Trendalert

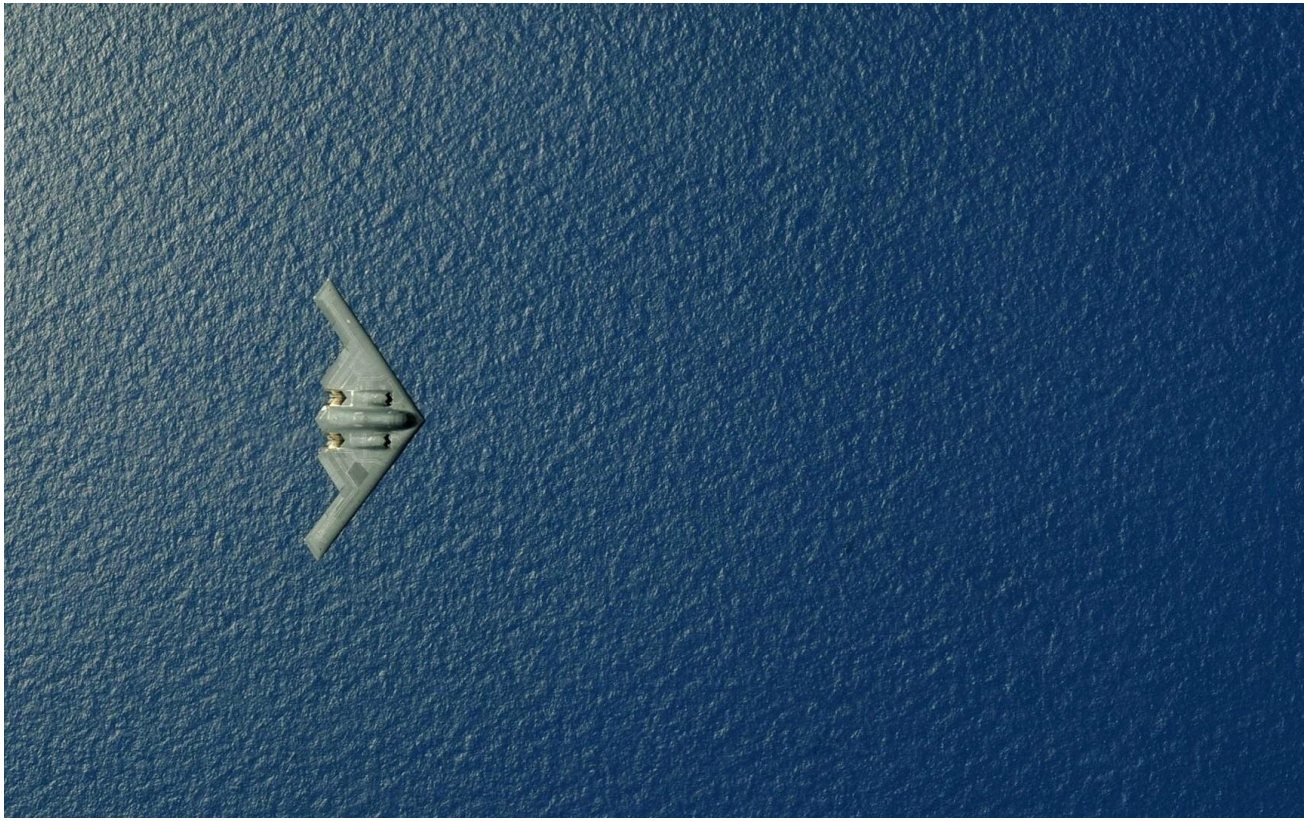
S E P T E D

Kwetsbaarheden rondom hybride oorlogsvoering en oorlogsdreiging

Auteur(s): Josje Brouwers

Samenvatting

Sinds de inval van Rusland op de Krim en de Donbas in 2014 en de grootschalige invasie van Oekraïne in 2022, wordt in Westerse media en door de Nederlandse overheid steeds vaker gesproken over de dreiging van *hybride oorlogsvoering*—een vorm van oorlog waarin de nadruk ligt op niet-conventionele strategieën zoals propaganda en desinformatie. Als we recente uitingen van onderzoekers en (inter)nationale veiligheidsdiensten mogen geloven lijkt die dreiging ook steeds urgenter. In de watersector wordt dit onderwerp ook opgepakt. Tegelijkertijd zien we dat daarin dat specifieke soorten dreiging meer aandacht krijgen andere. Zo lijk de huidige beschermingsinspanning zich vooral te richten op sabotage van kinetische aard of in digitale omgevingen. Maar zowel in de watersector als breed in de samenleving lijkt een antwoord op de dreiging van spionage, desinformatie en AI nog te ontbreken.



Een Northrop Grumman B-2 Spirit: een type militair vliegtuig dat werd ingezet door de Verenigde Staten bij de aanval op Iran op 22 juni 2025.

S E P T E D

Trendbeschrijving en achtergrond

Oorsprong, definitie en kritiek op het begrip *hybride oorlogsvoering*

De annexatie van de Krim in 2014 wordt over het algemeen aangewezen als het moment waarop hybride oorlogsvoering een mainstream begrip werd in de politiek en media. Maar in militaire kringen werd de term *hybride oorlogsvoering* al ver voor 2014 gebruikt. In eerste instantie verwees het voornamelijk naar strategieën die door militair zwakke(re) en non-statelijke actoren worden toegepast om politieke doelstellingen te behalen zonder een militair conflict uit te lokken. Hiermee proberen ze om de politieke eenheid en het maatschappelijk draagvlak van de tegenstander te ondermijnen. Dit wordt ook wel *horizontale escalatie* genoemd. Guerrillatactieken die werden ingezet door onafhankelijkheidsbewegingen in voormalige koloniën zijn hier een voorbeeld van, net als aanvallen van terreurbewegingen als de Taliban en IS.

