

MILITAIRE SPECTATOR

THE SUWALKI GAP DILEMMA



- Moral injury
- De cyber confidence-illusie

MILITAIRE SPECTATOR

Vooruitblik

In *Militaire Spectator* 12-2020 verschijnt onder meer: 'The Impact and Security Implications of Bosnia's Parallel Power Structures on Implementation of the Dayton Accords' van col U.S. Air Force (ret) Michael Dziedzic.

The General Framework Agreement for Peace in Bosnia and Herzegovina, commonly known as the Dayton Accords, was signed in 1995. The agreement envisioned deployment of an Implementation Force (IFOR) 'for a period of approximately one year.' 25 years later, a look at security issues shows that Bosnia has been unable to surmount embedded political instability, to advance toward Euroatlantic integration, or provide anything more than a semblance of democratic governance for its citizens. This is primarily the result of mis-diagnosis of the

conflict as resulting exclusively from 'ancient ethnic hatreds' while failing to recognize until far too late the role that parallel power structures (spoilers) in each of Bosnia's ethnic communities played in instigating the conflict, collaborating to profit from it economically and politically, and subsequently paralyzing Dayton's implementation.

Bosnia remains a dysfunctional state while the conflict is frozen. Illicit structures persist that sustain criminalized power brokers in each ethnic community. They share a common purpose in preventing the rule of law from taking root. The need to engender the rule of law and functional transparency and accountability mechanisms is obvious; however, the way to unravel this Gordian knot after 25 years is not. For NATO, essential for its future peace and stability operations will be developing a shareable assessment methodology with its prospective international partners to identify likely spoilers prior to drafting a mandate. ■



FOTO NAVO

MEDEDELING KVBK

KVBK-lid? Geef uw e-mailadres door aan de ledenadministratie

Van veel KVBK-leden ontbreekt het e-mailadres nog in de ledenadministratie. Het doorgeven van een e-mailadres kan via <http://www.kvbk.nl/e-mailadres-kvbk-lid> of door de hier afgebeelde QR-code te scannen. De KVBK gebruikt e-mailadressen alleen om leden te informeren over verenigingszaken en deelt ze niet met derden.



UITGAVE

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

Secretaris en ledenadministratie

luitenant-kolonel drs. D. Boissevain
E secretaris@kvbk.nl
Nederlandse Defensieacademie (NLDA)
Sectie MOW
Ledenadministratie KVBK
Postbus 90002, 4800 PA Breda
E ledenadministratie@kvbk.nl

REDACTIE

Igen b.d. ir. R.G. Tieskens (hoofdredacteur)
drs. A. Alta
kol Marns drs. G.F. Booij EMSD
kol drs. A.J.H. Bouwmeester
prof. dr. A. ten Cate
dr. A. Claver
drs. P. Donker
bgen prof. dr. mr. P.A.L. Ducheine
cdre KLu b.d. F. Groen (plv. hoofdredacteur)
kol ir. M.P. Groeneveld
kap (R) L.J. Leeuwenburg-de Jong MA
(e-outreach)
kol mr. drs. B.M.J. Pijpers
drs. E.N. van der Steenhoven
mr. drs. A. van Vark KMar
ktz drs. H. Warnar

BUREAUREDACTIE

M. Katsman MA
dr. F.J.C.M. van Nijnatten (eindredactie)
NIMH
Postbus 90701
2509 LS Den Haag
T 070 – 316 51 20
E redactie.militaire.spectator@mindef.nl
www.militairespectator.nl
facebook.com/militaire-spectator
twitter.com/milspectator

De Militaire Spectator is
aangesloten bij de European
Military Press Association

**LIDMAATSCHAP**

binnenland € 25,00
studenten € 17,50
buitenland € 30,00

OPMAAK

Coco Bookmedia

DRUK

Wilco Meppel
ISSN 0026-3869
Nadruk verboden

Coverfoto: U.S. Marines dismount
MK27 seven-ton vehicles during Exercise
Saber Strike 18 near Skrunda, Latvia
Foto: U.S. Marine Corps, Angel Travis

MILITAIRESPECTATOR

540 The Suwalki Gap Dilemma: A Strategic and Operational Analysis

L. Scholtz

Concerning the Suwalki Gap, NATO has the options to continue pretending that its present countermeasures are adequate to stop and even roll back a Russian invasion or to increase its defence spending considerably.

554 Moral injury: de psychische impact van moreel-kritische situaties tijdens en na uitzendingen

T. Molendijk

Militaire interventie kan grote morele impact hebben op uitgezonden militairen en om morele verwonding te helpen voorkomen en te verwerken is erkenning belangrijk op de niveaus van de militaire organisatie, politiek en maatschappij.

568 De cyber confidence-illusie

K. Arnold

Cyberaanvallen kunnen een bedreiging vormen voor internationale vrede en stabiliteit, maar het lukt de internationale gemeenschap niet om normen voor het gedrag van staten in cyberspace te ontwikkelen en te implementeren.

En verder:

Editoriaal	538
Gastcolumns	584
Tegenwicht	588
Boeken	590
RetroSpectator	603
Andere ogen	604

Amerikaanse invloeden op de Nederlandse verkiezingen

De verkiezingen in de Verenigde Staten zouden volgens de opiniepeilingen een grote overwinning opleveren voor de Democratische presidentskandidaat Joe Biden en zijn partijgenoten in het Congres. 3 november werd verwacht dat veel Amerikanen zouden kiezen voor verandering na vier jaar Donald Trump, en de vele controverses die sinds de aanstelling van de Republikeinse president hebben gespeeld. In combinatie met de coronapandemie met meer dan 200.000 doden, stijgende werkloosheid en een economische neergang moest een duidelijke winst voor Joe Biden mogelijk zijn. Heel de wereld was gekluisterd aan CNN, waar *soon* en *any moment now* een nieuwe betekenis kregen. Maar het duurde uiteindelijk dagen totdat Biden tot winnaar uitgeroepen kon worden, want zijn overwinning was allermist een *landslide*; er was een groter dan verwacht aantal Amerikanen dat voor Trump koos.

Hoe komt het dat Trump zo populair bleef na de dramatische gevolgen van de coronaviruspandemie, economische neergang en werkloosheid in de dubbele cijfers? Hoe was het mogelijk dat velen toch op hem stemden na de talloze schandalen, na het Mueller-rapport en zijn *impeachment*, na de grote hoeveelheid veroordelingen in zijn omgeving, na diverse boeken waarin een donker beeld geschetst werd van zijn

karakter, na berichtgeving over minachting voor de troepen en zijn openlijke bewondering voor dictators? En vooral na zijn niet aflatende Twitterberichten, waarin hij de bestaande normen en waarden niet volgde en velen persoonlijk schoffeerde?

Kortom, waarom brachten onverwacht toch zoveel miljoenen Amerikanen hun stem op Trump uit?

Natuurlijk zijn er veel binnenlandse traditionele verklaringen in Amerika. *Evangelicals* en hoger opgeleide sociaalconservatieven zagen dat Trump zich als geen ander een weg gebaad heeft door wat hij de diepgewortelde bureaucratie en het liberale establishment noemt. Met hulp van de Senaat stelde hij meer dan 200 conservatieve rechters aan, onder wie drie voor het Hooggerechtshof, ter ondersteuning van anti-abortuswetgeving en ander sociaalconservatief beleid. Daarnaast heeft hij de belastingen verlaagd, met name de vennootschapsbelasting, en vele economische en milieuregels afgeschaft. Dit alles, naast het erkennen van Jeruzalem als de hoofdstad van Israël, het actief veroordelen van Iran en het verbieden van de toegang tot de VS voor talloze moslims, was blijkbaar voor velen genoeg aanleiding om over de verwaarloosde waarden

en normen en persoonlijke antipathie heen te stappen, de vele aanwijzingen over corruptie door de vingers te zien en op Trump te stemmen.

Ook op het gebied van defensie heeft de Amerikaanse president zich de afgelopen jaren niet onbetuigd gelaten. Door het grote aantal incidenten dat er heeft gespeeld, is het moeilijk te duiden hoe de Amerikaanse kiezer de plannen van Trump heeft gewaardeerd om eventueel de Nationale Garde de straat op te sturen bij rellen of zijn plan om Amerikaanse militairen uit Duitsland terug te trekken. Trumps unilaterale optreden binnen NAVO-missies en zijn ontbrekende solidariteit met bondgenoten tegen bijvoorbeeld de Russische vergiftigingen in het Verenigd Koninkrijk en Duitsland en de moord op Khashoggi hebben de kracht van de alliantie verzwakt. Ook het verbreken van andere belangrijke multilaterale afspraken zoals de Iran-deal hebben ervoor gezorgd dat het niet de meest voorspoedige jaren zijn geweest voor de trans-Atlantische link. Aan de andere kant is Trump voor NAVO-bondgenoten wel duidelijk geweest over wat hij verwacht van de bijdrage aan defensie die iedereen in 2014 in Wales heeft toegezegd. Het lijkt wel vast te staan dat Trump veel kiezers heeft verloren onder militairen na de berichtgeving over zijn uitspraken tegen veteranen. Het aantal generaals, meestal gepensioneerd, dat openlijk afstand nam van zijn defensiebeleid is tekenend voor het gebrek aan steun in die hoek.

De populist Trump heeft ook zijn vinger aan de pols van het lager opgeleide blanke deel van Amerika. Hij kwam zijn afspraken na, bouwde een muur aan de grens met Mexico en ging het gevecht aan met China. Hij heeft het gevoel voor nationalisme hersteld en de politie verdedigd. En – niet onbelangrijk – hij heeft in de coronacrisis gehamerd op een positieve boodschap: het openen van de economie in plaats van het sluiten. Maar wat is er nog meer aan de hand? Hoe kon Trump al deze effecten bereiken en de verkiezingsopkomst drastisch verhogen? Is er een veel fundamentele trend die ook consequenties heeft voor Nederland en mogelijk verregaande gevolgen voor onze liberale demo-

cratieën. Er is in elk geval één belangrijke trend die ook in Nederland opgeld doet.

Al in 2016 hadden de Amerikaanse verkiezingen last van de verspreiding van desinformatie via bijvoorbeeld Facebook, gecombineerd met het hacken van onder meer de Democratische Partij en e-mails van presidentskandidaat Hillary Clinton. Er is sindsdien veel aandacht voor de aanpak van desinformatie door socialemedia-platforms, maar er is weinig grip op. Sociale media kunnen desinformatie, samenzwerings-theorieën en leugens disproportioneel over de hele wereld verspreiden en geven populist en autocraten daarmee een platform voor gerichte propaganda. Criminelen, statelijke actoren of andere groeperingen kunnen nauwelijks gehinderd door sancties en regels mensen beïnvloeden met verschillende doelen.

Ook in Nederland zijn deze effecten merkbaar. Dezelfde sociale media zijn immers ook bij ons beschikbaar. Onderscheid tussen op feiten gebaseerde berichtgeving en *fake news* zijn soms moeilijk te maken. Het afdoen van wetenschappelijke bewijzen als ‘ook maar een mening’ is een gevaarlijke trend. Onze verkiezingen van 2021 zullen mogelijk, net als in de VS, niet alleen gaan over beleid en argumenten daarvoor, maar ook over de feiten die daaraan ten grondslag liggen. De gedeelde waarheid, normen en waarden waarop onze liberale democratie is gebaseerd, is geen vanzelfsprekendheid meer. Stemmen winnen gaat daarom niet meer alleen over overtuigen op basis van ideeën maar ook over het overtuigend rechtzetten van continu in twijfel getrokken feiten.

Voor nu zullen velen opgelucht ademhalen, het multilateralisme lijkt met de winst van Biden voorlopig gered. De democratie leeft nog en normen en waarden zullen door de nieuwe president zeker worden hersteld. Maar laat de mogelijke invloed van desinformatie, het gebrek aan onafhankelijke op feiten gebaseerde informatie en een open debat daarover, die de Amerikaanse verkiezingen hebben gedomineerd, een goede waarschuwing zijn voor ons bij de verkiezingen in maart volgend jaar. ■

The Suwalki Gap dilemma

A strategic and operational analysis

Leopold Scholtz*

In NATO circles, considerable concern was caused by Russian President Vladimir Putin's aggressive posture, especially since the invasion, occupation and annexation of Crimea, and his support for separatist rebels in eastern Ukraine. The general expectation was that any future aggression would either come in Ukraine or the Balkans, or perhaps rather in the areas adjacent to the Baltic Sea. There, it is feared, Putin could try to regain control over the Baltic republics, Estonia, Latvia and Lithuania, territories that used to be part of the Soviet Union until its demise at the end of 1991.¹ If that happens, the operational focus would fall on the so-called Suwalki Gap, the some 90-km-wide gap between the Russian exclave of Kaliningrad and the nominally independent ex-Soviet republic of Belarus. It is through this gap that NATO would have to rush reinforcements and supplies from Poland to the Baltic republics, and it is this gap that Russia would have to close to prevent that. It is possible that events may quickly spiral out of control once the fuse is lit. The purpose of this article is, therefore, to analyse the strategic and operational aspects surrounding the possible scenarios regarding the Suwalki Gap in the event of a Russian attempt to retake the Baltic republics.



The article begins by analysing the broad Russian approach to international politics and how the Russians view their own place in the world, after which these insights will be applied to the Russian position towards the Baltic states. Subsequently, NATO's contrasting view is analysed, as is the crucial operational importance of the Suwalki Gap between Poland and the Baltic states for countering a Russian offensive. The article concludes with a possible scenario of how such a Russian offensive against the Baltics may unfold, and how it may escalate very quickly into a general war.

Vladimir Putin's grand strategy

When trying to read Vladimir Putin's mind to assess his grand strategy, several things must be kept in mind. The first is a maxim by the British strategist Sir Basil Liddell Hart, who drew up

several battlefield guidelines for military commanders. One of them was: 'Take a line of operation which offers alternative objectives. For you will thus put your opponent on the horns of a dilemma, which goes far to assure the chance of gaining one objective at least – whichever he guards least – and may enable you to gain one after the other.'²

Liddell Hart was, of course, writing about the operational level of war, but his words may

* Dr. Leopold Scholtz is a retired political commentator, writing for several news media. He is also a military historian and the author of *The SADF in the Border War 1966-1989* (Cape Town, Tafelberg, 2013) as well as *The Battle of Cuito Cuanavale* (Solihull, Helion, 2016) and *Ratels on the Lomba: The story of Charlie Squadron* (Johannesburg, Jonathan Ball, 2017). He is a research fellow at North-West University's Research Focus Area Social Transformation (Potchefstroom campus). He retired as a captain in the Reserve Force of the South African Army.

1 See for instance Larisa Brown, 'Putin's dry run for invading Europe', in: *Daily Mail*, 21 December 2017.

2 Basil H. Liddell Hart, *Strategy* (New York, Praeger, 1954) 348.

German soldiers of NATO's Very High Readiness Task Force conduct a river crossing training

PHOTO NATO, MARC-ANDRÉ GAUDREAU





A Ukrainian soldier sits atop a BMP-1 infantry-fighting vehicle during Exercise Combined Resolve in Hohenfels; the 2014 Russian take-over of Crimea and part of Ukraine was an important wake-up call for the West

PHOTO NATO

equally apply to security strategy as well. With this in mind, let us read one pair of analysts' uncertainty: 'Many analysts emphatically insist that Russia is fundamentally revisionist. Others reject this interpretation and maintain precisely the opposite. The first camp believes that Russia harbours irredeemably expansionist ambitions and strives to reassert imperial control over the region. Though Russia is willing to use force to achieve this goal, it is content to use subversion and provocation to shape conditions until the time is right for a *fait accompli*. The second camp takes a more sympathetic view and portrays Russia as a defensive actor. Fear rather than imperial impulses animate Russian foreign and defense policy. It begrudgingly accepts that Estonia, Latvia, Lithuania and Poland are members of NATO. Yet Russia is justifiably

concerned that the United States will do everything in its power to prevent Russia from occupying its rightful place as a great power peer... Compounding the problem is that Russia's actions are entirely consistent with both narratives.'³

A third element is the introduction of the concept of hybrid warfare (called 'new-generation warfare' by the Russians)⁴ by the Chief of the Russian General Staff, General Valery Gerasimov. In an article in a Russian military journal in February 2013, he wrote of new methods of warfare, which he defined as 'military means of a concealed character, including carrying out actions of informational conflict and the actions of special-operations forces. The open use of forces – often under the guise of peacekeeping and crisis regulation – is resorted to only at a certain stage, primarily for the achievement of final success in the conflict.' He went on, referring to 'non-standard' applications of force: 'Frontal engagements of large formations of forces at the strategic and

3 Michael A. Hunzeker and Alexander Lanoszka, 'Threading the needle through the Suwalki Gap', 26 March 2019. See: <https://www.eastwest.ngo/idea/threading-needle-through-suwa%C5%82ki-gap>.

4 Ulrich Kühn, *Preventing Escalation. A NATO Playbook* (Washington, Carnegie Endowment for International Peace, 2018) 15.

operational level are gradually becoming a thing of the past. Long-distance, contactless actions against the enemy are becoming the main means of achieving combat and operational goals... Asymmetrical actions have come into widespread use, enabling the nullification of an enemy's advantages in armed conflict. Among such actions are the use of special-operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as informational actions, devices, and means that are constantly being perfected.⁵

In his testimony before the Armed Services Committee of the U.S. House of Representatives, Christopher S. Chivvis of the RAND Corporation translated the 'Gerasimov doctrine' into three objectives: Capturing territory without resorting to overt or conventional military force; creating a pretext for overt, conventional military action, and using hybrid measures to influence the politics of countries in the West and elsewhere. This includes information operations, using cyberspace, proxies, clandestine measures, and economic and political influence.⁶

The Russian take-over of Crimea, and part of Ukraine, may serve as an excellent example. During the night of 27-28 February 2014, heavily armed men, clad in camouflage uniforms without identifying insignia, appeared all over Crimea. They speedily moved to seal off all Ukrainian military bases and police stations, and occupied all key points in the territory, including broadcasting centres and government buildings. President Putin feigned ignorance, saying that these were 'local self-defence forces'. Later a clearly amused Putin admitted on television that the 'green men', as they became known, were in fact Russian soldiers acting under his command.⁷ Tactically, it was brilliant. By misleading and surprising Ukraine and the West, and using overwhelming force for the crucial first 48 hours, Putin ensured that Crimea was taken without a shot being fired.

In 2015, Putin told an American academic, Professor Daniel Treisman (University of California) that 'the operation to seize the

[Crimean] peninsula was 'spontaneous' and 'not at all' planned long in advance'.⁸ This fits in with the view that Putin is primarily an excellent tactician with an unerring eye for a gap, rather than a thoughtful strategist with a master plan. At times, he gives the impression that he would like to restore either the entire Soviet Union or, at any rate, the core areas, being the Russian Federation, Ukraine, Belarus, the Baltic republics and, perhaps, Georgia.

