

Dreigingsbeelden van toen en nu

Prof. dr. ir. Bas Rietjens*

Het militaire dreigingsbeeld in de Koude Oorlog kwam tot stand via processen waarbij inlichtingendiensten op basis van feiten en aannames probeerden zo volledig mogelijk de kracht en intenties van de Sovjet-Unie in te schatten. Na de Russische invasie van Oekraïne in 2022 zeiden sommige veiligheidsexperts dat de Koude Oorlog terug is. Maar in hoeverre is het vijandbeeld zelf en de manier waarop dat destijds tot stand kwam bruikbaar om de huidige tijd te analyseren?

Jan Hoffenaar, Anselm van der Peet en Quirijn van der Vegt beschrijven in deze speciale editie van de *Militaire Spectator* op fascinerende wijze het militaire vijandbeeld in de Koude Oorlog en hoe de drie Nederlandse militaire inlichtingendiensten zich dat toen vormden. Er is maar weinig onderzoek gedaan naar dit thema en de artikelen geven een goed inzicht in het werk van de diensten en de uitdagingen waar ze voor stonden. Maar de vraag rijst ook in hoeverre de vijandbeelden zelf en de manier waarop ze tot stand kwamen bruikbaar zijn om de huidige tijd te analyseren. De afgelopen jaren en

met name sinds de inval van Rusland in Oekraïne halen hooggeplaatste militairen, politici en analisten immers vaak de Koude Oorlog aan in hun commentaren en duiding. ‘De Koude Oorlog is terug’, zegt de voormalige Duitse minister van Buitenlandse Zaken Joschka Fischer,¹ terwijl het Nederlandse officierenblad *Carré* meerdere artikelen onder de titel ‘Lessen uit de Koude Oorlog’ publiceert.² Tegelijkertijd klinken er verschillende tegengeluiden en nuances in relatie tot deze vergelijking.³ In dit essay verken ik hoe het militaire vijandbeeld en de totstandkoming ervan in de Koude Oorlog zich verhoudt tot dat van vandaag.

Een veranderend dreigingsbeeld

Bij het bekijken van de huidige dreigingsanalyses van westerse militaire inlichtingendiensten zoals de Militaire Inlichtingen- en Veiligheidsdienst (MIVD),⁴ het Amerikaanse Defense Intelligence Agency (DIA)⁵ of de Franse Direction du Renseignement Militaire (DRM) valt een aantal zaken op. Allereerst is de geschetste dreiging zeer pluriform. Waar de dreiging tijdens de Koude Oorlog hoofdzakelijk van de

* Bas Rietjens is hoogleraar Intelligence in War and Conflict aan de Universiteit Leiden en hoogleraar Inlichtingen & Veiligheid aan de Nederlandse Defensie Academie.

1 Joschka Fischer, ‘De Koude Oorlog is terug’, *Project-Syndicate.org*, 3 oktober 2022.

2 Christian Kamphuis, ‘Lessen uit de Koude Oorlog #1. Parallellen met de Koninklijke Landmacht in de jaren tachtig: organisatie en optreden’, *Carré*, No. 5 (augustus 2023) 8-16; Christian Kamphuis, ‘Lessen uit de Koude Oorlog #2. Parallellen met de Koninklijke Landmacht in de jaren tachtig: echelonering, logistiek en de nationale sector’, *Carré*, No. 6 (september 2023) 8-17.

3 Zie bijvoorbeeld David Petraeus en Robert Andrews, *Conflict. The Evolution of Warfare from 1945 to Ukraine* (New York, HarperCollins, 2023); Peter Giesen, ‘Een nieuwe Koude Oorlog? Waarom terugblikken verleidelijk is, maar niet erg zinvol’, *de Volkskrant*, 14 maart 2022.

4 Militaire Inlichtingen- en Veiligheidsdienst, *Openbaar jaarverslag 2022* (Den Haag, MIVD, 19 april 2023).

5 Defense Intelligence Agency, ‘Threat reports’, *dia.mil* (Washington, D.C.).



FOTO PICTURE ALLIANCE/ZB/THOMAS LEHMANN

Afvoer van Warschaupactjagers naar het museum. Is de Koude Oorlog met het bijbehorende vijandbeeld nu weer terug?