Over de tijd zien we een verschuiving van de associatie met de term *hybride oorlogsvoering*. Waar het eerst alleen verwees naar een militaire strategie die door militair zwakkere en niet-statelijke actoren werd gebruikt, wordt het tegenwoordig ook gerelateerd aan militair machtige en statelijke actoren. In het Westen, zowel in de media als in wetenschappelijke publicaties, wordt het nu vooral gebruikt in relatie tot Rusland en (in mindere mate) China, Iran en Noord-Korea.

Deze verschuiving van betekenis is een weerspiegeling van een veelvoorkomende kritiek op (het gebruik van) de term *hybride oorlogsvoering*, namelijk dat het vooral een weerspiegeling is van het vijandbeeld van een bepaalde periode in plaats van een duidelijke, herkenbare vorm van oorlogsvoering. Een andere vorm van kritiek luidt dat *hybride oorlogsvoering* zo breed wordt gedefinieerd dat het indoet voor bruikbaarheid. Dit zien we bijvoorbeeld terug bij de nieuwsmedia als de NOS, die hybride oorlogsvoering definieert als '*een militaire strategie die de conventionele oorlogsvoering mengt met niet-militaire middelen zoals desinformatie, propaganda en politieke intimidatie*'. Deze definitie geeft weinig houvast omdat dit op vrijwel alle militaire conflicten kan worden toegepast.

Het voornaamste probleem van een gebrek aan een eenduidige definitie van *hybride oorlogsvoering* is dat het daardoor moeilijk vast te stellen is of en wanneer er sprake is van oorlog of niet.

In de wetenschappelijke literatuur op dit onderwerp wordt ook gesproken over het gebrek van consensus over wat *hybride oorlogsvoering* wel en niet inhoudt en de complexiteit van het vinden van een bruikbare definitie. Wat wel duidelijk is, is dat bij de huidige vorm van hybride oorlogsvoering (post 2014) een sterkere nadruk ligt op niet-militaire conflicten dan voorheen, en met name op zogenoemde informatieoorlog (i.e., *information warfare*). Hieronder valt zowel het gebruik van propaganda, verspreid via verfijnde sociale mediacampagnes, en het zaaien van twijfel en verdeeldheid over waarheden.

