

Hernieuwd veiligheidsdenken: dronewaarnemingen in Nederland

L.M.H. Polderman-Borst, LL.M., kapitein der Koninklijke Marechaussee, en P.R. Wolf MA EMSD, kolonel der Koninklijke Marechaussee*

Europa bevindt zich momenteel in de grey zone, de fase tussen vrede en oorlog. In deze competitiefase nemen hybride tactieken voor spionage, sabotage en beïnvloedingsoperaties, die de nationale veiligheid in Nederland kunnen bedreigen, toe. Commerciële en/of andere kleine drones hebben recentelijk het dagelijks leven beïnvloed. De groeiende media-aandacht voor de droneactiviteiten leidt tot maatschappelijke bezorgdheid en verhoogt de perceptie van onveiligheid. De huidige competitiefase vraagt om herziening van het veiligheidsdenken. De benodigde nationale capaciteit kan via Artikel 3 van het NAVO-verdrag worden uitgebreid en internationale samenwerking geïntensiveerd. Samenwerking met (inter)nationale partners is essentieel voor het tijdig herkennen van hybride dreigingen en het nemen van passende maatregelen. De Koninklijke Marechaussee heeft vanuit de Politiewet een belangrijke rol in force protection ter bescherming van civiele- en militaire- overheidsterreinen en overheidsgebouwen en de burgerluchtvaart en in de opsporing van verdachten van spionage en sabotage via drones. Hierbij kan de KMar vanuit haar politietaak om legitieme bijstand van andere krijgsmachtdelen verzoeken voor bijvoorbeeld counterdrone-operaties.

* Liselotte Polderman is PhD Researcher bij de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie, sectie Irregular Warfare; Pascal de Wolf is Plaatsvervangend Directeur Operaties bij de Koninklijke Marechaussee.

1 C. Heil, 'Met luchtverdediging win je geen oorlog, maar zonder verlies je hem', DGLC. *Defensiemagazine*. 7 februari 2025, zie: https://magazines.defensie.nl/landmacht/2025/02/07_luchtverdediging.

2 In dit artikel beperken de auteurs zich tot de tactisch kleinere en commercieel verkrijgbare drones, ook bekend als 'Low, Slow, and Small flying objects to which the basic set up merely consists of an operator, a remote control, a c2 link and the aircraft or 'drone' itself', zie: A. Haider, 'A Comprehensive Approach to Counter Unmanned Aircraft Systems', *Joint Air Power Competence Centre* (2023) 11-13. Deze kleinere drones worden primair gemaakt voor informatieverzameling, surveillance en het verkennen van gebouwen en terreinen, zie: <https://www.jouav.com/blog/drone-types.html>.

3 S. Aurel, 'Hybrid threats and the law: Building legal resilience', *The European Center of Excellence on Countering Hybrid Threats* (2021) Research Report 3; S. Rietjens, 'Hybrid CoE Strategic Analysis 22. A Warning system for hybrid threats – is it possible?', *The European Centre of Excellence on Countering Hybrid Threats* (2020) 1-10.

In Nederland worden steeds vaker ongeïdentificeerde commerciële en andere kleine onbemande luchtvaartsystemen (hierna: drones) waargenomen in de nabijheid van militaire terreinen en overheidsgebouwen.¹ Waar deze dronewaarnemingen voor Nederland relatief nieuw zijn, is dit in Oost-Europese landen al langer dagelijkse realiteit. Zo hebben Estland, Letland, Litouwen en Finland al jarenlang te maken met uiteenlopende hybride dreigingen zoals spionage-, sabotage- en beïnvloedingsoperaties waarvoor ook tactische kleinere en/of commerciële drones worden gebruikt.² Voor deze landen zijn dergelijke activiteiten een terugkerend fenomeen dat steeds minder invloed heeft op de dagelijkse bedrijfsprocessen.³ Hybride dreigingen zijn een combinatie van militaire, politieke, economische en informatie-tactieken die op een veelzijdige manier worden



Oefening van een scenario waarin een aanslag op de metro is gepleegd met een drone

FOTO MCD, SJOERD HILCKMANN

ingezet om met minimale kosten en risico's macht en invloed in de regio uit te oefenen.⁴ Attributie van deze hybride activiteiten wordt bemoeilijkt door de dubbelzinnigheid die van de intentie van de dreigingen uitgaat en de verhulling van de (in)directe opdrachtgever.⁵ Met de Baltische staten heeft ook Polen herhaaldelijk melding gemaakt van drone-waarnemingen en sabotageacties gericht op onder andere spoorweginfrastructuur.⁶ Terwijl drone-activiteiten met een (semi)ontwrichtend karakter eerder in Oost-Europa plaatsvonden, verschenen deze in 2023 ook in West-Europa. In 2023 werden voor het eerst drones gesignaleerd nabij energie-installaties voor de kust van Noorwegen.⁷ In 2025 kwamen daar nieuwe waarnemingen in Noorwegen en tegelijkertijd Denemarken bij.⁸ Sinds de zomer van 2025 zijn er ook dronewaarnemingen in België, Duitsland en Nederland nabij civiele- en militaire- overheidsterreinen en overheidsgebouwen.⁹ In Nederland zijn er verschillende waarnemingen gedaan boven civiele- en militaire- overheidsterreinen en overheidsgebouwen die invloed hadden op de

