



Aan de gemeenteraad

Op 23 juni 2025 stelde D.A. van Groningen - de Haas (VVD) ons schriftelijke vragen over digitale aanvallen als groeiende bedreiging voor onze veiligheid en in hoeverre de Veiligheidsregio hierop is voorbereid. Gezien de aard van de vragen, wordt geacht dat deze aan de burgemeester zijn gesteld.

Inleidend wordt gesteld:

Digitale aanvallen vormen een groeiende bedreiging voor onze veiligheid. Van tunnels tot drinkwater: onze publieke infrastructuur leunt volledig op digitalisering. Dat terwijl onze overheidsorganisaties, bedrijven en nutsvoorzieningen steeds vaker het doelwit zijn van (buitenlandse) hackers, zoals vandaag nog, toen gemeenten als Den Haag en Delft slachtoffer werden van een aanval op raads- en Statenstukken, opgeëist door de Russische hackersgroep NoName05716, zo valt in De Telegraaf te lezen.

Naar ons weten worden cyberaanvallen nauwelijks meegenomen in rampenoefeningen binnen de Veiligheidsregio. Onbegrijpelijk, zeker nu buitenlandse hackers steeds brutaler opereren en maatschappelijke ontwrichting op de loer ligt. Grootschalige digitale aanvallen kunnen leiden tot ontwrichting van openbare orde, veiligheid en economische stabiliteit in onze veiligheidsregio. De Rotterdamse VVD vindt dat we op alles voorbereid moeten zijn.

Hieronder volgen de vragen en mijn beantwoording:

Vraag 1:

Is het college bekend met de aanval op gemeentesites zoals die van Den Haag en Delft, zoals gemeld door NotuBiz?

Antwoord:

Ja.



Vraag 2:

Maakt de gemeente Rotterdam ook gebruik van de diensten of systemen van NotuBiz of vergelijkbare leveranciers? Zo ja, waren deze de afgelopen dagen volledig of deels onbereikbaar?

Antwoord:

Op 23 juni 2025 is leverancier NotuBiz getroffen door een DDoS-aanval van de groep NoName. Dit soort aanvallen zorgt ervoor dat websites of applicaties tijdelijk slecht of niet bereikbaar zijn, zonder dat er sprake is van inbraak of datadiefstal. Verschillende gemeenten en organisaties die gebruikmaken van NotuBiz-producten ondervonden hierdoor tijdelijke hinder. De gemeente Rotterdam maakt gebruik van enkele diensten van NotuBiz. De primaire gemeentelijke dienstverlening is niet geraakt door dit incident. Bij een aantal afdelingen was er kortdurend hinder, bijvoorbeeld het publiceren van vergaderstukken bij de COR-vergaderingen. De leverancier heeft snel maatregelen genomen, waarna de systemen binnen een paar uur weer normaal functioneerden.

Vraag 3:

Zijn er signalen dat Rotterdam (mede) doelwit is geweest van deze aanval of dat gemeentelijke systemen afwijkend verkeer hebben opgemerkt?

Antwoord:

Het Security Operations Center (SOC) van IIFO/ICT bewaakt continu het netwerkverkeer van de gemeente Rotterdam. Op 23 juni zijn er geen aanwijzingen geweest dat onze systemen doelwit waren van deze aanval. Als gemeente zijn we waakzaam en nemen we voortdurend maatregelen om dit soort verstoringen zoveel mogelijk te voorkomen, vroegtijdig te signaleren en waar nodig snel op te treden. Als voorbeeld: in aanloop naar de NAVO-top zijn extra voorzorgsmaatregelen genomen, zoals een freeze op wijzigingen IT-systemen en verscherpte monitoring. Samen met de leverancier van Rotterdam.nl is bekeken hoe aanvullende bescherming tegen DDoS-aanvallen kon worden ingezet. Deze gezamenlijke aanpak heeft effect gehad — pogingen tot verstoring zijn succesvol afgeweerd en de website is beschikbaar gebleven.

Vraag 4:

Herkent en erkent het college het risico dat grootschalige digitale aanvallen een gevaar kunnen vormen voor onze regio?

