

Hoofdpijnen omgang Defensie met vertrouwelijkheid van informatie

Defensie draagt de verantwoordelijkheid het parlement conform artikel 68 te informeren en de Kamers in staat te stellen hun controlerende functie te laten uitvoeren. In het kader van de verslechterde veiligheidssituatie en de noodzaak om gevoelige informatie te beschermen verstrekt het ministerie van Defensie bepaalde informatie uitsluitend vertrouwelijk aan de Tweede Kamer. Zoals wanneer openbaarmaking de nationale veiligheid, operationele inzetbaarheid van de krijgsmacht, internationale samenwerking of de veiligheid van militairen en andere betrokkenen kan schaden.

Belangenweging

Veiligheid van de Staat	Relevant wanneer openbaarmaking van informatie de nationale veiligheid schendt. Dit kan gaan om beveiliging van gegevens met betrekking tot vitale sectoren waarvan de geheimhouding noodzakelijk is om de veiligheid van de staat te garanderen. Hieronder valt ook informatie met betrekking tot het tegengaan van terrorisme en militaire geheimen.
Internationale en diplomatieke belangen	De inhoud van vertrouwelijke gesprekken en onderhandelingen met vertegenwoordigers van andere landen en internationale organisaties, ook als dit de Nederlandse Staat niet direct schaadt, maar een andere Staat of organisatie wel. Informatie over andere landen valt hier ook vaak onder (bijvoorbeeld onderhandelingsposities en standpunten die niet openbaar zijn).
Vertrouwelijk verstrekte bedrijfsinformatie	Het openbaar verstrekken van bedrijfsgegevens die vertrouwelijk horen te blijven kan schade opleveren voor het bedrijf in kwestie. Onder andere de reputatieschade die de Staat hiermee oploopt kan schadelijk zijn voor het belang van de Staat.
Financiële en economische belangen van de staat	Economische of financiële belangen van de overheid zelf. Bijvoorbeeld aanbestedingen, lopende onderhandelingen of in relatie met een ander bestuursorgaan.

Vertrouwelijke informatie categorieën

Informatie uit plannen die inzicht geeft in de toekomstige krijgsmacht

- Details en getallen uit plannen, budgetten, investeringen, en prognoses.
- Details en getallen over materieel, operationele IT (wapensystemen), vastgoed en innovatie.

Informatie die inzicht geeft in de inzetbaarheid van de krijgsmacht

- Details en getallen over personele gereedheid, zoals capaciteit (instroom, uitstroom), specifieke kwaliteiten, vaardigheden of kennisgebieden.
Bijvoorbeeld informatie over de samenstelling (beroeps, reservisten, burgers) van defensieonderdelen of over tekorten van specialisten binnen de krijgsmacht.
- Details en getallen over materiele gereedheid, zowel militair materieel als operationele IT, zoals typen, specificaties, aantallen (verbruik, bestellingen en voorraad) en kwaliteit (gebreken, modificaties, onderhoud).

Bijvoorbeeld informatie over normen en tekorten BKI (Beleidskader Inzetvoorraden) of details over de materiele gereedheid per wapensysteem.

- Details en getallen over geoefendheid (oefeningen in Nederland en internationaal), zoals aantallen militairen, reservisten, betrokken burgers, specifiek materieel, specifieke ervaringen.

Informatie over operationele inzet

- Operationele details over inzet.
Bijvoorbeeld, informatie over voorraadniveaus, reactietijden van reserves, hoeveel reserves we hebben, posities van commandoposten en hoofdwapensystemen (zoals lanceerinstallaties, tanks, vliegtuigen, schepen) en dergelijke.
- Details over knelpunten of kwetsbaarheden die zich tijdens inzet hebben gemanifesteerd of zijn gerapporteerd, niet van de Nederlandse krijgsmacht noch van bondgenoten of de samenwerking daarmee (interoperabiliteit).
Bijvoorbeeld, informatie over tekorten (aan munitie of delen van wapensystemen), tekortkomingen in verbindingen of C2 systemen, niet beschikbaarheid van systemen e.d.

Operationele informatie van derden dan wel inlichtingendiensten

- Defensie is geen eigenaar van informatie van verdragsorganisaties (NAVO, EU, VN e.d.), bondgenoten en (commerciële) partners. Hiervoor zijn we gehouden aan de relevante wetgeving, verdragen, contracten en andere afspraken. Defensie maakt dus nooit operationele informatie van andere organisaties openbaar.
- Een bijzondere categorie informatie zijn inlichtingen die door de MIVD zijn verstrekt aan de defensie-organisatie. Ook al is de MIVD onderdeel van defensie, geldt ook hiervoor dat de MIVD daarvan eigenaar is en blijft van deze informatie. MIVD-informatie mag nooit openbaar worden gemaakt zonder toestemming van de MIVD.

Grondregels voor een sterke regie op het openbaar maken van informatie

1. Denk altijd na over het openbaar maken van informatie. Handel nooit op basis van routines of afwegingen en besluiten uit het verleden. Ontwikkelingen in de omgeving kunnen vereisen dat informatie meer geheimgehouden (of toch openbaar gemaakt) moet worden.
2. Dat informatie eerder al openbaar is gemaakt, is niet altijd een argument dat het weer kan. Opnieuw openbaar maken is altijd een bevestiging van al openbaar gemaakte informatie en vaak ook een verrijking hiervan (detaillering, actualisering, beoordeling, etc.).
3. Bescherm details bij het openbaar maken van informatie. Verstrek geen details over personen en personeel, materieel en IT, vastgoed, locaties, belangrijke gebeurtenissen en over operationele plannen, gereedheid en inzet. Als dat toch nodig is, dan neem je maatregelen om de verspreiding te beperken.
4. Zorg voor de juiste rubricering van informatie en handel daarnaar. Besef ook dat je zelfs ongerubriceerde informatie alleen op 'need-to-know' basis mag delen. Dit betekent dat ook deze informatie niet geschikt is om publiekelijk, bijvoorbeeld op internet, te publiceren.
5. Bespreek afwegingen over openbaarmaking en geheimhouding van informatie. Je collega's, leidinggevende en specialisten, zoals de beveiligingsfunctionaris, zijn er ook om hierbij te helpen. Bespreekbaar maken helpt ook om het bewustzijn hierover actueel te houden.