- 4 P. Cullen, 'Hybrid threats as a new wicked problem for early warning', Hybrid Centre of Excellence Strategic Analysis 8. Hybrid Centre of Excellence in Countering Hybrid Threats (2018) 1-8.
- 5 Algemene Inlichtingen- en Veiligheidsdienst, Militaire Inlichtingen- en Veiligheidsdienst en Nationaal Coördinator Terrorisme en Veiligheid, *Dreigingsbeeld statelijke actoren 2* (2022) 1-22.
- 6 J. Frankhuisen, 'Drones vliegen boven Polen en sabotage spoorweg', *NOS*, 10 september 2025, zie: <https://nos.nl/collectie/13965/artikel/2581960-russische-drones-boven-polen-dit-levert-rusland-zeeen-aan-informatie-op>; 'Polen zet na sabotage spoor 10.000 militairen in om infrastructuur te beschermen', *NOS*, 19 november 2025, zie: <https://nos.nl/artikel/2591136-polen-zet-na-sabotage-spoor-10-000-militairen-in-om-infrastructuur-te-beschermen>.
- 7 Dronewaarnemingen voor de kust van Stavanger, *NOS*, 23 oktober 2025, zie: <https://tpo.nl/2022/10/23/noorwegen-vreest-russische-drone-aanvallen-op-gas-en-olieplatforms/>
- 8 O. Soceur, 'Grey Zone Maritime Threats in European Waters Demand New Security Challenges', *3GimBals* (2025) zie: <https://3gimbals.com/insights/grey-zone-maritime-threats-in-european-waters-demand-new-security-strategies/>; NCTV, *Dreigingsbeeld Statische Actoren. Aanhoudende dreigingen in tijden van groeiende onzekerheid*, Nationaal Coördinator Terrorisme en Veiligheid (2025) 1-53.
- 9 'Mediaberichten over dronewaarnemingen in de Belgische steden Doel en Luik', *NRC*, 10 november 2025, zie: <https://www.nrc.nl/nieuws/2025/11/10/drones-in-belgie-ontglipten-klasseke-bestrijdingstechnieken-a4912256>; 'Drones gezien bij Belgische kerncentrale Doel en luchthaven Luik', *NOS*, 9 november 2025, zie: <https://nos.nl/artikel/2589862-drones-gezien-bij-belgische-kerncentrale-doel-en-luchthaven-luik>; 'Dronewaarnemingen in Duitsland in de steden München en Berlijn', *NOS*, 4 oktober 2025, zie: <https://nos.nl/artikel/2585095-vliegverkeer-munchen-opnieuw-stilgelegd-na-melding-van-drones>; 'Vliegverkeer rond Berlijn verstoord vanwege drones', *NOS*, 1 november 2025, zie: <https://nos.nl/artikel/2588761-vliegverkeer-rond-berlijn-verstoord-vanwege-drones>.

De recente dronewaarnemingen in Nederland en andere Europese landen vinden plaats in een fase tussen oorlog en vrede: de zogeheten grey zone competition



dagelijkse bedrijfsvoering.¹⁰ Deze dronewaarnemingen krijgen veel aandacht in de media, wat leidt tot tal van (ongefundeerde) analyses op diverse (online) fora. De toegenomen media-belangstelling leidt tot groeiende maatschappelijke onrust, wat een sneeuwbaaleffect aan online content veroorzaakt, mede doordat populariteit van content de algoritmen van sociale media beïnvloedt.¹¹ Naarmate meer informatie over de dronewaarnemingen beschikbaar wordt, groeit ook de perceptie van onveiligheid onder de bevolking.

Vanuit militair en veiligheidsperspectief roepen de waarnemingen vragen op wie hiervoor

verantwoordelijk is en welke (onderliggende) doelstellingen worden nagestreefd. Dit leidt vervolgens tot de vraag wat dit betekent voor het nationale veiligheidsperspectief, zoals het handelingskader bij korte afstands-lucht-verdediging en de verdeling van rollen en verantwoordelijkheden, zowel binnen nationale kaders als via internationale samenwerkingsverbanden. Dit artikel beschrijft hoe drones kunnen worden ingezet als instrument binnen hybride operaties in *grey zone competition* en analyseert hoe de toenemende complexiteit en intensiteit van dergelijke activiteiten het nationale veiligheidsdenken beïnvloedt.