Antwoord:

Het college erkent dat cyberincidenten een toenemend risico vormen voor onze regio. In rapportages zoals het Cybersecuritybeeld Nederland 2024¹, het AIVD Jaarverslag 2024² en de AIVD/MIVD-rapportage over de Russische cyberactor Laundry Bear van mei 2025³ staat een toegenomen digitale dreiging voor Nederland beschreven. Wij erkennen dat de regio Rotterdam-Rijmond met haar haven een internationaal logistiek knooppunt is en daarmee een interessant doelwit vormt. Daarnaast heeft Rotterdam-Rijnmond een groot chemisch cluster, waardoor bij digitale aanvallen ook gevaarlijke fysieke scenario's denkbaar zijn.

¹ [Cybersecuritybeeld Nederland 2024 | Nationaal Coördinator Terrorismebestrijding en Veiligheid](#)

² [Jaarverslag 2024 | Jaarverslag | AIVD](#)

³ [AIVD en MIVD onderkennen nieuwe Russische cyberactor | Publicatie | AIVD](#)



Vraag 5:

Op welke manier worden op dit moment digitale dreigingen gesimuleerd in crisisoefeningen van de Veiligheidsregio Rotterdam-Rijnmond?

Antwoord:

Digitale dreigingen worden gesimuleerd via concrete interactieve oefeningen met netwerkpartners. Hierbij ligt het accent op het beperken van de maatschappelijke gevolgen van een digitale verstoring. De oefendoelen hierin zijn het in beeld brengen welke samenwerkingspartners specifieke expertise voor het duiden van de situatie kunnen leveren, tijdige opschaling en aandacht voor voorkomen of beperken van keteneffecten op korte en (middel)lange termijn.

Daarnaast nemen VRR en gemeente Rotterdam gezamenlijk deel aan het Europese project 'Agile'.⁴ Dit project doet onderzoek naar High Impact Low Probability (HILP) crises. Hiervoor worden dit jaar meerdere stresstesten uitgevoerd. In september is geoefend met een scenario gericht op grootschalige ontwrichting ten gevolge van cyberaanvallen.

Vraag 6:

Is het college bereid om bij een volgende grootschalige rampenoefening expliciet het scenario van een digitale aanval (zoals een DDOS-aanval op vitale infrastructuur) mee te nemen?

Antwoord:

Ja, en voor wat betreft de regiobrede (grootschalige) rampenoefening, zal het college dit verzoek bij het bestuur van de VRR adresseren. Tegelijkertijd wil ik u ook informeren dat de gemeente en de VRR in 2023 hebben deelgenomen aan de grote landelijke cyberoefening ISIDOOR IV waar de vitale sectoren betrokken waren. Het streven van de VRR is om in 2027 wederom deel te nemen aan de grote ISIDOOR V oefening.

Vraag 7:

Hoe is momenteel de samenwerking met partners als het Rijk, de Provincie, Defensie, Deltalinqs en gemeentelijke organisaties?

Antwoord:

De samenwerking vanuit de VRR verloopt via verschillende samenwerkingen en gremia, met betrekking tot zowel de koude als warme fase. De VRR en gemeente Rotterdam werken nauw met elkaar samen in zowel de warme als de koude fase. Landelijk zijn de samenwerkingsafspraken vastgelegd in het Landelijk Crisisplan Digitaal, voor de warme fase. De samenwerking met Defensie is vastgelegd in de afspraken Intensivering Civiel Militaire Samenwerking (ICMS) en specifiek met de VRR vastgelegd in een convenant. Op basis daarvan is bij de afdeling crisisbeheersing (waar cybergevolgbestrijding onder valt) een Regionaal Militair Operationeel Adviseur (RMOA) van het Ministerie van Defensie gedetacheerd. Ook is de VRR lid van FERM. Alle Nederlandse zeehavens participeren hier sinds dit jaar in. Uiteraard is daarnaast ook bilateraal nauwe afstemming tussen de VRR en het Havenbedrijf Rotterdam. Daarnaast vindt er afstemming plaats via verschillende landelijke werkgroepen, zoals de werkgroep Digitale verstoringen. Grote oefeningen met veel partners, zoals de hierboven genoemde ISIDOOR oefening, helpen ook bij een effectieve samenwerking.

Gemeente Rotterdam werkt vanuit de integrale regionale aanpak op digitale veiligheid samen met gemeenten uit de regio.

