Betreft: **Notitie t.b.v. rondetafelgesprek over de Tijdelijke wet cyberoperaties**
Datum: **23 maart 2023**

Geachte leden van de Tweede Kamer der Staten-Generaal,

Het digitale domein biedt landen die met elkaar concurreren of met elkaar op gespannen voet staan allerlei mogelijkheid om elkaar te ondermijnen, economisch te verzwakken (via digitale spionage of sabotage), te destabiliseren (door via nepnieuws onrust te stoken of verkiezingen te beïnvloeden) of zelfs aan te vallen (zoals bij Stuxnet in Iran). In het digitale domein kunnen deze vormen van agressie voor een groot deel onder de radar blijven. Het kan er daarom stevig aan toe gaan. Omdat er geen sprake is van een oorlogstoestand heeft de krijgsmacht in principe geen rol. De inlichtingen- en veiligheidsdiensten hebben daarentegen wel een rol in dit internationale digitale spanningsveld. De diensthoofden van de AIVD en MIVD hebben recent zowel in besloten kring als in het openbaar op de alarmknop gedrukt: zij kunnen de nationale veiligheid onvoldoende beschermen met het huidige wettelijke kader. Een dergelijk signaal behoort serieus te worden genomen; de op het spel staande belangen zijn nu eenmaal groot.

Onlangs is besloten dat het bedrijf ASML niet de modernste lithografiemachines (EUV en ook DUV) aan China mag leveren. De reactie van China laat zich raden: het gaat de kennis zelf halen. Recent stelde ook ASML-topman Peter Wennink dat hij verwacht "dat China de maatregelen aangrijpt om nog harder te werken aan een eigen chipmachine en mogelijk te proberen ASML's technologie te stelen" (*NRC Handelsblad*, 10 maart 2023). Het is goed voorstelbaar dat digitale spionage om de modernste lithografiekennis te verwerven nu een van de hoogste inlichtingenprioriteiten van China wordt. De vraag is dan vooral: gaan we de diensten die ons tegen dergelijke digitale aanvallen moeten beschermen passende bevoegdheden onthouden?

De Tijdelijke wet beoogt de diensten tijdelijk meer armslag te geven in operaties tegen landen met een op Nederland gericht offensief cyberprogramma. Dit voorstel loopt als het ware vooruit op de herziening van de WIV 2017. Op zichzelf is de gekozen figuur – een tijdelijk, afwijkend regime voor bepaalde operaties – bijzonder. Het toch al complexe juridisch kader voor de AIVD en de MIVD zal erdoor nog ingewikkelder worden. Bovendien bestaat het risico dat in concrete operaties onduidelijk is welke regels nu precies van toepassing zijn: geldt de WIV 2017 of de Tijdelijke wet? Zoals ook de Raad van State heeft geconstateerd, staat mede daarom niet op voorhand vast dat deze maatregelen leiden tot de gewenste toename van de operationele snelheid en wendbaarheid bij cyberoperaties.

Toch menen wij dat de voorgestelde aanpak verstandig is, zeker in het licht van de toenemende internationale agressie in het cyberdomein. De Evaluatiecommissie WIV 2017 (de commissie Jones-Bos) heeft een groot aantal aanbevelingen gedaan. Het implementeren daarvan vergt een omvangrijke wijziging van de WIV 2017. Dat wordt een lastig en tijdrovend wetgevingsproces. Tijd om dat af te wachten is er echter niet. De Russische invasie in Oekraïne en de toenemende Chinese assertiviteit op het wereldtoneel laten zien hoezeer de veiligheidssituatie verandert, juist op cyberterrein. Vanuit geopolitiek machtsdenken geredeneerd is het cruciaal dat de diensten goed geëquipeerd zijn om zicht te krijgen en te houden op andere statelijke actoren. Wij onderschrijven dan ook de noodzaak om hun cyberslagkracht zo snel mogelijk in lijn met het evaluatierapport te versterken.

Het wetsvoorstel zal ervoor zorgen dat de AIVD en de MIVD een aantal bevoegdheden daadwerkelijk of op effectievere wijze kunnen inzetten. Het gaat hier niet de introductie van geheel nieuwe bevoegdheden, maar om inhoudelijke verbeteringen en aanpassingen van de bestaande normering. Vrijwel alle voorstellen vinden steun bij de toezichthouders. Op uitdrukkelijke wens van de Tweede Kamer zijn de TIB en de CTIVD ook actief betrokken geweest bij de voorbereiding van dit voorstel. Zij achten het geheel 'toezichtbaar', mits zij extra personele capaciteit krijgen (zie de reacties op het conceptwetsvoorstel en *NRC Handelsblad*, 15 april 2022). Wij zijn het daar graag mee eens.

