Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

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

3252

Vragen van de leden **Omtzigt** (Omtzigt) en **Jasper vanDijk** (SP) aan de Ministers van Binnenlandse Zaken en Koninkrijksrelaties, van Justitie en Veiligheid, voor Rechtsbescherming en van Defensie en de Minister-President over *het gebruik van hacksoftware, zoals Pegasus, in Nederland* (ingezonden 30 mei 2022).

Antwoord van Minister **Bruins Slot** (Binnenlandse Zaken en Koninkrijksrelaties) en van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid) (ontvangen 23 juni 2022).

Vraag 1
Herinnert u zich dat in het regeerakkoord van 2017 is afgesproken: «Voor de uitvoering van de Wet Computercriminaliteit III komt 10 miljoen euro extra beschikbaar. Daarbij zal slechts in een specifieke zaak hacksoftware worden ingekocht door opsporingsdiensten. Leveranciers van dergelijke software worden gescreend door de AIVD en verkopen niet aan dubieuze regimes. Statistieken over het gebruik van hacksoftware worden jaarlijks openbaar gemaakt. Bij de evaluatie van de wet na twee jaar wordt bezien in hoeverre deze regeling de effectiviteit van de wet ernstig aantast. In dat geval wordt alsnog de aanschaf van hacksoftware voor algemeen gebruik overwogen.»?

Antwoord 1
Ja.

Vraag 2
Heeft Nederland in de afgelopen jaren hacksoftware, zoals Pegasus, aangeschaft? Zo ja, wanneer is welke software aangeschaft?

Antwoord 2
In het algemeen geldt dat het Nederlandse organisaties niet is toegestaan binnen te dringen in geautomatiseerde werken. Uitzonderingen zijn gemaakt voor justitie en politiediensten ter opsporing van strafbare feiten in het kader van de Wet
Computercriminaliteit III (de Wet CCIII), en voor inlichtingen- en veiligheidsdiensten ter bescherming van de nationale veiligheid in het kader van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017).
De Wet CCIII vormt de grondslag voor het aanschaffen en inzetten van soft- en hardware door de opsporingsdiensten om binnen te dringen in geautomatiseerde werken. Dit doen de opsporingsdiensten ten behoeve van het

ah-tk-20212022-3252
ISSN 0921 - 7398
's-Gravenhage 2022

uitvoeren van de bijzondere opsporingsbevoegdheid zoals vastgelegd in artikelen 126nba, 126uba en 126zpa. De uitvoering van deze bevoegdheid is centraal belegd bij een technisch team dat is ondergebracht bij de Landelijke Eenheid van de politie. De Wet CCIII is op 1 maart 2019 in werking getreden. Vanaf dat jaar is commerciële binnendringsoftware aangeschaft bij een externe ontwikkelaar.
De politie gebruikt extern ontwikkelde binnendringsoftware voor het uitvoeren van de bijzondere opsporingsbevoegdheid van artikel 126nba Sv. Binnendringen gebeurt met verschillende onderzoeksdoeleinden, te weten: (a) het identificeren van het geautomatiseerd werk of gebruiker en (b) de vastlegging van gegevens. Bestaande doelen zijn (c) tap, opslaan vertrouwelijke informatie, afluisteren, (d) observatie en (e) ontoegankelijk maken. Binnendringsoftware is hierbij een zwaar maar noodzakelijk middel voor de uitvoering van de wettelijke bijzondere opsporingsbevoegdheid die is gebonden aan diverse waarborgen.
Als de officier van justitie bepaalt dat gebruik van binnendringsoftware van een externe leverancier noodzakelijk is, wordt dit centraal bij het OM getoetst alvorens in een specifieke zaak wordt overgegaan tot aanschaf door de politie.
Het verstrekken van informatie aan derden over welke specifieke software de politie beschikt en gebruikt bij de inzet van deze bijzondere opsporingsbevoegdheid, brengt onaanvaardbare risico's met zich mee voor de inzetbaarheid van die middelen en daarmee het opsporingsbelang. De verwerving van binnendring soft- en hardware vindt bij de politie onder geheimhouding plaats. Het is voor de afscherming van middelen en methodieken niet mogelijk om openbaar inzicht te geven in welke software de politie gebruikt bij de uitvoering van deze bevoegdheid.
De Wiv 2017 bevat de bijzondere bevoegdheid van het binnendringen van een geautomatiseerd werk ex artikel 45 Wiv 2017. Over de wijze waarop de inlichtingen- en veiligheidsdiensten gebruikmaken van hun wettelijke bevoegdheden kan in het openbaar geen mededeling worden gedaan.

Vraag 3
Indien hacksoftware is aangeschaft, welke diensten (zoals politie, AIVD, MIVD en NCTV en anderen) hebben gebruik gemaakt van de hacksoftware of hebben er gebruik van kunnen maken?

