Jaargang 190 nummer 10 - 2021

MILITAIRESPECTATOR

THE IMPACT OF BREXIT ON THE UK-NETHERLANDS DEFENCE AND SECURITY COOPERATION

- The art of deception revisited (part 2): the unexpected annexation of Crimea in 2014
- Cyberoperaties in de gray zone

FOTO MCD, AD BIERSTEKER

In *Militaire Spectator* 11-2021 verschijnt onder meer: 'Patrouilles in een notendop. De inzet van landingsvaartuigen voor maritieme veiligheidsoperaties' van Martin Hoekstra. Het einde van de Koude Oorlog luidde voor de Koninklijke Marine een nieuw tijdperk in, waarbij de aandacht verschoof van regulier vlootoptreden naar maritieme veiligheidsoperaties. De zeemacht moest zichzelf traditionele marinetaken als smokkel- en piraterijbestrijding opnieuw aanleren. Tijdens haar deelname aan de antipiraterijmissies nabij Somalië (2008-2017) ontwikkelde de Koninklijke Marine een operatieconcept dat opvallende overeenkomsten vertoonde met de werkwijze tijdens de Indonesische Onafhankelijkheidsoorlog (1945-1949), ruim een halve eeuw eerder. ■

AANKONDIGING KVBK

Mars en Mercuriussymposium 'Slag om Europa <> Slagveld Europa'

Sprekers: Rob de Wijk, Hester Somsen, Frans Kleyheeg en Bart Groothuis
Datum: Woensdag 3 november 2021
Tijd: 14:00 tot 18:00, aansluitend een borrel en maaltijd
Locatie: Generaal-majoor Kootkazerne (Stroe) en online

Aanmelden via: www.marsenmercuriussymposium.nl (of scan de QR-code)

Informatiegestuurd optreden, ja duh?

Logistiek? Kwaliteitszorg? Leidinggeven? Allemaal thema's die hun oorsprong kennen bij Defensie, maar toch bieden ook externe adviesbureaus de cursus 'leidinggeven' aan, waar wij – militairen, defensiemedewerkers – dan op kunnen inschrijven. Best merkwaardig eigenlijk. Ook IGO, informatiegestuurd optreden, is van hetzelfde laken een pak. IGO is helemaal *hot* bij Defensie. Op alle lagen en binnen alle krijgsmachtdelen zijn de staven bezig om hier richtlijnen over te vervaardigen, met vaak als centrale struikelblok: wat is IGO eigenlijk?

Maar laten we de vraag eens omdraaien: hoe opereerde Defensie voordat de recente IGO-hype uitbrak? Inderdaad… op basis van data, inlichtingen en kennis. Iedereen die ooit een operationeel planningsproces heeft doorlopen weet dat zonder inlichtingen het proces niet eens start. Laten we elkaar niet gek maken: wij, Defensie, doen al eeuwenlang aan IGO. Vandaar ook dat velen zo stoeien met de vraag wat IGO is. Immers, hoe leer je Garry Kasparov schaken?

Komt de hype dan uit het niets? Nee, er zijn wel degelijk zaken veranderd, maar dat heeft niet zozeer met IGO te maken. Ten eerste is de informatieomgeving gedigitaliseerd, zaken zijn virtueel geworden, gedematerialiseerd en de aanduiding 'cyber' is niet meer weg te denken. De digitalisering zorgt voor meer toegang tot meer data, meer mogelijkheden om data op te slaan en daar met algoritmes betere trends en analyses uit te halen. Steeds krachtigere computers en geavanceerde software zorgen ook voor het sneller doorlopen van de besluitvormingscyclus, alsook voor een grotere interoperabiliteit tussen de verschillende wapensystem. Ofwel: IGO 2.0 op basis van een gedigitaliseerde informatieomgeving.

Digitalisering van de informatieomgeving zorgt echter ook nog voor een tweede noviteit, namelijk de inzet van informatie als wapen. IGO 2.0 heeft gevolgen voor alle aspecten van de militaire operatie: van inlichtingen verzamelen en de commandovoering tot het uitvoeren van een actie. De gedigitaliseerde informatieomgeving maakt het daarnaast mogelijk om niet alleen de traditionele kinetische operaties uit te voeren, maar ook operaties waarbij wij de opponent beïnvloeden met woorden, foto's en beeldmateriaal. Was dat in het verleden niet zo dan? Zeker, maar de mogelijkheden om groepen te beïnvloeden via sociale media zijn exponentieel gestegen. Waar de psychologische oorlogvoering van de Amerikanen of Russen vroeger de politieke elite kon bereiken zijn dat nu mondiale doelgroepen en daarnaast heeft de verspreidingssnelheid virale eigenschappen. De beïnvloeding in de gedigitaliseerde informatieomgeving ofwel cyberspace overstijgt daarmee ruim de klassieke spionage of contra-inlichtingen, maar blijft toch onder het niveau van geweld.

Maar is dat dan wel een taak voor Defensie? Touché! Laten we ook die vraag eens omdraaien. De voordelen en mogelijkheden van de gedigitaliseerde informatieomgeving gelden niet alleen voor ons, maar ook voor onze opponenten. En dit zijn niet langer enkel statelijke actoren en hun inlichtingendiensten; ook niet-statelijke actoren hebben gemakkelijk en vrijwel zonder kosten toegang tot de digitale snelweg, vanuit het buitenland, of van binnenuit. Het is wellicht waar dat het gebruik van informatie als wapen niet het prerogatief van Defensie is. De vraag die dan rest is wie ons gaat beschermen als de opponent dit wapen wél inzet. ■

KVBK
KONINKLIJKE VERENIGING
TER BEOEFENING VAN
DE KRIJGSWETENSCHAP

UITGAVE
Koninklijke Vereniging ter Beoefening van de Krijgswetenschap
www.kvbk.nl
E info@kvbk.nl
facebook.com/KVBKsecretaris
twitter.com/kvbk1

Secretaris en ledenadministratie
Majoor R. Verheijen MA
E secretaris@kvbk.nl
Nederlandse Defensieacademie (NLDA)
Sectie MOW
Ledenadministratie KVBK
Postbus 90002, 4800 PA Breda
E ledenadministratie@kvbk.nl

De Militaire Spectator is aangesloten bij de European Military Press Association

LIDMAATSCHAP

binnenland	€ 30,00
studenten	€ 22,50
buitenlandtoeslag	€ 5,00

OPMAAK
Coco Bookmedia

DRUK
Wilco Meppel
ISSN 0026-3869

Coverfoto: Nederlandse NH90's (860 squadron Defensie Helikopter Commando) trainen onderzeebootbestrijding in de Engelse wateren rondom Culdrose
Foto: MCD, Gerben van Es

FOTO U.S. NAVY, JANIEL ADAMES

480

The impact of Brexit on the UK-Netherlands defence and security cooperation

W. Sillevis Smitt and A. Willemen

The UK and the Netherlands have a strong defence relationship. Brexit led to new opportunities, but it is clear the relationship is also facing serious challenges.

Verslag Maritieme strategie: 'Rule the Ways'

Maarten Katsman

In Kiel vond het International Seapower Symposium plaats over maritieme strategie. China was de olifant in de kamer, maar voor welke andere uitdagingen staan westerse marines?

524

MILITAIRESPECTATOR

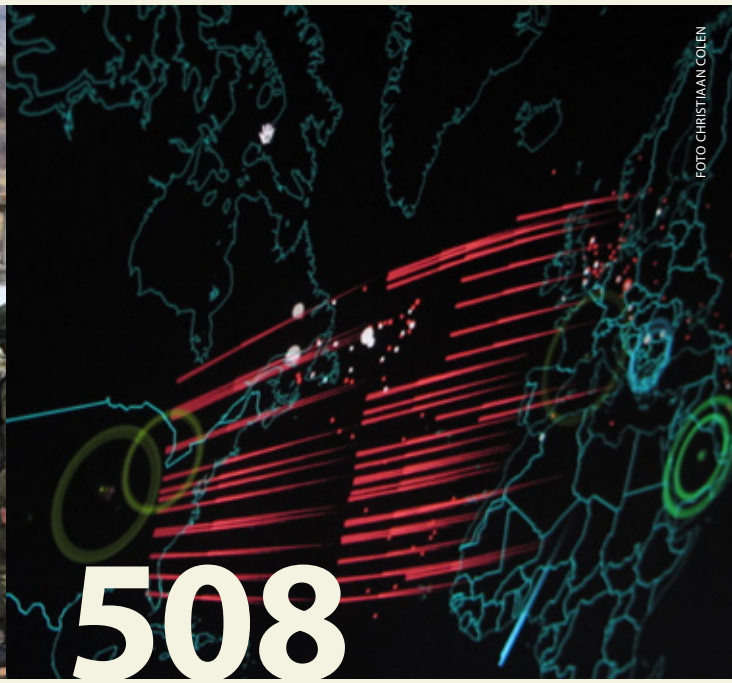
JAARGANG 190 NUMMER 10 – 2021

494

The art of deception revisited (part 2): the unexpected annexation of Crimea in 2014

H. Bouwmeester

How were the Ukrainian authorities deceived during the annexation of Crimea in 2014? Part 2 of the diptych on the art of deception focuses on Russia's application of the concept.



508

Cyberoperaties in de gray zone

W. Bos en P. Pijpers

Wat zijn de juridische grenzen voor activiteiten in de gray zone, en welke rol heeft de Nederlandse krijgsmacht hierin te spelen?

EN VERDER

The impact of Brexit on the UK-Netherlands defence and security cooperation

Captain Wolter Sillevis Smitt and Lieutenant Colonel Alexander Willemen*

The signing of the joint vision statement by the UK Secretary of State for Defence Sir Michael Fallon and the Dutch Minister of Defence Jeanine Hennis-Plasschaert in June 2017 marked a formal step forward to strengthen the bilateral defence cooperation between the UK and the Netherlands. But what has been the impact of Brexit on this relationship in terms of Defence and Security? To understand the strengths and vulnerabilities of UK-NL bilateral defence cooperation at the strategic, operational and tactical levels, the five most relevant of twelve characteristics developed by Zandee et al. for defence cooperation, and Valasek's research on EU military collaboration can be applied. It is clear that Brexit led to new opportunities, but the relationship is also facing serious challenges.

Zr.Ms. Evertsen (left) takes part in the UK Carrier Strike Group 2021

During his State Visit in 2018, amid Brexit uncertainty, His Majesty King Willem-Alexander addressed the House of Commons in the following words: 'Our ties will never be broken. However high the waves may rise, the United Kingdom will always remain an important partner'.[1] While the United Kingdom's (UK) departure from the European Union (EU) has had a significant impact on international relations in Europe, the bilateral defence relationship between the UK and the Netherlands has seemingly continued to flourish. This paper aims to identify the impact of Brexit on the bilateral relationship between the UK and the Netherlands in terms of defence and security in order to better understand why this close relationship endures.

Before identifying the specific strengths and weaknesses of the bilateral relationship between the UK and the Netherlands, a brief outline of the theoretical rationale of defence and security cooperation between nations will be given. For this purpose a conceptual framework of small state behaviour and asymmetric relationships, focusing specifically on military cooperation between the armed forces as a key aspect of foreign policy, will be used. Drawing on public information and current British, Dutch and EU policy documents, this paper will then address British and Dutch defence cooperation policy and its impact upon their bilateral relationship. Finally, it will discuss the opportunities and risks to future defence cooperation resulting from Brexit and then conclude that Brexit has initially increased the UK's appreciation of its long-standing bilateral defence relationships with the Netherlands and other allies, creating new opportunities for cooperation. However, since the UK's departure from the EU remains in practice embryonic, and with the UK and the EU rebalancing their defence and security priorities, uncertainty in bilateral affiliation will remain for the foreseeable future.

* Captain (RNLN) Wolter Sillevis Smitt is an operational Navy Officer with a broad working experience in operations, international relations and human resources. From 2017 – 2020, he was Defence and Naval Attaché at the Netherlands Embassy in London. He was a member of the Royal College of Defence Studies in London. In August 2021 he was appointed Director at the Netherlands Defence College in Breda. Lieutenant Colonel ACDM (Alexander) Willemen is a combat engineer by trade with working experience on the strategical, operational and tactical level. The last three years he acted as the Dutch Exchange Officer at the Concepts Team within the Future Force Developments branch at the British Army Headquarters. Currently he is a member of the Directing Staff at the Dutch Advanced Command and Staff Course in Breda.

1 'Speech by His Majesty the King on the occasion of his visit to the House of Commons and the House of Lords', London, 23 October 2018. See: https://www.royal-house.nl/documents/speeches/2018/10/23/speech-by-his-majesty-the-king-on-the-occasion-of-his-visit-to-the-house-of-commons-and-the-house-of-lords-palace-of-westminster.

PHOTO UK MINISTRY OF DEFENCE

Understanding the UK-Netherlands bilateral relationship

The social theory of international politics describes the behaviour of states in international politics while promoting their national values and interests. Alexander Wendt identifies four interests for a state to survive: physical survival, autonomy, economic well-being, and collective self-esteem. One of the strategies to address these interests is through multilateral and bilateral cooperation.[2] For instance, after the Second World War the Netherlands drastically altered its security policy from neutrality to positively integrating itself fully in the international community. As one of the founders of the North Atlantic Treaty Organisation (NATO) and the EU, it secured both its physical security and economic interests at the cost of reduced autonomy.[3] Alternatively, the UK as a former world player and, arguably, today still formidable power, seems to have some more leeway to prioritise autonomy and self-esteem. Among other motives, such as immigration and living conditions, this seemingly contributed to the slender majority vote to leave the EU.[4]

In their defence and security policies both the UK and the Netherlands seek international cooperation to promote their national security objectives and recognise the importance of their bilateral relationship. The UK's approach to defence engagement, published in 2017, aims to (1) develop understanding, (2) prevent conflict, (3) build capability and capacity, (4) promote prosperity and (5) gain access and influence.[5] Based on these principles and underpinned by the recently published 2021 Defence Command Paper (DCP) – *Defence in a competitive age* - the UK armed forces collaborate extensively with many partners worldwide, both multilaterally and bilaterally.[6] The UK still appreciates the Netherlands as a close ally with whom it has shared views on security threats and extensive bilateral defence initiatives and engagements.[7]

In its 2018 Defence White Paper, the Dutch government recognised the need for increased international defence and security collaboration, especially with the EU, NATO and its six strategic partners, the United States (US), the UK, Germany, France, Belgium, and Norway.[8] The aim was: (1) to support political-strategic objectives, (2) enhance military capabilities, and (3) achieve military efficiency.[9] Cooperation with the UK may serve all these objectives. The Netherlands values its close links with the UK because of its position at the world stage, including its membership of the UN Security Council, the G7 and G20, strong ties with the US, mature intelligence infrastructure, and credible armed forces.

The Dutch approach to its defence and security cooperation is motivated by its relative size within Europe, where the Netherlands may be regarded as 'the biggest of the small, or the smallest of the big powers'.[10] Consequently, the 'small state strategy' of 'harnessing the multilateral order', as described by Hillary Briffa, sufficiently explains the behaviour of the Netherlands.[11] This approach to offset the structural limitations of its capabilities by pooling together with others to benefit from collective security, perfectly encapsulates the Dutch practice of joining several multilateral security constructs, such as the UK-led Joint

2 Alexander Wendt, *Social Theory of International Politics* (Cambridge, Cambridge University Press, 1999) 235.
3 Nick Perre, 'Dutch Strategic Culture-A Case Study', (MA Thesis, Leiden University, 2018) 21-22.
4 Christopher Browning, 'Brexit Populism and Fantasies of Fulfilment', in: *Cambridge Review of International Affairs* 32 (2019) (3) 222–244. See: https://doi.org/10.1080/09557571.2019.1567461.
5 UK Ministry of Defence (MoD), *UK's International Defence Engagement Strategy*, 2017, 20.
6 UK MoD, *Defence in a Competitive Age,* 2021.
7 Linda Dann, 'The Future of the Arnhem Spirit', in: Paul Dimond, Jane Fenoulhet and Elisabeth Salverda (eds.), *North Sea Neighbours-British and Dutch Interaction Over 100 Years* (London, Anglo-Netherlands Society, 2020) 155–56.
8 NL MoD, *2018 Defence White Paper,* 2018. See: https://english.defensie.nl/downloads/policy-notes/2018/03/26/defence-white-paper.
9 NL MoD, 'Kamerbrief 2 33 279 - Internationale Militaire Samenwerking', 2015. See: https://zoek.officielebekendmakingen.nl/kst-33279-16.html.
10 Jorg Noll and René Moelker, 'Netherlands', in: Alexandra Biehl, Heiko Biehl, Bastian Giegerich (eds.), *Strategic Cultures in Europe: Security and Defence Policies Across the Continent* (Wiesbaden, Springer Fachmedien Wiesbaden, 2013) 257. See: https://doi.org/10.1007/978-3-658-01168-0.
11 Hillary Briffa, 'Small States and the Challenges of the International Order', in: Seth Center and Emma Bates (eds.), *After Disruption-Historical Perspectives on the Future of International Order*, CSIS, 2020, 50–59. See: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200901_Bates_History_FullReport_v1.pdf.

King Willem-Alexander and Queen Máxima arrive at the Houses of Parliament during their State Visit in 2018 PHOTO UK PARLIAMENT

Expeditionary Force (JEF)[12] and the French-led European Intervention Initiative, and establishing strategic defence partnerships with several close and significant allies.

The UK and the Netherlands not only acknowledge the general importance of international collaboration, but they also specifically mention each other in their strategic documents, albeit not exclusively. The Netherlands refers to the UK as one of its six strategic partners, whilst the UK commends the Netherlands for being its partner in the JEF and one of the four partners (together with the US, France and Norway) with which it focuses on deep inter-operability.[13] A 2021 House of Lords report on UK Bilateral Defence Cooperation acknowledges the UK-NL bilateral relationship as one of the UK's three primary bilateral defence cooperation relationships with EU-countries (together with France and Germany).[14] Hence, both the UK and the Netherlands specifically appreciate their bilateral partnership in a broader international defence framework.

Strengths and vulnerabilities in the bilateral relationship

Defence cooperation may be established at three different levels of a military operation.[15] First, at the *strategic* level, collaboration includes strategic dialogue, joining and supporting multilateral defence and security structures, and structured cooperation, with a significant impact on a nation's autonomy. Second, *operational* level cooperation covers collaboration at the level of single or multiple (joint) services, participation in operational staffs, operational

12 The Joint Expeditionary Force (JEF) is a pool of high-readiness forces from nine countries – Denmark, Estonia, Finland, Latvia, Lithuania, the Netherlands, Norway and Sweden and the UK, which leads it. These countries share a commitment to democracy, individual liberty and the rule of law as well as a long history of operating together.

13 UK MoD, '*Defence in a Competitive Age*', 19.

14 Claire Brader, 'UK Bilateral Defence Cooperation', London, 2021. See: https://lordslibrary.parliament.uk/uk-bilateral-defence-cooperation/.

15 Daniel Sukman, 'The Institutional Level of War', Real Clear Defense, 2016. See: https://www.realcleardefense.com/articles/2016/05/06/the_institutional_level_of_war_109338.html.

support and deployments, and aligning major investment programmes. Finally, military cooperation on the *tactical* level constitutes improving interoperability through combined operations, training and exercises, personnel exchange programmes, and sharing information.[16]

To understand the strengths and vulnerabilities of UK-NL bilateral defence cooperation at these levels, the five most relevant of twelve characteristics developed by Dick Zandee et al. for defence cooperation, and Tomas Valasek's research on EU military collaboration, will be applied to this case study.[17]

Firstly, Zandee et al. consider geographic proximity and shared history a significant enabler of cooperation. Being 'North Sea neighbours', the UK and the Netherlands share a maritime focus and a vital interest in safe, secure and responsible exploitation of the North Sea. Both are significant stakeholders.[18] Similarly, shared historical experiences add to like-mindedness and a fruitful bilateral relationship. The historical ties between the UK and the Netherlands date back at least four centuries. The two countries are constitutional monarchies with shared bonds and are former colonial powers. Both, traditionally, have a global view, embrace liberal democratic values, and promote the international rules-based order. Several decades of maritime rivalry and war in the 17th century were followed by centuries of close cooperation and a strong friendship. During WWII, the British government offered a safe home to the Dutch Royal family, the Dutch government in exile in London and the Dutch armed forces, who joined the Allied forces in the liberation of Western Europe.[19] As recently as June 2017, the British and the Dutch jointly and amicably commemorated the 350th anniversary of the Raid on Chatham by Admiral the Ruyter

16 Brandon Kinne, 'Defense Cooperation Agreements and the Emergence of a Global Security Network', in: *International Organization* 72 (2018) (4) 803. See: https://doi.org/10.1017/S0020818318000218.

17 Dick Zandee, Margriet Drent and Rob Hendriks, 'Defence Cooperation Models: Lessons Learned and Usability', (The Hague, Clingendael, 2016) 4-6; Tomas Valasek, 'Surviving Austerity-The Case for a New Approach to EU military cooperation', (London, CER, 2011) 17-23. See: https://www.cer.org.uk/sites/default/files/publications/attachments/pdf/2011/rp_981-141.pdf.

18 House of Lords-European Union Committee, 'The North-Sea Under Pressure: Is Regional Marine Co-Operation the Answer HL 137', 10 March, 2015, 78. See: http://www.publications.parliament.uk/pa/ld201415/ldselect/ldeucom/137/13702.htm.

19 The first Dutch Special Forces (KCT) were formed in 1942 in Scotland as No. 2 Dutch Troop. See: Arthur ten Cate and Martijn van der Vorm, *Callsign Nassau. Het moderne Korps Commandotroepen 1989-2012* (Amsterdam, Boom Uitgeverij, 2012) 12.

Dutch amphibious forces exercise in Scotland during Joint Warrior (2019)

in 1667, also known as the Battle of Medway, under the banner 'From fire to friendship' in the presence of their Royalties. Moreover, British units of the Parachute Regiment still contribute yearly to the commemoration of Operation Market Garden near Arnhem. These notable examples indicate the close relationship nurtured by the two countries.

Secondly, Zandee et al. and Valasek argue that a resemblance of strategic cultures stimulates collaboration, especially when deploying the military in operations abroad in the high-end spectrum.[20] A comparison of the strategic cultures of the UK and the Netherlands reveals many similarities but also some significant differences. Both countries favour the same foreign policy orientation, considering NATO as the foundation of collective security in the Euro-Atlantic area. Furthermore, they feel a shared sense of responsibility towards global security, giving precedence to multilateralism and favouring international cooperation.[21] The alignment of strategic culture plausibly enabled the Netherlands to join the UK, the US, and Canada in taking the lead in Regional Command South (RC-South) in Afghanistan in 2006.

On the other hand, differences in strategic cultures present potential vulnerabilities in the relationship between the partners. The nature of the political system in the Netherlands and the persistent hesitation among some political parties to deploy military power regularly result in a reluctance to commit to international missions. These domestic politics contributed to the decision of the Netherlands to stop its commitment to RC-South in 2010 which is arguably why the UK/NL-Amphibious Force has not been deployed more often.[22,23] Generally, the UK could be considered the more forward-

20 Zandee et al., 'Defence Cooperation Models', 4-5. Valasek, 'Surviving Austerity', 21-22.
21 Paul Cornish, 'United Kingdom', in: *Strategic Cultures in Europe*, 371–84.
22 In 2010, after four years of intense allied cooperation, the Dutch coalition government was not able to politically agree on the continuation of Dutch military support to NATO-operations in RC-South.
23 Valasek, 'Surviving Austerity', 17-23.

PHOTO MCD, JASPER VEROLME

Despite the differences between the UK and the Netherlands in size and strategic culture, both have a lot in common

leaning partner of the two, with a military doctrine emphasising a warrior ethos.[24] The Dutch less ambitious defence budget also represents the reluctant military culture of the Netherlands. While these dissimilarities in strategic culture effectuate limitations in deploying forces jointly, other bilateral defence cooperation elements, such as training and education, remain viable.

Thirdly, Zandee et al. recognise joint planning and standardisation of equipment, doctrines, and equipment as vital enablers of defence cooperation at the operational and tactical level.[25] Especially, the British Royal Navy (RN) and its counterpart, the Royal Netherlands Navy (RNLN), have established a long tradition of aligning exercise and training programmes. For instance, the RNLN is a standing partner of the RN's Operational Sea Training (OST) organisation for training crews aboard warships, resulting in commonality in maritime doctrines and procedures. Furthermore, both countries coordinate the equipment programmes of their Marines to ensure interoperability within the UK/NL-Amphibious Force.

A fourth characteristic is the size of the partners. Zandee et al. and Valasek both conclude that cooperation between partners of comparable size will work better than between partners of different size. In its bilateral relationship with the UK, the Netherlands is the minor and secondary partner; in 2020, its GDP was 34 per cent relative to the $3,019 trillion of the UK, its population of 17.2 million is considerably smaller than the 66.4 million in the UK, and its defence spending of $13,1 billion in 2020 is only approximately a fifth of the UK's $61.9 billion.[26] Because of these differences, the bilateral relationship between the UK and the Netherlands is subject to the dynamics of an asymmetric relationship.

