© Belgian Defence

De rol van Defensie in het gevecht tegen desinformatie in operatie

Mark VANHALLE & Ruben HUYLEBROECK

Kapitein-commandant Mark VANHALLE (KMS – 139 AW) vervoegde de toenmalige Information Operations Group, nu Civil-Military Engagement Group (Ci-MEG), in 2011 en is sindsdien continu actief binnen dit domein in verschillende functies. Zijn uitgebreide ervaring heeft hij opgedaan in een groot aantal NAVO-, EU- en VN-opdrachten op drie continenten. Sinds 2018 is hij de commandant van het Ci-MEG-detachement te Nieuwpoort.

Kapitein-commandant Ruben HUYLEBROECK is Lic. Communicatiewetenschappen en Master in Overheidsmanagement. In het verleden voerde hij voornamelijk functies uit binnen de artillerie en van 2018 tot 2020 was hij werkzaam in Ci-MEG. Hij nam deel aan drie buitenlandse operaties en is sinds 2020 tewerkgesteld op COMOPSLAND-3D.

La désinformation est une menace très sérieuse pour notre société occidentale actuelle, y compris pour la Défense qui est souvent la cible de fake news. Quel est son impact potentiel sur nos opérations et comment pouvons-nous protéger nos troupes à l'étranger contre cette menace ? Le bon « mindset » associé à certains ajustements structurels nécessaires au sein de la Défense et complété par une coopération interdépartementale et internationale offre les meilleures chances de succès pour relever ce défi.

Sinds de bestorming van het Capitool in Washington in januari 2021 staat de bestrijding van desinformatie hoog op de internationale politieke agenda, maar is het ook relevant vanuit militair oogpunt? Betrouwbare informatie is noodzakelijk om correcte beslissingen te kunnen nemen, zeker in tijden van crisis. Dit is niet alleen van toepassing binnen het militaire domein, maar in de gehele maatschappij. In de militaire context hebben recente ontwikkelingen in informatietechnologie echter de aard van conflicten veranderd door er een bijkomende laag aan complexiteit aan toe te voegen. Allerhande partijen maken handig gebruik van de mogelijkheden die de nieuwe communicatietechnologieën bieden om specifieke doelgroepen te beïnvloeden d.m.v. desinformatie.

Een belangrijke hedendaagse uitdaging binnen het veiligheidsdomein is het verzekeren van voldoende *resilience* (weerbaarheid) tegen de dreigingen van een mogelijke hybride oorlogsvoering, waarbij conventionele en irreguliere militaire operaties worden gecombineerd met cyber-operaties, economische en diplomatieke drukkingsmiddelen, enz. om een strategisch effect te bereiken. Desinformatie is slechts één aspect binnen deze *hybrid warfare*, maar wel een aspect van primordiaal belang en al zeker in de aanloopfase van een conflict. De reden hiervoor is tweeledig: enerzijds kan het reeds in vredestijd grootschalig ingezet worden zonder risico om de *threshold of armed* conflict te overschrijden. Anderzijds is het moeilijk om de verantwoordelijkheid van desinformatiecampagnes onbetwistbaar toe te schrijven aan een specifieke actor (probleem van de attributie).

Door middel van desinformatiecampagnes kunnen organisaties en natiestaten rechtstreeks invloed uitoefenen op het democratische proces in een land of de perceptie tegenover de overheid beïnvloeden. Dit stelt hen in staat om een wig te drijven tussen de bevolking, de overheid, politieke partijen en internationale allianties om een kritieke kwetsbaarheid, namelijk (inter)nationale eenheid en cohesie, aan te vallen en zo hun tegenstander te verzwakken.

