Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

25 124 Nieuwe infrastructuur mobiele communicatie (C2000)

Nr. 96 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 26 april 2019

Met mijn brief van 17 september 2018 heb ik uw Kamer geïnformeerd over de voortgang van de vernieuwing van het C2000 spraaknetwerk en de in dit kader door mij voorgenomen beveiligingsonderzoeken.[1] Met mijn brief van 14 december 2018 heb ik u verder geïnformeerd over de beveiligingsonderzoeken naar het vernieuwde C2000 spraaknetwerk, aanvullend op de beveiligingsmaatregelen die al zijn getroffen.[2] Over het beveiligingsbeleid van C2000 bent u eerder geïnformeerd bij brieven van 18 april 2016[3] en 29 maart 2017[4]. In mijn brief van 15 april 2019 heb ik u geïnformeerd over de planning voor de vernieuwing en beveiliging van het C2000 spraaknetwerk en de uitrol van 5G.[5] In deze brief informeer ik u over de uitkomsten van de beveiligingsonderzoeken, de getroffen maatregelen en het vervolgtraject. Met deze brief kom ik tevens tegemoet aan de motie van het lid Laan-Geselschap (VVD)[6] en de motie van de leden Den Boer (D66), Van Dam (CDA) en Verhoeven (D66).[7]

C2000 is een vitaal systeem. De hulpdiensten zijn er voor hun onderlinge mobiele communicatie van afhankelijk. Bij het ontwerpen en bouwen van het nieuwe C2000 staan de robuustheid en betrouwbaarheid van het systeem centraal. De opdracht tot vernieuwing van C2000 is in 2015 gegund aan een combinatie van drie bedrijven, waaronder Hytera Mobilfunk GmbH (een voormalig deel van het Duitse bedrijf Rohde und Schwarz), een dochter van het Chinese bedrijf Hytera (hierna: Hytera China). Uw Kamer is hierover bij brief van 16 oktober 2015 geïnformeerd.[8]

[1] Kamerstuk 25 124, nr. 91.
[2] Kamerstukken 25 124 en 29 628, nr. 92.
[3] Kamerstukken 29 628 en 25 124, nr. 631.
[4] Kamerstukken 25 124 en 29 628, nr. 84.
[5] Kamerstukken 25 124 en 24 095, nr. 94.
[6] Kamerstuk 29 628, nr. 829.
[7] Kamerstuk 29 628, nr. 828.
[8] Kamerstuk 25 124, nr. 77.

kst-25124-96
ISSN 0921 - 7371
's-Gravenhage 2019

De zorgen rondom statelijke actoren die op steeds assertievere wijze eigen belangen centraal stellen, zijn in de afgelopen jaren toegenomen. Dit blijkt ook uit het jaarverslag van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) waarvan ik kennis heb genomen.[9] Uw Kamer is bij brief van 18 april 2019 geïnformeerd over het kabinetsbeleid over het tegengaan van statelijke dreigingen en de accenten in de aanpak voor de komende tijd.[10] Digitalisering maakt dat deze dreiging nieuwe vormen kan aannemen. Het Cyber Security Beeld Nederland 2018 en de jaarverslagen van de inlichtingendiensten laten zien dat digitale middelen door staten worden ingezet ten behoeve van onder andere manipulatie, sabotage en digitale spionage. Dit zorgt ervoor dat bepaalde risico's inherent zijn aan het gebruik van digitale systemen, zeker door de onderlinge verbondenheid binnen het digitale domein. Daarmee zijn ook voor C2000 geen absolute veiligheidsgaranties te geven. Bovendien kan ieder netwerk uitvallen door een technische storing of langdurige stroomuitval. De operationele diensten (Politie, Brandweer, Ambulancediensten en Koninklijke Marechaussee (Defensie)) hebben continuïteitsplannen die bij dergelijke situaties tijdelijk in werking treden om de hulp aan burgers zo goed als mogelijk te waarborgen.