Grey zone competition en de beïnvloeding van het veiligheidsdenken

De recente dronewaarnemingen in Nederland en andere Europese landen vinden plaats in een fase tussen oorlog en vrede: de zogeheten *grey zone competition*. Deze fase is feitelijk een competitiefase die wordt gekenmerkt door toenemende geopolitieke spanningen en (in) directe statelijke dreigingen.¹² Drones worden als instrument in deze competitiefase ingezet, waarbij tegenstanders als Rusland gebruikmaken

10 'Mediaberichten over dronewaarnemingen in Volkel, Eindhoven en Maastricht', NOS, 22 november 2025, zie: <https://nos.nl/artikel/2591497-luchtmacht-heeft-wapens-ingezet-5-tot-10-drones-boven-vlieg-basis-volkel>; 'Vliegverkeer Eindhoven twee uur plat, Defensie neemt maatregelen tegen drones', NOS, 22 november 2025, zie: <https://nos.nl/artikel/2591558-vliegverkeer-eindhoven-twee-uur-plat-defensie-neemt-maatregelen-tegen-drones>; 'Vrijdag meerdere drones gespot boven Zuid-Limburg, politie zette helikopter in', NU.nl, 11 november 2025, zie: <https://www.nu.nl/binnenland/6375581/vrijdag-meerdere-drones-gespot-boven-zuid-limburg-politie-zette-helikopter-in.html>.

11 G. Ciampaglia e.a., 'How algorithmic popularity bias hinders or promotes quality', *Scientific Reports* (2018) 1-7; P. Vasterman, 'Media-HypeSelf-Reinforcing news waves. Journalistic Standards and the Construction of Social Problems', *European Journal of Communication* (2005) 1-10; 'Waarom risicovolle digitale trend vaak mainstream worden', *herautonline.nl*, zie: <https://www.herautonline.nl/nieuws/zakelijk-nieuws-landelijk/96976/waarom-risicovolle-digitale-trends-vaak-mainstream-worden>.

van provocerende strategieën. Om het gebruik van commerciële en/of andere kleine drones als hybride dreiging te doorzien, is het essentieel om ook het perspectief van de tegenstander te begrijpen.

Waar het Westen onder de NAVO-alliantie handelt volgens internationaal en nationaal recht, en in geval van het bereiken van de drempelwaarden van een gewapend conflict, collectieve verdediging via Artikel 5 van het NAVO-verdrag of Artikel 2(4) van het Handvest van de Verenigde Naties worden ingeroepen, kent Rusland dergelijke drempelwaarden niet. Vanuit Russisch perspectief wordt voornamelijk provocerend geopereerd binnen de manoeuvreerruimte die het Westen biedt.¹³ Deze ruimte ontstaat doordat Nederland en andere landen inconsistent acteren op (gecoördineerde) operaties, waardoor (meer) manoeuvreerruimte ontstaat.¹⁴ Het benutten van geboden en nieuw ontstane manoeuvreerruimte via de inzet van non-kinetische middelen is niet nieuw en staat bekend als *liminal manoeuvre*.¹⁵ Rusland past het sinds het pre-Sovjettijdperk toe met een stijl die maskirovka genoemd wordt.¹⁶

Rusland gebruikt maskirovka enerzijds om zijn tegenstanders in algemene zin te misleiden door operaties te verbergen en anderzijds het eigen handelen te maskeren, waarbij Moskou zich zwakker of sterker voordoet dan de werkelijkheid.¹⁷ Maskirovka is een paraplubegrip dat vele verschijningsvormen kent en vier principes omvat:

- een bepaalde vorm van wreedheid die wordt gebruikt om de tegenstander via gemanipuleerde ideeën en indrukken ertoe te bewegen onjuiste inschattingen van de situatie te maken;
- alle maskirovkapogingen moeten een bepaalde geloofwaardigheid bevatten die tegenstanders iets laat geloven wat in werkelijkheid niet zo is;
- herhaling van maskirovkapatronen moet worden vermeden, om voorspelbaarheid te voorkomen en
- het gebruik van maskirovka vindt continu in zowel oorlogs- als vreedstijd plaats.¹⁸ De terugkerende kernelementen van maskirovka zijn verhulling en bedrog.¹⁹

Rusland maskeert zijn ware intenties van specifieke operaties doordat de tegenstander zich blijft afvragen tegen welke (reële) dreiging hij zich moet wapenen en welke gelegitimeerde reactie vervolgens passend is. Tegelijkertijd zorgt de ambiguïteit rond de intenties van drone-activiteiten door mogelijk Rusland al voor een maatschappelijk gevoel van onveiligheid. Hoewel recente droneactiviteiten nog niet zijn geattribueerd aan Rusland is dit scenario, zoals eerder geschetst, wel voorstelbaar. Het gebruik van kostenefficiënte kleinere drones door Rusland²⁰ past ook in Moskou's narratief van afschrikking van tegenstanders zoals het Westen en voedt de oorlogseconomie.²¹ Bovendien gebruikt Moskou westerse beschuldigingen van droneactiviteiten voor zijn binnenlandse politiek om aan te tonen dat het Westen feitelijk een hybride oorlog voert tegen Rusland.²²