Sovjet-Unie kwam, is er momenteel een grote verscheidenheid aan dreigingen tegen de westerse veiligheidsbelangen. Deze dreigingen variëren geografisch. Denk alleen al aan Rusland (de oorlog in Oekraïne en de dreiging tegenover NAVO-partners zoals de Baltische staten), het Midden-Oosten (de ontwikkeling van kernwapens door Iran; de belemmering van de vrije vaart door de Rode Zee; de oorlog in Gaza), China (een mogelijke aanval op Taiwan; beschikbaarheid cruciale grondstoffen; technologische ontwikkeling) en Noord-Korea (nucleaire proliferatie). Om deze geografische diversiteit te benadrukken spreekt de Franse DRM sinds kort over een ‘360-gradenanalyse’.⁶ Naast het geografische aspect is ook de aard van

de betrokken actoren gevarieerd. Waar tijdens de Koude Oorlog de focus op statelijke actoren lag, kenmerken de huidige dreigingen zich door betrokkenheid van verschillende combinaties van statelijke en niet-statale spelers. Zo komt de Chinese spionagedreiging niet alleen van het ministerie van Staatsveiligheid, maar ook van onderzoeksinstituten en de naar schatting 150.000 *state-owned enterprises*, waaronder luchtvaartorganisaties en technologiebedrijven.⁷ Een laatste variatie van het dreigingsbeeld die ik

6 Murielle Delaporte, ‘French military intelligence office reorganizing post-Ukraine, with ‘360 degree’ threatanalysis’, *Breakingdefense.com*, 26 mei 2023.

7 Nicholas Eftimiades, ‘On the Question of Chinese Espionage’, *Brown Journal of World Affairs*, Vol. 26, No. 1 (2019) 125-142.

Door de globalisering vervaagt het onderscheid tussen interne en externe veiligheid, het onderscheid tussen de publieke en de private sector en wat precies de kwalificatie militair of civiel moet krijgen

hier benoem is die tussen het fysieke, cognitieve en virtuele domein. Stonden tijdens de Koude Oorlog het fysieke en cognitieve domein centraal, de afgelopen decennia is het virtuele domein steeds belangrijker geworden. Denk hierbij aan cyberaanvallen en digitale spionage. En nog meer dan vroeger bestaat de dreiging uit een samenspel van activiteiten in deze drie domeinen, al dan niet actief gecoördineerd.

Naast pluriform is de dreiging die de inlichtingendiensten schetsen complex. Hoewel sommigen dit afdoen als een betekenisloos *buzzword*, zegt het wel degelijk veel over de huidige dreiging. Complexiteit wordt gekenmerkt door onduidelijke oorzaak-gevolgrelaties, een hoge mate van ambiguïteit en een gebrek aan bestaande kennis en standaarden om de gewenste doelstelling te bereiken. En als er al iets is dat in de buurt komt van een oplossing, dan is dit geen *one-size-fits-all*, maar verschilt deze van situatie tot situatie. En waar vroeger duidelijke scheidslijnen waren tussen oorlog, georganiseerde criminaliteit en grootschalige schending van mensenrechten, zijn deze lijnen in veel van de recente conflicten vervaagd. Er worden veel verschillende termen gebruikt om dit te benoemen, waaronder hybride oorlogvoering, *grey-zone warfare* of *non-linear warfare*. Of, zoals Mark

Galeotti dit in zijn meest recente boek omschreef, de ‘*weaponisation of everything*’.⁸ Concrete voorbeelden hiervan zijn de vluchtelingen die president Loekasjenko van Belarus laat ophalen in Syrië om ze vervolgens de grens over te zetten naar Polen. Of de inzet van wetgeving door China om zijn staatsburgers wereldwijd te verplichten bij te dragen aan zijn inlichtingenpositie. Het duiden van deze ontwikkelingen en het beschermen tegen de veelheid aan dreigingen leidt tot een immense uitdaging voor inlichtingendiensten.