Door de toegenomen zorgen over de groeiende invloed van statelijke actoren en veranderende geopolitieke verhoudingen achtte ik het noodzakelijk een risicobeoordeling te laten uitvoeren inzake de betrokkenheid van Hytera Mobilfunk GmbH bij de vernieuwing van het spraaknetwerk van C2000. Ook door uw Kamer zijn hier vragen over gesteld.[11]

Zoals aan uw Kamer bericht, opereert het kabinet bij het beoordelen van risico's ten aanzien van spionage, beïnvloeding of sabotage door statelijke actoren of andere derde partijen bij digitale producten als volgt.[12] Op een zeer zorgvuldige en *case-by-case*-basis worden deze risico's bezien. Daarbij worden de volgende overwegingen in ogenschouw genomen:

1. Is de partij die de dienst of product levert afkomstig, of staat hij onder controle van een partij, uit een land met wetgeving die commerciële of particuliere partijen verplicht samen te werken met de overheid van dat land, in het bijzonder met staatsorganen die zijn belast met een inlichtingen- of militaire taak, of is de partij een staatsbedrijf?
2. Is de partij die de dienst of product levert afkomstig uit een land met een actief offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen of een land waarmee de Nederlandse relatie dusdanig gespannen is dat acties die Nederlandse belangen aantasten voorstelbaar zijn?
3. A. Krijgt de partij die de dienst of product levert uitgebreide toegang tot gevoelige locaties, gevoelige ICT-systemen en vitale infrastructurele installaties of werken, waarbij misbruik een nationaal veiligheidsrisico kan vormen?
   B. Zijn er beheersmaatregelen mogelijk en realiseerbaar die de nationale veiligheidsrisico's die in het geding zijn voldoende beschermen?

Bovenstaande overwegingen zijn gehanteerd bij de risicobeoordeling ten aanzien van het vernieuwde C2000. Concluderend en samenvattend zijn mijn bevindingen naar aanleiding van de verschillende onderzoeken in lijn met de conclusies en het advies van de AIVD[13]:

---

[9] Kamerstuk 30 977, nr. 154
[10] Kamerstuk 30 821, nr. 72.
[11] Kamerstukken 29 517 en 28 684, nr. 155.
[12] Kamerstukken 25 124 en 29 628, nr. 92.
[13] In zowel het AIVD Jaarverslag 2018 (Kamerstuk 30 977, nr. 154) als bijgevoegd AIVD advies «Beantwoording advies-opdracht C2000», raadpleegbaar via www.tweedekamer.nl.

- Dat het in algemene zin onwenselijk is als gerubriceerde informatie en vitale processen binnen de rijksoverheid afhankelijk zijn van ICT-systemen uit landen waarvan is vastgesteld dat ze een offensief cyberprogramma tegen Nederland voeren, zoals China en Rusland.
- Dat het voor de betrouwbaarheid en beschikbaarheid van C2000 van belang is dat de migratie naar het vernieuwde C2000 doorgaat.
- Dat de betrokkenheid van een Chinese aandeelhouder bij C2000 een laag risico heeft maar permanente oplettendheid vraagt.
- Dat daarom wordt geadviseerd voor verantwoord gebruik van C2000 tijdens en na de migratie extra beveiligingsmaatregelen bij de leverancier en bij de beheerorganisatie te nemen.
- Dat wordt geadviseerd om zo snel mogelijk over te gaan naar een oplossing waarbij de afhankelijkheid van landen met een offensief cyberprogramma gericht tegen Nederlandse belangen is geminimaliseerd. De AIVD adviseert om parallel aan de migratie te starten met een vervangingstraject.

In het onderstaande ga ik in op:
A. De opdrachten voor de beveiligingsonderzoeken
B. De uitkomsten van de beveiligingsonderzoeken
C. De bevindingen
D. De aanvullende beveiligingsmaatregelen
E. Het alternatieve scenario
F. De conclusie en het vervolgtraject
G. De bredere context en het toekomstperspectief