Putin himself made it crystal clear: '[O]ur country will continue to actively defend the rights of Russians, our compatriots abroad, using the entire range of available means.' He added: 'I am referring to those people who consider themselves part of the broad Russian community; they may not necessarily be ethnic Russians, but they consider themselves Russian people.'⁹

German political scientist Hannes Adomeit concludes that the old USSR is Putin's 'conceptual point of reference', rather than 'a precise geographic and geopolitical frame of reference that determines his policies'. In 2008 Putin said at an international conference: 'The fall of the USSR was a great [sometimes wrongly translated as 'the greatest'] political catastrophe of the 20th century.' And in 2011 he said the USSR was simply 'Russia under a different name.' To him, above all, the USSR's value was in its status as a superpower, equal to that of the USA.¹⁰

-
- 5 Valery Gerasimov, 'Russian military doctrine by General Valery Gerasimov' (translated by Robert Coalson). See: <https://www.facebook.com/notes/robert-coalson/russian-military-doctrine-article-by-general-valery-gerasimov/10152184862563597/>. In March 2019 Gerasimov repeated these thoughts in a speech in Moscow. See: Andrew E. Kramer, 'Russian General pitches 'Information' operations as a form of war', in: *The New York Times*, 2 March 2019).
 - 6 Christopher S. Chivvis, 'Understanding Russian 'hybrid warfare' and what can be done about it', Rand Corporation, 22 March 2017. See: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf.
 - 7 Martin Murphy and Gary Schaub jr., 'Sea of peace' or sea of war: Russian maritime hybrid warfare in the Baltic Sea', in: *Naval War College Review* 71 (2018) (2) 1-2; Michael Kofman et al, 'Lessons from Russia's operations in Crimea and eastern Ukraine' (Santa Monica, RAND Corporation, 2017) 5-25.
 - 8 Daniel Treisman, 'Why Putin took Crimea', in: *Foreign Affairs* 95 (2016) (1) 47.
 - 9 Ivo Daalder, 'Responding to Russia's resurgence', in: *Foreign Affairs* 96 (2017) (6) 33.
 - 10 Hannes Adomeit, 'Putin's 'Greater Russia': misunderstanding or mission?', *Raam op Rusland*, 27 February 2019. See: <https://www.raamoprusland.nl/dossiers/roesski-mir/878-putin-s-greater-russia-misunderstanding-or-mission>.

Putin's tactical brilliance does not mean that he has no grand strategy. Building on Putin's public utterances, Vasily Gatov offers the following reconstruction of Putin's highly nationalist world-view: 'Mother Russia is the absolute good. Positive, educated and well-behaved, it fosters the good for all the neighbors and even non-neighbors. Though sometime before Russia was humiliated and surpassed by some obscure forces, it persistently revives itself and wants to spread the good it represents. But the entire world is ruled by illiterate others (that are also forces from the past) who persistently conspire to harm Russia and its legitimate interests. All these others are villains by default; their goal is to dissect and destroy Russia. This is the world of negation and denial; all others are liars and hypocrites. In order to confront this terminal clash of civilizations Russia needs to employ the spiritual power of its history and faith. Russia is wealthy and resourceful and the others envy its richness and potential. In order to pursue their conspiratorial goals, others make propaganda against Russia, send spies and recruit traitors among Russians. Villains also are persistently lecturing an educated and ingenious Russia about what is appropriate and what is not. Cultured and reasonable Russia needs no lecturing from anyone. The behavior of the others shows their hypocrisy and evil goals.'¹¹

Putin and the Baltic states

Russia lacks defensible borders.¹² This facilitated the invasions by Napoleon in 1812 and Hitler in 1941. Therefore, the real Russian obstacles to invaders are its vast spaces and the intense cold of winter. The distance between Russia's western border and Moscow is so great that even the German mechanised forces, experienced in *Blitzkrieg*, did not reach the capital before the onset of the unbelievably cold winter weather. This was one of the reasons Josef Stalin placed



PHOTO NATO/BUNDESWEHR, MARCO DOROW

the greater part of Central Europe under his control in the late forties. Those countries offered a huge buffer territory which, added to the endless Russian distances, made any invasion by the West totally impossible.

However, the dissolution of the Warsaw Pact (NATO's communist counterpart) and of the Soviet Union itself in 1990-1991, changed Russia's geopolitical position dramatically. The more than 2,000 kms from Hannover near the intra-German border to Moscow were reduced to about 800 kms between the border of the nearest NATO member, Latvia, and Moscow. This contributed to a feeling of insecurity in the

11 Vasily V. Gatov, 'Contagious tales of Russian origin and Putin's evolution', in: *Society* 53 (2016) (6) 620-621.

12 Robert Kaplan, *The Revenge of Geography: What the Map tells us about Conflicts and the Battle against Fate* (New York, Random House, 2012) 155.



Exercise of NATO's Very High Readiness Taskforce. Once the Baltic states are invaded, their fate is sealed

Kremlin; in the 2015 Russian National Security Strategy it is expressly cited as a threat.¹³

In an important policy speech in 2007, Putin identified NATO's eastward expansion expressly with America's aim – in his eyes – to dominate the world. He complained about '[o]ne single centre of power. One single centre of force. One single centre of decision-making. It is a world in which there is one master, one sovereign.'¹⁴

Putin himself expressed the Russian fear in 2014: 'Sometimes I think, maybe it would be better for our bear to sit quiet, rather than to chase piglets in the forest and to eat berries and

honey instead. Maybe they will leave [our bear] in peace. They will not. Because they will always try to put him on a chain... They will rip out its fangs and its claws. Once they've ripped out its claws and fangs, the bear is no longer needed. They will make a stuffed animal out of it... It is not about Crimea. We are protecting our sovereignty and our right to exist.'¹⁵

13 Joe Kyle, 'Contextualizing Russia and the Baltic States', Foreign Policy Research Institute, Winter 2019, 107.

14 Cited in Ivo Daalder, 'Responding to Russia's resurgence', in: *Foreign Affairs* 96 (2017) (6) 32.

15 Cited in Natalya Bugalyova, *How we got here with Russia: The Kremlin's World View* (Washington, Institute for the Study of War, 2019) 21.

As viewed from the Kremlin, the Baltic republics – and, more importantly, their membership of NATO – form a clear threat to Russia’s military security. The question is, how far would Moscow go? In the short term, it seems, not beyond covert measures to undermine Baltic independence. The presence of sizeable Russian-speaking populations in Estonia (25.2 per cent), Latvia (26.9 per cent), and Lithuania (5.8 per cent),¹⁶ may, however, provide the Russian government with a potential Trojan horse to stir up trouble. These Russian-speakers are concentrated in the border regions. For instance, 73 per cent of the population of the Estonian county of Ida-Viru are Russian-speaking, and the region’s largest city, Narva, contains 82 per cent of Russian-speakers.¹⁷ This may then be utilised as a pretext for an invasion.¹⁸

It is very unlikely that Russia is actively seeking to get embroiled in a war with NATO. Vladimir Putin is not Adolf Hitler. He may rather be seen as a chess master, looking for gaps in his opponents’ forces and striking only where there is a reasonable chance of success and where he can neutralise immediate countermeasures through deception and hybrid warfare. Based on what is known about Putin’s political convictions and his tactical flair, it may be assumed that he will wait until a suitable opportunity arises before striking. And then any actions will start off as plausibly deniable hybrid operations along the lines suggested by General Gerasimov.

Once the Baltic states are invaded, their fate is sealed. The Baltic defence forces may slow down the invaders to a limited extent, but will not be able to stop them, let alone repulse them. In a series of wargames in 2014 and 2015, the RAND Corporation’s conclusions were stark: ‘As currently postured, NATO cannot successfully defend the territory of its most exposed members. Across multiple games using a wide range of expert participants in and out of uniform playing both sides, the longest it has taken Russian forces to reach the outskirts of the Estonian and/or Latvian capitals of Tallinn and Riga, respectively, is 60 hours.’¹⁹

At any rate, whether Russia is actively considering military action against the Baltics or not, Putin is clearly putting the West ‘on the horns of a dilemma’. According to the Russian minister of Defence, Sergei Shoigu, the Russian military forces in the areas adjacent to Norway, Finland, Poland and the Baltic republics were reinforced with two divisions and three independent brigades, as well as 5,000 units of new and overhauled weapons systems and pieces of equipment. More than 350 ‘military facilities’ were made operational.²⁰ In addition, the exclave of Kaliningrad (of which more later) has been reinforced with strong conventional land and naval forces and strategic missiles.²¹

At the same time, the Russian defence force has stationed three mechanised divisions along the Ukraine border.²² This means that the Russians are well-placed to strike wherever they want, while NATO is kept guessing as to the Kremlin’s intentions.

The view from Brussels

Obviously, the view from Brussels – and Riga, Tallinn and Vilnius – looks very different. NATO sees Russia as a threat. In 2013, the RAND Corporation analysed the Baltic states’ defence against a possible Russian invasion. The conclusion, as stated previously, was that ‘NATO cannot successfully defend the territory of its most exposed members’, especially that of the Baltics. At the most, it would take between 36

16 Aleksandra Kuczyńska-Zonik, ‘The Securitization of National Minorities in the Baltic States’, in: *Baltic Journal of Law & Politics* 10 (2017) (2) 26-45.

17 Joe Kyle, ‘Contextualizing Russia and the Baltic States’, 108.

18 Linda Robinson et al: *Modern Political Warfare. Current Practices and Possible Responses* (Washington, RAND Corporation, 2018) 85-102.

19 David A. Shlapak and Michael W. Johnson, *Reinforcing Deterrence on NATO’s Eastern Flank. Wargaming the Defense of the Baltics* (Washington, RAND Corporation, 2016) 1.

20 Jaroslaw Adamowski, ‘Amid Russian military buildup, Poland reacts’, *Defense News*, 27 August 2018.

21 Christopher Woody, ‘Russia appears to be building up its military bases near a weak point in the NATO alliance’, *Business Insider*, 11 July 2018. See: <https://www.businessinsider.nl/russia-building-up-military-base-in-kaliningrad-near-suwalki-gap-2018-7/?international=true&r=US>.

22 Catherine Harris and Frederick W. Kagan, *Russia’s Military Posture: Ground Forces Order of Battle* (Washington, Institute for the Study of War, 2018) 1.

and 60 hours for the Russian forces to reach the Estonian and Latvian capitals, Tallinn and Riga, on the Baltic coast. 'Such a rapid defeat would leave NATO with a limited number of options, all bad: a bloody counteroffensive, fraught with escalatory risk, to liberate the Baltics; to escalate itself, as it threatened to do to avert defeat during the Cold War; or to concede at least temporary defeat, with uncertain but predictably disastrous consequences for the Alliance and, not incidentally, the people of the Baltics.'²³

What would NATO's response be to such an invasion? There is some difficulty to interpret President Donald Trump's position. At various times, he has said that the US would not automatically come to the aid of small states threatened by Russia.²⁴ Nevertheless, NATO has taken measures to bolster the Baltics' defence. While the Baltics themselves have strengthened their modest military capability to 57,000 full-time soldiers and reservists,²⁵ NATO decided at its Wales summit in 2014 to establish an

'enhanced Forward Presence' of 5,000 personnel in the Baltics. This force – three infantry battalions, one in each of the Baltic republics, and a fourth in Poland – would consist of contingents supplied by several member states and rotated every few months. They would serve as a kind of 'trip wire' to slow down invasion forces and alert the rest of NATO. Then the so-called NATO Spearhead Force (13,000 troops) would be mobilised and made ready for deployment within 48 hours. It could be at the front within a week. This force's task would then be to win time for the rest of NATO to be made ready for a bigger war. Finally, they would be followed by the Very

23 Shlapak and Johnson, *Reinforcing Deterrence on NATO's Eastern Flank*, 1.

24 Max Fisher, 'Donald Trump's ambivalence on the Baltics is more important than it seems', in: *The New York Times*, 22 July 2017; John Wagner, 'Trump says defending tiny NATO ally Montenegro could lead to World War III', in: *The Washington Post*, 18 July 2018.

25 Kyle, 'Contextualizing Russia and the Baltic States', 109; Stephen Flanagan et al, *Detering Russian Aggression in the Baltic States Through Resilience and Resistance* (Santa Monica, RAND Corporation, 2019).

A military parade in the Russian exclave of Kaliningrad, which turned out to be an excellent forward position to threaten both the Baltic states and Poland

PHOTO ANP/TASS, VITALY NEVAR



High Readiness Joint Task Force (27,000 troops), but these troops' presence on the battlefield would only be felt after 30 days.²⁶

It is here that the so-called Suwalki Gap comes into play. Before we come to that, there is another factor to be looked at, namely the role played by maritime connections across the Baltic Sea. According to a Danish analysis, 'The Baltic Sea is also a major conduit for energy supplies from Russia to Europe, which continues to be a major customer for Russian crude oil. The bulk of this traffic is shipped by tanker from the ports of Primorsk and Ust-Luga near St. Petersburg via the Baltic to northwestern Europe. Furthermore, the Nord Stream gas pipeline runs along the seabed. This consists of two parallel pipes that run from Vyborg in Russia to Greifswald in Germany. The first came on-stream in November 2011 and the second almost a year later. It is currently the longest undersea pipeline in the world.'²⁷

In other words, if a war in this region cuts the flow of gas and oil to Europe, it could have a devastating economic effect in the short term, especially on the NATO member states. In the longer run, of course, Russia too would suffer, but if the Russians could finish the operation rapidly and present the West with a *fait accompli*, things might return to 'normal' rather quickly.²⁸

The Suwalki Gap

The Suwalki Gap takes its name from a Polish town in the far north-east of the country, near the Lithuanian border. Squeezed in between Lithuania and Poland, there is a Russian exclave, approximately 140 square kilometres in size, known as the *Oblast* (region) Kaliningrad, named after the capital city, Kaliningrad. Until 1945, the city was the capital of East Prussia and known as Königsberg. East Prussia was a German

exclave which was divided into two pieces in 1945. The south-western half was given to Poland (then a Soviet satellite state), and the north-eastern half to the Soviet Union as the Oblast Kaliningrad. The German inhabitants fled or were forcibly expelled.

The region was placed under the administrative control of the Russian Federation, the dominant constituent state of the Soviet Union. While the USSR existed, this posed no problem. But when it fell apart at the end of 1991 into its 15 constituent republics, Kaliningrad found itself cut off from Russia, separated by the newly independent Belarus.

The existence of the region as an exclave poses strategic problems for Russia, but has also some advantages. The main problem was that its exposed position makes it vulnerable to attack and difficult to defend, unless very strong deterrent forces are stationed there. On the other hand, Kaliningrad turned out to be an excellent forward position, able to threaten both the Baltic states and Poland. And, being the base of medium-range nuclear missiles, it also threatens the Central European capitals of Warsaw, Budapest, Prague, Bratislava, and even Vienna and Berlin.

Should President Putin ever decide to take the Baltics, geography dictates an invasion from the Russian territory immediately east of Estonia and Latvia, as well as from Kaliningrad. This means that the Baltic republics may be invaded simultaneously from the east and the southwest, making any defence difficult.

If NATO theory is put into practice, the Alliance will then mobilise its Spearhead Force. While the Spearhead Force, together with the Baltic militaries, tries to slow down the Russian advance, the Very High Readiness Joint Task Force will assemble along the border between Lithuania and Poland and try to hit the Russian invaders' southern flank.

This border, about 90 kilometres long, is the Suwalki Gap. But hitting the Russian invaders will not be easy. On the western side the border

26 Jens Ringsmose and Sten Rynning, 'The NATO Response Force: A qualified failure no more?', in: *Contemporary Security Policy* 38 (2017) (3) 447.

27 Martin Murphy, Frank G. Hoffman and Gary Schaub jr., *Hybrid Maritime Warfare and the Baltic Sea Region* (Centre for Military Studies, University of Copenhagen, November 1916) 7.

28 Murphy, Hoffman and Schaub, *Hybrid Maritime Warfare and the Baltic Sea Region*, 9.

ends at the Oblast Kaliningrad; on the eastern side at the Belarusian border. Belarus is an independent ex-Soviet state, but normally stays close to Russia in its foreign policy. It is quite conceivable that the country may allow Russia to utilise its territory for an invasion of Lithuania and to close off the Suwalki Gap.²⁹ The Kaliningrad region at the other end of the Gap is well-placed to plug the hole as well.

Any NATO force trying to get through to Lithuania and the other Baltic countries will, therefore, have to fight its way through a Russian army which, in the short term, will be considerably stronger. As Professor Mark Galeotti of the Royal United Services Institute points out: 'The Russian calculus is that there may not be a longer term, especially if it was able to threaten nuclear strikes or similarly-disabling precision conventional ones to a bring a conflict to an early end.'³⁰

In other words, although Russia's relatively weak economy makes the country vulnerable in a longer war, its stronger forces at the flashpoint give them an advantage not to be trifled with, especially if they succeed in achieving tactical and operational surprise. They may then confront NATO with a *fait accompli*, making a longer war unnecessary.

A study co-authored by a former General commanding US forces in Europe, Lieutenant-General Ben Hodges, makes it clear exactly how important the Suwalki Gap is. Three features are identified:

- It separates the Russian motherland from Oblast Kaliningrad and its naval bases.
- Cutting off the corridor could strangle the three Baltic states and prevent NATO aid from getting through.
- Closing the corridor 'would provide Moscow with a contiguous military front between the Baltic Sea and Ukraine, consolidate its political stranglehold over Belarus, and more directly threaten Poland's sovereignty and territorial integrity.'³¹

The Russians' possession of Kaliningrad is a very strong tactical and operational advantage. Logic

The exclave Kaliningrad poses strategic problems for Russia, but also some advantages

dictates that the Alliance will have to do something about the exclave very soon after hostilities break out. Nikolai Sokov, a Russian-American academic, refers to 'the artillery and short-range missiles' stationed in Kaliningrad. He paints an interesting picture of the difficulties NATO forces would encounter in the Suwalki region: 'Terrain is difficult and there are only two roads [as well as one railway line – LS] that allow fast reinforcement. The bottom line – Russia does not have to send tanks, as everyone fears, to prevent NATO reinforcements: it can use artillery or other strike assets to destroy the roads and keep them closed for a fairly extended period of time. If the RAND Corporation estimate (thirty-six to sixty hours) is to be believed, then these reinforcements should arrive hours sooner, perhaps in twenty-four hours or so. If one imagines a more efficient Russian offensive, then they should be in place twelve to eighteen hours after commencement of hostilities.'³²

Moreover, the report co-authored by General Hodges makes it clear that the vicinity is not very conducive to manoeuvre warfare: 'One of

29 Mason Clark and Nataliya Bugayova, 'Russia in review, May 9 – 13, 2019', *Institute of the Study of War*. See: <http://iswresearch.blogspot.com/2019/05/russia-in-review-may-9-13-2019.html>; David Axe, 'Is Russia trying to take over Belarus', in: *The National Interest*, 14 May 2019.

30 Mark Galeotti, 'Russia and NATO both think that time is on their side', *Raam op Rusland*, 17 April 2019. See: <https://www.raamoprusland.nl/dossiers/militaire-beleid/1267-russia-and-nato-both-think-time-is-on-their-side>.

31 Ben Hodges, Janus Bugajski and Peter B. Doran, 'Securing the Suwalki Corridor: Strategy, Statecraft, Deterrence and Defense', *Center For European Policy Analysis*, 9 July 2018, 22.