- 12 M. Azad, M. Haider en M. Sadiq, 'Understanding Gray Zone Warfare from multiple perspectives', *Journal of World Affairs* (2023) 1-23; H. Brands, 'Paradoxes of the Gray Zone', *SSRN* (2016) 1-13; C. Marsh, 'Maskirovka and the Grey Zone. The Utility of the Grey Zone Concept after Russia's Invasion of Ukraine', in: James Kiras en M. Kitzen (red.), *Into the Void. Special Operations Forces after the War on Terror* (Londen, Hurst and Company, 2024) (3) 57-73.
- 13 D. Kilcullen, *The Dragons and the Snakes. How the Rest learned to Fight the West* (Oxford, Oxford University Press, 2019) 100-120.
- 14 D. Kilcullen, *The Dragons and the Snakes. How the Rest learned to Fight the West*. (Oxford, Oxford University Press, 2019) 130-145.
- 15 M. Galeotti, 'Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?', *Small wars and insurgencies* (2016) (27) (2) 282-301.
- 16 M. Galeotti, 'Gangsters at war. Russia's use of organized crime as an instrument of statecraft', Research report, *Global Initiative against transnational organized crime* (2024) 1-62; M. Galeotti, '(Mis)Understanding Russia's two 'hybrid wars'', *Eurozine* (2018) 1-23.
- 17 H. Bouwmeester, *Krym Nash. An Analysis of Modern Russian Deception Warfare* (Utrecht, Utrecht University Repository 2020) 23-38.
- 18 Idem, 24.
- 19 C. Marsh, 'Maskirovka and the Grey Zone. The Utility of the Grey Zone Concept after Russia's Invasion of Ukraine', in: J. Kiras en M. Kitzen (red.), *Into the Void. Special Operations Forces after the War on Terror* (Londen, Hurst and Company, 2024) (3) 57-73.
- 20 Hoewel de auteurs zich bewust zijn van het gebruik van drones door verschillende (niet)statelijke actoren, beperken zij zich in deze bijdrage tot Rusland.
- 21 A. Prokopenko, 'Russia's Economic Gamble. The Hidden Costs of War-Driven Growth', *Carnegie Politica* (2024), 20 December 2024.
- 22 J. Godzimirski, 'Russian Strategic Communication Towards Europe. Goals, Means and Measures', in: H. Mölder e.a. (red.), *Russian Federation in Global Knowledge Warfare* (Cham, Springer Nature Switzerland, 2021) 51-78; H. Mölder, 'The war of Narratives. Putin's Challenge to International Security Governance in Ukraine', *Sõjateadlane (Estonian Journal of Military Studies)* (2016) (2) 88-113.

Om het gebruik van drones als hybride dreiging te doorzien, is het essentieel om het perspectief van de tegenstander te begrijpen

Russische strategie en het effect op de westerse samenleving

Rusland hanteert in zijn operaties een *zero-sum game*-benadering: elk verlies voor de tegenstander wordt gezien als winst en vice versa. Het ontplooiën van hybride tactieken zoals spionage, sabotage en beïnvloedingsoperaties (via sociale media) creëert maatschappelijke onrust.²³ Dit leidt ertoe dat westerse landen worden afgeleid door – in dit geval – dronewaarnemingen en daarmee de aandacht en mogelijk prioriteiten verschuiven. Hierin maakt het niet uit of de activiteiten een reële dreiging vormen, zolang de activiteiten als dreiging worden gepercipieerd is het doel van het verzwakken van de tegenstander en dus eigen gewin bereikt.²⁴ Het disruptieve effect op de dagelijkse bedrijfsvoering is hierin leidend; de middelen zijn daaraan ondergeschikt.

Bij veel van deze droneactiviteiten blijft het de vraag of er sprake is van een directe of indirecte statelijke dreiging. In de analyse lijkt een binaire interpretatie te worden gebruikt: ofwel het is een directe dreiging die onmiddellijke opschaling en anticipatie vereist, of niet. Ongeacht de reactie bereikt Rusland door de gecreëerde maatschappelijke onrust en verstoring van dagelijkse processen al één van zijn doelstellingen.²⁵ Of de drone-inzet daadwerkelijk een inbreuk vormt op de statelijke soevereiniteit of slechts een versturende situatie van dagelijkse activiteiten oplevert, is hierin ondergeschikt; de perceptie van onveiligheid heeft een disruptief en daardoor verzwakkend effect.

Ontwrichtend karakter en scenario's

Hoewel de maatschappelijke weerbaarheid in Nederland geleidelijk toeneemt, raken de dronewaarnemingen een gevoelige snaar en veroorzaken zij maatschappelijke onrust. Voor een lange tijd werden droneactiviteiten als *safety*-risico aangemerkt, bijvoorbeeld voor de vliegveiligheid. Recentelijk worden deze activiteiten steeds meer gelabeld als *security*-risico, waardoor autoriteiten als de NCTV meer in beeld komen. De media suggereren al snel dat een statelijke actor, mogelijk via een proxy, verantwoordelijk is voor deze drone-activiteiten.²⁶ Hoewel er aanwijzingen zijn dat de toename van dronewaarnemingen als hybride dreiging (door een statelijke actor) kan worden gezien, is het belangrijk om alternatieve scenario's niet uit te sluiten. Een te sterke focus op één scenario kan leiden tot hypersensitiviteit, een onevenredige inzet van capaciteit en mogelijk voorbarige escalatie, terwijl er ook andere verklaringen mogelijk zijn.