Bij gebrek aan een breed gedragen definitie, is het wellicht nuttiger om hybride oorlogsvoering te benaderen vanuit een aantal soorten aanvallen die veelal hieraan worden toegeschreven. In onderstaande box staan zeven categorieën van aanvallen binnen hybride oorlogsvoering. Deze zijn ontleend aan een DSWI-denktanksessie van 13 maart 2024.

S E P T E D

Typen hybride aanvallen

- **Kinetische dreiging**. Fysieke aanvallen of operaties, zoals bombardementen, grondinvasies of militaire confrontaties, gericht op het veroorzaken van schade aan infrastructuur, troepen of eigendommen van een tegenstander
- **Spionage**. Het heimlijk verzamelen van gevoelige informatie zoals militaire plannen, technologische ontwikkelingen of diplomatieke gesprekken, met als doel strategische voordelen te behalen of de activiteiten van een tegenstander te ondermijnen
- **Sabotage**. Doelbewuste acties om de werking van infrastructuur, apparatuur of systemen te verstoren, beschadigen of vernietigen, met als doel chaos te veroorzaken, economische schade toe te brengen of de operationele capaciteit van een tegenstander te ondermijnen.
- **Desinformatie**. Het verspreiden van valse, misleidende of gemanipuleerde informatie om verwarring te zaaien, de publieke opinie te beïnvloeden, verdeeldheid te creëren of het vertrouwen in instellingen, regeringen of leiders te ondermijnen.
- **Beïnvloedingsoperaties**. Acties gericht op het manipuleren of beïnvloeden van politieke processen, verkiezingen, maatschappelijke groeperingen of individuen om politieke doelstellingen te bereiken, zoals het beïnvloeden van stemgedrag, het versterken van pro-overheidsstandpunten of het destabiliseren van tegenstanders.
- **Cyberaanvallen.** Aanvallen op computersystemen, netwerken of digitale infrastructuren met als doel het verstoren, saboteren, spioneren of manipuleren van gegevens, communicatie of operationele processen, zoals het uitschakelen van vitale infrastructuur, het stelen van gevoelige informatie of het verspreiden van malware.
- **AI als threat multiplier**. Het gebruik van kunstmatige intelligentie (AI) om bestaande dreigingen te verbeteren of nieuwe bedreigingen te creëren door middel van geautomatiseerde analyse, besluitvorming en uitvoering van acties, zoals het verbeteren van cyberaanvallen, spionageactiviteiten of deinformatiecampagnes.

Hybride oorlogsvoering als hedendaags maatschappelijk en politiek thema

In de afgelopen jaren en maanden zien we op allerlei maatschappelijke terreinen steeds meer aandacht voor het onderwerp hybride oorlogsvoering, waaronder wetenschap, de NAVO, de nationale overheid, de watersector zelf en onder de bevolking. Voorbeelden van het type hybride aanvallen uit de categorisering van DWSI zijn dikgedrukt.

NAVO

In juni bracht de Groene Amsterdammer een speciale editie uit over hybride oorlogsvoering. In een van de artikelen waarschuwt Jean Ellermann-Kingombe—de huidige adjunct-secretaris-generaal op het gebied van Innovatie, Hybride en Cyber bij de NAVO—voor een langdurige, grotendeels onzichtbare confrontatie tussen Rusland en het Westen waarbij de Russen '*intensief en met een groeiende risicobereidheid*' te werk gaan. De adjunct-secretaris-generaal benoemt hierbij onder andere **sabotageacties** gericht op kritieke infrastructuur (zoals onderzeese kabels voor stroom en data) en **beïnvloeding van nationale verkiezingen** in Europese landen.

S E P T E D

Ook in de maanden sinds de top blijft de NAVO benoemen dat we ons moeten voorbereiden op oorlog met Rusland. In een recente toespraak van 11 december sprak Rutte over een oorlog '*van een omvang die onze grootouders en overgrootouders hebben meegemaakt*'.