32 Nikolai Sokov, 'How NATO could solve the Suwalki Gap dilemma', in: *The National Interest* 1 May 2019. See: <https://nationalinterest.org/feature/how-nato-could-solve-suwalki-gap-challenge-55347>.

the most significant takeaways: large parts of the Suwalki Corridor can be a nightmare for maneuver. The region's confined rolling fields are disrupted by chain lakes, rivers, streams, thick stands of forest, and muddy soil during rainy seasons, favoring the defender. Only two narrow roads physically connect the Polish-Lithuanian border — making for a tight and predictable funnel through which to move brigade-sized or larger formations.³³

The Kaliningrad problem

We have seen how the Oblast Kaliningrad, being cut off from the Russian motherland, is an exposed territory, but, at the same time, a valuable forward asset. Its main value lies in the possibility of augmenting a Russian invasion

into the Baltics from the east with a simultaneous advance from the southwest, of helping to close down the Suwalki Gap, and to blackmail the eastern NATO members with nuclear missiles.³⁴

Any NATO general pondering how to respond to a Russian invasion of the Baltic states will have to focus on Kaliningrad as well. If the planned NATO counteroffensive is to happen, the threat from Kaliningrad will have to be neutralised at all cost and very quickly. Therefore, according to Sokov, a 'massive increase of NATO presence in the vicinity of the Suwalki Gap should remain part of the menu of options'.³⁵

Another obvious course of action is to take out the Russian military in the Kaliningrad region almost from the first hour of fighting. This may entail a ground offensive to occupy the region. But that would be very risky in view of the huge military buildup in the exclave and the danger of escalation, perhaps even to the nuclear level. The other alternative is an overwhelming air

33 Hodges, Bugajski and Doran, 'Securing the Suwalki Corridor', 18.

34 Sokov, 'How NATO could solve the Suwalki Gap dilemma'.

35 Ibidem.



*Former commander of U.S. Army Europe
Lieutenant-General Ben Hodges
co-authored a study on the importance of
the Suwalki Gap*

PHOTO U.S. DEPARTMENT OF DEFENSE, STEPHEN MALONE

and missile bombardment to paralyse the Russian forces in the vicinity right from the beginning. In the light of the incomparably smaller risk to NATO, it stands to reason that this option would be favoured by the Alliance's military and political structures. That would, however, only be possible if the NATO forces in Poland and Lithuania are considerably strengthened.³⁶ Kaliningrad, in any language, amounts to a very tough nut to crack.

A war scenario

Let us now imagine a – theoretical – war scenario between Russia and NATO in the Baltic region.³⁷ Given the Russian propensity for avoiding conventional clashes in favour of hybrid warfare, it is logical to assume that Russia will not attempt a full-scale invasion after a period of increasing tension and build-up of its forces along the border. That would give NATO ample warning to start countermeasures. Instead, one may assume a lightning strike without warning. Combined with a smoke screen, figuratively speaking, to place NATO 'on the horns of a dilemma' and mislead the West, this would slow down any NATO response considerably. It stands to reason that the invaders would strive to stay, as it were, below the Article 5 threshold as long as possible.

In an ideal situation – from Moscow's perspective – NATO could even be persuaded not to intervene at all. One may assume that Russia will see to it that a plausible excuse for its own military movements is given, one that effectively paints NATO as the aggressor, instead of Russia.

In the light of the Crimea intervention, one may imagine heavily armed 'green men' in unmarked uniforms popping up in the eastern regions of Estonia and Latvia adjacent to Russia, and in the western part of Lithuania next to Kaliningrad. The Kremlin says that the Baltic states are conducting operations against the Russian-speaking areas close to the Russian border. Confusion reigns in NATO capitals as intelligence services and politicians scramble to make sense of what is happening.

The 'green men' are rapidly reinforced, and within 24 – perhaps 36 – hours, it is clear that they are in fact Russian troops. By which time they are well on their way to the Baltic coast and the three republics' capital cities. The Baltic military and the NATO troops in these countries succeed in slowing down the Russian advance, but not in stopping it. At the same time, asymmetric tactics, information and cyber warfare, are used to disrupt infrastructure and to increase general confusion. As the RAND Corporation concluded in a 2017 report: 'Information warfare is part of the Russian approach to non-linear warfare that encompasses old and new methods and tools. One such example is the Soviet 'reflexive control' that aims to interfere with the decisionmaking processes of the adversary through disinformation and deception and the use of today's information technologies and media, not only in Russian but many other languages. It also encompasses 'strategic masking,' which is spreading disinformation via media and manipulation of the adversary into believing reports of military movements. With the proliferation of information technologies and the amounts of private information that people make available online, national governments, international organisations and societies have become more vulnerable to information warfare.'³⁸

To this one may add the fact that Russia's military intelligence department, known by its acronym GRU, is known to have recruited inhabitants of regions (such as the Baltics) which

36 Charlie Gao, 'NATO's worst nightmare: Russia's Kaliningrad is armed to the teeth', in: *The National Interest*, 25 May 2018. See: <https://nationalinterest.org/blog/the-buzz/natos-worst-nightmare-russias-kaliningrad-armed-the-teeth-25958>.

37 Several such scenarios have been written. Anders Puck Nielsen, 'How would a war between Russia and the West play out?', *Romeo Squared*, 1 January 2018. See: <https://romeosquared.eu/2018/01/01/the-military-scenario/>; Kris Osborn, 'NATO vs. Russia in a war for the Baltic states: Who wins?', in: *The National Interest*, 8 November 2018. See: <https://nationalinterest.org/blog/buzz/nato-vs-russia-war-baltic-states-who-wins-35532>; Ulrich Kühn, *Preventing Escalation in the Baltics: a NATO Playbook* (Washington, Carnegie Endowment for International Peace, 2018); Douglas Barrie et al, *Defending Europe: Scenario-based Capability requirements for NATO's European Members* (London, International Institute for Strategic Studies, April 2019).

38 Marta Kepe, 'NATO: Prepared for countering disinformation operations in the Baltic States?', *The Rand Blog*, 7 June 2017. See: <https://www.rand.org/blog/2017/06/nato-prepared-for-countering-disinformation-operations.html>.

Russia could arguably forcibly annex. These would spread fake news or instigate riots against the Baltic governments in order to lessen their capacity to resist an invasion. Baltic officials refer to 'Russian influence tactics' and 'sleeper cells'.³⁹ This would fit in entirely with General Gerasimov's hybrid warfare doctrine.

In the meantime NATO mobilises its Spearhead Force and rushes it to the border between Poland and Lithuania. In addition, Poland fears that the Russians will not stop at the border and orders a general mobilisation. The NATO troops,

in conjunction with the Polish, move up to the Suwalki Gap. They are, however, slowed down by Russian air attacks, causing considerable casualties. Other reinforcements are brought in by sea, but subjected to severe Russian air and naval attacks originating from the Kaliningrad and St. Petersburg areas. NATO bombers and warships unleash a concerted bombardment on Russian troops and military installations in the Oblast Kaliningrad, dealing the Russians a heavy blow.

Things now get dangerous. If the Russians fear that NATO may invade Kaliningrad, they may decide to escalate the war, which hitherto has been confined to the Baltic area. According to

39 'How the Baltic states spot the Kremlin's agents', in: *The Economist*, 1 August 2019.



NATO exercise around the Suwalki Gap

PHOTO NATO

the usually very well-informed US investigative journalist Bob Woodward, Russia 'had privately warned [Defence Secretary General Jim] Mattis that if there was a war in the Baltics, Russia would not hesitate to use tactical nuclear weapons against NATO'.⁴⁰ But even if that does not happen, they may very well widen the operational area by stirring trouble or even invading Ukraine and the Balkan NATO members. If that threshold is passed, what started off as a regional clash may degenerate into a Third World War.

To prevent this scenario, a RAND Corporation study found, a force of about seven mechanised brigades, including three heavy armoured

brigades, adequately supported in the air and at sea, was the minimum required to defeat the Russians.⁴¹ However, even the Very High Readiness Force does not provide this. And that assumes that the forces reach the operational area in time to prevent the Russians from confronting NATO with a *fait accompli*.⁴²

It does not seem as if NATO would be able to prevent Russia from occupying the Baltic states. As with Crimea, if the Russians have possession of the Baltics, it is extremely unlikely that they will relinquish their gains. They will probably sit tight and wait for the storm to subside.

NATO, therefore, has two options and one hope. The first option is to continue pretending that its present countermeasures are adequate to stop and even roll back a Russian invasion, and to do nothing further. The second is to increase its defence spending considerably and to establish ready forces strong enough to deal with Russian aggression. In the absence of this, one hope remains: That President Putin will not risk a full-blown war with NATO, even one he can win in the short term. If so, it will not be because NATO's present countermeasures have intimidated him, but rather because Russia's vulnerable economy cannot sustain a war with NATO for any considerable period of time. Nevertheless, a seasoned observer like ambassador Wolfgang Ischinger, Chairman of the Munich Security Conference, writes about 'our sleepwalking into a serious confrontation over the Baltics'.⁴³

It is a huge dilemma for Western leaders. How to deter Russia without provoking a general war? It will require nerves of steel as well as an absence of the kind of testosterone which one finds in abundance in too many world statesmen. Perhaps for inspiration one could look to the likes of Otto von Bismarck, rather than Donald Trump. ■

40 Bob Woodward, *Fear. Trump in the White House* (London and New York, Simon & Schuster, 2018) 132.

41 Shlapak and Johnson: *Reinforcing Deterrence on NATO's Eastern Flank*, 8.

42 Kyle, 'Contextualizing Russia and the Baltic States', 113.

43 Cited in Ulrick Kühn, *Preventing Escalation in the Baltics: a NATO Playbook* (Washington, Carnegie Endowment for International Peace, 2018) i.

Moral injury

De psychische impact van moreel-kritische situaties tijdens en na uitzendingen

Dr. Tine Molendijk*

Militaire interventie kan grote morele impact hebben op uitgezonden militairen. Hoewel dit bekend is, hanteren begrippen zoals posttraumatische stressstoornis (PTSS) vooral een individueel gericht perspectief met weinig aandacht voor morele en contextuele aspecten van aan uitzendingen gerelateerde problematiek. Recentelijk is echter een nieuw concept opgekomen: *moral injury* of morele verwonding. Dit artikel bespreekt het fenomeen morele verwonding en de rol van politieke praktijken en publieke percepties hierin aan de hand van kwalitatief onderzoek onder 80 Nederlandse (oud)militairen. De bevindingen van dit onderzoek geven aanleiding tot enkele aanbevelingen.

Al snel na zijn indiensttreding voelde Jan (een pseudoniem)¹ zich 'helemaal thuis in het leger'. Hij is altijd al een doener geweest en houdt van de actie en de broederschap die de krijgsmacht kent. Hoewel hij niet als primaire doelstelling had om de wereld de verbeteren, vond hij het bovendien een mooi idee 'om mensen te kunnen helpen'. Zijn eerste uitzendingen ervoer hij ook zo, of in ieder geval als waardevolle avonturen waarin hij zijn

training in de praktijk kon brengen. Maar dit gold niet voor zijn derde uitzending; die bleek anders.

* Tine Molendijk promoveerde in 2020 met het proefschrift *Soldiers in conflict. Moral injury, political practices and public perceptions* aan de Radboud Universiteit Nijmegen en werkt als universitair docent en onderzoeker aan de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie.

1 Dit verhaal komt voort uit interviews die de auteur afnam tijdens haar promotieonderzoek.



Interviews met veteranen die zijn ingezet in Afghanistan en Bosnië werpen licht op het morele spanningsveld waarin militairen opereren

FOTO MCD, GERBEN VAN ES

Jan had gehandeld 'als een goede militair', maar voelde zich 'geen goed mens'

Tijdens die missie verbleven Jan en zijn eenheid een tijd in een huiscompound. Elke nacht hoorde hij in het donker een jongen van een jaar of veertien huilen. De jongen was, zoals dat onder de westerse troepen bekend stond, een *chai-boy*: hij was eigendom van een rijke, invloedrijke man en moest op verzoek entertainment en seksuele diensten verlenen.² Overdag zag Jan de jongen vaak naar hem kijken. 'Die zit gewoon om hulp te roepen', dacht hij dan bij zichzelf. 'Maar je mocht niks doen. Je kon hem niet meenemen of zo. Dus daar zat je dan 's avonds op je wachtpost en dan hoorde je dat kind gewoon janken', weet hij nog. 'Dat ging door merg en been heen. En dan voelde je je zó klote'. Tragisch genoeg was dit nog niet alles. Enkele dagen later hoorde Jan 'dat het kind zich die dag met een AK door zijn kop had geschoten'. Tot op de dag van vandaag ligt hij daar wakker van. Dan kwelt de gedachte hem: 'had ik maar wat

gedaan'. Daarnaast kwelt het hem dat hij niks mócht doen. Het was een lokaal gebruik onder machthebbende mannen en samenwerking met hen was hard nodig voor het slagen van de missie. 'Dat zijn dubbelheden die aan je vreten', aldus Jan. Hij had gehandeld 'als een goede militair', maar voelde zich 'geen goed mens'.

Na thuiskomst ontwikkelde Jan diepe schuldgevoelens. Hij ging 'veel drinken en hard rijden', om maar niet te hoeven denken aan de dingen die aan hem knaagden. Tijdens het rijden dacht hij vaak: 'ik hoef alleen maar het stuur om te gooien en dan is het klaar'. Hij was zelfdestruc-tief bezig, zo realiseerde hij zich later, omdat hij onbewust dacht dat hij het verdiende. Hij voelde heel sterk 'dat ik op de één of andere manier nog gestraft moest worden voor wat er was gebeurd'. Een tijdlang had hij hierdoor zelfs de paranoïde gedachte dat zijn moeder hem wilde vergiftigen. Tegelijkertijd voelde hij zich verraden en in de steek gelaten door Defensie en de politiek. Hij was op een missie gestuurd waar samengewerkt werd met *warlords* die kinderen misbruikten, terwijl niemand hem vertelde dat het hebben van *chai-boys* 'ook volgens de lokale wet daar gewoon illegaal was'. Daarnaast hadden hij en zijn collega's veel moeten vechten in deze missie, waarbij ook veel burgerdoden waren gevallen, terwijl de missie 'thuis verkocht werd als een wederopbouwmissie'. Op al deze punten ervoer Jan dubbelheden die hij niet kon oplossen in zijn hoofd. Inmiddels gaat het beter met hem, maar dat heeft hem een lange strijd gekost.

Morele verwonding in de militaire praktijk

Het verhaal van Jan is één van de vele voorbeelden die aantonen dat de militaire praktijk een moreel spanningsveld is, een veld waarin vragen over goed en slecht continu aan de orde zijn en verschillende waarden met elkaar kunnen conflicteren. Zoals Jans verhaal ook laat zien kunnen waardenbotsingen met verstrekkende gevolgen een militair zelfs psychisch beschadigen. Hij of zij kan moreel verwond raken. Op het eerste gezicht is dit alles niet zo duidelijk. Het spat niet van de dagelijkse

2 In Afghanistan heet deze praktijk 'bacha bazi'. Zie ook Michelle Schut and Eva van Baarle, 'Dancing Boys and the Moral Dilemmas of Military Missions: The Practice of Bacha Bazi in Afghanistan', in: *International Security and Peacebuilding: Africa, the Middle East, and Europe*, Abu Bakarr Bah (red.)



In hedendaagse missies moeten militairen vaak opereren tussen en met de lokale bevolking, terwijl zij meestal niets kunnen doen aan lokale armoede, ziekte en lijden

FOTO MCD, EVA KLIJN

praktijk af dat de militaire wereld een 'moreel spanningsveld' is en wie op de werkvloer zulke termen gebruikt, loopt de kans op gelach van collega's. Veel militairen zullen zeggen dat hun werk voor hen moreel net zo ingewikkeld is als elk ander type werk. 'Je weet toch wel wat goed en fout is', zal de een schouderophalend zeggen. En een ander: 'Je moet gewoon je boerenverstand gebruiken'. Voor een deel zal de oorzaak van dat schouderophalen liggen in de *can do*-mentaliteit: concreet en oplossingsgericht zijn en bij twijfel niet stilstaan met wollige termen als 'moreel spanningsveld'. Een ander deel van de oorzaak is dat termen als deze vaak uitzonderlijke, Hollywoodachtige beelden oproepen, bijvoorbeeld van scherpschutters die moeten besluiten of ze wel of niet een kindje zullen doden. Dan is er nog het heersende idee dat alleen directe confrontaties met fysiek gevaar tot serieus te nemen psychische problematiek kunnen leiden, waardoor stress

die wordt veroorzaakt door andere situaties al snel als een persoonlijk gebrek wordt gezien.

Maar bij nadere beschouwing blijkt het tegenstelde waar. Moreel-kritische gebeurtenissen, hoewel niet zo extreem als in Hollywoodfilms, komen relatief vaak voor in de militaire praktijk en militairen worden dan ook betrekkelijk vaak overvallen door situaties waarin nog niet zo duidelijk is wat het juiste is om te doen. In hedendaagse missies moeten militairen vaak opereren tussen en met de lokale bevolking, terwijl zij meestal niet de mogelijkheden hebben om iets te doen aan lokale armoede, ziekte en lijden. Bovendien is niet altijd duidelijk in hoeverre de zogeheten vijand nu echt een kwaadwillende vijand is. Wanneer deze complexiteiten tot uiting komen in een concrete kritische situatie kunnen zich gevoelens van schuld, schaamte of verraad ontwikkelen. Zoals een granaatscherf een vleeswond kan veroor-

zaken en zoals een levensbedreigende gebeurtenis de stressregulatie kan verstoren, zo kan het zien, begaan of ondergaan van handelingen die de eigen morele overtuigingen geweld aandoen leiden tot een morele verwonding, ofwel moral injury in de Engelstalige literatuur.

In het kader van mijn promotieonderzoek naar moral injury nam ik kwalitatieve diepte-interviews af met 80 militairen, van wie 40 Dutchbat-veteranen (Srebrenica, Bosnië) en 40 TFU-veteranen (Uruzgan, Afghanistan). Deze interviews analyseerde ik tegen de achtergrond van informatie over de operationele, politieke en maatschappelijke kenmerken van hun missies, en in relatie tot psychologische, filosofische en sociaal-wetenschappelijke theorieën.³ Eerst bespreek ik het begrip morele verwonding en het onderscheid met posttraumatische stressstoornis (PTSS). Vervolgens ga ik in op de aard en mogelijke oorzaken van morele verwonding, door zowel individuele dimensies als politieke en maatschappelijke dimensies van morele verwonding te bespreken. Ten slotte kijk ik naar mogelijke antwoorden op deze problematiek en formuleer ik enkele aanbevelingen.

Posttraumatische stressstoornis en morele verwonding

Jans verhaal zal bij velen de term posttraumatische stressstoornis oproepen. Het is vandaag de dag de heersende term voor psychische problematiek onder militairen, zo bekend dat zelfs de afkorting PTSS inmiddels ingeburgerd is. Maar is het ook de meest passende term voor ervaringen zoals die van Jan? Een diagnose op basis van een kort verhaal is natuurlijk nooit mogelijk, maar enkele punten kunnen worden opgemerkt.

