> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Nationaal Coördinator Terrorismebestrijding en Veiligheid

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.nctv.nl

Ons kenmerk

2639346

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 1 juli 2019
Onderwerp Maatregelen bescherming telecomnetwerken en 5G

Inleiding

Mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties informeren wij uw Kamer over het volgende. Digitale connectiviteit is onmisbaar in onze huidige samenleving. We maken steeds meer gebruik van mobiel en vast internet. Nederland beschikt over een hoogwaardige infrastructuur.[1] Zo heeft Nederland meerdere mobiele 4G-netwerken en twee vaste netwerken. Deze netwerken zijn aangemerkt als vitaal proces en leveren een belangrijke bijdrage aan het gunstige ondernemings- en vestigingsklimaat in Nederland. Het is van belang die sterke positie ook in de toekomst te behouden. Dit past ook binnen de ambities van dit kabinet om digitaal koploper van Europa te zijn. Daar is de uitrol van 5G-netwerken voor nodig. Telecombedrijven bereiden zich voor op deze nieuwe 5G-toepassingen. Denk hierbij aan de zelfrijdende auto, medische operaties op afstand en het verder optimaliseren van productieprocessen. Deze 5G-netwerken hebben onder meer hogere pieksnelheden en lagere reactietijden dan de 4G-netwerken. De 5G-netwerken zijn geen geïsoleerd netwerk, maar bouwen verder op de bestaande netwerken.[2]

Er bestaat, ook bij uw Kamer, ongerustheid over risico's bij de uitrol van 5G die samenhangen met toeleveranciers van technologie voor deze telecommunicatienetwerken. Er zijn meerdere moties door uw Kamer ingediend over dit onderwerp, waarin u onder andere de urgentie van de aanpak van deze problematiek en de noodzaak voor een gecoördineerde EU aanpak benadrukt.[3] Ook is door uw Kamer eerder gevraagd om een reactie op de artikelen "Expert: angst voor gluurgevaar uit Azië is terecht" en "VS waarschuwt providers in andere landen voor Huawei".[4] Verder heeft lid Klaver (GroenLinks) tijdens de Regeling van Werkzaamheden op 3 april 2019 (Handelingen II 2018/19, nr. 70) verzocht om een debat te voeren over onder andere de uitrol van 5G, voordat onomkeerbare besluiten worden genomen.

[1] Europese Commissie (2018), The Digital Economy and Society Index (DESI).
[2] Europese Commissie (2019), Aanbeveling Cyberbeveiliging van 5G
[3] Motie van het lid Weverling c.s. (Kamerstuk 21501-33, nr.734), en motie van het lid Van den Berg c.s. (Kamerstuk 21501-33, nr.747), Motie van lid Weverling c.s. (Kamerstuk 24 095, nr. 471), en motie lid Sjoerdsma c.s. (Kamerstuk 24 095, nr. 476).
[4] 28-11-2018, Kenmerk 2018Z22045/2018D57007

Deze brief geeft nadere invulling aan deze moties en verzoeken uit de Kamer en informeert u over de uitkomsten van de Taskforce Economische Veiligheid zoals toegezegd aan uw Kamer.[5]

Nationale Veiligheid en 5G

Het kabinet deelt de zorgen van uw Kamer waar het gaat om toenemende risico's en dreigingen vanuit statelijke actoren, zoals eerder al gemeld aan uw Kamer.[6] De inlichtingen- en veiligheidsdiensten verwijzen ook in hun laatste jaarverslagen naar de dreigingen die uitgaan van spionage en sabotage door statelijke actoren. In de afgelopen jaren zien de AIVD en de MIVD een toename van het aantal *'supply chain attacks'* door statelijke actoren. In diverse publicaties, al dan niet gerubriceerd, zijn de AIVD en de MIVD ingegaan op de dreigingen van statelijke actoren, gebaseerd op een eigenstandige informatie positie, gericht op de telecomsector, waarbij specifiek is ingegaan op de mogelijke risico's van de introductie van 5G in relatie tot de nationale veiligheid. Bij *supply chain attacks* worden dienstverleners, zoals internet service providers, telecomproviders en managed service providers, ingezet als springplank om doelwitorganisaties te infiltreren. Er wordt dan misbruik gemaakt van de hard- en software van deze dienstverleners om zo toegang te krijgen tot het netwerk van doelwitorganisaties. Het misbruiken van de hard- en software van deze dienstverleners is interessant voor statelijke actoren, omdat het omvangrijke, diepgravende en structurele toegang geeft tot data(stromen) in de netwerken van de doelwitorganisaties. Dit biedt spionagemogelijkheden door zo op grote schaal persoons-, technisch-wetenschappelijke, financieel-economische, militaire en politiek-bestuurlijke gegevens van zowel publieke, militaire en private organisaties te vergaren.