Een heikel punt bij de totstandkoming van de WIV 2017 was de zogeheten onderzoeksopdracht gerichte interceptie ('OOG'-interceptie). Eenmaal wettelijk verankerd, bleek de inzet ervan technisch en juridisch moeilijk te realiseren. Gegevens dienen immers 'zo gericht mogelijk' te worden verzameld. Om aan dat

vereiste te voldoen, zijn de diensten gaan 'snapshotten'. Het onderhavige voorstel introduceert daarvoor een zelfstandige grondslag. Formeel heet dit het 'ter verkenning intercepteren van gegevensstromen'. Men zou ook kunnen spreken over 'een proefinterceptie'. Zoiets heeft als functie om de potentiële inlichtingenwaarde van communicatieverkeer vast te stellen en om een latere aanvraag voor een gerichte interceptie te onderbouwen. Verkennen is uit de aard der zaak ongericht. Verzekerd moet dan ook zijn dat niet alle vergaarde data het inlichtingenproces ingaat, maar eerst wordt bestudeerd op relevantie voor een bepaald onderzoek; niet-relevante gegevens dienen zo snel mogelijk te worden vernietigd. Zulks is reeds geëxpliciteerd in artikel 6 van het voorstel en de daarbij behorende toelichting: snapshots mogen niet gebruikt worden in het daadwerkelijke inlichtingenonderzoek. Onder het nieuwe regime mag de CTIVD bij onrechtmatigheden direct ingrijpen. En volledigheidshalve: de TIB heeft dan reeds toestemming gegeven voor de desbetreffende interceptie. Al met al is volgens ons sprake van robuuste waarborgen tegen misbruik.

Dit wetsvoorstel verschuift het zwaartepunt van het toezicht op cyberoperaties in beperkte mate van de TIB naar de CTIVD. Zo sluit het toezicht beter aan bij de operationele dynamiek. Het stelt de diensten in staat om sneller mee te bewegen als aanvallers wisselen van digitale infrastructuur. Dat is nodig. Van een afschaling van de rechtsbescherming is onzes inziens geen sprake. Integendeel, onder de streep ontstaan er méér toezichtarrangementen en méér mogelijkheden om direct in operaties in te grijpen. De TIB blijft bestaan en blijft toetsen. Wat de TIB 'verliest', wint de CTIVD. De CTIVD wordt zelfs flink versterkt. Deze toezichthouder mag voortaan operaties stilleggen en het wissen van vergaarde gegevens afdwingen. Zulke interventiebevoegdheden zijn (letterlijk) ingrijpend en kunnen vergaande operationele consequenties hebben. Rechterlijke tegenmacht, in de vorm van een beroepsprocedure bij de Raad van State, is dan op haar plek. Temeer omdat er de afgelopen jaren al enkele (interpretatie)geschillen zijn ontstaan tussen de diensten en de toezichthouders, die nu niet kunnen worden opgelost.

De herschikking van het toezichtstelsel raakt een beperkt aantal operaties. Ook daarbij geldt: er is geen garantie dat de beoogde doelen worden behaald. Onder de huidige wet verloopt de samenwerking tussen de diensten en de toezichthouders soms nog stroef. Het kan zijn dat die stroefheid door de voorgestelde verdere formalisatie toeneemt. Maar het tegenovergestelde effect – het daadwerkelijk verhelpen van bestaande problemen in het toezichtstelsel – is evengoed denkbaar. Uiteindelijk zal het van de opstelling van de diensten én van de toezichthouders afhangen of dit nieuwe 'dynamisch toezicht' succesvol is.

Wij zien de Tijdelijke wet cyberoperaties vooral als een experimenteerwet. Op deze manier kan worden getest hoe nieuwe toezichtmechanismen in de praktijk uitpakken. Dat is nuttig. De verworven inzichten zullen ongetwijfeld waardevol zijn voor de beoogde herziening van de WIV 2017. Het is beter om eerst maatregelen te nemen met een beperkte tijdsduur en voor een beperkt aantal – op het buitenland gerichte – operaties, juist op het terrein waar het nu urgent is, alvorens het toezicht over de volle breedte te hervormen. Het doorvoeren van dit soort grote veranderingen kan immers leiden tot administratieve lastenverzwaringen. Indien de overgang van het oude naar het nieuwe (tijdelijke) regime niet soepel verloopt, kan dat nadelig uitpakken voor de slagkracht van de diensten en daarmee voor de nationale veiligheid. De moeizaam verlopen implementatie van de WIV 2017 heeft dat wel duidelijk gemaakt.

Fundamentele discussies over de diensten, over hun taken en bevoegdheden, en over het toezicht daarop zijn belangrijk, maar kunnen beter worden uitgesteld tot de herziening van de WIV 2017 zodat de diensten nu effectiever kunnen optreden tegen dreigingen in het cyberdomein. Wij adviseren dan ook om een pragmatisch besluit te nemen en in te stemmen met de Tijdelijke wet cyberoperaties.

Hoogachtend,

Prof. dr. Bart Jacobs
Hoogleraar Security, Privacy en Identity, Radboud Universiteit
Lid van de Kenniskring CTIVD en voormalig lid van de Evaluatiecommissie WIV 2017

Mr. drs. Rowin Jansen
Promovendus Algemene rechtswetenschap, Radboud Universiteit
Promotieonderzoek: Toezicht op de inlichtingen- en veiligheidsdiensten