De kracht en kwetsbaarheid van het digitale krijgsmachtnetwerk NAFIN

2024

Algemene Rekenkamer

Inhoud

1. Samenvatting

Het *Netherlands Armed Forces Integrated Network* (NAFIN) is een glasvezelnetwerk van het ministerie van Defensie en KPN dat veilige communicatie tussen Defensie-onderdelen mogelijk maakt. Het staat los van het internet en van de reguliere, publieke glasvezelnetwerken waar Nederlanders gebruik van maken. Het netwerk ontstond in 1996 toen losse communicatieverbindingen van Defensie verouderden en te kostbaar werden. Met integratie naar 1 nieuw netwerk kon meer capaciteit worden gerealiseerd en kon Defensie kosten besparen. Maar Defensie probeerde in de jaren 2000 ook geld te verdienen en zo kosten te dekken van het netwerk, door het open te stellen voor andere gebruikers van de rijksoverheid. Zo is het gehele rijksoverheidnetwerk voor alle ministeries en Hoge Colleges van Staat uiteindelijk aan het NAFIN verbonden. Daarnaast zijn meerdere vitale processen, zoals de inzet van de politie en de meldkamers van noodnummer 112, inmiddels ook volledig afhankelijk van het NAFIN. Het is daarmee een belangrijk netwerk voor het behoud van onze nationale veiligheid dat niet alleen goed door de minister van Defensie beschermd dient te worden, maar ook door zijn andere gebruikers.

Er heeft de afgelopen jaren een toenemend aantal sabotageacties plaatsgevonden op kritieke Europese infrastructuren. Dit was aanleiding voor ons om te onderzoeken hoe het ministerie van Defensie het NAFIN beschermt. Uit ons onderzoek dat is uitgevoerd in 2024 blijkt dat het NAFIN qua opzet goed in elkaar zit, maar in de praktijk onvoldoende beveiligd is.

Het ministerie van Defensie heeft in 1996 het NAFIN aangelegd. Defensie stelde bij de oprichting twee randvoorwaarden. Alleerst zou het netwerk, vanwege zijn belangrijke functie voor de inzet van Defensie, nooit mogen uitvallen. Never out

noemt Defensie dat. Ten tweede zou het NAFIN *military owned and controlled* moeten zijn. Dat wil zeggen dat Defensie in elke situatie zelf de regie moet hebben om aanpassingen te doen aan het netwerk. Wij trekken 3 conclusies, die laten zien dat deze 2 randvoorwaarden in het gedrang komen: er is een gebrek aan strategie, het netwerk is in de praktijk onvoldoende beveiligd en er is beperkte militaire regie over het netwerk.

Ontbrekende strategie Defensie op rol en toekomst van het NAFIN

Onze eerste conclusie is dat de minister van Defensie geen strategie voor of visie op de rol en de toekomst van het NAFIN heeft. Het NAFIN werd in die tijd met goede redenen opgericht met het idee geld te besparen. Maar de randvoorwaarden waaraan het netwerk te allen tijde moet voldoen zijn toen niet, en ook nu nog niet, uitgewerkt in beleid. Geld lijkt vaak een belangrijke drijfveer voor Defensie te zijn bij strategische keuzes voor het NAFIN. Hierdoor werd het netwerk in 2001 bijna aan de markt verkocht. Tevens heeft de minister van Defensie ervoor gekozen om het netwerk fors uit te breiden voor civiele partners, zoals de ministeries. Technisch gezien is hier goed over nagedacht. Maar we missen bij dit soort besluiten beleid en scenario's die verder kijken dan de techniek. Hoe groot mag het NAFIN eigenlijk worden? En wie mag er wel of geen gebruik van maken?

Op dit soort vragen heeft de minister van Defensie nog geen antwoord. Defensie geeft aan dat overheidspartijen mogen worden aangesloten 'zolang het Defensie-belang niet wordt geschaad', maar dit is niet verder geconcretiseerd. Ook is het netwerk niet door de minister van Defensie aangewezen als 'vitaal' voor de Nederlandse samenleving, terwijl meerdere processen die wel 'vitaal' zijn niet kunnen functioneren zonder het NAFIN. Bovendien weten we dat als het netwerk uitvalt, de maatschappelijke gevolgen groot zijn. Dat zagen we op 28 augustus 2024, toen door een storing bij het NAFIN de krijgsmachtonderdelen, Eindhoven Airport, de hulpdiensten, gemeenten, DigiD en de Kustwacht in de problemen kwamen.

Fysieke beveiliging van het NAFIN is onvoldoende

Het netwerk moet vanwege het maatschappelijke belang aan de hoogste beveiligingseisen voldoen. Maar een tweede conclusie is dat de fysieke beveiliging van het NAFIN onvoldoende is. We zien dat het NAFIN technisch gezien goed opgezet is. Het ministerie van Defensie zorgt ervoor dat het netwerk regelmatig updates krijgt zodat het aan de laatste technische standaarden voldoet. De glasvezelkabels zijn zo aangelegd dat er voldoende uitwijkmogelijkheden zijn voor het dataverkeer als er sprake is van een kabelbreuk. De kans op totale uitval van het netwerk is klein en de beschikbaarheid van het netwerk hoog. Op papier heeft

Defensie een goed beveiligingsbeleid voor het NAFIN. Er zijn middelen om een cyberaanval te detecteren en er zijn procedures om hier goed op te reageren.

Echter, in de praktijk zien we dat de detectiemiddelen niet volledig worden benut. Ook de fysieke toegang tot het netwerk op Defensie-locaties is onvoldoende beveiligd. Hoewel er op papier strikte toegangsprocedures zijn, kregen wij in de praktijk in alle 3 de testen als onbevoegden de sleutels tot de netwerkruimtes mee. In 2 gevallen ging er een alarm af bij het netwerk, maar werd er niet adequaat geïntervenieerd door medewerkers van Defensie.

Vergelijkbare bevindingen bij de beveiliging van militaire objecten deden wij in ons verantwoordingsonderzoek naar Defensie in 2022 en 2023.[1] De urgentie bij de minister van Defensie om de tekortkomingen in de beveiliging van militaire objecten aan te pakken bleek te ontbreken. Het is zorgelijk dat we soortgelijke bevindingen bij de beveiliging van het NAFIN aantreffen. Dit leidt ons tot de conclusie dat Nederland in een zeer gespannen geopolitieke situatie militair gezien onvoldoende alert is op sabotagerisico's door statelijke actoren.

Beperkte militaire regie en controle vanuit Defensie over het netwerk
De derde conclusie is dat het ontbreekt aan militaire regie en controle vanuit Defensie over het netwerk. Om de glasvezelkabels voor het NAFIN aan te leggen heeft de minister van Defensie een contract afgesloten met KPN. De minister van Defensie werd in dat contract de economisch eigenaar van het NAFIN. KPN werd de juridisch eigenaar. Dat betekent dat het netwerk in feite niet volledig *military owned* is en Defensie afweek van deze eigen randvoorwaarde. Defensie is afhankelijk van KPN voor aanleg en aanpassingen in het netwerk en kan praktisch gezien niet meer overstappen op een andere provider. KPN huurt voor het werk aan de glasvezel onderaannemers in, die op hun beurt weer onderaannemers kunnen inschakelen.

Om werk aan KPN uit te besteden moet Defensie staatsgeheime informatie met KPN delen, zoals informatie over waar de NAFIN-kabels liggen of waar de netwerkruimtes precies staan. Defensie toetst daarom KPN om te onderzoeken of het bedrijf genoeg beveiligingsmaatregelen neemt om deze geheime informatie te beschermen. Wanneer het hieraan voldoet krijgt het een autorisatie om aan het werk te gaan. KPN is er vervolgens voor verantwoordelijk dat zijn onderaannemers getoetst worden door Defensie en geldige autorisaties hebben. Wij constateren dat de verplichte autorisatie bij 1 van de 3 onderaannemers van KPN al sinds 2021 verlopen was. Defensie was hier niet van op de hoogte. Het zicht van Defensie op welke bedrijven de onderaannemers op hun beurt vervolgens inschakelen en welke veiligheids-maatregelen zij nemen, is nog beperkter.

We concluderen daarom dat Defensie te weinig overzicht en grip heeft op wie er aan de kabels van het NAFIN werken. Daarnaast is Defensie voor de beveiliging van het netwerk afhankelijk van hoe zijn gebruikers het netwerk behandelen en beveiligen. Defensie stelt aansluitvoorwaarden en beveiligingseisen voor het NAFIN op, maar controleert niet of zijn gebruikers zich hieraan houden.

Het NAFIN wordt momenteel door een kleine groep technici van Defensie goed ingericht en aangepast aan de laatste standaarden. Maar het veilig houden van het netwerk, zeker in tijden van sabotage op vitale infrastructuur op land en op zee in Europa, is een gezamenlijke verantwoordelijkheid van vele partijen. Ook de beveiligings- en bewakingsorganisatie en het IT Operations Center van Defensie hebben een belangrijke rol in het beschermen van dit netwerk. Ook buiten het ministerie van Defensie liggen verantwoordelijkheden voor het veilig houden van het NAFIN: bij de gebruikers van het netwerk binnen de rijksoverheid, bij de contract-manager van KPN en bij de onderaannemers die aan het netwerk werken. Het is aan de minister van Defensie als economisch eigenaar van dit netwerk, om hier regie en controle op te voeren en het netwerk beter te beschermen voor de toekomst.

1.1 Aanbevelingen

Aanbevelingen aan de minister van Defensie:

- Ontwikkel een strategische visie op de rol van dit netwerk in de Nederlandse samenleving voor nu en in de toekomst, bepaal welke bescherming, mensen en middelen daarvoor nodig zijn en verklaar het NAFIN tot ‘vitaal’.
- Neem maatregelen om zowel de detectie van als respons op ongeoorloofde toegang tot het netwerk te verbeteren. Er moet continue monitoring zijn door Defensie op mogelijke sabotage en spionage op de NAFIN-kabels. Het veiligheidsbewustzijn van de betrokken medewerkers van Defensie, KPN en de onderaannemers moet verder omhoog en de beveiliging van NAFIN-netwerk-ruimtes moet periodiek fysiek en digitaal getest worden.
- Overweeg of het mogelijk is het werk aan minder partijen uit te besteden en houd beter toezicht op de uitvoering van de beveiligingsmaatregelen en autorisaties voor de private partijen en hun onderaannemers die aan het NAFIN moeten werken, om te voorkomen dat staatsgeheime informatie over het NAFIN in de verkeerde handen terecht komt.

2. Over het onderzoek

De Algemene Rekenkamer onderzoekt het presteren en functioneren van de rijksoverheid. IT- voorzieningen zijn voor de overheid tegenwoordig onmisbaar om de burger te bedienen en resultaten te boeken. Daarom onderzoeken wij regelmatig hoe de IT beveiligd is en kijken we naar de algoritmen en cloudtoepassingen die de overheid gebruikt. Ook hebben we oog voor informatiebeveiliging en cybersecurity.

Sinds 2018 onderzoekt de Algemene Rekenkamer hoe Nederland zijn vitale infrastructuur beschermt tegen cyberdreigingen. We doen hier onderzoek naar omdat uitval, verstoring of misbruik van IT-systemen kan leiden tot maatschappelijke ontwrichting. In 2019 publiceerden we het onderzoek *Digitale dijkverzwaring: cybersecurity en vitale waterwerken*[2] bij Rijkswaterstaat en in 2020 volgde ons onderzoek *Digitalisering aan de grens*[3] naar de cybersecurity van het grenstoezicht door de Koninklijke Marechaussee op Schiphol. Kenmerkend voor de onderzoeken in deze reeks is dat we verder kijken dan 'papier en beleid'. We voeren digitale en fysieke praktijktesten uit in samenspraak met de gecontroleerde (zie de methodologische verantwoording).

2.1 Wat is het NAFIN?

Voor dit onderzoek onderzochten wij een essentieel communicatienetwerk voor de rijksoverheid en voor Defensie in het bijzonder: het *Netherlands Armed Forces Integrated Network* (NAFIN). Dit is een glasvezelnetwerk dat door heel Nederland ligt, separaat van het reguliere glasvezelnetwerk dat Nederlanders gebruiken voor het internet. Dit netwerk is voortgekomen uit een publiek-private samenwerking tussen het ministerie van Defensie en Koninklijke PTT Nederland N.V. (verder te noemen KPN).

KPN is juridisch gezien de eigenaar van het netwerk. Defensie is economisch gezien de eigenaar en heeft exclusief eeuwigdurend gebruikersrecht. Het ‘gesloten’ glasvezelnetwerk staat los van het internet. Het is zo’n 3.500 kilometer lang en maakt het mogelijk data te versturen voor de uitvoering van overheidstaken.

Figuur 1 *Het NAFIN is een eigenstandig glasvezelnetwerk van het ministerie van Defensie (fictieve weergave)*

Het NAFIN verbindt niet alleen zo’n 180 Defensie-locaties met elkaar, maar ook 70 locaties die niet van Defensie zijn. Dit zijn onder meer alle andere ministeries en de 4 overheidsdatacenters, de Eerste Kamer en de Tweede Kamer, politielocaties en de meldkamers van 112. Bovendien maakt het NAFIN koppelingen met de militaire netwerken van België en Duitsland en met het NAVO-hoofdkwartier. Zonder dit netwerk kunnen Defensie en de rijksoverheid niet effectief communiceren.

2.2 Waarom onderzoeken we het NAFIN?

De geëxplodeerde Nordstream-pijpleiding, opgepakte spionnen met explosieven voor militaire transporten, talloze doorgeknipte internetkabels op zee en op land en in juli 2024 grootschalige sabotage van het Franse treinverkeer. Er heeft de afgelopen jaren een toenemend aantal sabotageacties plaatsgevonden op kritieke Europese infrastructuren. De daders worden niet altijd gevonden. Maar duidelijk is dat sinds de invasie van Rusland in Oekraïne deze vorm van hybride oorlogsvoering in Europa toeneemt. Volgens de inlichtingen- en veiligheidsdiensten is het risico van sabotage op kritieke, vitale digitale infrastructuren reëel en actueel.

De Militaire Inlichtingen- en Veiligheidsdienst (MIVD) waarschuwt al dat Russische spionageschepen in de Noordzee de Nederlandse energievoorziening in kaart proberen te brengen.

Waar we ons in de eerste twee cybersecurityonderzoeken hoofdzakelijk focusten op het cybersecurityrisico van software, richten we ons gezien de dreiging nu op de hardware van een digitale infrastructuur: de fysieke kabels van het NAFIN en de routers op het netwerk die het dataverkeer mogelijk maken. We onderzoeken hoe kwetsbaar deze onderdelen zijn voor cyberdreigingen. In het vakgebied van cybersecurity worden kwetsbaarheden over het algemeen onderverdeeld in risico's ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid. De beschikbaarheid van het NAFIN kan in het geding komen als iemand fysieke toegang krijgt tot de glasvezelkabel of de netwerkruimtes en de werking hiervan saboteert. De integriteit van het netwerk kan worden aangetast wanneer bijvoorbeeld de configuratie van de routers wordt aangepast. En tot slot kan de vertrouwelijkheid van het NAFIN worden geschaad wanneer de glasvezelkabels worden afgetapt voor spionage.

