloning' kopiëren ze de stem van een vriend of familie. Die vraagt je bijvoorbeeld om snel geld over te maken of persoonlijke gegevens te delen. Drie seconden kan al genoeg zijn om je stem te kunnen klonen.
Cybersecurity en -safety	Beveiligingsmaatregelen die getroffen worden om schade te voorkomen door een storing, uitval of misbruik van een informatiesysteem of computer ('eigen huis op orde'). Hieronder vallen ook de maatregelen die worden genomen om schade te beperken en/of te herstellen als die is ontstaan. Het betreft zowel technisch maatregelen als maatregelen gericht op bewustzijn en gedrag.
NIS2	In het licht van alle digitale ontwikkelingen is er sinds 2020 vanuit de Europese Unie gewerkt aan de Network and Information Security (NIS2) directive. Deze richtlijn is gericht op een verbetering van de digitale en economische weerbaarheid van Europese lidstaten. In Nederland wordt de NIS2-richtlijn geïmplementeerd in de vorm van de Cyberbeveiligingswet (Cbw). Op het moment dat de Cbw wordt aangenomen, vervangt deze de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni).
Meer begrippen	*Het Cybersecurity Woordenboek legt zo'n 780 cybersecurity termen uit in begrijpelijke taal.*

2. Interventies per doelgroep

Jongeren

Hackshield

Hackshield is een cybersecurity game voor kinderen tussen de 8 en 12 jaar. Op een speelse manier leren kinderen zich wapenen tegen digitale ervaringen. Kinderen worden dan Junior Cyber Agent en worden gestimuleerd het geleerde ook over te brengen op hun (groot)ouders.
De gemeente speelt in dit project een belangrijke rol aangezien de burgemeester de kinderen per videobericht zelf oproept op het spel te spelen en Junior Cyber Agent te worden. Na enige tijd zal de burgemeester de kinderen live huldigen wat voor die kinderen extra motivatie geeft om het geleerde ook daadwerkelijk toe te passen.

Cyberrijbewijs

Mijn Cyberrijbewijs is een gratis lesprogramma dat bijdraagt aan de digitale weerbaarheid van leerlingen uit groep 7 en 8 van het primair onderwijs. Aan de hand van illustrerende thema's zoals online hate speech, online fraude, doxing, hacking en sexting leren en ervaren kinderen meer over online slachtoffer- en daderschap. Van kennis, via inzicht naar gedrag met handelingsperspectief.

Hackright

Wanneer jongeren strafbare feiten plegen op het gebied van cybercriminaliteit, kunnen ze naar Halt worden verwezen. In onze interventie krijgen jonge hackers inzicht in de gevolgen van hun daden. Halt heeft samen met andere instanties, waaronder het Openbaar Ministerie, politie, Reclassering en IT-bedrijven, de aanpak Hack_Right ontwikkeld. Deze aanpak voor cyberveiligheid wordt aangeboden aan cyberdaders tussen de 12 en 23 jaar. Naast het uitvoeren van de gebruikelijke onderdelen van het Halt-traject, moeten zij een werkopdracht uitvoeren bij een IT-bedrijf. Door deze opdracht leren ze hoe zij hun talent op een positieve en nuttige manier kunnen inzetten.

Geldezelaanpak

Vanuit de City Deal 'Lokale Weerbaarheid Cybercrime' werkt het CCV momenteel aan de leidraad Gemeentelijke aanpak geldezels. In de leidraad wordt zoveel mogelijk kennis gebundeld vanuit wetenschap en praktijk. Er wordt een uitwerking gemaakt op de volgende 4 thema's:

- Samenwerking met partners zoals politie, OM, veiligheidshuis, onderwijs, jongerenwerk e.d., inclusief een convenant voor gegevensuitwisseling.
- Algemene voorlichting om bewustzijn en risicoperceptie te vergroten; offline (bijvoorbeeld op scholen) en online (via social media campagne) gericht op jongeren in de leeftijd van 12 tot 23 jaar.
- First offender aanpak: een geldezel zonder criminele antecedenten ervan doordringen dat zijn misstap niet moet leiden tot verder crimineel gedrag, nagaan wat ertoe leidde om als geldezel op te treden en die oorzaak proberen weg te nemen.
- Aanpak voor geldezels met meerdere antecedenten: een geldezel met criminele antecedenten laten stoppen met zijn criminele gedrag en zorg aanbieden.

re_B00TCMP

Met re_B00TCMP leren jongeren over de kansen en uitdagingen in de digitale wereld. Dit programma helpt hen om onlinegrenzen te herkennen en te respecteren, en bereidt hen voor op een veelbelovende toekomst in de IT-arbeidsmarkt.

