Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

370

Vragen van het lid **Sylvana Simons** (BIJ1) aan de Minister van Justitie en Veiligheid over *het gebruik van een Israëlisch tapsysteem door de afdeling Interceptie & Sensing van de nationale politie* (ingezonden 4 oktober 2022).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid) (ontvangen 18 oktober 2022).

Vraag 1
Bent u bekend met het nieuwsbericht «Opsporing komt in gevaar door disfunctioneren tapkamer politie» in de NRC?[1]

Antwoord 1
Ja, ik heb kennisgenomen van dit bericht. Op 4 oktober jl. heb ik ook een brief aan uw Kamer gestuurd met daarin mijn reactie op dit artikel (Kamerstuk 29628–1124).
Over hetzelfde bericht zijn ook schriftelijke vragen gesteld door het lid Bisschop (SGP) met nummer (Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 368) en de leden Helder en Wilders (PVV) met nummer (Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 369). De vragen komen gedeeltelijk overeen; ik zal daarom de beantwoording van beide sets vragen gelijktijdig aan u doen toekomen.

Vraag 2
Was u op de hoogte van de problemen met het aan de Israëlische overheid gelieerde Elbit-systeem? Zo ja, hoe lang al? En waarom is de Kamer niet eerder op de hoogte gebracht van deze problemen?

Antwoord 2
Mijn departement wordt regelmatig geïnformeerd over de voortgang van de invoering van het tapsysteem door de politie. De Tweede Kamer is vanaf de start van de aanbesteding geïnformeerd over de werving van het nieuwe tapsysteem. Mijn ambtsvoorganger heeft op 1 juli 2019[2] de Kamer geïnformeerd over de aanschaf van het nieuwe systeem. Vervolgens is in 2020[3]

[1] NRC 28 september 2022, (https://www.nrc.nl/nieuws/2022/09/28/opsporing-komt-in-gevaar-door-disfunctioneren-tapkamer-politie-a4143537).
[2] Kamerstuk 29 628 nr. 890.
[3] Kamerstuk 29 628 nr. 948.

ah-tk-20222023-370
ISSN 0921 - 7398
's-Gravenhage 2022

gemeld dat vanwege de complexiteit van het gehele project de implementatie tot ten minste 2022 zal gaan duren.

Vraag 3
Wat was het programma van eisen voor deze aanbesteding? In hoeverre en op welke wijze voldoet Elbit wel en niet aan deze eisen?

Antwoord 3
Het aanbod op basis waarvan deze opdracht aan Elbit is gegund voldoet aan het programma van eisen. Eerder heb ik uw Kamer gemeld het aanbestedingstraject een open en gesloten fase kende. Omdat het programma van eisen onderdeel uitmaakt van het gesloten deel van de aanbesteding worden daar inhoudelijk geen mededelingen over gedaan.

Vraag 4
Waarom is door uw Ministerie nooit aan de Kamer gemeld dat men terugvalt op een aanvullend systeem van het Nederlandse security bedrijf Fox-IT?

Antwoord 4
De politie valt niet terug op dit systeem: Replay werd ingezet om te kunnen voldoen aan de behoefte om IP-data te analyseren die op basis van de toenmalige standaard voor de aanlevering van telecomgegevens door aanbieders werd geleverd. Het toenmalige tapsysteem kon dat toen nog niet. Het systeem is reeds enkele jaren geleden uitgefaseerd.
In de tijd dat Replay – het systeem van Fox-IT – ontwikkeld werd, vanaf 2003, was het niet gebruikelijk dit soort systemen te melden. De politie volgt de reguliere verwervings- en aanbestedingsprocedures en die worden niet standaard gecommuniceerd aan de Tweede Kamer. Sinds 2019 is de politie aangesloten op het stelsel van het Adviescollege ICT-toetsing voor projecten met een ICT-component van meer dan 5 miljoen euro. Via deze toetsing wordt uw Kamer geïnformeerd. Alle andere bijzonderheden, bijvoorbeeld bij hoog risico, meldt de politie via reguliere rapportages. Op basis van de rapportages van politie kan mijn ministerie besluiten de Kamer te informeren. Hoewel de Kamer nu meer geïnformeerd wordt over ICT-systemen, bijvoorbeeld door het Adviescollege ICT-toetsing, wordt ook nu terughoudend omgegaan met het publiek maken van de gebruikte systemen met het oog op veiligheidsrisico's.

Vraag 5
Waarom beweerde uw Ministerie jarenlang onterecht dat een dergelijk tapsysteem niet in Nederland ontwikkeld kan worden en dat dat het argument is om terug te vallen op Israëlische systemen, eerst van Verint (nu Cognyte) en nu van Elbit, ondanks de daarbij behorende risico's met betrekking tot staatsveiligheid en privacy?