Een derde kenmerk van de dreigingsanalyses is het vervagen van de grenzen van wat precies militair is. De artikelen in deze *Militaire Spectator* schetsen een beeld van de verschillende inlichtingendiensten die specifiek voor hun krijgsmachtdeel de militaire capaciteiten en activiteiten van het Warschaupact in kaart brachten. Hierbij trad vaak overschatting op, zoals bijvoorbeeld blijkt uit de inschatting van de hoeveelheid onderzeeboten die de Sovjet-Unie tot haar beschikking had (zie het artikel van Anselm van der Peet). Het in kaart brengen van de intenties van het Sovjetleger en het Kremlin was verder erg moeilijk, zo niet onmogelijk. Wat dat betreft lijkt er niet zoveel veranderd te zijn. Nog steeds houden verschillende onderdelen van de militaire inlichtingendiensten en de krijgsmachtdelen zich bezig met de analyse van de activiteiten, capaciteiten en intenties van hun opponenten. En nog steeds is het makkelijker om activiteiten en capaciteiten in te schatten dan intenties bloot te leggen. Wat echter wel degelijk veranderd is ten opzichte van de Koude Oorlog is de wereldwijde connectiviteit, zowel op politiek, economisch, militair als cultureel vlak. Door deze globalisering vervaagt het onderscheid tussen interne en externe veiligheid, het onderscheid tussen de publieke en de private sector en wat precies de kwalificatie militair of civiel moet krijgen. Een treffend voorbeeld van deze vervagende grenzen is de afhankelijkheid van het Oekraïense leger van de Starlink-satellietverbindingen voor zijn operationele communicatie.⁹ Ook het Chinese strategische doel van civiel-militaire fusie is illustratief. Het komt neer op een grote vermenging van het militair-industrieel complex met de civiele industrie in

8 Mark Galeotti, *The Weaponisation of Everything. A Field Guide to the New Way of War* (New Haven, Yale University Press, 2022).

9 Lonneke Peperkamp en Patrick Bolder, ‘The Space Domain and the Russia-Ukraine War’, in: Maarten Rothman, Lonneke Peperkamp en Bas Rietjens (red.), *Reflections on the Russia-Ukraine War* (Leiden, Leiden University Press, 2024) 257-273.



Minister Stef Blok (Buitenlandse Zaken) presenteert de China-strategie (2019). Hoe beschermt Nederland zijn belangen bij een Chinese civiel-militaire fusie?

uiteenlopende gebieden zoals personeel, technologie, R&D en het productieproces. Dit maakt het onduidelijk wat nog precies militair is en wat niet.

Totstandkoming van het dreigingsbeeld

Het veranderende dreigingsbeeld stelt (militaire) inlichtingendiensten voor veel grote uitdagingen. De omvang van dit essay laat een uitgebreide behandeling niet toe. Ik zal er daarom een paar uitlichten en presenteren langs de lijn van de fasen van de inlichtingencyclus: sturing, verzameling, verwerking & analyse en verspreiding.

Volgens de klassieke manier geven politici en militaire commandanten richting aan het inlichtingenproces door het formuleren van inlichtingenbehoeften. Volgens Donald Rumsfeld, voormalig minister van Defensie van de VS, impliceert dit het op zoek gaan naar

zogeheten *known unknowns*, zaken waarvan we weten dat we ze niet weten. Het ingaan op deze inlichtingenbehoeften is nog steeds zeer belangrijk, maar in het huidige dreigingsbeeld allang niet meer voldoende. Zowel de inlichtingenorganisaties als de afnemers van hun producten bevinden zich steeds vaker in een positie die dezelfde Rumsfeld duidt als *unknown unknowns*, ofwel ongekende dreigingen. In dit geval weten behoeftezoekers en inlichtingendiensten niet wat ze zoeken en waar ze dat zouden moeten doen. Het vooraf formuleren van inlichtingenbehoeften is dan niet altijd langer werkbaar.