Stéfanie von Hlatky captures these asymmetries in her theory of asymmetric security cooperation. She explains the trade-offs that partners might face, especially a potential loss of autonomy in foreign policy decision-making. Challenges could arise if the dominant ally wishes to intervene in response to an international threat, which its secondary allies may not share. Alliance considerations may become a compelling motive.[27] For example, in 2003, the Dutch government found itself in a difficult position when asked by its UK and US allies to support the disputed invasion of Iraq, and did so only politically. However, Hlatky clarifies that minor powers may smartly exploit essential resources for security interdependence, such as geography, capability specialisation and legitimacy. For instance, the Dutch could enhance defence cooperation by leveraging its military presence in the Caribbean and its world-class cyber capabilities.[28]

Finally, Zandee et al. and Valasek argue that defence cooperation's most crucial success factor is trust, confidence and understanding, primarily when operating together. Trust can grow over time and help overcome vulnerabilities related to differences in size.[29] The

24 Margriet Drent, Wouter Hagemeijer and Kees Homan, 'Internationale Militaire Samenwerking: Knelpunten en Kansen', *Clingendael Policy Brief*, no. 6 (2011) 6.
25 Zandee, 'Defence Cooperation Models', 6.
26 Population and GDP (in $) according to the OECD. See: https://data.oecd.org/pop/population.htm and https://data.oecd.org/gdp/gross-domestic-product-gdp.htm#indicator-chart. Defence spending (in $) according to NATO, 'Defence Expenditure of NATO Countries (2014-2021) PR/CP(2021)094, 11 June 2021, 7. See: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210611-pr-2021-094-en.pdf.
27 Stéfanie von Hlatky, 'Theory of Asymmetric Security Cooperation', in: *American Allies in Times of War: The Great Asymmetry*, 15:583–605. (Oxford: Oxford Scholarship, 2013).
28 'Digital Dominance-A New Global Ranking of Cyber-Power Throws up Some Surprises', in: *The Economist*, 19 September, 2020. See: https://www.economist.com/science-and-technology/2020/09/19/a-new-global-ranking-of-cyber-power-throws-up-some-surprises.
29 Zandee, 'Defence Cooperation Models', 4-5.

British and the Dutch armed forces have established activities to build trust and confidence through joint training and exercises (e.g., the yearly Dutch participation in the UK's Joint Warrior exercises), exchange of military personnel between all services, joining each other's staff-colleges, and frequent staff-talks and bilateral meetings. Consequently, despite their differences in size and strategic culture, the British and Dutch armed forces have a lot in common, which has resulted in a solid base for robust close cooperation in defence and security.

As a result, until 2017 the UK-NL defence cooperation mainly evolved at the operational and tactical level and concentrated on long-standing navy-to-navy relations. This includes over 60 years of participation in the Operational Sea Training (OST); almost 50 years of cooperation between the Royal Marines and the Royal Netherlands Marine Corps in the integrated UK/NL-Amphibious Force, collaboration in the Submarine Command Courses, and decades of exchange programmes at staff and tactical levels and in the field of operational education. Consequently, this has enabled a high level of standardisation and interoperability, exchange of personnel and knowledge, and efficient bilateral use of scarce capital resources, such as amphibious ships and helicopters.[30]

Cooperation between respective armies and air forces has also grown; however, not to the extent of the Atlantic-orientated naval and marine cooperation. The Netherlands Army, whose focus is more continental, primarily cooperates with Germany. Because of its equipment, the Royal Netherlands Air Force predominantly cooperates with the US. Nevertheless, the British and Dutch armies and air forces share doctrines and information, exchange personnel, and regularly conduct combined training.

Opportunities and challenges following Brexit

Where operational and tactical cooperation has continuously evolved, political developments have also had strategic implications. The decision of the British government to leave the EU in 2016 has impacted British foreign and defence policy and the political dynamics in this field in Europe. The EU lost a partner with considerable 'hard power' capabilities. The UK separated from the EU, a notable 'soft power' actor, focusing on crisis prevention, crisis management, and post-conflict stabilisation. During Brexit negotiations the subjects of defence and security were hardly mentioned, so 'the formal cooperation with the UK on defence matters will now be subject to strict rules on third-country participation', constraining the UK-EU defence and security cooperation significantly.[31] Consequently, for its European defence and security cooperation the UK now principally depends on NATO, the Joint Expeditionary Force (JEF), its trilateral relationship with France and Germany, and other bilateral initiatives.

As such, it was anticipated that the UK would emphasise the importance of NATO, the JEF, its bilateral relationships, and smaller multilateral formats to limit the negative impact of Brexit on European defence.[32] It followed then that bilateral cooperation with the Netherlands and others received new attention and created new opportunities. The signing of the joint vision statement by the UK Secretary of State for Defence Sir Michael Fallon and the Dutch Minister of Defence Jeanine Hennis-Plasschaert in June 2017 marked a formal step forward to strengthen the bilateral defence cooperation between the UK and NL.[33] It enhanced collaboration at the strategic level by introducing a formal structure for dialogue and an

30 Royal Navy, 'Anglo-Dutch task groups link up in Mediterranean', 25 September, 2020. See: https://www.royalnavy.mod.uk/news-and-latest-activity/news/2020/september/25/20200925-anglo-dutch-task-groups-link-up-in-mediterranean.

31 Claire Mills and Ben Smith, 'End of Brexit Transition: Implications for Defence and Foreign Policy Cooperation', *House of Commons Library Briefing Paper*, no. 9117, 19 January, 2021. See: https://commonslibrary.parliament.uk/research-briefings/cbp-9117/.

32 Ana-Isabel Xavier, 'The impact of Brexit on security and defence multilateralism: more cooperation or overlapping interests?', in: *Marmara Journal of European Studies* 26 (2018) (1) 101–118. See: https://avrupa.marmara.edu.tr/dosya/avrupa/mjes arsiv/vol 26_1/6_Xavier.pdf.

33 UK MoD, 'Defence Secretary Agrees Stronger Partnership with Netherlands', 17 June, 2017. See: https://www.gov.uk/government/news/defence-secretary-agrees-stronger-partnership-with-netherlands.

A Royal Navy helicopter delivers goods to the Dutch Joint Support Ship Zr.Ms. Karel Doorman PHOTO MCD, EVA KLIJN

action plan to direct the deepening and widening of the partnership towards new areas such as cybersecurity and space.[34]

It was not until March 2021 that the British government published a clear post-Brexit vision: the UK's Integrated Review of Security, Defence, Development and Foreign Policy (IR). It outlines the UK's interests concerning sovereignty, security, and prosperity.[35] The IR heralds a step-by-step change in how the UK envisions engaging and operating across the world and stresses the importance of relationships with allies and partners. Following the IR, the DCP sets out what this means for UK's defence.[36] It acknowledges today's threats, the existence of global competition over trade, values and interests and the ways in which new technologies may potentially do damage without fighting in the open. Both papers reiterate the UK's increased global interests while remaining unequivocally committed to European security through NATO, the JEF and strong bilateral relations.[37]

The UK's analysis of the future security environment, as presented in the DCP, predominantly corresponds to the Dutch *Defence Vision 2035* (DV2035).[38] The UK as well as the Netherlands underline the importance of flexibility of action, multi-domain integration, operations below the threshold of war with technology at the heart of the new approach, and international cooperation as a prerequisite. Furthermore, due to the limited size of the Dutch armed forces, there is an increased focus on quality, both in equipment and training, rather than on quantity.

34 Dann, 'The Future of the Arnhem Spirit', 155–58.

35 UK Government, *The Integrated Review 2021*, 16 March, 2021. See: https://www.gov.uk/government/collections/the-integrated-review-2021.

36 UK Government, *Defence Command Paper – Defence in a competitive age*, March, 2021. See: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/974661/CP411_-Defence_Command_Plan.pdf.

37 UK Government *Global Britain in a Competitive Age,* London, 2021; UK MoD, *Defence in a competitive age*, 28-29.

38 NL MoD, *Defence Vision 2035*, 15 October, 2020. See: https://english.defensie.nl/downloads/publications/2020/10/15/defence-vision-2035.

From these similar assessments new opportunities and areas of cooperation on the strategic, operational and tactical level may arise. For example, the two armed forces can join efforts to develop new doctrines and capabilities to operate on the 'future battlefield'. The Netherlands, being the less powerful partner, may continue to smartly exploit its strengths, such as its EU membership, position in the Caribbean, cyber capabilities, and availability of scarce high-end military capabilities, such as air defence frigates and amphibious ships. In this way, the UK and the Netherlands can capitalise on the strong foundations of their bilateral relationship by creating new opportunities to offset some of the disadvantages of the UK's departure from the EU.

The Netherlands, being the less powerful partner, may continue to smartly exploit its strengths

In the maritime domain an already solid naval cooperative relationship will be further enhanced with the current integration of a Dutch frigate, as the only foreign partner alongside the US, into the 2021 UK Carrier Strike Group's operational maiden tour to the Indo-Pacific. The cooperation during this significant deployment underlines the continuation of the close ties between the UK and the Netherlands in the post-Brexit era. Additionally, the need to advance NATO's amphibious capabilities presents an opportunity for increased cooperation in this critical area.[39] Consequently, the two nations are developing a mutual Maritime Roadmap to further enhance structural bilateral maritime collaboration into the next decade.

In the land domain similar opportunities present themselves. The British Army has published its plans as 'Future Soldier – Transforming the British Army', including introducing the Brigade Combat Teams (BCT), a newly-established Army Special Operations Brigade and the introduction of future technologies to modernise and transform its forces.[40] The Army's investment programmes have significant overlap with the Royal Netherlands Army (RNLA) vision of being a robust, agile and reliable partner.[41] Specifically, the further development of the Army's Information Manoeuvre and Unconventional Warfare forces[42], and the choice of the British Army to buy the Boxer multirole armoured fighting vehicle, which is already in use by the Dutch and German Armies, are potentially excellent opportunities for strengthening further bilateral cooperation at the operational and tactical level.

In the air domain the two countries deploy a growing set of similar airframes; F35, Apache, Chinook, MQ9 Reaper, C130, and C17 Globemaster. With a decrease of the strategic air fleet the Dutch-led international A330 MRTT programme could be the impetus for more collaborative programmes. Moreover, the Royal Air Force will make a £2bn strategic investment in the Future Combat Air System (FCAS). The development of this technologically innovative mix of crewed and un-crewed platforms,

39 J.D. Williams, et al. *Unlocking NATO's Amphibious Potential: Lessons from the Past, Insights for the Future* (Santa Monica, CA, Rand Corporation, 2020). See: https://www.rand.org/pubs/perspectives/PEA695-1.html.

40 UK MoD, *Future Soldier – Transforming the British Army*, 22 March, 2021. See: https://www.army.mod.uk/media/11826/20210322-army-future_soldier-publication-final.pdf.

41 RNLA Directorate of knowledge and innovation, 'IMC Strategy 2021-2025: Interoperability as key', Utrecht 2021, 12-13.

42 6th (United Kingdom) Division prepares and generates forces, such as 77th Brigade and 1 ISR Brigade, for both constant competition and war fighting, as well as routinely conducting operations below the threshold of armed conflict in the virtual and physical dimensions.

Dutch infantry exercise with the Boxer armoured vehicle. The British Army also acquires Boxers, creating opportunities for strengthening further bilateral cooperation at the operational and tactical level

PHOTO MCD, JOYCE RUTJES

combined with the current fleet of airframes, provides a fertile basis for further cooperation in training, research, and development.

Finally, with an investment of at least £6.6bn in research and development over the next four years, UK Armed Forces seek to sustain their strategic advantage through science and technology, especially in the cyber and space domain, and full integration across all domains (MDI).[43] The MOD significantly contributes to the joint establishment of the UK National Cyber Force and establishes a new Space command to enhance the UK's military command and control in space.[44] The Dutch Defence Cyber Command and its single services might want to closely monitor these developments and adoptions in new technologies and try to find cooperation in the collective ability to operate as partners in these new domains.

Despite these opportunities, the bilateral relationship between the UK and the Netherlands is also facing the serious challenges of the years ahead. While Brexit signified a blow to European security cooperation, it also spurred renewed interest in developing a more integrated approach to European security, mainly along the French-German axis.[45] New EU

43 Multi Domain Integration (MDI) is the posturing of military capabilities in concert with other instruments of national power, allies and partners; configured to sense, understand and orchestrate effects at the optimal tempo, across the operational domains and levels of warfare (JCN 1/20).

44 The UK NCF is a joint mission of the MoD, the Government Communications Headquarters (GCHQ), and the Secret Intelligence Service (SIS).

45 Øyvind Svendsen, 'Brexit and the Future of EU-Defence: A Practice Approach to Differentiated Defence Integration', in: *Journal of European Integration* 41 (2019) (8) 1003. See: https://doi.org/10.1080/07036337.2019.1622540.

To remain trustworthy partners, intentions need to be followed up by action

initiatives on Common Security and Defence Policy, such as Permanent Enhanced Cooperation, the European Defence Fund and operational EU-deployments, could compete with increased bilateral UK cooperation. For instance, in 2019 the Netherlands did not choose to join the US-UK-led International Maritime Security Construct for maritime stability and security around the Arabian Peninsula, but instead joined the European Maritime Awareness mission, a mission with a similar objective. Moreover, although the EU and UK favour the democratic liberal order, differences may arise in their strategic approaches towards Russia, China, or Iran concerning foreign policy challenges. In case of conflicting interests and scarcity of resources, the Netherlands is likely to follow the EU approach in its foreign and defence policy, which may strain the bilateral relationship.[46]

Other risks relate to the limited resources relative to both British and Dutch ambitions. James identified the 'overstretched Armed and Diplomatic Services' as one of the UK's grand strategic thinking weaknesses, creating challenges to deliver on its high ambitions, including refocusing on new partners and the Indo-Pacific.[47] Likewise, in its DV2035 the Netherlands similarly declared insufficient financial and personnel resources as one of the most pressing issues to be solved.[48] Therefore, the two partners must balance their defence commitments multilaterally and bilaterally. Consequently, shortage of capabilities, money and workforce is a risk, potentially leading to a lack of focus and the inability to deliver on the bilateral opportunities and ambitions, conceivably endangering the relationship.

Finally, the UK as well as the Netherlands should realise that the process of the UK forming a new relationship with the EU is not finished yet. Still, many uncertainties about the future partnership remain, with the risk of a further increase of tensions, for instance, over fisheries, handling the COVID-19 crisis, or Northern Ireland. In 2019 Dutch Prime Minister Mark Rutte reiterated the Dutch commitment to more and closer EU cooperation, 'because if the chaos of Brexit teaches us anything, it's that there's no such thing as splendid isolation'.[49] Therefore, a deteriorating connection between the UK and the EU could become harmful to British-Dutch bilateral relations.

To conclude, this paper sought to identify the impact of Brexit on the bilateral defence relationship between the UK and the Netherlands. Before Brexit, over a long period of time the two countries developed strong bonds between their defence forces, mainly supported by a shared history, close geographic proximity, and a high level of interoperability. Vulnerabilities because of differences in size and strategic culture are compensated through frequent dialogue and trustful collaboration.

While the decision of the UK to leave the EU potentially had a detrimental impact on the bilateral relationship, it has not directly affected

46 Benjamin Martill and Monika Sus, 'Post-Brexit EU/UK-Security Cooperation: NATO, CSDP+, or "French Connection"?', in: *The British Journal of Politics and International Relations* 20 (2018) (4) 846–63. See: https://doi.org/10.1177/1369148118796979.

47 William James, 'Between a Pandemic and a Hard-Brexit', in: *The RUSI Journal* 165 (2021) (7). See: https://doi.org/10.1080/03071847.2021.1889232.

48 *Defence Vision 2035*, 17.

49 Lisa ten Brinke, 'From Cautious Member to Bold Leader? The Netherlands and EU after Brexit', London School of Economics, 11 April, 2019. See: https://blogs.lse.ac.uk/brexit/2019/04/11/from-cautious-member-to-bold-leader-the-netherlands-and-eu-after-brexit/.

PHOTO MCD, LOUIS MEULSTEE

Princess Beatrix and Prince Charles attend the 2019 commemoration ceremony of Operation Market Garden in Ede

defence and security yet. Instead, either country took the opportunity to expand its bilateral defence cooperation in word and deed. During the aforementioned 2018 State Visit, Her Majesty the Queen stated, 'As we continue to work together to ensure peace, prosperity and security, I am confident that this friendship between The United Kingdom and The Netherlands, which we greatly treasure, will continue to deepen, and to prosper'.[50]

However, Brexit is still fresh, and many uncertainties remain, especially if the foreign and security policies of the UK and EU deviate. It is also questionable if the UK and the Netherlands can deliver on the bilateral opportunities, especially because of scarce resources, high ambitions and different international priorities. Building confidence and trust through continuous dialogue and new initiatives will therefore remain essential to continuing a strong and mutually beneficial bilateral relationship. However, dialogue alone will not be enough. To remain trustworthy partners, intentions need to be followed up by action. ■

50 'Speech by HM the Queen at The Netherlands State Banquet', 23 October, 2018. See: https://www.royal.uk/queens-speech-netherlands-state-banquet.

The art of deception revisited (part 2): the unexpected annexation of Crimea in 2014

Colonel Han Bouwmeester, PhD*

'Of course, the Russian servicemen did back the Crimean self-defence forces. They acted in a civil but a decisive and professional manner'.

- Russian President Vladimir Putin, April 17, 2014[1]

This second part of the diptych on the art of deception revisited is about Russian deception and the way it was applied during the annexation of Crimea in 2014. During the annexation, armed soldiers dressed in dark green uniforms without insignias turned up and took control of the Ukrainian peninsula. There was no armed confrontation between these unidentified men and Ukrainian military and security forces. Only a few skirmishes took place in which predominantly armed civilians and paramilitary groups were involved. Who were these 'green' men? Where did they come from? And what were their intentions? Many questions arose, and initially Ukraine and the West struggled to come up with answers. Even now, more than seven years on, it is still highly relevant to reconstruct the annexation to gain a better understanding of Russia's actions, which prompts the following question and focus of this article: How were the Ukrainian authorities deceived during the annexation of Crimea in 2014?

This article begins with an explanation of Russian deception, also known as maskirovka. Obviously, the effects of surprise and manipulated perception play a major role. The article continues with the run-up to the annexation, including the violent demonstrations that took place on Maidan Square in Kiev, followed by a descriptive account of the annexation itself. A display of the deception techniques the Russian authorities used to take over Crimea as non-violently as possible concludes the article.

Maskirovka

The origin of the term maskirovka is disputed. Russian scholars go back to the Battle of Kulikovo, which took place on 8 September 1380.[2] The battlefield, some 120 miles south of Moscow, was the venue where Prince Dmitry Ivanovich Donskoy of Moscow divided his mounted fighters into two groups and thus

* Colonel Han Bouwmeester, PhD is an Associate Professor of military strategy and land operations at the Netherlands Defence Academy

1 President of the Russian Federation, 'Direct Line with Vladimir Putin', Kremlin Website, 17 April 2014. See: http://en.kremlin.ru/events/president/news/20796.

2 Charles Smith, 'Soviet Maskirovka', in: *Air Power Journal* 2 (1988) (1)29.

A military base at Perevalne during the 2014 Crimean crisis. This article looks into Russian deception and the way it was applied during the annexation of Crimea in 2014

PHOTO ANTON HOLOBORODKO

fooled the Mongol Golden.[3] Others believe that maskirovka was merely a military idea dating back to the Czar's Imperial Army in the nineteenth century.[4] Till World War II maskirovka was considered a typical military tool, but that changed during the Cold War when Soviet authorities started employing it as one of many Soviet government activities. In 1966, Russian strategist Major General Vasilii Reznichenko acknowledged that maskirovka was more than simply a military tactic for deception. He defined maskirovka as a 'set of measures that consists of such actions as concealing true targets and installing simulated ones to deceive and confuse the enemy […], and the use of disinformation.'[5] It reflects the mechanisms of hiding and showing as mentioned in part 1 of this diptych.

Evgeni Messner: Creating manageable chaos

After the Cold War the work on subversive warfare written by Russian refugee Evgeni Messner became better known in the Russian Federation. In the early 1920s Messner fled to Yugoslavia after the White Army, in which he served, was defeated by the Bolsheviks. After World War II he emigrated to Argentina, where he established himself as publicist. Messner initially shaped his views during the Russian Civil War, experiencing first-hand combat against an opponent that used irregular methods, terror and propaganda. Later, during World War II, he witnessed guerrilla tactics used by the *Chetniks* in the Balkans whose partisan operations he studied intensively. Messner compiled his experiences in the concept of *myatezh voina*, or subversive warfare, therein expressing his belief that future conflicts would no longer be fought on front lines. Psychological operations were an important element of warfare.[6] Messner emphasized the use of maskirovka in order to destabilize command structures and to create 'fog of war'.[7] The main purpose was to create a manageable form of chaos.[8] While Messner's publications had been officially banned in the Soviet Union because of his anti-Communistic views, it came as no surprise that his writings enjoyed a considerable revival during the Putin era. In 2005, the library of the Russian Military Academy issued a Russian publication, based on the legacy of Messner with the title 'If you want peace, defeat the rebellion!'[9] Today Messner's ideas are taught in Russian officers' training courses.

The long-standing form of maskirovka turned out to be an umbrella concept that encompasses many English terms such as camouflage, concealment, deception, imitation, disinformation, secrecy, stratagem, feints, diversion, and simulation. In order to understand the concept of maskirovka it is vital to grasp the entire concept rather than just its components.[10] The modern version of maskirovka is often applied in the information environment, being part of deceitful strategic communications.[11] The main components of present-day maskirovka are concealment, disguising own activities, and deceit, openly showing off to impress the opponent. The overall aim of maskirovka is to surprise a possible opponent or to create manipulated perceptions. Once maskirovka is applied the challenge is to maintain the opponent's status of surprise.[12] Maskirovka is therefore very similar to deception in general, as was concluded in part 1 of this diptych.

A large part of maskirovka consists of active measures, which was a Soviet term for active intelligence operations with the purpose to

3 Mark Thompson, 'The 600 Years of History Behind Those Ukrainian Masks', TIME Online, 18 April 2014, http://time.com/67419/the-600-years-of-history-behind-those-ukrainian-masks/.

4 Timothy Thomas, *Recasting The Red Star: Russia Forges Tradition and Technology Through Toughness* (Fort Leavenworth, KS (USA), Foreign Military Studies Office, 2011) 107.

5 Vasilii Reznichenko, *Taktika* (Moscow (USSR), Military Publishing Office of Ministry of Defence, 1966) 148.

6 Ofer Fridman, *Russian Hybrid Warfare: Resurgence and Politicisation* (London (UK), C. Hurst & Co. Publishers Ltd, 2018) 49-74.

7 Mirosław Banasik, 'Russia's Hybrid Warfare in Theory and Practice, in: *Journal on Baltic Security* 2 (2016) (1) 165-168.

8 Fridman, *Russian Hybrid Warfare*, 49-74.

9 Evgeny Messner and Igor Marchenkov, *Хочешь мира, победи мятежевойну! Творческое наследие Е. Э. Месснера: Русский путь* (*Khochesh' mira, pobedi myatezhevoynu! Tvorcheskoye nasledive Ye. E. Messnera: Russkiy put'* ('If you want peace, defeat the rebellion! The creative heritage of E. E. Messner: the Russian way') (Moscow (RF), Russian Military Academy Library, 2005).

10 Smith, 'Soviet Maskirovka', 28-39.

11 Joergen Oestroem Moeller, 'Maskirovka: Russia's Masterful Use of Deception in Ukraine', *HUFFPOST Website*, 23 April 2014. See: http://www.huffingtonpost.com/joergen-oerstroem-moeller/maskirovka-russias-master_b_5199545.html.

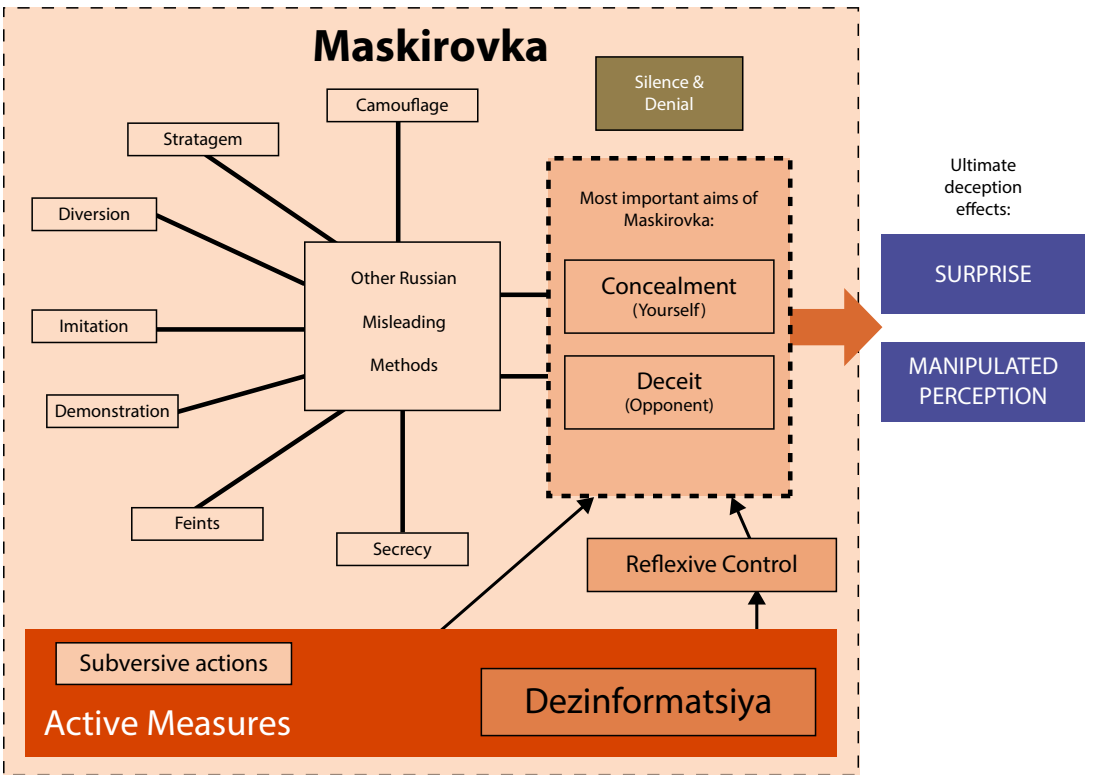


Figure 1 Overview of maskirovka, reflexive control and dezinformatsiya

influence humans or world events in order to reach one's own geopolitical aim. It includes propaganda, subversive actions, counterfeiting official documents, the deployment of agents of influence and exerting different forms of religious suppression.[13] One of the mechanisms used for active measures is reflexive control, particularly used in the information environment to control the decision-making process of an opponent.[14] Reflexive control contains four main elements: (1) putting on power pressure, (2) *dezinformatsiya*, (3) affecting an opponent's decision-making algorithm, and (4) creating time pressure.[15] Reflexive control is not a stand-alone mechanism; the Russian Federation will always harmonize its use with other governmental influence activities. It constantly uses reflexive control, and it does not stop applying reflexive control when operations are over.[16]

One of the means belonging to active measures to exercise reflexive control is dezinformatsiya, the Russian version of disinformation. Dezinformatsiya is the intentional spread of inaccurate or manipulated information by Russian authorities and media with the purpose to deceive other persons. The Soviets already found out that effective dezinformatsiya also needs to contain some credible information, otherwise nobody will trust it.[17]

12 Andrei Grechko and Nikolai Ogarkov, *The Soviet Military Encyclopedia* (1976), English Language Edition, Vol. 1 (Boulder, CO (USA), Westview Press, 1993) 345-346.
13 Aristedes Mahairas and Mikhail Dvilyanski, 'Disinformation - Дезинформация (Dezinformatsiya)', in: *The Cyber Defense Review* 3 (2018) (3) 21.
14 Christian Kamphuis, 'Reflexive Control: The Relevance of a 50-year-old Theory Regarding Perception Control', in: *Militaire Spectator* 187 (2018) (6) 326.
15 Mikhail Ionov, 'On Reflexive Control on the Enemy in Combat', in: *Voyennaya Mysl* (Military Thought), 1 (1995) 46-48.
16 Daniel Bagge, *Unmasking Maskirovka: Russia's Cyber Influence* (New York, NY (USA), Defense Press, 2019) 50.
17 Ladislav Bittman, *The Deception Game: Czechoslovak Intelligence in Soviet Political Warfare*, Syracuse University Research Corporation (New York, NY (USA), Ballantine Books/Random House, 1972) 20.