Defensie maakt om veiligheidsredenen weinig informatie publiekelijk bekend over het NAFIN. De Algemene Rekenkamer heeft er vanwege het belang van dit onderwerp wel voor gekozen een openbaar rapport te schrijven. Tijdens het rapportageproces hebben we het rapport voorgelegd aan de beveiligingsautoriteit van Defensie en aan de MIVD om ons te laten adviseren of wat er in dit rapport staat openbaar kan worden. Rapporten van de Algemene Rekenkamer zijn in beginsel openbare stukken. De Comptabiliteitswet 2016 legt aan de Algemene Rekenkamer bij de openbaarmaking van onderzoek nauwelijks beperkingen op. Het beleid van de Algemene Rekenkamer is openbaarmaking van onderzoeksbevindingen achterwege te laten als dit onevenredig grote schade aan bepaalde belangen zou kunnen toebrengen. In het geval van dit onderzoek is ervoor gekozen bepaalde informatie alleen vertrouwelijk te delen met de Tweede Kamer.

2.3 Wat hebben we onderzocht?

De Algemene Rekenkamer heeft onderzocht hoe de minister van Defensie ervoor zorgt dat het NAFIN weerbaar is tegen cyberaanvallen. Hiervoor waren onderstaande onderzoeksvragen leidend.

Hoofdvraag

Hoe kwetsbaar is het publiek-private krijgsmachtnetwerk NAFIN voor cyberaanvallen?

Onderzoeksvragen

1. Wat zijn de doelen van het krijgsmachtnetwerk NAFIN en wie maken er gebruik van?
2. Functioneert de publiek-private samenwerking t.a.v. cybersecurity van het krijgsmachtnetwerk NAFIN voldoende?
   a. Is er een duidelijke verantwoordelijkheidsverdeling tussen de minister van Defensie en de private partijen?
   b. Zijn de private partijen geautoriseerd om aan het netwerk te werken en is het toezicht hierop voldoende?
   c. Welke afspraken zijn gemaakt met aansluitende publieke partijen over cyberveiligheid en is het toezicht hierop voldoende?
4. Beschikt het krijgsmachtnetwerk NAFIN over doeltreffende detectie-maatregelen? (opzet en bestaan)
5. Zijn er heldere responsscenario's bij incidenten op het krijgsmachtnetwerk NAFIN en zijn deze responsmaatregelen effectief? (opzet en bestaan)
6. Zijn de detectie- en responsmaatregelen voor het krijgsmachtnetwerk NAFIN effectief in de praktijk? (werking)

2.4 Onderzoeksmethoden

Voor het beantwoorden van de onderzoeksvragen bestudeerden we in de periode november 2023 tot en met maart 2024 openbare bronnen en interne documenten bij het ministerie van Defensie. Ook deden we onderzoek ter plekke bij het IT Operations Center van Defensie (ITOC) en spraken we met medewerkers van KPN. We waren 2 keer aanwezig bij werkzaamheden aan het NAFIN, zowel binnen in een netwerk-ruimte als buiten langs de openbare weg. We voerden gesprekken met betrokkenen bij het NAFIN op verschillende niveaus in de organisatie. Hierbij keken we naar de opzet van de maatregelen en voorbeelden van de werking in de praktijk.

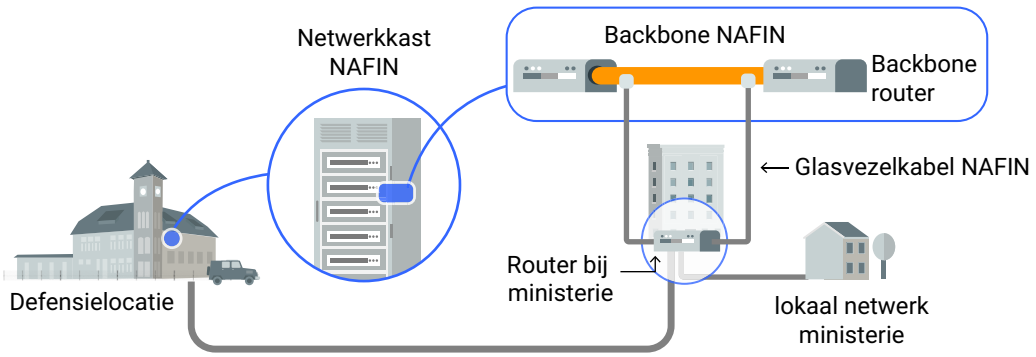
Op ons initiatief hebben we voor dit onderzoek samen met specialisten van het ministerie van Defensie de weerbaarheid van het netwerk in de praktijk getoetst met inlooptesten en een digitale test. Als normenkader voor ons onderzoek hanteerden we het cybersecurityraamwerk van het National Institute of Standards and Technology (NIST, zie methodische bijlage).

2.5 Afbakening

Om goed te functioneren heeft het NAFIN zowel hardware- als softwareonderdelen nodig. De hardware betreft de glasvezelkabels in de grond en de routers daarop die ervoor zorgen dat data fysiek van A naar B over de kabel kunnen stromen. Er is software is nodig om dit efficiënt, betrouwbaar en integer te laten gebeuren. Zoals uit figuur 2 blijkt, richt de scope van ons onderzoek zich op de hardware die noodzakelijk is om dit dataverkeer mogelijk te maken. We hebben het dataverkeer zelf niet onderzocht. Voor dit onderzoek kijken we uitsluitend naar de kern van het NAFIN dat door Defensie wordt beheerd. We laten de lokale netwerken van alle gebruikers die zijn aangesloten buiten beschouwing.

Figuur 2 *Scope van het onderzoek*

Dit onderzoek richt zich op de hardware van het NAFIN

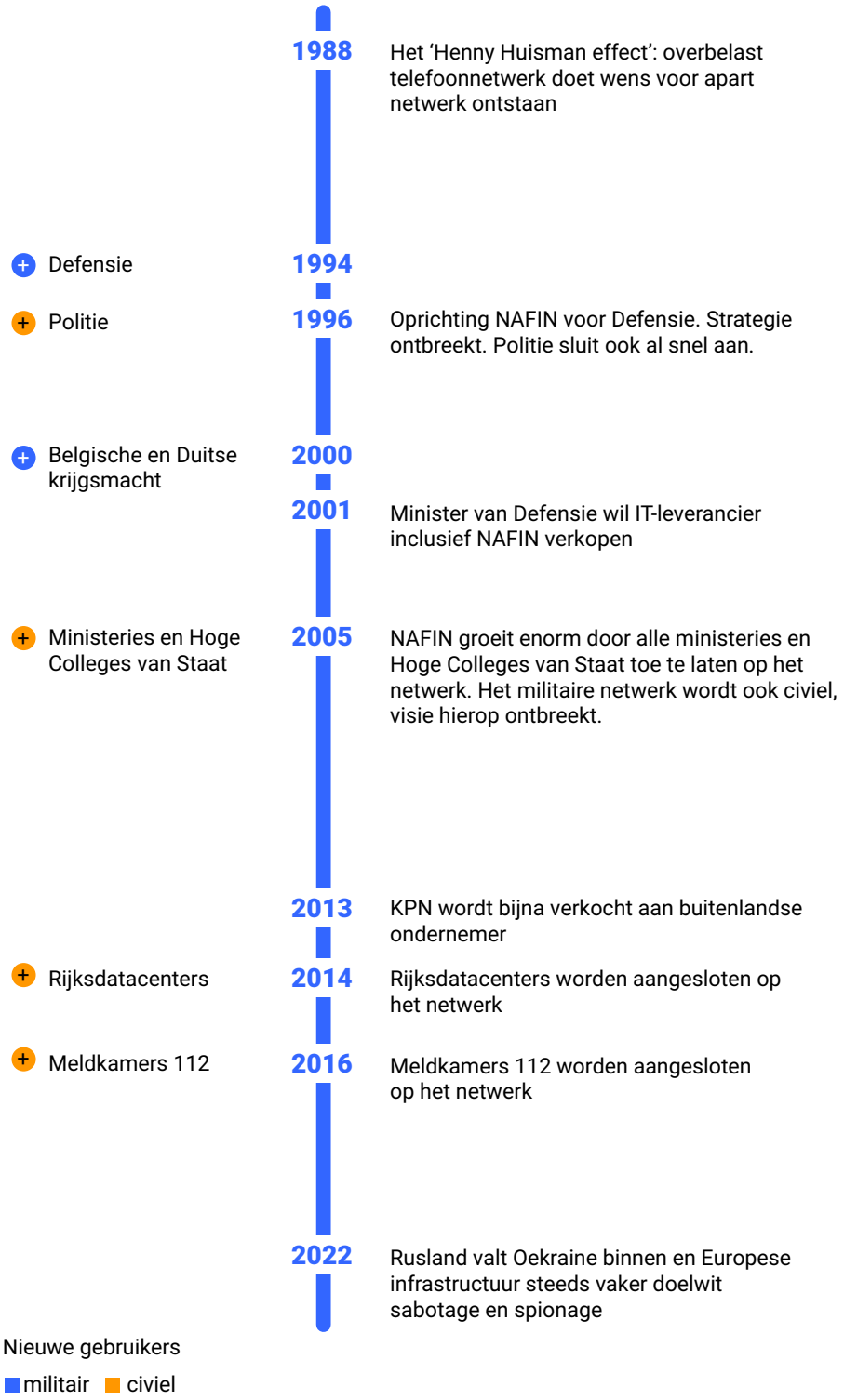


2.6 Leeswijzer

We vervolgen het rapport met hoofdstuk 3 over het ontstaan van het NAFIN in 1996 en de ontwikkeling die het netwerk sindsdien heeft doorgemaakt. We beantwoorden in dit hoofdstuk de eerste onderzoeksvraag over de doelen en de gebruikers van het NAFIN. In hoofdstuk 4 rapporteren we over de beveiliging van het NAFIN en behandelen we de onderzoeksvragen over detectie en respons. Ook lichten we hier de resultaten uit de praktijktesten toe. In hoofdstuk 5 volgen de resultaten over de

publiek-private samenwerking met KPN en over de cybersecuritymaatregelen die Defensie heeft genomen. In hoofdstuk 6 staan de conclusies en aanbevelingen en we sluiten het rapport af met de reactie van de minister van Defensie en ons nawoord in hoofdstuk 7.

Figuur 3 *Tijdlijn belangrijke momenten in de ontwikkeling van het NAFIN*



3. De ontwikkeling van het NAFIN

In dit hoofdstuk gaan we terug naar de start van het NAFIN in 1996, wat was de aanleiding voor de oprichting en hoe is het NAFIN sindsdien gegroeid? Deze achtergrond is van belang om het huidige NAFIN te begrijpen. Vervolgens kijken we hoe het NAFIN zich sindsdien heeft ontwikkeld van een militair netwerk naar ook een civiel netwerk. We eindigen met de staat van het NAFIN in 2024. In deze ontwikkeling die in figuur 3 in een tijdlijn staat weergegeven zien wij een eerste kwetsbaarheid van het NAFIN. Al vanaf 1996 ontbreekt het aan een strategie die verder kijkt dan techniek. Ook in 2024 heeft de minister van Defensie nog geen strategische visie op NAFIN.

3.1 Oude militaire verbindingen

NAFIN ontstond in de jaren 90 van de vorige eeuw. Voor die tijd communiceerde Defensie via verschillende militaire verbindingsstelsels. Daarnaast was het nodig om extra verbindingen te huren bij het toenmalige Staatsbedrijf der Posterijen, Telegrafie en Telefonie (PTT), nu KPN. De kosten van die inhuur stegen omdat de behoefte om data te versturen sterk toenam. Al in 1973 lag er een advies om de verbindingsstelsels van Defensie te integreren en daarmee kosten te besparen. Dit advies kwam van een speciale commissie van civiele en militaire deskundigen die gevraagd waren de minister-president en de minister van Defensie, na kritisch onderzoek, te adviseren hoe Nederland haar taak bij de NAVO het beste kon invullen. Pas in de jaren 90 kwam dit advies opnieuw op tafel. Toen bleken de verouderde defensieverbindingen aan vervanging toe. Ook liet de staatssecretaris van Defensie aan de Tweede Kamer weten te voorzien dat door privatisering van PTT de kosten van de huurverbindingen zouden oplopen met een factor 6, tot 80 miljoen gulden (omgerekend nu € 36 miljoen) per jaar.

Het huren van telefoonlijnen bij KPN was niet alleen duur, het maakte Defensie ook afhankelijk van het niet-militaire communicatieverkeer in Nederland. En dat kon kwetsbaar zijn, bleek al in 1988. Tijdens de finale van het televisieprogramma de Soundmixshow deed presentator Henny Huisman voor het eerst in de televisie-geschiedenis een oproep aan kijkers om telefonisch hun stem door te geven voor hun favoriete kandidaat. Ongeveer 1 miljoen mensen belden tegelijkertijd met een overbelast landelijk telefoonnet als gevolg. Tijdelijk was niemand in Nederland telefonisch bereikbaar. Hulpdiensten konden niet gebeld worden, vliegtuigen konden niet meer landen op Schiphol en ook Defensie was dus niet meer in staat te communiceren. Door dit incident realiseerde Defensie zich dat het niet zelf de volledige regie had over de eigen communicatie. Het netwerk dat Defensie toen gebruikte, werd immers gebruikt door heel Nederland.

3.2 Naar één nieuw glasvezelnetwerk

Begin jaren 90 werd het plan om voor Defensie 1 eigen glasvezelnetwerk te bouwen concreet. Het project *Netherlands Armed Forces Integrated Network* (NAFIN) zou de verouderde bestaande stelsels vervangen, goedkoper zijn en in de toekomstige verbindingsbehoefte kunnen voorzien. Voor Defensie was het bovenal van belang dat commandanten van de krijgsmachtsonderdelen met behulp van het NAFIN operaties konden plannen, leiden en de inzet van eenheden en wapensystemen konden controleren. Of dit nu bij crisis, oorlog of tijdens vredesmissies was. Defensie wilde in alle denkbare situaties veilig kunnen communiceren. Daarom stelde Defensie als randvoorwaarde voor NAFIN dat het netwerk nooit uit zou mogen vallen. Never out noemde Defensie dat. Wat Defensie onder deze randvoorwaarde precies verstaat en welke eisen daaruit voortvloeien is op dat moment, maar ook later niet uitgewerkt.

Een tweede randvoorwaarde was dat het netwerk *military owned and controlled* moest zijn. Dit wil zeggen dat Defensie de volledige beschikkingsmacht heeft over het netwerk en daarbij niet afhankelijk is van derden. Defensie moet zelf het netwerk operationeel kunnen houden, wijzigingen aan kunnen brengen of herstelacties uit kunnen voeren wanneer delen van het netwerk uitvallen. Deze randvoorwaarde is toen niet en nog steeds niet duidelijk afgebakend of vertaald in normen voor het netwerk.