A. Opdracht beveiligingsonderzoeken

Ik heb in de zomer van 2018 opdracht gegeven om te onderzoeken of de betrokkenheid van Hytera Mobilfunk GmbH leidt tot specifieke risico's met betrekking tot de invloed van statelijke actoren op C2000 en in hoeverre het mogelijk is om maatregelen te nemen om de beveiligingsrisico's in kwestie te verkleinen. De volgende beveiligingsonderzoeken hebben plaatsgevonden:
1. Het Nationaal Bureau Verbindingsbeveiliging (NBV) van de AIVD heeft onderzocht of door de betrokkenheid van Hytera Mobilfunk GmbH bij de vernieuwing van C2000, de democratische rechtsorde, de veiligheid of andere gewichtige belangen van de staat worden geschaad.
2. Het bedrijf Xebia heeft een security audit uitgevoerd naar de technische en organisatorische maatregelen die Hytera Mobilfunk GmbH als onderdeel van de vernieuwing van C2000 neemt.
3. Naar aanleiding van de security audit van Xebia heeft het bedrijf Valori verdiepend technisch onderzoek uitgevoerd, onder meer naar twee applicaties van het nieuwe spraaknetwerk die door Hytera China ontwikkeld zijn. Tevens heeft Valori audits uitgevoerd op de beheerprocessen van Hytera Mobilfunk GmbH.

In aanvulling op deze beveiligingsonderzoeken voert het bedrijf Fox-IT zogenoemde penetratietesten uit op het vernieuwde C2000. Bij deze penetratietesten wordt gepoogd daadwerkelijk het systeem binnen te dringen. Op basis van de uitkomsten ervan kunnen maatregelen worden genomen die de beveiliging van C2000 bevorderen. Penetratietesten vinden zowel voor als na migratie van het spraaknetwerk plaats en maken zo deel uit van het totaal van beveiligingsmaatregelen rond C2000.

Om de resultaten van deze onderzoeken in samenhang te bezien, heb ik professor dr. Bart Jacobs, als hoogleraar beveiliging en correctheid van programmatuur verbonden aan de Radboud Universiteit Nijmegen en lid

van de Cyber Security Raad, verzocht mij over het totaal aan onderzoeken en aanvullende maatregelen te adviseren.

Ik heb bovendien de maatregelen die ik op basis van het advies van de AIVD heb genomen weer ter beoordeling aan de AIVD voorgelegd.

Naast de bovengenoemde beveiligingsonderzoeken heb ik, voor het geval dat de bovengenoemde onderzoeken hier aanleiding toe zouden geven, verkend wat het alternatief is als besloten zou moeten worden om de huidige vernieuwing van C2000 op verantwoorde wijze af te breken.

B. Uitkomsten beveiligingsonderzoeken

Conform mijn eerdere toezeggingen[14] informeer ik u over de uitkomsten van de beveiligingsonderzoeken. Deze brief aan uw Kamer bevat openbare informatie. Om veiligheidsredenen is het op specifieke punten niet mogelijk in detail te treden omdat dan inzicht wordt gegeven in concrete aspecten van de beveiliging van C2000.

Op hoofdlijnen leveren de onderzoeken de volgende conclusies op:

- De AIVD concludeert dat de betrokkenheid van Hytera Mobilfunk GmbH bij de vernieuwing van C2000 op dit moment een laag risico geeft op misbruik door de Chinese overheid. Andere landen met een offensief cyberprogramma vormen een matig risico voor C2000.
- De security audit van Xebia geeft adviezen gericht op de bevordering van informatiebeveiliging van Hytera Mobilfunk GmbH, zowel vanuit het perspectief van maatregelen tegen Chinese statelijke actoren als in algemene zin. Xebia beoordeelt het huidige *security maturity* niveau[15] van Hytera Mobilfunk GmbH als «*not bad*».[16] Xebia karakteriseert dit als een gemiddelde score; dit betekent dat een basisniveau bereikt is maar dat verbeteringen nodig zijn om de informatiebeveiliging bij Hytera Mobilfunk GmbH op een hoger niveau te brengen. Xebia merkt in zijn audit op dat Hytera Mobilfunk GmbH zichzelf beschouwt als een Duits bedrijf en sterk hecht aan zijn onafhankelijkheid van Hytera China.
- Xebia wijst als één van de potentiele kwetsbaarheden op twee applicaties van het spraaknetwerk die door Hytera China zijn ontwikkeld en adviseert hierop passende maatregelen te treffen.
- Uit het verdiepend technisch onderzoek uitgevoerd door het bedrijf Valori naar de twee applicaties van het spraaknetwerk die door Hytera China zijn ontwikkeld, komt naar voren dat de functies transparant zijn en dat er geen indicaties zijn dat er door Hytera China «*backdoors*» zijn ingebouwd.
- Valori heeft tevens gekeken naar de beheerprocessen van Hytera Mobilfunk GmbH. Hieruit blijkt dat er een goede basis is om te komen tot beter beheerste processen op het gebied van security. Valori adviseert aanvullende maatregelen om in specifieke scenario's de weerstand tegen ongewenste invloed door statelijke actoren verder te verhogen.
- Voor de penetratietest zijn conform het advies van de AIVD de kritieke onderdelen in de infrastructuur (de zogeheten kroonjuwelen) van het vernieuwde C2000 bepaald en door Fox-IT getoetst om te bepalen of extra beveiliging en monitoring noodzakelijk is. Uit de test zijn