Antwoord 3
Ten aanzien van de politie is bekend, zoals onder andere weergegeven in de inspectieverslagen van de Inspectie Justitie & Veiligheid en het jaarverslag Politie dat uw Kamer ieder jaar ontvangt, dat commerciële binnendringsoftware aangeschaft bij een externe ontwikkelaar wordt gebruikt bij de inzet van de bevoegdheid van artikelen 126nba, 126uba en 126zpa.
De AIVD en de MIVD mogen onder strikte wettelijke voorwaarden bijzondere bevoegdheden inzetten ter bescherming van de nationale veiligheid. Deze bevoegdheden zijn in Nederland aan voorwaarden verbonden, die zijn vastgelegd in de Wiv 2017. Voor wat betreft de inlichtingen- en veiligheidsdiensten houden zowel de Toetsingscommissie Inzet Bevoegdheden (TIB) als de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) toezicht op de juiste toepassing van die wet. In het openbaar kunnen de diensten geen uitspraken doen over de inzet van bijzondere bevoegdheden. De NCTV heeft nooit gebruik gemaakt van binnendringsoftware en zal dat ook in de toekomst niet doen.

Vraag 4
Hoeveel geld is in elk van de afgelopen jaren uitgegeven voor de aanschaf van spionagesoftware?

Antwoord 4
Het is, gezien de wettelijke zorgplicht van de AIVD en de MIVD voor afscherming van de modus operandi, niet mogelijk om openbaar inzicht te geven in uitgaven die verband houden met de inzet van bijzondere bevoegdheden. Hetzelfde geldt voor de politie. Het is voor de afscherming van middelen en methodieken niet mogelijk om openbaar inzicht te geven in de uitgaven voor dit soort software.

Vraag 5
Kunt u aangeven waar de beloofde statistieken over hacksoftware gepubliceerd zijn en kunt u ze (nogmaals) naar de Kamer sturen, ook als het gebruik van hacksoftware nul is?

Antwoord 5
In de jaarverslagen van het Ministerie van Justitie en Veiligheid staat opgenomen hoe vaak commerciële binnendringsoftware is ingezet. Tevens doet de Inspectie Justitie en Veiligheid hiervan sinds de afgelopen drie jaar verslag inzake het toezicht op de binnendringbevoegdheid van de politie.

Vraag 6
Kunt u de jaarstatistieken over het gebruik uitsplitsen naar wie het gebruikt heeft?

Antwoord 6
Zie antwoorden bij de vragen 2 en 3.

Vraag 7
Kunt u de lijst van misdrijven geven waarvoor de hacksoftware is ingezet?

Antwoord 7
In opsporingsonderzoeken waarin binnendringsoftware is ingezet, was hoofdzakelijk sprake van een verdenking van een combinatie aan strafbare feiten.
Het betrof een combinatie van de volgende artikelen uit het wetboek van strafrecht, de Opiumwet (Ow), de Wet Wapens en munitie (Wwm), de wet op het financieel toezicht (Wft) en de Wet economische delicten (WED):

- art. 96 lid 2 (handelingen met het oogmerk tot voorbereiding/bevorderen van misdrijven tegen de veiligheid van de staat), 140 (deelneming aan een criminele organisatie), 140a (deelneming aan een terroristische organisatie), 157 (brandstichting/teweegbrengen ontploffing), 170 (vernieling van gebouwen), 177 (omkoping van ambtenaren), 225 (valsheid in geschriften), 227a (niet naar waarheid gegevens verstrekken), 287 (doodslag), 289 (moord), 310/311 (gekwalificeerde diefstal), 317 (afpersing), 326 (oplichting), 328ter (omkoping van anderen dan ambtenaren), 416/417 (gewoonte heling) en 420bis/420ter Sr (gewoonte witwassen).
- art. 2 jo. 10 Ow, 3 jo. 11 Ow en 10a Ow
- art. 26 en 55 Wwm
- art. 3a WFT jo. art. 1, 2 en 6 WED

Vraag 8
Is de hacksoftware alleen ingezet bij verdenking van zware misdrijven en/of terrorisme? Zo nee, wanneer is de hacksoftware nog meer inzet?

Antwoord 8
De bevoegdheid om heimelijk en van afstand binnen te dringen in een geautomatiseerd werk en onderzoekshandelingen te verrichten mag alleen worden ingezet bij ernstige misdrijven waarvoor voorlopige hechtenis mogelijk is en die gezien de aard of samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert. De AIVD en de MIVD doen onderzoek in het kader van de nationale veiligheid waaronder dreigingen voor de democratische rechtsorde. Om de Nederlandse rechtsstaat en democratische rechtsorde te beschermen is het van groot belang om zicht te krijgen en zicht te houden op de dreigingen om ons heen. Om personen waarvan een dreiging uitgaat voor de nationale veiligheid de pas af te snijden of in de gaten te houden, kan de inzet van bijzondere inlichtingenmiddelen (zoals tappen en hacken) essentieel zijn en soms de enige manier waarop de diensten informatie kunnen vergaren over activiteiten, capaciteiten en intenties.
Dat gebeurt altijd onder strikte wettelijke voorwaarden na bindende toetsing vooraf door de TIB en het onafhankelijke toezicht door de CTIVD.