Nationale overheid

Nationale overheidsinstanties spreken zich ook uit over (de dreiging van) hybride oorlogsvoering. Een gezamenlijk uitgegeven dreigingsbeeld van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), het Ministerie van Defensie en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) uit 2024 waarschuwt dat een militair conflict *'in de regel wordt voorafgegaan door hybride dreigingen*' en dat '*Nederland er serieus rekening mee moet houden dat de grens van een gewapend conflict wordt genaderd*'. In het dreigingsbeeld wordt onder andere gewaarschuwd voor toenemende **fysieke aanvallen** door Rusland en China op vitale infrastructuur. Het gaat dus niet (meer) alleen over digitale aanvallen). Daarnaast wordt waarschuwen de auteurs van het dreigingsbeeld voor doelbewuste **economische ondermijning** door het werven van unieke en strategische Nederlandse kennis en technologie.

Wetenschap

In december 2024 publiceerde onderzoekers van de Universiteit Leiden hun resultaten over Russische **sabotageacties**. De onderzoekers—waaronder Bart Schuurman, hoogleraar Terrorisme en Politiek Geweld aan de Universiteit Leiden—creëerden een overzicht van voorvallen die hebben plaatsgevonden sinds de inval van Rusland in Oekraïne in februari 2022. Uit dit overzicht van iets meer dan 50 acties maakte ze op dat zowel het aantal als de mate van agressiviteit van deze acties in 2024 sterk toenamen ten opzichte van 2022 en 2023. Daarnaast werd geconcludeerd dat het toneel van deze sabotageacties steeds verder richting Nederland verschuift, waarbij Nederlandse watervoorzieningen expliciet als doelwit worden benoemd.

Watersector

In de watersector is onder leiding van het Ministerie van Infrastructuur en Waterstaat in 2023 en 2024 het programma 'Versterken **cyberweerbaarheid** in de watersector' opgestart. Dit samenwerkingsverband tussen het ministerie, Rijkswaterstaat, waterschappen, provincies, gemeenten en drinkwaterbedrijven richt zich met name op de operationele technologieën die worden gebruikt in het leveren van drinkwater, keren en beheren van oppervlaktewater en het transporteren en zuiveren van afvalwater.

Bevolking

Dat Nederland bedreigd wordt door een hybride oorlog met Rusland is ook voelbaar onder de bevolking. Onderzoekers van het Clingendael Instituut brachten afgelopen maart een rapportage uit met betrekking tot de internationale trends die Nederlanders als het meest bedreigend (en het meest hoopgevend) ervaren. Hoewel het instituut dit sinds 2022 jaarlijks doet, springt de dreiging van hybride oorlogsvoering er in 2025 uit. Aldus het rapport met de titel: '*Nederlanders één in vrees voor hybride dreigingen en oorlog te midden van voortdurende grote verdeeldheid*.'

Conclusie: we zitten al in een hybride oorlog

Uit de genoemde ontwikkelingen op internationaal, nationaal en sectoraal niveau kunnen we opmaken dat hybride oorlogsvoering als een reële dreiging wordt beschouwd voor het Westen en voor Nederland en dat de watersector bovendien een specifiek doelwit is. Het is vooral ook duidelijk dat we niet te maken hebben met

S E P T E D

een toekomstige dreiging, maar met een huidige. Of zoals Rutte het onlangs verwoorde: '*De frontlinie heeft allang onze grenzen gepasseerd*.'

Los van discussie over hoe hybride oorlogsvoering wordt gedefinieerd, is het duidelijk dat wel al te maken hebben met de door DWSI genoemde type aanvallen. In bovengenoemde uitingen van de maatschappij zien we voorbeelden van sabotage, (bescherming tegen) cyberaanvallen en beïnvloedingscampagnes. Weliswaar is er (nog) geen sprake van een gewapend conflict, maar de NAVO, defensie en nationale veiligheidsdiensten sluiten niet uit dat we hier in de nabije toekomst (voor het eind van dit decennium) alsnog mee te maken krijgen.