Posttraumatische stressstoornis versus morele verwonding

Volgens de laatste officiële definitie kan PTSS zich ontwikkelen na het ervaren of direct of indirect getuige zijn van 'feitelijke of dreigende dood, ernstige verwonding of seksueel geweld',⁴ en volgens de meeste PTSS-modellen zijn het angstreacties die de kern vormen van posttraumatische stress.⁵ Hoewel Jans verhaal inderdaad getuigenissen van geweld bevat, lijkt het ook af te wijken van bovengenoemde kenmerken. Centraal in zijn verhaal staan niet zozeer blootstelling aan dreiging en aan angst gerelateerde reacties, maar eerder ervaringen van moreel conflict en daaruit voortvloeiende gevoelens van schuld, schaamte en boosheid. Dit laatste is precies waar het begrip morele verwonding wel over gaat. Hoewel PTSS en morele verwonding elkaar niet uitsluiten en in de praktijk deels overlappen, hebben ze een verschillende focus. Er bestaat nog geen overeenstemming over de precieze definitie van morele verwonding – het is een relatief nieuw begrip – maar het huidige onderzoek beschrijft het meestal als 'de psychologische, biologische en sociale impact van een schending van fundamentele morele overtuigingen en verwachtingen, waarbij de moreel verwonde persoon zowel het slachtoffer, de getuige als de dader kan zijn geweest, in ieder geval in eigen ogen'.⁶ Anders dan bij PTSS ligt bij morele verwonding specifiek de nadruk op de morele dimensie van schokkende gebeurtenissen. En dat is meteen ook de reden waarom verschillende behandelaars van militairen, onder wie Jonathan Shay en Brett Litz, alsook veteraan en filosoof Camilo Bica, het begrip eind jaren 90 hebben opgeworpen.⁷ Met

-
- 3 Het promotieonderzoek van Tine Molendijk naar moral injury is te vinden via: <https://repository.ubn.ru.nl/handle/2066/208863>. Het zal binnenkort verschijnen als handeseditie onder de titel *Moral Injury and Soldiers in Conflict. Political Practices and Public Perceptions* (Londen, Routledge).
- 4 Zie DSM-5, *The Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition* (Arlington, VA, American Psychiatric Association, 2013).
- 5 Zie bijvoorbeeld Anne DePrince en Jennifer Freyd, 'The Harm of Trauma: Pathological Fear, Shattered Assumptions, or Betrayal', in: Jeffrey Kauffman (red.), *Loss of the Assumptive World. A Theory of Traumatic Loss* (New York, Brunner-Routledge, 2002) 71-82.
- 6 Zie onder meer Brett Litz, Nathan Stein e.a., 'Moral Injury and Moral Repair in War Veterans. A Preliminary Model and Intervention Strategy', in: *Clinical Psychology Review*, 29.8 (2009) 695-706; Jonathan Shay, 'Moral Injury', in: *Psychoanalytic Psychology*, 31.2 (2014) 182-91; Sheila Frankfurt en Patricia Frazier, 'A Review of Research on Moral Injury in Combat Veterans', in: *Military Psychology*, 28.5 (2016) 318-30.
- 7 Jonathan Shay, *Achilles in Vietnam. Combat Trauma and the Undoing of Character* (New York, Simon and Schuster, 1994). Litz, Stein e.a., 'Moral Injury and Moral Repair in War Veterans', 695-706. Camilo Bica, 'A Therapeutic Application of Philosophy. The Moral Casualties of War: Understanding the Experience', in: *International Journal of Applied Philosophy*, 13.1 (1999) 81-92.



In een onderzoek onder Amerikaanse militairen zei ruim een kwart ethische situaties te hebben meegemaakt waarin ze niet wisten hoe te reageren

het begrip moral injury wilden zij opnieuw de aandacht vestigen op die vaak zo cruciale morele dimensie, die in de mainstream PTSS-theorie veelal ondergesneeuwd was door een focus op angst.

Enkele cijfers

Een eerste conceptueel model van morele verwonding werd in 2009 geïntroduceerd.⁸ Sindsdien heeft het begrip snel aan bekendheid gewonnen in onderzoek, behandeling en beleid gericht op militairen en veteranen. Dit is gezien de cijfers niet verrassend. Neem bijvoorbeeld een recente enquête onder Amerikaanse militairen. Meer dan een tiende van hen rapporteerde betrokken te zijn geweest bij morele schendingen en ruim een vierde bleek morele schendingen door anderen te hebben gezien.⁹ In een andere survey gaf meer dan een kwart bovendien aan *ethical situations* te hebben meegemaakt

waarin ze niet wisten hoe te reageren.¹⁰ De impact van zulke gebeurtenissen kan groot zijn: verschillende studies laten percentages tussen de 5 en 25 zien van militairen die lijden aan gevoelens van schuld, schaamte of boosheid vanwege hun uitzendervaringen.¹¹

8 Zie Litz, Stein e.a., 'Moral Injury and Moral Repair in War Veterans', 695-706.

9 Zie Blair Wisco e. a., 'Moral Injury in U.S. Combat Veterans. Results from the National Health and Resilience in Veterans Study', in: *Depression and Anxiety*, 34.4 (2017) 340-47.

10 MHAT-V, *Operation Iraqi Freedom 06-08: Iraq, Operation Enduring Freedom 8: Afghanistan* (Washington, D.C., Office of the Surgeon Multi-National Force: Mental Health Advisory Team, 14 februari 2008) zie: http://www.armymedicine.army.mil/reports/mhat/mhat_v/mhat-v.cfm.

11 Joseph Currier e.a., 'Initial Psychometric Evaluation of the Moral Injury Questionnaire – Military Version', in: *Clinical Psychology & Psychotherapy*, 22.1 (2015) 54-63; Craig Bryan e.a., 'Measuring Moral Injury. Psychometric Properties of the Moral Injury Events Scale in Two Military Samples', in: *Assessment*, 23.5 (2016) 557-70; Wisco e. a., 'Moral Injury in U.S. Combat Veterans', 340-47.

Moreel verwonde militairen kunnen kampen met gevoelens van schuld en schaamte en boosheid ten opzichte van anderen of zelfs de wereld als geheel

Moreel verwondende gebeurtenissen

Potentieel moreel verwondende gebeurtenissen zijn volgens de literatuur onder meer het verwonden en doden van anderen, het niet kunnen voorkomen van leed onder collega's of burgers, en nalatigheid door een leider of andere autoriteit.¹² Dit toont aan dat morele verwonding niet alleen voorkomt onder militairen in oorlogsmisaties, maar ook kan ontstaan in vredesoperaties. Een studie onder Nederlandse veteranen van vredesmissies bevestigt dit. Van de geënquêteerde *peacekeepers* zei een kwart zich schuldig te voelen over de uitzending, en ten minste een derde van dit kwart gaf aan dat het schuldgevoel substantieel lijden had veroorzaakt.¹³ Overigens lijken ook beroepsgroepen zoals medici en politiepersoneel aanzienlijk risico te lopen op morele verwonding.

Schuld en beschuldiging: misplaatst of gepast?

Het is zeker niet het geval dat de morele dimensie van trauma al die tijd onopgemerkt is gebleven in PTSS-onderzoek. Toen het begrip PTSS in de jaren tachtig naar aanleiding van de Vietnamoorlog opkwam werd juist erg veel aandacht besteed aan zowel schuldgevoel als woede ten opzichte van militaire en politieke leiders.¹⁴ In de decennia erna raakten deze morele emoties buiten beeld, maar tegenwoordig krijgen ze weer aandacht. De meest recente definitie van PTSS omvat zelfs expliciet als mogelijk symptoom van PTSS 'persisterende en verstoorde cognities over de oorzaak of gevolgen van de traumatische gebeurtenis(sen) die ertoe leiden dat de betrokkene zichzelf of anderen er de schuld van geeft'.¹⁵ Maar, zoals deze omschrijving ook aangeeft, worden schuld en beschuldiging in huidig PTSS-onderzoek vooral benaderd als het resultaat van irrationele gedachten, oftewel als misplaatste gevoelens. De literatuur over morele verwonding daarentegen gaat expliciet in tegen een dergelijke benadering, en de naam 'verwonding' in plaats van 'stoornis' lijkt dan ook geen toeval. Bij morele verwonding wordt benadrukt dat morele overwegingen en oordelen serieus genomen moeten worden, en dat gevoelens van schuld, schaamte en/of verraad daarom beschouwd moeten worden als mogelijk 'gepaste' emoties (zie ook tabel 1). Het zijn immers morele overwegingen en emoties die een mens tot mens maken.

Individuele dimensies van morele verwonding

De 'rommeligheid' van morele kompassen

In de krijgsmacht wordt vaak gesproken van een ethisch kader of een moreel kompas. Hoewel dit deels passende metaforen voor de waarden en normen van een persoon zijn, is het belangrijk te beseffen dat deze nooit een mooie harmonieuze eenheid vormen, maar altijd een complex, zelfs 'rommelig' geheel.¹⁶ Dit geldt voor alle mensen, en dus ook voor militairen, en misschien zelfs specifiek voor militairen. Zoals alle mensen maken militairen deel uit van een familie, een vriendenkring, verschillende subculturen en de samenleving als geheel en

12 Zie Brandon e.a., 'Moral Injury: An Integrative Review', in: *Journal of Traumatic Stress*, 32.3 (2019) 350-62.

13 Zie Natasja Rietveld, *Voorkomen Is Beter Dan Genezen. De Geestelijke Gezondheid van Militairen En Politiepersoneel: Risico's en Beschermende Factoren* (Apeldoorn, Politieacademie, 2015).

14 Zie bijvoorbeeld Robert Jay Lifton, *Home from the War. Learning from Vietnam Veterans* (New York, Other Press, 1973).

15 Zie de eerder genoemde DSM-5.

16 Zie bijvoorbeeld Lisa Tessman, *Moral Failure. On the Impossible Demands of Morality* (Oxford, Oxford University Press, 2014); Jarrett Zigon, *Morality. An Anthropological Perspective* (New York, Berg, 2008).

	Heersende PTSS-modellen	Moral injury-model
Oorzaak	(Levens)bedreigende situatie De beleving van veiligheid wordt geweld aangedaan	Situatie die morele overtuigingen en verwachtingen schendt De beleving van een rechtvaardige wereld wordt geweld aangedaan
De eigen rol in de situatie	Slachtoffer of getuige	Slachtoffer, getuige of (in eigen ogen) verantwoordelijke
Centrale emoties	Angstgerelateerde emoties, zoals gevoelens van gevaar en dreiging	Morele emoties zoals gevoelens van schuld, schaamte en verraad
Benadering van eventuele veroordeling van zelf of anderen	Misplaatst, resultaat van 'verstoorde cognities', deresponsibilisering nodig	Eventueel gepast, (zelf)vergiftigenis nodig

Tabel 1 Heersende PTSS-modellen en het moral injury-model

al die sociale werelden kennen hun eigen specifieke waarden en normen die niet per se keurig op elkaar afgestemd zijn. Daarnaast zijn militairen lid van de militaire gemeenschap, met waarden en normen die kunnen botsen met die van de samenleving en bovendien ook onderling kunnen conflicteren: militairen moeten loyaal zijn aan hun 'broederschap', maar ook de veiligheid van burgers waarborgen, en daarbij dienen zij zich te allen tijde aan hun politieke opdracht te houden. Bovendien moeten ze al deze waarden en normen zien te managen in risicovolle contexten, als potentiële doelwitten, getuigen en uitvoerders van geweld.¹⁷

Tegenstrijdigheid en desoriëntatie

Gezien deze complexiteiten is het niet verbazingwekkend dat militairen situaties kunnen meemaken die leiden tot gevoelens van schuld, schaamte of verraad. Tegelijkertijd zijn deze situaties, ook juist door bovengenoemde complexiteiten, vaak gekenmerkt door tegenstrijdigheid. Dit geldt bijvoorbeeld voor Jans verhaal over de ervaring van een conflict tussen het zijn van een goede militair en een goed mens. Tegenstrijdigheid is ook te zien in gevallen van normvervaging, waarbij militairen achteraf beseffen dat ze morele grenzen hebben overschreden, maar ook weten dat dit gebeurde juist omdat deze grenzen tijdelijk niet meer zo helder waren. Dit soort ervaringen is complexer dan een eenduidig gevoel dat er onmiskenbaar een

morele code is overtreden of dat er onmiskenbaar is afgeweken van het eigen morele kompas. De ervaringen kenmerken zich door conflictgevoelens.

Als gevolg van dit soort ervaringen kunnen moreel verwonde militairen kampen met zowel gevoelens van schuld en schaamte als boosheid ten opzichte van anderen, of zelfs ten opzichte van de wereld als geheel. Daarnaast kunnen militairen moreel gedesoriënteerd raken en een diepgaande verwarring ontwikkelen over wat eerder gewoon een kwestie van boerenverstand leek te zijn. Allerlei vragen kunnen zich daarbij opdringen, zoals: 'Was ik een goede militair en is een goede militair ook een goed mens?', 'Maken mijn schuldgevoelens mij een goed of juist een slecht mens?', 'Hoe kun je eigenlijk ooit goeddoen in situaties die je dwingen te kiezen tussen twee kwaden?' en 'Wat betekent goed en slecht überhaupt?'. Dit zijn ethische vragen die normaal gesproken vooral ethici en moreelpsychologen stellen, maar wanneer morele verwonding dit soort vragen oproept zijn het geen abstracte wetenschappelijke, maar diep persoonlijke en vaak zeer pijnlijke kwesties. Ze kunnen moreel verwonde militairen het vertrouwen doen verliezen in de goedheid van

17 Zie bijvoorbeeld Ted van Baarda en Desiree Verweij, *Military Ethics: The Dutch Approach. A Practical Guide*. (Leiden, Martinus Nijhoff, 2006).

Negatieve mediaberichten over hun handelen raken militairen, zeker als hun omgeving daardoor gaat denken dat zij ‘fout’ zijn geweest

zowel henzelf als de wereld om hen heen, en zelfs in het idee van goedheid als zodanig.¹⁸

Politieke en maatschappelijke dimensies van morele verwonding

Moreel verwonde militairen kunnen ook boosheid ontwikkelen, bijvoorbeeld ten opzichte van de politiek en de samenleving.¹⁹ Militairen zijn immers instrumenten van de staat, die hun werk doen uit naam van de samenleving. Specifiek met betrekking tot de militaire praktijk zijn vragen van goed en kwaad daarom geen privé-eigendom van de militair, maar vragen die expliciet gesteld en bediscussieerd worden in het politieke en maatschappelijke

domein. De missies in Vietnam, Rwanda en Bosnië zijn beruchte voorbeelden van hoe falende politieke besluitvorming desastreuze gevolgen kan hebben. Het zijn daarmee tevens voorbeelden van de verhitte publieke debatten die over deze gevolgen kunnen ontstaan. Hoewel dit extreme voorbeelden zijn, zijn ze in principe niet uniek. Militairen van veel verschillende missies, zoals Jan, hebben verhalen te vertellen hoe politieke en publieke praktijken leidden tot moeilijke situaties tijdens en na de uitzending.

Ervaringen van politiek verraad

Als militairen tijdens hun uitzending moreel verwondende gebeurtenissen meemaken die in hun perceptie verband houden met vermijdbaar politiek falen, kan dat leiden tot een sterk gevoel van politiek verraad. Dit gevoel kan zich op zijn beurt uiten in wantrouwen, boosheid en meer concreet in het zoeken naar genoegdoening. Zo hebben honderden Nederlandse Bosniëveteranen recentelijk de regering aangeklaagd voor de emotionele schade die zij door hun missie hebben opgelopen. Formeel ging het om een collectieve claim voor financiële schadevergoeding, maar veel veteranen zochten vooral symbolische compensatie in de vorm van erkenning. Een rechtszaak zagen zij, zoals een van hen zei, ‘als de enige manier om de staat te laten boeten’.²⁰ Toen de regering aankondigde een grootschalig onderzoek te zullen doen naar de zorgbehoeften van Bosniëveteranen, lieten zij hun collectieve geldclaim dan ook vallen. Waar komt zo’n diepgaand gevoel van verraad en behoefte aan genoegdoening en erkenning nu precies vandaan? Het begint bij de afhankelijkheidsverhouding die er is tussen de militair en de staat. Wat er op het spel staat in die relatie is niet gering. Het gaat om de fysieke en geestelijke gezondheid van militairen, zelfs hun leven. Om in hun werk te kunnen functioneren moeten militairen er dus op kunnen vertrouwen dat zij in goede handen zijn bij de eigen regering, of op zijn minst niet in verkeerde handen. Wordt deze relatie van afhankelijkheid en vertrouwen geschonden, dan wordt in de ervaring van militairen mogelijk een cruciale morele relatie geweld aangedaan. Daar komt het gevoel van verraad en de behoefte aan genoegdoening

18 Voor een uitgebreidere bespreking van dit punt, zie: Tine Molendijk, ‘Toward an Interdisciplinary Conceptualization of Moral Injury. From Unequivocal Guilt and Anger to Moral Conflict and Disorientation’, in: *New Ideas in Psychology*, 51 (2018) 1-8.

19 Voor een uitgebreidere bespreking van deze paragraaf, zie: Tine Molendijk, ‘The Role of Political Practices in Moral Injury. A Study of Afghanistan Veterans’, in: *Political Psychology*, 40.2 (2019) 261-75; Tine Molendijk, ‘Moral Injury in Relation to Public Debates. The Role of Societal Misrecognition in Moral Conflict-Colored Trauma among Soldiers’, in: *Social Science & Medicine*, 211 (2018) 314-20.

20 Uit: Tine Molendijk, *Soldiers in Conflict. Moral Injury, Political Practices and Public Perceptions* (Nijmegen, Radboud University, 2020) 117.

FOTO UNPROFOR



De missies in Vietnam, Rwanda en Bosnië zijn beruchte voorbeelden van hoe falende politieke besluitvorming desastreuze gevolgen kan hebben

vandaan. Dit verraad kan gevoeld worden ten opzichte van de staat en de regering, maar ook ten opzichte van de organisatie of – nog concreter – de commandant.

Ervaringen van maatschappelijke miskennenning

Naast politiek of organisatorisch verraad kunnen militairen een gevoel van miskennenning door de samenleving ervaren. Die ervaren miskennenning gaat niet zozeer – of niet alleen – om een gebrek aan gevoelde waardering. Natuurlijk raakt het militairen als media negatief berichten over hoe zij hebben gehandeld op een missie, zeker wanneer hun naaste omgeving hierdoor gaat denken dat zij ‘fout’ zijn geweest. Maar ook heldenbeelden en verhalen waarin militairen als slachtoffers van trauma worden geportretteerd blijken vaak problematisch voor hen, want militairen die tegen hun eigen waarden in

hebben gehandeld voelen zich nu eenmaal niet heldhaftig of zielig. De maatschappelijke miskennenning die militairen kunnen ervaren gaat dus vooral om het gevoel dat hun uitzend-ervaringen worden versimpeld en verdraaid in de publieke opinie en dat zijzelf daarmee tot karikaturen zoals ‘dader’, ‘held’ of ‘slachtoffer’ worden gemaakt. Miskennenning in deze zin betekent dat de ervaringen van militairen gereduceerd worden tot simplificaties, en daarmee dat het mens-zijn hun ontzegd wordt.