Er moet bijvoorbeeld nog steeds rekening worden gehouden met de mogelijkheid van een verdwaalde drone, die door een burger met bonafide intenties wordt bestuurd. Deze persoon kan puur uit interesse voor de locatie of door onwetendheid op het verkeerde moment op de verkeerde plek zijn.²⁷ Een ander scenario is dat een of meerdere personen, mogelijk gerekruteerd door online (statelijk geaffilieerde)

23 K. Metcalf, 'Information Aggression: A Battlefield of Smartphones', in: H. Mölder e.a. (red.), *Russian Federation in Global Knowledge Warfare* (Cham, Springer Nature Switzerland, 2021) 195-211.

24 Tweede Kamer der Staten-Generaal, *Kamerstukken II*, vergaderjaar 2024/25, 36 280, Nr. 3, blz. 2 en verder, Memorie van Toelichting bij de wijziging van het wetboek van Strafrecht en het Wetboek van Strafrecht BES in verband met de uitbreiding van de strafbaarheid van spionage.

25 H. Mölder en E. Shiraev, 'Global Knowledge Warfare, Strategic Imagination, Uncertainty, and Fear', in: H. Mölder e.a. (red.), *Russian Federation in Global Knowledge Warfare* (Cham, Springer Nature Switzerland, 2021) 13-32; T. Thomas, 'The Evolution of Russian Military Thought. Integrating Hybrid, New-Generation, and New Type Thinking', *The Journal of Slavic Military Studies* (2016) 554-575.

26 *Evangelische Omroep*, 11 november 2025, <https://dit.eo.nl/artikel/vlogen-er-russische-drones-boven-zuid-limburg-nederland-mogelijk-doelwit-belgie-drone-rusland-navo>

27 Zoals ook de Denen ondervonden wanneer bij nader onderzoek naar vermeende dronewaarnemingen een gedeelte van deze waarneming onjuist bleek te zijn. En een aantal van deze waarnemingen kon worden herleid naar bestuurders met bonafide intenties die slechts op de verkeerde plek op het verkeerde tijdstip besloten drones te laten (over)vliegen.

organisaties, drones laten vliegen boven civiele en militaire overheidsterreinen en overheidsgebouwen om een reactie uit te lokken die vervolgens geanalyseerd kan worden. Een derde mogelijkheid is dat een statelijke actor via een criminele of andere malafide organisatie een persoon, via bijvoorbeeld de applicatie Telegram, betaalt om drones boven gevoelige plekken te laten vliegen, enkel en alleen om een reactie uit te lokken.

Ongeacht de intentie van de bestuurder of mogelijke (statelijke) sponsor zijn droneactiviteiten boven civiele- en militaire overheidsterreinen en overheidsgebouwen vanwege het disruptieve effect ongewenst en in veel gevallen verboden. Maar wanneer de intentie of modus operandi van de bestuurder onbekend is, moeten alle scenario's openblijven. Tegelijkertijd kunnen de drones een dreiging voor de veiligheid zijn die weggenomen moet worden, bijvoorbeeld wanneer zij zich bevinden bij terreinen of gebouwen waar dat niet is toegestaan.

Hernieuwd veiligheidsdenken en handelingsperspectief

Waar Rusland inzet op misleiding, kiezen westerse landen zoals Nederland in de huidige competitiefase voor een zorgvuldige analyse van droneactiviteiten voorafgaand aan anticipatie. Hierbij ligt de nadruk op het achterhalen van de eigenaar of bestuurder, het attribueren van de activiteiten aan een (statelijke) actor en soms het correleren van deze activiteiten met andere activiteiten.

Het zorgvuldig analyseren en waarborgen van fundamentele rechtsbeginselen is enerzijds cruciaal om via opsporingsmiddelen een redelijke verdenking vast te stellen en daarmee optreden te legitimeren. Zoals dat bijvoorbeeld het geval is bij een verdenking van spionage-, sabotage- of beïnvloedingsoperaties ten behoeve van een buitenlandse mogendheid, zoals vastgelegd in artikel 98D van het Wetboek van Strafrecht. Hierbij dient opgemerkt dat sabotage een bereik kan hebben van non-kinetisch verstoren van (bedrijfs-)processen tot kinetische