Relevantie

Kwetsbaarheid van processen en infrastructuur

Onder processen verstaan we de productie van drinkwater of de zuivering van afvalwater. Aldus verschillende collega's uit de watersector is de beveiliging van productie- en zuiveringslocaties al flink aangescherpt naar aanleiding van de aanslag op de Twin Towers in 2001.

Onder infrastructuur verstaan we de het netwerk van waterbronnen en drinkwater- en rioolleidingen. Waar de proceslocaties beperkte ruimte innemen en daardoor nog redelijk te beschermen zijn, is dat vrijwel onmogelijk voor infrastructuur gezien de grootte en complexiteit ervan. Dit maakt de infrastructuur met name kwetsbaar voor kinetische en sabotage aanvallen.

Sinds de opkomst van cybertechnologieën en de groeiende aandacht voor de mogelijkheid van cyberaanvallen neemt ook de beschermingsinspanning tegen deze vorm van hybride aanvallen toe. Dit wordt geïllustreerd door het eerdergenoemde programma van het ministerie IenW, maar ook door verscheidene inspanningen van Vewin en de Unie van Waterschappen om meer aandacht te vragen voor cybersecurity in de drinkwatersector en de waterschappen.

Spionage, desinformatie en AI een blinde vlek binnen de sector?

Wat opvalt aan de maatschappelijke en politieke aandacht die uitgaat naar het thema hybride oorlogsvoering en de huidige inspanningen van de watersector, is dat specifieke vormen van dreiging daarin meer aandacht lijken te krijgen dan andere.

Er gaat met name aandacht uit naar de dreiging van sabotage, beïnvloedingscampagnes, fysieke conflicten en cyberweerbaarheid. Daarentegen lijkt er minder aandacht te zijn voor de mogelijke impact van spionage, desinformatie en AI. Toch is het niet ondenkbaar dat ook deze vormen van hybride oorlogsvoering een significante impact kunnen hebben op de sector. Spionage acties kunnen er uiteraard voor zorgen dat gevoelige informatie terecht komt bij partijen die daar misbruik van willen maken, terwijl desinformatie, zeker gekoppeld met AI, kan leiden tot een verlies van vertrouwen in waterveiligheid en drinkwaterkwaliteit, met als gevolg maatschappelijke onrust of zelfs paniek en verdeeldheid. Het zou daarom interessant zijn om in nader onderzoek specifiek in te gaan op specifiek deze dreigingen. Wellicht dat scenario-studies daarbij kunnen helpen om inzicht in de mogelijke gevolgen kunnen vergroten.

Fysieke opgave: ruimte maken

De toenemende oorlogsdreiging creëert een vraag naar meer ruimte voor defensie. Er is meer ruimte nodig in het binnenland voor onder andere opslagplaatsen, kazernes, laagvlieggebieden en oefenterreinen. In juni 2023 is het Nationaal Programma Ruimte voor Defensie (NPRD) van start gegaan, met als doel om in kaart te

S E P T E D

brengen waar in Nederland ruimte zou kunnen worden gemaakt voor de defensiebehoefte. Afgelopen mei werd een conceptversie ingediend ('Ontwerp Nationaal Programma Ruimte voor Defensie') en eind 2025 wordt naar verwachting het programma definitief gemaakt.

Gezien de ingeschatte ruimtebehoefte van defensie enerzijds en andere maatschappelijke ruimtevragen anderzijds (woningbehoefte, energietransitie, natuur) wordt in het NPRD zoveel mogelijk gekeken naar het combineren van functies. In hoofdstuk 7 van het in mei opgeleverde NPRD-ontwerp wordt op een rijtje gezet welke specifieke ruimtebehoeftes defensie heeft en (per behoefte) wat de voorkeurslocaties zijn en welke mogelijke gevolgen dit heeft voor andere functies in de omgeving. Een combinatie van militaire functies en watersector-gerelateerde functies wordt hierbij niet uitgesloten. Een aantal van de benoemde voorkeurslocaties hebben bijvoorbeeld betrekking op waterwegen en -keringen.