⁴ [The AGILE Horizon Europe Project - Agnostic risk management](#)



Daarnaast wordt nauw samengewerkt met de VeiligheidsAlliantie Rotterdam (VAR), die alle gemeenten in onze regio vertegenwoordigt. Ook voeren wij regelmatig gesprekken in G4 verband. Via deze weg lopen onder andere ook linken met de Vereniging van Nederlandse Gemeenten (VNG) die weer alle gemeenten in het land vertegenwoordigen. Op het gebied van digitale veiligheid in brede zin, is regelmatig contact met het ministerie van Justitie en Veiligheid. Vooral op het gebied van online aangejaagde ordeverstoringen. Vanuit de aanpak op weerbaarheid lopen lijnen richting Defensie en vanuit de aanpak op Maritiem is contact met Deltalinqs. Gezien de vele ontwikkelingen en initiatieven die er zijn op het gebied van weerbaarheid en digitale veiligheid specifiek, blijft er wel aandacht nodig voor een goede aansluiting tussen de verschillende partners voor zowel de VRR als de gemeente.

Vraag 8:

Welke bestaande plannen en scenario's liggen er om de digitale veerkracht van de regio te versterken en wat is de rol van de gemeente hierin?

Antwoord:

Cyberdreigingen zijn als scenario onderkend in het Regionaal Risicoprofiel. De VRR werkt aan een informatiekaart voor cybergevolgbestrijding, die dit jaar wordt afgerond in samenwerking met regionale partners zoals gemeenten (waaronder Rotterdam), Stedin, Evides en waterschappen. De informatiekaart beschrijft de verschillende stappen die genomen kunnen worden in het kader van crisismanagement en gevolgbestrijding rondom verschillende scenario's van digitale ontwrichting. Er is hierbij tevens afstemming met andere Veiligheidsregio's.

Samen met de gemeenten werkt de VRR aan het versterken van de weerbaarheid van de samenleving. Hiervoor worden voorbereidingen getroffen voor het inrichten van coördinatie- en lokale noodsteunpunten. De gemeenten zijn daarnaast ook vertegenwoordigd in de planningsstaf Geopolitieke dreigingen en ontwikkelingen. Hier ligt de aandacht op het vergroten van de maatschappelijke veerkracht ongeacht de oorzaak, dus is dit ook van belang ter voorbereiding op digitale verstoringen. Daarnaast worden vanuit Agile (zie vraag 5) tools ontwikkeld om met complexe crises om te gaan. VRR en gemeente Rotterdam organiseren stresstesten en oefenen samen met belangrijke stakeholders met cyber-scenario's. Daarnaast wordt er vanuit de gemeente preventief in samenwerking met de Zeehavenpolitie en het Platform Veilig Ondernemen (PVO) ingezet op het weerbaar maken van het MKB in het havengebied. Hierbij ligt de focus op dit moment specifiek op de Waalhaven als startpunt.

Vraag 9:

In hoeverre raken de bezuinigen de uitwerking van scenario's en simulaties voor rampen?

Antwoord:

De bezuinigingen zullen geen effect hebben op oefeningen en simulaties.

Vraag 10:

Staat u ervoor open om samen met de collega's in de VRR te kijken hoe we kunnen samenwerken met Defensie?



Antwoord:

Ja, deze samenwerking is al structureel, zie ook de beantwoording op vraag 7, maar geldt ook voor toekomstige ontwikkelingen in het kader van Host Nation Support (het verplaatsen van legereenheden in NAVO-verband, mogelijkkerwijs via de Rotterdamse Haven).

Vraag 11:

In hoeverre zou u willen lobbyen bij Defensie om ook een financiële bijdrage te doen aan de VRR om ervoor te zorgen dat we voorbereid zijn op de toekomst en de hybride dreigingen?

Antwoord:

Tijdens de NAVO-top is besloten 1,5% van het BNP vrij te maken voor aan defensie gerelateerde zaken. Het college is bereid zich hard te maken voor het aanwenden van deze middelen voor de lokale (gemeente) en regionale (VRR) inzet gericht op het vergroten van de weerbaarheid tegen hybride dreigingen.

De burgemeester,

C.J. Schouten