Vraag 9
Is hacksoftware ook ingezet tegen advocaten, protestgroepen zonder terroristisch oogmerk en/of politieke groepen? Zo ja, kunt u uw antwoord dan heel precies toelichten?

Antwoord 9
De verantwoording van de inzet van bijzondere opsporingsbevoegdheden door opsporingsdiensten en het openbaar ministerie vindt plaats bij de behandeling van een strafzaak door de rechter. Om die reden kan geen inzage worden gegeven tegen welke specifieke verdachten in opsporingsonderzoeken de bevoegdheid ex art. 126nba Sv is ingezet.
Over de werkwijze van de inlichtingen- en veiligheidsdiensten worden in het openbaar geen uitspraken gedaan. In zijn algemeenheid hebben journalisten en advocaten binnen de Wiv 2017 extra bescherming. Inzet van bijzondere bevoegdheden op advocaten en journalisten kan namelijk alleen als de rechtbank Den Haag daarvoor toestemming heeft verleend. De jaarverslagen van AIVD en MIVD geven inzicht in de aandachtsgebieden van de beide diensten.
In het kader van opsporingsonderzoeken die door de politie worden uitgevoerd inzake een (mogelijke) strafrechtelijke vervolging door het openbaar ministerie kent de bijzondere opsporingsbevoegdheid van 126nba, 126uba en 126zpa geen uitzonderingen voor advocaten, protestgroepen zonder terroristisch oogmerk en/of politieke groepen. Het vereiste van een voorafgaande rechterlijke toetsing biedt de burger verdere bescherming tegen willekeurige inmenging door de overheid in de privésfeer. Daarnaast gelden voor de inzet van bijzondere opsporingsbevoegdheden ten aanzien van journalisten en advocaten aanvullende waarborgen[1].
Voordat wordt overgegaan tot inzet van de bevoegdheid ex artikel 126nba, 126uba, 126zpa vindt een uitgebreid toetsingstraject[2] plaats. Dit toetsingstraject geldt voor alle typen zaken waarvoor het is toegestaan om deze bevoegdheid in te zetten.
Wanneer een zaaksofficier voornemens is in een zaak de bevoegdheid ex artikel 126nba, 126uba, 126zpa Sv in te zetten wordt het voornemen voorgelegd aan de rechercheofficier van justitie en de hoofdofficier van justitie van het betrokken parket. Als beiden instemmen, wordt de voorgenomen toepassing ter goedkeuring voorgelegd aan het College van procureurs-generaal (het College). Dit gebeurt door tussenkomst van en na advisering door de Centrale Toetsingscommissie (CTC).
De CTC beoordeelt het verzoek aan de hand van (onder meer) de verdenking, de wet- en regelgeving, proportionaliteit, subsidiariteit, de kans van slagen van de inzet van het middel en eventuele gevoeligheden/risico's en stelt een advies op voor het College.
Het College beslist, met inachtneming van het advies van de CTC, of de bevoegdheid ex art. 126nba, 126uba, of 126zpa mag worden ingezet. Als het College toestemming heeft verleend, dient de zaaksofficier van justitie een vordering tot machtiging voor het geven van een bevel ex art. 126nba, 126uba, of 126zpa aan de rechter-commissaris te doen. Na machtiging door de rechtercommissaris beveelt de zaaksofficier van justitie de inzet.

Vraag 10
Kunt u een lijst geven van Nederlandse staatsburgers waarvan bij u bekend is dat hacksoftware is ingezet, maar deze software niet door de Nederlandse staat is ingezet? Deze lijst kan ofwel vertrouwelijk zijn, ofwel geanonimiseerd, zoals: advocaat, veroordeelde crimineel, militair, activist, journalist, etc.

Antwoord 10
Het kabinet beschikt niet over een dergelijke lijst waarop gegevens zouden staan van personen die zijn gehackt met het middel.
In november 2021 heeft Apple aangekondigd gebruikers die zijn geïnfecteerd met

[1] Aanwijzing toepassing opsporingsbevoegdheden en dwangmiddelen tegen advocaten (2011A003) en Aanwijzing strafvorderlijk optreden tegen journalisten (2020A002).
[2] Instructie voor de inzet van de bevoegdheid ex. Art. 126nba, 126uba, 126zpa en 126ffa Sv (2021l002) (om.nl)

Pegasus via een bericht te informeren. In het kader van de weerbaarheid bevorderende taak van de AIVD is eind november 2021 een cyberadvies aan de rijksoverheid gestuurd. Daarin werd rijksambtenaren die een dergelijke melding ontvingen geadviseerd dit via hun beveiligingsambtenaar bij de AIVD te melden. Het kabinet zal via de geëigende kanalen inzicht geven in het aantal meldingen.