Meer informatie

- EenVandaag. (2025, juni 20). *Het gaat volop over hybride oorlogsvoering, maar wat is het eigenlijk? Dit moet je weten*. EenVandaag. https://eenvandaag.avrotros.nl/artikelen/het-gaat-volop-over-hybride-oorlogsvoering-maar-wat-is-het-eigenlijk-dit-moet-je-weten-160566
- Ho, M. S. D., Elchardus, M., & Houtkamp, C. (z.d.). *Nederlanders één in vrees voor hybride dreigingen en oorlog te midden van voortdurende grote verdeeldheid*.
- Hvide Beim, J., & Svendsen, J. (2025, juni 18). 'Ruslands hybride aanvallen stoppen niet als de Oekraïne-oorlog voorbij is', zegt Navo-topadviseur Jean Ellermann-Kingombe. *De Groene Amsterdammer*. https://www.groene.nl/artikel/ruslands-hybride-aanvallen-nemen-toe
- Johnson, R. (2018). Hybrid War and Its Countermeasures: A Critique of the Literature. *Small Wars & Insurgencies*, *29*(1), 141-163. https://doi.org/10.1080/09592318.2018.1404770
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Algemene Inlichtingen- en Veiligheidsdienst, Ministerie van Defensie, & Militaire Inlichtingen- en Veiligheidsdienst. (z.d.). *Dreigingsbeeld militaire en hybride dreigingen*. https://open.overheid.nl/documenten/dpc-f48ff1696bcd9dd7f701d815d842ed375db98bd4/pdf
- Ministerie van Defensie. (2025). *Ontwerp Nationaal Programma Ruimte voor Defensie. Ruimte voor vrede, veiligheid en bescherming.* (p. 78).
- *NAVO-generaal Broeks waarschuwt voor 'hybride oorlogsvoering' vanuit Rusland*. (2017, november 20). https://nos.nl/artikel/2203750-navo-generaal-broeks-waarschuwt-voor-hybride-oorlogsvoering-vanuit-rusland
- Reichborn-Kjennerud, E., & Cullen, P. (2016). *What is Hybrid Warfare?* Norwegian Institute of International Affairs (NUPI). https://www.jstor.org/stable/resrep07978
- *Rutte waarschuwt opnieuw voor dreiging: 'Wij zijn volgende doelwit van Rusland'*. (2025, december 18). https://nos.nl/artikel/2594125-rutte-waarschuwt-opnieuw-voor-dreiging-wij-zijn-volgende-doelwit-van-rusland
- Transatlantic Task Force. (2025, juli 2). *NATO Summit The Hague 2025: Strategic Outcomes and Key Issues | Beyond the Horizon ISSG*. https://behorizon.org/nato-summit-the-hague-2025-strategic-outcomes-and-key-issues/
- Versteegh, K. (2024, december 18). Onderzoekers: De Russische sabotage schuift op naar het Westen, ook richting Nederland. *NRC*. https://www.nrc.nl/nieuws/2024/12/18/onderzoekers-de-russische-sabotage-schuift-op-naar-het-westen-ook-richting-nederland-a4877102

S E P T E D

- Vewin. (2025, mei). *Waterpoort: Waterweerbaarheid actueler dan ooit*. https://www.vewin.nl/nieuws/waterpoort-waterweerbaarheid-actueler-dan-ooit/
- Wither, J.K. (2016). Making Sense of Hybrid Warfare. *Connections, 15*(2), 73-87. http://www.jstor.org/stable/26326441

Keywords
Oorlog, dreiging, hybride, cyber

Auteur(s)
Josje Brouwers

Kwaliteitsborger
Henk-Jan van Alphen

Opdrachtgever
KWR Waterwijs | Integraal

Projectnummer
404300