Senioren/laaggeletterden

Echt of Nep?
In dit project is door de VAR de interactieve film 'Echt of Nep?' ontwikkeld, waarmee gemeenten via ouderenwerk, politie, bibliotheken, enzovoort, het gesprek aan kunnen gaan met senioren over veilig internetgebruik. In de film zitten keuzemogelijkheden waarbij de film wordt stopgezet en aan de senioren wordt gevraagd wat zij in deze situatie zouden doen. De film gaat daarna verder met de keuze die gemaakt is. Door te ervaren wat er gebeurt als er een verkeerde keuze wordt gemaakt, blijft de opgedane kennis beter hangen. Onderwerpen die aan bod komen zijn: hulpvraagfraude/Whatsapp fraude, helpdeskfraude, phishing/ smishing, spoofing en datingfraude. In de bijgeleverde handleiding interactieve training vind je alles wat je moet weten over het laagdrempelig organiseren van een bijeenkomst voor senioren en het gebruik van de film om de weerbaarheid van ouderen te versterken.

Bordspel weerbaar op het web
Het fysieke bordspel "Weerbaar op het web" is afgestemd voor laaggeletterde en minder digitaal vaardige mensen. Met dit spel leert de speler (gevaarlijke) e-mails, websites en bijlagen te herkennen. Dit spel is (gratis) beschikbaar via de VAR en de bibliotheken.

Ondernemers

PVO Regio Rotterdam gaat op het gebied van cybercrime programmatisch te werk. Dit is gericht op: bewustwording, advies en borging. Het Platform Veilig Ondernemen Regio Rotterdam (PVO) organiseert onder andere kosteloze bijeenkomsten en trainingen voor ondernemers uit de regio Rotterdam. Hieronder meer over het aanbod:

Cybercrime-bijeenkomsten
Bijeenkomsten waar ondernemers voorlichting krijgen over de werkwijze van hackers, kennisoverdracht en bewustwording van de gevaren en de daarbij toe te passen veiligheidsmaatregelen.

Cyberadviesgesprek
Een PVO-adviseur bezoekt een onderneming en kijkt naar de kwetsbaarheden binnen de digitale omgeving. Tijdens het bezoek worden veiligheidsrisico's en beveiligingsmaatregelen met de ondernemer besproken. De ondernemer ontvangt na het bezoek een adviesrapport met concrete aanbevelingen om deze risico's te verminderen en de veiligheid van de onderneming te vergroten.

Cybernetwerken van en door ondernemers
Binnen de regio zijn er meerdere netwerken, zoals Cybernetwerk Drechtsteden/ Zuid-Hollandse Eilanden van en voor ondernemers die in samenwerking met gemeenten en private partijen informatie uitwisselen, de lokale trends in de gaten te houden en awareness trainingen verzorgen.

Virtual Reality (VR)
PVO heeft een VR-game op het gebied van cybercrime ontwikkeld. Via een VR-experience wordt de ondernemer bewust gemaakt van de risico's binnen zijn of haar onderneming. Door een debriefing van het PVO worden de kwetsbaarheden inzichtelijk gemaakt en wordt handelingsperspectief geboden.

Hacksimulaties
Door middel van hacksimulaties worden ondernemers geactiveerd om noodplannen voor zijn of haar eigen onderneming op te stellen. PVO stelt de ondernemer in staat om in een veilige setting een hack te ervaren.

Algemeen

Vanuit de Rijksoverheid zijn er verschillende campagnes inclusief toolbox beschikbaar die ingezet kunnen worden door gemeenten en ketenpartners,

De bibliotheken hebben een rol bij digitale inclusie/burgerschap, inclusief het bevorderen van cyberweerbaarheid. Zij hebben voor hun netwerk een inspiratiegids uitgebracht.

3. Themadagen

Er zijn ieder jaar vele verschillende themadagen. De verschillende themadagen zijn interessant om bijvoorbeeld een campagne op te starten, activiteit te organiseren of aandacht aan te besteden op social mediakanalen.

28 januari: Privacy Day

1 februari: Change your password day

11 februari: Safer Internet Day

Maand april – senioren en veiligheid

21 mei 2025 Regionale Actiedag "Echt niet vandaag"

Maand oktober: European Cyber Security Maand

6 – 10 oktober: Week van de Veiligheid

24 november: Nationale Check Je Wachtwoorden-dag

28 november: Black Friday
Een dag voor het thema digitale veiligheid en dan vooral gericht op misleidende informatie en aanbiedingen rondom Black Friday.