Het bleek echter niet mogelijk helemaal onafhankelijk van de private markt te opereren. Voor de aanleg van het glasvezelnetwerk was Defensie toch nog afhankelijk van KPN. Dit had 2 redenen. Allereerst heeft Defensie in vredestijd geen ‘grond-roerdersrechten’ en mag het dus niet in de bodem graven om een glasvezelnetwerk

aan te leggen. Ten tweede zou Defensie met de aanleg van het NAFIN een netwerk-provider worden, en het kabinet had besloten dat die zich moest houden aan de Telecommunicatiewet. Dit betekende dat Defensie andere partijen zou moeten toelaten op het netwerk als die daarom verzochten. Daarnaast vereiste deze wet registratie van het NAFIN zodat het zichtbaar zou zijn voor iedereen die in de grond wil graven. Vanwege het vertrouwelijke karakter van het dataverkeer was dit voor Defensie niet wenselijk, het wenste de locatie van het netwerk geheim te houden.

Al met al moest Defensie dus toch uitwijken naar een private partij. Alleen KPN kon aan alle voorwaarden van Defensie voldoen. In 1994 sloot Defensie een raam-overeenkomst met KPN. Daarin legden de partijen vast dat PTT-Telecom de juridische eigenaar van het NAFIN werd, maar Defensie het exclusieve economische gebruikersrecht op het netwerk zou krijgen. Als juridische eigenaar is KPN wettelijk gezien de eigenaar van het NAFIN, als economisch eigenaar is Defensie de exclusieve gebruiker en draagt het verantwoordelijkheid voor alle daarvoor aangewezen rechten en plichten. In 1996 was het NAFIN klaar.

3.3 NAFIN bijna verkocht

Het NAFIN is vanaf de start onderdeel van de Defensie Telematica Organisatie (DTO), dat een agentschap was van de Defensie Materieel Organisatie (DMO). Het agent-schap leverde IT-diensten aan Defensie en ketenpartners binnen de rijksoverheid. In 2001 maakte Defensie ten tijde van bezuinigingen serieuze plannen om de hele DTO, inclusief het NAFIN, te verkopen op de commerciële markt. Het NAFIN werd een belangrijk discussiepunt. Zowel de bevelhebbers van Defensie, medewerkers van de DTO als de civiele medegebruikers bij de ministeries van Binnenlandse Zaken en Koninkrijksrelaties en van Justitie en Veiligheid kwamen hiertegen in opstand. Zij gaven aan dat het belangrijk was dat het NAFIN om veiligheidsredenen *military owned and controlled* bleef.

De staatssecretaris van Defensie liet daarop een onderzoek uitvoeren om te kijken of uitbesteding van het NAFIN mogelijk zou zijn. De staatssecretaris concludeerde uit deze onderzoeken dat dit onder bepaalde stringente voorwaarden kon. Ook een eventuele ontvlechting van het NAFIN uit de DTO kwam ter sprake. De medezeggen-schapsraad van de DTO sprak zich uiteindelijk in een open brief in het NRC Handelsblad uit tegen de verkoop van de DTO uit: ‘‘Elke vorm van ontvlechting van het beheer van het glasvezelnetwerk, zal deze complexiteit exponentieel doen toenemen en daarmee de kosten onbeheersbaar maken.’’

De medezeggenschaapsraad van de DTO was dus tegen het ontvlechten van het NAFIN. Bovendien zou eventuele verkoop van de DTO zonder het NAFIN financieel niet aantrekkelijk zijn. Het NAFIN was ‘de kip met de gouden eieren’ die zorgde voor inkomsten voor DTO. Daarnaast zou de overheid als klant van het NAFIN afhaken als het in private handen zou komen. Uiteindelijk besloot de staatssecretaris van Defensie het NAFIN en de DTO, vanwege het belang van de veiligheid van het NAFIN, niet uit te besteden.

3.4 Van militair naar civiel netwerk

Al vanaf het begin van het NAFIN zegde de staatssecretaris van Defensie de Tweede Kamer toe te onderzoeken of het militaire netwerk eveneens geschikt was voor andere gebruikers. Dit bleek zo te zijn en er was interesse. Nog in het jaar dat het NAFIN operationeel werd, sloot de politie een overeenkomst om haar netwerk op het NAFIN aan te sluiten.

Zoals in paragraaf 3.3 beschreven maakte het NAFIN deel uit van de DTO. Dit was een agentschap van het ministerie van Defensie, dat zijn eigen geld moet verdienen als ICT-bedrijf van Defensie. Vanuit deze financiële doelstelling dacht Defensie na over het businessmodel van het NAFIN. Hoe meer verbindingen in het NAFIN zouden worden aangelegd, hoe lager de kostprijs. “Medegebruik door andere overheden is niet alleen voordelig voor de schatkist, maar levert tevens voor Defensie budgettaire voordelen op, omdat de tarieven dan omlaag gaan”, zo staat in een interne Defensienotitie. Defensie richtte zich voor dat medegebruik in eerste instantie op de aanverwante sectoren openbare orde en veiligheid van de rijksoverheid.

Maar het NAFIN beperkte zich niet tot deze sectoren, zo bleek toen een grotere groep nieuwe gebruikers zich meldde. Net als Defensie een decennium eerder, ontstond bij de gehele rijksoverheid begin jaren 2000 de wens om afzonderlijke netwerken te integreren om zo kosten te besparen. Eerst moesten de hoofd-vestigingen van de ministeries met elkaar worden verbonden in een ‘Haagse Ring’. Maar uiteindelijk was het grotere plan om ook uitvoeringsorganisaties van de rijksoverheid buiten Den Haag aan dit netwerk te koppelen.[4] We hebben in de archieven niet kunnen terugvinden wanneer en waarom de rijksoverheid het verzoek deed om dit netwerk aan het NAFIN te koppelen. Wel blijkt dat de secretaris-generaal van Defensie werd aangewezen als politiek opdrachtgever van het project om de ICT-netwerken van de rijksoverheid te bundelen.[5] Ook constateren we dat Defensie een onderzoek heeft gedaan naar de veiligheid van medegebruik van het NAFIN. “Door het aansluiten van externe partijen op NAFIN ontstaat er risico dat

kwaadwillenden van buiten Defensie het defensiegebruik van NAFIN kunnen verstoren (..) dit kan tot een mogelijk gevaar voor de staatsveiligheid leiden" staat in een interne Defensienota uit 2003. Dit alles leidde tot een uitgebreid onderzoek van Defensie naar de vraag hoe dit medegebruik veilig kon worden vormgegeven.
Een interne stuurgroep concludeerde dat als men zich aan bepaalde kaders houdt veilig medegebruik mogelijk is. Het betrof een voornamelijk technische afweging. Een strategische afweging of onderbouwing voor deze keuze lag hier niet aan ten grondslag.

In 2005 tekende de DTO waartoe het NAFIN behoorde een mantelovereenkomst met de ministeries. De Haagse Ring voor communicatie tussen kerndepartementen kon worden gebouwd en op het NAFIN worden aangesloten. Dit zien wij als een belangrijk strategisch moment voor het netwerk. Het NAFIN veranderde daarmee van karakter: niet langer was het een puur militair netwerk, het NAFIN maakte vanaf dat moment de communicatie van en tussen civiele partijen mogelijk. Bovendien betekende dit besluit dat Defensie zich tot en met de dag van vandaag zou commiteren aan het zijn van een belangrijke IT-leverancier van hardware voor de rest van de overheid.

3.5 Een groeiend netwerk

In de jaren daarna sloten steeds meer rijksoverheidlocaties aan op het NAFIN. Diensten en uitvoeringsorganisaties van binnen en buiten Den Haag. Ook de Hoge Colleges van Staat, zoals de Eerste en de Tweede Kamer en de Algemene Rekenkamer maken inmiddels gebruik van het NAFIN. De rijksoverheid koos er uiteindelijk voor om ook de verbindingen tussen de 4 overheidsdatacenters (ODC's), waarvan een aantal buiten Den Haag staat, via het NAFIN te laten verlopen. In deze overheidsdatacenters worden alle servers van de rijksoverheid draaiende gehouden. Met deze datacenters erbij is het NAFIN de digitale infrastructuur geworden waar het gehele rijksoverheidsnetwerk op draait.

En naast deze nieuwe grote groep gebruikers bleef het NAFIN verder groeien. Zo sloten in 2016 de meldkamers van 112, die zorgen voor communicatie met hulp-diensten, aan. Bovendien legde het NAFIN koppelingen met het netwerk van het hoofdkwartier van de NAVO in Brussel en met de Belgische en Duitse militaire netwerken.

Met elke koppeling die het NAFIN maakt met een nieuwe gebruiker, neemt het belang dat het netwerk nooit mag uitvallen verder toe. Tegelijkertijd kunnen nieuwe gebruikers voor problemen zorgen op het netwerk. Eind 2022 bleek in een incident

dat het combineren van militair en civiel dataverkeer niet zonder risico is. Een grote hoeveelheid verzonden data van de Belastingdienst op het netwerk zorgde ervoor dat de militaire luchtverkeersleiding niet meer kon communiceren (zie kader en figuur 4 hierna). Binnen het NAFIN is technisch geregeld dat bepaalde verbindingen voorrang krijgen op andere, maar in dit geval werkte dit mechanisme niet goed. Na het vaststellen van de oorzaak van het probleem heeft Defensie meteen mitigerende maatregelen getroffen en geïmplementeerd. Dit probleem werd opgelost en heeft zich niet meer voorgedaan. Het geeft wel aan dat het civiele dataverkeer in een incident als dit de veiligheid van Defensie kan beïnvloeden.

Combineren militair en civiel dataverkeer niet zonder risico

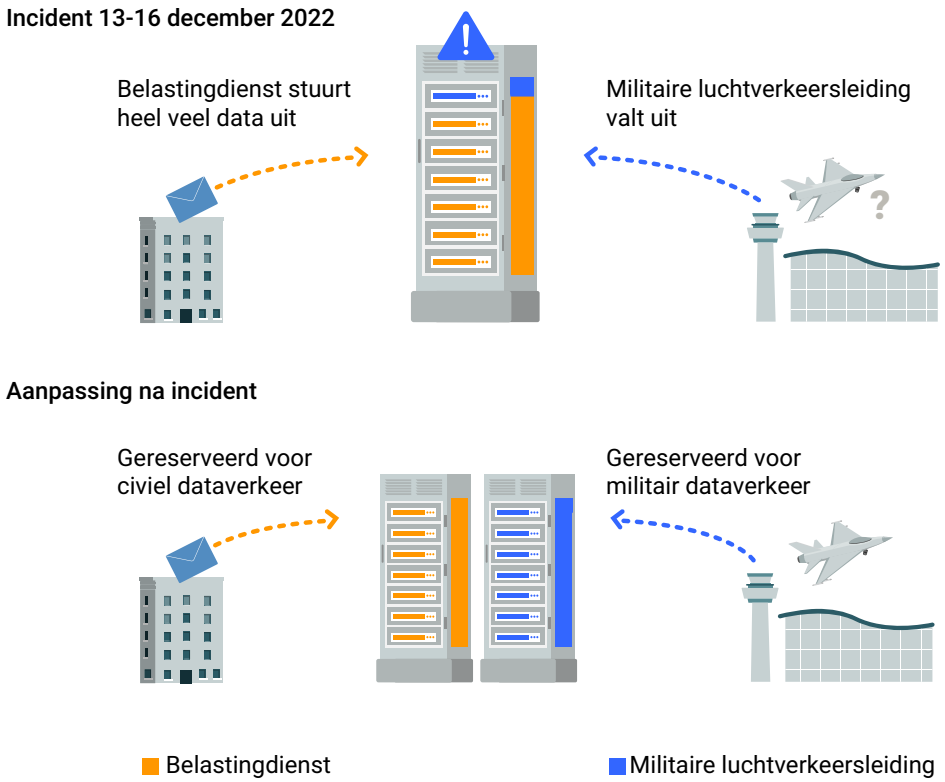
Op 5 december 2022 komt er een melding van een verstoring binnen bij de Servicedesk Defensie. Een IT-afdeling moet met spoed nakijken of er op 5 verschillende dagen – de eerste is 18 november – verstoringen zijn geweest op een aantal specifieke verbindingen. Het gaat om verbindingen die in gebruik zijn bij de militaire luchtverkeersleiding en de vliegveiligheid in het gedrang kunnen brengen. Defensie kan op dat moment de oorzaak van de verstoringen nog niet vinden.

Op 13 december stuurt een majoor een bericht rond met ‘Spoed!!!: de communicatiesystemen van de militaire luchtverkeersleiding werken niet’. Escalatie volgt. De volgende dag komt een aantal teamleden van NAFIN bijeen. De majoor licht tijdens de meeting de impact van de verstoring toe en maakt duidelijk dat ze snel verholpen moet worden. De verstoringen zijn zo ernstig dat er serieuze operationele beperkingen aan de gebruikers zijn opgelegd. Op een aantal militaire vliegvelden is het luchtverkeer beperkt. De lokale luchtverkeersleiding kan op sommige momenten niet meer met de centrale luchtverkeersleiding op Schiphol communiceren, noch met de vliegers in de lucht. De vraag is of de militairen nog door kunnen gaan met vliegen of dat dit preventief moet worden stopgezet.

Op dat moment lijkt de oorzaak van het probleem in NAFIN te zitten, maar doordat het probleem maar af en toe optreedt en omdat de hele keten van systemen complex is, is het nog niet duidelijk wat het probleem veroorzaakt. Dagelijks is er een voortgangscall. 3 dagen na het begin van de escalatie wordt de oorzaak van de verstoring gevonden. De verstoring is veroorzaakt door ‘verkeersdrukte’ op de hoofdring van het netwerk. Het blijkt dat op 2 andere verbindingen de Belastingdienst enorme hoeveelheden data verstuurde, zoveel dat het de datacapaciteit op de verbinding van de luchtverkeersleiding wegdrukte.

Figuur 4 *Illustratie incident en aanpassing die Defensie daarna heeft doorgevoerd*

Hoe de Belastingdienst per ongeluk militaire luchtverkeersleiding stillegde



Tot op heden is een aantal zaken over het medegebruik van het NAFIN nog onduidelijk. Defensie krijgt bijvoorbeeld nog steeds verzoeken om meer gebruikers toegang te geven tot het NAFIN. Hoe groot wil Defensie het netwerk laten worden? En wat moet de balans zijn tussen Defensie-gebruikers en gebruikers vanuit de rijksoverheid? We troffen geen richtlijnen of visie aan over hoe groot het mede-gebruik mag worden. Defensie gaf aan dat overheidspartijen mogen worden aangesloten ‘zolang het Defensiebelang niet wordt geschaad’, maar dit is niet verder geconcretiseerd.