[14] Kamerstukken 29 517 en 28 684, nr. 155, Kamerstuk 25 124 en 29 628, nr. 92 en Kamerstuk 25 124, nr. 93.

[15] Het *security maturity* niveau ziet niet alleen op de feitelijke beveiliging, maar bijvoorbeeld ook het veiligheidsbewustzijn van het personeel.

[16] Xebia hanteert in dergelijke onderzoeken de volgende schaal: «terrible»-«better than nothing»-«not bad»-«good»-«next level».

aanbevelingen naar voren gekomen gericht op de versterking van de weerbaarheid van het netwerk. Onder leiding van het programmateam Implementatie en Vernieuwing C2000 is het opvolgen van de aanbevelingen in gang gezet en worden zowel door het voorgenoemde programma als bij het Meldkamerdienstencentrum van de politie maatregelen genomen.

Als bijlagen bij deze brief zijn gevoegd het openbare advies van het Nationaal Bureau Verbindingsbeveiliging van de AIVD (bijlage 1)[17],[18] de openbare samenvatting van de security audit van Xebia (bijlage 2)[19], het advies van professor Jacobs (bijlage 3)[20]. Het rapport van Xebia laat ik ter vertrouwelijke inzage leggen bij uw Kamer (Kamerstuk 25 124, nr. 95).

De hoofdbevindingen uit het advies van professor Jacobs luiden als volgt:
- Hij geeft aan dat het huidige C2000 dringend aan vervanging toe is, niet alleen met betrekking tot de functionaliteit, maar ook met betrekking tot beveiliging van het systeem.
- Hij constateert dat Hytera Mobilfunk GmbH het C2000 vernieuwingsproject is gestart zonder sterke beveiligingscultuur en zonder bewustzijn van de gevoeligheid van Chinese betrokkenheid. Hij constateert dat dit in de loop van het traject is verbeterd.
- Leidend bij de oordeelsvorming zijn voor hem de rapportages van de AIVD.
- Hij adviseert voort te gaan met de vernieuwing van C2000, op de ingeslagen weg, met de betrokken partijen, met voortdurende krachtige focus op beveiligingsaspecten, en met inachtneming van een aantal verbeterpunten. Deze verbeterpunten neem ik over en adresseer ik verderop in deze brief.

C. Bevindingen

Ik heb een intensief traject doorlopen om de risico's van spionage, beïnvloeding of sabotage door een statelijke actor voor het vernieuwde C2000 in kaart te brengen. De beveiligingsonderzoeken stellen mij, in het licht van de eerder in deze brief genoemde overwegingen ten aanzien van de risico's voor digitale producten door statelijke actoren, in staat een aantal belangrijke uitspraken te doen over de beveiliging van het vernieuwde C2000:
- Juist bij processen die van vitaal belang zijn voor de nationale veiligheid, zo ook bij het vernieuwde C2000, is een hoog niveau van beveiliging noodzaak. Evenwel is het onmogelijk om elke vorm van misbruik bij het ontwikkelen van het systeem uit te sluiten. Dat betekent dat naast de aandacht voor beveiliging bij het ontwerp en ontwikkelen van het systeem er veel en continue aandacht en alertheid moet zijn voor de beveiligingsmaatregelen rondom een dergelijk vitaal systeem. Dit betreft onder andere de beveiliging van verbindingen, firewalls, autorisatiebeheer, encryptie en een monitorings- en detectiesysteem waarmee eventuele aanvallen op het systeem tijdig kunnen worden onderkend.
- Er is een goede basis voor de beveiliging van het vernieuwde C2000, zo blijkt uit onderzoeken van Xebia en Valori. De *security maturity* van Hytera Mobilfunk GmbH dient echter te worden verbeterd. Ik zal daar scherp op toezien.

