



Wet voor de bescherming van de nationale veiligheid door de inlichtingen- en veiligheidsdiensten

Dreigingen voor onze nationale veiligheid nemen toe en zijn complexer. De regering heeft als hoofdtaak om de veiligheid van haar burgers te beschermen. Tegen dreigingen van buitenaf en binnenuit. De Wet bescherming nationale veiligheid (Wbmv) biedt de AIVD en MIVD meer slagkracht en wendbaarheid om Nederland en zijn bondgenoten veilig te houden.



De Wbmv



Dreiging



Militaire of oorlogsdreiging

Een militair conflict is niet langer ondenkbaar; dreigingen naderen de grenzen van Europa. Ook lijken tegenstanders vitale sectoren, zoals onze energievoorziening, te willen verstoren.

Ontregeling en economische veiligheid

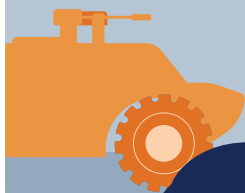
Landen zoals Rusland en China gebruiken een *whole of society* aanpak. Van sociale media tot spionnen, van maatschappelijke organisaties tot hackers: alle middelen worden ingezet om onze samenleving te ontregelen.

Spionage en digitale aanvallen

Technologie zoals AI maakt het voor tegenstanders makkelijker om cyberaanvallen te automatiseren en op grote schaal uit te voeren, ongeacht geografische locatie.

Terroristische dreiging

Jihadistisch terrorisme blijft aanwezig; een jongere, online radicaliserende generatie manifesteert zich. De oorlog rond Iran vergroot de aanslagdreiging, het dreigingsniveau staat op 4 (substantieel).



Het dreigingsniveau in Nederland is substantieel.

Pijlers

1 Dreigingsgericht werken

Onze inlichtingen- en veiligheidsdiensten hebben een goed beeld van de landen en organisaties die de Nederlandse samenleving bedreigen. Denk bijvoorbeeld aan de Russische geheime diensten, Chinese hackers en terroristische organisaties als IS.

De nieuwe wet biedt de mogelijkheid om sneller onderzoek te doen naar dit soort tegenstanders. Deze versoepeling geldt niet voor onderzoek naar bijvoorbeeld binnenlands extremisme, daarvoor gelden andere waarborgen.

Organisaties die zijn aangewezen als buitenlandse militaire of andere evidente dreigingen vallen onder het opponentenregime. Eenmaal aangewezen als opponent is er geen externe rechtmatigheidstoets meer nodig voor de afzonderlijk inzet van enkele bijzondere bevoegdheden. Denk aan het aftappen van telefoon- en internetverkeer. Uitzonderingen zijn bulkinterceptie, DNA-afname en het binnentreden van woningen. Daarvoor is wel altijd een voorafgaande externe toets nodig. Ook de inzet op bijzondere categorieën personen, zoals advocaten en journalisten, zijn uitgezonderd.

Ook wordt het staatsnoodrecht geïntroduceerd: dat geeft de overheid tijdens een gewapend conflict extra bevoegdheden om normale procedures en waarborgen tijdelijk buiten werking te stellen.



Opponentenregime:

- De ministers wijzen organisaties aan die werken vanuit landen met een offensief programma richting Nederland en zijn bondgenoten of die op de EU-sanctielijst tegen terrorisme staan.
- Organisaties als de FSB, IS of een vijandige krijgsmacht kunnen worden aangewezen als 'evidente dreiging'.
- Op het aanwijzen van organisaties als dreiging geldt een rechtmatigheidstoets. Op het aanwijzen van personen als onderdeel van die organisatie geldt bindend toezicht.
- De drie toetsingsnormen blijven gelden:
 - > **Noodzakelijkheid:** is de inzet van deze bevoegdheid nodig om het onderzoeksdoel te bereiken?
 - > **Proportionaliteit:** staat de inbreuk op bijvoorbeeld privacy in verhouding tot het belang dat de inzet van de bevoegdheid voor het onderzoek heeft?
 - > **Subsidiariteit:** is er geen lichter middel beschikbaar waarmee hetzelfde doel kan worden bereikt?

2 Samenwerking verbeteren

Dreigingen stoppen niet bij landsgrenzen of binnen sectoren. In de nieuwe wet wordt de samenwerking met medeoverheden, bedrijven, kennisinstellingen, en met buitenlandse inlichtingen- en veiligheidsdiensten versterkt. Ook komt er een uitbreiding van de verstrekingsplicht voor online platforms en financiële instellingen om gegevens aan te leveren bij de AIVD en de MIVD.