3.6 Een vitaal netwerk?

Het valt op dat de minister van Defensie het NAFIN niet heeft aangemerkt als ‘vitaal’, in tegenstelling tot andere cruciale overheidsprocessen. Het officieel aanmerken door een minister van een systeem, onderdeel of proces als ‘vitaal’ is een manier om de hoogste bestuurlijke aandacht binnen de rijksoverheid te krijgen wanneer dit nodig is. De term ‘vitaal’ wordt toegewezen als verstoring, uitval of manipulatie van een proces of dienst dermate ernstige gevolgen kan hebben dat deze de nationale

veiligheid kunnen schaden. Bij een crisis rond een vitaal proces of systeem wordt gelijk opgeschaald naar de hoogste bestuurstafels. Het ministerie dat verantwoordelijk is voor het systeem of proces bepaalt of het vitaal is of niet. De minister van Defensie heeft het NAFIN niet officieel aangewezen als vitaal, hoewel uitval van het NAFIN de nationale veiligheid wel degelijk kan schaden. Opvallend is dat het NAFIN randvoorwaardelijk is voor een aantal processen die op zichzelf wel de officiële stempel ‘vitaal’ hebben gekregen. Voorbeelden hiervan zijn de inzet van Defensie, de inzet van politie, de werking van de 112-meldkamers en informatieverschaffing vanuit de overheid aan burgers. Zonder het NAFIN kunnen deze belangrijke ‘vitale’ processen voor de Nederlandse samenleving geen doorgang vinden.

4. Beveiliging van het NAFIN

De digitale en fysieke beveiliging van het NAFIN moet vanwege de essentiële diensten die erop draaien van hoog niveau zijn. Defensie stelt de randvoorwaarde dat het netwerk nooit uitvalt. Het netwerk is technisch zo opgezet dat de kans op grootschalige uitval klein is. Maar omdat de maatschappelijke impact van grootschalige uitval heel groot is, zoals we op 28 augustus 2024 zagen, is de tolerantie voor kwetsbaarheden laag. In dit hoofdstuk kijken we hoe het NAFIN digitaal en fysiek beveiligd wordt, hoe opgemerkt kan worden of er iets aan de hand is en hoe Defensie hier vervolgens op reageert. We concluderen dat de beveiliging op papier op orde is, maar in de praktijk onvoldoende.

4.1 Beveiligingsbeleid en processen op orde

Volgens het integraal beveiligingsbeleid van Defensie moeten er regelmatig risicoanalyses worden gedaan op gehele systemen en netwerken zoals het NAFIN. Voor het NAFIN gebeurde dat in 2020 voor het laatst. Uit de dreigingsanalyse die deel uitmaakte van deze risicoanalyse komt naar voren dat statelijke actoren een steeds groter risico vormen. Daarnaast werd gewezen op mogelijkheden om glasvezelkabels af te tappen. Vervolgens heeft Defensie het NAFIN uitvoerig onderzocht met een aantal mogelijke dreigingen als richtlijn. Voorbeelden van dit soort dreigingen zijn het risico op uitval, op storingen, op cybercrime, op sabotage maar ook risico's naar aanleiding van natuurgeweld. Hieruit blijkt dat Defensie op het technische vlak veel maatregelen heeft genomen om de kwetsbaarheden op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid van het NAFIN te beperken. Maar er kwam ook een aantal kwetsbaarheden uit de risicoanalyse naar boven, die we vanwege de vertrouwelijke aard hier niet delen. We zien dat Defensie deze kwetsbaarheden na de

risicoanalyse heeft opgepakt. De volgende risicoanalyse staat voor eind 2024 gepland. Defensie verwacht dat er vanwege de huidige geopolitieke situatie meer dreigingen onderkend gaan worden dan in 2020.

Naast dit algemene beleid heeft Defensie beleid voor specifieke aspecten zoals de eerder beschreven personele beveiliging in de vorm van screeningen en industrieveiligheid in de vorm 'ABDO-autorisaties (Algemene Beveiligingseisen Defensieopdrachten)'. Tevens heeft Defensie beleid voor de fysieke beveiliging van locaties. Wanneer bijvoorbeeld een monteur op een NAFIN-locatie moet zijn voor werkzaamheden is er een toegangsprocedure afgesproken. Voor de netwerkruimtes is een speciale lijst met beveiligingsmaatregelen opgesteld, zoals eisen aan de stroomvoorziening en aan de beveiliging van de netwerkkasten. Tot slot zijn er eisen voor hoe belangrijke Defensie-systemen worden aangesloten op het netwerk. Zo moeten de belangrijkste systemen altijd via 2 kabels worden verbonden met het NAFIN zodat, wanneer 1 kabel stukgaat, het systeem alsnog kan functioneren.

Uiteraard is het de bedoeling dat dit NAFIN-beveilingsbeleid in de praktijk wordt opgevolgd. Ook moet er voortdurende monitoring van het netwerk en de fysieke omgeving van het netwerk plaatsvinden door Defensie. Op deze manier kan Defensie afwijkingen op tijd detecteren en maatregelen nemen. De fysieke en digitale toegang tot het netwerk zou moeten worden beperkt tot bevoegde gebruikers. Als onbevoegden toch toegang weten te krijgen tot het netwerk, zou de respons hierop van Defensie adequaat moeten zijn. In de volgende paragrafen bekijken we hoe het beleid in de praktijk wordt nageleefd.

4.2 Digitaal up-to-date, maar toch kwetsbaar

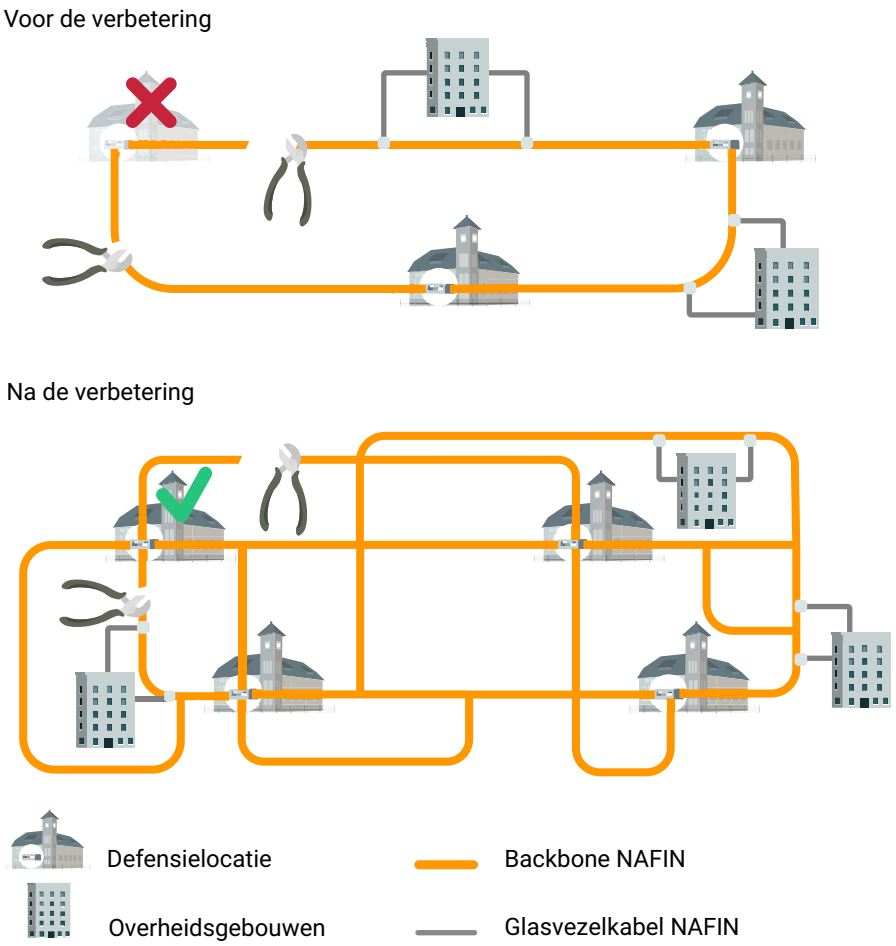
Het is belangrijk dat het NAFIN niet storingsgevoelig is en dat het alle data die worden verzonden kan verwerken. Een aantal aspecten is daarbij van belang. Het netwerk moet genoeg capaciteit hebben om het dataverkeer aan te kunnen. De structuur van het netwerk moet goed in elkaar zitten zodat dataverkeer kan worden omgeleid bij een storing en er moet goed autorisatiebeheer zijn zodat onbevoegden geen digitale toegang kunnen krijgen.

De mate van digitale communicatie nam vanaf de aanleg in 1996 enorm toe. Het NAFIN moest met de tijd meegaan en zijn capaciteit vergroten voor grotere hoeveelheden dataverkeer. Sindsdien verving Defensie alle actieve routers en groeide de bandbreedte van het netwerk. We constateren dat het technisch personeel van dit netwerk toegewijd werkt en kundig is. Zij maken strategische

plannen om het netwerk up-to-date te houden en zorgen voor het lifecycle-management. Dit is binnen de rijksoverheid geen vanzelfsprekendheid, maar het ministerie van Defensie heeft dit voor het NAFIN goed op orde. Naast deze specialisten werkt een team van Defensie-medewerkers in buitendienst aan het netwerk. Zij houden toezicht op de kwaliteit van het werk van de onderaannemers bij mutaties en projecten.

In de huidige versie van het netwerk zijn door het NAFIN-team wijzigingen in de structuur van het netwerk aangebracht om de beschikbaarheid en de capaciteit van het netwerk verder te verhogen. Wanneer het dataverkeer door een breuk in de glasvezelkabel ergens stokt, zijn er met de nieuwe update meer uitvalsmogelijk-heden om het dataverkeer toch via een andere route te laten plaatsvinden. De kans op totale uitval van het netwerk is daarmee klein en de beschikbaarheid van het netwerk hoog. Het aantal incidenten dat op het NAFIN plaatsvindt betreft ongeveer 25 verstoringen per jaar, bijna altijd veroorzaakt door graafschade. Maar er kan ook softwarematig een probleem optreden waardoor het gehele NAFIN geraakt wordt. Zo bleek op 28 augustus 2024 toen het NAFIN urenlang en bij sommige organisaties enkele dagen niet beschikbaar was.

Figuur 5 *Upgrade van het NAFIN*



Voor digitale toegang tot het netwerk zijn maatregelen genomen om ongewenste toegang tot het NAFIN of spionage van gegevens te voorkomen. Er is adequaat autorisatiebeheer, zodat gebruikers alleen toegang hebben tot de functionaliteiten die ze nodig hebben om hun taken uit te voeren. Zoals in figuur 5 te zien is heeft het NAFIN-team een upgrade aan het netwerk aangebracht om te zorgen dat data-stromen geheim blijven. Informatie over welke servers met elkaar communiceren, wat voor type verkeer wordt verstuurd en met welke prioriteit is geheim. De feitelijke data en de inhoud zijn veelal versleuteld zodat deze niet onmiddellijk zichtbaar zijn als iemand toegang krijgt tot de datastroom. Het versleutelen van de data gebeurt niet door het NAFIN-team, maar dit moeten de gebruikers van het netwerk zelf doen. Defensie houdt niet bij of dit ook daadwerkelijk gebeurt.

We hebben de digitale beveiliging in de praktijk getest. Het NAFIN-team heeft dit een aantal jaar geleden ook gedaan en de kwetsbaarheden die daaruit naar voren kwamen

destijds opgelost. Onze 3 nieuwe testen leverden opnieuw een aantal kwetsbaarheden op, zoals in paragraaf 4.5 blijkt.

4.3 Detectie op sabotage en spionage moet beter

De kabels van het NAFIN liggen overal door Nederland in de grond. De geografische kaart van het NAFIN is door Defensie gerubriceerd als staatsgeheim. Als de locatie van het netwerk bekend is kunnen statelijke actoren plannen maken voor sabotage of spionage van het netwerk. Defensie heeft geen aanwijzingen dat een dergelijke cyberaanval heeft plaatsgevonden. Maar ook per ongeluk kan het NAFIN beschadigd worden. Bij bouwwerkzaamheden wordt er weleens per ongeluk een kabel geraakt. Zo zijn kabels eens door een grasmaaier of door de palen van een circustent doorboord. Gemiddeld gaat circa 25 keer per jaar onbedoeld een NAFIN-kabel stuk.

De belangrijkste kabels die onder de grond liggen zijn bewaakt met een meter met een alarm. Wanneer een kabel te veel beweegt, in kwaliteit daalt of wordt doorgeknipt, geeft de meter een alarm af dat de glasvezelkabel niet naar behoren werkt. Dit alarm komt terecht bij het IT Operations Center (ITOC) van Defensie. Zo kan Defensie vroegtijdig een kabelbreuk of verdachte activiteiten opsporen. Dit scheelt Defensie in het geval van graafschade aan de kabels veel tijd. Het hoeft niet meer te wachten op een monteur die op locatie metingen kan verrichten waaruit blijkt waar de breuk zit. De meting is namelijk al verricht. Volgens Defensie kunnen deze meters een belangrijke bescherming bieden tegen sabotage of spionage. Als er afluisterapparatuur zou worden geplaatst moet de meter opmerken dat de kwaliteit van de glasvezel minder wordt. Wanneer een kabel wordt doorgeknipt moet er een alarm afgaan. Betrokken NAFIN-medewerkers bleken te veronderstellen dat het ITOC verdachte activiteiten aan een kabel onmiddellijk opmerkt aangezien volledige, continue monitoring van het netwerk een belangrijke cybersecuritynorm is waaraan voldaan moet zijn.

Wij constateren echter dat het ITOC de meters van de kabels niet optimaal monitort. Verder constateren wij dat het voor het ITOC lastig is te bepalen wat de gevolgen zijn van een verstoring wanneer het op de hoogte is van een verstoring of een kabelbreuk. Op het NAFIN zijn veel verschillende systemen aangesloten en het ITOC kan niet snel zien welke gebruiker of dienst op welke plek in het NAFIN zit. Daarvoor is het ITOC afhankelijk van de gebruiker die de servicedesk belt en aangeeft hoe ernstig het probleem is. Daardoor ontstaat het risico dat sommige verstoringen niet de juiste prioriteit krijgen van het ITOC.

Nog niet overal een verplichte dubbele aansluiting op het NAFIN

Om grote problemen te voorkomen heeft Defensie besloten dat systemen en objecten die het kenmerkt als onmisbaar voor de bedrijfsvoering via 2 kabels met de kern van het NAFIN verbonden moeten zijn. Zodat wanneer er één kabel breekt, de dienstverlening via de andere kabel door kan gaan. Uit een incident in januari 2024 bleek dat dit in de praktijk nog niet overal gerealiseerd is. Bij werkzaamheden aan het netwerk viel een kritiek systeem uit dat meerdere krijgsmachtonderdelen van vitale informatie voorziet. Door de onderbreking werd contact met missiegebieden verbroken voor een periode van ruim 2 uur. Defensie heeft vooraf niet goed genoeg ingeschat dat dit risico kon ontstaan bij deze werkzaamheden. Duidelijk werd dat dit vitale systeem via 1 kabel verbonden is met het NAFIN en dus geen terugvaloptie heeft van een tweede kabel.

Het is niet duidelijk waarom hier 1 enkelvoudige verbinding lag en waarmee dus niet volgens de regels is gehandeld. Defensie geeft aan dat voorheen Defensie-locaties eigen netwerken konden opbouwen. Om kosten te besparen, konden de Defensie-locaties ervoor kiezen om het lokale netwerk van een gebouw (en daar draaiende systemen) enkelvoudig te ontsluiten met het NAFIN. Daardoor zijn er nog enkelvoudige verbindingen in het netwerk, maar onbekend is welke (kritieke) diensten daaraan vast zitten. Defensie staat enkelvoudige aansluitingen van lokale netwerken op NAFIN niet meer toe. Deze netwerken worden de komende jaren allemaal vervangen voor een dubbele aansluiting. Onbekend is wanneer dit gereed is.