De AIVD en de MIVD hebben vastgesteld dat infiltratie van de dienstverleners door statelijke actoren spionage faciliteert. Tevens kan het een risico vormen voor innesteling in de Nederlandse vitale infrastructuur voor mogelijke sabotagedoeleinden. Hierdoor kunnen de aan het internet gekoppelde besturings- en controlesystemen van vitale infrastructuren, zoals drinkwatervoorziening, elektriciteitsdistributie en betalingsverkeer, verstoord worden. Daar bovenop komt dat diverse landen nationale wet- en regelgeving hebben om dienstverleners te dwingen tot medewerking aan inlichtingenactiviteiten. Er wordt dan door statelijke actoren gebruik gemaakt van de legitieme toegang die de dienstverlener heeft binnen de netwerken van doelwitorganisaties, waardoor preventie en detectie van misbruik bemoeilijkt wordt. De risico's voor de nationale veiligheid worden significant vergroot als deze dienstverleners ook nog eens afkomstig zijn uit landen die een offensief cyberprogramma voeren tegen de Nederlandse belangen.

5G faciliteert naar verwachting een significante toename van de aan het internet gekoppelde hard- en software in de persoonlijke levenssfeer van burgers, het bedrijfsleven, de vitale infrastructuur, Defensie en de (Rijks)overheid. Daardoor zal het goed functioneren van de Nederlandse maatschappij steeds meer afhankelijk zijn van 5G. De keerzijde van deze afhankelijkheid is dat we als gehele Nederlandse samenleving in toenemende mate kwetsbaar zijn bij potentieel misbruik door digitale spionage en sabotage. Hierdoor creëert de introductie van 5G substantiële risico's voor de privacy van burgers en voor de vertrouwelijkheid van gevoelige bedrijfs- en overheidsinformatie. Daarnaast is de

[5] Tweede Kamerbrief d.d. 1 april 2019 'Reactie op bericht KPN gaat in zee met Huawei voor aanleg 5G.'

[6] Tweede Kamerbrief Tegengaan Statelijke dreigingen (Kamerstuk 30 821, nr. 72) en het Cybersecurity Beeld Nederland 2019

continuïteit en beschikbaarheid van het bedrijfsleven en de vitale infrastructuur en de dienstverlening van de (Rijks)overheid in het geding. In potentie zal misbruik ertoe kunnen leiden dat grote delen van de Nederlandse samenleving kunnen uitvallen.

Werkwijze en bevindingen Taskforce Economische Veiligheid
Vanwege deze dreiging is onder leiding van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) een interdepartementale Taskforce Economische Veiligheid opgericht met vertegenwoordigers van de ministeries van J&V (NCTV), EZK, BZK, BZ, BHOS, Defensie, Fin en de AIVD en MIVD om te adviseren over deze problematiek.[7] De Taskforce is voor wat betreft samenstelling en activiteiten zo opgezet dat evenwichtige besluitvorming kan plaatsvinden waarbij zowel rekening wordt gehouden met veiligheids- als economische belangen. Het advies van de Taskforce is mede gebaseerd op (dreigings)analyses van de AIVD en de MIVD. De door alle partijen onderschreven voorgestelde maatregelen van de Taskforce geven een adequaat antwoord op de dreiging.

De Taskforce heeft met medewerking van de drie grote telecomaanbieders (KPN, T-Mobile en VodafoneZiggo) een risicoanalyse uitgevoerd naar de kwetsbaarheid van telecommunicatienetwerken voor misbruik via leveranciers van technologie. Telecomaanbieders treffen al verscheidene maatregelen hiertegen. Op basis van deze analyse zullen telecomaanbieders worden verplicht om aanvullende beveiligingsmaatregelen te nemen om de weerbaarheid tegen bovenbedoelde dreiging te verhogen.

Een van de maatregelen die wordt genomen is dat extra hoge eisen worden gesteld aan leveranciers van diensten en producten in de kritieke onderdelen in het telecomnetwerk. De kritieke onderdelen zijn geïdentificeerd op basis van de risicoanalyse. Hiermee wordt de kwetsbaarheid van de telecommunicatienetwerken voor misbruik via leveranciers van technologie voor deze netwerken verder verminderd. De noodzakelijke aanscherpingen van de eisen die worden gesteld aan de veiligheid en integriteit van de mobiele telecommunicatienetwerken zullen worden vastgelegd in een algemene maatregel van bestuur, die dit najaar zal worden gepubliceerd. Vanwege risico's voor de nationale veiligheid zal de Kamer in een vertrouwelijke setting nader worden geïnformeerd over de bevindingen van de Taskforce.

