Betreft: Reactie Tijdelijke wet cyberoperaties
Datum: 15 april 2022

Geachte ministers,

Via deze weg geven wij u graag enkele aandachtspunten mee inzake het wetsvoorstel Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma. In onze reactie gaan wij achtereenvolgens in op de reikwijdte van het wetsvoorstel, de inzet van de hackbevoegdheid in het kader van strategische operaties en het voorgestelde beroepsstelsel.

1. Reikwijdte wetsvoorstel
De aanleiding van het wetsvoorstel is dat Nederland en Nederlandse belangen in toenemende mate geconfronteerd worden met 'dreigingen in het cyberdomein'. Het wetsvoorstel is specifiek toegesneden op de dreiging die uitgaat van offensieve cyberprogramma's van staten. Door het verleggen van toezicht vooraf naar toezicht tijdens en achteraf bij de inzet van hackbevoegdheid en onderzoeksopdrachtgerichte interceptie wordt de diensten (deels) meer armslag gegeven.

In de afgelopen jaren is in rapporten van de AIVD, de MIVD en het NCSC de dreiging die uitgaat van statelijke actoren op het gebied van cybersecurity voor de nationale veiligheid al beschreven. Wij geven de suggestie mee in de memorie van toelichting bij het wetsvoorstel die straks vermoedelijk naar de Tweede Kamer wordt gestuurd, ook te verwijzen naar deze rapporten om context te geven aan de bedreiging waarmee Nederland zich ziet geconfronteerd.

Het wetsvoorstel roept ook de vraag op waarom juist de dreiging van criminele groeperingen op het gebied van cybersecurity voor de nationale veiligheid wordt uitgesloten van het voorstel. Vorig jaar stelde het NCSC in het 'Cyber Security Beeld Nederland' - dat mede met inbreng van de AIVD en de MIVD tot stand komt – dat *ransomware* (van criminele groeperingen) een bedreiging voor de nationale veiligheid vormt. Natuurlijk kan de wetgever kiezen voor een smaller wetsvoorstel dat zich richt op statelijke actoren (en proxy-organisaties die worden ingezet door statelijke actoren), maar het vraagstuk blijft open welke rol de Nederlandse inlichtingen- en veiligheidsdiensten spelen in het tegengaan van bedreigingen voor de nationale veiligheid die uitgaan van criminele groeperingen.

Helderheid over de reikwijdte van het wetsvoorstel en wat dus wel of niet binnen het wetsvoorstel valt, is met name van belang voor de toepassing van de wet in aanvragen voor de hackbevoegdheid en onderzoeksopdrachtgerichte interceptie die (ook) aan de TIB worden voorgelegd.

2. Strategische operaties
Hoewel de Evaluatiecommissie heeft aangedrongen op een nadere duiding van de strategische inzet van de hackbevoegdheid, lijkt het wetsvoorstel deze niet te geven. Het wetsvoorstel biedt daarmee mogelijk onvoldoende handvatten voor de TIB in hun beoordeling van de strategische inzet van de hackbevoegdheid. De TIB geeft dit ook zelf aan in haar reactie op het wetsvoorstel.

De informatiepositie die door een strategische inzet van de hackbevoegdheid kan worden verworven is onzes inziens echter bij uitstek geschikt om offensieve cyberprogramma's van staten proactief tegen te gaan. Daarmee kan op internationaal niveau worden aangesloten bij de toenemende implementatie van het concept *active cyber defence* door staten. Dit concept gaat uit van de gedachte dat een louter reactieve cybersecuritystrategie huidige mondiale cyberdreigingen niet voldoende het hoofd kan bieden. Wij stellen voor de dat de wetgever aansluit bij het concept van active cyber defence in de toelichting van het wetsvoorstel en het onderdeel dat ziet op strategische operaties beter uitlegt.