Bij de verwerving van data valt op dat er naast de inlichtingendiensten veel andere actoren actief zijn. Dit zijn onder andere individuen, commerciële bedrijven, departementen en, sinds een aantal jaren, ook zogeheten non-profitcollectieven. Deze collectieven bestaan uit een netwerk van vrijwilligers en maken gebruik van de grote hoeveelheid beschikbare openbare bronnen. Bellingcat is het bekendste voorbeeld. Maar

ook een organisatie als Amnesty International heeft met behulp van 28.000 vrijwilligers en door gebruik te maken van publiek toegankelijke satellietbeelden bewijsmateriaal verzameld van oorlogsmisdaden in Soedan.

Waar tijdens de Koude Oorlog samenwerking tussen westerse inlichtingendiensten belangrijk was, is dit speelveld nu uitgebreid met deze grote hoeveelheid externe actoren. Het organiseren van deze samenwerkingsverbanden is voor een (militaire) inlichtingendienst van groot belang, maar niet bepaald makkelijk gezien de organisatiecultuur die vaak de voorkeur geeft aan geheimhouding.

Kijkend naar de fase van verwerking & analyse dan springt de implementatie van het datagedreven werken in het oog. Waar veel inlichtingenteams vooral gebruik maken van traditionele en kwalitatieve analyses, hebben zij nu in potentie de beschikking over een exponentieel groeiende hoeveelheid (open source) data, snel toenemende rekenkracht van computers en de beschikbaarheid van modellen voor data-analyse. Dit maakt de implementatie van datagedreven werken essentieel. Militaire inlichtingendiensten zoals de MIVD ondervinden hierbij echter grote uitdagingen. Veel betrokkenen wijzen direct op het geringe aantal medewerkers met een bètaprofiel. Hoewel dit zeker het geval is, zijn er veel andere uitdagingen, zoals de beschikbare infrastructuur (onder meer hardware, software en applicaties), het data-analfabetisme van veel analisten en een groot deel van het management, de integratie tussen kwalitatieve en kwantitatieve analyses en, niet in de laatste plaats, de informatiehuishouding. Wat hiernaast meespeelt zijn de verschillende dreigingspercepties. In de Koude Oorlog werd de dreiging redelijk eenduidig gepercipieerd (grote activiteiten van een Sovjetlegerkorps duiden bijvoor-

beeld op gevaar), maar bij de huidige dreigingen is dit lang niet altijd het geval. Bij veel grote dossiers zoals kennisveiligheid,¹⁰ kritieke infrastructuur¹¹ of migratie¹² is er een clash van belangen en mede als gevolg daarvan een wisselende dreigingsperceptie. Dit maakt het ook problematisch om te spreken over vijanden en vijandbeelden. Termen als dreiging en dreigingspercepties lijken daarom beter te passen.

Tot slot is er nog de verspreiding van inlichtingen. De relatie tussen inlichtingenproducenten en -consumenten is niet langer dichotoom, maar gelaagd en genuanceerd.¹³ Organisaties zijn soms zowel producent als consument. Zo gebruiken inlichtingenorganisaties eenheden van de krijgsmacht bijvoorbeeld als sensor, maar leveren zij tevens inlichtingenanalyses aan deze zelfde eenheden. Ook de kwestie hoe dichtbij of veraf producenten en consumenten zich van elkaar bevinden is hierbij van belang. Waar