Het is vanwege deze simplificatie dat een gevoel van miskennenning moreel verwendend genoemd kan worden: er wordt onrecht gedaan aan de eigen ervaring. En juist wanneer een mens worstelt met pijnlijke ervaringen is de behoefte aan herkenning en erkenning ervan door anderen vaak groot. Een gevoel van miskennenning

kan dan ook leiden tot grote woede, vervreemding en zelfisolering. Bovendien kan een mismatch met de publieke opinie militairen ernstig hinderen in het benoemen en verwerken van hun ervaringen, omdat ze in bestaande maatschappelijke verhalen geen passende woorden voor hun ervaringen kunnen vinden. Tot slot kunnen militairen gevoelens van schuld en schaamte ontwikkelen waar die emoties er anders misschien niet zouden zijn. Immers, schuld en schaamte gaan om hoe een persoon zichzelf bekijkt door de bril van anderen.

Aanbevelingen: recht doen aan morele verwonding

Vele, verschillende factoren kunnen een rol spelen in morele verwonding. En aangezien de militaire praktijk per definitie een moreel spanningsveld is zal morele verwonding nooit volledig te voorkomen zijn. Meer algemeen is het aannemelijk dat morele verwonding een tragisch risico van het leven is, zeker van het militaire leven. Toch blijken er meer en minder effectieve manieren te zijn om met deze problematiek en het risico erop om te gaan. Ik sluit dit artikel daarom af met enkele aanbevelingen.

Niet veroordelen, goedpraten of wegwuiven

Morele verwonding kan deels beschouwd worden als een ethische worsteling met vragen over goed en kwaad. Daarom moeten gevoelens van schuld, schaamte of boosheid niet te snel als onnodig of misplaatst worden weggewuifd, maar beschouwd als mogelijk gepast. Het wegwuiven helpt de persoon in kwestie niet en kan zelfs leiden tot een verdieping van de morele verwonding. Het miskennen van morele emoties betekent immers geen recht doen aan de betreffende emoties.²¹

Natuurlijk kan het ook bij morele verwonding zo zijn dat de militair in kwestie overdreven veel schuld bij zichzelf of anderen legt. In de praktijk zit de verantwoordelijkheid van personen voor een situatie echter bijna altijd ergens tussen nul en volledige verantwoordelijkheid en dan zijn gevoelens van schuld, schaamte of boosheid nog wel degelijk op zijn plaats. Tegelijkertijd kan het zinnig zijn om moreel verwonde militairen te helpen bij het overwegen van verschillende perspectieven, niet zozeer om hen van gedachten en oordeel te doen veranderen, maar om hen te helpen er meer grip op te krijgen. Uiteindelijk kan het voor een moreel verwonde militair nodig zijn op zoek te gaan naar vergiffenis voor zichzelf of van anderen. Dat is overigens niet zomaar gedaan. Vergiffenis is een proces dat tijd kost en alleen zinvol is als het oprecht is.²²

Stress- en ethiektraining

Bij het voorkomen van morele verwonding is het allereerst cruciaal om het bestaan van iets als morele verwonding te herkennen en erkennen. Dit betekent onder meer dat er bij trainingen niet alleen nadruk komt te liggen op stressoren zoals vuurgevechten, maar dat er ook aandacht is voor stress die kan ontstaan door confrontaties met onrecht, morele dilemma's en normvervaging. Daarnaast is het belangrijk om recht te doen aan de morele spanningen die zulke situaties kunnen veroorzaken, en eventuele morele schendingen ook hier niet te snel goed te praten, maar serieus te nemen. Meer specifiek is het van belang te erkennen dat er onoplosbare conflicten kunnen ontstaan tussen persoonlijke en professionele waarden, tussen professionele waarden en een politieke opdracht en dat de zin van uitzendsituaties bovendien twijfelachtig kan zijn. Hoe verleidelijk het misschien ook is om meer geruststellende dingen te verkondigen, het 'opleggen' van rechtvaardigingen en zingeving zal een morele verwonding eerder verdiepen dan genezen.²³

Voor het leren herkennen en erkennen van moreel verwondende situaties kan kennis van ethische begrippen zeer nuttig zijn. Wie niet precies weet wat waarden, normen en morele dilemma's inhouden kan immers ook niet

21 Zie Molendijk, 'Moral Injury in Relation to Public Debates', 314-20.

22 Zie bijvoorbeeld Brett Litz, Leslie Lebowitz e.a., *Adaptive Disclosure. A New Treatment for Military Trauma, Loss, and Moral Injury* (New York, Guilford Press, 2015).

23 Zie bijvoorbeeld Roy Eidelson, Marc Pilisuk en Stephen Soldz, 'The Dark Side of Comprehensive Soldier Fitness', in: *American Psychologist*, 66.7 (2011) 643-44.

communiceren over morele verwonding. Hier blijkt nog eens de meerwaarde van ethiekonderwijs. Momenteel is ethiekonderwijs echter grotendeels beperkt tot lessen in het klaslokaal, zodat morele dilemma's al snel *brainteasers* zijn in plaats van concrete situaties waarin emoties en stress een grote rol kunnen spelen.²⁴ Een expliciete verwerking van ethiek in oefeningen zou daarentegen realistische training in morele veerkracht mogelijk maken. Momenteel zijn morele dilemma's al expliciet onderdeel van sommige oefeningen. Dit soort letterlijk toegepaste ethiek lijkt zeer waardevol en zou frequenter mogen zijn, bij voorkeur direct gevolgd door collectieve evaluatie en discussie onder leiding van een hiertoe opgeleide begeleider.

Politieke besluitvorming en verhalen

Het voorkomen van morele verwonding ligt maar ten dele in de handen van militairen zelf. De militaire praktijk is een collectieve aangelegenheid. De politiek bepaalt op welke missie militairen worden gestuurd en wat zij daar al dan niet moeten doen, en op breder maatschappelijk niveau vindt de discussie plaats of een missie al dan niet gelegitimeerd en zinvol was. Niet alleen bij de individuele militair zou daarom een antwoord op morele verwonding

24 Zie Megan Thompson en Rakesh Jetly, 'Battlefield Ethics Training. Integrating Ethical Scenarios in High-Intensity Military Field Exercises', in: *European Journal of Psychotraumatology*, 5.1 (2014) 1-10.

Om militairen beter voor te bereiden op bepaalde situaties kunnen morele dilemma's worden toegevoegd aan oefeningen

FOTO MCD, JARNO KRAAYVANGER





Het voorkomen van morele verwonding ligt maar ten dele in de handen van militairen zelf, want de militaire praktijk is een collectieve aangelegenheid

moeten worden gezocht, maar ook op het niveau van politieke besluitvorming en publieke debatten.

Op politiek niveau is het belangrijk morele principes zoals die van de traditie van de rechtvaardige oorlog daadwerkelijk mee te nemen in de besluitvorming over militaire interventie. Deze principes zijn opgenomen in het internationaal Humanitair Oorlogsrecht (inclusief de Geneefse Conventies en het Handvest van de Verenigde Naties) en in het

Toetsingskader dat de Nederlandse regering gebruikt bij besluitvorming over uitzending van Nederlandse militairen. Dit alles om te zorgen dat militairen om rechtvaardige redenen worden uitgezonden en op rechtvaardige wijze hun werk kunnen doen. Het is belangrijk die morele principes oprecht te bespreken in besluitvormingsprocessen en niet alleen af te vinken als juridische checklist. Dat is makkelijker gezegd dan gedaan. Net zo belangrijk is dan ook dat de regering in de communicatie de zaken niet mooier maakt dan ze zijn, maar transparant



FOTO MCD, CINTHIA NIJSSEN

complexiteit van de militaire praktijk. Neem de rituelen van het vroege Christendom. Hierin ondergingen terugkerende krijgers standaard verschillende handelingen van boetedoening en reiniging om zo verschoond te worden van de morele ‘vervuiling’ van oorlog. De krijgers werden niet gezien als zondaars, maar wel als mensen die betrokken waren geweest bij het ‘gerechtvaardigde kwaad’ van oorlog.²⁵ Nog altijd bestaan er in verschillende samenlevingen dergelijke rituelen, bijvoorbeeld in gemeenschappen in zuidelijk Afrika, waar de rituelen dienen om terugkerende militairen te ontdoen van de geesten van gedode mensen.²⁶ In Nederland kennen we dit soort geïnstitutionaliseerde rituelen niet meer. Wel blijkt dat worstelende veteranen soms dan maar hun eigen rituelen creëren, bijvoorbeeld door in groepsverband terug te keren naar hun gebied van uitzending om daar samen met de lokale bevolking een mars te lopen.²⁷ Het bestaan van zulke zelfgecreëerde rituelen toont het belang ervan aan en tegelijkertijd het gemis ervan in onze huidige samenleving. Het lijkt daarom goed om te kijken naar wat veteranen zelf al aan activiteiten ondernemen.

Om morele verwonding te helpen voorkomen en te verwerken zijn herkenning en erkenning belangrijk. Niet alleen na de uitzending, maar ook al aan de voorkant. Het moet via training en therapie niet alleen gericht zijn op het individu, maar via ethisch-sensitieve besluitvorming, eerlijke, genuanceerde verhalen en adequate militaire reïntegratie ook op de niveaus van de militaire organisatie, politiek en maatschappij. Alleen zo is het mogelijk om recht te doen aan morele verwonding. ■

en eerlijk durft te zijn. Hoe transparanter en eerlijker, hoe meer politieke besluitvorming bescherming tegen morele verwonding biedt.

Maatschappelijke rituelen

Op maatschappelijk niveau blijken rituelen waardevol te kunnen zijn, zoals de purificatie- en reïntegratierituelen die militairen in vroegere samenlevingen moesten ondergaan. In plaats van portretten van ‘dader’, ‘held’ of ‘slachtoffer’ te schetsen gingen deze rituelen namelijk uit van genuanceerde ideeën over de morele

25 Zie B.J. Verkamp, *The Moral Treatment of Returning Warriors in Early Medieval and Modern Times* (Scranton, University of Scranton Press, 1993).

26 Zie Paulo Granjo en Beatrice Nicolini, ‘Back Home: Post-War Cleansing Rituals in Mozambique’, in: *Studies in Witchcraft, Magic, War and Peace in Africa (19th and 20th Centuries)* (Lampeter, Edwin Mellen Press, 2006) 277-94.

27 Zie Bart Hetebrij, ‘Terugkeerreis als pelgrimage’, in: *Carré*, 10 (2010) 14-17.

De cyber confidence-illusie

Hardnekkige hindernissen op weg naar cyber confidence-building measures

Cyberaanvallen kunnen een bedreiging vormen voor internationale vrede en stabiliteit. Vertrouwenwekkende maatregelen, *confidence-building measures*, voor cyberspace kunnen ongewenste escalatie voorkomen. De internationale gemeenschap heeft ervaring met dit soort maatregelen voor bijvoorbeeld nucleaire wapens. Waarom slagen de belangrijkste spelers er vooralsnog niet in om normen voor het gedrag van staten in cyberspace te ontwikkelen en te implementeren? Dit artikel beschrijft hardnekkige hindernissen die dit belemmeren.

Luitenant-kolonel ing. K.L. Arnold EMSD MSc*

In 2015 opende toenmalig minister van Buitenlandse Zaken, Bert Koenders, de Global Conference on CyberSpace in Den Haag. Tijdens zijn openingspeech uitte hij zijn zorgen over de complexe veiligheidssituatie in de fysieke en de virtuele wereld. Omdat cyberaanvallen een bedreiging kunnen vormen voor internationale vrede en stabiliteit, bepleitte hij een systeem van *confidence-building measures*.¹ Een jaar later concludeerde Koenders teleurgesteld dat verscheidene cyber-uitdagingen niet waren verminderd.

Sterker nog, ze waren toegenomen. De minister uitte zijn bezorgdheid over de vele cyberaanvallen die worden uitgevoerd door of namens verscheidene landen om politieke conflicten te beslechten. Hij benadrukte nogmaals de behoefte aan de regulering van normen en gedrag van staten in cyberspace.²

Een gemeenschappelijk besef dat schadelijke cyberactiviteiten wereldwijd een bedreiging vormen voor de internationale vrede en veiligheid heeft geresulteerd in de roep om politiek bindende, vertrouwenwekkende maatregelen voor cyberspace.³ Toch lukt het de internationale gemeenschap niet om kaders voor normen en gedrag van staten in cyberspace vast te leggen en, belangrijker nog, daadwerkelijk te implementeren. Sinds de eerste ontwerp-resolutie van Rusland uit 1998 staat het onderwerp op de agenda van de Verenigde Naties. Ongeveer twintig jaar later blijkt consensus binnen het daartoe samengestelde United Nations Group of Governmental Experts (UN GGE), nog altijd ver te zoeken.⁴

De wens is geuit om kaders voor normen en gedrag van staten in cyberspace vast te leggen, maar waarom lukt het dan niet om politiek aanvaardbare maatregelen te ontwikkelen en te implementeren? Dit artikel beschrijft enkele

* Lt-kol Kraesten Arnold is als (cyber)onderzoeker en docent verbonden aan de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie in Breda. Dit artikel is een geactualiseerde bewerking van de master thesis 'Cyber Confidence-Building Measures, Ten stumbling blocks which complicate the development and implementation of worldwide politically acceptable cyber confidence-building measures', 25 november 2016. Zie: <https://www.csacademy.nl/images/scripties/2017/Arnold-Thesis-final-version-25-nov-2016.pdf>.

1 Bert Koenders, *Opening speech*, Global Conference on Cyber Security, Den Haag, 16 april 2015. Zie: <https://www.government.nl/documents/speeches/2015/04/16/opening-speech-gccs-bert-koenders>.

2 Bert Koenders, *Speech at the Münchner Sicherheitskonferenz*, Den Haag, 12 februari 2016. Zie: <https://www.government.nl/documents/speeches/2015/02/09/speech-by-minister-koenders-at-munchner-sicherheitskonferenz>.

3 United Nations Office for Disarmament Affairs, *Factsheet: Developments in the field of information and telecommunications in the context of international security*, juli 2019. Zie: <https://www.un.org/disarmament/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf>.

4 United Nations Office for Disarmament Affairs, *Developments in the field of information and telecommunications in the context of international security*. Zie: <https://www.un.org/disarmament/ict-security/>.

initiatieven die zijn ontplooid op dit gebied. Vervolgens komen acht barrières aan de orde die de ontwikkeling en implementatie van die gewenste vertrouwenwekkende maatregelen voor het cyberdomein belemmeren.

Cyber confidence-building measures

Er bestaat geen vaste definitie voor confidence-building measures (CBM),⁵ maar over het algemeen zijn CBM gericht op het vergroten van onderling vertrouwen, voorspelbaarheid en stabiliteit, en omvatten daarom vaak afspraken over transparantie en samenwerking. Het zijn maatregelen die bij spanningen en conflicten de angst voor geweld of een (gewapende) aanval verminderen. Volgens de VN is, behalve politieke toezeggingen en de wil tot samenwerken, ook de mogelijkheid tot voortdurende verificatie essentieel. Een universeel CBM-model is niet realistisch.⁶ Uiteindelijke cyber-CBM zouden kunnen leiden tot een mondiale visie op verantwoordelijk gedrag van staten in cyberspace.⁷

Permanent Monitoring Panel en het eerste cyber-CBM-initiatief

Een van de eerste initiatieven op dit gebied kwam van de World Federation of Scientists. Sinds 2001 streeft haar information security Permanent Monitoring Panel (PMP) naar een mogelijkheid om cyberconflicten te beheersen. Het PMP beveelt een alomvattend juridisch kader aan, alsook richtlijnen voor verantwoordelijk gedrag van staten.⁸ Dat vraagt een gezamenlijke inspanning van de gehele internationale gemeenschap, waarbij het PMP een leidende rol voorziet voor de VN bij het beschermen van cyberspace. De VN zou zich moeten inzetten voor een *comprehensive Law of Cyberspace*.⁹

Initieel streefde het PMP naar een universeel verdrag met juridisch bindende afspraken. Het panel realiseerde zich echter dat dit een lang en onhaalbaar traject zou worden. Het PMP besloot om zich te concentreren op CBM en normatieve gedragscodes; geen juridisch bindende afspraken, maar politiek-bindende.¹⁰

UN Group of Governmental Experts

In lijn met het PMP-voorstel stelde de VN in 2009 een Group of Governmental Experts samen (UN GGE).¹¹ De groep kende deskundigen uit, onder meer, Brazilië, China, India, Rusland en de VS en streefde naar haalbare maatregelen om de mondiale cyberveiligheid te vergroten. In 2010 kwam de UN GGE met vijf aanbevelingen voor de ontwikkeling van CBM. De voorgestelde maatregelen gingen onder meer over eenduidige begrippen en definities, normen voor het gedrag van statelijke actoren, vertrouwenwekkende maatregelen en nationale standpunten over het 'gebruik van ICT' in conflictsituaties.¹² Door aanzienlijke meningsverschillen lukte het de GGE niet om in 2010 met een consensusrapport te komen.¹³ Sinds 2010 publiceert de UN GGE geregeld haar aanbevelingen.¹⁴

In 2015 constateerden de experts een significante toename in cyberincidenten als gevolg van schadelijke software door statelijke én niet-statale actoren. Als katalysator voor een toenemende dreiging noemden zij de ontwikkeling van cybercapaciteiten voor militaire doeleinden, de vele kwaadwillende niet-statale

-
- 5 OSCE, *Guide on Non-Military Confidence-Building Measures (CBMs)*, Wenen, 2012, 9. Zie: <https://www.osce.org/files/f/documents/6/0/91082.pdf>.
- 6 UN document A/51/182, *Report of the Disarmament Commission, annex F*, paragraaf 2.3.
- 7 Katharina Ziolkowski, *Confidence Building Measures for Cyberspace*, in: Katharina Ziolkowski (red.), *Peacetime Regime for State Activities in Cyberspace*, (NATO CCD COE Publication, Tallinn, 2013) 533.
- 8 Henning Wegener, *Information Security Permanent Monitoring Panel World Federation of Scientists*, 457.
- 9 Henning Wegener et al., *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar*, Report and Recommendations, World Summit on Information Society, Genève 2003 – Tunis 2005, Document WSIS-03/GENEVA/CONTR/6-E 19 November 2003, 14 - 18.
- 10 Wegener, *Information Security Permanent Monitoring Panel World Federation of Scientists*, 458-459.
- 11 Voluit: *The Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*.
- 12 UN document A/65/201, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 30 juli 2010, 6-8.
- 13 Eneken Tikk-Ringas, 'Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012', *Ict4Peace Cyber Policy Process Brief*, (ICT4Peace Publishing, Genève, 2012) 7. Zie: <https://ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf>.
- 14 Sinds 2004 hebben UN GGE-bijeenkomsten plaatsgevonden en er zijn rapporten gepubliceerd in de jaren 2004/2005, 2009/2010, 2012/2013, 2014/2015, 2016/2017 en 2019/2020. Zie: <https://dig.watch/processes/un-gge#view-7541-3>.