FOTO: RIJKSOVERHEID, LOES SPRUIT-VAN DER MEER



Ongeacht de intentie van de bestuurder of mogelijke (statelijke) sponsor zijn droneactiviteiten boven civiele- en militaire overheidsterreinen en overheidsgebouwen vanwege het disruptieve effect ongewenst en in veel gevallen verboden

vernietiging van zaken. Van non-kinetische sabotage kan bijvoorbeeld sprake zijn als een overheidswebsite of server is gehackt waardoor het gebruik van de website of server onmogelijk is gemaakt. Van kinetische sabotage kan sprake zijn als een spoorweg is vernield waardoor goederenvervoer niet (langer) plaatsvindt. De strafbepaling van artikel 98D kan worden gebruikt voor het duiden van dronewaarnemingen, waarbij de bewijslast beperkt blijft tot het slechts aantonen van voorwaardelijke opzet.²⁸ Tegelijkertijd kost het verrichten van opsporingsonderzoek tijd. Deze tijd is vaak

28 Eerste Kamer der Staten-Generaal, *Kamerstukken I*, 2024/25, 36 280, nr. E, p. 1 en verder, Nota naar aanleiding van het tweede verslag.

essentieel in de anticipatie op de mogelijke verstoring, en schade te voorkomen of beperken, wanneer drones over civiele- en militaire-overheidsterreinen en overheidsgebouwen vliegen.

Samenwerking met (inter)nationale partners

Het proactief bestrijden van drone-activiteiten als hybride dreiging vraagt om nauwe samenwerking tussen (inter)nationale partners. Deze incidenten vormen primair een veiligheids-aangelegenheid in de grey zone-competitiefase tegen een onbekende, mogelijk statelijke, tegenstander. Doordat er geen sprake meer is van een vrede noch van een oorlogssituatie ontstaat er ruimte om via het NAVO-verdrag de samenwerking te intensiveren, met name door gebruikmaking van Artikel 3 en – in bepaalde situaties – Artikel 4.

Artikel 3 van het NAVO-verdrag richt zich op het voortdurend versterken van zowel de individuele als collectieve verdedigingscapaciteit van de lidstaten. Hierbij staat niet alleen zelfhulp centraal, maar ook het gezamenlijk versterken van de verdediging van het bondgenootschap. Het uiteindelijke doel is het waarborgen van de veiligheid en onafhankelijkheid van de NAVO-lidstaten.

Bovendien biedt Artikel 3 de ruimte om, buiten de nationale veiligheidskaders, internationale samenwerking te versterken, met daarin de nadruk op regionale samenwerking. De regio West-Europa kent namelijk een ander dreigings-niveau dan bijvoorbeeld de regio van de Baltische staten in Oost-Europa. Het primair clusteren van informatie en analyses per regio zal bijdragen aan een betere *situational awareness* over waargenomen patronen van droneactiviteiten evenals trends. Gezien eerdere en waarschijnlijk toekomstige dronewaarnemingen in buurlanden zoals Duitsland en België is een gezamenlijke regionale trendanalyse van grote waarde om patronen en uitdagingen te herkennen en proactief evenals effectief te kunnen reageren.²⁹ Een van de uitdagingen kan zijn dat verschillende organisaties en partijen in bepaalde mate bevoegd zijn om in specifieke gevallen handhavend of opsporend op te treden. Deze uitdaging kan leiden tot versnippering van bevoegdheden waardoor vertraging in handelen kan ontstaan. Obstakels in versnippering van bevoegdheden worden ook in België en Duitsland ondervonden.³⁰ Een tegenstander kan (in lijn met de Russische stijl van liminal manoeuvre) de bestaande jurisdictie-uitdagingen ook gebruiken door bewust in deze grensgebieden te opereren, door competentievraagstukken uit te buiten. De verkregen inzichten kunnen vervolgens gedeeld worden met andere Europese regio's om een betere *situational understanding* van de mogelijke dreiging evenals successen van het (pro)actief en repressief handelen te krijgen.

In een verder escalerend scenario kan, in specifieke gevallen, ook Artikel 4 van de NAVO worden ingeroepen, zoals Polen onlangs deed.³¹ Dat artikel maakt het mogelijk om een concrete kwestie formeel voor te leggen aan de Noord-Atlantische Raad van de NAVO, zodat mogelijke vervolgstappen in aanloop naar een Artikel 5-situatie besproken kunnen worden.

Nationaal perspectief: rolverdeling en verantwoordelijkheden

Binnen het nationale kader moet duidelijk worden vastgesteld welke veiligheidsactoren

29 V. Sazanov, 'Russian Strategic Narratives against Ukraine and the West and Political Anticipation of Possible Hybrid War by Russia', Panel discussion Paper Anticipatory Approaches on Conflict and War, *European consortium for Political Research* (2023), zie: <https://ecpr.eu/Events/Event/PaperDetails/67326>.