In het kader van militaire operaties is desinformatie natuurlijk geen nieuw gegeven. In Rusland maken zowel *maskirovka* (deceptie) als *desinformazija* sinds lang een essentieel deel uit van hun doctrine en worden deze in belangrijke mate geïntegreerd in de *Psychological Operations* (PSYOPS) en *Information Operations* om hun strategische objectieven te bereiken. Steeds meer andere landen slaan dezelfde weg in. Zo focust een belangrijk deel van de huidige hervormingen binnen de Chinese strijdmacht zich op *information-centric warfare*, waarbij *information dominance* (zhixin xiquan) het ultieme doel is. België, als gastland voor zowel verschillende EU-instellingen als het hoofdkwartier van de NAVO, is uiteraard een voor de hand liggend doelwit voor dit soort desinformatiecampagnes, zoals gebleken in het verleden. We herinneren ons allemaal de beschuldigingen in 2016 over burgerslachtoffers veroorzaakt door Belgische F16's in de strijd tegen *Daesh*, alsook de gemediatiseerde beschuldigingen in 2019 dat de Belgische geheime dienst een gifgasaanval in Syrië aan het voorbereiden was.

Sociale media zijn één van de belangrijkste recentere communicatietechnologieën en ze werden door verschillende naties en terroristische organisaties al snel geïmplementeerd als een volwaardig wapensysteem voor het voeren van Information *Warfare*. Deze

wapensystemen zijn gemakkelijk en goedkoop in gebruik, maar met potentieel enorme effecten. Ze laten echter ook toe om methodes te gebruiken die niet in lijn zijn met onze westerse waarden en normen. Voor onze strijdkrachten vormt dit een niet te onderschatten nadeel, aangezien het actieterrein sterk gelimiteerd wordt door het huidige legale en ethische raamwerk, terwijl onze tegenstanders hiervan weinig of geen beperkingen ondervinden. Op korte termijn bestaat hiervoor geen eenvoudige oplossing: bijkomende regulering van de sociale mediasector is niet alleen zeer complex, controversieel en tijdrovend, maar ook inefficiënt, aangezien onze tegenstanders permanent hun methodes aanpassen en zodoende het initiatief behouden met innovatieve technologieën en technieken zoals bots (geautomatiseerde softwareprogramma's), internet trols, hijacken, … De technologische evolutie binnen dit domein lijkt niet af te remmen, met als verontrustende ontwikkeling de opkomst van de *deepfaking*-techniek, waarbij op zeer realistische wijze valse videobeelden kunnen worden gecreëerd. De integratie van artificiële intelligentie in deze *deepfake*-technologie zal mogelijk leiden tot een gamechanger op het vlak van desinformatie.

Impact van desinformatie op militaire operaties: een nieuwe uitdaging?

Belgische troepen die ontplooid zijn in het buitenland kunnen, al dan niet bewust als doelwit, het slachtoffer worden van desinformatie. Buitenlandse mogendheden en zowel nationale als internationale slechtgezinde organisaties maken zich schuldig aan het verspreiden van desinformatie in conflictgebieden, om op onrechtstreekse wijze hun belangen in deze regio's te vrijwaren of te vergroten. Deze activiteiten werden reeds gedetecteerd in de meeste operatietonelen waar Belgische Defensie momenteel actief is. Dit is geen nieuw verschijnsel, maar een probleem dat door de nieuwe communicatiemiddelen aan bijkomend belang heeft gewonnen en potentieel een significante impact kan hebben op de veiligheid van onze troepen. We herinneren ons de desastreuze uitkomst van "*Radio Télévision Libre des Mille Collines*" tijdens de Rwandacrisis in 1994. Indien hun boodschap actueel zou verspreid worden door middel van sociale media, dan kan men dezelfde impact realiseren met een nog groter doelpubliek.