A prelude to the annexation

After discussing maskirovka in some detail, what comes next is a survey of the events in Crimea and how deception was practised there by the Russian authorities. The series of events started in Ukraine. Years before the annexation of Crimea in 2014, the Russian authorities had set their sights on Crimea because of the many ethnic Russians living in the peninsula and tasked the GRU,[18] Russia's military security service, to deploy a number of its operators in Ukraine and Crimea, using fake Ukrainian-owned companies to gain long-term residency in the Ukraine. Known as the GRU 'fire-starters', these operators were tasked with destabilising the situation in Ukraine by spreading disinformation, creating chaos and confusion, and sometimes provoking incidents.[19] The GRU's influence in Ukraine progressively increased.

Meanwhile Russian unit 26165, known as GRU 85 Main Special Service Centre, home to the Russian military's best mathematical minds and believed to be responsible for hacking campaigns in the investigations into the downing of Malaysian airline MH17 and the 2016 US elections,[20] also employed cyber espionage operations targeting different segments of Ukrainian society. Operation Armageddon began in mid-2013 to target Ukrainian governmental institutions, law enforcement units, military leaders and journalists. This operation occurred just when Ukraine and the EU had started negotiations for economic support. A few months later, in November 2013, an advanced malware named *Snake* infected the Ukrainian Prime Minister's office and several Ukrainian embassies abroad. The operations were constructed in such a manner to avoid discovery and attribution. These advanced espionage techniques provided the Russian authorities with insights into Ukraine's strategic thinking. Furthermore, the Russian authorities used targeted journalists to get a better understanding of public opinion, to identify dissidents and to create channels to disseminate disinformation and pro-Russian messaging.[21]

At the same time Ukrainian President Yanukovych refused to sign a Ukraine-European Union agreement, opting for a Russian bail-out loan and closer ties with the Russian Federation. Russian authorities had offered the Ukrainian President a $15 billion package to buttress the dire Ukrainian economy and a basic debt-remission agreement regarding Russian natural gas deliveries that could have come close to an additional $2 billion.[22] Yanukovych favoured the Russian deal since his constituency in Ukraine comprised an extensive ethnic-Russian element. His decision sparked a series of protests and civil unrest in Ukraine, because most Ukrainians favoured a deal with the EU.[23] During the night of 21 November 2013, Mustafa Nayyem, a Ukrainian journalist of Afghan descent, set up a Facebook account urging people to gather in protest in *Maidan Nezalezhnosti*, the Independence Square in Kyiv. Consequently, at first a few Ukrainians responded to his call, but their numbers rapidly increased in the following days. Most of the demonstrators refused to leave and wanted their government to listen to them.[24] The protests, later called 'Euromaidan', were soon followed by calls for the resignation of the president and his entire government. During the actions the protesters became more and more convinced of widespread government corruption and violations of human rights in Ukraine.[25]

During Euromaidan, protests gradually became violent confrontations in which protesters clashed with the police and the *Berkut*, Ukraine's special police. Meanwhile, the Euromaidan rally

18 GRU stands for *Galvnoye Razvedyvatel'noye Upravelenie* (Main Intelligence Office), the Russian Military Intelligence Service.

19 Jack Laurenson, 'Russian Spies in Ukraine Stoke Kremlin's War, *Kyiv Post Website*, 28 November 2018. See: https://www.kyivpost.com/ukraine-politics/russian-spies-in-ukraine-stoke-kremlins-war.html?cn-reloaded=1.

20 Roland Oliphant, 'What is Unit 26165, Russia's Elite Military Hacking Centre?', *The Telegraph Website*, 4 October 2018. See: https://www.telegraph.co.uk/news/2018/10/04/unit26165-russias-elite-military-hacking-centre/.

21 Azhar Unwala and Shaheen Ghori, 'Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict', in: *Military Cyber Affairs: The Journal of the Military Cyber Professionals Association* 1 (2015) (1) 4-5.

22 Matthew Crosston, *Russia Reconsidered: Putin, Power, and Pragmatism* (Dallas, TX (USA), Brown Books Publishing Group, 2018) 70-72.

23 Yuriy Shveda and Joung Ho Park, 'Ukraine's Revolution of Dignity: The Dynamics of Euromaidan', in: *Journal of Eurasian Studies* 7 (2016) 85-89.

24 David Patrikarakos, *War in 140 Characters: How Social Media Is Reshaping Conflict in the Twenty-First Century* (New York, NY (USA), Basic Books, 2017) 97-101.

25 Shveda and Park, 'Ukraine's Revolution of Dignity', 90-91.

Ukrainian protesters in Maidan Square, Kyiv, 2014

PHOTO EUROPEAN COMMISSION

erupted after the Ukrainian Parliament approved anti-demonstration laws, with the occupation of government buildings across Ukraine as a result. Mid-February 2014 Euromaidan escalated when riot police advanced towards Maidan, using live and rubber ammunition and when Berkut-snipers opened fire at the dissenters. A total of 111 protesters were killed, later often framed by Ukrainian sources as the 'Heavenly Hundred', while 18 police officers were also killed during the confrontation. As a result, Yanukovych, together with the leaders of the parliamentary opposition, signed the 'Agreement on the Settlement of Political Crisis in Ukraine', which came about through mediation of the EU and the Russian Federation. Shortly after signing the agreement Yanukovych fled the country, while the protesters occupied his personal estate and government buildings. Subsequently, the Ukrainian Parliament installed Oleksandr Turchynov, a former secret service chief, until Petro Poroshenko was sworn in as the new Ukrainian President on 7 June 2014.[26] Almost simultaneously, Russian politicians and state media launched an unprecedented propaganda campaign claiming that the United States was behind the protests, without providing any evidence.[27]

During the protests that led to the fall of the Ukrainian President hints of heavy FSB[28] involvement emerged. Ukrainian activists, protesting against Yanukovych, claimed that the FSB, Russia's internal security service, supported

26 Leonid Peisakhin, 'Euromaidan Revisited: Causes of Regime Change in Ukraine One Year On' (Washington, D.C. (USA), The Woodrow Wilson Center/The Kennan Institute, 2015) 4-6; Ivan Katchananovski, 'The "Snipers" Massacre on the Maidan in Ukraine', *Elsevier Website*, August 2015. See: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2658245.

27 Catherine Belton, *Putin's People: How the KGB Took Back Russia and Then Took on the West* (New York, NY (USA), Farrar, Straus and Giroux, 2020) 386.

28 FSB stands for *Federalnaya Sluzhba Bezopastnosti* (Federal Counter-Intelligence Service).

the Berkut as they violently crushed the protests. During the weeks following the Maidan protests, the number of accusations of GRU involvement in the unstable situation in Ukraine grew fast, which would signify a shift in power because Ukraine had long been considered the FSB's territory for gathering intelligence. The media were the first to signal that the GRU got the upper hand over the FSB in Ukraine and Crimea.[29] Russian companies owned property rights in most of the Ukrainian and Crimean telecommunications infrastructure, making it fairly easy for the GRU, and to a lesser extent the FSB, to access and understand telephone calls. This assumption is supported by a text message received by many participants of an anti-Russian demonstration, reading: 'Dear subscriber, you are registered as a participant in a mass disturbance.'[30] This can be interpreted as a form of micro-targeting, not used for political purposes but just to scare the demonstrators.

The unrest in Ukraine ignited a political crisis in Crimea with demonstrations against the new interim government in Ukraine. A number of Crimean inhabitants were afraid that Russia's influence would disappear from Ukraine. The situation rapidly deteriorated. The Crimean parliament was divided; some members of parliament (MPs) wished to join the Russian Federation while others, including the supporters of President Yanukovych, respected the agreement between the Ukrainian president and the Euromaidan protesters.[31] President Putin became highly concerned about the situation in Crimea. On 22 February 2014, Putin organized an all-night meeting with his Chief of Staff, the Secretary of the Russian Security Council, the Minister of Defence, and the chiefs of the Russian intelligence services and in the early hours, at 7 a.m., the decision about the annexation of Crimea was made.[32]

That same day, Sunday 23 February 2014, was not only the final day of the 2014 Winter Olympic Games in Sochi, but also a day that saw several demonstrations, pro-Euromaidan as well as anti-Ukrainian, taking place in Crimea. The notorious Russian motor gang 'The Night Wolves', overtly supported the pro-Russian activists with whom they formed civilian defence squads.[33] The following days pro-Russian protesters blocked the Crimean Parliament, demanding the non-recognition of the Ukrainian government, while at the same time the Regional State Administration in Simferopol was blockaded by hundreds of activists urging for a referendum on secession. On 26 February 2014 clashes took place near the Supreme Council of Crimea in Simferopol between, on the one hand, Crimean Tatars and supporters of Euromaidan and, on the other, pro-Russian demonstrators.[34]

On 27 February 2014 Russian KSO forces,[35] Russian special forces referred to earlier in this article as unidentified men and also known in the Western world as 'little green men', seized government buildings in Simferopol and raised the Russian flag. Russian troops erected barricades, cut off all communication with the buildings and confiscated the telephones of Crimean MPs. Late February 2014, KSO troops took control of the main roads to Sevastopol, and a military checkpoint was established on the highway between Sevastopol and Simferopol.[36] Within a few hours, KSO troops assisted by Berkut isolated Crimea from Ukraine.[37] *ChVK*[38] *Wagner,* a Russian Private Military Company, also appeared in Crimea and acted

29 Stratfor, *Reviving Kremlinology* (Austin, TX (USA), Stratfor Enterprises LLC, 2015) 15.
30 Unwala and Ghori, 'Brandishing the Cybered Bear', 4.
31 Andrew Wilson, *Ukraine Crisis: What It Means for the West* (New Haven, CT (USA), Yale University Press, 2014) 99-117.
32 Крым Путь на Родину (*'Krym Put na Rodinu'* or *'Crimea: Homeward Bound'*), the Russian Documentary on Crimea by *Rossiya-1*, Director: Sergey Kraus, *YouTube Website*, 18 March 2015. See: https://www.youtube.com/watch?v=68CwJVO8U1k.
33 Howard Amos, 'Ukraine Crisis Fuels Secession Calls in pro-Russian South', *The Guardian Website*, 23 February 2013. See: https://www.theguardian.com/world/2014/feb/23/ukraine-crisis-secession-russian-crimea.
34 Interfax Ukraine, 'Ukraine Asking UN to Monitor Security Situation in Crimea Round the Clock, Says Security Service Chief', *Interfax Website*, 26 February 2014. See: https://en.interfax.com.ua/news/general/193029.html.
35 KSO stand for *Komandovanie sil Spetsial'nalnykh Operatsiy* (Russian Special Operation Forces Command). The KSO are considered Tier 1 Special Operational Forces.
36 Mark MacKinnon, 'Globe in Ukraine: Russian-backed Fighters Restrict Access to Crimean City', *The Globe and Mail Website*, 26 February 2014, Updated 12 May 2018. See: https://www.theglobeandmail.com/news/world/tension-in-crimea-as-pro-russia-and-pro-ukraine-groups-stage-competing-rallies/article17110382/#dashboard/follows/.
37 United States Army Special Operations Command (USASOC), *"Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014* (Fort Bragg, NC (USA), 2015) 29-31.

alongside the KSO troops. ChVK Wagner, believed to be registered in Argentina, was formed from the remnants of the 'Slavonic Corps', a mercenary unit with a disgraceful reputation in Syria in 2013.[39] The main training camp of ChVK Wagner located at the Molkino base in the region of Krasnador is also the home base of the 10 *Spetsnaz* Brigade of the GRU.[40] When the annexation began it emerged that GRU unit 74455, also known as Advanced Persistent Threat 28 or Fancy Bear, had created several fake accounts and put a number of posts on Facebook and the Russian version, Vkontakte, named as 'Eastern Front' and 'For Crimean Independence'. The aim of these online activities was to stir up negative feelings towards the government in Kyiv and to alienate the Crimean population from pro-Western parties.[41]

On 28 February 2014 the State *Duma* adopted a bill to change the Russian procedure for adding territory to ensure a smooth transition of Crimea from Ukraine to the Russian Federation.[42] Meanwhile in Crimea, KSO troops placed the airport and state television under pro-Russian supervision. Likewise, they surrounded and blockaded Ukrainian military bases. Ukraine also saw its docked fleet blockaded by Russian naval vessels. Ukrainian headquarters and air defence locations were seized by Russian troops to ensure the security of additional Russian forces arriving by air. Concurrently, Russian authorities ordered so-called 'snap' exercises[43] involving large numbers of Russian conventional army troops on Russian territory along the border with Ukraine and close to the Crimean Peninsula.[44] On 1 March 2014 newly-appointed Prime Minister Aksyonov requested President Putin's assistance in safeguarding peace and public order in Crimea. In response, Putin, authorised by the Federation Council of the Russian Federation, sent in more troops.[45]

The KSO troops in Crimea turned out to be members of 22 Spetsnaz Brigade of the GRU together with elements from 810th Naval Infantry Brigade from Russia's Black Sea Fleet in Sevastopol. These troops were supplemented with well-organised pro-Russian civilians and proxy groups, like ChVk Wagner and the Night Wolves. Russian units that linked up later in Crimea originated from *Vozdushno-Desantnye Voyska* (VDV), the Russian airborne forces, and a reconnaissance regiment.[46] On the Russian mainland, Battalion Tactical Groups in the Southwestern Military District were tasked to conduct the snap exercises along the borders with Ukraine.[47] Overall, such a comprehensive operation requires detailed coordination and

> Effective dezinformatsiya needs to contain some credible information, otherwise nobody will trust it

38 *ChVK* stands for *Chastnyye Voyennyye Kompanii* (*частные военные компании*), which means Private Military Company.
39 Pierre Vaux, 'Fontanka Investigates Russian Mercenaries Dying for Putin Syria and Ukraine', *The Interpreter Website*, 29 March 2016. See: http://www.interpretermag.com/fontanka-investigates-russian-mercenaries-dying-for-putin-in-syria-and-ukraine/.
40 Sarah Fainberg, *Russian Spetsnaz, Contractors and Volunteers in the Syrian Conflict* (Paris (FRA), *Institut Français des Relations Internationales*, 2017) 18.
41 Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (London (UK), Profile Books, 2020) 353.
42 Venice Commission, *Draft Federal Constitutional Law "Amending the Federal Constitutional Law on the Procedure of Admission to Russian Federation and Creation of a New Subject of the Russian Federation in Its Composition" of the Russian Federation*, 10 March 2014, (Strasbourg (FRA), Council of Europe, 2014).
43 A 'snap' exercise is an exercise in which Russian units suddenly start moving troops and equipment, often at night, as if they were about to attack their neighbouring countries.
44 Roger McDermott, *Brothers Disunited: Russia's Use of Military Power in Ukraine*, Monograph (Fort Leavenworth, KS (USA), United States Army, Foreign Military Studies Office, 2015) 11-12.
45 USASOC, *Little Green Men,* 29-31.
46 Mark Galeotti, *Spetsnaz: Russia's Special Forces* (Oxford (UK), Osprey Publishing, 2015) 48-51.
47 USASOC, *"Little Green Men*, 42-52.

central command and control of all the units involved to prevent them from disrupting each other's sub-operations or, worse, from committing fratricide.

On 4 March, President Putin ordered to stop Russian exercises at the borders, while the following day the Russian Navy blockaded the Ukrainian Navy at Novoozerne. In the following two weeks KSO troops together with pro-Russian civilians seized additional sites in Crimea and consolidated their positions.[48] On 16 March 2014, the Crimean Parliament held a highly disputed status referendum on joining the Russian Federation. A large majority of the population of Crimea voted in favour of a connection with the Russian Federation. Russia's President, Vladimir Putin, still denied any Russian involvement, but two days later it was officially announced that Crimea had become part of the Russian Federation.[49] That same day Russian and Crimean representatives officially signed the Treaty on Accession of the Republic of Crimea to the Russian Federation.[50]

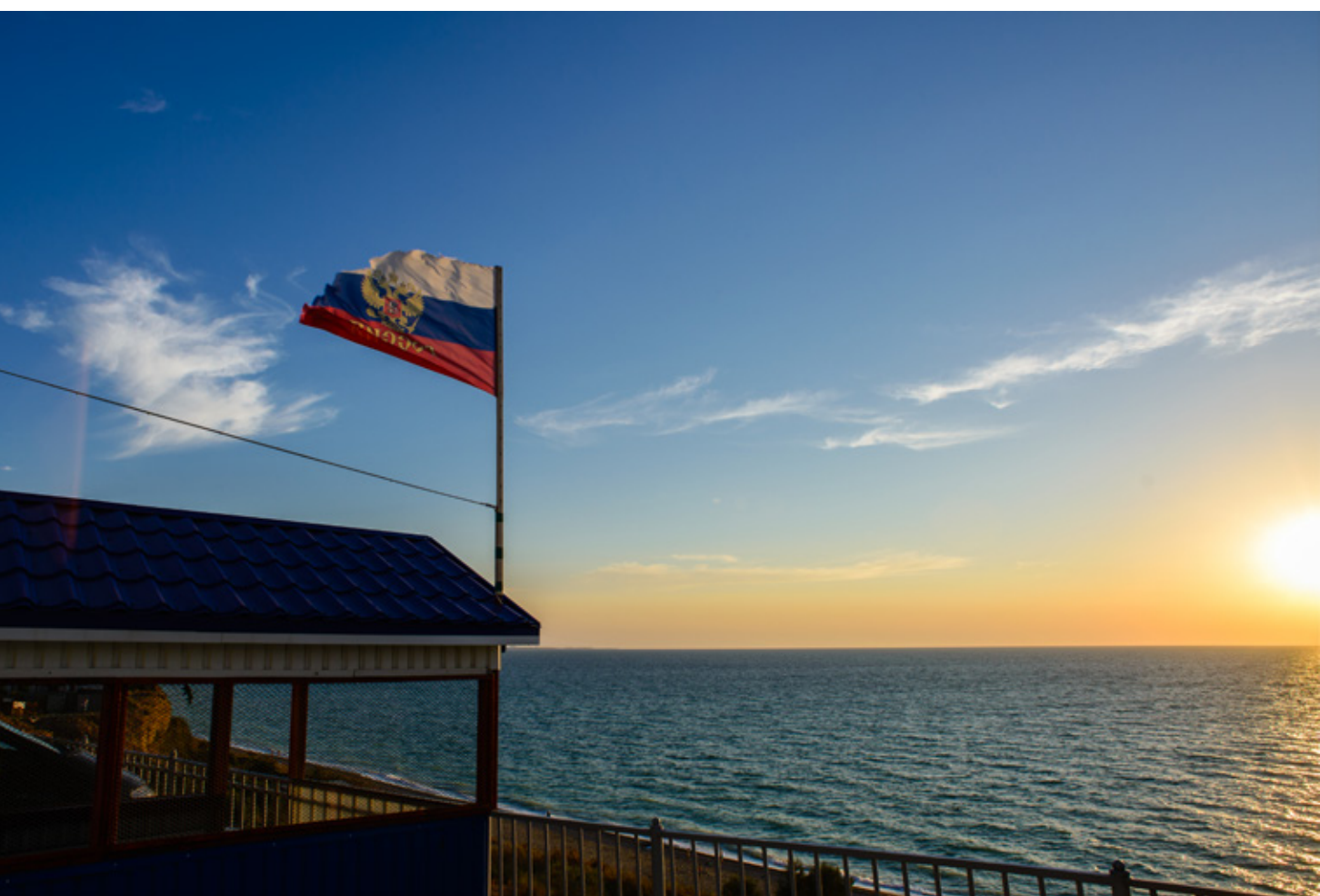
A week after the signing, Ukraine's 22,000 troops in Crimea finally laid down their weapons, exhausted by the annexation, abandoned by their government, and suffering from a severe loyalty crisis. The Ukrainian armed forces collapsed like a house of cards, while Ukrainian security forces stationed in Crimea kept very calm.[51] Reportedly, in total four people died

48 Ibidem, 42-52.

49 Marvin Kalb, *Imperial Gamble: Putin, Ukraine, and the New Cold War* (Washington, D.C. (USA), Brookings Institution Press, 2015) 161-163.

50 President of the Russian Federation, *'Договор между Российской Федерацией и Республикой Крым о принятии в Российскую Федерацию Республики Крым и образовании в составе Российской Федерации новых субъектов'* (The Agreement Between the Russian Federation and the Republic of Crimea on the Admission to the Russian Federation of the Republic of Crimea and the Formation of New Entities in the Russian Federation), *Kremlin Website*, 18 March 2014. See: http://kremlin.ru/events/president/news/20605.

51 Anton Lavrov, 'Russia Again: The Military Operation for Crimea', in: Colby Howard and Ruslan Pukhov (eds.), *Brothers Armed: Military Aspects of the Crisis in Ukraine,* (Minneapolis, MN (USA), East View Press, 2015) 178.



during the annexation of Crimea, two pro-Russians, one pro-Ukrainian demonstrator, and a local Crimean warrior.[52] Furthermore, a Ukrainian soldier was shot by a Russian sniper a few hours after the official signing of the treaty, while another Ukrainian soldier was wounded.[53]

The success of the operation can be measured by the fact that in just a few weeks' time, without firing a single shot, the morale of the Ukrainian troops plummeted and all of their 190 bases on the Crimean Peninsula were surrendered. Instead of relying on a mass deployment of armoured units supported by air power, the Russian authorities deployed fewer than 10,000 troops, mostly naval infantry that were already stationed in Crimea and supplemented with KSO-troops and some airborne units, poised against more than 22,000 Ukrainian troops.[54]

During the annexation of Crimea, Russian authorities were extremely successful in creating a surprise effect as well as maintaining manipulated perception. Ukrainian leaders, and indeed the rest of the world, were aghast when insignificant numbers of unidentifiable soldiers gradually took over control of the peninsula. It certainly took a few weeks to discover who these soldiers and their origin really were. This worked to the advantage of Russian authorities. Meanwhile the Crimean population had decided in a referendum that the peninsula would become part of the Russian Federation. This gave credence to the assertion of Russian authorities that the takeover of Crimea was the will of the local population and that the decision had been taken democratically. A regulated flow of information, speed and secrecy encouraged a surprise effect at the time of the annexation of Crimea which had a crippling effect on the response of the Ukrainian leadership. Its ability to respond quickly and adequately was seriously hampered.

The Russian flag flies in Crimea. During the annexation of Crimea, Russian authorities were extremely successful in creating a surprise effect as well as maintaining manipulated perception

PHOTO NICK S

The media only reported fragments and incomplete images of Russia's operations, while an overview of the situation was missing. The Ukrainian leaders, followed by many Western leaders, wanted a quick explanation for the events. So, an artificial narrative came into being, constructed from information particles and observations, some of which even without further explanation, while large chunks of information were absent. In using allusions to Nazism, Russian media, publicists and various authorities tried to put Ukrainian leadership in a bad daylight.[55] It was an attempt to link the past to the present, focusing on the distortion of history and trying to manipulate people's perception. Maintaining those perceptions was also well taken into account in these Russian actions. It was only six weeks later that President Putin admitted that the Russian Federation was behind the annexation of Crimea.[56]

Applied Russian deception methods

The previous paragraphs have given a comprehensive picture of the Russian takeover of Crimea. The next sections take a closer look at the methods of deception used by the Russian authorities. Many researchers in recent years have focused on partial aspects of Russian deception, but in order to enhance understanding of the Russian deception used, all Russian activities must be considered holistically.

52 J.C. Finley, 'Unrest in Crimea Leaves 2 Dead; Government Buildings Seized', *United Press International Website*, 27 February 2014. See: https://www.upi.com/Top_News/World-News/2014/02/27/Unrest-in-Crimea-leaves-2-dead-government-buildings-seized/6371393516263/.

53 Gavin Williams, 'Introduction: Sound Unmade', in: Gavin Williams (ed.), *Hearing the Crimean War: Wartime Sound and the Unmaking of Sense* (New York, NY (USA), Oxford University Press, 2019) vx.

54 Jānis Bērziņš, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy* (Riga (LTV), National Defence Academy of Latvia, Center for Security and Strategic Research, 2014) 4.

55 NATO's Strategic Communications Centre of Excellence (NATO StratCom CoE), *Analysis of Russia's Information Campaign Against Ukraine: Examining Non-military Aspects of the Crisis in Ukraine from a Strategic Communications Perspective* (Riga (LTV), 2015) 16.

56 President of the Russian Federation, 'Direct Line with Vladimir Putin'.

1. Creating uncertainty

An important condition for creating deception is uncertainty, as discussed in part 1 of this diptych. Both before and during the annexation of Crimea, Russian authorities were able to create periods of great confusion and chaos, resulting in a high level of unpredictability and uncertainty among the Ukrainian population and authorities. During the annexation of Crimea, there were two aspects that caused a great deal of uncertainty.