---

[17] Raadpleegbaar via www.tweedekamer.nl

[18] De onderbouwing van de conclusies zoals opgenomen in het advies van de AIVD zijn gerubriceerd omdat verspreiding ervan inzage zou geven in de beveiligingsmaatregelen rond C2000 en in de werkwijze en het kennisniveau van de AIVD.

[19] Raadpleegbaar via www.tweedekamer.nl

[20] Raadpleegbaar via www.tweedekamer.nl

- In zijn advies brengt professor Jacobs het beveiligingsniveau binnen de hulpdiensten onder de aandacht, waarbij hij constateert dat de zorgen daar primair gericht zijn op operationele continuïteit (Verbeterpunt 1). Dit is, in lijn met bovengenoemde overweging 3B van de risicocriteria ten aanzien van digitale producten, een belangrijk punt. Onderstaand ga ik in de paragraaf «conclusie en vervolgtraject» in op de wijze waarop ik in het heden maar ook na migratie wil blijven investeren op beveiligingsmaatregelen.

D. Aanvullende beveiligingsmaatregelen

De beveiligingsonderzoeken hebben geleid tot aanvullende contractuele, technische en organisatorische maatregelen ter verhoging van het beveiligingsniveau van het vernieuwde C2000. Deze maatregelen zien zowel op het tegengaan van ongewenste invloed van Chinese statelijke actoren als beveiliging in algemene zin. Ik noem u de belangrijkste maatregelen:

- Ik heb Hytera Mobilfunk GmbH opdracht gegeven tot het ontwikkelen van een verbeterplan om zijn *security maturity* niveau te verhogen. Ik laat de uitvoering daarvan nauwlettend monitoren door het programma Implementatie Vernieuwing C2000.
- Er zijn afspraken gemaakt over strikte compartimentering tussen de Chinese eigenaar en het Duitse ontwikkel-, productie- en beheerproces, en een meldplicht in het geval van wijzigingen daarvan. Er zal periodiek een audit worden uitgevoerd op de beheerprocessen van Hytera Mobilfunk GmbH, waarbij ook de feitelijke werking van de gemaakte afspraken getoetst wordt.
- Ik heb opdracht gegeven de verdere ontwikkeling en beheer van de hierboven genoemde applicaties die door Hytera China werden ontwikkeld over te brengen naar Hytera Mobilfunk GmbH in Duitsland.
- Ten aanzien van de broncode van Hytera Mobilfunk GmbH heb ik het recht te allen tijde inspecties te laten uitvoeren op de code. Dit recht heb ik reeds uitgeoefend door Valori een *source code review* te laten uitvoeren van de twee applicaties van het spraaknetwerk die door Hytera China zijn ontwikkeld. Daarbij zijn geen code-constructies aangetroffen die wijzen op oneigenlijke inmenging. Ik heb inmiddels met Hytera Mobilfunk GmbH afgesproken dat de broncode van deze twee door Hytera China ontwikkelde applicaties gepubliceerd wordt als *open source code*. Bij de verdere ontwikkeling van noodhulpcommunicatie wordt bezien hoe vorm kan worden gegeven aan de aanbeveling van professor Jacobs om systematischer gebruik te maken van *open source software* (Verbeterpunt 4).

De beveiligingsketen rondom het vernieuwde C2000 beslaat niet slechts Hytera Mobilfunk GmbH. Ook van de toekomstige beheerder van het vernieuwde C2000, het Meldkamerdienstencentrum van de politie, verwacht ik een adequaat beveiligingsniveau. De penetratietesten van Fox-IT richten zich daarom mede op dat deel van de beveiliging van het vernieuwde C2000 waarvoor het Meldkamerdienstencentrum verantwoordelijk is en zal ook daar tot aanvullende beveiligingsmaatregelen leiden. Verder wordt er binnen het Meldkamerdienstencentrum bijvoorbeeld ter voorbereiding op de nieuwe beheertaak geïnvesteerd in extra *(cyber)security*-trainingen. De aanbeveling van professor Jacobs die betrekking heeft op de verankering van de kennis en expertise ten aanzien van de beveiliging van C2000 binnen de betrokken hulpdiensten neem ik over (Verbeterpunt 2). Over de concrete uitwerking van deze aanbeveling vindt nader overleg met de hulpdiensten plaats.