Mogelijke manieren waarop militaire operaties het doelwit kunnen worden van vijandelijke desinformatiecampagnes zijn legio. Ze gaan van het politiek-strategische niveau tot het laagste tactische niveau en onderstaande voorbeelden hebben effectief plaatsgevonden tijdens militaire operaties: het insinueren van een alternatieve politieke agenda voor de inzet van een internationale troepenmacht om de aanvaarding en steun van de lokale bevolking aan de operatie in gedrang te brengen (Ops Barkhane & EUTM Mali, 2014-2021); in diskrediet brengen van de commandant d.m.v. gemanipuleerde informatie om het vertrouwen en de loyaliteit van de ondergeschikten negatief te beïnvloeden (eFP Letland, 2017); desinformatie over de bestaande krachtverhoudingen en intenties om de mentale weerbaarheid en motivatie van de troepen te verminderen (eFP Estland, 2019), het verklaren van actuele gebeurtenissen door historische referenties (vermeende neokolonialistische aspiraties van West-Europese landen, Maritime Capacity Building 2019). Onderzoek van het *NATO Strategic Communications Centre of Excellence* tijdens militaire oefeningen heeft bovendien aangetoond dat ontplooide militairen weinig *resilient* zijn tegenover contactverzoeken door *honeytraps* (aanlokkelijke valse profielen op sociale media) en zeer makkelijk werden beïnvloed door de desinformatie die door hen werd verspreid.

Recent heeft de *Digital Media Monitoring & Analysis Section* (DMMAS) van de *Civil-Military Engagement Group* (Ci-MEG) ook verschillende *narratives* van desinformatie rond COVID-19 vastgesteld in de verschillende operatietheaters in Afrika waar Defensie momenteel actief is. Zo werd bijvoorbeeld het nieuws verspreid dat westerse mogendheden vaccins tegen COVID-19 eerst willen testen op de Afrikaanse bevolking vooraleer deze in eigen land te gebruiken, en zijn er beschuldigingen dat westerse naties betrokken waren bij de ontwikkeling van het coronavirus in een labo te Wuhan. Deze desinformatie rond COVID-19 vormt een risico voor onze aanwezige militairen indien zij onterecht worden aanzien als oorzaak of verspreider van deze ziekte. Dit had tijdens de eerste COVID-golf trouwens een enorme impact op de uitvoering van de opdracht van minstens één detachement ontplooid in Afrika. Zodra binnen dit contingent gevallen van COVID-19 werden vastgesteld, werden sommige opdrachten buiten de compound tijdelijk geschrapt, onder andere om te vermijden dat vijandige propaganda de verantwoordelijkheid voor de verdere verspreiding van deze ziekte bij het detachement kon leggen.

Het is dus noodzakelijk dat de tactische commandanten in een operatietheater zich niet alleen bewust zijn van al deze risico's en de mogelijke impact ervan op de operatie, maar dat ze tevens beschikken over de vereiste capaciteiten en procedures om zich er zo goed als mogelijk tegen te beschermen.

Niet enkel in operatie ontplooide militairen kunnen trouwens het slachtoffer zijn van dit soort desinformatiecampagnes: het komt steeds frequenter voor dat hun familie en vrienden worden bestookt met *fake news* en bedreigingen, om op deze manier het moreel van de troepen te ondermijnen. Het is dus belangrijk dat we niet enkel de weerbaarheid van onze soldaten tegen desinformatie verzekeren, maar ook die van hun naasten.

Desinformatie: een uitdaging voor het heden en de toekomst

Het is essentieel dat we vooruitkijken en klaar zijn om het hoofd te bieden aan de conflicten van morgen. Toekomstige conflicten zullen zich niet louter beperken tot het "manu militari" bezetten van fysiek terrein, maar de focus zal meer en meer liggen op het beïnvloeden van besluitvorming en sociale identiteit. Een verdere capacitaire ontwikkeling binnen Defensie is dus noodzakelijk om onze troepen in operatie te ondersteunen.

Eerst en vooral moet er aan de hand van opleiding & training op alle echelons voldoende bewustzijn gecreëerd worden met betrekking tot de dreiging van desinformatie voor militaire operaties. De eerste stappen hierin zijn reeds gezet door Ci-MEG met de ontwikkeling van een *Disinformation Awareness*-briefing. Gezien de recente incidenten m.b.t. desinformatie zou deze briefing verplicht moeten deel uitmaken van de *pre-deployment* training van alle detachementen die in operatie vertrekken. In dit kader werd er trouwens ook een gids ontwikkeld voor tactische commandanten die hen praktische tips aanreikt om desinformatie te counteren, evenals een *fake news leaflet* voor familie en vrienden die achterblijven in België.