First, since 2008, Russian authorities had issued passports to ethnic-Russians in Crimea, which caused immense uncertainty.[57] After the Soviet Union collapsed in December 1991, more than 25 million ethnic-Russians became 'compatriots' in new post-Soviet republics.[58] Ukraine harboured almost 8.3 million ethnic-Russians, which was 17 per cent of its total population. Nearly 1.5 million ethnic-Russians lived in Crimea, which was 67 per cent of the total Crimean population.[59] Dual citizenship was forbidden by law in Ukraine, because a second nationality was seen as a threat to the nation.[60] The issue of Russian passports, which also took place prior to the Russo-Georgian armed conflict in 2008,[61] meant that the Ukrainian authorities no longer had a clear picture of their citizens' nationality and what this meant for their loyalty, and they could not oversee the consequences of the random issue. In many cases it could lead to the change of a person's nationality without the officials knowing. The handing out of passports also provided an excuse to the Russian Federation to intervene as soon as ethnic-Russian citizens, the compatriots, were threatened by powers considered to be unfriendly by the Russian government.[62]

Second, the annexation of Crimea took place during the Olympic Games 2014. Here, too, a comparison with the Russian-Georgian armed conflict is evident, as the 2008 Beijing Olympics took place just before the outbreak of this conflict. The Olympic Games in fact provided an ideal cover. All eyes were on the Games while the Russian Federation used the opportunity to start a conflict in a very veiled manner. On 7 February 2014, President Putin opened the 2014 Winter Olympics in the Russian summer resort Sochi with a sparkling show and featured again in the equally impressive closing ceremony on Sunday 23 February 2014.[63] That same day Putin gave his final approval for the annexation, which had without any doubt already been prepared in advance. The Russian annexation of Crimea was a huge wake-up call for the world at large, leading to general surprise and disbelief as the world was initially groping in the dark about Russia's real intentions. It might be pure coincidence, but the Games were of course a perfect distraction for carrying out activities that had to remain hidden for as long as possible.

2. A rapid and stealthy intervention

After the annexation of Crimea, the Western world struggled to find an explanation for the quick take-over of the peninsula. A new element was the intervention of phantom troops, unidentifiable, unassailable, and therefore frightening. The KSO troops and naval infantry wore the new Russian *Ratnik* equipment, thus enhancing the deception effect.[64] At an earlier stage, the pro-Russian civilians had been recruited, organised, equipped and trained by the GRU, which ran a fire starter programme. The Russian authorities denied any involvement, initially at least. The speed of the operation also

57 Anya Tsukanova, 'Cheney urges divided Ukraine to unite against Russia threat', *The Sydney Morning Herald Website*, 6 September 2008. See: https://www.smh.com.au/world/cheney-urges-divided-ukraine-to-unite-against-russia-threat-20080906-4auh.html.

58 Jeff Diamant, 'Ethnic Russians in Some Former Soviet Republics Feel a Close Connection to Russia', *Pew Research Center Website*, 24 July 2017. See: https://www.pewresearch.org/fact-tank/2017/07/24/ethnic-russians-in-some-former-soviet-republics-feel-a-close-connection-to-russia/.

59 Zvi Gitelman, 'Nationality and Ethnicity in Russia and the Post-Soviet Republics', in: Stephen White, Alex Pravda and Zvi Gitelman (eds.), *Developments in Russian and Post-Soviet Politics* (London (UK), The MacMillan Press, Ltd, 1994) 238-246.

60 *Verkhovna Rada* (Ukrainian Parliament), *The Law of Ukraine on Citizenship*, Chapter 1, Article 2 (2008).

61 Alexi Gugushvili, *Country Report: Georgia* (Florence (ITA), European University Institute, 2012) 3-13.

62 Scott Littlefield, 'Citizenship, Identity and Foreign Policy: The Contradictions and Consequences of Russia's Passport Distribution in the Separatist Regions of Georgia', in: *Europe-Asia Studies* 61 (2009) (8) 1478.

63 Oleg Golubchikov, 'From a Sports Mega-event to a Regional Mega-project: the Sochi Winter Olympics and the Return of Geography in State Development Priorities', in: *International Journal of Sport Policy and Politics* 9 (2017) (2) DOI: 10.1080/19406940.2016.1272620.

64 Galeotti, *Spetsnaz*, 56-57.

played a role in the surprise effect. It was a stealth operation; nobody knew what was happening or could officially attribute any action to the Russian Federation. Private Military Companies (PMCs), paramilitary organizations and pro-Russian civilians supported unknown troops and that also made it very difficult to attribute the annexation activities and responsibility to Russian authorities. In 2012 Putin had attempted to legalise PMCs and indicated that PMCs 'constitute an instrument for achieving national [Russian] interests without the direct participation of the authorities'.[65]

3. The use of Nazi symbols and terminology

After Ukrainian President Yanukovych had left office, Russian media tried to frame the new Ukrainian government as the Nazi regime. Evidently in Russian media World War II was still continuing in 2014. Russia's unfinished narrative was based on the notion that 'fascism had not been extinguished', and the general public is called upon to 'defeat the fascists'.[66] Blaming the opponent of Nazi sympathies had to induce an appeal to Russian emotions and to spark certain action. However, the Russian authorities were not very successful in manipulating the Ukrainian citizens. Russians in their homeland and ethnic Russians in Ukraine were sensitive to this defamation, but the Ukrainian leaders were not. Remarkably, Russian media continued their propaganda, although Russian authorities soon deduced that the war rhetoric of the Russian media did not impress non-Russians. They were the perfect audience to influence and to convince of the 'good' Russian intentions, but the excessive use of Nazi symbolism had the opposite effect. Russian media caused disgust amongst the Ukrainian non-Russian population. Making the Ukrainian government suspect of fascist sympathies can be seen as an attempt to create a manipulated perception. However, it did not have the intended effect and can therefore be considered a failed attempt to mislead the Ukrainian population and public opinion.

4. The use of conspiracy narratives

The Putin Presidency, which started (again) in 2012, marked a strong increase in the application of conspiracy theories in the communication of the Russian policy.[67] The annexation of Crimea and later the Ukrainian conflict in the Donbas region were an exceptional stage in the development of the creation and usage of conspiracy theories.[68] The increased production and consumption of anti-Western conspiracy theories became the norm in everyday Russian life. These theories were aimed at creating a sharp dichotomy, like the 'righteous Russians' versus the 'cunning Americans and Westerners supporting the bloody Ukrainian fascists'. The Russian media and public figures, all loyal to the Russian authorities, interpreted Euromaidan as the outcome of subversive Western actions aimed at brainwashing Ukrainian citizens, while intervention in Crimea had been justified by the pretence of protecting compatriots abroad from Ukrainian fascists backed by the West.[69] The conspiracy theories were meant to strengthen the exalted Russian identity in the Russian Federation, but also to instil fear in Crimea and to scare Ukrainian and Crimean leaders, especially those who favoured Western support. Conspiracy theories can be regarded as an essential part of Russia's dezinformatsiya activities to deceive and manipulate decision-makers as well as the general public.

The dissemination of conspiracy theories is not exclusive to present-day Russian authorities. Yet the idea of a possible alternative to the official discourse and the accusation of conspiracy against powerful groups or individuals had always been present below the surface in Russian and Soviet history.[70] A most suitable example of this is the notorious anti-Semitic pamphlet of 'The Protocols of the Elders of Zion', a conspiracy narrative, which was Russian

65 Emmanuel Dreyfus, *Private Military Companies in Russia: Not So Quiet on the Eastern Front?* (Paris (FRA), *Institut de Recherche Stratégique de l'Ecole Militaire*, 2018) 9.

66 NATO StratCom CoE, *Analysis of Russia's Information Campaign Against Ukraine*, 16.

67 Ilya Yablokov, *Fortress Russia: Conspiracy Theories in the Post-Soviet World* (Cambridge (UK), Polity Press, 2018) 183-187.

68 Konstantin von Eggert, 'All Politics are Local: Crimea Explained', in: *World Affairs* 177 (2014) (3) 51-52.

69 Yablokov, *Fortress Russia*, 183-187.

70 Marlène Laruelle, 'Conspiracy and Alternate History in Russia: A Nationalist Equation for Success?', in: *The Russian Review* 71 (2012) (4) 565-567.

in origin. These protocols sketch the image of a number of powerful Jews discussing world domination and were considered to be a reaction to the first Zionist World Congress in Basel in 1897.[71] In the 1920s, Russian *émigrés* spread the protocols to Western Europe and the United States, and thus the protocols found their way in history. New discoveries about the protocols are still hot news in Russian media.[72] This example indicates how long such theories continue to have an effect on history and on people.

5. Large-scale exercises

The large-scale exercises along the border with Ukraine in 2014, in retrospect, contributed to the overwhelming stealth effects of the Russian offensive operations. These exercises were meant to look threatening, foreboding a large-scale Russian attack on Crimea and Ukraine. The Russian exercise in 2014 had all the trappings of a military show of force. These demonstrations are a way of frightening and impressing others in order to evoke an alternative perception and belong to the concept of maskirovka. During the annexation Ukrainian and Crimean authorities no longer knew what to expect from the Russian Federation. What were its intentions?

It was not the first time that Russian authorities used large-scale exercises as a disguise for their operations. Prior to the Soviet invasion at the time of the Hungarian Revolution in 1956 and the invasion of Czechoslovakia in 1968 by the Warsaw Pact, the Soviet Union held major exercises to deter the local authorities. In addition, just before the Yom Kippur War in 1973 in the Middle East, the Egyptian armed forces, assisted by the Soviet GRU-Spetsnaz and regular Soviet personnel, held large-scale exercises to deceive the Israeli authorities.[73] The Russian Federation has since built a reputation for large scale exercises held prior to, or during, military operations it was actively or passively involved in.

6. Increasing activities in cyber space

Over the last two decades the use and abuse of cyber space has increased exponentially. During the annexation of Crimea, the application possibilities of the Internet had increased considerably, and social media platforms were also actively used. The Russian authorities again managed to use vague shadow organizations with criminal reputations, such as CyberBerkut. Now, the methods before and during the annexation were a sophisticated form of micro-targeting, by which demonstrators were personally contacted on their mobile phones during Euromaidan and later during the protest actions in Crimea. Vague on-line criminal organisations using social media make it difficult to link these cyber activities with the Russian authorities, which adds to uncertainty and deception.

7. Maintaining the manipulated perception

In March 2015, NATO's Supreme Allied Commander (SACEUR), General Philip Breedlove, explained to a wide NATO audience that Russia's occupation of Crimea was a massive concern to NATO. Breedlove considered the 'informationally' aspect, which refers to the content as well as the dissemination of information, as the most impressive part of Russia's approach. He emphasized that the Russians were able to exploit a conflict situation and create manipulated perceptions of this situation. In Breedlove's opinion, all they did was to apply the mechanisms of information manipulation: create a false narrative, get this false narrative out quickly and support that false narrative with all the tools that were there.[74] The Russian authorities were able to constantly confront the rest of the world with unexpected activities and to provide only pieces of information. People try to make sense of the world from one moment to the next. Every situation is overloaded with all kinds of information and to make sense of it, the human brain quickly figures out how chunks of

71 Michael Hagemeister, 'The Protocols of the Elders of Zion: Between History and Fiction', in: *New German Critique*, 35 (2008) (1) 83-95; Richard Evans, *The Hitler Conspiracies* (Oxford (UK), Oxford University Press, 2020) 13-20.

72 Hagemeister, 'The Protocols of the Elders of Zion', 83-90.

73 Isabella Ginor and Gideon Remez, *The Soviet-Israel War 1967-1973: The USSR's Military Intervention in the Egyptian-Israel Conflict* (London (UK), C. Hurst & Company Ltd., 2017) 327-346.

74 United States Department of Defense, 'NATO Commander Breedlove Discusses Implications of Hybrid War', *DoD News Website*, 23 March 2015. See: https://dod.defense.gov/News/Article/Article/604334/nato-commander-breedlove-discusses-implications-of-hybrid-war/.

US General Philip Breedlove in Ukraine in 2015. He was NATO's SACEUR at that time and described Russia's annexation of Crimea as a major concern to NATO. Especially the information aspect was impressive, according to Breedlove

PHOTO U.S. ARMY EUROPE

information are connected.[75] Particularly in the security environment, narratives are deliberately created with the purpose of activating a certain feeling, emotion or opinion.[76] This was what Russian authorities did over time, providing the rest of the world with chunks of information, and the Western world was very keen to attach its own perception to that information. Therefore, the Russian authorities managed to sustain the deception effects during and after the annexation of Crimea for at least another month and a half before Russian President Putin himself gave a confirmative answer.

Concluding remarks

The purpose of this article was to provide answers to the question: How were Ukrainian policymakers misled during the 2014 annexation of Crimea? In a nutshell, Ukrainian authorities were confronted with six elements of modern Russian deception warfare, which were instrumental in the quick and smooth takeover of Crimea. These six elements, which must be considered in conjunction with each other, include: (1) creating uncertainty through issuing random Russian citizenship and using a world event as distractor for an intervention, (2) using conspiracy narratives, (3) intervening rapidly and stealthily, (4) staging large-scale exercises, (5) increasing activities in cyber space, and (6) maintaining manipulated perception. Furthermore, the Russian authorities also tried to manipulate the Ukrainians' perception by accusing their leaders of Nazi sympathies, but this attempt ultimately failed. All in all, it can be concluded that with these activities in the Crimean Peninsula, the Russian authorities surprised not only Ukrainian policy makers but also the rest of the world. Moreover, with their holistic approach, the Russian authorities have managed to add a new chapter to the phenomenon of deception in conflicts. ■

75 Rob Brotherton, *Suspicious Minds: Why We Believe Conspiracy Theories* (New York, NY (USA), Bloomsbury Sigma, 2016) 161-173.

76 Beatrice de Graaf, George Dimitriu and Jens Ringmose, *Strategic Narratives, Public Opinion and War* (Abingdon (UK), Routlegde, 2015) 7-8.

Cyberoperaties in de gray zone

Juridische overwegingen omtrent de rol voor de krijgsmacht

Willemijn A. Bos en Peter B.M.J. Pijpers*

Met de doctrine van 'Persistent Engagement' geven de Verenigde Staten aan dat zij in vredestijd naast inlichtingenoperaties ook cyberoperaties buiten de eigen landgrenzen verrichten: een juridisch controversieel thema. Lastig, want terwijl de regelgeving inzake grensoverschrijdende cyberactiviteiten onder het niveau van geweld nog niet is uitgekristalliseerd, vinden juist in deze 'gray zone' de meeste cyberactiviteiten plaats. In dit artikel onderzoeken we de juridische grenzen voor activiteiten in de gray zone, zoals bepaald door de beginselen van soevereiniteit en non-interventie in cyberspace, en tasten we af welke rol de krijgsmacht hierin heeft. Nederland staat voor een dilemma: de krijgsmacht is niet voorbestemd om zonder mandaat op te treden in de gray zone, terwijl opponenten zich hier juist op toeleggen.

Cyberactiviteiten zijn aan de orde van de dag, niet alleen binnen een staat maar ook tussen staten onderling. Of het nu gaat om kwaadaardige software (hierna: *malware*) op een computer zetten; een netwerk vertragen of tijdelijk buiten werking stellen door grootschalige *Distributed Denial of Service* (DDoS)-'aanvallen'; of door het beïnvloeden van de publieke

* Kornet Willemijn A. Bos is jurist en reservist bij de Koninklijke Marechaussee en is vanuit het Defensity College werkzaam geweest bij de NLDA. Kolonel Peter B.M.J. Pijpers is universitair hoofddocent Cyber Operations bij de Faculteit Militaire Wetenschappen aan de NLDA. De auteurs danken lt-kol Arnold MSc, bgen prof. dr. Ducheine & prof. dr. Zwanenburg voor hun reflecties op eerdere versies van het artikel.

1 Zie bijvoorbeeld FireEye, 'APT28: A Window Into Russia's Cyber Espionage Operations?', *Fire Eye Threat Research*, 27 oktober 2014. Zie: https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html.

opinie via gefabriceerde *social media*-berichten. Het scala aan activiteiten dat actoren uitvoeren via cyberspace en het internet is groot, net zo groot als de variëteit aan actoren: van *script kiddies* op zolder tot aan zogeheten *Advanced Persistent Threats* (APT), professionele *hackers* en socialemedia-experts, vaak gelieerd aan statelijke inlichtingendiensten.[1]

Oefening met elektromagnetische en cybermiddelen. Wat zijn de juridische grenzen in de gray zone, en welke rol heeft de krijgsmacht?

FOTO MCD, JARNO KRAAYVANGER

De vraag die de bovengenoemde voorbeelden oproepen is: mag dit wel? Naast politieke en ethische overwegingen gaat het in dit artikel primair om de vraag of dit internationaalrechtelijk (in de relatie tussen staten) is toegestaan. Een vervolgvraag is: en wat betekent dit voor de inzet van de krijgsmacht? Een andere staat de wil opleggen is van oudsher een activiteit waarin het militaire machtsinstrument, veelal de krijgsmacht, een prominente rol heeft, zeker tijdens een gewapend conflict.

Het gros van de cyberactiviteiten vindt echter niet plaats tijdens oorlog en conflict, maar juist onder het niveau van geweld, zoals bedoeld in artikel 2(4) VN-Handvest dat interstatelijk geweldgebruik verbiedt.[2] Juridisch betekent dit, dat noch het *ius ad bellum*, het recht omtrent interstatelijk geweldgebruik,[3] noch het *ius in bello* (humanitair oorlogsrecht), het geldende regime tijdens gewapend conflict, van toepassing zijn. Echter, het feit dat (cyber) activiteiten onder het niveau van geweld blijven, betekent niet dat ze daarom zijn toegestaan onder het internationaal recht. Ook onder het niveau van geweld zijn interstatelijke activiteiten gereguleerd. Zo moet een staat onder meer de soevereiniteit van andere staten respecteren en mag hij zich niet mengen in de interne aangelegenheden van een andere staat – het beginsel van non-interventie.

De vraag naar de rol van de krijgsmacht is daarmee nog interessanter. Waar het prerogatief van de krijgsmacht lag bij conflict en oorlog, zien we in cyberspace – waar de grens tussen oorlog en vrede vervaagt – dat krijgsmachten buiten de landsgrenzen zeer (pro-)actief zijn onder het niveau van geweld; in de zogeheten gray zone.[4] Denk daarbij aan de Russische beïnvloedingsoperaties tijdens de Amerikaanse verkiezingen van 2016 of de eufemistisch genaamde 'persistent engagement' of 'hunt forward'-activiteiten van het U.S. Cyber Command,[5] activiteiten die strategisch interessant, maar juridisch controversieel zijn.[6]

De centrale vraag in dit artikel is: 'wat is het juridische kader voor staten bij grensoverschrijdende operaties in cyberspace onder het niveau van geweld, en welke rol heeft de krijgsmacht in de zogenoemde gray zone'? Het doel van dit artikel is de onduidelijkheid over het optreden in de grijze zone te verkleinen en de discussie over de rol van de krijgsmacht daarin te starten. Eerst staan wij stil bij de vraag wat cyberoperaties zijn om vervolgens het juridisch raamwerk te schetsen voor grensoverschrijdende activiteiten onder het niveau van geweld, met daarbij de nadruk op de beginselen van soevereiniteit en non-interventie. Aansluitend toetsen wij de cyberoperaties aan het juridische raamwerk. Na enkele reflecties op de consequenties voor de krijgsmacht sluiten wij af met een conclusie.

De beperking van dit artikel is dat het cyberoperaties in de gray zone analyseert vanuit internationaal publiekrechtelijk perspectief en daarmee wegblijft van nationale wetgeving, de rol van nationale rechtshandhavers,[7] of van een politieke of ethische duiding. Voor de toepassing van het internationale recht in cyberspace hanteren wij de *Tallinn Manual*.[8] Verder zijn de

2 Harriet Moynihan, 'The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention', *Chatham House*, 2 december 2019, 22.

3 Zoals bijvoorbeeld het geweldsverbod uit artikel 2(4) en de zelfverdedigingsclausule uit artikel 51 van het VN-Handvest.

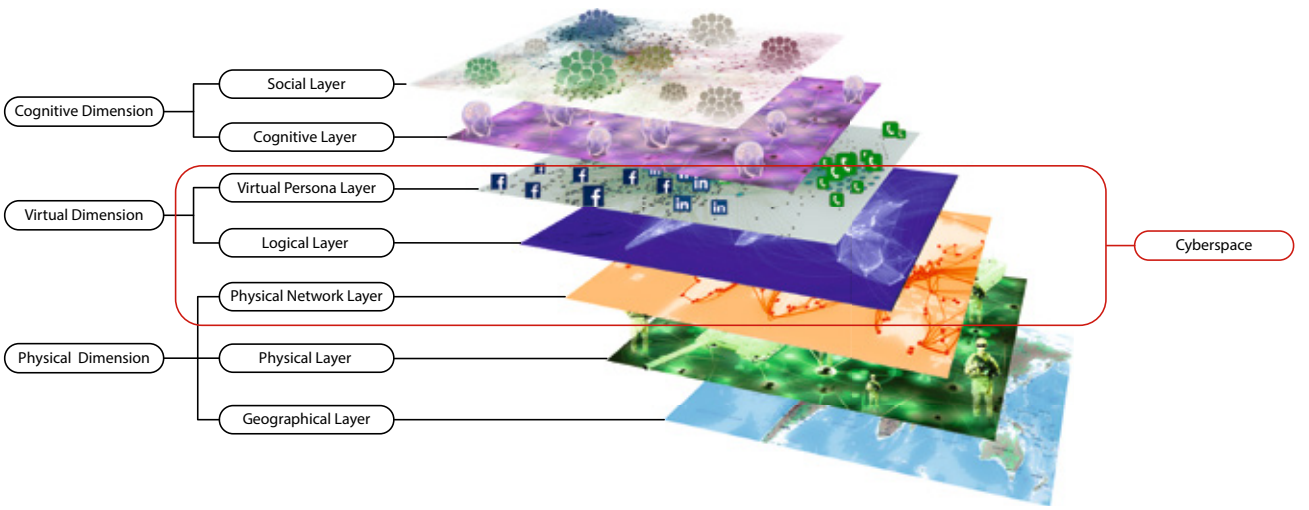
4 Elizabeth G. Troeder, 'A Whole-of-Government Approach to Gray Zone Warfare', *U.S. Army War College SSI*, 26 december 2019, 2; Michael N. Schmitt, 'Grey Zones in the International Law of Cyberspace', in: *The Yale Journal of International Law* 42 (2017) (2) 1–21. Juridisch bestaat het grijze gebied uit a) het vraagstuk of soevereiniteit een beginsel of een bindende verplichting is in cyberspace; en b) of een 'remote cyber operation' die geen schade aanricht wederrechtelijk is.

5 Zie bijvoorbeeld Louk L.C. Faessen en Deborah Lassche, 'Persistent Engagement in het Cyberdomein: Stabilisatie of Escalatie?', in: *Militaire Spectator* 189 (2020) (12) 636–47; Paul M. Nakasone and Michael Sulmeyer, 'How to Compete in Cyberspace: Cyber Command's New Approach', *Foreign Affairs*, 2020; Joshua Rovner, 'More Aggressive and Less Ambitious: Cyber Command's Evolving Approach', *War On The Rocks*, 2020.

6 Michael P. Fischerkeller and Richard J. Harknett, 'Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace', *Lawfare*, 2018; Robert Chesney, 'The Domestic Legal Framework for US Military Cyber Operations', *Hoover Institution Aegis Paper*, 2020; Max Smeets, 'Cyber Command's Strategy Risks Friction With Allies', *Lawfare*, 2019.

7 Te denken valt aan de hack-back bevoegdheid van het Digital Intrusion Team van de politie op grond van wet Computer Criminaliteit III.

8 De *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations* (hierna: *Tallinn Manual*) uit 2017 is een gezaghebbend 'handboek' dat beschrijft hoe het internationale recht van toepassing is op cyberoperaties (tussen staten onderling). Het handboek is geen wetboek, maar geschreven door een internationale groep experts op het gebied van internationaal recht. De opzet van de TM2 is gefaciliteerd en begeleid door het NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE).



Figuur 1 Cyberspace en de informatieomgeving[11]

casus en het juridische kader instrumenteel voor het doel van het artikel en daarmee vereenvoudigd weergegeven.

Cyberoperaties

Een cyberoperatie is voor dit artikel gedefinieerd als een activiteit die effecten genereert in of via cyberspace.[9] Cyberspace bestaat uit een fysiek en een virtueel deel. De virtuele dimensie van cyberspace bestaat uit de 'virtual personae' en de logische laag.[10] Virtual personae geven mensen en organisaties de mogelijkheid om cyberspace te betreden via een digitale identiteit, zoals een e-mailadres of een *username*, en daarmee toegang te krijgen tot de tweede 'logische' virtuele laag. De logische laag bevat de firmware, operating systems, software, applicaties maar ook de data van cyberspace. De virtuele dimensie van cyberspace leunt op de fysieke netwerklaag, bestaande uit fysieke componenten zoals computers, routers en kabels. De drie lagen van cyberspace bevatten tevens de potentiële objecten die relevant zijn voor defensieve en offensieve militaire cyberoperaties.

Cyberoperaties zijn in te delen in hard- en soft-cyberoperaties.[12] Een cyberoperatie die met een digitaal 'wapen' effecten genereert in cyberspace, zoals het veranderen van de software of het manipuleren van data, is een hard-cyberoperatie. Ook het langs digitale weg vernietigen van soft- of hardware valt hieronder. Het gebruikte digitale 'wapen' om objecten en data in cyberspace te manipuleren is code, ofwel een programma van 'nullen en enen'. Soft-cyberoperaties, zoals het beïnvloeden van verkiezingen met desinformatiecampagnes, hebben geen initieel effect in cyberspace, maar gebruiken cyberspace als vector om effecten te bereiken in de cognitieve dimensie – perceptie, begrips- en besluitvorming. Het 'wapen' van soft-cyberoperaties is de inhoud (*content*) van een bericht.

9 Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, Cambridge University Press, 2013) 258; Cyberspace en het cyberdomein zijn inwisselbaar, in dit artikel gebruiken wij cyberspace. Naast het domein van cyberspace bestaan onder meer het land-, lucht-, zee-, en ruimtedomein. Zie voor de dimensies en de domeinen ook de Nederlandse Defensie Doctrine (2019), hoofdstuk 4.