Professor Jacobs dringt bovendien aan op het uitwerken van draaiboeken om in situaties van internationale spanning C2000 van de buitenwereld te isoleren (Verbeterpunt 3). De digitale veiligheid van C2000 wordt bewaakt door het Security Operations Centre van de politie. Bij oplopende spanningen en een toenemende internationale dreiging tegen Nederlandse belangen kunnen het Security Operations Centre en het Meldkamerdienstencentrum van de politie, in overleg met de NCTV, verscherpte veiligheidsmaatregelen nemen, waaronder het isoleren van C2000.

E. Alternatief scenario

Naast de beveiligingsonderzoeken heb ik, voor het geval dat de bovengenoemde onderzoeken hier aanleiding toe zouden geven, verkend of het mogelijk is om op verantwoorde wijze de huidige vernieuwing van C2000 af te breken en opnieuw te starten met de vernieuwing van het spraaknetwerk van C2000. In de kern komt dit scenario neer op het continueren van het huidige C2000 gedurende een aantal jaren en het met andere leveranciers starten van een nieuw traject voor de vernieuwing. In dit scenario zullen de belangrijkste doelen van het huidige vernieuwingstraject gedurende meerdere jaren niet gerealiseerd worden. Dit betreft de technische continuïteit, het verbeteren van de spraakcapaciteit bij rampen en crises en het verbeteren van de dekking van het spraaknetwerk.

Dit scenario bevat daarnaast een aantal forse risico's. Deze zijn onder andere gelegen in de veiligheid van burgers en hulpverleners. De hulpdiensten zullen immers voor een niet op voorhand voorzienbare termijn aangewezen blijven op het bestaande C2000, waarvan de stabiliteit en continuïteit in de nabije toekomst in toenemende mate onder druk komt te staan en waarvan geen up-to-date beveiliging mogelijk is.

De huidige leveranciers hebben eind 2012 aangegeven dat het eind van de technische levensduur in zicht was[21] en het systeem grote investeringen behoefde. Het netwerk bevat verouderde techniek waarvan steeds meer onderdelen niet meer verkrijgbaar zijn. Daardoor ontstaat een aanzienlijk risico op uitval van het huidige C2000. Tijdens uitval van het systeem is er geen communicatie via C2000 mogelijk tussen hulpdiensten onderling en tussen hulpdiensten en de meldkamer. Cruciale informatie over de situatie kan dan niet tussen hen gedeeld worden. Het kan daarbij gaan om (levens)gevaarlijke situaties voor hulpverleners en burgers. Voor de hulpdiensten zijn dan de C2000-verbindingen via hun portofoons en mobilofoons de *life-line* met elkaar en met de meldkamer. In geval van nood moeten Politie, Brandweer, Ambulancediensten en de Koninklijke Marechaussee (Defensie) blindelings kunnen vertrouwen op de werking ervan. Betrouwbare communicatie is bijvoorbeeld essentieel in situaties waarin vuurwapengeweld dreigt of bij ernstige ordeverstoringen, wanneer ambulancepersoneel communiceert met de meldkamer over levensreddende handelingen of wanneer er dringende communicatie nodig is bij een grote brand.

Het huidige spraaknetwerk kan slechts worden gecontinueerd door hier geen of slechts in beperkte mate wijzigingen in aan te brengen omdat aanpassingen kunnen leiden tot instabiliteit van het systeem. Dit betekent dat nieuwe operationele behoeften nauwelijks kunnen worden geïmplementeerd in het bestaande netwerk. Het huidige C2000 biedt daarmee ook niet de mogelijkheid om in te springen op nieuwe technologische ontwikkelingen, zodat de wendbaarheid van het systeem laag is.

---

[21] Bijlage bij Kamerstuk 25 124, nr. 87.