Antwoord 5
Er is niet beweerd dat een dergelijk tapsysteem niet in Nederland ontwikkeld kan worden. De politie heeft voorafgaand aan de aanbesteding overwogen of zij zelf een tapsysteem kon bouwen, waardoor zij ook zelf de volledige regie zou hebben op de toegang tot het systeem. Dit idee is echter verworpen omdat het zelf bouwen van een tapsysteem zeer complex is, er goede alternatieven in de markt beschikbaar zijn, regie en toegangsvereisten meegenomen kunnen worden bij verwerving en de benodigde specifieke IV-expertise en -capaciteit van de politie begrensd is.
Nederlandse bedrijven konden gewoon meedoen aan de aanbesteding.

Vraag 6
Waarom gaf u aan dat het beheer en onderhoud van het systeem bij en door de politie zelf gebeurt, terwijl nu blijkt dat dat niet zo is?

Antwoord 6
Het beheer en onderhoud van het tapsysteem gebeurt bij en door de politie. Bij het antwoord op vraag 7 staat nader toegelicht hoe dat is ingericht.

Vraag 7
Vindt u het geoorloofd dat medewerkers van het Israëlische bedrijf Elbit permanent aanwezig zijn in de tapkamer in Driebergen, een extra beveiligde ruimte waar ook tal van andere gevoelige informatie ligt opgeslagen? Kunt u uw antwoord toelichten?

Antwoord 7
Dit is niet het geval. Het nieuwe systeem dat wordt geleverd door Elbit wordt niet op de locatie Driebergen ontwikkeld. Er zijn daar dan ook geen medewerkers van Elbit aanwezig.
Bij het huidige systeem zijn beheermaatregelen en procedurele afspraken gemaakt met betrekking tot de locatie Driebergen. Het systeem wordt beheerd door de politie. De technisch beheerder van de leverancier is ingebed in het beheerteam. Deze is op dezelfde wijze gescreend als de medewerkers van de politie. De technisch beheerder van de leverancier kan niet vrij rondlopen in het pand van de politie. Hij wordt opgehaald bij de ingang en begeleid naar zijn werkplek. Er is collegiaal zicht op wat de technisch beheerder doet en er is toegangs- en toezichtscontrole op het handelen van de leverancier. De technisch beheerder van de leverancier kan niet zelfstandig bepaalde handelingen in het systeem verrichten, maar kan dat alleen doen met toestemming van de politie. Hierover is uw Kamer eerder geïnformeerd.[4]
Bij het nieuwe systeem is het beheer anders ingericht. Hier heeft de politie ervoor gekozen dat de nieuwe leverancier, Elbit, alleen software en derdelijns support levert. Voor de inrichting van de maatregelen daarbij verwijs ik naar het antwoord op vraag 8.
Zowel het huidige als het nieuwe tapsysteem bevinden zich in het hoog beveiligde rekencentrum van de politie waar slechts daarvoor geautoriseerde personen toegang toe hebben.

Vraag 8
Welke garantie kunt u geven dat onze gegevens en informatie in veilige handen zijn nu deze worden getapt met een Israëlisch systeem waar vanaf het begin in de Kamer al zorgen over bestonden vanwege de spionage risico's? Hoe plaatst u deze risico's in het licht van recente Israelische spionageschandalen zoals het Pegasus-schandaal van het tevens Israëlische bedrijf NSO?

Antwoord 8
Uiteraard zijn ook bij het nieuwe systeem afspraken gemaakt en beheersmaatregelen genomen zodat de leverancier geen toegang heeft tot gevoelige locaties en ICT-systemen. Ter borging hiervan zijn onder andere diverse eisen met betrekking tot logging en monitoring contractueel vastgelegd. Verder voeren de beveiligingsexperts van de politie en externe experts periodiek beveiligingsonderzoeken uit waaronder toetsing op kwetsbaarheden en is er constante monitoring van ongewenst netwerkverkeer. Hiermee worden kwetsbaarheden en risico's tijdig in kaart gebracht.
Zoals bij vraag 7 aangegeven staat ook het nieuwe tapsysteem in het hoog beveiligde rekencentrum van de politie. Tijdens de huidige implementatieperiode als ook na ingebruikname van het systeem door de politie heeft de leverancier geen fysieke en logische toegang tot productiedata (tapdata). De leverancier levert software maar verwerkt geen tapdata en heeft dan ook geen toegang tot de tapdata.