10 Peter B.M.J. Pijpers en Kraesten L. Arnold, 'Conquering the Invisible Battleground', in: *Atlantisch Perspectief* 44 (2020) (4).

11 Figuur 1 is gebaseerd op een indeling van de informatieomgeving gebaseerd op werk van Paul A.L. Ducheine, Jelle van Haaster, and Richard van Harskamp, 'Manoeuvring and Generating Effects in the Information Environment', in: Paul A.L. Ducheine and Frans P.B. Osinga (red.), *Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crisis - NL ARMS 2017*, 2017; Jelle van Haaster, 'On Cyber: The Utility of Military Cyber Operations During Armed Conflict', 2018. Noot: volgens Van Haaster bevat cyberspace ook de 'geographical layer', zie On Cyber, blz. 159.

12 Pijpers en Arnold, 'Conquering the Invisible Battleground'. Zie ook eerdere gedachten hierover in: Paul A.L Ducheine en Jelle van Haaster, 'Cyber-Operaties en Militair Vermogen', in: *Militaire Spectator* 182 (2013) (9) 378.

FOTO GAGE SKIDMORE

Podium voor een campagnebijeenkomst van Hillary Clinton in 2016. De Russische hack van de Democratische Partij en Clintons campagne was een hard-cyberoperatie, daarna volgde een cyberoperatie gericht op de cognitieve dimensie

Om de cyberoperaties tastbaarder te maken en te kunnen toetsen aan een juridisch raamwerk van soevereiniteit en non-interventie, volgen enkele gray zone-casussen van hard- en soft-cyberoperaties;[13] in Oekraïne, Georgië en de Verenigde Staten (VS).

Op 23 december 2015 meldde een Oekraïens regionaal distributiebedrijf storingen in de elektriciteitslevering.[14] Kort na de storing beweerden Oekraïense regeringsfunctionarissen dat de uitval was veroorzaakt door een cyberaanval en dat Russische veiligheidsdiensten, meer specifiek de 'Sandworm'-APT, daarvoor verantwoordelijk waren.[15] Bij deze aanval, waarbij 225.000 klanten gedurende drie uur geen stroom hadden, is gebruik gemaakt van 'BlackEnergy malware' om via e-mails toegang te krijgen tot de controlesystemen van de energiecentrale.[16] Vervolgens is de geïmplanteerde KillDisk-software geactiveerd om data te wissen. Tot slot is de centrale van de buitenwereld afgesloten door het overbelasten van de telefoonverbindingen (Telephony Denial of Service (TDoS)), waardoor zij de storing niet direct waarnam.

Tijdens dit incident op het Oekraïense elektriciteitsnet is voor het eerst een digitaal wapen gebruikt om een elektriciteitsnet met een cyberactiviteit vanuit het buitenland plat te leggen, zonder fysiek in de doelstaat aanwezig te zijn. Vele zouden volgen, zoals in Georgië.[17] Op 28 oktober 2019 zijn meerdere cyberaanvallen uitgevoerd tegen Georgië, door het verstoren, schenden, ongewenst aanpassen (*defacement*) en onderbreken van meer dan 2.000 private en publieke websites waaronder van de nationale televisiemaatschappij. De actie is wederom toegeschreven aan de Sandworm-APT van de Russische militaire inlichtingendienst.[18]

Naast hard-cyberoperaties kan een cyberoperatie zich ook direct richten op de cognitieve dimensie, zonder effecten teweeg te brengen in cyberspace.[19] Het Mueller-rapport, een onderzoeksrapport naar aanleiding van mogelijke verstoring in aanloop naar de presidentsverkiezingen van 2016 in de VS, geeft aan dat de 'Russian government interfered in the 2016 presidential election in sweeping and systematic fashion.'[20] Het gaat daarbij vooral om het lekken van informatie en data rondom presidentskandidate Clinton, na een eerdere hack (een hard-cyberoperatie) in de bestanden van de Democratische Partij en het campagneteam van Clinton, en het stelselmatige uitbuiten van

13 Zie voor meer voorbeelden: https://cyberlaw.ccdcoe.org/wiki/Main_Page of https://www.cfr.org/cyber-operations/. Noot: In de praktijk zijn hard- en soft-cyberoperaties minder goed te scheiden zoals bij de hack-and-leak-operaties, zie James Shires, 'Hack-and-Leak Operations: Intrusion and Influence in the Gulf', in: *Journal of Cyber Policy* 4 (2019) (2) 235–56.

14 Robert Lee, Michael Assante, en Tim Conway, 'Analysis of the Cyber Attack on the Ukrainian Power Grid', *SANS Industrial Control Systems Security Blog*, 2016.

15 De groep Sandworm-APT is onder meer bekend onder de volgende namen: Sandworm Team, Black Energy (/BlackEnergy), Quedagh, Voodoo Bear, TEMP.Noble, Electrum, TeleBots en Iron Viking. Zie ook: United States District Court, Indictment (United States v Andrienko) "Sandworm" (2020).

16 'Cyber Law Toolkit: Power Grid Cyberattack in Ukraine (2015)', CCDCoe, 2020. Zie: https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015).

17 Voor een overzicht zie: Council on Foreign Relations, Cyber Operations Tracker, https://www.cfr.org/cyber-operations/#Timeline.

18 United States Department of State, 'The United States Condemns Russian Cyber Attack Against the Country of Georgia', (2020).

19 Denk daarbij aan beïnvloeding van referenda (2016 Brexit) of verkiezingen (Franse verkiezingen in 2017, verkiezingen VS van 2016 en 2020). Zie bijvoorbeeld: Office of the Director of National Intelligence, 'Foreign Threats to the 2020 US Federal Elections', 2021.

20 Robert S. Mueller, 'Report On The Investigation Into Russian Interference In The 2016 Presidential Election', vol. I and II, 2019, 1.

sociale media door de aan de Russische regering gelieerde 'trollenfabriek' Internet Research Agency (IRA), met als doel 'to provoke and amplify political and social discord in the United States.'[21]

Het juridisch kader

Een staat die, buiten een gewapend conflict, een weloverwogen operatie uitvoert in een andere staat via cyberspace, bevindt zich geenszins in een soort wetteloos Wilde Westen.[22] Een (virtuele) inmenging in een ander land is, net als bij een fysieke ingreep, gebonden aan regels van internationaal recht, in het bijzonder het verbod op interventie en respect voor de soevereiniteit van andere staten.[23] Meerdere rechtsbeginselen reguleren het gedrag van staten, zoals verplichtingen uit mensenrechtenverdragen, het zelfbeschikkingsrecht of *due diligence*.[24] Dit deel beschrijft echter specifiek soevereiniteit en non-interventie omdat de casussen uitgaan van de slachtofferstaat, en daarnaast omdat het specifiek om statelijke actoren gaat. Beide beginselen zijn ook geldig bij activiteiten in cyberspace, met als premisse dat de actie is toe te rekenen aan een staat.

Soevereiniteit

Staten zijn soeverein, ongeacht de grootte of samenstelling ervan.[25] Een gezaghebbende omschrijving van soevereiniteit is die van de arbiter in de Island of Palmas-zaak uit 1928: 'Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.'[26]

Soevereiniteit is derhalve gebaseerd op territoriale integriteit en politieke onafhankelijkheid, inhoudende dat een staat de exclusieve bevoegdheid en beschikkingsmacht heeft over zijn grondgebied, bevolking en activiteiten op dat grondgebied.[27]

Het internationaal publiekrecht is van toepassing op cyberspace,[28] zo ook het principe van staatssoevereiniteit.[29] De *Tallinn Manual* verwoordt dit als volgt: '[a] State must not conduct cyber operations that violate the sovereignty of another State.'[30]

Figuur 2 Cyberaanvallen van Staat A op Staat B

Cyberoperaties kunnen plaatsvinden door Staat A, vanaf het territoir van Staat B, gericht op Staat B. Staat A is dan fysiek al binnengedrongen in het territoir van Staat B (de groene pijlen in figuur 2). De casus rondom schending van territoriale integriteit is dan juridisch relatief eenvoudig en analoog aan een fysieke inbreuk.[31] Een statelijk orgaan van A, dat cyberoperaties uitvoert in (en tegen) Staat B, en aanwezig is zonder toestemming of rechtvaardigingsgrond schendt diens soevereiniteit.

21 Mueller, 'Report on the Investigation', 4.
22 Michael N. Schmitt, 'Taming the Lawless Void: Tracking the Evolution of International Law', in: *Texas National Security Review* 3 (2020) (3) 33.
23 Paul A.L. Ducheine, 'Militar Cyber Operations', in: Terry D. Gill en Dieter Fleck (red.), *The Handbook of the International Law of Military Operations*, 2nd ed. (Oxford, Oxford University Press, 2015) 465-470.
24 Michael N. Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law", in: *Chicago Journal of International Law* 19 (2018) (1) 53-58.
25 Artikel 2(1) VN-Handvest.
26 PCA, Island of Palmas Case (The Netherlands v United States), II Reports of International Arbitral Awards 829–71 (1928) 838.
27 Hieronder valt naast het territoir ook de territoriale zee en het luchtruim boven het territoir en territoriale zee.
28 United Nations GGE 2015 Report, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - A/70/174', vol. 12404, 2015.
29 Niet alle staten zijn overtuigd dat soevereiniteit ook een bindende regel van recht is in cyberspace, zie bijvoorbeeld Jeremy Wright, 'Cyber and International Law in the 21st Century', 2018.
30 Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge, Cambridge University Press, 2017); Rule 4, 17.
31 Schmitt, Rule 4 (6) 18-19. Zie ook: RIIA, Rainbow Warrior (New Zealand v France) (1990). Franse agenten brachten in Nieuw Zeeland een schip van Greenpeace tot zinken.

Lastiger is het bij cyberaanvallen die niet zijn gepleegd vanaf het grondgebied van Staat B, maar 'op afstand'. Naast dat het in de praktijk lastig te bepalen is wie de aanval heeft uitgevoerd,[32] veroorzaken deze *remote cyber-attacks* in ieder geval geen fysieke inbreuk op het territoir van de Staat B.

Om te bepalen of deze remote cyber-attacks een schending van de soevereiniteit op kunnen leveren, noemt de *Tallinn Manual* een aantal toetsingscriteria, opgesplitst naar schendingen van de territoriale integriteit en de politieke onafhankelijkheid; beide kunnen een schending van soevereiniteit opleveren.

Territoriale integriteit is geschonden wanneer bij een actie fysieke schade is ontstaan of gewonden zijn gevallen. Dit kan gebeuren wanneer malware de aansturing van mechanische systemen ontregelt, zoals in de 'Stuxnet'-operatie,[33] waarbij het Iraanse nucleaire verrijkingsprogramma in Natanz het doelwit was. Functionele schade is een tweede criterium. Denk daarbij aan het hacken van een computer en het verspreiden van een virus waardoor computers, harde schijven, routers of hele netwerken niet langer functioneren, wat kan resulteren in de noodzaak om computers of software te vervangen. De 'Shamoon'-cyber-operatie is hier een voorbeeld van.[34] Hoewel de *Tallinn Manual* -experts het eens waren dat verlies van functionaliteit 'schade' oplevert en daarmee een inbreuk op de soevereiniteit kan zijn, bereikten zij geen consensus over de precieze drempel voor functionele schade.[35] Cyberactiviteiten onder het niveau van fysieke of functionele schade, tot slot, kenmerken zich in het vertragen van de processorsnelheid van een computer; een tijdelijke onbruikbaarheid van cyberinfrastructuur of een website; of het kopiëren van gegevens zonder verdere gevolgen. De experts kwamen niet tot overeenstemming of remote cyber-attacks, die geen fysieke of functionele gevolgen hebben, te kwalificeren zijn als een schending van de soevereiniteit.[36]

Naast de territoriale integriteit kan een remote cyber-attack ook de politieke onafhankelijkheid van een staat schenden. Het gaat daarbij om het overnemen van of bemoeienis met inherente overheidsactiviteiten (ofwel: *state functions*),[37] gedefinieerd als 'an activity that is so intimately related to the public interest as to mandate performance by government personnel.'[38] Dit zijn overheidstaken die enkel de overheid kan uitvoeren, gekoppeld aan de vitale belangen van de staat, zoals het houden van verkiezingen, het innen van belasting, de nationale verdediging of rechtshandhaving. Materiële schade is bij deze schendingen via cyberspace niet vereist. Een inbreuk op de politieke onafhankelijkheid vindt plaats bij het (zonder toestemming) overnemen van inherente overheidsactiviteiten.[39] Bijvoorbeeld als Staat A, zonder toestemming van B, verdachten aanhoudt in B, of informatie verzamelt in politiedatabases in Staat B. Naast het overnemen van taken kan ook bemoeienis (*interference*) met de inherente overheidstaken, zoals het platleggen van de site van de belastingdienst waardoor het innen van belasting onmogelijk is, een schending van de politieke onafhankelijkheid en daarmee soevereiniteit opleveren. De grens tussen onrechtmatige en ongezochte bemoeienis is echter lastig te trekken, niet in de laatste plaats omdat staten steeds nauwer samenwerken, bindende verdragen sluiten en deels integreren.

Non-interventie

Het beginsel van non-interventie, een regel van internationaal gewoonterecht, verbiedt staten

32 Essentieel is dat de remote cyber-attack toe te schrijven is aan een staat of een groep onder staatscontrole, immers de notie van soevereiniteit geldt enkel tussen staten. Zie Schmitt, *Tallinn Manual 2.0*, Commentaar bij Rule 4.

33 Jon R. Lindsay, 'Stuxnet and the Limits of Cyber Warfare', in: *Security Studies* 22 (2013) (3) 365-366.

34 Bij deze aanval is het Saoedische staatsoliebedrijf Saudi Aramco zwaar getroffen, zie: Max Smeets, 'The Strategic Promise of Offensive Cyber Operations', in: *Strategic Studies Quarterly* 12 (2018) (3) 93.

35 Schmitt, *Tallinn Manual 2.0*, Rule 4(13) 20-21.

36 Moynihan, 'The Application of International Law to State Cyberattacks - Sovereignty and Non-Intervention', 21-24; Schmitt, *Tallinn Manual 2.0*, Rule 4(14) 21.

37 Schmitt, *Tallinn Manual 2.0*, Rule 4 (15-19) 21-23.

38 U.S. Department of the Interior, Federal Activities Inventory Reform (FAIR) Act of 1998. Zie: https://www.doi.gov/pam/programs/acquisition/fair-activities-inventory-reform-act.

39 Zoals het ontvoeren van Adolf Eichmann door Israël en daarmee de wetshandhavende taak van Argentinië overnemend. Zie: United Nations Security Council, 'Resolution 138 (1960) Question Relating to the Case of Adolf Eichmann', 138 § (1960).

met dwang in te grijpen in de interne of externe aangelegenheden van andere staten. Het interventieverbod is verwoord door het Internationaal Gerechtshof in de bodemprocedure in de zaak tussen Nicaragua en de Verenigde Staten uit 1986: 'A prohibited intervention must … be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.'[40]

De *Tallinn Manual* stelt daarom dat voor cyberspace: 'A State may not intervene, including by cyber means, in the internal or external affairs of another State.'[41]

Om een handeling, waaronder een cyberoperatie, te kwalificeren als onrechtmatige interventie, moet de handeling ten eerste betrekking hebben op die aangelegenheden waarin staten vrijelijk kunnen beslissen, zoals keuzes gerelateerd aan politiek, economie en buitenlands beleid.[42] Dit zogeheten *domaine réservé* is niet onbeperkt omdat staten rekening moeten houden met internationaal bindende verplichtingen,[43] zoals voortkomend uit internationale mensenrechtenverdragen.[44]

Ten tweede moet de handeling *coercive*, ofwel dwingend van aard zijn. Er is geen generieke definitie van dwang in het internationaal recht. In de digitale context suggereert de *Tallinn Manual* dat 'the coercive effort must be designed to influence outcomes in, or conduct with respect to, a matter reserved to a target State'.[45] Cruciaal is dat de handeling het oogmerk heeft om de slachtofferstaat te dwingen een actie te ondernemen die hij anders niet zou ondernemen, of juist daarvan af te zien.[46]

Staten moeten ook bij grensoverschrijdende cyberactiviteiten de beginselen van soevereiniteit en non-interventie respecteren. Echter, doordat de toepassing van de beginselen van soevereiniteit en non-interventie in cyberspace nog niet is uitgekristalliseerd zijn er interpretatie-

FOTO MINISTERIE VAN BUITENLANDSE ZAKEN

Toenmalig minister van Buitenlandse Zaken Bert Koenders nam in februari 2013 de Tallinn Manual 2.0 in ontvangst. Dit handboek behandelt internationaal recht en cyberoperaties

verschillen opgetreden over 'hoe' het recht toe te passen is in cyberspace, waardoor 'normative uncertainty'[47] ontstaat. Deze interpretatieverschillen zorgen ervoor dat het lastig is een eensluidend juridisch oordeel te geven over gray zone- activiteiten, zoals bij onderstaande toetsing zal blijken, te meer omdat handelen van staten in de gray zone niet per definitie onrechtmatig is.

40 Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US) (Merits) [1986] ICJ Rep 14, para 205.
41 Schmitt, *Tallinn Manual 2.0*, Rule 66, 312.
42 Denk ook aan de erkenning van staten en lidmaatschap van internationale organisaties. Zie: Ministry of Foreign Affairs, 'Letter to the President of the House of Representatives on the International Legal Order in Cyberspace - Appendix : International Law in Cyberspace' (2019) 3.
43 PCIJ, Nationality Decrees in Tunis and Morocco - Advisory Opinion, Series B PCIJ Reports (1923) 24; Katja S Ziegler, 'Domaine Réservé', in: *Max Planck Encyclopedia of International Law*, April 2013. Domaine réservé is de 'areas where States are free from international obligations and regulation'.
44 Schmitt, 'Grey Zones in the International Law of Cyberspace', 4.
45 Schmitt, *Tallinn Manual 2.0*, Commentaar bij Rule 66, para 19, blz. 318.
46 Schmitt, *Tallinn Manual 2.0*, Commentaar bij Rule 66, para 19, 21, 27, blz. 318; Zie ook: Ministry of Foreign Affairs, 'Letter to the President of the House of Representatives on the International Legal Order in Cyberspace - Appendix : International Law in Cyberspace' 3.
47 Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law".

Het gros van de cyberactiviteiten vindt niet plaats tijdens oorlog en conflict, maar juist onder het niveau van geweld

Toetsing van cyberoperaties aan juridisch kader

In dit deel toetsen we de eerder beschreven cyberoperaties aan de interpretatie van soevereiniteit respectievelijk non-interventie in cyberspace. Mits toerekenbaar aan een staat zijn de criteria voor een schending van de soevereiniteit en non-interventie als volgt samen te vatten:

Schending van soevereiniteit:
- Is de territoriale integriteit geschonden?
  - Fysieke schade of gewonden;
  - Functionele schade;
  - Acties onder functionaliteitsverlies.
- Of, is politieke onafhankelijkheid geschonden?
  - Overnemen van, of
  - Bemoeienis met inherente overheidsfuncties.

Schending van het non-interventie beginsel:
- Is het *domaine réservé* geschonden?
- Was er sprake van dwang?

De cyberaanval op het Oekraïense elektriciteitsnet

Het platleggen van het Oekraïense elektriciteitsnet in 2015 lijkt op het eerste gezicht een duidelijke zaak. Er is sprake van fysieke schade doordat de geïnstalleerde malware een deel van de ICT-infrastructuur vernielde, en tevens trad functionele schade op door het wissen van bestanden. Activiteiten onder het niveau van functionaliteitsverlies vonden plaats in de vorm van de TDoS aanval en het installeren van malware.[48] Aangenomen dat de schending door een staat, of door een staat gecontroleerde groepen,[49] is verricht, is voldaan aan de criteria voor het schenden van de territoriale integriteit.

Of de politieke onafhankelijkheid is geschonden, hangt af van invulling van het begrip 'inherente overheidstaken'. Energievoorziening, in Oekraïne grotendeels in private handen, valt daar niet onder. De overheid maakt weliswaar energievoorzieningsbeleid, inclusief gerelateerd aan de invoering van nieuwe vormen van energie, maar de elektriciteitsvoorziening als geheel is geen generieke staatstaak.

Een schending van het interventieverbod vereist een inbreuk op het domaine réservé van Oekraïne. Energievoorziening is weliswaar geen 'inherent governmental function', maar valt wel onder het domaine réservé, omdat de rechtsmacht op dit vlak niet is ingeperkt door bindende regels van internationaal recht. Daarnaast moet de interventie op een dwingende wijze hebben plaatsgevonden. Een tijdelijke black-out van de energievoorziening in een ander land kan daar zeker onder vallen.[50] Het vermoeden is dat de Russische Federatie de intentie had Oekraïne te dwingen af te zien van verdere investeringen in alternatieve brandstof, wat ingaat tegen Russische economische belangen.

Concluderend stellen we dat in dit geval de soevereiniteit naar alle waarschijnlijkheid is geschonden op grond van een inbreuk op de territoriale integriteit. Mogelijk heeft er ook een onrechtmatige interventie plaatsgevonden.

48 Przemysław Roguski, 'Violations of Territorial Sovereignty in Cyberspace — an Intrusion-Based Approach', in: Dennis Broeders en Bibi van den Berg (red.) *Governing Cyberspace*, 2020, 65–84.

49 Zie ook: Jake Styczynski and Nate Beach-Westmoreland, 'When the Lights Went Out', 2019; Tatiana Jancarkova and Kubo Macak, 'Cyber Law Toolkit: Scenario 03 - Cyber Operation against the Power Grid', CCDCoe, 2021. Zie: https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015).

50 Harriet Moynihan, 'Cyberspace: Sovereignty and Non-Intervention', *Just Security*, 2019. Zie de sectie over 'principles of non-intervention'. *Coercion* houdt dan onder meer in 'cyber-attacks on another state's critical infrastructure such as disrupting transport services, causing temporary black-outs, or restricting access to government websites'.

Cyberaanvallen op Georgië

Georgië was in oktober 2019 slachtoffer van een grootschalige cyberaanval. Van de aanval is niet bekend of materiële schade is ontstaan. De aanval betrof een defacement, een ongewenste aanpassing van websites, die in principe geen schade met zich meebrengt. Er is ook, voor zover bekend, geen sprake van functionele schade aan de cyberinfrastructuur. Desondanks had de actie significante gevolgen in Georgië: meer dan 2.000 overheids- en private websites waren (tijdelijk) ontoegankelijk waardoor veel Georgiërs hinder ondervonden. En dergelijk aanval op Georgië zou kunnen vallen in de laagste categorie zoals beschreven in de *Tallinn Manual*, namelijk onder het niveau van functionaliteitsverlies.

Naast de mogelijke schending van de territoriale integriteit door deze remote cyber-attack kan ook de politieke onafhankelijk van Georgië zijn ondermijnd. De cyberaanvallen ontsierden naast websites van private partijen en van non-gouvernementele organisaties ook sites van de centrale overheid en de rechterlijke macht, en er vielen uitzendingen van de staatsomroep stil.[51] De laatste categorie kan onderdeel uitmaken van de inherente overheidstaken. Daarnaast moet de aanval tot doel hebben die overheidstaak over te nemen of te verstoren, wat het geval is als de overheid via de getroffen websites publieke informatie communiceert.[52] Dit is echter lastig te beoordelen, omdat de Georgische overheid geen nadere toelichting op de effecten van de aanval heeft gegeven. Als de overheid een van haar taken niet meer had kunnen uitvoeren door deze cyberaanval, was er sprake geweest van soevereiniteitsschending op grond van een inbreuk op de politieke onafhankelijkheid.

Het domaine réservé van Georgië is met deze aanval geraakt. Onder het domaine réservé valt immers de bevoegdheid om wetgeving en overheidsbeleid vast te stellen dat ook het verkeer van private partijen reguleert.[53] De interventie is onrechtmatig als de schending van het domaine réservé op een dwingende wijze is verlopen.[54] Of dat in de Georgië-casus van toepassing is, is moeilijk te achterhalen. Rusland ontkent dit in ieder geval: 'Russia did not plan, and is not planning to, interfere in Georgia's internal affairs in any way.'[55]

Al met al zou de Georgische soevereiniteit kunnen zijn geschonden. De territoriale integriteit is aangetast maar vermoedelijk niet geschonden omdat er geen fysieke of functionele schade ontstond. Wel is het mogelijk dat de politieke onafhankelijkheid is geschonden, omdat een onrechtmatige bemoeienis met de inherente overheidsfuncties heeft plaatsgevonden. En hoewel het domaine réservé wel is aangetast, is een schending van het interventieverbod niet te bewijzen.

Beïnvloeding van de Amerikaanse presidentsverkiezingen

In de aanloop naar de presidentsverkiezingen van 2016 zijn computers gehackt en zijn de gestolen data gelekt, maar bovenal zijn sociale-mediaplatforms gebruikt om de maatschappij te ontwrichten, te polariseren en twijfel te zaaien bij de Amerikaanse kiezers.

Los van het binnendringen in de computers van de Democratische Partij, is het beïnvloeden van de Amerikaanse verkiezingen via sociale media primair een 'remote' soft-cyberoperatie die het territorium niet schendt. Bij gebrek aan fysieke of functionele schade maakt de beïnvloeding van de Amerikaanse verkiezingen daarom geen inbreuk op de territoriale integriteit. Omdat verkiezingen een inherente overheidsfunctie zijn, kan het bemoeilijken hiervan wel in strijd zijn met het beginsel van politieke onafhankelijkheid.

51 UK Government, 'UK Condemns Russia's GRU over Georgia Cyber-Attacks', 2020. Zie: https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks.

52 Denk aan overheidscommunicatie over of crisismanagement tijdens Covid-19. Zie: Marko Milanovic en Michael N. Schmitt, 'Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic', in: *Journal of National Security Law & Policy* 11 (2020) 255.