4.4 Beveiliging op Defensie-locaties qua opzet in orde

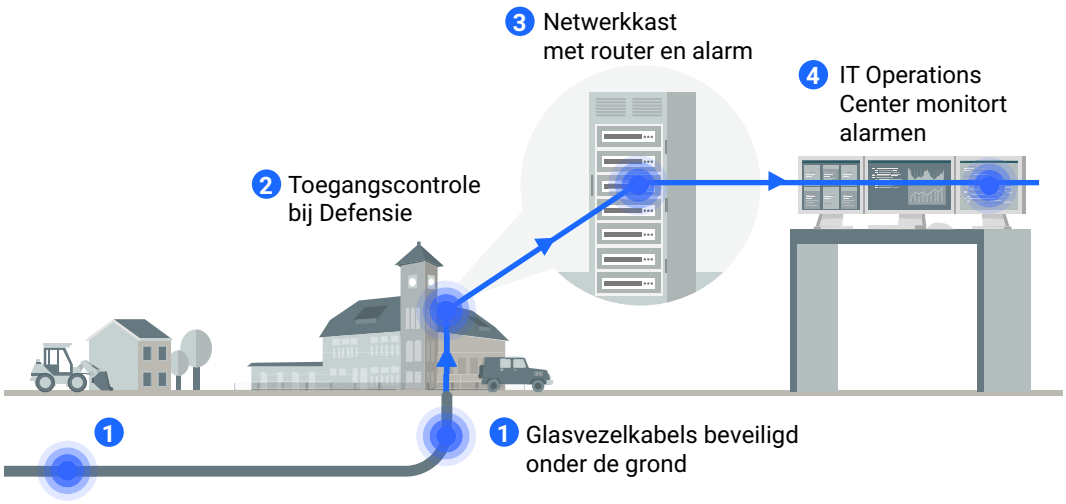
De NAFIN-kabels komen op tientallen Defensie-locaties boven de grond in netwerkkasten in netwerkruimtes. Niet elke locatie is even belangrijk als de andere. Soms heeft een netwerkkast alleen een aansluiting met een lokaal netwerk, maar er zijn ook netwerkruimtes die de kern van het NAFIN vormen. Deze locaties moeten extra goed fysiek en digitaal beveiligd zijn zodat onbevoegden bijvoorbeeld geen spionageapparatuur aan het netwerk kunnen bevestigen of het netwerk kunnen vernielen. Voor mensen die aan het netwerk moeten werken, zoals monteurs, geldt een speciale toegangsprocedure. Zij moeten allereerst gescreend zijn. Daarnaast moet hun bezoek vooraf worden aangekondigd, met namen en tijdstippen zodat het bezoek kan worden geautoriseerd door de wacht. Als aan de voorwaarden wordt voldaan kan de wacht de sleutels van de netwerkruimte aan hen geven. Mocht een

kwaadwillende de toegangsprocedure omzeilen en zelf bij de netwerkkasten komen, dan moeten de kasten versleuteld zijn. De belangrijkste netwerkkasten moeten nog een sensor hebben met detectie. Het ITOC hoort een alarm te krijgen als deze kasten worden geopend. Zie figuur 6 voor een overzicht van de maatregelen waarmee Defensie het NAFIN wil beschermen.

Ook hier is het beleid anders dan de praktijk. Het ITOC houdt deze alarmen niet actief in de gaten. Er gaan namelijk ook vaak loze alarmen af wanneer de netwerk-kasten moeten worden opengemaakt voor onderhoud. Dit is een door Defensie geaccepteerd risico waar nog geen alternatief voor is bedacht. Bij belangrijke locaties heeft de buitendeur van de netwerkruimte een alarm. Als dat alarm afgaat moet de Defensie Bewakings- en Beveiligingsorganisatie (DBBO) onmiddellijk naar de locatie toe om in te grijpen bij mogelijk ongeautoriseerde toegang.

Figuur 6 *Beveiliging van de hardware van het NAFIN in opzet*

NAFIN hardware moet op verschillende manieren worden beveiligd



4.5 Beveiliging van het NAFIN in de praktijk onvoldoende

We concluderen dat de beveiliging van het NAFIN door Defensie in de praktijk onvoldoende is (zie ook figuur 7). We hebben de beveiliging van NAFIN op een aantal Defensie-locaties in de praktijk getest door op 2 locaties 3 inlooptesten te doen. Daarnaast hebben we de digitale beveiliging van de hardware getest. Deze praktijk-testen zijn door het Defensie Cyber Security Centrum (DCSC) in opdracht van de Algemene Rekenkamer en (grotendeels) in aanwezigheid van onderzoekers van de

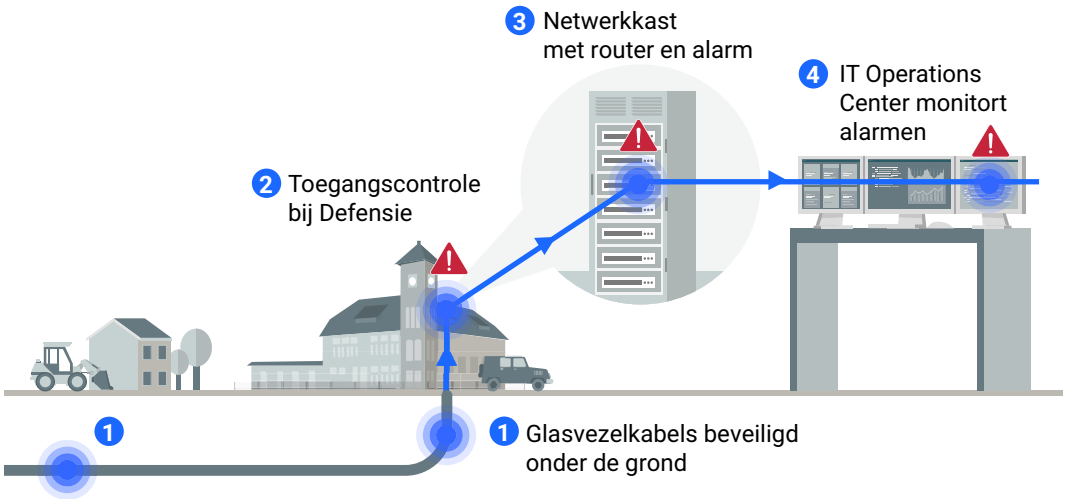
Algemene Rekenkamer uitgevoerd. We werkten vanuit het *insider threat*-scenario: dat wil zeggen dat 1 van de ongeveer 70.000 medewerkers van Defensie, of iemand die zich voordoet als medewerker van Defensie, pogingen tot sabotage of spionage onderneemt.

Het testteam heeft gepoogd toegang te krijgen tot een belangrijke netwerkruimte van het NAFIN, waar de kern van het netwerk draait. Het team had een Defensie-pas, maar was niet geautoriseerd om de hoog beveiligde NAFIN-ruimte te betreden. Ook was hun bezoek niet aangekondigd. Bij de wacht kreeg het testteam echter wel de sleutel van deze netwerkruimte mee. Bij een andere test op een NAFIN-locatie kreeg het testteam ook ongeautoriseerd de sleutels mee van de netwerkruimte.

Bij 2 testen is bij het openen van de netwerkruimte de DBBO van het ministerie van Defensie gealarmeerd. Zij kwamen na enige tijd ter plaatse, maar hinderden het testteam verder niet en het team kon vervolgens doorgaan met de test. In de netwerkruimte bleek de detectie op de netwerkkasten vervolgens ondermaats te functioneren. Ook ging bij 1 van de testen geen alarmsignaal af bij het ITOC toen het testteam toegang tot het netwerk probeerde krijgen. Uit deze testen concluderen we dat de beveiliging van de hardware op een aantal locaties van het NAFIN meerdere kwetsbaarheden bevat (zie ook figuur 7).

Figuur 7 *Beveiligingsmaatregelen NAFIN werken in de praktijk niet*

Kwetsbaarheden in de beveiliging van het NAFIN



De uitkomsten van deze fysieke praktijktesten zijn in lijn met de bevindingen uit onze onderzoeken in 2022 en 2023 naar de beveiliging van militaire objecten[6] (zie kader) door Defensie.

Beveiliging militaire objecten al jaren niet op orde

In ons verantwoordingsonderzoek Defensie van 2022 en 2023 onderzochten wij de beveiliging van militaire objecten. We constateerden dat de militaire objecten die het zwaarst beveiligd horen te zijn, dat in de praktijk niet zijn. Verouderde gebouwen, ernstig vertraagde elektronische systemen en een (te) laag veiligheidsbewustzijn bij Defensie-personeel spelen hierbij een rol. Als de zwaarst beveiligde militaire objecten beschadigd of ontvreemd worden, kan dit (zeer) ernstige gevolgen hebben voor de veiligheid of andere zwaarwegende belangen van de staat of zijn bondgenoten. Ook kunnen de operationele gereedheid en inzetbaarheid van de krijgsmacht hieronder lijden. Dit heeft geleid tot een onvolkomenheid in 2022 en in 2023 die nog niet is opgelost door de minister van Defensie. De urgentie bij de minister van Defensie om de tekortkomingen in de beveiliging van militaire objecten uit 2022 aan te pakken bleek in 2023 te ontbreken.

Het gebrek aan veiligheidsbewustzijn bij medewerkers zagen we opnieuw bij onze praktijktesten op de fysieke beveiliging van het NAFIN. In 2022 werden we niet tegengehouden maar zelfs geholpen door Defensie-medewerkers tijdens onze praktijktest om toegang te krijgen tot militaire objecten. En ook in 2023 hielden Defensie-medewerkers ons niet tegen. Het is zorgelijk dat deze omissies in de fysieke beveiliging in 2023 nog niet waren opgelost en we ze bij de fysieke beveiliging van het NAFIN eind 2023 terugzien.

In mei 2025 zullen we in ons Rapport bij het Jaarverslag 2024 van het Ministerie van Defensie weer rapporteren over de beveiliging van militaire objecten in 2024.

5. Militaire regie over het NAFIN

In dit hoofdstuk kijken we naar de publiek-private samenwerking bij het NAFIN. De belangrijkste private partner van Defensie ten aanzien van het NAFIN is KPN. KPN levert de glasvezelkabel van het NAFIN en legt hem aan. Het tweede bedrijf waar Defensie voor het NAFIN intensief mee samenwerkt is Nokia. Nokia levert hardwarecomponenten zoals routers, die het mogelijk maken om data over glasvezel te versturen. De samenwerking van Defensie met KPN is zeer intensief en de afhankelijkheid van dit bedrijf is groot. Hoe zorgt Defensie ervoor dat KPN volgens zijn beveiligingseisen werkt? Hiervoor onderzochten we autorisaties voor private bedrijven en de samenwerking met onderaannemers. Tot slot kijken we naar de civiele gebruikers van het netwerk. We concluderen dat Defensie maar beperkt regie voert over hoe de beveiligingseisen voor het NAFIN door onderaannemers in acht worden genomen en dit onvoldoende controleert.

5.1 KPN legt het netwerk voor Defensie aan

De raamovereenkomst tussen het ministerie van Defensie en Koninklijke PTT Nederland (later KPN) van 5 april 1994 ligt aan de basis van de relatie tussen Defensie en KPN. Deze overeenkomst werd voor onbepaalde tijd gesloten en er wordt in latere contracten naar verwezen. In de overeenkomst sprak men af dat het NAFIN-glasvezelnetwerk juridisch eigendom is van KPN en dat Defensie het exclusieve gebruiksrecht heeft. Het ministerie van Defensie betaalt en bepaalt. Het is daarmee financieel en functioneel verantwoordelijk voor het NAFIN. Defensie investeert en maakt zelf keuzes rond het ontwerp van NAFIN. Defensie is daarmee economisch eigenaar van het NAFIN. KPN is juridisch eigenaar van het NAFIN.

Dat betekent dat het netwerk niet volledig *military owned* is en het ministerie van Defensie daarmee afwijkt van zijn eigen randvoorwaarde.

In de praktijk werkt KPN aan de fysieke glasvezelkabels die in de grond zitten. KPN heeft een NAFIN-team in dienst dat uitsluitend voor Defensie en het NAFIN werkt. Het NAFIN-team van KPN bestaat uit: 1 servicemanager, die rapportages voor Defensie maakt; 4 projectmanagers, die veel op pad zijn om bij werkzaamheden aan het NAFIN aanwezig te zijn en 1 administratief medewerker die de netwerkadministratie doet. Het daadwerkelijke uitvoerende werk aan de kabel laat KPN door onderaannemers doen. De belangrijkste werkzaamheden van KPN ten aanzien van het NAFIN vallen uiteen in 4 taken:

- **Mutaties**: ongeveer 35 keer per jaar vraagt Defensie een mutatie of wijziging aan. Dit kan zijn omdat bijvoorbeeld een kazerne verdwijnt en de glasvezelkabel daar dan moet worden opgeruimd.
- **Reconstructies**: ongeveer 35-40 keer per jaar dient een reconstructie van de kabel plaats te vinden. Dit is bijvoorbeeld omdat een gemeente een rotonde wil plaatsen en de kabel hierdoor onder asfalt zou komen te liggen. De kabel wordt dan verlegd naar een andere, toegankelijkere plek.
- **Onderhoud**: elke paar weken komt er een verstoring door een externe oorzaak voor. Dit komt bijvoorbeeld door de bouw van een nieuwe woonwijk waarbij een NAFIN-kabel per ongeluk wordt geraakt bij graafwerkzaamheden.
- **Projecten**: dit betreft grootschalig werk, zoals updates aan het netwerk.

Defensie en KPN hebben meerdere keren per jaar overleg op strategisch, tactisch en operationeel niveau tussen het NAFIN-team en KPN, tussen inkopers van Defensie en KPN en met KPN en onderaannemers. Ook is er wekelijks een operationeel overleg tussen KPN en Defensie over actualiteiten.

5.2 Defensie controleert private partijen onvoldoende

Defensie kan niet al zijn werkzaamheden zelf uitvoeren en geeft daarom regelmatig opdrachten aan private partijen. Soms moet Defensie vertrouwelijke informatie delen met deze bedrijven om hen het werk te kunnen laten uitvoeren. Wanneer hier sprake van is, volgt er een ABDO-toets om te onderzoeken of het bedrijf staatsgeheime informatie toevertrouwd kan worden.

Defensie moet inzichtelijk maken welke geheime informatie het moet delen met de private partij om werk uit te kunnen besteden. Bijvoorbeeld informatie over de buizen die worden gebruikt, over de glasvezels en over de postcodes van de plaatsen waar

de kabels komen te liggen. Dit is informatie die bij een cyberaanval gebruikt zou kunnen worden. Defensie onderzoekt vervolgens het bedrijf op een aantal punten: heeft het bedrijf een beveiligingsfunctionaris? Een beveiligingsplan? Is de locatie beveiligd en zijn de medewerkers gescreend om met staatsgeheime informatie om te gaan? Defensie brengt een bezoek aan het bedrijf om te kijken of het de juiste maatregelen heeft genomen om informatie veilig te verwerken en op te slaan. Als alles in orde is, geeft Defensie een ABDO-autorisatie af en mag het bedrijf voor een bepaalde tijd en voor die specifieke opdracht aan het werk voor Defensie.