Vanwege de hoge, directe oorlogsdreiging, is een betere samenwerking met de krijgsmacht noodzakelijk. Daarom worden de volgende maatregelen opgenomen in de nieuwe wet:

- Diensten en de krijgsmacht kunnen straks makkelijker en sneller gegevens delen. Ook ruwe en operationele gegevens in plaats van alleen verwerkte gegevens.
- De MIVD en de krijgsmacht kunnen elkaar over en weer ondersteunen met technische apparatuur en gespecialiseerd personeel.
- Ook wordt het staatsnoodrecht geïntroduceerd: dat geeft de overheid tijdens een gewapend conflict extra bevoegdheden om normale procedures en waarborgen tijdelijk buiten werking te stellen.



Pijlers

3 Zorgvuldig omgaan met gegevens

Bulkgegevens zijn een verzameling persoonsgegevens die betrekking hebben op een zeer groot aantal personen. Het merendeel van deze personen zijn geen onderwerp van onderzoek van een dienst en zal dat ook niet worden. Met deze grote sets aan gegevens, zoals kentekenregisters of bankgegevens, kunnen koppelingen gemaakt worden tussen verschillende type gegevens die het ontbrekende puzzelstukje voor een onderzoek van de dienst kan zijn. Zo kan bijvoorbeeld een telefoonnummer aan een mailadres worden gekoppeld, of een bankrekening aan een woonlocatie. Het gebruik van (bulk)gegevens is daarom essentieel voor de diensten.

Om de privacy van burgers te waarborgen is het belangrijk dat zorgvuldig met die gegevens wordt omgegaan door de diensten. In de nieuwe Wiv zijn de regels daarvoor toegevoegd. Om bulkgegevens te mogen gebruiken zijn drie zaken belangrijk: de privacy gevoeligheid van de gegevens, of de diensten er logischerwijs over kunnen beschikken en voor welk doel de gegevens gebruikt worden. Dit heeft invloed op welke medewerkers toegang hebben tot en hoe lang die gegevens bewaard mogen worden.

Er zijn verschillende waarborgen voor drie categorieën bulkgegevens. In principe vallen bulkgegevens in de standaard categorie. De bewaartermijn voor deze gegevens is drie jaar en kan worden verlengd met steeds drie jaar. Op de noodzaak om te verlengen is bindend toezicht. Wanneer het logischerwijs te verwachten valt dat de diensten over de bulkgegevens beschikken, zoals het KvK-register, mogen de diensten de gegevens bewaren zolang het nodig is. Op het juiste gebruik van deze gegevens door de diensten is bindend toezicht.

Gegevens die de diensten niet meer nodig hebben worden vernietigd.

Als de bulkgegevens via bulkinterceptie verkregen zijn, gelden zij als bijzondere categorie. Omdat hierbij de potentiële inbreuk op de privacy van mensen het grootst is, gelden de grootste waarborgen: een eenmalige bewaartermijn van drie jaar en een bindende toets wanneer de diensten die gegevens willen raadplegen.

Daarnaast legt de nieuwe wet vast hoe de diensten AI en algoritmen mogen gebruiken. Dit is op zo'n manier omschreven dat niet iedere technologische ontwikkeling die nog gaat komen een wetswijziging vereist. Om goed voorbereid te zijn op de gevolgen van AI voor de Nederlandse veiligheid is het belangrijk dat de diensten AI begrijpen en het met de juiste waarborgen kunnen inzetten. Wanneer het gebruik van AI veel risico met zich meebrengt, moet de minister toestemming geven. Ook is een betrouwbaarheidsonderzoek en een gebruiksinstructie verplicht. De inzet van AI is altijd een hulpmiddel ter ondersteuning van het onderzoek. Mensen zijn en blijven altijd verantwoordelijk voor de uitkomsten.



4 Nieuwe wet met nieuwe waarborgen

Het werk van de diensten wordt sneller en complexer, en het huidige stelsel van toezicht sluit daar onvoldoende op aan. Daarom gaan de TIB en de CTIVD op in één nieuwe organisatie, het College van Toetsing en Toezicht (CTT), dat makkelijker samenwerkt en een stevigere organisatie wordt.

Het CTT toets enerzijds bevoegdheden vooraf op rechtmatigheid en anderszijds houdt zij toezicht op al het werk van de diensten. In bepaalde risicovolle gevallen is dat bindend. Ook kunnen burgers met klachten over het werk van de diensten bij het CTT terecht.

Bij een verschil van inzicht tussen dienst en CTT over een bindend oordeel velt de rechter het eindoordeel. Voor de inzet van operationele bevoegdheden, zoals tappen of volgen, tegen journalisten of advocaten moet de rechter vooraf toestemming geven. Dit word uitgebreid naar parlementariërs en leden van de CTT.

Grondrechten blijven gewaarborgd en de wet blijft voldoen aan het Europees Verdrag voor de Rechten van de Mens (EVRM). Ook het interne toezicht bij de diensten wordt versterkt.

Het werk van de diensten wordt sneller en complexer. Het toezicht beweegt mee.