53 Ziegler, 'Domaine Réservé', Bullet 2.

54 *Tallinn Manual 2.0*, Commentaar bij Rule 66, para 21; zie ook Ministerie van Buitenlandse Zaken, 'Letter to the President of the House of Representatives on the International Legal Order in Cyberspace – Appendix: International Law in Cyberspace', 5 juli 2019, 3.

55 Margarita Antidze en Jack Stubbs, 'Georgia, Backed by U.S. and Britain, Blames Russia for "paralyzing" Cyber Attack', *Reuters*, 2020. Zie: https://www.reuters.com/article/us-georgia-cyber-idUSKBN20E1W3.

FOTO MCD, VALERIE KUYPERS

Ook in cyberspace is het de taak van de krijgsmacht om de internationale rechtsorde en andere vitale belangen te beschermen. Voor de marechaussee is er bijvoorbeeld een rol in rechtshandhaving

De Russische beïnvloeding raakt een bevoegdheid uit het domaine réservé. Verkiezingen organiseren is een inherente overheidstaak, maar hoe een staat zijn verkiezingen regelt, is een onderdeel van zijn rechtsmacht, en daarmee het domaine réservé voor zover dit niet is ingeperkt.[56] De vraag is echter of de Russische acties coercive waren. Hier is geen eensluidend antwoord op te geven. De Russische intentie om de acties op een weloverwogen manier uit te voeren, is hoogstwaarschijnlijk aanwezig,[57] maar of Rusland het doel had het Amerikaanse beleid te veranderen op een manier die de Amerikanen niet zelf hebben gewild, blijft de vraag. Mogelijk is er geen dwang toegepast bij de beïnvloeding, maar de beïnvloeding via de socialemediaplatforms was wel manipulatief. Doordat Russische agenten gebruik maakten van onbewuste wijze van beïnvloeding (middels heuristieken) en zich voordoen als Amerikanen,[58] zijn de onafhankelijke keuzes en vrije wil van de kiezer ondermijnd, waardoor een zekere mate van dwang niet te ontzeggen is.

De conclusie is dat op basis van de hier gepresenteerde data de territoriale integriteit niet geschonden is, maar dat de soevereiniteit

56 Zo heeft in de EU iedere burger actief en passief kiesrecht bij de gemeenteraadsverkiezingen in de lidstaat van verblijf, ex. artikel 40 van het Handvest van de Grondrechten van de Europese Unie (2012/C 326/02).

57 Thomas Paterson en Lauren Hanley, 'Political Warfare in the Digital Age: Cyber Subversion, Information Operations and "Deep Fakes"', in: *Australian Journal of International Affairs* 74 (2020) (4) 443.

58 United States Senate Committee on Intelligence, 'Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election - Volume 2: Russia's Use of Social Media', vol. 2, 2019, 30.

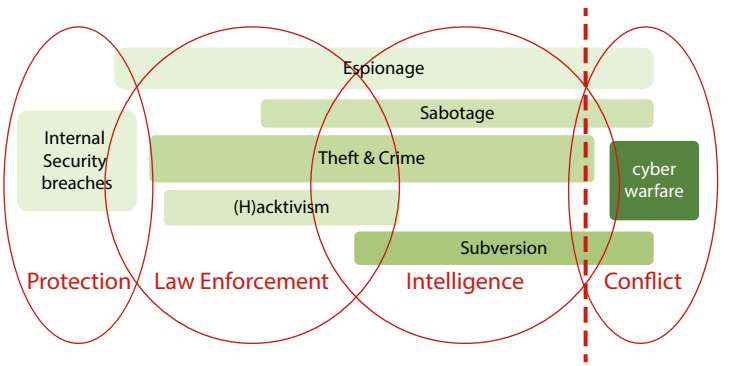
mogelijk wel geschonden is door een inbreuk op de politieke onafhankelijkheid door de bemoeienis met de verkiezingen, wat een inherente overheidstaak is. Of de inmenging ook een interventie heeft opgeleverd is lastig aan te tonen.

Reflectie op de rol van de krijgsmacht

Veel hedendaagse conflicten vinden plaats in de gray zone. Dit zijn grensoverschrijdende assertieve activiteiten onder het niveau van geweld. Uit de besproken casus komt naar voren dat, ondanks de onzekerheid over 'hoe' het internationale recht op cyberspace toepasbaar is, cyberoperaties al snel het soevereiniteitsbeginsel en/of het non-interventiebeginsel schenden.

Mede als gevolg van de onzekerheid en interpretatieverschillen ontstaat er een tweedeling tussen staten die de gray zone daardoor als een kans zien, en staten die zich geremd voelen om op te treden. De activiteiten in de gray zone vertroebelen nog verder omdat bij veel van deze remote cyber-attacks juist militaire cybereenheden of inlichtingendiensten opererend via cyberspace een prominente rol spelen, zoals de Russische GRU[59] of het Amerikaanse NSA/Cyber Command.[60]

Hoewel er een internationaalrechtelijk juridisch kader is, blijkt dat toepassing ervan op cyberacties in de gray zone lastig is. Feit is wel dat actoren actief zijn in de gray zone, ook tegen Nederland. De vraag is vervolgens welke rol de Nederlandse krijgsmacht heeft in de gray zone. Cyberspace lijkt ver weg te staan van de traditionele taak van de krijgsmacht: het verdedigen van het Koninkrijk. Is de krijgsmacht daarmee uitgespeeld? Nee, zeker niet! Ook in cyberspace is het de taak van de krijgsmacht om de internationale rechtsorde en andere vitale belangen te beschermen en waar mogelijk te bevorderen. Paul Ducheine c.s. onderkennen hierbij enkele rollen (of paradigma's) voor de krijgsmacht in cyberspace;[61] een beschermingstaak gericht op eigen (defensie-)ICT-infrastructuur; rechtshandhaving door de marechaussee, een inlichtingen- en veiligheidsrol van de



Figuur 3 Cyber Security Paradigms[63]

Militaire Inlichtingen- en Veiligheidsdienst en een conflict-gerelateerde rol van het Defensie Cybercommando (DCC).[62]

Het model in figuur 3 geeft vier paradigma's van staatsoptreden weer. Ieder paradigma vertegenwoordigt een institutioneel raamwerk waarbinnen de staat kan optreden, op basis van een vigerend rechtsregime.[64] Het paradigma conflict geeft de militaire operaties in cyberspace weer, zowel oorlogvoering als de inzet van de krijgsmacht voor stabilisatie- of vredesmissies in cyberspace.[65]

De paradigma's maken niet specifiek onderscheid naar inzet boven of onder het niveau van geweld, dan wel nationale of internationale

59 GRU (Glavnoje Razvedyvatel'noje Upravlenije) is de Russische inlichtingendienst van de Generale Staf van Defensie.

60 NSA (National Security Agency) is de Amerikaanse inlichtingendienst van het ministerie van Defensie, een agentschap gecoloceerd met en onder dezelfde leiding als het U.S. Cyber Command.

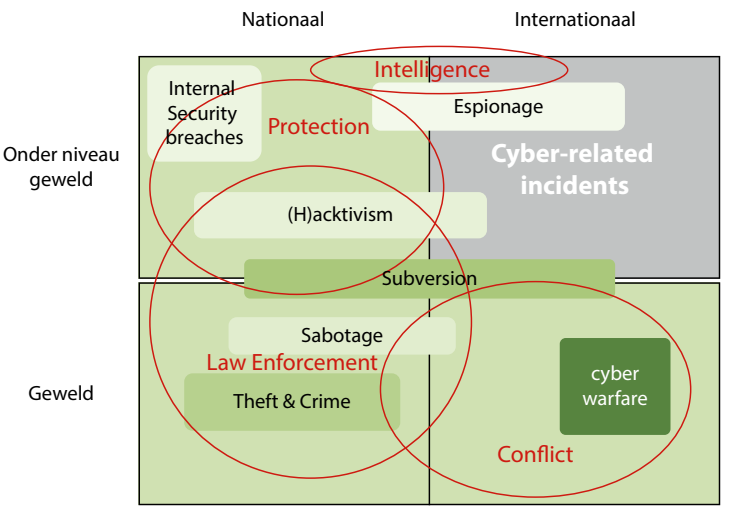
61 Paul A.L. Ducheine, 'Defensie in het Digitale Domein', in: *Militaire Spectator* 186 (2017) (4) 152–168; Paul A.L. Ducheine en Peter B.M.J. Pijpers, 'The Notion of Cyber Operations', in: Nicholas Tsagourias en Russell Buchan (red.), *Research Handbook on International Law and Cyberspace (Forthcoming)*, 2nd ed. (Edward Elgar, 2021).

62 De beschermende taak bij defensie ligt primair in handen van onder meer het Defensie Cyber Security Centre (DCSC). De indeling is schematisch, in de praktijk werken veel eenheden samen binnen deze paradigma's zowel binnen als buiten het ministerie van Defensie. Zo werkt de MIVD met de Algemene Inlichtingen en Veiligheidsdienst samen in de Joint Sigint Cyber Unit.

63 Ducheine, 'Defensie in het Digitale Domein', 157.

64 Ducheine en Pijpers, 'The Notion of Cyber Operations', 12.

65 Op basis van een mandaat van de VN-Veiligheidsraad, (collectieve) zelfverdediging zoals verwoord in artikel 51 van het VN-Handvest en artikel V van het NAVO-verdrag, of op uitnodiging van een andere staat.



Figuur 4 Gray zone: internationale cyberoperaties onder het niveau van geweld

inzet. In figuur 4 zijn, op basis van de paradigma's, de tegenstellingen (nationaal/ internationaal en boven/onder niveau van geweld) vereenvoudigd weergegeven, waarbij de gray zone inzichtelijk is gemaakt: het gebied van internationale cyberoperaties onder het niveau van geweld.[66]

In dit grijze kwadrant - waar het hierboven gepresenteerde juridische kader zich ook op richt - is de rol van de Nederlandse krijgsmacht, buiten activiteiten op basis van de Wet op de Inlichtingen en Veiligheidsdiensten (WIV) uit 2017, minimaal. Dit is echter exact de ruimte waar de Amerikaanse persistent engagement en de meeste cyberactiviteiten, inclusief de hiervoor beschreven casussen, plaatsvinden.

Wat betekent dit voor de Nederlandse krijgsmacht? De staat kan niet afzijdig blijven in de gray zone, niet in de laatste plaats omdat Nederland dagelijks doelwit is van cyberaanvallen vanuit het buitenland,[67] maar een pro-actievere houding levert een dilemma op. Wie gaat handelen en onder welk mandaat?

Kijkend naar de krijgsmacht heeft Nederland het DCC dat is voorbestemd om op te treden in cyberspace tijdens een conflict ter verdediging van, of om op te treden buiten, onze landsgrenzen: dit op basis van zelfverdediging, toestemming van het getroffen land, of een internationaal mandaat van de VN-Veiligheidsraad. De genoemde rechtsbases autoriseren echter geen optreden van het DCC in de gray zone. Optreden van de krijgsmacht buiten de landsgrenzen, onder het niveau van geweld is slechts beperkt mogelijk, en staat vaak op gespannen voet met het internationaal recht. Namens Nederland zou het DCC kunnen ondersteunen bij een (niet-gewelddadige) tegenmaatregel, na een eerder geweldgebruik van een andere staat, of zich beroepen op een *plea of necessity*,[68] waarbij het gaat om een rechtvaardigingsgrond van handelen dat in beginsel in strijd is met het internationaal recht. Ook zou het DCC kunnen optreden op basis van een nationaal mandaat voor speciale operaties,[69] maar dat vormt geen rechtsbasis onder internationaal recht.

Daarnaast is het verruimen van de bevoegdheden van de inlichtingen- en veiligheidsdiensten een optie. Zij kunnen nu na een lastgeving en binnen hun taakstelling op grondslag van de WIV grensoverschrijdende inlichtingenoperaties uitvoeren onder het niveau van geweld, ook in cyberspace.[70] De taak verruimen naar *alle* cyberoperaties – naar Amerikaans persistent engagement-model[71] – is op zijn minst controversieel omdat we daarmee

66 Grensoverschrijdende acties, onder het niveau van geweld, handelend conform de beginselen van het internationale recht, zoals een diplomatiek protest, zijn toegestaan en daarmee niet 'grijs'.

67 NCTV, 'Cybersecuritybeeld Nederland', 2020, 7-9.

68 Schmitt, *Tallinn Manual 2.0*, Rule 26, 135-142.

69 Paul A.L. Ducheine, Kraesten L. Arnold, en Peter B.M.J. Pijpers, 'Decision-Making and Parliamentary Control for International Miiltary Cyber Operations by The Netherlands Armed Forces', in: Rogier Bartels et al (red.), *Liber Amicorum*, 2020, 76-79. De inzet van de krijgsmacht voor operationele taken die passen binnen de eigen grondwettelijke taak van de krijgsmacht vindt plaats binnen een kader van voorwaarden in lijn met het geldende internationale recht. Het niet schenden van de soevereiniteit is een van die voorwaarden.

70 Het onderscheid tussen inlichtingenoperaties en (offensieve) cyberoperaties is lastig te maken, zie ook Herbert S. Lin en Amy Zegart (red.), *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Brookings Institution Press, 2019) 6.

71 De VS heeft een separate wet voor inlichtingenoperaties (Executive Order 12333 United States Intelligence Activities van 4 december 1981), en voor cyberoperaties (Sectie 1642 van de John S. McCain National Defense Authorisation Act van 2019). Zie ook: Chesney, 'The Domestic Legal Framework for US Military Cyber Operations'.

de beginselen van soevereiniteit en non-interventie schenden.

Tot slot zou de krijgsmacht, en meer in het bijzonder de marechaussee, gebruik kunnen maken van nationale wetgeving,[72] en extra-territoriale rechtsopsporingsbevoegdheden (onder het *law enforcement*-paradigma) gebruiken om dreigingen in de gray zone tegen te gaan. Dit is echter primair een politietaak, waarbij de krijgsmacht slechts ondersteunt.

Conclusie

Dit artikel schetste een juridisch kader voor internationale digitale acties van statelijke actoren buiten de context van geweld en conflict. Hoewel in die situatie het geweldsverbod en het humanitair oorlogsrecht geen rol spelen, betekent dit niet dat er wetteloosheid heerst. De internationaalrechtelijke regels voor soevereiniteit en non-interventie regelen, ook in cyberspace, het gedrag van staten in een internationale context. Het is staten niet toegestaan de territoriale integriteit of de politieke onafhankelijkheid van andere staten te schenden (soevereiniteit). Daarnaast is een interventie niet geoorloofd wanneer die een dwingend karakter heeft, wat inhoudt dat er een intentie is om het regeringsbeleid te veranderen op een wijze waar de andere staat zelf niet voor zou kiezen.

Internationaal optreden onder het niveau van geweld in cyberspace is dus juridisch begrensd, maar niet verboden zolang de remote cyber-attacks het internationale recht niet schenden. Het vraagstuk hoe hierin op te treden, levert voor de Nederlandse krijgsmacht een duivels dilemma op.

Het is kiezen tussen twee kwaden. Ofwel Nederland gaat acteren in de gray zone en voert grensoverschrijdende activiteiten uit onder het niveau van geweld. Het verruimt daarmee de bevoegdheid van het DCC of de inlichtingendiensten, door niet alleen inlichtingenactiviteiten, maar alle activiteiten in cyberspace uit te voeren naar analogie van het Amerikaanse

De staat kan niet afzijdig blijven in de gray zone, niet in de laatste plaats omdat Nederland dagelijks doelwit is van cyberaanvallen vanuit het buitenland

persistent engagement. Hoewel menig land, naast de VS ook Rusland en China, al geruime tijd aanwezig is in deze gray zone, rekt Nederland hier de nationale taken voor de krijgsmacht op, waardoor deze op gespannen voet komen te staan met het internationaal recht, en de grens daarvan wellicht overschrijden.

Of Nederland, en dus zijn krijgsmacht, blijft weg uit de gray zone. Dit zou logischer zijn; met optreden in de gray zone schendt Nederland immers een van zijn eigen vitale belangen, namelijk een goed functionerende internationale rechtsorde.[73] Nadeel hiervan is dat anderen wel in de gray zone optreden, en dat Nederland ondanks een bewuste afzijdigheid wel een potentieel doelwit is. Wie gaat Nederland dan verdedigen, als de krijgsmacht niet aan zet is?

Hoe dan ook, niets doen is geen optie. ■

72 Denk daarbij aan de wet Computer Criminaliteit III, Kamerstukken II, 2015-2016, 34 372, nr. 3.

73 NCTV, 'Nationale Veiligheid Strategie 2019', 2019.

Hup Veteraneninstituut en dag RZO

Frans Matser

In de afgelopen vier jaar heb ik mij onder andere bezig mogen houden met het adviseren over preventiemaatregelen en onderzoeken naar verbeterde behandelmethoden voor veteranen die met psychische problemen zijn teruggekomen van hun inzet.[1] De meest bekende categorie daarvan zijn natuurlijk de veteranen die een Post Traumatische Stress Stoornis (PTSS) hebben opgelopen en als gevolg daarvan na terugkeer moeilijk hun plaats in de maatschappij en de organisatie terugvinden. PTSS is feitelijk een normale reactie op (een reeks van) abnormale gebeurtenissen. Een organisatie die een belangrijke rol speelt is het Landelijk Zorgsysteem voor Veteranen (LZV), waarin Defensie (MGGZ, MDD en DGV[2]) en een tiental civiele gespecialiseerde zorgverleners samenwerken. De Raad voor Civiel-Militaire Zorg en Onderzoek (RZO) speelde hierbij de rol van toezichthouder en adviseur.

In vrijwel alle gevallen leidt PTSS tot een verlies van de greep op je eigen leven en tot een verslechtering van je relaties met je partner, je collega's en je vrienden. Veel PTSS-slachtoffers vluchten in gedrag dat de psychische problemen moet wegdrukken. Ze gaan heel veel en heel hard werken, heel hard sporten, of gaan zich te buiten aan wat in hulpverlenersjargon 'middelengebruik' heet: te veel drinken, roken, of drugs gebruiken. Dit leidt dan vaak weer tot verdere verslechtering van de relatie met het thuisfront. Zo belanden PTSS-slachtoffers in een neerwaartse spiraal en gaat het vaak van kwaad tot erger als niet op tijd wordt onderkend wat er aan de hand is en professionele hulp wordt geboden.

Hiervoor heeft Defensie binnen het LZV een uitgebreid netwerk van samenwerkende hulporganisaties ingericht die via één loket (het Veteranenloket) te benaderen zijn. Want kijkend naar de psychische zorg voor veteranen is er gelukkig ook goed nieuws. Om te beginnen is het belangrijk te beseffen dat veruit de meeste militairen zonder psychische problemen terugkomen van een uitzending. Het overgrote deel (70-80 procent) komt zelfs terug met een goed gevoel.[3] Dus niet elke veteraan komt terug als een tikkende tijdbom, zoals sommige media nogal eens onterecht suggereren.

Een vuistregel is dat 20 procent van de veteranen na terugkeer nog wel (tijdelijke) aanpassingsproblemen ervaart. De meesten kunnen dit zelf binnen enkele maanden oplossen via hun eigen sociale vangnet. Praten met partner, familie, collega's of misschien met de geestelijke verzorger of een maatschappelijk werker is vaak voldoende om weer in het oude ritme terug te komen.

Daarnaast zijn er dan de mensen (zo'n 5 procent) die structureel en langdurig klachten houden. Met goede professionele behandeling kan een deel daarvan ook weer volledig herstellen, maar dat kost tijd. Daarnaast is er ook een groep (van enkele procenten) die niet herstelt en die we moeten helpen te leren leven met hun aandoening. Dit kan soms ook een militair invalidenpensioen of een andere financiële compensatie zijn voor het in hun geval onherstelbare leed dat hen is overkomen. Feitelijk is dat niet anders dan hoe het met militairen gaat die fysieke verwondingen oplopen bij een inzet. Wel is het soms moeilijker aan de buitenwereld duidelijk te maken dat een depressie

of een angststoornis het leven net zo moeilijk (of zelfs moeilijker) kan maken dan het missen van een arm of een been.

De meest gangbare therapieën voor PTSS zijn EMDR,[4] cognitieve gedragstherapie en *exposure* therapie. De behandelresultaten van PTSS lieten de laatste 20 jaar een succespercentage van 40 tot 60 zien. Daar is dus nog wel ruimte voor verbetering. Wereldwijd wordt er veel onderzoek gedaan naar nieuwe therapieën die een beter succespercentage hebben of waarmee mensen die geen baat hebben bij de bestaande methodes, toch geholpen kunnen worden. De afgelopen jaren heeft Defensie jaarlijks minimaal één miljoen euro geïnvesteerd in onderzoek naar verbeterde behandelmethoden. Dit heeft geleid tot een hele reeks van vernieuwende en veelbelovende therapieën. Ik noem er een paar.

Het blijkt dat het soms combineren van bestaande therapieën met gebruik van (kleine hoeveelheden) chemische drugs zoals MDMA, ketamine en cannabis een duidelijke verbetering van het behandelsucces geeft. Daarnaast wordt er met 3MDR[5] en *virtual reality*-techniek (waardoor mensen hun trauma door techniek realistischer kunnen herbeleven) succes geboekt bij mensen die met de traditionele behandelingen niet verder komen. Ten slotte wordt steeds meer met onconventionele methoden geëxperimenteerd zoals terugkeerreizen onder begeleiding of animale assistentie, het gebruik van hulphonden of paarden bij de therapie. Nadeel van de laatste vorm van hulp is dat dit je mensen soms afhankelijk maakt en daarom komt het doorgaans pas aan de orde als verdere verbetering van de situatie met reguliere behandeling niet meer mogelijk lijkt en de veteraan moet leren leven met de beperkingen van zijn aandoening.

Nadat de RZO zich veertien jaar om de controle op en advies over deze zaken had bekommerd, hield dit adviescollege begin dit jaar geluidloos op te bestaan. De taken zijn overgenomen door de nieuw opgerichte Stichting Nederlands Veteraneninstituut, een samenwerkingsverband van zes veteranenorganisaties.[6] Van deze taakverschuiving merken de veteranen die in behandeling zijn weinig. De verwachting is dat deze unieke samenwerking zal leiden tot nog betere zorg aan de veteranen. Die verdienen dat namelijk. Er is zelfs een echte generaal benoemd als directeur. Dan hebben we nu naast en bezuinigingsgeneraal, een veiligheidsgeneraal en een stikstofgeneraal ook een veteranengeneraal. En dat is goed nieuws. Ik vond het werken voor de RZO leuk, maar troost me met de gedachte dat we niet gemist worden. ■

> We hebben nu ook een veteranengeneraal, en dat is goed nieuws

1 Om invulling te geven aan de zorg voor veteranen heeft de minister van Defensie op 5 juli 2007 de Raad voor Zorg en Onderzoek voor veteranen (RZO) geïnstalleerd. De RZO bewaakt de kwaliteit van het Landelijk Zorgsysteem voor Veteranen en bevordert de samenwerking tussen de betrokken partijen in dat zorgsysteem en het wetenschappelijk onderzoek naar uitzend-gerelateerde aandoeningen. De RZO adviseert de minister van Defensie gevraagd en ongevraagd over alle genoemde onderwerpen.

2 Militaire Geestelijke GezondheidsZorg, Maatschappelijk Dienst Defensie en Diensten Geestelijke Verzorging.

3 Dit percentage is natuurlijk missie-afhankelijk en wordt volgens veel onderzoekers beïnvloed door de aard en het succes van de missie.

4 Een behandeling waarbij de patiënt praat over zijn trauma, terwijl hij gelijktijdig wordt afgeleid door een bewegend object (lampje).

5 Techniek waarbij de patiënt op een onder begeleiding van een psycholoog op een loopband een visuele reconstructie van zijn uitzendgebied binnenloopt en door gebruik van foto's, filmbeelden en geluid wordt teruggebracht naar de plek waar hij zijn trauma heeft opgelopen.

6 De Stichting het Veteraneninstituut is een samenwerking tussen de Stichting Nederlandse Veteranendag, de Stichting de Basis, het programmabureau van het LZV, de zorgcoördinatie van ABP/APG, en de coördinatie van het nuldelijns-ondersteuningssysteem van het Veteranen Platform. In totaal zijn hierbij ruim 200 medewerkers betrokken.

Maritieme strategie: ‘Rule the Ways’

Kiel International Seapower Symposium

Maarten Katsman

‘China bouwt iedere vier jaar het equivalent van de totale Franse marine’, werd opgemerkt tijdens het symposium ‘Operationalizing Allied Maritime Strategy - Rule the Ways’ op 7 september. Dit was het derde en laatste deel in een reeks symposia over maritieme strategie door het Center for Maritime Strategy & Security van het Institut für Sicherheitspolitik an der Christian-Albrechts-Universität zu Kiel (ISPK).[1] China was de olifant in de kamer in Kiel, maar voor welke andere uitdagingen staan westerse marines? Hoe kunnen zij het maritieme initiatief behouden of herwinnen?

Amerikaanse marineschepen voeren Freedom of Navigation Operations uit

FOTO U.S. NAVY, MICHAEL A. COLEMAN BARRY

Onder de sprekers waren prominente marineofficieren, zoals de commandant van het Allied Maritime Command (MARCOM) van de NAVO en de bevelhebber van de Zweedse marine, en diverse academici. Er was helaas geen bijdrage van de Nederlandse zeestrijdkrachten.[2]

FOTO U.S. NAVY, SPENCER FLING

Voor geloofwaardige afschrikking door marines blijft de menselijke factor van belang

Seapower is manpower

Waar moeten de marines van NAVO-bondgenoten en hun partnerlanden zich op richten, welke issues zijn belangrijk voor het bepalen van de toekomstige strategie? Deze vragen stonden centraal in het eerste panel. Voor gastland Duitsland is samenwerking het toverwoord. De 'kleinste Duitse marine ooit' heeft een breed scala aan taken en wil desondanks meespelen op elk niveau, overal ter wereld. Duitsland is, net als Nederland, afhankelijk van een 'rules-based order' en het land wil die orde proactief kunnen beschermen. Operaties ver van huis, bijvoorbeeld in de Indo-Pacifische regio, moeten – naast meer patrouillegang in de Oostzee – mogelijk blijven. Samenwerken en interoperabiliteit met bondgenoten zijn daarom cruciaal. Concrete stappen die Duitsland hierin zet zijn lucht- en raketverdediging in samenwerking met Nederland, gezamenlijke aanschaf van onderzeeboten met Noorwegen en de integratie van buitenlands personeel op Duitse schepen, of andersom.