KPN is de leverancier voor de glasvezelkabels van het netwerk. KPN levert de kabels 'leeg' op, nog voordat het mogelijk is gemaakt om data via lichtsignalen over de glasvezelkabel te sturen. Het is daarmee nog geen product waar cybersecurityrisico's aan kleven. KPN levert daarnaast geen actieve diensten die over deze kabel heen gaan en kan de data niet bekijken. Wel heeft KPN toegang tot vertrouwelijke informatie over het netwerk, zoals de locaties waar het wordt aangesloten. Deze informatie is gerubriceerd als staatsgeheime informatie en dus is een ABDO-autorisatie vereist.

We constateren dat zowel KPN als Nokia in 2024 een geldige ABDO-autorisatie van Defensie had. KPN heeft aanvullende maatregelen genomen om de geheime informatie van het netwerk te beschermen. KPN huurt onderaannemers in om het werk te laten uitvoeren. KPN heeft 3 hoofdonderaannemers die het standaard inhuurt. Het is de verantwoordelijkheid van de partij die het werk uitbesteedt aan onderaannemers om een ABDO-toets aan te vragen bij Defensie. KPN is dus verantwoordelijk voor geldige autorisaties voor zijn hoofdonderaannemers. Wij hebben bij Defensie gecontroleerd of de 3 hoofdonderaannemers een geldige autorisatie hadden. Voor 2 van de 3 hoofdonderaannemers was dit het geval. Voor 1 hoofdonderaannemer was de autorisatie van Defensie al in 2021 verlopen. KPN heeft aangegeven dat dit bedrijf 1 van de 3 hoofdaannemers was waar het in 2023 en 2024 gebruik van maakte en dit blijkt ook uit Defensie-documenten. Het is voor Defensie (nog) niet mogelijk om automatisch in te zien wanneer ABDO-autorisaties verlopen zodat partijen gerappelleerd kunnen worden om een nieuwe autorisatie aan te vragen. Het is de taak van de aanvrager om in de gaten te houden dat zijn leveranciers een geldige autorisatie hebben. In dit geval heeft KPN dus de verlopen autorisatie niet op tijd opgemerkt en Defensie heeft KPN hier niet op gecontroleerd. De zorgelijke consequentie van een verlopen autorisatie kan zijn dat een bedrijf ongeautoriseerd toegang krijgt tot staatsgeheime informatie. Tijdens dit onderzoek diende KPN alsnog een aanvraag in bij Defensie voor een nieuwe ABDO-autorisatie voor dit bedrijf.

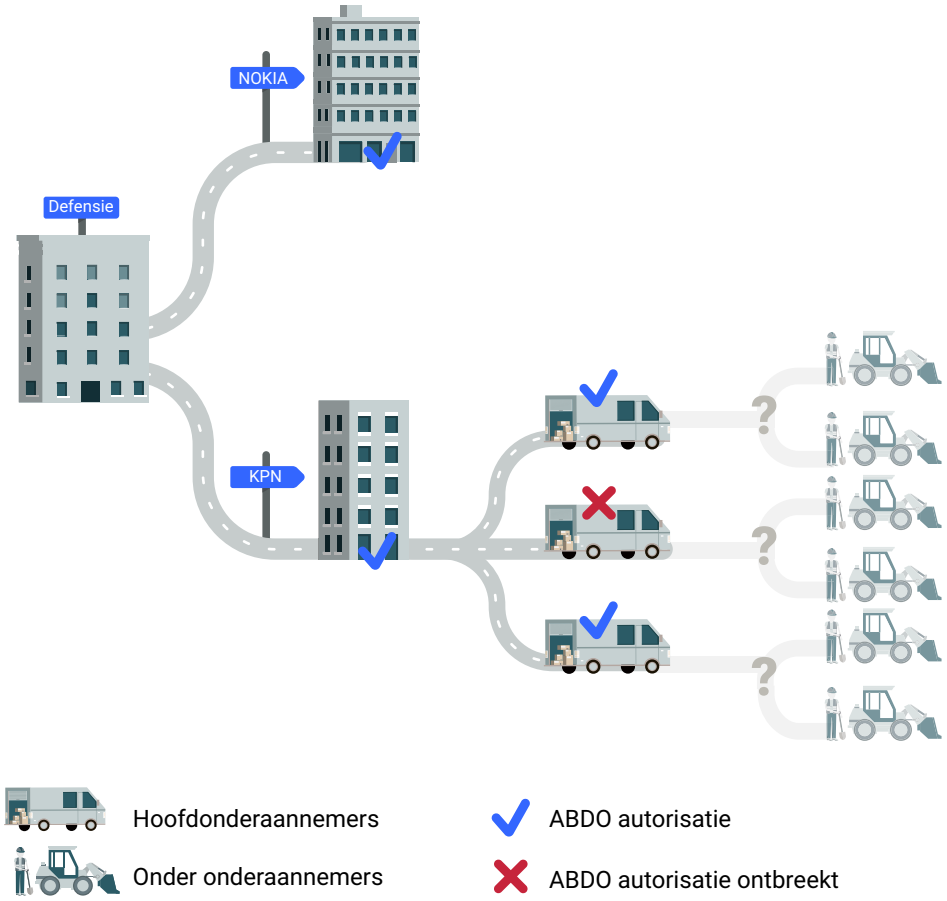
De 3 hoofdonderaannemers van KPN hebben ook onderaannemers. Alleen de opdrachtgevende partij kan bepalen welke informatie zij delen met een onderaannemer en of dit dan gerubriceerde informatie betreft. Zij zijn dus verantwoordelijk voor het aanvragen van de ABDO-toets van de onderaannemer. Dit gaat zo door naar andere onderaannemers, tot er geen gerubriceerde informatie gedeeld wordt. Een ABDO-toets voor het gehele bedrijf is overigens niet altijd noodzakelijk. Soms kan een beveiligingsmaatregel volstaan om aan het werk te mogen. Zoals wanneer een bedrijf met een geldige autorisatie toezicht houdt op het werk ter plekke, of dat alleen gescreende medewerkers aan het werk mogen. Defensie heeft een team dat aanwezig is bij projecten en mutaties die door de private bedrijven worden uitgevoerd. Dat team controleert ter plaatse of het werk kwalitatief goed wordt uitgevoerd. Maar het kan niet altijd aanwezig zijn.

Een andere waarborg is dat onderaannemers niet weten dat ze aan een Defensienetwerk gaan werken. Defensie heeft echter alleen zicht op losse Defensie-opdrachten waarvoor een ABDO-autorisatieaanvraag is ingediend of is afgegeven. Defensie kan uit zijn systemen niet eenvoudig een volledig overzicht halen van alle bedrijven die aan het NAFIN werken. Dit overzicht behoort Defensie, in samenwerking met KPN, wel te hebben. Tijdens ons onderzoek bleek een kleine onderaannemer van een hoofdonderaannemer aan het NAFIN te werken. Dit kleine bedrijf had geen ABDO-autorisatie van Defensie. Of en zo ja welke aanvullende beveiligingsmaatregelen met dit bedrijf zijn afgesproken is onbekend.

Defensie behoort niet alleen werkzaamheden van bedrijven te autoriseren, maar heeft ook als taak te controleren of het geautoriseerde bedrijf zich aan de gemaakte afspraken houdt. In de praktijk is de invulling van deze controletaak van Defensie door een gebrek aan personele capaciteit zeer beperkt. Wij constateren dat Defensie niet bij KPN en Nokia heeft gecontroleerd of aan de afspraken blijvend wordt voldaan. We concluderen daarom dat de minister van Defensie zijn aannemers en leveranciers onvoldoende controleert om te borgen dat het NAFIN voldoende beveiligd is (zie figuur 8).

Figuur 8 *Private partijen en ABDO-autorisaties*

Defensie controleert beveiligingsmaatregelen private partijen onvoldoende



5.3 Afhankelijkheid NAFIN van KPN

De afhankelijkheid die Defensie heeft ten opzichte van KPN gaat verder dan controle op onderaannemers. Defensie kan voor het NAFIN bijna niet meer overstappen naar een andere partij dan KPN. Het gehele netwerk van circa 3500 kilometer is verweven met het netwerk van KPN. Het ontvlechten en op een nieuwe plek leggen van het NAFIN is praktisch gezien een heel kostbare en tijdrovende operatie, die Defensie niet als een realistische optie beschouwt. Het is daarom cruciaal dat de belangen van Defensie in de constructie van het juridisch en economisch eigenaarschap bij KPN geborgd blijven. Defensie heeft in het contract met KPN daarom een waarborg ingebouwd tegen ongewenste verkoop. Contractueel is tussen Defensie en KPN in de raamovereenkomst vastgelegd: ‘‘PTT dan wel Defensie mag de uit deze Raam-overeenkomst of uit de daarop gebaseerde orders voortvloeiende verplichtingen noch geheel noch gedeeltelijk overdragen aan derden zonder schriftelijke toe-

stemming van Defensie c.q. PTT''. Toch is KPN in het verleden bijna verkocht (zie kader).

KPN bijna in buitenlandse handen

In 2013 toonde het Mexicaanse telecombedrijf América Móvil zich geïnteresseerd in een overname van KPN. De Mexicaanse eigenaar achter het bedrijf had eerder dat jaar 28% van de KPN-aandelen gekocht en deed daarna een bod op het volledige aandelenpakket. Als KPN in Mexicaanse handen zou vallen zou het onzeker worden hoe de belangen van het NAFIN voor zowel Defensie als voor de civiele overheidspartners zouden zijn geborgd. De stichting Preferente Aandelen van KPN maakte zich zorgen. Dit is een stichting die ten tijde van de privatisering van KPN in 1994 is ontstaan en 50% van de aandelen KPN in handen heeft. De stichting werd voorgezeten door een vijftal onafhankelijke bestuurders uit het bedrijfsleven. Zij vroegen het ministerie van Economische Zaken om meer informatie over de vitale diensten aangesloten op het NAFIN, zoals C2000 en het alarmnummer 112. Zowel bij het ministerie van Economische Zaken als bij de Nationaal Coördinator Terrorismebestrijding en Veiligheid leek op dat moment weinig kennis te zijn over harde infrastructuur in Nederland zoals het NAFIN.

KPN legde het ministerie uit dat deze diensten zo vervlochten zijn met de rest van het netwerk dat dit niet kon worden losgekoppeld in het geval van een verkoop aan América Móvil. De zorgen van de stichting hadden betrekking op de vitale dienstverlening die op het NAFIN draait. De randvoorwaarde dat het NAFIN netwerk ten alle tijden *military owned and controlled* is kwam niet op in deze discussie.

De stichting Preferente Aandelen besloot de overname tegen te houden met het uitgeven van extra preferente aandelen. Ze gaven in een persbericht aan tot deze interventie gekomen te zijn om de belangen van de Nederlandse samenleving als geheel veilig te stellen. América Móvil trok zich uiteindelijk terug en KPN bleef in Nederlandse handen.

De Wet ongewenste zeggenschap telecommunicatie, die in oktober 2020 in werking trad, moet voorkomen dat een statelijke actor zodanige zeggenschap krijgt over de Nederlandse telecommunicatie-infrastructuur dat daar misbruik van kan worden gemaakt. Deze wet werd geschreven na de bovengenoemde poging tot overname van KPN in 2013 door een buitenlandse partij. De minister van Economische Zaken en Klimaat is met deze wet bevoegd om een eventuele verkoop te verbieden.

De memorie van toelichting van deze wet stelt: “Een bijzonder risico ligt in de afhankelijkheid van overheidsdiensten van communicatiediensten. Opzettelijke uitval van deze diensten kunnen de overheid hinderen in haar functioneren, waarmee de nationale veiligheid in gevaar kan komen. Te denken valt daarbij aan de dienst-verlening ten behoeve van de noodcommunicatievoorziening (NCV), de communicatiedienstverlening aan Defensie, waaronder het Netherlands Armed Forces Integrated Network (NAFIN), en de dienstverlening ten behoeve van C2000”. Met deze wet heeft de Nederlandse overheid nu de mogelijkheid om KPN en daarmee NAFIN te beschermen tegen een (buitenlandse) overname.

5.4 Defensie controleert de ministeries niet op nakomen afspraken

Defensie is voor de aanleg en het voortbestaan van het netwerk afhankelijk van KPN. Voor de veiligheid van het netwerk is zij deels afhankelijk van zijn gebruikers.
De rijksoverheid is de grootste groep externe gebruikers, die zich laat vertegen-woordigen door het agentschap Logius van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Defensie legt het NAFIN voor Logius aan in netwerkruimtes van de departementen en garandeert dat dit netwerk betrouwbaar en beschikbaar is. Om daadwerkelijk gebruik te mogen maken van het netwerk moeten de ministeries de aansluitvoorwaarden van Defensie ondertekenen. Hierin staan eisen rond het veilig houden van de netwerkruimtes en regels over het dataverkeer die ministeries over het NAFIN mogen sturen. De ministeries moeten zich aan deze regels houden om het risico op cyberaanvallen te voorkomen.

In de basis houden alle ministeries zich aan de Baseline Informatiebeveiliging Overheid (BIO). Zij moeten een verklaring afgeven aan Defensie dat ze hieraan voldoen. Defensie controleert deze verklaringen niet en doet geen verdere audits om te controleren of zij zich aan de afspraken houden. Defensie heeft besloten dat het zich niet als een controlerende instantie opstelt. Andersom gebeurt dit soms wel. De ministeries willen als NAFIN-gebruiker namelijk verzekerd zijn van een veilig netwerk en vragen daardoor met enige regelmaat naar de ‘in-controlverklaringen’ van het ministerie van Defensie over het NAFIN.

Binnen Defensie zijn discussies over of het zich meer als een controlerende instantie richting de gebruiker moet opstellen, vanwege zorgen rondom het toestaan van ‘onvertrouwd verkeer’ op het netwerk. Dit is dataverkeer van buiten dat op het het NAFIN komt. Dit betreft bijvoorbeeld een e-mail van een bedrijf of burger aan een onderdeel van de rijksoverheid. Dit verkeer mag alleen worden toegelaten als het

ministerie voldoende tunneling (afscherming) of vercijfering (encryptie) toepast. Het is bij Defensie niet bekend of de ministeries dit op de juiste manier doen. Wanneer zij dit verkeer niet goed genoeg afschermen kan dit leiden tot beschikbaarheidsrisico's voor het NAFIN. We vinden het daarom opmerkelijk dat de minister van Defensie zich uitsluitend opstelt als leverancier van het netwerk. Periodieke controle op de naleving van de regels door gebruikers is vanwege het belang van van het NAFIN op zijn plaats.