Politiemotorrijders begeleiden voertuigen met deelnemers aan de Global Conference on CyberSpace in Den Haag (2015)

FOTO RIJKSOVERHEID, PETER MONTENY

actoren en het attributieprobleem (de toewijzing van activiteiten aan een dader).¹⁵ De UN GGE stelde voor om niet-bindende normen voor overheden op te stellen, die weergeven wat een land wel, of juist niet zou mogen doen in cyberspace. Die normen moeten ook beschrijven welke activiteiten van niet-statelijke actoren ongewenst zijn en niet mogen worden gedoogd. Landen moeten afzien van cyberaanvallen op de vitale infrastructuur van anderen en hun eigen vitale infrastructuur daartegen beschermen.¹⁶ Opmerkelijk is dat zowel Rusland als China instemde met de, initieel door de VS voorgestelde, vrijwillige normen. Frappant, aangezien Rusland en China de vrijwillige normen zagen als opmaat naar (ongewenste) wettelijk bindende normen.¹⁷

De meest recente bijeenkomsten van de UN GGE, in 2016 en 2017, leidden niet tot consensus over het eindrapport. Sterker, de fundamentele verschillen in inzicht tussen de VS en gelijkgestemde partners, en Rusland en China met

hun gelijkgezinde bondgenoten, resulteerden in een scheiding der wegen. In 2018 besloot de VN derhalve om niet alleen (weer) een nieuwe (westers georiënteerde) expertgroep samen te stellen (met 25 lidstaten), maar daarnaast ook een (breder) Open-Ended Working Group (OEWG) te vormen, toegankelijk voor alle VN-lidstaten.

OVSE

De Organisatie voor Veiligheid en Samenwerking in Europa (OVSE) wordt vaak beschouwd als ideaal platform om internationale samen-

15 UN document A/70/174, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 22 juli 2015, 6.

16 UN document A/70/174, 8.

17 Henry Röigas en Tomáš Minárik, '2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law', in: *Incyder News*, augustus 2015. Zie: <https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/>.

De U.S. International Security Advisory Board adviseerde dat de VS zich beter kon richten op de confrontatie met Rusland

werking en stabiliteit te bespreken en te bevorderen.¹⁸ In 2013 nam de OVSE een pakket van elf cyber-CBM aan. Het voorstel bestond voornamelijk uit vrijwillige, praktische en risico-verlagende maatregelen. De focus lag op samenwerken, informatie-uitwisseling en transparantie, en op het voorkomen van misverstanden en escalatie.¹⁹ In ruil voor zijn steun aan het OVSE-voorstel dwong Rusland een bijlage bij het document af. Daarin bedongen de Russen dat het beginsel van soevereiniteit, territoriale integriteit en politieke onafhankelijkheid voor alle landen, ook van toepassing is in cyberspace.²⁰

In maart 2016 nam de OVSE aanvullende maatregelen aan, onder meer gericht op de beveiliging van vitale infrastructuur en daaraan gerelateerde grensoverschrijdende ICT-net-

werken. Ook adviseerde de OVSE om ook de particuliere sector, universiteiten, expertisecentra en de burgermaatschappij te betrekken bij de uitwerking van de maatregelen.²¹ Ondanks de succesvolle start kwam het proces later in 2016 vrijwel tot stilstand. Tot op heden is daarin geen verandering gekomen. Door onenigheid en beschuldigingen van (staats-gesteunde) hackactiviteiten loopt de implementatie van eerder afgesproken maatregelen vertraging op.

Shanghai Cooperation Organisation

Reeds in 2001 diende de Russisch-Chinees geleide Shanghai Cooperation Organisation (SCO)²² een voorstel in bij de VN voor een cybergedragscode. De gedragscode behelsde onder meer soevereiniteit, territoriale integriteit en politieke onafhankelijkheid voor alle landen, maar ook het voorstel om geen ICT te gebruiken voor vijandige activiteiten of bedreigingen van de internationale vrede en stabiliteit. De gedragscode beoogde daarnaast de oprichting van een multilateraal, internationaal internet-managementsysteem, en bepleitte de rol van de VN om internationale gedragsnormen op te stellen. Naleving van de code had een vrijwillig karakter.²³

Veel westerse landen waren, om uiteenlopende redenen, tegen de voorgestelde gedragscode. De code zou de vrije informatiestroom bedreigen. Bovendien werd het voorstel gezien als opmaat naar een juridisch bindend verdrag om het gedrag van overheden te reguleren. Ironisch genoeg vreesden westerse landen de juridisch bindende gevolgen van de (Chinees-Russische) SCO-gedragscode, terwijl Rusland en China juist de juridisch bindende consequenties van het UN GGE 2015 rapport vreesden. Een andere reden voor de westerse weerstand tegen de gedragscode was de voorgestelde wijziging in het (tot dan toe Amerikaans-gedomineerde) internet-beheer. Door de meningsverschillen werd het voorstel niet in stemming gebracht.²⁴

Bilaterale initiatieven

Naast voornoemde initiatieven van VN, OVSE en de SCO hebben ook de Association of Southeast Asian nations (ASEAN)²⁵ en de Organisation of American States (OAS)²⁶ vergelijkbare, maar

18 Vooral door de ervaringen die de OVSE opdeed met vertrouwenwekkende maatregelen tussen de partijen uit de Koude Oorlog.

19 OSCE, *Decision No 1106: Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, PC.DEC/1106 (Organization for Security and Co-operation in Europe, Permanent Council, 975th Plenary Meeting, 3 December 2013) 1.

20 OSCE, *Decision No 1106, Interpretative Statement Under paragraph IV.1(A)6 of the rules of procedure of the Organization for Security and Co-operation in Europe*, Attachment, 4.

21 OSCE, *Decision No 1202: OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, PC.DEC/1202 (Organization for Security and Co-operation in Europe, Permanent Council, 1092nd Plenary Meeting, 10 March 2016) 3-5.

22 De Shanghai Cooperation Organisation is een Euraziatische politieke, economische, en militaire organisatie, opgericht in 2001 in Shanghai door de leiders van China, Kazachstan, Kirgizië, de Russische Federatie, Tadjikistan en Oezbekistan. Zie: 'What is SCO', <http://infoshos.ru/en/?id=51>.

23 UN document A/66/359, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, 14 september 2011, 4-5.

24 Anna-Maria Osula en Henry Rôigas (red.), *International Cyber Norms, Legal, Policy & Industry Perspectives* (NATO CCD COE, Tallinn, 2016), 17-18.

25 Het ASEAN Regional Forum (ARF) brengt niet alleen de tien ASEAN-lidstaten bij elkaar, maar ook zeven andere landen uit de regio, alsook tien gesprekspartners, waaronder de VS, Rusland, China en de EU.

26 De organisatie van Amerikaanse staten kent 35 onafhankelijke lidstaten. Zie: http://www.oas.org/en/about/who_we_are.asp.

eveneens schijnbaar vruchteloze, pogingen gedaan om tot vertrouwenwekkende cybermaatregelen of normen te komen. Amerika, Rusland en China hebben ook bilaterale afspraken gemaakt.

In 2013 kondigden de VS en Rusland een bilaterale cyber-samenwerkingsovereenkomst aan om onnodige escalatie van cyberincidenten te voorkomen. Speciale aandacht ging uit naar cyberdreigingen vanaf elkaars grondgebied.²⁷ De overeenkomst leek veelbelovend en er werd concrete vooruitgang geboekt, maar de Oekraïne-crisis (2014) en de Russische annexatie van de Krim verstoorden deze ontwikkeling. Sterker nog, de US International Security Advisory Board adviseerde dat de VS zich beter kon richten op de confrontatie met Rusland, dan te zoeken naar manieren om de betrekkingen te verbeteren.²⁸

In 2015 vonden Rusland en China elkaar in een bilaterale cyberovereenkomst over 'non-agressie in cyberspace' en 'cyber-soevereiniteit'. Het akkoord bouwt voort op de eerdergenoemde gedragscode van de SCO. De non-agressie-toezegging was vooral bedoeld om wederzijdse cyberspionage te beperken. Het gedeelte over soevereiniteit dient een breder politiek en strategisch doel. Beide landen beklemtonen de soevereine status van internet, waarin overheidsgezag geldt voor binnenlandse aangelegenheden; zonder enige inmenging van buitenaf. Rusland en China hebben daarom een gemeenschappelijk belang bij 'cyber-soevereiniteit', een standpunt dat haaks staat op het Amerikaanse pleidooi voor wereldwijde 'cyber-vrijheid'.²⁹

Ook de VS en China besloten in 2015 hun onderlinge cyber-samenwerking te intensiveren. Belangrijkste drijfveer voor een overeenkomst was de Amerikaanse wens om China's economische cyberspionage een halt toe te roepen.³⁰ Hoewel het akkoord niet is gepubliceerd, zijn enkele afspraken toch bekend geworden. Zo kwamen de landen overeen zich te onthouden van cyber-diefstal van intellectueel eigendom, bedrijfsgeheimen of andere vertrouwelijke zakelijke informatie. Ook kwamen beide landen overeen zich in te spannen voor normen op het gebied van overheidsgedrag in cyberspace.³¹ Wat

de VS heeft toegezegd aan China in ruil voor deze overeenkomst, is verder niet bekend.

Een jaar later is de voorlopige conclusie van het Amerikaanse cybersecuritybedrijf FireEye dat de Chinese economische cyberspionage inderdaad is gedaald.³² Ondanks de vermeende afname van het aantal hack-activiteiten, is het prematuur om te concluderen dat China zijn overheids-gestuurde (economische) cyberspionage daadwerkelijk heeft verminderd, laat staan permanent beëindigd. Misschien houdt China zich vooralsnog gedeisd, uit schaamte voor de openbaring van de staatsgesteunde cyberspionage, die in 2014 resulteerde in een Amerikaanse aanklacht tegen vijf Chinese militaire hackers.³³ Of China grijpt deze 'gevechtspauze' aan om technologisch meer geraffineerde capaciteiten te ontwikkelen, waarmee het voortaan wél onopgemerkt kan blijven.

De afgelopen vijf jaar zijn dergelijke bilaterale akkoorden niet meer gesloten.³⁴ Afspraken lijken gewenst, maar de magere resultaten laten tegelijk zien dat er een kloof bestaat tussen idealisme en pragmatisme.

-
- 27 White House Office of the Press Secretary, *Factsheet US-Russian agreement on cooperation on information and communications technology security*, 17 juni 2013. Zie: <https://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol>.
- 28 U.S. Department of State International Security Advisory Board, *Final Report of the International Security Advisory Board (ISAB) on U.S.-Russia Relations*, 9 december 2014, 3. Zie: <http://www.state.gov/documents/organization/235118.pdf>
- 29 Yuxi Wei, *China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty* (Jackson School of International Studies, University of Washington, 21 juni 2016). Zie: <https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/>.
- 30 Scott Warren Harold, *The US-China Cyber Agreement, a good first step*, (RAND corporation, 1 augustus 2016). Zie: <https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html>.
- 31 White House Office of the Press Secretary, *Fact sheet 'President Xi Jinping's State Visit to the United States*, 25 september 2015. Zie: <https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-State-visit-united-states>.
- 32 Reuters World News, 'Chinese economic cyber-espionage plummets in U.S.: experts', 21 juni 2016. Zie: <http://www.reuters.com/article/us-cyber-spying-china-idUSKCN0Z700D>.
- 33 U.S. Department of Justice, 'U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage', 19 mei 2014. Zie: <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>.
- 34 Mochten er wel (geheime) bilaterale akkoorden op dit gebied zijn gesloten, dan zijn de resultaten daarvan op moment van schrijven niet publiekelijk bekend.



Een Amerikaanse militair bereidt zich voor op een cyber-readiness-oefening

Acht obstakels op weg naar cyber-CBM

Uit het voorgaande blijkt dat cyber-CBM ontwikkelen moeizaam gaat. Implementatie van voorgestelde maatregelen blijkt evenwel nog lastiger. Hieronder beschrijf ik acht aspecten die mondiale cyber confidence-building measures belemmeren.

1. Geen eenduidige terminologie

De verschillende cyber-CBM-initiatieven tonen dat afspraken over een gemeenschappelijke cyberterminologie onbereikbaar lijken. Binnen internationale organisaties, zoals de VN, NAVO, OVSE en de EU, alsook binnen individuele landen, worden andere woorden gebruikt om hetzelfde te zeggen, of juist dezelfde woorden gebruikt om iets anders uit te drukken (cyber security, information security, ICT-security,

cyberspace, information space, information warfare, cyber warfare, cyber attack, cyber incident).

Daarnaast hechten landen vaak andere waarden aan dezelfde begrippen (zoals soevereiniteit, privacy, interne aangelegenheden, vrijheid van meningsuiting). Het gebrek aan eenduidige definities en verschillende interpretaties creëert een voedingsbodem voor misverstanden. Sterker, ze staan een goede discussie over cyber-CBM in de weg.

2. Te veel belanghebbenden

Internationale betrekkingen drijven van oudsher op interactie tussen soevereine staten. Bij gesprekken over eerdere CBM (voor nucleaire, biologische en chemische wapens, of beperking van conventionele en strategische wapens) waren slechts die partijen betrokken die derge-



FOTO U.S. DEPARTMENT OF DEFENSE, FRANKLIN R. RAMOS

lijke wapens hadden. Echter, door de huidige interconnectiviteit en internationale verwevenheid van netwerken en systemen kunnen cyberaanvallen overal ter wereld vandaan komen en overal ter wereld effecten creëren. Het aantal potentiële gesprekspartners neemt daardoor significant toe. Intergouvernementele organisaties zoals de VN, WTO, IMF en EU, alsook niet-gouvernementele en multinationale organisaties worden steeds invloedrijker en spelen een steeds grotere rol bij onderhandelingen. Bovendien is het aantal partijen dat is betrokken bij ontwerp, bouw, beheer en gebruik van cyberspace enorm.³⁵ Alle partijen hebben eigen meningen, waardes en belangen; vaak uiteenlopend, soms verstrengeld, soms tegengesteld.

Een voorbeeld van toegenomen invloed kwam in 2014 van Microsoft. Het bedrijf kwam met een

voorstel voor zes cyberveiligheidsnormen voor het gedrag van overheden in cyberspace, '[...] to better define what type of government behaviors in cyberspace should be "out of bounds" [...]',³⁶ om de kans op oorlog voeren te beperken. De wereld op zijn kop: een commercieel bedrijf dat landen 'voorschrijft' hoe hun overheden zich (onderling) in cyberspace moeten gedragen.

Er zijn te veel gesprekspartners met elk hun eigen standpunten. Dit leidt tot een paradox. Voor een optimaal resultaat van het cyber-CBM-proces is een brede discussie nodig tussen (veel te) veel belanghebbenden. Tegelijkertijd blokkeert die overmaat aan gesprekspartners ditzelfde proces.

3. Diepgeworteld wantrouwen

In 1998 stelde Rusland een VN-wapenbeheersingsverdrag voor dat het gebruik van cyberspace voor militaire doeleinden zou uitsluiten.³⁷ Rusland was de enige voorstander van deze (ontwerp)resolutie. In 2005 keerde het tij, nogal ironisch, doordat de VS voor het eerst actief tegen het voorstel stemde. Beide grootmachten mobiliseerden medestanders voor hun standpunt en in 2009 stond de teller op 30 vóór het Russische voorstel, inclusief China. Een jaar later herzag de VS plotseling zijn mening en sloot zich aan bij het Russische voorstel, waarschijnlijk in een poging hierop inhoudelijk invloed te kunnen uitoefenen.³⁸

In 2001 diende de Chinees-Russisch geleide Shanghai Cooperation Organisation een voorstel in voor een gedragscode. Ook dit voorstel stuitte op weerstand. Westerse democratieën wilden dat

35 Denk onder andere aan internet-serviceproviders, internet-beheerorganisaties, grote technologiebedrijven zoals Apple, Alphabet (het moederbedrijf van Google), Microsoft, Facebook en Amazon, commerciële bedrijven, inlichtingsdiensten, criminele organisaties, activistische hackers, individuele gebruikers, en een scala aan belanghebbenden die zich bezighouden met internationaal recht, soevereiniteit, privacy, vrije informatiestromen, universele mensenrechten, sociale, economische, historische en culturele aspecten.

36 Angela McKay (et al), *International Cybersecurity Norms, Reducing conflict in an Internet-dependent world*, (Microsoft, December 2014) 11. Zie: https://download.microsoft.com/download/7/6/0/7605D861-C57A-4E23-B823-568CFC36FD44/International_Cybersecurity_%20Norms.pdf.

37 Ziolkowski, *Confidence Building Measures for Cyberspace*, 533.

38 Ibidem, 571.

overheden ook verantwoordelijk zouden zijn voor cyberaanvallen van niet-statelijke actoren die opereren vanaf hun grondgebied. Het voorstel ging echter niet in op verantwoordelijkheid voor niet-statelijke proxy-actoren (partijen die acties uitvoeren namens anderen).³⁹

Een westers voorstel, de Convention on cyber-crime van de EU,⁴⁰ werd juist weer tegengewerkt door invloedrijke landen zoals China, Rusland, India en Brazilië. Deels omdat deze landen niet

waren betrokken bij de ontwerp-resolutie, deels omdat zij meenden dat de rechten van individuen en landen niet goed werden gewaarborgd.⁴¹ Bovendien waren Rusland en enkele gelijkgestemde landen tegen het voorstel, omdat goedkeuring hun soevereiniteit zou schaden.⁴²

De onderlinge geopolitieke en economische strijd van de VS, China en Rusland lijkt een zero-sum game en werkt effectieve onderhandelingen tegen. Een compromis over vertrouwen-wekkende maatregelen blijft uit, zolang de grootmachten niet enigszins hetzelfde denken over soevereiniteit, territoriale integriteit, internetbeheer, privacy, anonieme operaties, cyberspionage, cyberaanvallen, inzet van proxies, geheime operaties en het (gedogen van) schadelijke activiteiten.

4. Cyberspace is ondoorzichtig

Een relevant aspect van CBM betreft transparantie.⁴³ Cyberspace is echter verre van transparant. De manier waarop cyberspace is geconstrueerd, staat een hoge mate van anonimiteit

39 Tim Maurer, 'Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security', *Discussion Paper 2011-11* (Cambridge, Massachusetts: Belfer Center for Science and International Affairs, Harvard Kennedy School, september 2011) 6.

40 Council of Europe, *Convention on Cybercrime*, Budapest, 23 november 2001.

41 Sinha Shalini, 'Budapest Convention on Cybercrime – An Overview' (Center for Communication and Governance New Delhi, Legally India, Article 03, maart 2016). Zie: <https://www.legallyindia.com/blogs/budapest-convention-on-cybercrime-an-overview>.

42 Keir Giles, 'Russia's Public Stance on Cyberspace Issues', in: Cristian Czosseck, Rain Ottis, Katharina Ziolkowski (red.) *4th International Conference on Cyber Conflict 2012* (NATO CCD COE Publications, Tallinn, 2012) 65.