Vraag 11
Kunt u – zo nodig vertrouwelijk – de screening van de leveranciers door de AIVD aan de Kamer doen toekomen?

Antwoord 11
De procedure zoals genoemd in het regeerakkoord van 2017 – dat leveranciers van hacksoftware die wordt ingekocht door opsporingsdiensten worden gescreend door de AIVD – wordt door de AIVD uitgevoerd als een naslagverzoek conform de F-taak in de Wiv 2017 onder artikel 8 lid 2f. Dit artikel betekent dat de AIVD in de eigen systemen naar een specifieke persoon of instantie een naslag kan doen op verzoek van anderen, conform de Regeling naslag Wiv 2017. Gezien de wettelijke geheimhoudingsplicht in de Wiv 2017 kan over specifieke naslagverzoeken in het openbaar geen mededelingen worden gedaan. De Kamer wordt hierover via de geëigende kanalen nader geïnformeerd.

Vraag 12
Wordt de in Nederland gebruikte hacksoftware ook verkocht aan dubieuze regimes? Hoe heeft de regering zich daarvan vergewist?

Antwoord 12
In het Regeerakkoord 2017–2021 is vastgelegd dat leveranciers van hacksoftware die wordt ingekocht door opsporingsdiensten niet mogen leveren aan dubieuze regimes. Zoals aangegeven in de beantwoording van Kamervragen gaat het om landen die zich schuldig maken aan ernstige schendingen van mensenrechten of internationaal humanitair recht.[3] Om deze reden voert de politie een toets uit voordat over wordt gegaan tot de aanschaf van binnendringsoftware. In deze toets wordt de leverancier gevraagd niet te hebben geleverd aan landen waartegen vanuit de EU of de VN restrictieve sancties bestaan en wordt gecontroleerd of in het land waar de leverancier is gevestigd een exportcontroleregime bestaat waar mensenrechten een onderdeel is in de beoordeling voor het verstrekken van een exportvergunning.[4]
De politie past dit beleid toe en eist van leveranciers een bevestiging dat niet aan zulke dubieuze regimes wordt geleverd. Aanvullend hierop wordt door de politie deze toets periodiek herhaald.

Vraag 13
Klopt het dat de wet computercriminaliteit III op 1 maart 2019 in werking getreden is en dat deze na 2 jaar geëvalueerd zou worden?

Antwoord 13
De Wet CCIII is inwerking getreden op 1 maart 2019. In het parlementaire debat heeft de toenmalige Minister toegezegd dat een eerste evaluatie van de Wet CCIII al na twee jaar plaatsvindt (in plaats van de gebruikelijke vijf jaar). Bij deze eerste evaluatie wordt gekeken naar één onderdeel van de wet, namelijk de bevoegdheid tot het heimelijk en op afstand binnendringen en onderzoek doen in een geautomatiseerd werk. Het tweede deel van de evaluatie zal zich richten op de gehele wet, inclusief de bevoegdheid tot binnendringen. De in twee delen opgedeelde evaluatie heeft als voordeel dat sommige thema's die gedurende de eerste evaluatietermijn nog onvoldoende diepgaand aan de orde kunnen komen, bijvoorbeeld omdat de looptijd van het onderzoek relatief kort is en als gevolg daarvan de hoeveelheid empirisch materiaal beperkt, nader kunnen worden onderzocht.

---

[3] Handelingen I 2017/18, 34, item 5, p. 29.
[4] Kamerstukken, TK, 2018/2019, Aanhangsel Handelingen, vergaderjaar 2018–2019, nr. 3537.

Vraag 14
Op welk moment is het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) met de evaluatie begonnen en heeft u al een concept van het rapport ontvangen? Zo ja, wanneer?

Antwoord 14
Het eerste deel van de evaluatie van de Wet CCIII is in 2020 aangevangen en zou eind 2021 zijn afgerond, maar heeft wegens de onvoorziene omstandigheden van de COVID-19 pandemie wat vertraging opgelopen.

Vraag 15
Wanneer krijgt u de definitieve versie van het evaluatierapport?

Antwoord 15
Naar verwachting zal het eerste deel van de evaluatie in de zomer 2022 worden afgerond en vlak na de zomer 2022 gepubliceerd.

Vraag 16
Kunt u deze vragen een voor een en binnen drie weken beantwoorden?

Antwoord 16
De vragen zijn zo snel mogelijk beantwoord.