Op een hoger niveau kwam de terugkeer van strategische competitie aan bod, maar dan op een meer complexe manier dan tijdens de Koude Oorlog. Internationale verdragen zijn verzwakt of afgeschaft en de internationale gemeenschap krijgt steeds meer te maken met de tactiek van 'fait accompli' door staten die de bestaande orde willen eroderen, bijvoorbeeld de Russische annexatie van de Krim. Door deze factoren is een nieuwe, sterke focus op afschrikking hét middel voor de NAVO om de bovenhand te houden in de nieuwe strategische competitie.

Taken lager in het geweldsspectrum blijven onverminderd belangrijk. Klimaatverandering heeft bijvoorbeeld tot gevolg dat humanitaire operaties vaker nodig zijn, en die vergen een ander soort middelen dan voor afschrikking en inzet in het hoogste geweldsspectrum het geval is. Wat betreft het beschermen van vitale infrastructuur kan de marine bijdragen aan de veiligheid van onder meer datacentra en onderzeese kabelverbindingen.

Een van de grootste uitdagingen voor de marines van ongeveer alle NAVO-bondgenoten en partners is het werven en behouden van voldoende personeel. Dat blijft een belangrijke, wellicht beperkende factor. Sommige landen, zoals Zweden, voelen zich sterker bedreigd door een assertiever Rusland en hebben mede daardoor minder wervingsproblemen. In andere landen is die dreigingsperceptie veel lager. Onbemande systemen (USV's) kunnen een oplossing vormen voor een deel van het personeelsprobleem, maar een spreker benadrukte de diplomatieke rol die marines nog altijd spelen: dat gaat makkelijker met mensen. Om afschrikking geloofwaardig te maken gaat het soms juist om de zichtbaarheid van grote, goed bemande schepen waarmee een duidelijk statement kan worden gemaakt richting partners en rivalen. Zogeheten Freedom

1 Zie: https://www.kielseapowerseries.com/en/kiss-2021-maritime-strategy-ways.html.

2 Om de presentaties en discussies te bevorderen golden de Chatham House Rules, dit artikel is daarom een globale weergave van de inhoud van het symposium, zonder die aan personen toe te schrijven.

FOTO ISPK, JAN KONITZKI

Een van de panels op het Seapower-symposium in Kiel

of Navigation Operations (FONOPS) vereisen zichtbare personele inzet om hun doel te bereiken.

Maritiem initiatief behouden

Met de issues en operationele wensen op een rij gezet, was het tijd te kijken naar hoe het Westen het initiatief in het maritieme domein kan behouden, of herwinnen. Speciale aandacht was er hierbij voor kleine marines. Als voorbeeld werd de vaak onderbelichte regio rond de Zwarte Zee aangehaald. Dit gebied laat namelijk goed zien hoe China met economische middelen aan macht en invloed wint. Landen als Roemenië en Bulgarije, beide NAVO-bondgenoten, reageren verschillend op de ouvertures van Beijing. De Chinese investeringen en belangen in infrastructuur, havens met name, kunnen de Zwarte Zeelanden in een spagaat brengen: hoe riskant is het om China politiek-strategisch voor het hoofd te stoten, als dat aanzienlijke economische repercussies tot gevolg heeft? Roemenië houdt daarom de deur zoveel mogelijk dicht voor de Chinezen, om niet in die positie te worden gedwongen. Andere landen laten vooralsnog de economische belangen prevaleren, met alle risico's van dien.

Hoewel China de hoofdrol speelde in het toekomstige vijandbeeld werd er ook een positieve kanttekening geplaatst bij de expansie van dat land. Mogelijk heeft de macht van China een stabiliserende invloed op de Zwarte Zeeregio, omdat de 'oude vijand' Rusland dan met meer machtscentra rekening heeft te houden. Het zou zich dan gedwongen zien voorzichtiger op te treden.

Een ander onderdeel van dit panel was de relatie van de VS met zijn bondgenoten. Waar heeft Washington concreet behoefte aan, en wat kunnen de bondgenoten hierin überhaupt betekenen? Een belangrijk verschil met de tijd van de Koude Oorlog is de rol van technologie. Europa heeft nu geen 'excuus' meer om technologisch achter te blijven ten opzichte van de VS, omdat het continent rijk is, technologie meer en meer gedreven wordt vanuit de civiele sector, en vanuit meer centra over de hele wereld. De toegankelijkheid tot (militaire) technologie is

daarom enorm vergroot. Het is nu dus meer een kwestie van politieke wil van de Europese bondgenoten zelf, en niet meer de dominante maar terughoudende positie van de VS op dit gebied, die bepaalt welke capaciteiten de Europese marines kunnen opbouwen. Concreet gaat het daarbij om mijnenbestrijdingscapaciteit, en vooral om het opbouwen van een geloofwaardige afschrikking. 'Samenwerking' alleen is hiervoor niet langer meer voldoende. De bondgenoten en partners moeten hun onderlinge netwerken versterken en vergaand integreren, tot op dataniveau.

Plannen vs. de realiteit

'Everybody has a plan until they get punched in the mouth'. Met deze quote van bokser Mike Tyson vatte het programmaboekje van het symposium het thema van het derde panel kernachtig samen. Hoe blijven plannen relevant en bruikbaar als er een conflict uitbreekt?

Een spreker benadrukte het belang van oefeningen en wargaming, die vaak herhaald moeten worden en vooral echt competitief moeten zijn. Op die manier kunnen westerse strijdkrachten manieren bedenken om bijvoorbeeld Russische A2/AD-capaciteiten (anti-access/area denial) te omzeilen of te verzwakken. Vooralsnog ligt de focus namelijk te veel op bijvoorbeeld de kracht en het bereik van Russische raketten. Direct daaraan toegeven creëert 'no-go-zones' en daarmee zetten marines zichzelf meteen buitenspel. Aandacht voor maritieme geschiedenis is evenmin onbelangrijk: er zijn talloze voorbeelden denkbaar waarbij een op papier inferieure partij toch overwon. Het is niet nodig superieur te zijn in elk aspect, zolang je de sterke punten van de tegenstander kunt afzwakken of helemaal teniet kunt doen. Wargaming is cruciaal om die zwakke plekken te identificeren en uit te buiten.

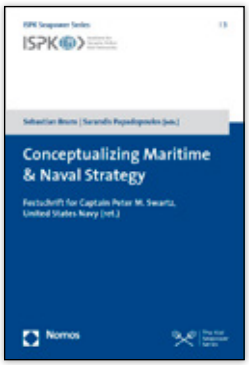
Er was in dit panel ook aandacht voor de verhouding EU-NAVO. De eerste spreekt steeds vaker de wens uit 'strategische autonomie' te bereiken. Is er dan geen risico op duplicatie van de NAVO, en daardoor verspilling van tijd en middelen? Een spreker benoemde het belang van een sterke EU voor de geloofwaardigheid en positie van de NAVO: wanneer de Unie zelf haar zuidflank op orde heeft en daarnaast haar oostflank significant versterkt, krijgt de NAVO het ook makkelijker.

Een deelnemer vroeg naar de dreigingsperceptie: voor Rusland en China is het vijandbeeld helder, dat is het Westen. Is dat een kracht of een zwakte voor het Westen? De sprekers benoemden eigenlijk allemaal het belang van solidariteit en bondgenootschappen. Illustrerend is in dit geval het aantal bondgenoten en partners van de VS, afgezet tegen de vriendenkring van Rusland en China. Het kost tijd, moeite en investeringen die onderlinge banden te behouden en versterken, maar op lange termijn betalen ze zich uit.

In het verlengde van het seapower-symposium vond een ISPK-werkgroep plaats: '21st Century Huntington. What's Next for Naval Strategy?'. Marine-experts discussieerden over hoe de kloof te overbruggen tussen huidige maritieme operaties, concepten, en strategie. Ook bespraken ze de relatie tussen marinehistorie en toekomstig marinebeleid. Dat deden zij aan de hand van de bundel *Conceptualizing Maritime & Naval Strategy: Festschrift for Captain Peter M. Swartz, United States Navy (ret.)*, zie de recensie hierna.

Met deze enigszins hoopvolle constatering eindigde het strategiesymposium in marinestad Kiel. De actualiteiten kort na het symposium lieten meteen zien hoe moeilijk het is voor het Westen eensgezind en met cohesie op te trekken. Het nieuwe AUKUS-verbond tussen Australië, het Verenigd Koninkrijk en de Verenigde Staten, en het bijbehorende onderzeebotencontract, resulteerde in diepgaande frictie met Frankrijk. Zolang in dit geval China niet bij alle westerse bondgenoten en partners even hoog op de prioriteitenlijst staat, gaat het vormen van een gezamenlijke (marine)strategie moeizaam. Beijing bouwt ondertussen gestaag verder aan een steeds grotere en krachtigere 'blue water navy'.[3] ■

3 Kees Homan, 'De nieuwe Chinese marine-strategie: zo wijd de wereld strekt', *Clingendael Spectator*, 11 juni 2019. Zie: https://spectator.clingendael.org/nl/publicatie/de-nieuwe-chinese-marine-strategie-zo-wijd-de-wereld-strekt.



Conceptualizing Maritime & Naval Strategy: Festschrift for Captain Peter M. Swartz, United States Navy (ret.)

Door Sebastian Bruns en Sarandis Papadopoulos (red.)
Baden Baden (Nomos Verlagsgesellschaft) 2020
373 blz.
ISBN 9783848757534
€ 97,-

Deze bundel is een hommage aan Captain USN (ret.) Peter Swartz. Deze oud-officier was gedurende zijn 26 jaar lange militaire carrière adviseur voor de Zuid-Vietnamese marine, diende in de staf van diverse Amerikaanse admiraals en geldt als een van de penvoerders van de *U.S. Maritime Strategy* in de jaren '80. Nadat hij zijn uniform inwisselde voor een burgeroutfit werd hij in 1993 onderzoeker bij het US Center for Naval Analyses en beïnvloedde hij met studies over strategie, planning en beleid maritieme experts in binnen- en buitenland, niet toevallig onder meer de redacteuren van deze bundel, alsook alle deelnemende scribenten.

Maritieme premier league

Het *Festschrift* is bepaald geen *Liber Amicorum*, waarin soms prikkelende bijdragen veelal worden afgewisseld met *petites histoires* of sympathieke carrièreschetsen van degene aan wie de publicatie is opgedragen. Deze bundel is werkelijk een wetenschappelijk-strategisch pareltje, nevens een welkom document voor menig marine en beleidsmaker. In een tijdsbestek dat geopolitiek terug is van weggeweest, met een alsmaar assertiever Rusland, de uitbouw van China als wereldmacht en instabiliteit in vooral het oostelijke Middellandse Zee-bekken en Zuidwest-Azië, neemt namelijk het gewicht van maritieme veiligheid en zeestrijdkrachten als instrument van buitenlands beleid allengs toe. Vragen zoals wat in het woelig internationaal vaarwater de rol en operationele taken van zeemacht zijn, en hoezeer staten en hun instituties maritieme doelen, handelswijzen en middelen hebben overdacht en vormgegeven, dringen zich meer en meer op.

Welnu, de bundel is een *Fundgrube* voor hen die handgrepen zoeken om een marinestrategie vorm te kunnen geven. De zestien bijdragen van een schrijverscollectief uit alle windstreken brengt welhaast de gehele huidige *premier league* van maritieme denkers samen, onder wie klinkende namen als John Hattendorf en Geoffrey Till. Deze waaier aan inzichten, vaak onderbouwd met historische voorbeelden, biedt een reeks criteria aan de hand waarvan een maritieme strategie is te ontwikkelen. In een notendop betreft het brede (inter)nationale intermenselijke discussies en contacten, en hiermee een netwerk waarin meerdere disciplines en belangengroepen zijn te vinden. Juist een dergelijk divers speelveld draagt, zo onderstrepen vooral de redacteuren, bij aan de benodigde brede inzichten om überhaupt een raamwerk als maritieme strategie te kunnen opzetten. Deze insteek vereist, zo benadrukken ook meerdere auteurs, dat ontwikkeling van een hoogwaardige maritieme strategie neerkomt op een zuiver analytisch proces, en niet het oordeel is van een handvol vlagofficieren en politici.

Drie hoofdzaken voor de Koninklijke Marine

Gelet op het kruispunt waarop de Koninklijke Marine zich momenteel bevindt, dat haar dwingt tot reflectie op maritieme strategie, vlootopbouw en inrichting van wapenplatforms, passeren hieronder de bijdragen van Peter Haynes, Sebastian Bruns en Jeremy Stöhs nadrukkelijk de revue. Het betreft respectievelijk de Amerikaanse heroriëntering van vlootvorming omstreeks 1970 als reactie op de kwantitatieve en kwalitatieve vlootopbouw van de Sovjet-Unie, de recente dreiging in de High North afgezet tegen post-Koude Oorlog-ontwikkelingen en de recente strategievorming bij *die Deutsche Marine*, een partner waarmee de Nederlandse marine gestaag nauwer samenwerkt.

Haynes behandelt Project SIXTY; een initiatief in 1970 van de Amerikaanse CNO-*admiral* Zumwalt die zijn staf binnen zestig dagen de *means*, *ends* en *needs* van de Amerikaanse marine laat opstellen. Zijn insteek is een beter personeelssysteem, vlootmodernisering en reductie verantwoord te laten samengaan en gelijktijdig het doel van de marine te duiden, waarbij de (foutief) gepercipieerde Sovjetdreiging van *sea control* leidend is. De studie veroorzaakt een intern

U.S. Navy-debat, maar doet de focus verschuiven van strategieontwikkeling en langetermijnplanning naar (operationeel) management van wapensysteemprogramma's en bemanningsproblematiek. Het gevolg: de Amerikaanse marine denkt tot 1980 veelal in op een incorrecte *threat assessment* gebaseerde *force structure* en hanteert in die jaren tezamen met onder andere de Koninklijke Marine een hiervan afgeleide, strategisch dubieuze defensieve doctrine.

Stöhs analyseert recente Europese defensiepolitiek en zeestrijdkrachten in de noordelijke regio van het oude continent. Twee strategische paradigma, effecten van een krimpend defensiebudget en een assertiever Rusland en terugkeer naar het concept van collectieve veiligheid, staan centraal. Hij stelt dat na de Koude Oorlog wereldwijde crisisoperaties voor westerse marines, naast investeringen in *network centric warfare*, de komst inhielden van grote en veelzijdiger platforms met een ruime actieradius als LPD's en escorterende *Air Defence*-schepen. Stöhs illustreert dat Europese marines, met de Nederlandse als leidend voorbeeld, niettemin door structureel krimpend budget falen in de handhaving van slagkracht van 'both high quality as well as significant quantity'. Met alle gevolgen van dien voor de *naval superiority* en *backup* van de NAVO in onder andere de (noordelijke) Noorse Zee. Stöhs vraagt om een maritiem-strategische westerse/NAVO-aanpak waarbij landen als Nederland een meer afgewogen eigen en collectieve verdediging opzetten. Zijns inziens is een door strategisch debat gevoed maatregelenpakket raadzaam, zoals bestudering van de strategische cultuur van de tegenstander en afschrikking met een geloofwaardige verdedigingsstructuur wat betreft omvang, geïntegreerde samenwerking en slagkracht in het lage, maar *bovenal* hoge(re) geweldsspectrum.

Bruns gaat in op de trans-Atlantische en interculturele strategieontwikkeling voor de Duitse marine. Tijdens de Koude Oorlog gebruikte deze bij interne discussie en vorming van een eigen strategie veelvuldig Amerikaanse voorbeelden. Een handelswijze niet veel anders dan de Koninklijke Marine de facto bezigde bij de *U.S. Maritime Strategy* in de jaren 1980 en *From the Sea* in de jaren 1990 met 'veiligheid op en vanuit zee'. Na 1991 raakte *die Deutsche Marine* overbelast met enerzijds terugkerende taken in de Middellandse Zee, de Hoorn van Afrika, Operation Enduring Freedom en indeling bij NAVO-smaldelen als SNMG/SNMCMG, anderzijds personeelsproblematiek en een te krap budget. Bekende geluiden. Eind december 2014, na de geopolitieke aardverschuiving van de Krimbezetting alsook de verdere oriëntering van Washington op Oost-Azië, kwam het tot de opzet van een informele strategische adviesgroep voor de Duitse marineleiding. Een institutionalisering ervan bleef bewust achterwege. Dit bevorderde het vrijdenken van (in hun *spare time*!) deelnemende officieren en burgerexperts. Bruns benadrukt hierbij het belang van de 'structured use of talent and knowledge from the civilian field by the military, and an embrace of strategy and defense subjects by political scientists to become true experts in maritime and military strategy'. Iets wat in zijn ogen te lang ontbrak voor het kunnen opzetten van Duitse (maritieme) strategie.

Doctrine voor postmoderne marines

Dit nieuwe marinedocument (aanvang 2016) is gericht op beleidsmakers, de samenleving en strijdkrachten, maar ook bondgenoten als Nederland. Hoofdpunten zijn het voorzien en verklaren van de strategische oriëntatie van *die Deutsche Marine*, het vaststellen en prioriteren van politieke en geografische *areas of responsibility* zoals de Noorse Zee, alsook de integratie van gaande ontwikkelingen, bestaand en toekomstig beleid, en operationele plannen. Dankzij onder andere Amerikaans advies en het betrekken van het publiek kwam het gaandeweg, zo geeft Bruns welhaast enthousiast te kennen, niet zozeer tot een nationale maritieme strategie, maar een meer internationaal doctrinedocument voor, zoals Till dit aanduidt, 'postmoderne' marines. Te weten die vlootorganisaties van westerse democratieën die het internationale systeem bewaken, in plaats van nationale wateren et cetera. Hier neigt Bruns ertoe, ondanks oog voor de Russische *sea sontrol*-uitdaging, *soft power* inzake *seapower* wel erg te benadrukken, met verdere verwijzingen naar contacten met burgerautoriteiten, permanente marinecoöperatie en (tijdelijke) integratie, EU- bemanningen, et cetera. Niettemin biedt het marinedocument, zo merkt Bruns terecht op, met zijn brede benadering, de vloot van onze oosterburen meer kansen op vernieuwing en betere *readiness* doordat ze hiermee meer verankerd is in de maatschappij, en deze zeestrijdkrachten een hogere waardering van de eigen samenleving en politiek opleveren dan voorheen.

Uit deze drie bijdragen, maar ook overige hoofdstukken, valt op te

maken dat het komen tot een nationaal (maritiem) strategieproces an sich een uitdaging is, maar bepaald geen onmogelijkheid. In hun conclusie benadrukken beide redacteuren van deze verzorgde en prettig leesbare bundel vooral het belang van het samen optrekken in dit proces van operators en academici. Kortom: een samengaan van top-downplannen (realpolitieke alsook door internationaal recht en *global governance* ingegeven), strategieën en bottom-up-ideeën gedreven door *threat driven* militaire slagkracht. De maritiem-strategische uitkomst van deze vervlechting moet vervolgens de horde nemen van belangengroepen, politici, media en de (inter)nationale waan van de dag. Ware strategisch denkers als Swartz, zo stellen redacteuren Bruns en Papadoupoulos, kunnen in een dergelijke situatie hun punt maken en invloed uitoefenen door vasthoudend hun superieuren van advies te blijven dienen. De kracht van Swartz is dat hij zijn (politieke) bazen (indirect) meermalen liet inzien wat de operationele marine uit strategisch oogpunt nodig had, alsook vice versa de U.S. Navy ervan overtuigde wat vanuit correct strategisch perspectief als insteek moest dienen voor het doorvoeren van haar operaties. ■

Dr. Anselm van der Peet (NIMH)

De wraak van Diponegoro

Begin en einde van Nederlands-Indië
Door Martin Bossenbroek
Amsterdam (Atheneum-Polak & Van Gennep) 2020
798 blz.
ISBN 9789025301514
€ 39,99

De Amerikaanse politicoloog Charles Tilly zei het ongeveer zo: 'war makes states and states make war'. De Nederlandse staatsrechtgeleerde Leonard Besselink zei min of meer hetzelfde in juridische termen; hij formuleerde bij zijn proefschrift twee stellingen die in samenhang in dezelfde richting wijzen: '1. De politieke wetenschappen zijn naar hun aard historische wetenschappen, 2. Het staatsrecht is een politieke wetenschap'. Het staatsrecht is aldus een historische wetenschap. Krijgsgeschiedenis vormt een cruciaal onderdeel van de historische wetenschappen. Krijgsgeschiedenis is een essentieel onderdeel van het staatsrecht. Tilly en Besselink samengevat: bij staatsvorming komt geweld te pas. Gelauwerd historicus Martin Bossenbroek heeft al veel geschreven over Indië, in het bijzonder over de werving van en het vervoer van militairen voor Indië. Hij is onderweg nog een keer uitgestapt in Zuid-Afrika. In zijn nieuwste boek beschrijft hij het gewelddadige ontstaan en de gewelddadige ontbinding van Nederlands-Indië. Hij laat de geschiedenis niet beginnen bij de VOC en J.P. Coen, maar aan het begin van de negentiende eeuw. Het is ook een fictie dat 'wij' 350 jaar een koloniaal rijk hebben gehad. De VOC, die wegens faillissement in 1800 door de Nederlandse staat (in casu de Bataafse Republiek) werd overgenomen, ging het niet om landbezit, maar om commercie. Men had handelsposten en onderweg hier en daar een voorraadhaven.

De buffel en de tijger

Zei ik: staten maken oorlog? Ja, maar evenzeer is waar: mensen maken oorlog. Bossenbroek vertelt de geschiedenis aan de hand van vier hoofdpersonen, die paarsgewijs tegenover elkaar staan. Aan het begin de Javaanse prins Diponegoro tegenover de Nederlandse generaal De Kock en aan het eind de Indonesische president Soekarno tegenover de Nederlandse luitenant-gouverneur-generaal Van Mook, twee politici en twee krijgsheren. Afkomst en ambitie bepaalden de loopbaan en het lot van de vier hoofdrolspelers: Diponegoro (ook Ngabdoelkamid genaamd), een bastaardkleinzoon van de sultan van Yogyakarta, Hendrik de Kock, zoon van Nederlandse patriotten-militair die ongelukkigerwijs toch de dood vindt onder de revolutionaire guillotine, Soekarno, de Javaans-Balinesische ingenieur, en

Huib van Mook, een in Indië geboren en aan Indië verknochte Europeaan.

Bossenbroek verbeeldt de strijd om de macht als een gevecht tussen een buffel en een tijger. Het Indische eilandenrijk is de buffel, de Europese kolonisator de tijger. De strijd tussen een buffel en een tijger kennen we ook uit het verhaal over Saidjah en Adinda, onderdeel van *Max Havelaar*. Het beestenduel is vastgelegd op het schilderij 'De Boschbrand', dat op het boekomslag staat afgebeeld. Het is geschilderd in 1847-1850 door de Javaanse kunstenaar Raden Saleh, die het cadeau deed aan koning Willem III. Het bleef jarenlang in bezit van de familie Oranje. In 2006 werd het opgerold gevonden in een koninklijk paleis en gerestaureerd. Het cadeau uit 1850 werd in 2013 door de veertien erfgenamen van Juliana voor ettelijke miljoenen verkocht aan een museum in Singapore. Hoe aardig zou het zijn geweest als Willem-Alexander - na zijn op 10 maart 2020 in Jakarta wat hakkelend uitgesproken excuses voor het geweld bij de opheffing van het Nederlandse heerschappij in de Oost - dat schilderij met een royaal (!) gebaar als hoofd van het huis Oranje had aangeboden aan de Republik Indonesia. Excuses die de aanbieder ervan persoonlijk (financieel) een beetje pijn doen klinken meer oprecht.

Confrontatie van culturen

Over Van Mook en Soekarno zijn wel biografieën geschreven. Over Diponegoro en De Kock niet. Alleen al daarom vond ik het eerste deel van Bossenbroek extra boeiend. De Java-oorlog van 1825-1830 staat veel minder op het netvlies dan de oorlog van 1945-1950, althans op het netvlies van Nederlandse ogen. De Java-oorlog was niet alleen een gevecht met de wapens, maar ook een confrontatie van culturen. De rituelen, codes en tradities van de koninklijke Vorstenlanden werden vaak beantwoord met tamelijk lomp gedrag van de Hollandse autoriteiten, terwijl in het 1945-1950-conflict van beide zijden met grote regelmaat wreed werd opgetreden. Maar uiteindelijk ging het om de blote macht, zowel in de periode 1825-1830 als in de periode 1945-1950. In de negentiende eeuw gingen de Hollanders er met de hoofdprijs vandoor, in de twintigste eeuw de Indonesiërs.

De hoofdpersonen van de drama's zijn duidelijk. Maar er zijn ook nog allerlei bijrollen te verdelen. Voor de eerste periode Daendels, Van den Bosch, de adellijke familie van Diponegoro en Toontje Poland, de van huis weggelopen soldaat van Napoleon en de latere legendarische KNIL-militair over wie Johan Fabricius een kinderboek geschreven heeft. Voor de tweede periode worden de hoofdrolspelers geflankeerd door onder meer Hatta, Sjahrir, Spoor, De sultans van Yogyakarta, Hamengkoeboewono's met verschillende volgnummers, treden op in beide opvoeringen. Gezien de focus op de hoofdrolspelers is het verhaal over de Java-oorlog meer gericht op de militaire strijd, terwijl bij het eindspel de nadruk ligt op de politieke interactie.

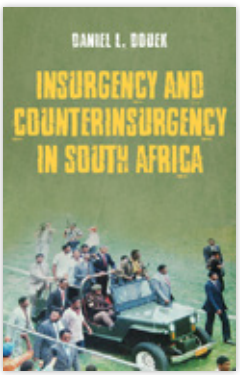
Prachtig leesboek

Het boek van Bossenbroek is geen volledige geschiedenis van de Nederlands-Indonesische betrekkingen van 1800 tot 1950. De Atjeh-oorlog wordt nauwelijks belicht, Indië in de Eerste Wereldoorlog (min of meer in de steek gelaten door het moederland) slechts aangestipt, de muiterij op de Zeven Provinciën alleen in contouren aangeduid. Ik constateer dat hier nu wel, maar bij het lezen van het boek voelt dat niet als een gemis.