Deze beperkingen en het risico van uitval kunnen grote gevolgen hebben voor de veiligheid van burgers en van hulpverleners en op het functioneren van de diensten als zodanig. De operationele diensten hebben mij hier op gewezen en vanuit hun verantwoordelijkheid voor de veiligheid van hun medewerkers en burgers, het voorkomen van schade en maatschappelijke impact nadrukkelijk gepleit om voort te gaan met de vernieuwing.

Bij het volgen van dit scenario moet daarnaast rekening worden gehouden met de volgende elementen:

- De bestaande contractuele verhouding met Hytera Mobilfunk GmbH moet worden verbroken en de geïnstalleerde fysieke onderdelen van het nieuwe netwerk moeten ontmanteld worden. De juridische en financiële risico's kunnen hier, vanwege de potentiële consequenties voor de positie van de Nederlandse Staat in een mogelijke toekomstige procedure, slechts in algemene termen benoemd worden. Aan beëindiging zitten forse financiële en juridische risico's met een grote onzekerheidsmarge. De te verwachten financiële impact is enorm. Er zal rekening moeten worden gehouden met een langjarige afwikkeling van deze kwestie.
- Het continueren van het huidige C2000 leidt tot het terugbrengen van ambities op andere trajecten. Stappen die afhankelijk zijn van de vernieuwing van C2000, waaronder de samenvoegingen van meldkamers, de realisatie van de nieuwe ICT-infrastructuur van de landelijke meldkamers, de inrichting van het operatiecentrum van de Koninklijke Marechaussee (Defensie) en de vernieuwing van het meldkamersysteem GMS zullen ten minste forse vertraging oplopen. Alle operationele hulpdiensten zullen daar in meer of mindere mate hinder van ondervinden.
- De huidige kwetsbaarheid van de meldkamers blijft bestaan. Er kan niet tegemoet gekomen worden aan de operationele noodzaak het aantal werkplekken op meldkamers uit te breiden en meer randapparatuur in te zetten. De ontwikkelingen op dit punt komen stil te staan. Bestaande en nieuwe dekkingsissues kunnen niet opgelost worden waardoor de ontvangstzekerheid voor de hulpverleningsdiensten terugloopt, met alle gevolgen van dien. Daardoor kunnen noodzakelijke capaciteitsuitbreidingen in verband met bijvoorbeeld terrorismebestrijding slechts plaatsvinden ten koste van andere gebruikers op het netwerk.

Samenvattend constateer ik dat de doelen die de vernieuwing van C2000 beoogt in dit scenario niet op korte termijn gerealiseerd zullen worden. Daarnaast is er een aantal forse risico's aan verbonden. Met name het risico op het in het gedrang komen van de veiligheid van burgers en hulpverleners weegt voor mij zwaar.

F. Conclusie en vervolgtraject

Het totaal van de uitgevoerde beveiligingsonderzoeken heeft op een grondige wijze plaatsgevonden. Daarnaast is een verkenning naar een alternatief scenario uitgevoerd. Het jaarverslag en advies van de AIVD zijn nadrukkelijk meegewogen in de besluitvorming over het vervolgtraject. Naar aanleiding van de uitkomsten van de beveiligingsonderzoeken zijn en worden gerichte maatregelen getroffen die leiden tot een hogere weerbaarheid van het nieuwe C2000 tegen zowel het specifieke risico van betrokkenheid van Hytera China als tegen de dreiging van andere (statelijke) actoren. Ik heb in lijn met het advies van de AIVD voor verantwoord gebruik van C2000 tijdens en na de migratie extra beveiligingsmaatregelen bij de leverancier en bij de beheersorganisatie genomen. Ik zal daarop ook in de toekomst inzetten.

Een stuurgroep met daarin vertegenwoordigers van de operationele diensten adviseert mij over de vernieuwing van het systeem. Het vernieuwde C2000 is technisch nagenoeg gereed. Zodra het systeem operationeel ingezet kan worden, zal de stuurgroep mij van een advies voorzien over een geschikt moment voor migratie. Op basis daarvan kan ik vervolgens een besluit nemen over de migratiedatum. Ik vind een gedegen voorbereiding van de migratie van groot belang. De operationele diensten hebben aangegeven minimaal drie maanden nodig te hebben voor een zorgvuldige operationele voorbereiding van de migratie.