De 5G netwerken bouwen voort op het huidige netwerk en dat maakt dat de voor het huidige netwerk uitgevoerde risico analyse ook van belang is voor het toekomstige 5G netwerk. Een structurele aanpak is nodig omdat er continu ontwikkelingen zijn in het dreigingsbeeld, technologische ontwikkelingen binnen de telecomsector razendsnel gaan en het belangrijk is om goed zicht te hebben op de (technische) werking van de telecomnetwerken om te identificeren waar maatregelen nodig zijn. In samenwerking met de telecomaanbieders wordt een structureel proces ingericht, waarbij ontwikkelingen in dreiging en techniek in samenhang worden bezien, passend bij de huidige verantwoordelijkheden en rollen. Voor zover de nationale veiligheid hierdoor niet in het geding komt wordt zo veel mogelijk rekening gehouden met de bedrijfseconomische aspecten.

[7] Tweede Kamerbrief d.d. 1 april 2019 'Reactie op bericht KPN gaat in zee met Huawei voor aanleg 5G.'

Het kabinet steunt een gezamenlijke Europese aanpak
De veiligheid van de 5G-telecommunicatienetwerken staat Europees op de agenda. Een Europese aanpak kan bijdragen aan de effectiviteit van de maatregelen. Zoals aangegeven in de Nederlandse Cybersecurity Agenda[8] maakt het grensoverschrijdende karakter van cybersecurity internationale samenwerking door bijvoorbeeld internationale wetgeving, coalitievorming of internationale ontwikkeling van normen en standaarden, in het bijzonder in Europees verband, noodzakelijk. Daarom heeft het kabinet conform de moties Weverling en Van den Berg[9] gepleit voor meer Europese samenwerking op het gebied van 5G veiligheid. Het kabinet is daarom verheugd dat de Europese Commissie dit onderwerp actief oppakt, middels de aanbeveling "Cyberbeveiliging van 5G-netwerken", van 26 maart jongstleden.[10]

Het kabinet steunt dan ook een gezamenlijke Europese aanpak die via deze aanbeveling vorm krijgt. Er wordt daarbij vooral toegevoegde waarde gezien in het uitwisselen van risicoanalyses en het delen van oplossingsrichtingen tussen lidstaten. Nederland zal aan het Europese traject voortvloeiend uit deze aanbeveling een actieve bijdrage leveren, en daarbij zijn ervaringen uitdragen. De aanbeveling stelt dat eind 2019 het EU traject moet resulteren in een instrumentarium dat maatregelen bevat om (nationaal) geïdentificeerde risico's te kunnen aanpakken. Het BNC-fiche, dat het gedetailleerde kabinetsstandpunt over deze aanbeveling bevat, ontvangt u separaat.

Ter afsluiting
Het adresseren van de zorgen rondom kwetsbaarheden in de telecomsector past binnen de bredere aanpak op het tegengaan van statelijke dreigingen en het bevorderen van cybersecurity zoals met uw Kamer gedeeld.[11] Naast de telecomsector spelen ook in andere vitale diensten en processen zorgen over dreigingen die uitgaan van statelijke actoren. Het kabinet acht het van groot belang dat bij het toetsen van nationale veiligheidsrisico's in relatie tot de vitale infrastructuur, gebruik wordt gemaakt van consistente, op dreiging gebaseerde en technische up to date zijnde criteria, en dat, omwille van het tijdig anticiperen op ontwikkelingen, inzichtelijk is hoe de Nederlandse vitale infrastructuur zich technisch en organisatorisch ontwikkelt. Zoals aangegeven in de Nationale Veiligheid Strategie zal het kabinet daarom, in samenwerking met al deze partijen, een versterkte aanpak van bescherming van de vitale infrastructuur ontwikkelen. Onderdeel van deze aanpak is een structuur om kennis, kunde en expertise te bundelen om nationale veiligheidsrisico's ten behoeve van de vitale infrastructuur, nu en in de toekomst, adequaat te adresseren.[12]

[8] Nederlandse Cybersecurity Agenda (Kamerstuk 26 643, nr. 536).
[9] Motie van het lid Weverling c.s. (Kamerstuk 21501-33, nr.734) en motie van het lid Van den Berg c.s. (Kamerstuk 21501-33, nr.747)
[10] Europese Commissie (2019), Aanbeveling Cyberbeveiliging van 5G-netwerken.
[11] Tweede Kamerbrief Tegengaan Statelijke dreigingen (Kamerstuk 30 821, nr. 72) en Nederlandse Cybersecurity Agenda (Kamerstuk 26 643, nr. 536).
[12] Nationale Veiligheidsstrategie 2019, aangeboden aan de Tweede Kamer op 7 juni 2019

Nationaal Coördinator Terrorismebestrijding en Veiligheid

Datum
1 juli 2019

Ons kenmerk
2639346

De Minister van Justitie en Veiligheid,

Ferd Grapperhaus

De Staatssecretaris van Economische Zaken en Klimaat,

mr. drs. M.C.G. Keijzer