43 Ziolkowski, *Confidence Building Measures for Cyberspace*, 12.

Cyberaanvallen kunnen overal ter wereld vandaan komen en overal ter wereld effecten creëren

FOTO UK MINISTRY OF DEFENCE



toe. Het is mogelijk om weinig tot geen traceerbare sporen en privéinformatie achter te laten, waardoor cyberaanvallers hun werkelijke identiteit en intenties kunnen verhullen en overheden de verantwoordelijkheid voor cyberacties vrij gemakkelijk kunnen ontkennen. De toewijzing van activiteiten aan een dader is daardoor veelal een tijdrovende en forensische uitdaging ('het attributieprobleem'). De mogelijkheid om operaties quasi-anoniem uit te voeren, draagt bij aan misverstanden en valse beschuldigingen.

Een aanvaller in het cyberdomein heeft als voordeel dat een aanval voor het doelwit veelal onvoorspelbaar en onzichtbaar is. Om het risico op ontdekking te verkleinen, kan een agressor de aanval bovendien laten uitvoeren door een proxy-actor. Deze kan hiertoe de digitale identiteit van onschuldige derden vervalsen en misbruiken. Pas zodra de aard en omvang van de effecten zich openbaren, kan het slachtoffer een inschatting maken waar de aanval vandaan komt. Aangezien attributie vaak een probleem vormt, blijft het een uitdaging om de verantwoordelijke achter een aanval aan te wijzen.

Een voorbeeld van een attributieprobleem is discussie rond de verantwoordelijkheid voor de in 2014 uitgevoerde cyberaanval op Sony Pictures. De Amerikaanse FBI wees Noord-Korea aan als vermeende dader; het land ontkende. Verscheidene journalisten en cyberveiligheidsexperts twijfelden openlijk aan de beschuldiging.⁴⁴ Hackers kunnen cyberidentiteiten nabootsen en daarmee de verdenking van schadelijke activiteiten neerleggen bij anderen. Inmiddels is een scala aan partijen aangemerkt als dader, waaronder Noord-Korea, Rusland, China, de Verenigde Staten, de FBI, Sony-werknemers, hacktivisten en de (cyber)criminele Lazarus Group.

Transparantie speelt ook een belangrijke rol bij het beschermen van cyberspace, vooral bij het beschermen van vitale infrastructuur die nationale grenzen overstijgt.⁴⁵ Het VN GGE-rapport 2015 deed een voorstel voor normen in die richting.⁴⁶ De voorgestelde normen impliceerden dat verantwoordelijk overheidsgedrag

onder meer inhoudt dat landen – vanaf hun grondgebied – geen acties stimuleren of gedogen die dit soort kritieke infrastructuur bedreigt. Van landen werd verwacht dat zij de integriteit van de gehele IT-keten garanderen. Landen moeten afstand nemen van het manipuleren van hardware, software of protocollen, en afzien van verspreiding van schadelijke cybermiddelen en technieken. Zolang die normen er niet zijn, kunnen overheden fabrikanten dwingen (bewust) kwetsbaarheden of 'achterdeurtjes' in te bouwen in hun soft- en hardwareproducten.⁴⁷

Dat vrijwel de gehele IT-keten (hardware, software, protocollen en dergelijke) kan worden gemanipuleerd, bleek wel uit Edward Snowdens gelekte documenten over de Amerikaanse National Security Agency (NSA). De NSA bleek meerdere kwetsbaarheden uit te buiten in producten van Microsoft, Cisco en Huawei. De dienst onderschepte bepaalde – door hun doelwitten bestelde – elektronica, en voorzag die van kwaadaardige software.⁴⁸ Die geheime 'elektronische achterdeurtjes' waren voornamelijk gericht op (het misbruiken van kwetsbaarheden in) firewalls en routers.⁴⁹ Eenmaal ingebouwd zijn dergelijke elektronische achterdeurtjes lastig te ontdekken. En eenmaal ontdekt, is het lastig de daadwerkelijke daders met zekerheid aan te wijzen.

Anonimiteit en het attributieprobleem zorgen ervoor dat identiteiten en intenties kunnen worden verhuuld, waardoor overheden de verantwoordelijkheid voor schadelijke cyber-

44 Post Staff Report, 'New evidence Sony hack was 'inside' job, not North Korea', *New York Post*, 30 december 2014. Zie: <http://nypost.com/2014/12/30/new-evidence-sony-hack-was-inside-job-cyber-experts/>; Kim Zetter, 'The evidence that North Korea hacked Sony is flimsy', *Wired Magazine*, 17 december 2014. Zie: <https://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/>.

45 Zoals elektriciteitsnetwerken, olie- en gaspijpleidingen, internetverbindingen.

46 UN document A/70/174.

47 Christian Czosseck, 'State Actors and their Proxies in Cyberspace', in: Katharina Ziolkowski (red.), *Peacetime Regime for State Activities in Cyberspace*, (NATO CCD COE Publication, Tallinn, 2013) 14.

48 Spiegel Staff, 'Documents Reveal Top NSA Hacking Unit', *Spiegel Online International*, 29 december 2013. Zie: <http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html>.

49 Bruce Schneier, 'Major NSA/Equation Group Leak', *Schneier on Security*, 16 augustus 2016. Zie: https://www.schneier.com/blog/archives/2016/08/major_nsaequati.html.

acties vrij gemakkelijk kunnen ontkennen. Cyberspace is ondoorzichtig, terwijl transparantie juist essentieel is voor vertrouwenwekkende afspraken.

5. Gebruik van proxies

Landen mogen niet doelbewust toestaan dat hun grondgebied wordt gebruikt voor activiteiten die andere soevereine staten schaden.⁵⁰ In de *Tallinn Manual*,⁵¹ een handleiding voor een juridische interpretatie van het internationale recht op het cyberdomein, wordt dit principe doorgetrokken naar cyberspace.⁵² Zodra een land weet van een onrechtmatige daad die resulteert in ernstige schade voor een andere staat, moet het hiertegen optreden. Dit 'due diligence'-principe betekent overigens niet dat een land per definitie alles moet ondernemen om een aanval te vermijden.⁵³

Desondanks maakt een overheid soms juist dankbaar gebruik van 'proxy-actoren', die namens hen schadelijke cyberaanvallen uitvoeren op andere landen. Dat kan zijn omdat overheden niet de juiste cybercapaciteiten hebben, maar een andere reden kan zijn dat bepaalde activiteiten niet stroken met de wettelijke, ethische of culturele waarden van het land. Het belangrijkste argument is echter de mogelijkheid dat een overheid (directe) betrokkenheid bij cyberaanvallen kan ontkennen door zich te verschuilen achter niet-staatelijke actoren zoals patriottische hackers,

criminel of activisten. De benodigde capaciteiten zijn ook in te huren. Opvallend is dat deze 'cyber-crime-as-a-service' niet uit bekende schurkenstaten komt, maar vooral uit de VS (ongeveer 50 procent), het VK, Portugal, IJsland, Rusland en Nederland.⁵⁴

De cyberaanval op het Amerikaanse Democratic National Committee (DNC) in 2016 werd in eerste instantie toegerekend aan Russische, staatsgesteunde proxies. Het technische bewijs (zoals gebruikte middelen, IP-adressen, taal en locatie-instellingen) wees op duidelijke betrokkenheid van de Russische overheid. Toch speelt ook hierbij het attributieprobleem. Je kunt 'technisch bewijs' vervalsen, Russische middelen en technieken hergebruiken, en taal- en locatie-instellingen eenvoudig instellen. Andere inlichtingenbronnen zijn dan ook onontbeerlijk om de daadwerkelijke daders te achterhalen. De verdenking van Russische inmenging werd overigens herhaald in het Mueller-rapport uit 2019, op basis waarvan twaalf medewerkers van de Russische militaire inlichtingendienst GRU zijn aangeklaagd voor hun betrokkenheid.⁵⁵

In het conflict tussen Rusland en de Oekraïne waren meerdere proxy-actoren actief die offensieve acties uitvoerden voor, of namens de strijdende partijen. Russische hackers vielen Oekraïne aan met Denial-of-Service (DOS)-aanvallen en website defacements (waarbij de inhoud van een gehackte site wordt gewijzigd). Oekraïense hackers sloegen terug met soortgelijke cyberaanvallen op Russische doelen. Ook de NAVO gebruikte tijdens dit conflict een proxy, het Roemeense staatsbedrijf Rasirom, om de Oekraïense cyberverdediging te verbeteren.

Een overheid kan verklaren zich te houden aan afgesproken normen voor verantwoord gedrag in cyberspace. Echter, zolang overheden proxies blijven gedogen, stimuleren of steunen, en geen verantwoordelijkheid nemen voor hun acties, zijn dergelijke (in beginsel) vertrouwenwekkende toezeggingen van generlei waarde.

6. Cyberwapens

Cybermiddelen kun je gebruiken voor 'informatie-operaties' (beïnvloeding, psychologische

50 Benedikt Pirker, 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace', in: Katharina Ziolkowski (red.), *Peacetime Regime for State Activities in Cyberspace*, (NATO CCD COE Publication, Tallinn, 2013) 204.

51 Michael N. Schmitt (red.), *Tallinn Manual 2.0 on the international law applicable to cyber warfare* (Cambridge, Cambridge University Press, 2017).

52 De Tallinn Manual is een academisch boekwerk met daarin verzamelde meningen en interpretaties van wetenschappers en academici en heeft tot doel bij te dragen aan de discussie omtrent de toepasbaarheid van het internationale recht op het cyberdomein. De handleiding is geen beschrijving van wetgeving of een normstellend document.

53 Robin Geiß en Henning Lahmann, 'Freedom and Security in Cyberspace: Non-Forcible Countermeasures and Collective Threat-Prevention', in: Katharina Ziolkowski (red.), *Peacetime Regime for State Activities in Cyberspace*, (NATO CCD COE Publication, Tallinn, 2013) 655.

54 Rick M. Robinson, 'Cybercrime-as-a-Service Poses a Growing Challenge', *Security Intelligence*, 4 september 2016. Zie: <https://securityintelligence.com/cybercrime-as-a-service-poses-a-growing-challenge/>.

55 Robert S. Mueller III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election* (Volume II of II, maart 2019, Washington, D.C.). Zie: https://www.justice.gov/storage/report_volume2.pdf.



Amerikaanse militairen oefenen cyberoperaties met hun Zuid-Koreaanse bondgenoten

U.S. DEPARTMENT OF DEFENSE, DEVON DOW

oorlogsvoering of strategische communicatie), maar ook voor traditioneel kinetische doeleinden. De middelen zijn vrij eenvoudig te verkrijgen: een computer, software en een internetverbinding volstaan. En hoewel de kennis en vaardigheden om die middelen effectief te benutten een uitdaging kunnen vormen, zijn ook die relatief eenvoudig toegankelijk (via online handleidingen of als aangeboden (betaalde) service). Dezelfde capaciteiten kunnen zowel defensief als offensief worden benut. In vergelijking met traditionele wapensystemen zijn cyberwapens relatief goedkoop te maken, gemakkelijk te verbergen, eenvoudig te transporteren en daardoor lastig te ontdekken. Toezeggingen om geen 'cyberwapens' te ontwikkelen, zijn dan ook gemakkelijk te omzeilen en niet verifieerbaar.

Met de toename van technologisch hoogwaardige middelen voor moderne krijgsmachten, nemen de mogelijkheden om hiertegen cybermiddelen in te zetten navenant toe. Cyberwapens zijn daardoor aantrekkelijk voor asymmetrische oorlogvoering, wat een risico op proliferatie impliceert. Toch staat de ontwikkeling van cyberwapens wereldwijd nog in de

kinderschoenen. Dit geldt zeker voor cyberwapens die (direct of indirect) resulteren in de dood of lichamelijk letsel van mensen, of die leiden tot ernstige fysieke schade. Sinds de ontdekking van 'Stuxnet', de vermeende Amerikaans-Israëlische cyberaanval op een Iraanse uranium-verrijkingsinstallatie in 2010,⁵⁶ zijn er weinig cyberaanvallen bekend die een militair doel nastreefden.⁵⁷ Desondanks heeft Stuxnet het potentieel dodelijk en vernietigend effect van (toekomstige) cyberwapens gedemonstreerd.

Militaire systemen en netwerken vormen mogelijke doelwitten voor cyberoorlogvoering, maar een tegenstander kan in beginsel ieder digitaal object aanvallen. Objecten met een civiel-militaire functie (soms aangeduid als

56 John C. Richardson, 'Stuxnet as Cyberwarfare Applying the Law of War to the Virtual Battlefield', in: *The John Marshall Journal of Information Technology & Privacy Law* 29 (2011) (1).

57 Voorbeelden van militair gebruik van cyberwapens zijn te vinden in Estland (2007), Georgië (2008) en Oekraïne (2013-2015). Verder zijn er militaire cyberincidenten geweest in de Libische burgeroorlog (2011), de Syrische burgeroorlog (2013), en de strijd tussen Israël en Hamas (2014). Emilio Iasiello, 'Are Cyber Weapons Effective Military Tools?', in: *Military and Strategic Affairs* 7 (2015) (1). Zie: http://www.inss.org.il/uploadImages/systemFiles/2_lasiello.pdf.

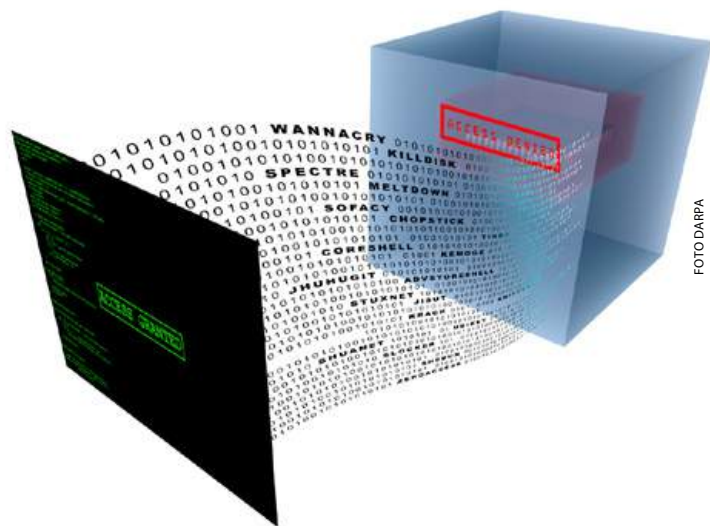


FOTO DARPA

Het feit dat landen elkaar bespioneren, is natuurlijk niet nieuw, maar cyberspionage en de omvang ervan zijn dat wel

dual-use) of zelfs volledig civiele vitale infrastructuur (waterwerken, drinkwatervoorziening) kunnen daardoor óók doelwit worden van kwaadwillende cyberaanvallers. Hoewel deze niet-militaire objecten volgens het humanitair oorlogsrecht geen doelwit zouden *mogen* zijn, *kunnen* deze objecten in de praktijk wel degelijk schade ondervinden; opzettelijk toegebracht of als onbedoelde nevenschade. Landen die hun tegenstanders niet kunnen treffen met traditionele wapens (letterlijk danwel figuurlijk) kunnen dit wel dankzij de nagenoeg onbeperkte reikwijdte en veelzijdige mogelijkheden van cyberwapens. Een pleidooi om tijdens een gewapend conflict of oorlog af te zien van relatief goedkope, maar doeltreffende cyberwapens is voor dergelijke landen niet aantrekkelijk.

Belangrijker dan cyberwapens zelf, zijn de kennis en vaardigheden om die cyberwapens te creëren. Mocht een land als vertrouwenwekkende maatregel verklaren geen cyberwapens te maken, dan kan het wel investeren in personeel en technische capaciteiten om deze wapens later alsnog te ontwikkelen. En zegt een land toe zelf niet te investeren in offensieve cybercapaciteiten, dan kan een proxy dat gat wellicht opvullen.

Bij traditionele CBM zijn afspraken te maken over ontwerp, ontwikkeling, productie of testen van wapens. Die toezeggingen zijn te inspecteren en te verifiëren. Door de bijzondere kenmerken van cyberwapens zijn dezelfde afspraken voor cyberwapens nauwelijks te maken.

7. Cyberspionage

Industriële, commerciële, politieke, diplomatieke en veiligheidsgerelateerde data kun je vergaren uit open bronnen, maar ook verkrijgen via spionage. Het feit dat landen elkaar bespioneren, is natuurlijk niet nieuw. Maar cyberspionage en de omvang ervan zijn dat wel.

In 2009 wist China terabytes aan vertrouwelijke gegevens over de Amerikaanse Joint Strike Fighter (F-35) buit te maken.⁵⁸ En in 2013 kwamen Canadese onderzoekers naar buiten met real-time bewijs dat een voornamelijk in China gevestigd computerspionagenetwerk in 103 landen computers van overheden en private ondernemingen had gehackt.⁵⁹ Ook het Amerikaanse cybersecuritybedrijf Mandiant wees in 2013 met een beschuldigende vinger naar China vanwege massale externe spionageactiviteiten. In zijn rapport onthulde het bedrijf het bestaan van 'Unit 61398', een afdeling van het Chinese leger, gespecialiseerd in (commerciële) cyberspionage.⁶⁰

Cybersecuritybedrijf FireEye claimde in 2014 voldoende bewijs te hebben om een langdurige spionage-inspanning in (Oost-)Europa – uitgevoerd door de Russische hackergroep 'APT-28' – te kunnen bestempelen als een 'door de Russische staat gesteunde actie'. Vermoedelijk begonnen de spionage-inspanningen al in 2007.⁶¹

58 Wendell Minnick, 'Chinese businessman pleads guilty of spying on F-35 and F-22', *Defense News*, 24 maart 2016. Zie: <http://www.defensenews.com/story/breaking-news/2016/03/24/chinese-businessman-pleads-guilty-spying-f-35-and-f-22/82199528/>.

59 'Cyber Spy Networks Hacks Computers in 103 Countries', *Fox News*, 30 maart 2009.

60 Mandiant, *APT1 Exposing One of China's Cyber Espionage Units*, 3. Zie: <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>.

61 FireEye, Special Report, *APT28: A Window into Russia's Cyber Espionage Operations?*, 28. Zie: <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf>.

Nu worden China en Rusland wel vaker beschuldigd van cyberspionage, voornamelijk door de VS. Toch blijken zij niet de enige grootmachten die zich hieraan bezondigen. In 2013 onthulde de eerder genoemde Edward Snowden het bestaan van het 'PRISM-programma' van de Amerikaanse NSA,⁶² een surveillanceprogramma waarmee de Amerikaanse overheid heimelijk gebruikersinformatie kon vergaren van bedrijven als Microsoft, Google, Apple en Yahoo.⁶³ Daarnaast gebruikte de NSA het programma om wereldwijd ambassades en niet-statelijke actoren te bespioneren.⁶⁴

Ook Nederland houdt zich bezig met digitale spionage. Bijvoorbeeld door, op zoek naar bewijs voor cyberactiviteiten voor of namens de Russische overheid, computersystemen binnen te dringen van Russische hackergroepen zoals 'Cozy Bear'.⁶⁵

Door computers, netwerken en bepaalde software te gebruiken, kun je tegenwoordig snel en relatief eenvoudig spioneren; op afstand en met beperkt risico.⁶⁶ Cyberspionage maakt computersystemen en netwerken van doelwitten (en derden) inherent onveilig en doet daarmee afbreuk aan het, voor cyber-CBM, noodzakelijke onderlinge vertrouwen en gewenste stabiliteit.