6. Conclusies en aanbevelingen

6.1 Conclusies

Het NAFIN is een essentieel communicatienetwerk voor zowel Defensie als de rijksoverheid. Het ministerie van Defensie heeft dit netwerk technisch gezien goed opgezet. Het ministerie van Defensie zorgt ervoor dat het netwerk regelmatig updates krijgt zodat het aan de laatste technische standaarden voldoet. De glasvezelkabels zijn zo aangelegd dat er voldoende uitwijkmogelijkheden zijn voor het dataverkeer als er sprake is van een kabelbreuk. Hierdoor is de kans op een grootschalige uitval door een cyberaanval klein. Hoewel de kans op grootschalige uitval klein is, is de impact ervan heel groot voor Nederland, zoals we hebben gezien op 28 augustus 2024. Toen was er geen vliegverkeer mogelijk van Eindhoven Airport en veroorzaakte de storing bij het NAFIN problemen bij hulpdiensten, de Kustwacht, de Koninklijke Marechaussee, DigiD, een aantal gemeentelijke diensten, de ministeries en de GGD. Dit betekent dat er een lage tolerantie is voor kwetsbaarheden. Uit ons onderzoek, dat is uitgevoerd in 2024, blijkt dat NAFIN op dit moment onvoldoende beveiligd is door de minister van Defensie. Wij trekken hieronder 3 conclusies over de cyberweerbaarheid van het NAFIN.

Ontbrekende strategie Defensie op rol en toekomst NAFIN

De eerste conclusie is dat het ontbreekt aan strategie. Al vanaf de oprichting van het NAFIN in 1996 lijkt geld een belangrijke drijfveer voor Defensie te zijn bij strategische keuzes. Hierdoor werd het netwerk bijna verkocht en heeft Defensie ervoor gekozen om het netwerk fors uit te breiden voor civiele partners. Technisch gezien is hierover nagedacht. Maar we missen bij dit soort besluiten beleidsstukken en scenario's die verder kijken dan de techniek. Ook zien we geen nieuwe risicoanalyses nu de wereld

is veranderd of een visie op welke rol het NAFIN in onze maatschappij behoort te vervullen. En wat betekent het dat Defensie een IT-leverancier is voor zoveel civiele partners zoals een luchthaven en een groot aantal hulpdiensten?

Fysieke beveiliging van NAFIN is onvoldoende

Het netwerk moet vanwege het maatschappelijke belang aan de hoogste beveiligingseisen voldoen. Maar uit onze praktijktesten blijkt dat op een aantal Defensie-kazernes waar het NAFIN staat het veiligheidsbewustzijn van defensiepersoneel onvoldoende is. In de testen kregen wij meermaals als onbevoegden de sleutels mee tot de netwerkruimtes van het NAFIN. Daarnaast bleken de detectie van onze ongeautoriseerde toegang en de respons hierop niet aan de normen te voldoen die Defensie zelf stelt voor de beveiliging van het netwerk. Vergelijkbare bevindingen deden wij in ons verantwoordingsonderzoek naar Defensie in 2022 en 2023.[7] Het is zorgelijk dat we dit opnieuw bij het NAFIN aantreffen. Daarnaast vonden wij in digitale testen kwetsbaarheden die gebruikt kunnen worden voor een cyberaanval op het NAFIN. Dit leidt ons tot de conclusie dat Nederland in een zeer gespannen geopolitieke situatie militair gezien onvoldoende alert is op sabotagerisico's door statelijke actoren.

Beperkte militaire regie en controle vanuit Defensie over het netwerk

De laatste conclusie is dat Defensie zeer afhankelijk is van zijn private partner KPN. Zonder KPN kan het glasvezelnetwerk niet worden aangelegd of gewijzigd. Overstappen naar een andere partij is niet mogelijk. We zien dat Defensie waarborgen rond cybersecurity heeft genomen om te zorgen dat KPN goed omgaat met de staatsgeheime informatie van het netwerk. Maar KPN besteedt de werkzaamheden aan het NAFIN uit aan onderaannemers, die het ook weer uitbesteden aan onderaannemers. Het zicht op wie er aan het NAFIN werkt en welke beveiligingsmaatregelen met deze partijen zijn afgesproken verdwijnt. Zo kon het gebeuren dat een onderaannemer 2 jaar lang werkte zonder geldige autorisatie. De minister van Defensie heeft hier onvoldoende overzicht over en grip op.

Het NAFIN veilig en in de lucht houden is een essentiële taak van de minister van Defensie. In de praktijk betekent dit dat veel mensen binnen Defensie hierin een rol moeten vervullen. De technici, de wacht, de beveiligings- en bewakingsorganisatie en het IT Operations Center bijvoorbeeld. Deze gezamenlijke verantwoordelijkheid om het NAFIN te beschermen is groot. Het incident op 28 augustus 2024 maakte nog eens glashelder hoeveel publieke organisaties op het NAFIN vertrouwen. Dit betekent dat zelfs buiten het ministerie van Defensie verantwoordelijkheden liggen voor het veilig houden van NAFIN: bij de gebruikers van het netwerk in de

rijksoverheid, of bij de contractmanager van KPN en bij de onderaannemers die aan het netwerk werken. Gezien de huidige geopolitieke situatie, waar sabotage op Europese digitale infrastructuur op land en op zee een realistische dreiging is, is het wat ons betreft zeer zorgelijk dat de minister van Defensie de beveiliging van het NAFIN nog onvoldoende op orde heeft.

6.2 Aanbevelingen

- Ontwikkel een strategische visie op de rol van dit netwerk in de Nederlandse samenleving voor nu en in de toekomst, bepaal welke bescherming, mensen en middelen daarvoor nodig zijn; en verklaar het NAFIN tot ‘vitaal’;
- Neem maatregelen om zowel de detectie als respons op ongeoorloofde toegang tot het netwerk te verbeteren. Er moet continue monitoring zijn door Defensie op mogelijke sabotage en spionage op de NAFIN-kabels. Het veiligheidsbewustzijn van de betrokken medewerkers van Defensie, KPN en de onderaannemers moet verder omhoog en de beveiliging van NAFIN-ruimtes moet periodiek fysiek en digitaal getest worden;
- Overweeg of het mogelijk is om het werk aan minder partijen uit te besteden en houd beter toezicht op de uitvoering van de beveiligingsmaatregelen en ABDO-autorisaties voor de private partijen en hun onderaannemers die aan het NAFIN moeten werken, om te voorkomen dat staatsgeheime informatie over het NAFIN in de verkeerde handen terechtkomt.

7. Reactie minister en staatssecretaris van Defensie en nawoord Algemene Rekenkamer

De minister en de staatssecretaris van Defensie hebben gezamenlijk op 11 oktober 2024 gereageerd op ons conceptrapport. Hieronder geven wij deze reactie integraal weer. De volledige reactie staat eveneens op www.rekenkamer.nl. Dit hoofdstuk sluiten we af met een nawoord.

7.1 Reactie minister en staatssecretaris van Defensie

“Veiligheid heeft hoge prioriteit en daarom is uw kritisch onderzoek waardevol om de continuïteit en weerbaarheid van het krijgsmachtnetwerk NAFIN te kunnen waarborgen. Het stemt tevreden dat het NAFIN als essentieel communicatienetwerk voor Defensie en haar Rijksoverheid partners technisch gezien goed is opgezet en aan de laatste standaarden voldoet. Het NAFIN netwerk is echter onvoldoende fysiek beveiligd door Defensie en met uw aanbevelingen gaan wij aan de slag. Ik hecht er aan te benadrukken dat de recente storing van 28 augustus 2024 geen relatie heeft met de door u geconstateerde tekortkomingen in de fysieke beveiliging van het NAFIN netwerk. U trekt drie conclusies in het rapport over het NAFIN netwerk.

- Allereerst concludeert u dat binnen Defensie een gebrek is aan strategie en visie op de rol en toekomst van het NAFIN. Het netwerk is gerealiseerd in een periode van zware bezuinigingen. Hierdoor heeft de focus van de strategische richting van NAFIN lange tijd op kostenefficiëntie gelegen door de kosten van het netwerk te dragen met andere overheidspartners. In de context van de grote veranderingen in de internationale veiligheidssituatie, de hernieuwde focus op hoofdtaak 1 en weerbaarheid van de samenleving geeft deze conclusie Defensie de noodzaak en urgentie om ook de rol en toekomst van NAFIN te herijken.

- Daarnaast concludeert u in uw rapport dat de hardware op locaties van het NAFIN in de praktijk onvoldoende fysiek is beveiligd. De geconstateerde tekortkomingen van de fysieke beveiliging zijn ook door u geconstateerd in de onvolkomenheid beveiliging militaire objecten over 2022 en 2023. In 2022 is een actieplan opgesteld dat gedeeltelijk in uitvoering is. De voortgang loopt, maar is afhankelijk van schaarse specialistische capaciteit, te verbeteren veiligheidsbewustzijn en langdurige trajecten om vastgoed en elektronische systemen te verbeteren. Daarnaast wordt een oorzaakanalyse uitgevoerd die naar verwachting gereed is in oktober 2024. Mede op basis daarvan wordt dit jaar een herijkt plan van aanpak opgesteld. De door u in dit rapport geconstateerde tekortkoming van de fysieke beveiliging NAFIN wordt onderdeel van dit verbetertraject. Het onderwerp beveiliging militaire objecten is in de Defensienota 2024 als randvoorwaarde voor het goed functioneren van de Defensieorganisatie opgenomen. Hiermee heeft het oplossen van de onvolkomenheid beveiliging militaire objecten topprioriteit gekregen.
- Tot slot concludeert u in uw rapport dat er vanuit Defensie beperkte militaire regie en controle is over het netwerk. Voor werkzaamheden aan het NAFIN netwerk zijn contractueel afspraken gemaakt met KPN over ABDO autorisatie. Defensie dient wel eigenaarschap te tonen en toe te zien op naleving van deze afspraken.

Uw aanbevelingen in het rapport neem ik over en zal ik hieronder kort toelichten.

- Uw aanbeveling om een strategische visie op de rol van het NAFIN netwerk in de Nederlandse samenleving voor nu en in de toekomst te ontwikkelen neem ik over. Ik zal het huidige beleid gericht op kostenefficiëntie herijken op basis van de vernieuwde focus op hoofdtaak 1 en een weerbare samenleving. Dit zal in samenspraak met de huidige medegebruikers van NAFIN worden gerealiseerd. Het NAFIN netwerk heeft een essentiële rol in de Nederlandse samenleving. Defensie zal onderzoek doen naar de mogelijkheid om het netwerk als vitale infrastructuur aan te wijzen.

Ik zal uw aanbevelingen over detectie en respons op ongeoorloofde toegang tot het netwerk, verhogen veiligheidsbewustzijn, periodiek fysiek en digitaal testen overnemen en uitvoeren via drie lijnen:

- De detectie van ongeoorloofde toegang tot het netwerk en het digitaal testen is opgenomen in een IT-verbetertool. Het IT Operations Center (ITOC) zal verbetering doorvoeren in de continue monitoring en (digitale) bewaking van het NAFIN netwerk.
- Daarnaast is de respons op ongeoorloofde toegang tot het netwerk, het veiligheidsbewustzijn van Defensiemedewerkers en het periodiek fysiek testen

van de beveiliging van netwerkruimtes onderdeel geworden van de aanpak van het project onvolkomenheid beveiliging militaire objecten.
- Het veiligheidsbewustzijn van betrokken medewerkers van KPN en onder-aannemers zal nadrukkelijk onder de aandacht worden gebracht bij KPN als hoofdaannemer.

Verder doet u de aanbeveling om het werk aan het NAFIN netwerk aan minder partijen uit te besteden en beter toezicht te houden op de uitvoering van de beveiligingsmaatregelen en ABDO-autorisaties.
- Defensie gaat in overleg met KPN om de mogelijkheden te inventariseren om te werken met minder (onder)onderaannemers.
- Ten aanzien van het tijdig aanvragen van ABDO-autorisaties heeft KPN een eigen verantwoordelijkheid. Defensie zal KPN schriftelijk wijzen op hun verantwoordelijkheden en vragen om verbeteringen door te voeren in het juist naleven van de beveiligingsmaatregelen en ABDO-autorisaties.
- Defensie zal audits uitvoeren naar het naleven van de BIO door medegebruikers van het NAFIN netwerk en met onder meer het ministerie van Binnenlandse Zaken en Koninkrijksrelaties in gesprek gaan om te bezien of de Service Level Agreements (SLA) met deze medegebruikers op dit punt toereikend zijn."

7.2 Nawoord Algemene Rekenkamer

Wij waarderen de serieuze reactie waarin de minister en staatssecretaris van Defensie onze bevindingen erkennen en toezeggen om de aanbevelingen op te pakken. De bewindspersonen benoemen de nieuwe veiligheidssituatie in Europa en erkennen de noodzaak en urgentie om de rol en toekomst van het NAFIN te herijken. Ze zien het NAFIN als een belangrijk onderdeel in het streven naar een weerbare samenleving.

Ten aanzien van onze bevindingen rondom de gebrekkige fysieke beveiliging van de netwerkruimtes verwijzen de bewindspersonen naar een actieplan dat is opgesteld naar de beveiliging van de militaire objecten. Over 2022 concludeerden we onder andere op basis van 8 praktijktesten dat de beveiliging van militaire objecten in de praktijk ondermaats was en beoordeelden dit als een onvolkomenheid. In 2023 zagen we geen verbetering bij de beveiliging van militaire objecten in de praktijk en er was een gebrek aan urgentie bij Defensie. Over 2023 handhaafden we daarom de onvolkomenheid.

Wij blijven het onderwerp fysieke beveiliging daarom nauwlettend volgen en op verantwoordingsdag in mei 2025 presenteren wij onze bevindingen over de stand van zaken voor wat betreft de beveiliging van militaire objecten over 2024.

Wat betreft de naleving van beveiligingsvoorschriften door onderaannemers wijzen de bewindspersonen op de verantwoordelijkheden van KPN. Hoewel deze verantwoordelijkheid formeel bij KPN is belegd, vinden wij het belangrijk dat ook Defensie zich inspant om meer overzicht en grip te krijgen op wie er aan het NAFIN werkt.

Tot slot geven de minister en de staatssecretaris van Defensie aan dat zij audits gaan uitvoeren op de naleving van beveiligingsvoorschriften onder medegebruikers van het NAFIN. Wij denken dat dit een goede stap is in het verder verhogen van de cyberweerbaarheid van dit cruciale Defensienetwerk. Weerbaarheid tegen externe dreigingen op het NAFIN-netwerk is namelijk niet alleen de verantwoordelijkheid van de minister van Defensie, maar ook een verantwoordelijkheid van alle mede-gebruikers van het NAFIN. Hulpdiensten, andere ministeries, zelfstandige bestuursorganen, andere uitvoeringsorganisaties en ook de Hoge Colleges van Staat zoals de Staten-Generaal en de Algemene Rekenkamer zelf.