30 'Belgisch optreden en handhaven van luchtruim boven militaire terreinen en gebouwen wordt bemoeilijkt', *De Tijd*, 5 november 2025, zie: <https://www.tijd.be/politiek-economie/belgie/algemeen/drones-neerhalen-is-niet-alleen-praktisch-moeilijk-het-m-g-ook-niet-zomaar/10634419.html>; 'Vijf vragen over drones: 'Heel Brussel beschermen is onmogelijk'', *Bruzz*, 5 november 2025, zie: <https://www.bruzz.be/actua/veiligheid/vijf-vragen-over-drones-heel-brussel-beschermen-onmogelijk-2025-11-05>; 'Versnippering van bevoegdheden optreden en handhaven drones boven militaire terreinen Duitsland: Kabinett ermöglicht Drohnen-Abwehr durch Bundespolizei', *Mitteldeutscher Rundfunk*, 8 oktober 2025, zie: <https://www.mdr.de/nachrichten/deutschland/politik/polizei-drohnen-abwehr-bundeskabinett-polizeigesetz-dobrindt-100.html>; Charlotte Waaijers, 'Duitsland wil slagkracht tegen drones verbeteren', *NOS*, 8 oktober 2025, zie: <https://nos.nl/artikel/2585708-duitsland-wil-slagkracht-tegen-drones-verbeteren>.

31 'Inroepen Artikel 4 NAVO-verdrag door Polen', *NOS*, 10 september 2025, zie: <https://nos.nl/artikel/2581938-navo-broedt-na-russische-luchtruimschendingen-op-tegenmaatregelen>.



Gezien eerdere en waarschijnlijk toekomstige dronewaarnemingen in buurlanden zoals Duitsland en België is een gezamenlijke regionale trendanalyse van grote waarde om patronen en uitdagingen te herkennen

betrokken zijn bij de dreigings- en trendanalyse, detectie en handhaving bij droneactiviteiten rondom civiele- en militaire- overheidsterreinen en overheidsgebouwen. Het daadwerkelijk wegnemen van de dreiging via droneactiviteiten kan zowel een veiligheids- als een militaire connotatie hebben. Uit de feiten en omstandigheden in de veiligheidsdreigingsanalyse evenals het latere opsporingsproces zal blijken of een statelijke actor mogelijk betrokken is bij de activiteiten. Pas wanneer uit de analyse en het opsporingsproces blijkt dat er sprake kan zijn van een (statelijke) dreiging moet daarnaar gehandeld worden. In de opsporing van een verdachte speelt de marechaussee een prominente rol. Deze organisatie heeft zowel een militaire als een politietaken, en conform artikel 4(1)(C)(D)(E) van de Politiewet is zij belast met onder andere:

- de uitvoering van de politietaken op de luchthaven Schiphol, andere aangewezen luchtvaartterrein evenals de beveiliging van de burgerluchtvaart;
- het verlenen van bijstand alsmede samenwerken met de politie op het gebied van bewaken en beveiligen van objecten en diensten en
- de politietaken uitvoeren op terreinen onder beheer van de minister van Defensie (kazernes, vliegbases en marinehavens).

De verantwoordelijkheid voor de bewaking en beveiliging van militaire terreinen en andere onderdelen van Defensie ligt initieel bij de uitbater van het terrein en is verder belegd bij de Defensie Bewakings- en Beveiligingsorganisaties en operationele commando's.³²

De opsporing van dronebestuurders, als verdachten van het overtreden van het vliegverbod in een gecontroleerd luchtruim, maar ook als (mede)pleger en medeplichtige aan spionage en/ of sabotage, valt onder de juridische kaders van

³² Politietaken Koninklijke Marechaussee zie: <https://www.defensie.nl/organisatie/marechaussee/taken#:~:text=De%20Koninklijke%20Marechaussee%20waakt%20over,internationale%20en%20militaire%20politietaken.>

De marechaussee heeft de unieke positie om informatie uit te wisselen met zowel veiligheidspartners als krijgsmachtonderdelen

rechtshandhaving. Daarmee valt de opsporing van deze verdachten onder de politietaak van de Nationale Politie en indien het over onder andere defensie terreinen, aangewezen luchthavens en verboden plaatsen gaat, of als er defensiebelangen zijn geschaad, ook onder de politietaken van de marechaussee zoals omschreven in artikel 4 van de Politiewet. Deze politietaken beogen het beëindigen van het strafbare feit, de inbeslagname van daarvoor vatbare onderwerpen zoals de drones en de opsporing en vervolging van de verdachten. Daarnaast ligt er ook een taak voor diensten die verantwoordelijk zijn voor de (gewapende) beveiliging van objecten en subjecten, namelijk het leveren van *force protection*. Met het leveren van *force protection* aan bijvoorbeeld civiele- en militaire overheidsterreinen en overheidsgebouwen worden bewakings- en beveiligingsmaatregelen bedoeld die de kwetsbaarheid van

faciliteiten, materieel en personen minimaliseren.³³ Het ligt in de rede dat in het kader van deze drone-activiteiten een uitvoeringscombinatie van politietaken plaatsvindt van bewaken en beveiligen (*force protection*) met het beheersen van veiligheidsrisico's voor terreinen, gebouwen als personen.

Wanneer het gaat om dreigingen van militair-specifieke aard, zoals statelijke actoren of statelijk geaffilieerde organisaties met malafide intenties die gericht zijn op sabotage en het ondermijnen van de statelijke integriteit en soevereiniteit van Nederland, kan bredere inzet van de krijgsmacht wenselijk en zelfs noodzakelijk zijn.