Het boek van Bossenbroek kwam door het tijdstip van publicatie als vanzelf in een concurrentiestrijd met het boek 'Revolusi' van de Belg David van Reybrouck. Ik waag mij niet aan een vergelijkend waren-onderzoek tussen boeken van een journalist en een historicus. Voor het boek van Bossenbroek pleit in ieder geval dat hij ruim aandacht geeft aan de verovering van Indië door het jonge koninkrijk der Nederlanden. Deze verstatelijking van het kolonialisme hield ook de gouvernementele organisatie van de economische exploitatie in. Vooral in dit eerste deel beschrijft Bossenbroek personen en ontwikkelingen die in de Indische historiografie nog maar beperkte aandacht kregen. Hij vertelt de geschiedenis op levendige wijze. Ik houd van narratieve historie. Toegankelijk geschreven en goed gedocumenteerde boeken wakkeren de leeshonger aan. Bossenbroek heeft geen diepgravend studieboek, maar een prachtig leesboek geschreven.

De Indische samenleving is altijd opgesplitst geweest. De Indische krijgsmacht hoorde altijd bij een van de twee kampen, bij de dominante minderheid. De vijandelijke strijdmacht woonde in hetzelfde land en hoorde bij de massale meerderheid. De buffel heeft de tijger op de scherpe horens genomen. De nederlaag van Diponegoro is uiteindelijk gewroken. ■

Dr. Stan Meuwese



Insurgency and counterinsurgency in South Africa

Door Daniel L. Douek
Londen (C. Hurst & Co.) 2020
510 blz.
ISBN 9781849048804
€ 25,99

In nog geen eeuw tijd wisselden in Zuid-Afrika op militair historisch gebied tal van uitzonderlijke periodes en radicale omslagen elkaar af. Na koloniale 'small wars', die het gezag van de Britse Kaapkolonie en de blanke Boerenrepublieken vestigden, kwam het tussen hen zelf tot de Anglo-Boer War tussen 1899 en 1902, waarin guerrilla en COIN domineerden. In de periode erna, die minstens zo boeiend is, werd het nieuwe en hervormde 'nationale' leger vol ex-Boeren ingezet voor het neerslaan van opstanden van ontevreden Boeren (de Maritz-rebellie). Direct daarna volgde de meer conventionele militaire inzet in de Eerste Wereldoorlog, aan nota bene de Britse zijde. Tussen 1914 en 1918 vocht Zuid-Afrika onder andere tegen Duitse troepen in het huidige Namibië en tegen de eenheden Von Lettow-Vorbeck in oostelijk Afrika. Het leverde ook troepen aan het westelijke front, bijvoorbeeld in 1916 bij Delville Wood. In de Tweede Wereldoorlog bestond de militaire bijdrage van Zuid-Afrika uit heel diverse operaties: op land in Madagascar, bij El Alamein en in Italië, en vanuit de lucht in met name Noord-Afrika. In de periode na 1945 raakten het leger en andere veiligheidsdiensten juist betrokken bij het garanderen van 'interne veiligheid', in het kader van de Apartheid. Dit was ook de periode van de Borderwar, die wat betreft doelstellingen en tactieken nog het best kan worden vergeleken met de Vietnamoorlog, maar redelijk succesvol was. Daarna volgde de inzet van de veiligheidstroepen tegen de onrust in de *townships*, waarop de politieke omwenteling van 1994 volgde. Dat leidde er uiteindelijk toe dat het Zuid-Afrikaanse leger opnieuw werd omgevormd, nu tot de huidige South African National Defense Force.

Mislukte Security Sector Reform

Over die laatste omslag gaat het boek van Daniel L. Douek. Hij merkt in dit verband een vreemde discrepantie op. Tegen de verwachting van velen in maakte Zuid-Afrika namelijk rond 1994 een bijna voorbeeldige politieke omwenteling door. Het Apartheidsregime stond 'vrijwillig' zijn plaats af aan een nieuw bewind, met een parlementair democratisch systeem en evenredige vertegenwoordiging. Er werd algemeen kiesrecht ingevoerd. Daarop volgden verkiezingen die eerlijk verliepen. Er kwam een grondwet tot stand, met vooruitstrevende trekken. Het fundament werd gelegd voor een functionerende rechtstaat. De Truth and Reconciliation Commission speelde een belangrijke rol in het verwerken van de nationale trauma's. De economie bleef ondertussen overeind en Zuid-Afrika kon zich handhaven als regionale factor van belang. De *post-transition*-fase verliep kortom ordelijk en vreedzaam. Maar Douek benadrukt terecht dat tegelijkertijd ook de criminaliteits- en geweldcijfers tot de hoogste ter wereld gingen behoren. Dit begon volgens Douek eveneens rond 1994, met onder andere de burgeroorlogachtige taferelen tussen de gewapende strijders van Inkatha (Zulu) en die van het ANC (Xhosa). Het gebrek aan interne veiligheid is erna een groot probleem gebleven. Geweld lijkt endemisch geworden. Déze discrepantie vormt het startpunt voor Douek. De auteur vraagt zich af in *Insurgency and counterinsurgency in South Africa* hoe dit tot stand kon komen. Zijn verklaring is vrij simpel.

In feite betoogt Douek dat in Zuid-Afrika de Security Sector Reform die de politieke transitie begeleidde is mislukt, omdat die vanaf het begin bewust werd gesaboteerd door oude machthebbers en militaire leiders. Demobilisering, werving en training van politie en leger, en hervorming van de inlichtingendiensten zouden systematisch en langdurig zijn gedwarsboomd door een netwerk van mensen die waren gelieerd aan het oude Apartheidsregime. Dit had noodlottige gevolgen voor de veiligheidssituatie in Zuid-Afrika, van voor tot ver ná 1994. Dat was natuurlijk precies de bedoeling. Er zou een 'destabilisation and assassination campaign' zijn opgezet, met een combinatie van

psychologische oorlogvoering, terreur en zelfs *death squads*, die uiteindelijk dus in een disfunctionerend veiligheidsapparaat resulteerde. Er was volgens Douek hiermee sprake van een schaduwoorlog tussen oude *counterinsurgency forces* van het Apartheidsregime en de gewapende tak van het African National Congress, de zogenaamde Umkhonto we Sizwe ('speer van de natie' in iXhosa). De 'campagne' van de oude machten was succesvol, zoals blijkt uit het feit dat de meeste MK-guerrilla's na 1994 *niet* overgingen in de nieuwe veiligheidsdiensten, die zo geen legitimiteit verwierven en geen kwaliteit konden bieden.

Hidden histories

Om deze theorie over een langdurige doorwerking van de *authoritarian security elites* van het Apartheidsregime te onderbouwen, heeft Douek een set boeiende en relevante nieuwe bronnen aangeboord. Douek heeft kans gezien om meerdere ex-guerrilla's van het MK (de gewapende tak van ANC), te spreken over hun guerrilla-ervaringen, over de Zuid-Afrikaanse counterinsurgency en vooral over de transitieperiode rond 1994. Dáár ligt de kracht van dit boek, dat absoluut een belangrijke lacune opvult in de kennis over de cruciale overgangsperiode. Deze verhalen van ex-guerrilla's zijn fascinerend om te lezen; en op het huiveringwekkende af. Er wordt aan het begin van de studie bijvoorbeeld beschreven wat er gebeurde met een MK-strijder tijdens het proces van transitie en demobilisatie. Hij ging zich conform afspraak melden op een kazerne, om op te gaan in de NPKF (de National Peace Keeping Force). Binnen de poort werd hij ontwapend door de ex-vijand. Dat was volgens de regels. Maar dit was natuurlijk ook erg ongemakkelijk voor iemand die zich overwinnaar waande. Daarna werd hij individueel 'geïnterviewd'. Dit gebeurde door een 'zwarte' die overduidelijk al tijden voor 'het regime' werkte (een Askari). Toen bleek ook ineens dat een groot deel van zijn kameraden al was 'gedraaid'. Angst begon te overheersen en onderling wantrouwen nam toe. Sommigen van zijn medestrijders verdwenen uit de kazerne en keerden niet meer terug. Het werd de ex-guerrilla snel duidelijk dat degenen die hij gewapenderhand had bestreden en dacht te hebben overwonnen, nog steeds heel machtig waren. Hij maakte zich daarop uit de voeten.

Dít soort *hidden histories* is waardevol. Het biedt onderbouwing voor de these dat er sprake is geweest van een 'clandestine violent strategy calibrated to shape South Africa's democratic transition'. Dit valt ook eigenlijk niet te bestrijden. Er wás een *shadow state*. Die werkte met wat voor 1994 StratCom werd genoemd (Strategic Communication). Het omvatte tal van *covert*-operaties om de belangen van de witte minderheid te beschermen. Het liep uiteen van *hearts and minds*, tot aan moord op tegenstanders door *death squads*. Meerdere operators uit de hoek van de Zuid-Afrikaanse COIN hebben bevestigd dat het ANC en het Pan Africanist Congress, inclusief de gewapende takken, inderdaad bewust werden *getarget*, onder meer met *rogue units/third forces*, die zogenaamd niet aan de Nasionale Party gelieerd waren, maar er weldegelijk indirect door werden aangestuurd. Douek heeft hierover dus interessante interviews afgenomen. Hij heeft ook sets met andere boeiende interviews gebruikt, onder andere opgetekend door Wolfie Kodesh. Er is verder archiefonderzoek gedaan in het South African History Archive (Braamfontein/Johannesburg). Methodologisch lijkt kortom alles op orde en de centrale these lijkt goed te worden onderbouwd.

Mono-opname

Maar wie aandachtig leest, merkt echter al snel dat vrijwel alles in dit boek is gebaseerd op slechts dertien interviews met ex-guerrilla's. Zij worden bovendien geanonimiseerd opgevoerd als confidentiële bron. Dit is begrijpelijk. De ex-guerrilla's willen onbekend blijven. Maar het maakt veel claims ook oncontroleerbaar. Het blijft verder onduidelijk hoe het zit met de representativiteit van die relatief kleine set anonieme interviews. Echt keihard en controleerbaar bewijs voor zijn these levert Douek zo eigenlijk toch niet. Aanwijzingen voor de ondermijnende activiteiten van de oude elite zijn er. Maar Douek blijft ze op basis van een gering aantal gesprekken vooral steeds herhalen. Herhalen is natuurlijk niet hetzelfde als bewijzen. Daarnaast is er nog het netelige probleem van de onmiskenbare gekleurdheid van de auteur. Uiteraard moest hij het vertrouwen winnen van de betrokkenen. Dit is heel goed gelukt, gezien de openheid van de ex-guerrilla's. Maar het laat zich ook verklaren door het feit dat Douek erg sympathiek staat tegenover hun strijd. De auteur beseft dit. Hij geeft toe dat zijn onderzoek 'blurred the usual boundaries between researcher and subject' (blz. 20-24). Maar wat betekent dit engagement precies voor de kwaliteit van het onderzoek? Dit boek zou eigenlijk natuurlijk ook interviews hebben moeten bevatten met 'daders', om alles in balans te

krijgen. Wat er nu ligt is een mono- in plaats een stereo-opname.

Sterk is wel dat Douek in zijn studie het thema Security Sector Reform (SSR) heel goed uit de verf laat komen. Douek weet, ongetwijfeld omdat hij gedegen politicologisch/sociologisch is geschoold, hierover zeer veel interessants te vertellen. Douek doceert Political Science aan de Concordia University in Montreal, Canada en verwerkt de meest recente literatuur over democratiseringstheorieën en SSR op interessante wijze met de verontrustende verhalen die hij optekende over de *toxic legacies* van het oude regime. Het gekke is wel weer dat Douek hierbij vele mogelijke alternatieve verklaringen voor de geweldsexcessen na 1994 eerst zelf aandraagt, om ze direct daarna ook resoluut zelf weer te verwerpen, en lang niet altijd met overtuigende argumenten. Of het nu gaat om de verwijzing naar interne raciale spanningen, beroerde politieke leiding, corruptie, sociaaleconomische verklaringen, of wat dan ook, zonder enige toelichting of onderbouwing stelt Douek: 'Yet the origins of this violence can be understood properly only by examining the role of apartheid counterinsurgency forces…'. Kijk, als dát het uitgangspunt is, dan wordt het natuurlijk ook de conclusie.

Duidelijk goed-fout-schema

Terwijl de onplezierige werkelijkheid natuurlijk is dat de verklaring voor het huidige geweld in Zuid-Afrika óók moet worden gezocht in het falen en de corruptie van de ANC-elite, meerdere presidenten die het veiligheidsapparaat geen prioriteit hebben gegeven, sociaal-economische ellende, et cetera. Wat hier ontbreekt, kortom, is een bredere context en een scherp oog voor een complex van verklaringen. Uiteindelijk schuilt er achter dit boek een vrij simplistisch eendimensionaal geschiedbeeld. De auteur heeft de neiging de werkelijkheid te reduceren tot aan de ene kant edele vrijheidsstrijders, die streden vóór een proces van democratisering en vóór een goed veiligheidsapparaat, en aan de andere kant de oude 'autoritaire' Apartheids-elites wier donkere slagschaduw viel in een potentieel mooie toekomst, tot ver na 1994. Dat is een heldere plot met een duidelijk goed-fout-schema. Maar het is wat te gemakkelijk, vanwege het monocausale van de verklaring. Eén verklaring is geen verklaring. De auteur identificeert zich té sterk met het MK en maakt de oude blanke elite hoofdverantwoordelijke voor *alle* geweld in Zuid-Afrika, in verleden *en* heden. Waarschijnlijk heeft de *counterinsurgency legacy* van het *authoritarian regime* inderdaad de transitieperiode zeer fnuikend beïnvloed. Maar dit boek levert nog niet het definitieve en overtuigende bewijs daarvoor. Tegengeluiden en alternatieve verklaringen zullen ook moeten worden verdisconteerd. Vooral verklaringen die kunnen samengaan met de these van Douek, zoals sociaal-maatschappelijke en militair-historische. Zeker op dit laatste vlak laat Douek kansen liggen. Er worden wel politiek-theoretische studies verdisconteerd, maar nauwelijks tot geen studies over de militaire geschiedenis van Zuid-Afrika. Terwijl het onderwerp toch een gewapende opstand is, en COIN, en legerhervorming.[1]

Douek heeft al met al een stimulerende studie geschreven. Het overtuigt niet volledig door zijn geëngageerde eenzijdigheid. Juist hierdoor opent dit boek aan de andere kant wel interessante denkrichtingen en onderzoeksmogelijkheden die tot nu toe buiten beeld bleven. De centrale these eruit zal dan ook zeker moeten worden meegenomen in verder onderzoek naar de bijzondere omslag in Zuid-Afrika van 1994. Het zal uiteindelijk ongetwijfeld ook genuanceerd moeten worden. ■

Dr. Henk de Jong (NLDA)

1 Zie o.a.: Ian van der Waag, *A Military History of Modern South Africa* (Philidelphia and Oxford 2018; eerste editie 2015). Dit boek wordt niet gebruikt, terwijl het op pagina's 265 tot 307 toch uitgebreid ingaat op thema's zoals: *Toward a post-apartheid defence policy, The transformation of the Military: integration, rationalisation and demobilisation, The politics of integration and transformation en New roles for the armed forces*. Zie ook: Timothy J. Stapleton, *A Military History of South Africa. From the Dutch-Khoi Wars to the End of Apartheid* (Santa Barbara 2010), met daarin pagina's 152-191 over de Apartheids-periode en 191-195 over de post-Apartheid periode. De literatuur over Zuid-Afrikaanse COIN is trouwens ook breed en goed. Zie o.a.: Abel Esterhuyse, 'South African counterinsurgency: a historiographical overview' in: Paul B. Rich and Isabelle Duyvesteyn, *The Routledge Handbook of Insurgency and Counterinsurgency* (New York 2012) 347-358; Leopold Scholtz, *The SADF in the Border War 1966-1989* (Cape Town 2013).

Vijanden worden vrienden

FOTO RIJKSMUSEUM

Schilderij van De Tocht naar Chatham (juni 1667), waarbij de Nederlandse vloot schepen van de Engelse vloot verbrandde of buitmaakte

'Hoeveel indruk deze tocht op de Engelschen maakte, blijkt uit de boeken der Engelsche geschiedschrijvers, die vermelden, dat de bevolking van Londen uit angst door het opdringen van de Hollandsche vloot in paniek de stad verliet met achterlating van geld en goederen'. In een overzicht over de wapenfeiten van het Korps Mariniers mag de roemruchte Tocht naar Chatham (juni 1667) natuurlijk niet ontbreken.[1] Kort daarvoor was 'het landvolk, dat aan boord diende, het schuim der natie' vervangen door zeesoldaten in vaste dienst: het 'Regiment de Marine'.

Na de Tocht werd de Vrede van Breda gesloten: 'Het doel was bereikt; onder onzen dwang op Engeland was een voor ons voordelige vrede gesloten en de vloot keerde met roem beladen in het vaderland terug'.

Inmiddels kunnen de Engelsen wel leven met de nederlaag van 1667. In 2017 werd gezamenlijk en op vriendschappelijke wijze de 350e verjaardag gevierd van de Battle of Medway, zoals de gebeurtenis heet in Engeland. Prins Maurits opende in Engeland een tentoonstelling over de slag en nam de vlootschouw af van de inkomende Nederlandse vloot. De activiteiten in Chatham stonden vooral in het teken van vriendschap tussen het Verenigd Koninkrijk en Nederland. Het artikel 'The impact of Brexit on the UK-Netherlands defence and security cooperation' in deze editie liet zien dat die vriendschap, ook op militair gebied, tegenwoordig heel sterk is. ■

1 Redactie, 'Het Korps Mariniers 1665-1940', in *Militaire Spectator* 109 (1940) (12) 519-521.

Geef ze een zetel

Linda Polman

Geef Amazon, Facebook en Netflix zetels in de Verenigde Naties, zeggen sommige beursjongens. Multinationale giganten zijn toch al steeds moeilijker te onderscheiden van landen, met hun volksliederen (jingles), vlaggen (logo's), grondwetten (mission statements), ingezetenen (klanten) en bestuurders (aandeelhouders). Walmart heeft ongeveer hetzelfde aantal werknemers als Botswana inwoners, de omzet van Microsoft is net zo groot als het bnp van Brazilië en FedEx bezit meer vliegtuigen dan Air India.

Multinationals zijn bovendien vaak soevereiner dan staten, want die zijn genoodzaakt militair en economisch samen te werken om niet ten onder te gaan. Landsgrenzen betekenen niets meer door internationaal terrorisme en klimaatverandering en Covid-19 maakte duidelijk dat er hoogst specialistische antwoorden nodig waren waarvoor staten afhankelijk waren van multinationale farmaceutische giganten.

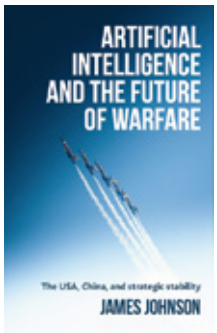
De deur tussen staten en multinationals draait al decennia soepel in het rond. Zonder private beveiligingsbedrijven kunnen staten geen oorlog meer voeren (tijdens de Global War on Terror liepen in Irak 48.000 huurlingen rond; twee of meer legerdivisies). CocaCola groeide tijdens de Tweede Wereldoorlog hand in hand met het Amerikaanse leger de pan uit. CocaCola beloofde dat elke geüniformeerde Amerikaan waar ook ter wereld voor 5 dollarcent een Coke moest kunnen kopen. Tegelijkertijd gaf generaal Dwight D. Eisenhower zijn leger orders om de bouw van Coke-bottelarijen te faciliteren. Er kwamen er totaal 64, allemaal zo dicht mogelijk rond slagvelden in Europa en Azië. Meer dan vijf miljard flesjes werden geconsumeerd door Amerikaanse militairen. Bonus was dat de lokale bevolkingen voor het eerst Coke proefden. Onmiddellijk na de vrede kwamen er tientallen bottelarijen bij. Intussen wappert de vlag van McDonald's trots boven Gitmo.

De CEO van ExxonMobil werd Donald Trumps minister van Buitenlandse Zaken en Facebook nam de Britse vicepremier Nick Clegg in dienst om alle klachten over Facebook als initiator van geweld en beïnvloeder van verkiezingen in ontvangst te nemen. We weten allemaal dat multinationals wetten kunnen wijzigen nog voordat ze worden aangenomen, en wetten die zijn aangenomen kunnen saboteren: Uber belooft de boetes te betalen voor mensen die de nieuwe abortuswetgeving in Texas overtreden.

Toen de eerste man voet zette op de maan was er geen discussie over welke vlag hij er zou planten: het moest de Amerikaanse zijn, ook al had de VS de maan zonder IBM nooit kunnen bereiken. Nu scheren de logo's van Virgin en Elon Musk door het zwerk. Musk bepaalde eenzijdig al dat Mars een 'vrije planeet' is en aardse regeringen geen zeggenschap hebben over wat commerciële bedrijven daar willen doen. Niemand spreekt hem tegen.

De VN gaf een waarnemerszetel aan een intergouvernementele organisatie die zich zorgen maakt over de zeebodem. Je kunt je afvragen of die relevanter is dan Twitter. Net als je je kunt afvragen of Zuid-Soedan, sinds 2011 de nieuwste VN-lidstaat, belangrijker is dan Jeff Bezos. Het bnp van Zuid-Soedan is 4 miljard dollar. Dat is twee procent van wat Bezos waard is. VN-secretaris-generaal António Guterres veroordeelde de 'miljardairs die joyriden in de ruimte terwijl op aarde miljoenen mensen honger lijden'. Maar ik denk toch dat hij liever met Jeff Bezos vergadert over de toekomst van de aarde dan met president Salva Kiir van Zuid-Soedan. ■

SIGNALERINGEN



Artificial Intellligence and the Future of Warfare

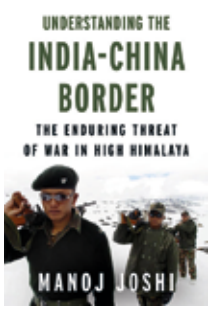
The USA, China and Strategic Stability
Door James Johnson
Manchester (Manchester University Press) 2021
240 blz.
ISBN 9781526145055
€ 95,-

In *Artificial Intellligence and the Future of Warfare* kijkt James Johnson naar de gevolgen die wapensystemen met kunstmatige intelligentie zullen hebben voor de strategische stabiliteit tussen de kernmachten VS en China. 'Disruptieve technologieën', zo concludeert Johnson, zijn een vast onderdeel geworden van de veiligheidsagenda. Het handhaven van de strategische stabiliteit is daar een onderdeel van. Johnson staat stil bij deterrence en escalatiemanagement, de invloed van artificial intelligence op het gedigitaliseerde slagveld en de snijvlakken met robottechnologie, drone swarming en big data. Volgens de auteur zal kunstmatige intelligentie de manier waarop beleidsmakers over nucleaire afschrikking denken diepgaand beïnvloeden.

Schaduwoorlog Uruzgan

De rauwe werkelijkheid van de Nederlandse missie in Afghanistan
Door Olof van Joolen en Silvan Schoonhoven
Amsterdam (Nieuw Amsterdam) 2021
272 blz.
ISBN 9789046829158
€ 20,99

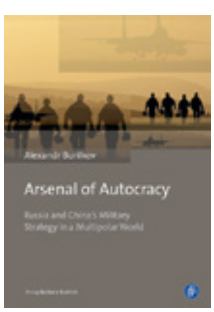
Olof van Joolen en Silvan Schoonhoven, verslaggevers van *De Telegraaf*, brengen in *Schaduwoorlog Uruzgan* de Nederlandse missie (2006-2010) in de Afghaanse provincie in kaart. Het was de grootste Nederlandse militaire operatie na de Tweede Wereldoorlog, door de politiek overwegend omschreven als een opbouwmissie. In werkelijkheid moesten Nederlandse militairen gevechten leveren met de Taliban, een irreguliere tegenstander. In het boek vertellen militairen over angstige momenten, kameraadschap en trauma's. Ook komt de vraag aan de orde of Nederland te veel geweld heeft gebruikt, zoals bij de Slag om Chora, of juist te weinig doortastend optrad. En wat is er met de missie bereikt?



Understanding the India-China Border

The Enduring Threat of War in High Himalaya
Door Manoj Joshi
Londen (Hurst) 2021
256 blz.
ISBN 9781787385405
€ 35,-

In 2020 kwamen China en India dicht bij een oorlog vanwege hun grensconflict in de Himalaya. Er braken gevechten uit die tientallen levens eisten, voordat de rust door overleg werd hersteld. Maar die rust is sowieso schijn, schrijft de Indiase journalist-onderzoeker Manoj Joshi in *Understanding the India-China Border*, want de hele, 4.000 kilometer lange grens tussen de twee kernmachten is omstreden. Vanaf de jaren 90 hebben India en China geprobeerd het grensconflict op te lossen, maar meer dan voorlopige akkoorden kwamen daar niet uit omdat de partijen bang zijn geopolitieke en strategische belangen op het spel te zetten.



Arsenal of Autocracy

Russia and China's Military Strategy in a Multipolar World
Door Alexandr Boerilkov
New York (Columbia University Press) 2021
250 blz.
ISBN 9783847423270
€ 47,-

Alexandr Boerilkov onderzoekt in *Arsenal of Autocracy* de militaire strategie en modernisering van Rusland en China na 2001. Boerilkov ziet een complex internationaal systeem, waarin de macht van de Verenigde Staten afneemt. Tegelijkertijd proberen andere landen, waaronder Rusland en China, hun invloed in de wereld uit te breiden, waarbij ze de Amerikanen in verschillende regio's, waaronder Azië, militair uitdagen. Boerilkov kijkt wat dit betekent voor de rol van de NAVO en hoe de Amerikanen de alliantie de afgelopen twintig jaar zijn gaan zien. Militair-strategisch kijken Rusland en China niet alleen naar het Westen, maar uiteindelijk ook naar elkaar.


N 326
326