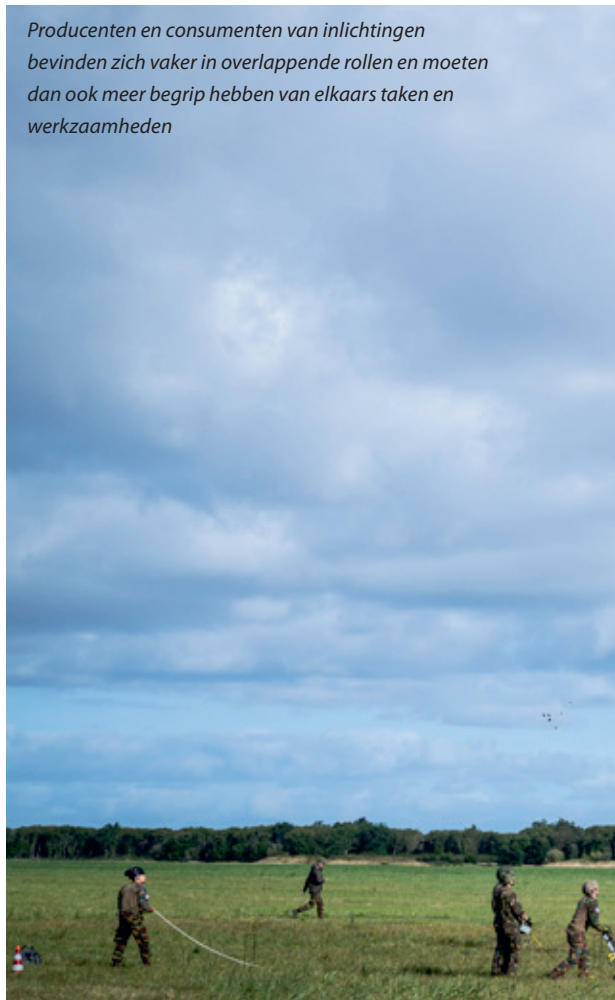
Producenten en consumenten van inlichtingen bevinden zich vaker in overlappende rollen en moeten dan ook meer begrip hebben van elkaars taken en werkzaamheden

10 David Snetselaar, 'Dreams Lab: assembling knowledge security in Sino-Dutch research collaborations', *European Security*, Vol. 32, No. 2 (2022) 233-251.

11 Hugo Meijer, *Awakening to China's Rise. European Foreign and Security Policies toward the People's Republic of China* (Oxford, Oxford University Press, 2022).

12 Sarah Léonard en Christian Kaunert, 'De-centring the Securitisation of Asylum and Migration in the European Union: Securitisation, Vulnerability and the Role of Turkey', *Geopolitics*, Vol. 27, No. 3 (2022) 729-751.

13 Saskia Pothoven, 'Voorbij de heilige huisjes. Militair perspectief op de inlichtingenproducent-klantrelatie', *Militaire Spectator* 191 (2022) (9) 476-485.



vroeger een duidelijke scheiding tussen inlichtingenanalyse en beleid was, laat het onderzoek van Saskia Pothoven zien dat deze scheiding niet langer houdbaar is.¹⁴ Producenten en consumenten bevinden zich vaker in overlappende rollen en moeten dan ook meer begrip hebben van elkaars taken en werkzaamheden.

Ten slotte

Zijn artikel over het vijandbeeld op het land eindigt Jan Hoffenaar met: 'Het laat nog maar eens zien hoe moeilijk, ja onmogelijk het zelfs nu nog steeds is een nauwkeurig en juist beeld van de militaire dreiging over land te krijgen'. Ook in deze tijd staat deze bewering recht overeind. Maar afgaande op het vijandbeeld en de totstandkoming ervan doet een vergelijking met de Koude Oorlog maar ten dele recht aan de huidige situatie. Zoals ik hierboven heb betoogd zijn er veel verschillen te identificeren. Inlichtin-

genorganisaties zijn dag en nacht bezig om zich aan te passen aan deze nieuwe situatie. Dit maakt adaptatie en innovatie de kern van het werk van inlichtingendiensten in deze snel veranderende wereld. Veel inlichtingenleiders onderschrijven het belang hiervan gelukkig volledig. Het is alleen verontrustend dat de kennis van hoe inlichtingenorganisaties moeten innoveren veelal gefragmenteerd en beperkt is.¹⁵ Daar moet de volledige inlichtingengemeenschap, inclusief wetenschap en technologiebedrijven, dan ook vol de schouders onder gaan zetten. Maar in deze snel veranderende wereld is het de vraag of dat genoeg zal zijn. ■

14 Ibidem.

15 Zie onder meer Niccolò Petrelli, 'Analytical Innovation in Intelligence Systems. The US National Security Establishment and the Craft of 'Net Assessment', *Intelligence and National Security* 37, No. 1 (2022) 1-18; Bas Rietjens, Stephen Coulthart en Rob Sinterniklaas, 'Innovate or perish: towards a research agenda for intelligence organisations', paper gepresenteerd tijdens de Netherlands Intelligence Studies Association Conference, Amsterdam, oktober 2023.