De Koninklijke Marechaussee kan per Artikel 62(1) Politiewet 2012 voor de uitvoering van *alle aan haar opgedragen politietaken*³⁴ in bijzondere gevallen verzoeken om specialistische bijstand van andere krijgsmachtonderdelen te ontvangen.³⁵ Dit bijstandsverzoek wordt gekenmerkt door een tekort aan een voor de taak noodzakelijk geachte kwaliteit of kwantiteit van personeel of materieel.³⁶ Van deze noodzaak is bijvoorbeeld sprake wanneer de nationale veiligheid wordt bedreigd, er zeer snel over voldoende specifieke deskundigheid en middelen moet worden beschikt, deze specifieke deskundigheid en capaciteit in onvoldoende mate aanwezig zijn bij de marechaussee, maar andere krijgsmachtonderdelen deze kennis en middelen reeds bezitten.³⁷ Zo kan de marechaussee bij droneactiviteiten die een mogelijke dreiging vormen voor specifieke gebouwen en terreinen, (tijdelijke) bijstand voor counterdrone-operaties bij andere krijgsmachtdelen vragen. Ook heeft de marechaussee de unieke positie om informatie uit te wisselen met zowel veiligheidspartners als krijgsmachtonderdelen.

Vooruitkijken: van safety naar security

De huidige competitiefase rondom drone-activiteiten zal naar verwachting de komende jaren aanhouden en mogelijk intensiveren. Dergelijke activiteiten vormen in de eerste plaats een veiligheidsaangelegenheid, vanwege de mogelijke betrokkenheid van een statelijke

33 NATO, Applied Joint Doctrine 3.14, Fundamentals of Force Protection p. 19 en verder.

34 Anders dan onder de voormalige Politiewet 2012, kan thans bijstand worden gevraagd en verleend voor alle politietaken, waaronder dus ook voor handhaving van de rechtsorde, strafrechtelijke handhaving van de rechtsorde en taken ten dienste van Justitie.

35 Tweede Kamer der Staten-Generaal, *Kamerstukken II*, vergaderjaar 2020/21, 36 759, nr. 3, p. 6 en verder, Memorie van Toelichting bij wijziging van de Politiewet 2012 in verband met enkele aanpassingen die volgen uit de evaluatie van deze wet.

36 Tweede Kamer der Staten-Generaal, *Kamerstukken II*, vergaderjaar 2006/08, 30 880, nr. 3, p. 59 en verder, Memorie van Toelichting bij de vaststelling van een nieuwe Politiewet (Politiewet 200).

37 Tweede Kamer der Staten-Generaal, *Kamerstukken II*, vergaderjaar 2020/21, 36 759, nr. 3, p. 8 en verder, Memorie van Toelichting bij wijziging van de Politiewet 2012 in verband met enkele aanpassingen die volgen uit de evaluatie van deze wet.



De marechaussee kan bij droneactiviteiten die een mogelijke dreiging vormen voor specifieke gebouwen en terreinen, (tijdelijke) bijstand voor counterdrone-operaties bij andere krijgsmachtdelen vragen

actor. Wat de situatie complex maakt is dat de doelstelling van deze droneactiviteiten vaak verhuuld blijft door de dubbelzinnigheid van de intentie waarmee ze worden uitgevoerd. Hoewel het vaak onduidelijk blijft wie de daadwerkelijke bestuurder of sponsor van de drone is, staat wel vast dat de loutere aanwezigheid van drones maatschappelijke onrust veroorzaakt. Daarnaast kunnen deze activiteiten een versturende uitwerking hebben op dagelijkse (operationele) bedrijfsprocessen. Het is van belang dat hierin verandering wordt aangebracht, zodat de geplande operationele prioritering de focus blijft.

In het hernieuwde veiligheidsdenken is het noodzakelijk om de samenwerking met nationale en internationale veiligheids- en militaire partners te intensiveren. Deze versterkte samenwerking is essentieel om

adequaat te kunnen reageren op hybride dreigingen die kunnen volgen uit drone-activiteiten. Tegelijkertijd is het belangrijk ruimte te bieden aan innovatieve oplossingen. Een voorbeeld hiervan is het tijdelijk onderbrengen van capaciteit van andere krijgsmachtdelen bij de marechaussee (of de Nationale Politie) via een bijstandsconstructie op grond van de Politiewet. Hierdoor worden inzetmogelijkheden tegen hybride dreigingen in het veiligheidsdomein uitgebreid en nemen handelingsopties toe. De legitimiteit van deze constructie waarborgt bevoegdheden en verantwoordelijkheden, bijvoorbeeld voor het uitvoeren van counterdrone-operaties en het opsporen van verdachten. Op deze manier kan de krijgsmacht gepast, flexibel en effectief inspelen op actuele dreigingen, terwijl andere noodzakelijke capaciteit behouden blijft. ■