Bijlagen

Bijlage 1 Methodologische verantwoording

Onderzoeksvragen

De hoofdvraag van het onderzoek was: hoe kwetsbaar is het publiek-private krijgsmachtnetwerk NAFIN voor cyberaanvallen? Deze hoofdvraag hebben we beantwoord met behulp van de volgende deelvragen:

1. Wat zijn de doelen van het krijgsmachtnetwerk NAFIN en wie maken er gebruik van?
2. Functioneert de publiek-private samenwerking t.a.v. cybersecurity van het krijgsmachtnetwerk NAFIN voldoende?
   a. Is er een duidelijke verantwoordelijkheidsverdeling tussen de minister van Defensie en de private partijen?
   b. Zijn de private partijen geautoriseerd om aan het netwerk te werken en is het toezicht hierop voldoende?
   c. Welke afspraken zijn gemaakt met aansluitende publieke partijen over cyberveiligheid en is het toezicht hierop voldoende?
4. Beschikt het krijgsmachtnetwerk NAFIN over doeltreffende detectiemaatregelen? (opzet en bestaan)
5. Zijn er heldere responsscenario's bij incidenten op het krijgsmachtnetwerk NAFIN en zijn deze responsmaatregelen effectief? (opzet en bestaan)
6. Zijn de detectie- en responsmaatregelen voor het krijgsmachtnetwerk NAFIN effectief in de praktijk? (werking)

Normen

Als normenkader bij de beantwoording van onderzoeksvragen 2 tot en met 5 hanteerden we het cybersecurityraamwerk van het National Institute of Standards and Technology (NIST). Het NIST is onderdeel van het Amerikaanse ministerie van Economische Zaken. Hun raamwerk voor cybersecurity wordt wereldwijd veel gebruikt en heeft relaties met beveiligingsstandaarden en -modellen als ISO 27001 en COBIT. Het NIST-raamwerk onderscheidt 5 hoofdfuncties, waaronder de voor ons onderzoek extra relevante functies 'detectie' en 'respons'. De categorieën binnen de hoofdfuncties hebben we gebruikt als hulpmiddel om de diversiteit aan inspanningen op het gebied van cybersecurity bij het NAFIN inzichtelijk te maken. Bij onderzoeksvraag 5 hebben we ook normen van het ministerie van Defensie meegenomen over fysieke beveiliging van het NAFIN. Ons uiteindelijke oordeel over de cybersecurity van het krijgsmachtnetwerk is niet uitsluitend gebaseerd op het al dan niet voldoen aan de specifieke normen binnen het NIST-raamwerk. Het oordeel is kwalitatief, gevormd op basis van onze bevindingen in brede zin die we per categorie bij het NAFIN hebben gedaan. Om het rapport toegankelijk te houden, hebben we de Engelse namen van de NIST-categorieën vermeden. Bijlage 2 geeft een overzicht van de gebruikte NIST-categorieën.

Onderzoeksactiviteiten

Voor het beantwoorden van de onderzoeksvragen en het toetsen van de normen bestudeerden we in de periode november 2023 tot en met maart 2024 interne documenten bij het ministerie van Defensie. In diezelfde tijd hebben we met relevante betrokkenen interviews afgenomen. Naar aanleiding van de interviews hebben we informatie gecontroleerd aan de hand van aanvullende documenten. 2 keer zijn we naar het Defensie-archief geweest om besluitvorming over het netwerk in de jaren 90 te reconstrueren. Ook legden we werkbezoeken af aan het IT Operations Center van Defensie, Bureau Industrieveiligheid van de MIVD en KPN. We waren 2 keer aanwezig bij werkzaamheden aan het NAFIN, zowel binnen in een netwerkruimte als buiten langs de openbare weg.

Praktijktesten

Op ons initiatief hebben we voor dit onderzoek samen met specialisten van het ministerie van Defensie de weerbaarheid van het netwerk in de praktijk getoetst met inlooptesten en een digitale test. De uitkomsten van deze testen zijn niet representatief voor alle NAFIN-locaties, maar geven wel een illustratie van hoe de beveiligingssituatie er in de praktijk uitziet. Onderzoekers van de Algemene Rekenkamer hebben aan 1 van de 3 fysieke inlooptesten op 2 locaties deelgenomen en aan de digitale test meegedaan. De resultaten van die testen zijn naderhand

ongefilterd en gelijktijdig met het ministerie van Defensie en ons gedeeld. Een aantal weken later zijn deze resultaten in aanwezigheid van de Algemene Rekenkamer aan meerdere betrokkenen binnen Defensie gedeeld via een presentatie, zodat er een plan kon worden gemaakt om de kwetsbaarheden op te lossen. Na ons onderzoek hebben we onze bevindingen besproken met het ministerie van Defensie.

Rubricering

Alle leden van het onderzoeksteam beschikten over een geldige MIVD-screening. Voor het beantwoorden van onze onderzoeksvragen hebben wij namelijk een aantal keren gerubriceerde informatie moeten inzien op locaties van Defensie. Tijdens het onderzoek bleek dat op de onderzoeksresultaten zelf ook een rubricering zou passen. Het rapport met de resultaten van de praktijktesten is daarom gedurende het onderzoek door Defensie gerubriceerd tot staatsgeheim confidentieel. De Algemene Rekenkamer heeft vervolgens maatregelen genomen om te zorgen dat we veilig met deze informatie konden werken. Ook de nota van bevindingen die alle onderzoeksbevindingen bevatte is door de Algemene Rekenkamer als staatsgeheim confidentieel gerubriceerd. De Algemene Rekenkamer heeft er vanwege het belang van dit onderwerp voor gekozen wel een openbaar rapport te schrijven. Tijdens het rapportageproces is het rapport voorgelegd aan de beveiligingsautoriteit van Defensie en aan de MIVD om te controleren dat alles wat er in staat ook openbaar kon worden. De Algemene Rekenkamer heeft vervolgens mede op basis van het advies van Defensie besloten welke informatie openbaar kon worden.

Bijlage 2 Normenkader

Normenkader NIST

Dit toetsingskader is opgesteld bij aanvang van dit onderzoek naar de cybersecurity van het krijgsmachtnetwerk NAFIN. We hebben voor dit toetsingskader gebruikgemaakt van de normatiek van Het National Institute of Standards and Technology (NIST) Cybersecurity Framework. NIST is onderdeel van het Amerikaanse ministerie van Commercie en had de opdracht de kritische infrastructuur van de Verenigde Staten weerbaarder te maken tegen cyberaanvallen. In dat kader heeft NIST met betrokken partijen een framework voor beheersing van cybersecurityrisico's ontwikkeld, op basis van bestaande standaarden, richtlijnen en praktijkvoorbeelden. Defensie maakt zelf ook gebruik van het NIST-normenkader.

Toegepaste normen

Uit het normenkader hebben we een aantal normen geselecteerd die van toepassing zijn op dit onderzoek, zie de tabel hieronder. Waar nodig hebben we de normen bijeengevoegd en gespecificeerd naar ons onderzoeksobject. Onderzoeksvraag 1 is een beschrijvende vraag en is niet aan het normenkader getoetst. Voor onderzoeksvragen 2, 3 en 4 hebben we gekeken naar opzet en bestaan. Bij onderzoeksvraag 5 hebben we met een praktijktest naar werking gekeken. Voor toetsing van deze vraag hebben we aanvullend op het normenkader ook gebruikgemaakt van de eigen normen die Defensie stelde aan fysieke beveiliging, zoals de normen rond Te Beschermen Belangen (TBB)[8], eisen aan de netwerkruimtes en toegangsprocedures. De feiten hebben we beoordeeld aan de hand van aangeleverde documentatie, gesprekken en waarneming tijdens gesprekken.

Tabel 1 *Normenkader*

NIST Categorie	Onderzoeks-vraag	Norm
Governance (ID.GV-1, ID.GV-2, ID. GV-3, ID.GV-4, ID. AM- 6)	2	De organisatie heeft beleid, rollen en processen rondom cybersecurity ingericht. Ook zijn de verantwoordelijkheden rondom cybersecurity duidelijk belegd en afgestemd met externe partners en leveranciers.
Supply Chain Management (ID.SC-2, ID.SC-3, ID. SC-4)	2	Leveranciers van belangrijke IT-onderdelen worden met het oog op cybersecurity zorgvuldig uitgekozen, getoetst en gecontracteerd.
Maintenance (PR.MA-1, PR.MA-2)	2	Onderhoud en reparaties van onderdelen van het netwerk worden uitgevoerd in overeenstemming met het beleid en de veiligheidsprocedures.
Risk Assessment (ID.RA-5, ID-RA-6, ID. RM-2)	3	Dreigingen worden in kaart gebracht en vertaald naar risico-analyses.
Anomalies and Events (DE.AE 1-5)	3	Onregelmatigheden of afwijkingen in het functioneren van het netwerk worden tijdig opgespoord en er wordt nagegaan wat de (potentiële) impact is.
Security Continuous Monitoring (DE.CM 1-8)	3	Er is voortdurende monitoring van het netwerk en de fysieke omgeving op cybersecurity-events en fysieke beveiligings-incidenten die zouden kunnen leiden tot cyberaanvallen.
Detection Processes (DE.DP 1-5)	3	Er vindt evaluatie plaats van de detectieprocessen.
Response Planning (RS.RP-1, ID.BE-5)	4	Er zijn processen en procedures opgesteld die in werking treden op het moment dat er een (mogelijk) cyberincident/-crisis/-aanval plaatsvindt.
Communications (RS.CO 1-5)	4	Er is coördinatie van responsactiviteiten en afstemming daarvan tussen interne en externe betrokkenen.
Analysis (RS.AN 1-5)	4	Er worden analyses uitgevoerd op de situatie, als basis voor een adequate reactie.
Mitigation (RS.MI 1-3, PR.IP-4)	4	Er zijn activiteiten/maatregelen om verspreiding/verdieping van de cybercrisis te voorkomen, de oorzaak weg te nemen, de effecten snel te dempen/mitigeren en zorg te dragen voor een snelle terugkeer naar de normale situatie.
Improvements (RS.IM 1-2)	4	Er worden lessen getrokken uit een cyberincident/-crisis en activiteiten om op basis van die lessen de detectie en response te verbeteren.
Identity Management, Authentication and Access Control (PR.AC-1, PR.AC-2, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-7)	5	De fysieke en digitale toegang tot het netwerk en bijbehorende voorzieningen wordt beperkt tot bevoegde gebruikers, processen en apparaten, en wordt beheerd in overeenstemming met het ingeschatte risico van ongeoorloofde toegang tot geautoriseerde activiteiten en transacties.

Bijlage 3 Afkortingenlijst

ABDO	Algemene Beveiligingseisen Defensie Opdrachten
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
BIO	Baseline Informatiebeveiliging Overheid
DBBO	Defensie Bewakings en Beveiligings Organisatie
DCSC	Defensie Cyber Security Commando
DMO	Defensie Materieel Organisatie
DTO	Defensie Telematica Organisatie
ITOC	IT Operations Centre
JIVC	Joint IV Commando
KPN	Koninklijke PTT Nederland
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
NAFIN	Netherlands Armed Forces Integrated Network
NIST	National Institute of Standards and Technology

Bijlage 4 Literatuur

Algemene Rekenkamer (2019). *Digitale dijkverzwaring: cybersecurity van vitale waterwerken.* Den Haag: eigen beheer.

Algemene Rekenkamer (2020). *Digitalisering aan de grens. Cybersecurity van het grenstoezicht door de Koninklijke Marechaussee op Schiphol.* Den Haag: eigen beheer.

Algemene Rekenkamer (2023). *Verantwoordingsonderzoek 2022, Ministerie van Defensie (X), Rapport bij het jaarverslag 2022.* Den Haag, mei 2023.

Algemene Rekenkamer (2024). *Verantwoordingsonderzoek 2023, Ministerie van Defensie (X), Rapport bij het jaarverslag 2023.* Den Haag, mei 2024.

Telecommunicatiewet (1998) Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie.

Tweede Kamer (1993). Vaststelling van de begroting van de uitgaven en van de ontvangsten van hoofdstuk X (Ministerie van Defensie) voor het jaar 1993, vergaderjaar 1992-1993, 22 800 X, nr. 46, Den Haag: Sdu.

Tweede Kamer (1994). Vaststelling van de begroting van de uitgaven en van de ontvangsten van hoofdstuk X (Ministerie van Defensie) voor het jaar 1994, vergaderjaar 1993-1994, 23 400 X, nr. 46, Den Haag: Sdu.

Tweede Kamer (2003). Modernisering van de overheid, vergaderjaar 2003-2004, 29 362, nr. 1 , Den Haag: Sdu.

Tweede Kamer (2019). Aanhangsel handelingen, vergaderjaar 2018-2019, nr. 2525, Den Haag: Sdu.

Tweede Kamer (2020). Aanhangsel handelingen, vergaderjaar 2019-2020, nr. 2924, Den Haag: Sdu.

Bijlage 5 Eindnoten

1. Algemene Rekenkamer (2023) Verantwoordingsonderzoek 2022, Ministerie van Defensie (X), Rapport bij het jaarverslag 2022 en Algemene Rekenkamer (2024) Verantwoordingsonderzoek 2023, Ministerie van Defensie (X), Rapport bij het jaarverslag 2023.
2. Algemene Rekenkamer (2019) Digitale dijkverzwaring: cybersecurity en vitale waterwerken.
3. Algemene Rekenkamer (2020) Digitalisering aan de grens. Cybersecurity van het grenstoezicht door de Koninklijke Marechaussee op Schiphol.
4. Tweede Kamer (2003) Modernisering van de overheid, vergaderjaar 2003-2004, 29 362, nr. 1. Den Haag: Sdu.
5. Tweede Kamer (2003) Modernsering van de overheid, bijlage F voortgangsrapportage, vergaderjaar 2003-2004, 29 362, nr. 1. Den Haag: Sdu.
6. Algemene Rekenkamer (2023) Verantwoordingsonderzoek 2022, Ministerie van Defensie (X), Rapport bij het jaarverslag 2022 en Algemene Rekenkamer (2024) Verantwoordingsonderzoek 2023, Ministerie van Defensie (X), Rapport bij het jaarverslag 2023.
7. Algemene Rekenkamer (2023) Verantwoordingsonderzoek 2022, Ministerie van Defensie (X), Rapport bij het jaarverslag 2022 en Algemene Rekenkamer (2024) Verantwoordingsonderzoek 2023, Ministerie van Defensie (X), Rapport bij het jaarverslag 2023.
8. Defensie heeft voor de beveiliging van zijn informatie, materieel, goederen en objecten een model van Te Beschermen Belangen (TBB) ingericht. Onder Te Beschermen Belangen (TBB) wordt verstaan: *'informatie, informatiesystemen, materieel, goederen en objecten die beveiligd moeten worden om de werking van Defensie zoveel mogelijk ongestoord doorgang te laten vinden. Kennisname of aantasting hiervan door vreemde mogendheden of derden kan de Nationale Veiligheid, het algemeen (economisch/ politiek) belang en/of de integriteit van Defensie aantasten.'*
   Er zijn 4 categorieën TBB, met elk hun eigen eisen aan organisatorische, bouwkundige, elektronische en informatietechnische beveiligingsmaatregelen. TBB-1 moet het strengst beveiligd worden, afbouwend naar TBB-4.

Algemene Rekenkamer
Postbus 20015
2500 EA Den Haag
telefoon (070) 342 44 00
voorlichting@rekenkamer.nl
www.rekenkamer.nl

De tekst in dit document is vastgesteld op 24 oktober 2024. Dit document is op 7 november 2024 aangeboden aan de Tweede Kamer.

Den Haag, november 2024