Een snelle detectie en identificatie van desinformatie en andere propaganda is onontbeerlijk om de dreiging snel en doeltreffend te kunnen counteren. De aanwezigheid van gespecialiseerd personeel in theater blijft in eerste instantie noodzakelijk voor de opvolging van de perceptie van de lokale bevolking over de Belgische troepen maar ook voor de analyse van de conventionele media (kranten, radio & televisie) en andere propagandakanalen. De opvolging van desinformatie in het digitale domein daarentegen kan op kostenefficiënte wijze gebeuren vanuit *reachback* door de DMMAS van de Ci-MEG.

Binnen Defensie bestaat een dringende nood aan integratie van de bestaande structuren die een rol spelen binnen dit verhaal. Heel recent werden hiervoor reeds de eerste initiatieven opgestart door het hoogste niveau van Defensie die een verregaande aanpassing van de bestaande concepten en samenwerkingsverbanden ambiëren. Op deze wijze tracht Defensie de noodzakelijke steun aan de troepen in operatie te verzekeren.

Om deze inspanning en investeringen te optimaliseren, is het eveneens noodzakelijk dat er een permanente en gestructureerde interdepartementale samenwerking op poten wordt gezet met betrekking tot desinformatie. Hedendaagse conflicten beperken zich immers niet enkel tot het militaire domein, maar vereisen een "samenlevingsbrede aanpak van veiligheid" om de hybride dreigingen te counteren, zoals vastgelegd in de EU-strategie voor de veiligheidsunie (juli 2020). Nauwe samenwerking en gestructureerde uitwisseling van informatie met FOD Buitenlandse Zaken is dan ook aangewezen teneinde coherent te kunnen reageren op de dreiging van desinformatie tegenover Belgische belangen in het buitenland.

Ook een internationale integratie ligt voor de hand, aangezien desinformatie via sociale media van nature grensoverschrijdend is. Een eerste noodzakelijke stap hiervoor is dat België lid wordt van het *NATO Strategic Communications Centre of Excellence* te Riga (Letland) om onze kennisontwikkeling en de informatie-uitwisseling binnen dit domein te versterken. Onze buurlanden hebben deze stap reeds gezet. Een doorgedreven samenwerking met het zeer recent door de NAVO opgerichte *Information Environment Assessment Capability* is een logische tweede stap om de verdere uitbouw van deze capaciteit te garanderen. Het is dus duidelijk dat ook de NAVO de impact van desinformatie erkent en de nodige initiatieven neemt om deze dreiging te counteren.

Last but not least: tot nu toe hadden de meeste NAVO-lidstaten een voornamelijk defensieve houding aangaande desinformatie. De focus lag hierbij enerzijds op de detectie en het ontkrachten van vijandelijke desinformatiecampagnes, en anderzijds het vergroten van het bewustzijn en de weerbaarheid van de bevolking met betrekking tot desinformatie. We moeten echter ook voorbereid zijn op conflicten van hogere intensiteit tegen evenwaardige tegenstanders, waarbij psychologische operaties gericht naar de bevolking en strijdkrachten van de tegenstander van groot belang zijn om tactische, operationele of zelfs politiek-militaire strategische objectieven te behalen. Geplande desinformatiecampagnes via sociale media kunnen het middel bij uitstek zijn om deze gewenste psychologische effecten te bereiken. Een meer offensieve *mindset*

in dit domein dient volgens ons absoluut overwogen te worden om een geloofwaardig antwoord te kunnen bieden op de uitdagingen van de toekomst, want enkel op deze manier zullen België en haar partners klaar zijn voor de *battle of the narrative*. De oprichting van *Information Manoeuvre* capaciteiten bij onze Britse en zeer recent ook Nederlandse collega's moet dan ook van nabij opgevolgd worden. Deze voorlopers bieden ons een ideale gelegenheid tot benchmarking om deze noodzakelijke evolutie binnen de Belgische Defensie te implementeren.

Trefwoorden: Desinformatie in militaire operaties, Civil-Military Engagement Group (Ci-MEG)