Inbreng rondetafelgesprek Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma – 5 april 2023

Prof. mr. dr. J.J. Oerlemans, Bijzonder hoogleraar Inlichtingen en Recht bij de Universiteit Utrecht & Senioronderzoeker CTIVD

De dreiging

De Tijdelijke cyberwet houdt zich bezig met de dreiging die uitgaat van statelijke actoren met een offensief cyberprogramma. De dreiging die uitgaat van landen met een offensief cyberprogramma zou voor ons allemaal volstrekt helder moeten zijn. Maar voor de zekerheid ben ik het nog even voor u nagegaan.

In 2007 rapporteerde de AIVD voor het eerst in een jaarverslag over 'digitale inbreuken op vitale Nederlandse ICT-netwerken die vanuit China werden geregisseerd'. De dienst waarschuwde vanaf 2013 steevast – nu al 10 jaar op een rij - voor het gevaar van digitale spionage voor de nationale veiligheid van Nederland. Ook de MIVD waarschuwt voor digitale spionage uit landen als China, Iran en Rusland.

Het NCSC (het Nationaal Cyber Security Centrum) rapporteert sinds 2019 in het 'Cybersecuritybeeld Nederland' dat de *grootste* digitale dreiging op cybersecuritygebied van statelijke actoren komt. Als doelwitten van digitale spionage worden onder andere genoemd: Nederlandse ministeries, organisaties in vitale sectoren, telecomproviders, universiteiten, onderwijsinstellingen, onderzoeksinstituten, denktanks en biotechnologiebedrijven.

De problematiek

Ruim vóór de Oekraïnecrisis zijn de Commissie Inlichtingen en Veiligheid (ook wel Commissie "stiekem" genoemd) en leden van partijen in de Kamer geïnformeerd over de problemen die zich bij de AIVD en de MIVD zich voordeden bij de uitoefening van cyberoperaties. De boodschap was dat de diensten het zicht dreigden te verliezen, omdat de AIVD en de MIVD operaties niet tijdig kunnen starten of ononderbroken kunnen voortzetten.

De problemen die de AIVD en de MIVD ervaren bij de uitoefening van cyberoperaties - en ik citeer uit stukken van een Woo-verzoek over de Tijdelijke wet – *"zijn het gevolg van de toetsing van de rechtmatigheid van toestemmingsverzoeken van de verantwoordelijke ministers door de Toetsingscommissie Inzet Bevoegdheden (TIB)"*.

Destijds, alweer 1,5 jaar geleden, werd onderzocht of vanwege de ervaren urgentie een *spoedwet* mogelijk is, maar op een gegeven moment werd besloten tot een normaal wetstraject waarin ook de TIB en de CTIVD zijn geconsulteerd.

Het wetsvoorstel

In feite zien alle voorstellen in het wetsvoorstel die tot meer armslag voor diensten moeten leiden, op het aanpassen en verleggen van de toets vooraf door de TIB naar toezicht tijdens de uitvoering naar de CTIVD. Die aanpassingen zien op de uitoefening van de bijzondere bevoegdheden van hackbevoegdheid en bulkinterceptie, omdat deze bevoegdheden in het bijzonder belangrijk zijn bij het verzamelen van inlichtingen over offensieve cyberoperaties van statelijke actoren. Daar komt op die aanpassingen bindend toezicht bij de CTIVD voor in de plaats.

De precieze wijzigingen ten aanzien van de hackbevoegdheid en bulkinterceptie zijn te veel en te gedetailleerd om allemaal te bespreken, maar de memorie van toelichting maakt duidelijk hoe het

wetsvoorstel voor de problemen tot een oplossing kan bieden. Ik heb die wijzigingen bijvoorbeeld in een blogartikel op een rijtje gezet en mijn promovenda Sophie Harleman heeft deze uitvoerig beschreven in een artikel in het Nederlands Juristenblad van afgelopen december 2022. Haar conclusie is dat het voorstel een goede balans kan opleveren tussen voldoende slagkracht voor de diensten en voldoende waarborgen voor de bescherming van fundamentele rechten. Daar sluit ik mij bij aan.

