Convergentie van inlichtingen- en beïnvloedingsoperaties

Peter Schrijver, PhD researcher FMW Breda

'Not too long ago, it was possible to plan military operations without giving much thought to a real-time social media and communication strategy, just as it was possible to scroll through Facebook without having to dodge first-person combat footage and depictions of wartime atrocities', schreven de Amerikanen Peter Singer en Emerson Brooking begin december in een artikel in Foreign Affairs.[1]

Het recente conflict in Gaza, dat op 7 oktober begon met een wrede aanval van Hamas op Israël, toont volgens beide auteurs aan dat fysieke en digitale slagvelden sterk met elkaar verweven zijn. Singer en Brooking zijn niet zomaar tot dit inzicht gekomen. Al in 2018 publiceerden zij het boek *LikeWar* over de invloed van sociale media op conflicten: 'If cyberwar is the hacking of online networks, LikeWar is the hacking of the people on them, using their likes and shares to make a preferred narrative go viral'.[2] Deze wereldwijde *battle of narratives* komt sterk naar voren op socialemediakanalen en in nieuwsprogramma's in binnen- en buitenland.
Een opvallend aspect hierbij is de rol van informatie in de fysieke strijd op de grond, waarbij met name de Israëlische strijdkrachten (IDF) zogeheten informatieactiviteiten inzetten om hun tactische doelen te bereiken. Het verzenden van sms-berichten, waarmee de IDF Palestijnse burgers waarschuwt voor aanstaande bombardementen, was al bekend van eerdere confrontaties. Niettemin vinden er op informatiegebied meer activiteiten plaats. Op de website van de IDF is te lezen dat IDF-operateurs vanuit het Intelligence Collection and Influence Center van militaire inlichtingeneenheid *504* 30.000 telefoongesprekken hebben gevoerd met Palestijnse leiders. Deze leiders is gevraagd hun achterban op te roepen tot evacuatie en tevens hebben de Israëliërs informatie gevraagd over locaties van Hamasstrijders. Unit 504 rapporteerde ook over verhoren van 300 gevangengenomen Hamasstrijders, waarbij relevante informatie over tunnels en gesprekken zo snel mogelijk werd gedeeld met IDF-eenheden aan het front.

Naast de voorbeelden van Unit 504 hebben de Israëliërs, op het snijvlak van inlichtingen- en beïnvloedingsoperaties, acties ondernomen die nog verder gaan. De IDF Spokesperson's Unit plaatste op socialemediakanalen diverse

opnames van telefoongesprekken tussen Israëlische human intelligence-operateurs en hun vaste Palestijnse contacten. In deze opnames deelden de Palestijnen informatie over leden van Hamas die burgers belemmerden om te evacueren, bijvoorbeeld door hun autosleutels af te pakken of hen helemaal niet toe te staan te vertrekken. De Israëliërs publiceerden ook onderschepte telefoongesprekken online waarin Palestijnse burgers klaagden over wangedrag van Hamas, zoals strijders die hulpgoederen in beslag namen. Verder plaatste de IDF een interceptie online van een gesprek tussen twee Hamasstrijders over een mislukte raketlancering door Hamas, waarbij een ziekenhuis werd geraakt in Gaza. Een incident dat veel internationale media aanvankelijk aan de Israëlische luchtmacht toeschreven.

Deze voorbeelden zijn opmerkelijk. De Israëliërs kiezen er bewust voor om informatie die is vergaard via inlichtingenmiddelen (*human intelligence* en *signals intelligence*) op sociale mediakanalen te delen om Hamas hiermee wereldwijd in een negatief daglicht te plaatsen. Dit ondanks het mogelijke afbreukrisico. Immers, de vertrouwelijke relatie tussen de humint-operateur en zijn Palestijnse contact komt in het gedrang, want zal deze persoon in de toekomst opnieuw informatie delen met zijn Israëlische *handler* als hij moet vrezen dat het gesprek op Facebook wordt geplaatst? En hoe zit het met de geheimhouding van de Israëlische interceptiesystemen? Een inlichtingenwetmatigheid is dat als de opponent weet welke mogelijkheden er zijn om af te luisteren, deze wellicht wel twee keer zal nadenken opnieuw informatie te delen over bijvoorbeeld een telefoonlijn.[3]

Hoe opmerkelijk het Israëlische handelen wellicht ook lijkt, het gebruik van ruw inlichtingenmateriaal op sociale media is anno 2023 geen zeldzaamheid meer. Zo publiceren de Oekraïense binnenlandse veiligheidsdienst SBU en de militaire inlichtingendienst HUR geregeld intercepties van telefonerende Russische militairen online. In deze gesprekken keren vaak dezelfde thema's terug: de slechte levensomstandigheden van Russische militairen aan het front, de corruptie van commandanten of gesprekken waarin Russische militairen vertellen over begane oorlogsmisdaden, zoals plunderingen, verkrachtingen en executies.[4] Hiermee ondermijnen de Oekraïense diensten het narratief van rechtmatige Russische aanwezigheid in Oekraïne en tonen zij hun eigen bevolking de essentie van het voortzetten van de strijd tegen de Russische indringer, gezien de wandaden waartoe de Russen in staat zijn.

Welkom in de 21e eeuw, waar inlichtingenmateriaal fungeert als content voor socialemediacampagnes

Welkom in de 21e eeuw, waar inlichtingenmateriaal fungeert als content voor socialemediacampagnes. Deze ontwikkeling transformeert diensten in Israël en Oekraïne, die historisch gezien opereerden vanuit een wereld van geheimhouding, tot deelnemers aan de door Singer en Brooking gedefinieerde battle of narratives. ■

1 Peter Singer en Emerson Brooking, 'Gaza and the Future of Information Warfare', *Foreign Affairs*, 5 december 2023.
2 Peter Singer en Emerson Brooking, *LikeWar. The Weaponization of Social Media* (New York, Eamon Dolan Books, 2018).
3 Robert Clark, 'The protection of intelligence sources and methods', *Intelligence Journal of U.S. Intelligence Studies* (Fall 2016) 61-66.
4 Peter Schrijver, ''The Wise Man Will Be Master of the Stars'': The Use of Twitter by the Ukrainian Military Intelligence Service', *Irregular Warfare Initiative*, 27 June 2023.