Vraag 9 en 10
Kunt u uitleggen waarom het Nederlandse Ministerie van Economische Zaken in 2021 samen met de Stichting Nederlandse Industrie voor Defensie en Veiligheid (NIDV) een promotiebijeenkomst voor Elbit heeft georganiseerd? Was dat onderdeel van deze of een andere overeenkomst met Elbit?
Kunt u toelichten in hoeverre het zakendoen met Elbit in overeenstemming is met de OESO (Organisatie voor Economische Samenwerking en

[4] Onder meer Vergaderjaar 2013–2014, Kamerstuk 33 750 nr. 95, Vergaderjaar 2015–2016, Kamerstuk 30 517 nr. 29, Vergaderjaar 2015–2016, Kamerstuk 30 517 nr. 30.

Ontwikkeling)-richtlijnen? Hoe plaatst u uw aanbesteding in het licht van het feit dat Elbit ook clustermunitie produceert?

Antwoord 9 en 10
Het Ministerie van EZK laat mij weten dat de informatiebijeenkomst met Elbit geen directe relatie had met het genoemde Elbit systeem, maar was georganiseerd om kabinetsbeleid beschreven in de Defensie-industrie Strategie (2018) te ondersteunen. Tijdens genoemde informatiebijeenkomst werd onderzocht of samenwerking met het bedrijf Elbit interessant kan zijn voor Nederlandse bedrijven. Mocht er door Nederlandse bedrijven opvolging worden gegeven aan deze informatiebijeenkomst – resulterend in een samenwerkingsverband en eventuele leveringen aan Israël vanuit Nederland, zullen deze zoals gebruikelijk onderhevig zijn aan exportcontrole in Nederland. Daarbij wordt onder andere getoetst of er een duidelijk risico is dat de uit te voeren goederen worden gebruikt bij het begaan van ernstige schendingen van mensenrechten of humanitair oorlogsrecht. Wanneer daar een risico op is, wordt geen vergunning voor uitvoer afgegeven. Uw Kamer is eerder over deze informatie bijeenkomst geïnformeerd op 13 september 2021 in antwoord op vragen van het lid Jasper van Dijk.[5]
Na de gunning van het nieuwe tapsysteem bleek dat Elbit Systems, het moederbedrijf van de leverancier, vanwege de overname van de firma IMI (eind 2018) door PAX werd aangemerkt als clustermunitieproducent. Voor het onderdeel van Elbit dat het tapsysteem aan de politie levert (Cyber Intelligence Ltd) geldt dat niet.

Vraag 11
Bent u, gezien het slecht functioneren van het huidige systeem, de spionage- en privacyrisico's en de link met mensenrechtenschendingen, voornemens om het huidige contract met Elbit te verbreken? Kunt u uw antwoord toelichten?

Antwoord 11
Ik zie daar vooralsnog geen aanleiding toe, het betreft een afgerond aanbestedingstraject, dat naar behoren is verlopen. In een aanbesteding wordt getoetst of op een inschrijver de wettelijke uitsluitingsgronden van de Aanbestedingswet van toepassing zijn. Er was destijds en er is nu geen reden om Elbit uit te sluiten. Het gaat hier om een leverancier die aan vele landen apparatuur levert en waar ook breder binnen de rijksoverheid zaken mee worden gedaan. Het opzeggen van het contract zou ook tot zeer grote vertraging leiden bij de oplevering van het nieuwe tapsysteem en het huidige tapsysteem is hoewel het nog voldoende functioneert inmiddels end-of-life. Ook betekent opzegging van het contract dat het hele verwervingsproces opnieuw gestart moet worden. Het zou de opsporing in Nederland voor grote problemen plaatsen en op achterstand zetten.

Vraag 12
Wat is uw visie op de mogelijkheid om de Nederlandse staatsveiligheid te bevorderen zonder handelsovereenkomsten af te sluiten met bedrijven die gelieerd zijn aan landen die verantwoordelijk zijn voor grove mensenrechtenschendingen?

Antwoord 12
In algemene zin biedt het wettelijk kader van de Aanbestedingswet 2012 en Europese regelgeving daaromtrent de mogelijkheid om bij aanbestedingen specifieke (veiligheids)eisen als voorwaarden te stellen aan de (mogelijke) opdrachtnemer. Hier kan op worden gecontroleerd tijdens het aanbestedingsproces en gedurende de looptijd van het contract. Zo mogen partijen uit landen die geen onderdeel zijn van de Government Procurement Act (GPA) worden uitgesloten.
Ook kunnen zogenoemde Internationale Sociale Voorwaarden van toepassing worden verklaard en in een overeenkomst worden opgenomen. Deze voorwaarden hebben betrekking op het terugdringen en uitbannen van schendingen van de mensenrechten in de productieketen. Dit verplicht de

[5] Aanhangsel Handelingen, vergaderjaar 2020–2021, nr. 4020.

opdrachtnemer onder andere om jaarlijks een due diligence uit te voeren om de risico's op het gebied van arbeids- en mensenrechten in de eigen productieketen in kaart te brengen.