3. De beroepsprocedure
De beroepsprocedure van de ministers tegen een beslissing van de TIB en de CTIVD in het kader van het wetsvoorstel, betreft een aanzienlijke wijziging in het Wiv-stelsel. Het omvat een substantieel onderdeel van het wetsvoorstel en toch blijft veel onduidelijk over de wijze waarop de beroepsprocedure functioneert. In de memorie van toelichting staat dat de Awb niet van toepassing is. Dat heeft mogelijk

ook tot gevolg dat de procesregeling van de Afdeling bestuursrechtspraak van de Raad van State niet van toepassing is, met daarbij de belangrijke mogelijkheid tot inzet van deskundigen en *amicus curiae* (ook wel *friend of the court* genoemd, die onafhankelijk van de procespartijen advies kan uitbrengen). Dit verdient heroverweging van de wetgever. Het wiel hoeft immers niet op alle punten opnieuw uitgevonden te worden. Ook moet worden gekeken hoe in het buitenland een rol voor de rechtspraak wordt ingepast, zoals bij de *United States Foreign Intelligence Surveillance Court* (FISC). Dit vergt een flinke nadere uitwerking en mogelijk nader onderzoek.

Uit het rapport van de Evaluatiecommissie Wiv 2017 en de het rapport 'De wet dwingt, de tijd dringt, de praktijk wringt' van de Algemene Rekenkamer volgt de indringende conclusie dat *"de inlichtingenpositie van AIVD en MIVD onder druk staat"*. Dat is onder meer het gevolg van meningsverschillen over wetsinterpretatie tussen de toezichthouder(s) en de diensten. Als door een verschil van mening in de toepassing of over de interpretatie van de wet een (bijzondere) bevoegdheid niet kan worden ingezet, dan kan dat ten koste gaan van de verwerving van inlichtingen ter bescherming van de nationale veiligheid. Het is goed in de memorie van toelichting expliciet te maken dat dit deels de achtergrond vormt van de beroepsprocedure: interpretatievraagstukken van de wet kunnen via de rechter worden opgelost en de beroepsmogelijkheid vormt een mogelijkheid voor de diensten om een bindende beslissingen van de TIB en de CTIVD aan te vechten en toch inlichtingen te verzamelen of te bewaren.

Voor de rechtsvorming is het bijzonder belangrijk dat uitspraken van de Afdeling in beginsel openbaar zijn. Bronnen, *modus operandi* en een actueel kennisniveau van de diensten moeten uiteraard worden beschermd, maar het huidige uitgangspunt "alles geheim" is stuitend. De volledige geheimhouding van de uitspraken van de Afdeling is niet wenselijk en passend in onze democratische rechtsstaat. Geheime rechtsinterpretatie leidt tot een gebrek aan democratische controle, een gebrek aan controle door de media en de onmogelijkheid van deskundigen of de wetenschap commentaar te leveren op de rechtspraak. Gezien de dynamiek van het rechtsgebied en de snelle ontwikkelingen in het cyberdomein, zal de taak van de Afdeling naar verwachting betekenisvol zijn. De interpretatie van de wet en de daarin opgenomen begrippen dienen ten minste transparant te zijn. Wij verzoeken de wetgever dringend het uitgangspunt van geheime vonnissen te heroverwegen.

Tot slot

Het onderliggende wetsvoorstel is tijdelijk. In de tussentijd wordt ook gewerkt aan een grotere wetswijziging ten aanzien van de Wet op de inlichtingen- en veiligheidsdiensten 2017. Wij bevelen aan deze wet door een onafhankelijke commissie tussentijds (bijvoorbeeld één jaar na inwerkingtreding) te evalueren. Dat is belangrijk, omdat het wetsvoorstel aanzienlijke wijzigingen voor het toezicht met zich meebrengt en klaarblijkelijk belangrijk is voor het bijzondere en relatief nieuwe domein van cybersecurity en nationale veiligheid. De bevindingen van een grotere evaluatie leiden dan tot input voor de grotere wetswijziging.

Hoogachtend,

Prof. mr. dr. Jan-Jaap Oerlemans
Bijzonder hoogleraar Inlichtingen en Recht, Universiteit Utrecht

Mr. Sophie Harleman
Promovenda Inlichtingen en Recht, Universiteit Utrecht