Hulpverleners hebben een grote operationele behoefte aan een robuust, betrouwbaar en veilig nieuw C2000. In mijn afwegingen heb ik tevens hun zorgen over de stabiliteit en houdbaarheid van het huidige C2000 meegenomen. Zij adviseren mij, gelet op de veiligheid van burgers en hulpverleners, met klem de lopende vernieuwing van het spraaknetwerk door te zetten.

Professor Jacobs geeft in zijn advies (bijlage 3 bij deze brief) aan dat absolute veiligheidsgaranties voor het vernieuwde C2000, net als voor andere moderne ICT-systemen, niet te geven zijn door de hoge mate van verbondenheid en verwevenheid met andere digitale systemen. Ook ik realiseer me dat er altijd bepaalde risico's bestaan bij de inzet van moderne digitale systemen. Risicoloze alternatieven bestaan niet. Niet voor het huidige C2000, niet voor het vernieuwde C2000 en niet voor de toekomst. Juist daarom kies ik steeds voor de minst risicovolle alternatieven, voorzien van passende beveiligingsmaatregelen en doorlopende monitoring.

De AIVD heeft bevestigd dat ik de geadviseerde maatregelen die in het gerubriceerde deel van zijn advies zijn opgenomen voortvarend heb opgepakt. Daarom kan de AIVD uitgaande van de huidige situatie, tot aan de vervanging, de keuze voor de uitrol van het vernieuwde C2000 onderschrijven, mits de adviezen betreffende verantwoord gebruik van het systeem ook na uitrol geborgd blijven. De brief van de AIVD van 19 april 2019 hierover is als bijlage bij deze brief gevoegd (bijlage 4).

Doorlopende aandacht, alertheid en middelen zijn nodig om het vereiste niveau van beveiliging in stand te houden en te versterken. Ook na de migratie van het spraaknetwerk, in de zogeheten beheerfase, is constante aandacht voor en investering op informatiebeveiliging noodzakelijk. Een samenstel van maatregelen zal ook na de migratie van het netwerk plaatshebben, waaronder begrepen:

- Periodieke beveiligingstesten.
- Geautomatiseerde inspectie van de apparatuur op signalen van misbruik.
- Penetratietesten en *red teaming*.
- Monitoring door het Security Operations Center van de politie.
- Permanente bevordering van informatiebeveiliging en informatiebeveiligingsbewustzijn onder personeel van zowel leveranciers en beheerders als gebruikers.

In het licht van het voorgaande kan ik op verantwoorde wijze vervolg geven aan de vernieuwing van het spraaknetwerk van C2000. Zodra het nieuwe systeem technisch gereed is, zal ik, op basis van een advies van de operationele diensten, een besluit nemen over de migratiedatum. Daarover zal ik uw Kamer uiteraard informeren. Ik ben gaarne bereid met uw Kamer nader in te gaan op mijn overwegingen om de vernieuwing van het spraaknetwerk van C2000 op verantwoorde wijze voort te zetten. Om te kunnen anticiperen op een besluit over de migratiedatum voor de zomer verzoek ik u hiervoor op korte termijn een moment te kiezen.

G. Bredere context en toekomstperspectief

Statelijke dreiging is in zijn aard veranderlijk en vraagt een adaptieve aanpak. Dit vereist ook voor vitale noodhulpcommunicatie een meerjarige strategie. De AIVD vindt het onwenselijk dat de rijksoverheid voor gevoelige informatie en vitale processen afhankelijk is van ICT-systemen uit landen waarvan is vastgesteld dat ze een offensief cyberprogramma voeren tegen Nederlandse belangen. Daarom adviseert de AIVD om zo snel mogelijk over te gaan op een oplossing waarbij deze afhankelijkheid is geminimaliseerd. Dit advies van de AIVD neem ik over. Ik heb onmiddellijk opdracht gegeven tot een verkenning naar een dergelijke oplossing en zal uw Kamer hierover na de zomer informeren. Volledigheidshalve merk ik op dat een traject van specificeren, marktverkenning, aanbesteding en realisatie naar alle waarschijnlijkheid rond de vijf jaar duurt.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus