Ministerie van Defensie

Ministerie van Defensie
Plein 4
MPC 58 B
Postbus 20701
2500 ES Den Haag
www.defensie.nl

Onze referentie
D2025-000744

Bij beantwoording, datum, onze referentie en onderwerp vermelden.

> Retouradres Postbus 20701 2500 ES Den Haag

de Voorzitter van de Tweede Kamer
der Staten-Generaal
Bezuidenhoutseweg 67
2594 AC Den Haag

Datum	20 maart 2025
Betreft	Evaluatie NAFIN storing

Geachte voorzitter,

In de nacht van 27 op 28 augustus 2024 heeft een technische storing plaatsgevonden op het Netherlands Armed Forces Integrated Network (NAFIN). De minister van Defensie heeft uw Kamer hierover geïnformeerd (Kamerstuk 26 642, nr. 1214) en toegezegd de storing en weerbaarheid van de betreffende IT-systemen met alle betrokkenen te evalueren en uw Kamer hierover te informeren. Defensie heeft het COT Instituut voor Veiligheids- en Crisismanagement (hierna: COT) en het adviesbureau Strict[1] gevraagd een evaluatie naar de NAFIN-storing uit te voeren en een gezamenlijke oplegger aan te leveren. In deze brief reageer ik, mede namens de minister van Defensie, op de belangrijkste aanbevelingen van COT en Strict en licht ik toe welke maatregelen ik tref. Beide rapporten en de gezamenlijke oplegger zijn vanwege het belang van NAFIN vertrouwelijk en worden in die vorm aangeboden aan uw Kamer[2]. Defensie erkent ook het maatschappelijk belang van de digitale weerbaarheid van NAFIN, en zal tot zover mogelijk te bevindingen en de actiepunten die hierop volgen delen met u.

De afhankelijkheid van IT is de afgelopen jaren exponentieel toegenomen. In een steeds meer gedigitaliseerde wereld is technologie essentieel geworden voor het waarborgen van de nationale veiligheid, het uitvoeren van militaire operaties en het effectief communiceren tussen verschillende overheidsinstanties en internationale partners. Het is dan ook van vitaal belang dat de digitale infrastructuur robuust, veilig en continu up-to-date blijft. IT-storingen zijn echter niet altijd te

[1] Strict is een Nederlands onafhankelijk adviesbureau gespecialiseerd in borgen van de bedrijfscontinuïteit en vergroten wendbaarheid bij organisatie die een essentiële rol spelen in de samenleving
[2] Ter vertrouwelijke inzage gelegd, alleen voor leden, bij het Centraal informatiepunt Tweede Kamer.

voorkomen, geen enkel systeem is immers volledig immuun voor technische problemen of onverwachte externe invloeden. Het is wel cruciaal om goed voorbereid te zijn en maatregelen te nemen om de impact van deze storingen te minimaliseren. De NAFIN-storing heeft duidelijk gemaakt dat Defensie niet voldoende voorbereid was op een grootschalige verstoring. De resultaten van de onderzoeken leveren waardevolle lessen en bieden Defensie concrete handvatten om de digitale weerbaarheid te versterken.

Achtergrond
Op dinsdagavond 27 augustus 2024 veroorzaakte een softwarefout het wegvallen van de routering in NAFIN. Dit leidde tot grote verstoringen bij onder meer de Koninklijke Marechaussee, de Kustwacht, Eindhoven Airport, meldkamercommunicatie en bij Defensie in het eigen Mulan netwerk. Ook de Haagse Ring ondervond de volgende ochtend hinder in de bedrijfsvoering, waardoor de daarop aangesloten organisaties met uitval van diensten te maken kregen. Gedurende de nacht van 27 op 28 augustus is gestart met het organiseren van het systeemherstel. NAFIN functioneerde weer in de loop van de ochtend van 28 augustus 2024.

Conclusies
Hieronder behandel ik, vanwege de vertrouwelijkheid op hoofdlijnen, de belangrijkste conclusies en aanbevelingen uit beide rapporten. Daarbij geef ik aan hoe ik invulling geef aan het opvolgen van de aanbevelingen. Ik herken de conclusies in de rapporten van COT en Strict en neem de aanbevelingen over.

COT en Strict concluderen dat ondanks de bestaande preventieve maatregelen die Defensie heeft genomen, deze storing niet had kunnen worden voorkomen. Dit incident benadrukt de complexiteit van onze IT-omgeving en de uitdagingen die gepaard gaan met het waarborgen van robuuste en veerkrachtige systemen.

In deze storing en de opvolging hiervan liggen waardevolle lessen voor Defensie, die kunnen helpen bij het verbeteren van de digitale weerbaarheid. Onderstaande zijn de zes belangrijkste conclusies van COT en Strict:

- <u>Defensie was onvoldoende voorbereid op een dergelijke verstoring.</u>
  Defensie moet werken aan betere voorbereidende maatregelen en plannen om de impact van storingen, incidenten of rampen te minimaliseren om de continuïteit te garanderen.

- <u>Er is laat intern geëscaleerd van de technische naar de bestuurlijke laag.</u>
  De escalatie van de technische laag naar de bestuurlijke laag heeft lang geduurd. Het tijdstip waarop de storing optrad speelt hierbij een belangrijke rol, aangezien de storing plaats vond buiten kantoortijden. Zodra de escalatie naar de bestuurlijke laag werd doorgezet, werd hier direct op gereageerd. De technische oorzaak van de verstoring is binnen 13 uur opgelost. Dit is ruim langer dan het streven van 4 uur dat hiervoor is afgesproken. Dit had dus sneller gemoeten.

- <u>Defensie heeft de crisis klein gehouden en mag groter denken over de bestuurlijke implicaties van een verstoring als deze.</u>
  De storing is door Defensie voornamelijk als interne aangelegenheid beschouwd, waardoor onvoldoende aandacht was voor brede maatschappelijke implicaties en partijen die op NAFIN zijn aangesloten.

- <u>Bij het afhandelen van de verstoring is er te laat en onvoldoende aandacht geweest voor de cyberrisico’s.</u>
  Binnen Defensie worden IT-incidenten en cyber-incidenten als twee aparte storingen behandeld. Cybersecurity expertise is wel in een vroeg stadium ingeschakeld, maar de nadruk lag

op het oplossen van het IT incident. Hierdoor werd het cyberonderzoek bemoeilijkt.

- De communicatie is zowel binnen Defensie als naar externe partners niet goed verlopen.
  Er was onduidelijkheid over de richtlijnen voor communicatie. De interne informatiestroom kwam daardoor moeizaam op gang, wat ook de communicatie naar buiten bemoeilijkt heeft. Daarbij trof de storing ook bepaalde reguliere communicatielijnen. Beschikbare informatie kwam hierdoor niet altijd op tijd bij de juiste partijen terecht.

- De prioritering van systemen voor opschalen na verstoring is nog onvoldoende geborgd.
  Het is nog onvoldoende duidelijk wat de prioritering is voor het herstellen van systemen na grootschalige uitval van IT. Dit is nodig voor het waarborgen van de bedrijfscontinuïteit en het verder minimaliseren van de impact op de organisatie.

Aanbevelingen en maatregelen
De NAFIN storing is veroorzaakt door een fout in de tijdsynchronisatie. Dit is een technisch mankement dat niet voorzien had kunnen worden. Deze storing heeft veel impact gehad. Daarom is het van belang dat snel wordt gehandeld om een dergelijke storing op te lossen wanneer die zich voordoet. De evaluaties geven aan dat dat sneller had gekund. Om die reden neemt Defensie een aantal maatregelen zodat een volgende storing beter is voorbereid en sneller kan worden gehandeld.

Voor een snellere afhandeling van een mogelijk volgende storing zijn continuïteitsplannen belangrijk. Deze plannen beschrijven welke instructies en procedures moeten worden gevolgd tijdens een verstoring, zodat Defensie kan blijven opereren. Naast het op zeer korte termijn inzetten op de implementatie van reeds uitgewerkte technische verbeteringen, is Defensie gestart met het grondig herzien van de continuïteitsplannen.

Bij het herzien van de continuïteitsplannen staan drie elementen centraal. Ten eerste is specifiek aandacht voor de uitgangspunten waarop de prioritering van (uitgevallen) systemen tijdens een dergelijke storing wordt bepaald. Defensie stelt hiervoor een lijst op van kritieke processen en de daaraan verbonden IT systemen. Op basis van deze lijst wordt bepaald met welke prioriteit systemen hersteld worden na storingen. Ten tweede zal Defensie in de toekomst in de beginfase van een dergelijke storing geen onderscheid meer maken tussen een IT-incident en cybersecurityincident. Op moment van de storing kenden deze incidenten eigen werkwijzen en procedures. De evaluaties leren ons dat het sneller en effectiever is om hiervoor één werkwijze op te stellen. Daarom zijn beide werkwijzen en procedures voor de beginfase van storingen inmiddels samengevoegd. De komende tijd wordt dit beproefd, bijvoorbeeld door middel van oefeningen in Q3 2025. Ten derde zorgt Defensie voor een duidelijk opschalingskader bij storingen, dat voor alle partijen aangesloten op NAFIN navolgbaar is. Een opschalingskader is een stappenplan dat bepaalt hoe een organisatie reageert als er een groot cyber of IT-probleem is. Aan de hand van dit opschalingskader kunnen IT-incidenten en cybersecurityincidenten goed gecoördineerd worden. Bij het opstellen van dit kader betrekt Defensie de NCTV en andere relevante overheidsorganisaties.

Gekoppeld aan deze continuïteitsplannen werkt Defensie ook aan een update van de bestaande crisiscommunicatieplannen, waarbij meer aandacht komt voor cyber- en IT-gerelateerde verstoringen. Hierin wordt vastgelegd welke informatie op welke manier gedeeld wordt tijdens storingen, zowel met interne als externe partners. Als onderdeel hiervan implementeert Defensie het Landelijk Crisis Management Systeem (LCMS) voor de landelijke communicatie tijdens crisissituaties. Hierdoor wordt snellere en betere communicatie met partners mogelijk.

De evaluatierapporten bevelen aan om vaker te oefenen met incidenten als de NAFIN-storing. Ik omarm deze aanbeveling en neem deze over. Er zijn reeds verschillende oefeningen gepland voor eind 2025. Tijdens deze oefeningen zullen bovengenoemde maatregelen beproefd worden. Na elke oefening wordt de effectiviteit van de genomen maatregelen geëvalueerd, waarna de maatregelen verder aangescherpt worden. Tijdens deze oefeningen komt ook expliciet aandacht voor het crisiscommunicatieplan. Daarnaast zal ook de rol van Defensie als maatschappelijke partner en dienstverlener terugkomen in de oefeningen. Door aandacht te besteden aan de bredere maatschappelijke implicaties in oefeningen draagt Defensie bij aan de digitale weerbaarheid van Nederland.

Naast bovengenoemde maatregelen waar nog aan gewerkt wordt, zijn er direct na de storing ook maatregelen getroffen die inmiddels zijn afgerond. Zo is bijvoorbeeld het aantal analoge middelen vergroot, zoals computers en printers die geen internet nodig hebben en papieren documenten met instructies en contactpersonen. Daarnaast zijn de opleidingen en trainingen voor personeel aangescherpt. Ook zal de Chief Information Officer (CIO) voortaan standaard aan tafel zitten bij het crisisteam dat verantwoordelijk is voor de bestuurlijke coördinatie van een crisis. Hierdoor is kennis over cybersecurity en IT voortaan vanaf het begin ook op bestuurlijk niveau betrokken.
Zoals genoemd in de Reactie op het rapport ‘De kracht en kwetsbaarheid van het digitale krijgsmachtnetwerk NAFIN’ van de Algemene Rekenkamer (Kamerstuk 36592-8) onderzoekt

Defensie of het netwerk aangemerkt moet worden als vitale infrastructuur. Dit onderzoek wordt voor de zomer van 2025 afgerond.

De afspraken over de dienstverlenging omtrent NAFIN zijn beschreven in verschillende documenten zoals een Nadere Overeenkomst (NOK), een dienstbeschrijving en een *Service Level Agreement* (SLA). Hiernaast heeft Defensie ook afspraken met de leveranciers, KPN, Nokia en Cisco, in kaart gebracht. Op basis van de aanbevelingen van COT en Strict zullen deze afspraken worden herzien en waar nodig aangevuld. Defensie heeft zicht op alle gebruikers van NAFIN, waaronder gebruikers in de Haagse Ring, meldkamers en het Rijksoverheidnetwerk (RON). Op dit moment is er geen alternatief voor NAFIN voor deze civiele gebruikers.

Slot

NAFIN is van essentieel belang voor zowel Defensie als de Rijksoverheid, waarbij de veiligheid en beschikbaarheid van het netwerk een hoge prioriteit heeft. De storing en de evaluaties laten zien dat Defensie hierin nog kan verbeteren. De bevindingen en aanbevelingen uit beide rapporten zijn waardevolle lessen die ik gebruik om te zorgen dat we beter voorbereid zijn op een mogelijk volgende verstoring.

Gezien de huidige geopolitieke situatie is Defensie zeer terughoudend om informatie over kwetsbaarheiden en gebruik van onze hoog-gerubriceerde systemen, processen en netwerken te delen. In deze brief bent u daarom op hoofdlijnen geïnformeerd.

Ik vertrouw erop uw Kamer hiermee voldoende te hebben geïnformeerd en zie uit naar de verdere dialoog hierover.

Hoogachtend,

DE STAATSSECRETARIS VAN DEFENSIE

Gijs Tuinman