Bulkinterceptie

De bepalingen over bulkinterceptie - formeel 'onderzoeksopdrachtgerichte interceptie' genoemd – licht ik uit, omdat het een controversiële bevoegdheid is. Het voorstel in de Tijdelijke wet zou volgens de memorie van toelichting een oplossing moeten bieden voor 'de verschillende zienswijzen van de Ministers en de TIB over de toepassing van het gerichtheidscriterium bij OOG-interceptie'. Ik wil hierover duidelijk maken dat we denk ik moeten accepteren en inzien dat bulkinterceptie inherent ongericht van aard is. De CTIVD heeft dit in januari 2022 ook bevestigd in een toezichtrapport over bulkinterceptie. De inherente ongerichtheid van bulkinterceptie staat ook in de internationale arena buiten kijf.

Dit wetsvoorstel doet meer recht aan waarvoor bulkinterceptie voor bedoeld is. Bij gerichte interceptie tap je bijvoorbeeld op basis van een telefoonnummer of IP-adres netwerkverkeer af. Bij bulkinterceptie tap je als het ware in één keer veel meer netwerkverkeer af en analyseer je daarna welk netwerkverkeer relevant is voor de uitvoering van een onderzoeksopdracht. In de context van digitale spionage gaat het dan bijvoorbeeld om het in kaart brengen van de digitale infrastructuur waar een Chinese inlichtingendienst voor digitale spionage van gebruik maakt. Het is een belangrijke taak van inlichtingen- en veiligheidsdiensten om te *ontdekken* waar de dreiging vandaan komt en niet alleen informatie te verzamelen op basis van reeds bekende indicatoren van bekende targets. Door meer ruimte te geven aan het verkennen van de communicatiestromen waarop je later bulkinterceptie op inzet, kunnen de diensten effectiever werken. Daar moeten voldoende waarborgen tegenover staan en dit wordt goed geregeld in het wetsvoorstel.

Kortom, de aanleiding en de problematiek van het wetsvoorstel zijn duidelijk. Mijns inziens vergroot deze wet de mogelijkheden om inlichtingen te vergaren over statelijke actoren met offensieve cyberprogramma's. Het biedt daarbij als tegenwicht belangrijke waarborgen in het toezicht. Ik ben om deze redenen een voorstander van deze wet. Wel raad ik aan de Tijdelijke cyberwet tussentijds te evalueren, zodat hieruit lessen kunnen worden getrokken voor de grote wijziging van de Wiv 2017.

Ook cyber*criminaliteit* kan de nationale veiligheid bedreigen!

Ten slotte merk ik op dat de reikwijdte van dit wetsvoorstel beperkt is. Naast mijn onderzoek naar nationale veiligheid en de Wiv en mijn werkzaamheden als onderzoeker bij de CTIVD, houd ik mij al meer dan 10 jaar bezig met onderzoek naar cybercriminaliteit. De belangrijkste trend in die 10 jaar zijn wat mij betreft de ernstige gevolgen die cybercriminaliteit met zich mee kan brengen.

Terecht merkt het NCSC al een aantal jaar op dat cybercriminaliteit, zoals ransomware, de nationale veiligheid kan bedreigen. Illustratief zijn de aanvallen die we in de afgelopen jaren hebben gezien in de haven van Rotterdam, ziekenhuizen en hele gemeenten in Nederland. Een adequate reactie van de overheid daarop blijft uit. Het is ook onduidelijk in hoeverre de AIVD en de MIVD actief inlichtingen vergaren over deze dreiging.

U kan als Tweede Kamer dit probleem aankaarten en de wens uitspreken dat de diensten hierover inlichtingen vergaren om de nationale veiligheid te beschermen. De Tijdelijke cyberwet vormt een mooie aanleiding om door te pakken op cybersecurity en de nationale veiligheid beter te beschermen.