8. Noodzaak snelle overeenkomst ontbreekt
Hoewel meerdere cyber-CBM-initiatieven zijn gestart, lijken landen de huidige internationale situatie omtrent cyberveiligheid, een soort patstelling, acceptabel te vinden. De juiste omstandigheden kunnen een impuls geven aan veranderingen in veiligheidsdenken, waardoor landen willen meewerken aan veranderingen, maar vooralsnog lijken die gunstige omstandigheden afwezig. Pas als meerdere landen gezamenlijk een hoge mate van ontevredenheid over de huidige internationale cyber-veiligheids-situatie delen, kunnen vertrouwenwekkende maatregelen bijdragen aan het verbeteren van de onderlinge veiligheidsrelaties.⁶⁷

Veel landen zien de potentiële risico's van cyberaanvallen tegen hun onderling verweven economieën en erkennen de noodzaak tot samenwerking om deze risico's te bestrijden.

Toezeggingen om geen cyberwapens te ontwikkelen zijn makkelijk te omzeilen en niet verifieerbaar

Dat verklaart de initiële medewerking van veel landen aan mondiale, regionale en lokale cyber-CBM-initiatieven. Grootschalige cyberaanvallen met desastreuze effecten zijn vooralsnog uitgebleven. Cyberaanvallen hebben nog niet geresulteerd in grote aantallen slachtoffers of aanzienlijke fysieke schade. Ondanks alarmerende waarschuwingen is de wereld nog niet getroffen door een cyber-Armageddon,⁶⁸ Pearl Harbor,⁶⁹ doomsday,⁷⁰ of 9/11.⁷¹

Zodra zich een apocalyptisch cyberscenario ontvouwt, zullen overheden en andere, niet-publieke partijen waarschijnlijk bereid zijn om snel vertrouwenwekkende cybermaatregelen op te stellen, af te spreken en na te leven. Tot die tijd zal die noodzaak niet breed worden gevoeld.

-
- 62 PRISM staat voor Planning tool for Resource Integration, Synchronization and Management.
- 63 T.C. Sottek and Joshua Kopstein, 'Everything you need to know about PRISM, a cheat sheet for the NSA's unprecedented surveillance programs', *The Verge*, 17 juli 2013. Zie: <https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet>.
- 64 Bruce Schneier, 'Espionage vs. Surveillance', *Schneier on Security*, 14 mei 2014. Zie: https://www.schneier.com/blog/archives/2014/05/espionage_vs_su.html.
- 65 Huib Modderkolk, *Het is oorlog maar niemand die het ziet* (Amsterdam, Uitgeverij Podium, 2019) 276.
- 66 Russell Buchan, 'The International Legal Regulation of State-Sponsored Cyber Espionage', in: Anna-Maria Osula en Henry Røigas (red.), *International Cyber Norms, Legal, Policy & Industry Perspectives* (NATO CCD COE, Tallinn, 2016) 66.
- 67 John Hamre, 'Confidence Building in the Arms Control Process: A Transformation View', Ottawa, Canada: Department of Foreign Affairs and International Trade, Arms Control and Disarmament Studies Number 2, 1996. JX 1974.M32 1996.
- 68 James Clapper, 'US Spy Chief Warns of Space Wars, North Korean Nukes, and Cyber Threats', *Vice News*, 9 februari 2016. Zie: <https://www.vice.com/en/article/xw3m8q/us-spy-chief-warns-of-space-wars-north-korean-nukes-and-cyber-armageddon>.
- 69 John Hamre, 'The 'electronic Pearl Harbor'', *Politico Magazine*, 9 september 2015. Zie: <https://www.politico.com/agenda/story/2015/12/pearl-harbor-cyber-security-war-000335/>.
- 70 'Obama's doomsday cyberattack unrealistic – experts say', *NBC News*, 21 juli 2012. Zie: http://www.nbcnews.com/id/48265682/ns/technology_and_science-security/t/obamas-doomsday-cyberattack-scenario-unrealistic-experts-say/#.VyoRmvmLSM8.
- 71 Bert Koenders, *Speech at the Münchner Sicherheitskonferenz*.

Tenzij zich binnenkort één of meer cyberrampen voordoen, zal het ontwikkelen van mondiaal geaccepteerde, politiek-bindende cyber-CBM een langdurig, zonet onmogelijk proces blijken.

Tot slot

Nederland onderschrijft het belang van cyber-CBM. De eerdergenoemde Global Conference on CyberSpace in 2015 leidde tot de lancering van het The Hague Program for Cyber Norms, een meerjarig onderzoeksprogramma naar het

ontwikkelen en implementeren van internationale normen voor omgangsvormen in cyberspace.⁷² Een ander Nederlands initiatief betrof de oprichting van de Global Commission on the Stability of Cyberspace (GCSC),⁷³ een internationale multi-stakeholder-organisatie, gericht op het bevorderen van stabiliteit in cyberspace.⁷⁴

De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) adviseerde al eerder dat het internet een speerpunt moet zijn van het Nederlandse buitenlands beleid, met als doel een internationale norm die de publieke kern van het internet kan vrijwaren van oneigenlijke interventies van overheden.⁷⁵ Nederland zet zich actief in voor internationale, politiek aanvaardbare maatregelen en normen. De jarenlange ervaring met onderhandelen en samenwerken met allerlei belanghebbenden ('polderen') kan in zijn voordeel werken en Nederland een voortrekkersrol opleveren.⁷⁶

Toch is niet iedereen onverdeeld positief over de Nederlandse visie op internationale afspraken over vertrouwenwekkende maatregelen en gemeenschappelijke normen. Zo constateert vredesorganisatie PAX in een recent verschenen artikel van het Rathenau Instituut dat niet alleen de VS, Rusland en China een dubbelrol spelen op dit gebied; ook Nederland doet dat. Diplomatie, de-escalatie en internationale afspraken over normen en verantwoord gedrag in cyberspace staan in de ogen van PAX haaks op de gelijktijdige ontwikkeling van offensieve cybercapaciteiten.⁷⁷

De snelheid en het volume waarmee tegenwoordig digitale data worden gecreëerd, verstuurd of opgeslagen, zijn ongekend. Tegelijkertijd is onze maatschappij zo afhankelijk geworden van digitale netwerken, processen en systemen, dat kwaadwillenden dat kunnen misbruiken. Niet alleen criminelen buiten de zwakheden van onze computersamenleving uit. Uit het 'Cyber Security Beeld Nederland 2019' bleek andermaal dat in toenemende mate juist statelijke actoren onze maatschappij dreigen te ontwrichten door cyberactiviteiten zoals digitale spionage, sabotage en/of versterking. Onvoldoende overeenstemming en verschillen van inzicht over



FOTO WHITE HOUSE, SHEALAH CRAIGHEAD

Wantrouwen en het opzeggen van bestaande verdragen werken averechts

72 *The Hague Program for Cyber Norms* valt onder het the Institute of Security and Global Affairs (ISGA) bij de Faculty of Governance and Global Affairs van Leiden University. Zie: <https://www.thehaguecybern timers.nl/about-us>.

73 *The Global Commission on the Stability of Cyberspace* is geïnitieerd door twee onafhankelijke denktanks, The Hague Centre for Strategic Studies (HCSS) en de EastWest Institute (EWI). Zie: <https://cyberstability.org/report/#appendix-c-history--goals-and-processes-of-the-gcsc>.

74 Beide initiatieven zijn gelanceerd door het Ministerie van Buitenlandse Zaken, maar ook het Ministerie van Economische Zaken zet zich in voor dezelfde doelen. Dit leidde bijvoorbeeld tot de oprichting van het 'Nederlands Internet Governance Forum' (NL IGF) en het Electronic Commerce Platform Nederland (ECP) | Platform voor de InformatieSamenleving.

75 Wetenschappelijke Raad voor het Regeringsbeleid, *De publieke kern van het internet; Naar een buitenlands internetbeleid* (Amsterdam, Amsterdam University Press, 2015) 116.

76 ECP Platform voor de InformatieSamenleving, 'Nederland kan voorloper zijn op gebied van cybernormen', *Verslag van de Dag*, 14 november 2019 Zie: <https://ecp.verslagvandedag.nl/artikel/%E2%80%9Cnederland-kan-voorloper-zijn-op-gebied-van-cybernormen%E2%80%9D/?encr=undefined>.

77 Rathenau Instituut, 'Zonder gemeenschappelijke afspraken is uiteindelijk iedereen slechter af', 22 mei 2020. Zie: <https://www.rathenau.nl/nl/digitale-samenleving/zonder-gemeenschappelijke-afspraken-uiteindelijk-iedereen-slechter-af>.

internationale normen en waarden voor cyberspace vergroten tegelijkertijd de digitale dreiging.⁷⁸

Het U.S. Cyber Command onderkende ook de digitale dreiging van statelijke actoren en stelde in 2018 een 'Persistent Engagement'-strategie voor. Een aanpak waarbij de VS structureel en wereldwijd – dus ook buiten Amerikaanse netwerken en systemen – opereert in cyberspace; naadloos afwisselend tussen defensieve en offensieve acties.⁷⁹ Allereerst wil de VS zichzelf daarmee beschermen en zijn tegenstanders dwarszitten. Daarnaast wil de VS zichzelf hiermee een betere onderhandelingspositie verschaffen voor toekomstige onderhandelingen over (on)acceptabel gedrag in cyberspace.⁸⁰

Diepgeworteld wantrouwen, conflicterende politieke, geopolitieke, sociale, economische en culturele agenda's, geheime operaties, spionage en de zero-sum-concurrentiestrijd van grootmachten om mondiale invloed, belemmeren ontwikkeling en implementatie van cyber-CBM. Inmenging in verkiezingen, handelsoorlogen en het opzeggen van bestaande, vertrouwenwekkende (!) verdragen werken averechts (de VS en Rusland zegden in 2019 het Intermediate range Nuclear Forces (INF)-verdrag op⁸¹ en in 2020 trok de VS zich terug uit het Open Skies-verdrag).⁸²

Pas als zich een *game-changing* mondiale cyber-catastrofe voordoet (een soort cyber-coronavirus), ligt de weg open naar de creatie en implementatie van effectieve, wereldwijd acceptabele, politiek-bindende cyber-CBM. En zelfs zo'n mondiale catastrofe blijkt geen garantie voor internationale samenwerking en solidariteit.

Zullen die wereldwijde maatregelen er ooit komen? Mondiale consensus over ieder willekeurig onderwerp was problematisch in het verleden, is problematisch in het heden en is waarschijnlijk ook in de toekomst problematisch. Mondiale cyber-CBM zijn daarop geen uitzondering. Bestaande geopolitieke rivaliteit blijft een rol spelen in iedere discussie. Cybergerelateerde beslissingen kun je niet nemen

zonder andere geopolitieke belangen af te wegen. De VN concludeerde reeds dat een wereldomvattend CBM-model in de praktijk onhaalbaar is; maatregelen moeten worden toegesneden op een specifieke situatie of regio. Deze constatering staat evenwel haaks op de pogingen van de achtereenvolgende expertgroepen van de VN (de UN GGE's) die vooralsnog alle juist een allesomvattende, mondiale cyber-CBM nastreefden; tot op de dag van vandaag zonder succes.

Cyberspace is een relatief nieuw domein en de ontwikkelingen rond (cyber-)CBM speelden zich af in recente jaren. In de discussies over de eventuele verschillen tussen cyberspace en andere disciplines waarop het CBM-proces van toepassing is, wordt vaak betoogd (voornamelijk door diplomaten), dat vooruitgang vooralsnog sneller gaat dan vooraf verwacht. De vraag is natuurlijk of dit optimisme ook op langere termijn is gerechtvaardigd, zeker als concrete, succesvolle eindresultaten uitblijven.

In het belang van internationale vrede en stabiliteit is het gewenst en noodzakelijk om de diplomatieke inspanningen voor vertrouwenwekkende maatregelen voor cyberspace te continueren, niet in de laatste plaats omdat de gesprekken, discussies en onderhandelingen op zichzelf al een wezenlijk onderdeel van het grotere confidence-building-proces behelzen. ■

78 Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), *Cybersecuritybeeld Nederland 2019* (Den Haag, 12 juni 2019) 39. Zie: <https://www.ncsc.nl/documenten/publicaties/2019/juni/12/cybersecuritybeeld-nederland-2019>.

79 'Achieve and Maintain Cyberspace Superiority', *Command Vision for U.S. Cyber Command*, april 2018, 6.

80 Michael P. Fisher en Richard J. Harknet, 'Persistent Engagement and Tacit Bargaining: a Path toward Constructing Norms in Cyberspace', *Lawfare* 9 november 2018. Zie: <https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace>.

81 'Opzegging van het verdrag betekent dat Rusland en de VS ongemoeid (nucleaire) raketten voor de middellange afstand kunnen stationeren, waardoor Europa in de gevarenzone komt te liggen.' Uit: Margriet Drent en Adája Stoetman, 'Opzegging van het INF-verdrag: Europa aan zet?', *Europa NU*, 25 februari 2019. Zie: https://www.europanu.nl/id/vkw7h56951x1/nieuws/opzegging_van_het_inf_verdrag_europa_aan?ctx=vhsjhdhfktnpb.

82 U.S. Department of Defense, 'U.S. DOD Statement on Open Skies Treaty Withdrawal', 21 mei 2020. Zie: <https://www.defense.gov/Newsroom/Releases/Release/Article/2195239/dod-statement-on-open-skies-treaty-withdrawal/source/GovDelivery/>.

Geopolitieke overlevingslessen uit het cyberdomein

Hugo Vijver MA*

Sinds afgelopen zomer hoorden we bekende geluiden uit de hoek van de Amerikaanse inlichtingendiensten, dat buitenlandse mogendheden zoals Rusland, China en Iran op heimelijke wijze probeerden de Amerikaanse verkiezingsinfrastructuur te saboteren en de uitkomst van de verkiezingen te beïnvloeden.¹ Vanzelfsprekend is de VS een belangrijk doelwit van Rusland en andere mogendheden. Er valt simpelweg veel te halen en beïnvloeding van het beleid van de VS of van de keuze voor een president kan wereldwijd een groot verschil maken. Maar wie denkt dat wij in Europa niet zo'n interessant doelwit zijn voor strategisch misbruik door wereldmachten, vergist zich. Ook in Europa valt veel te halen: een grote, kapitaal-krachtige interne markt, kennis en innovatie, terwijl interne verdeeldheid en sociale onrust brandstof zijn voor de machtspositie van andere mogendheden. Caroline de Gruyter waarschuwde in *NRC Handelsblad* dat assertieve wereldmachten Europa willen verzwakken. De Turkse president Erdogan chanteert Europa met het doorlaten van vluchtelingen, de VS trekt militairen uit Duitsland terug, Rusland verspreidt desinformatie over het coronavirus en China duwt ons Huawei door de strot. De Gruyters conclusie – de enig juiste – is dat Europa niet meer op anderen kan rekenen en zijn geo-

politieke zaken in het vervolg zelf zal moeten regelen.² De vraag is: hoe moet Europa dat doen? De Gruyter geeft ook hier een zinnig advies over als ze verwijst naar de Russische president Poetin: 'Als we niet willen vechten, prima. Maar laten we dan op zijn minst iets anders doen: man en paard noemen, ophouden met wegduiken (...), alsmaar 'dialogoek zoeken' om hem niet te tarten – dit verandert zijn gedrag niet.'³

We hoeven inderdaad ook niet meteen te vechten, als met vechten conventionele oorlogvoering bedoeld wordt. Dat is hopeloos ouderwets en veroorzaakt altijd onevenredig veel leed en schade, vooral bij mensen die niets met het conflict te maken hebben. Maar vechten kan ook anders. Man en paard noemen is ook een goed idee, helemaal bij de imago-gevoelige leiders van autocratische wereldmachten die zich agressief aan de wereld opdringen als prima alternatief voor het Westen. We kunnen voor beide zaken – vechten en man en paard noemen – inspiratie opdoen in het cyberdomein. Om dat te illustreren gaan we kort terug in de tijd.

Persistent engagement

In het voorjaar van 2019 maakte een delegatie van Buitenlandse Zaken en Defensie een rondje Washington, om met partijen als Defensie, FBI, Justitie en het State Department te praten over ontwikkelingen in en samenwerking op het gebied van cyber. In het Pentagon werd met enkele leiders van het US Cyber Command (het Amerikaanse krijgsmachtsdeel verantwoordelijk voor inzet in het cyberdomein) en onderminister voor cyberbeleid Ed Wilson het nieuwe visiedocument van het Command, *Achieve and Maintain Cyberspace Superiority*, besproken. Wilson legde, met veel jargon maar overtuigend, uit dat

* De auteur is senior adviseur bij de Bestuursstaf van het ministerie van Defensie.

1 Zie bijvoorbeeld 'Statement by NCSC Director William Evanina: Election Threat Update': <https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public> (7 augustus 2020) en de briefing voor het Amerikaanse Congres door FBI-directeur Chris Wray op 17 september 2020: <https://www.axios.com/fbi-director-russia-election-ac152f12-a992-4882-8677-b7d5d16dc918.html>.

2 Caroline de Gruyter, 'Corona brengt EU-landen nader tot elkaar', in: *NRC Handelsblad*, 11 september 2020.

3 Caroline de Gruyter, 'We moeten Poetin nu krachtig veroordelen en bestraffen', in: *NRC Handelsblad*, 4 september 2020.

de *strategic environment* fundamenteel gewijzigd is. Met name Rusland en China halen steeds meer strategisch voordeel uit hun optreden onder het traditionele niveau van gewapend conflict, waar het cyberdomein zich uitstekend voor leent. De VS heeft hier te lang geen antwoord op gehad. Kern van het verhaal was dat het cyberdomein wordt gezien als een domein van *persistent engagement*, vrij vertaald aanhoudend treffen, of aanhoudende wrijving. Waar in de traditionele domeinen direct militair conflict met de VS veelal uit de weg wordt gegaan, zijn er in het cyberdomein juist voortdurend botsingen met strategische tegenstanders. Het US Cyber Command heeft zich daarom ten doel gesteld aanvallen in het cyberdomein voortaan te stoppen door zo dicht mogelijk bij de oorsprong actief te verdedigen. De timing kon niet mooier zijn, want een dag eerder stond breed in de Amerikaanse pers uitgemeten dat het US Cyber Command een Russische trollenfabriek, die het voorzien gehad zou hebben op de tussentijdse verkiezingen van eind 2018, met een digitale aanval offline had gehaald.⁴ De visie was daarmee in praktijk gebracht. In het verlengde van het gesprek roemde Wilson de persconferentie van minister Bijleveld in oktober 2018, waarin ze bekendmaakte dat de MIVD een hackoperatie van de Russische militaire inlichtingendienst GRU in Den Haag had weten te voorkomen. Niet zonder gevoel voor drama, maar geheel terecht, noemde Wilson deze man-en-paard-actie 'very powerful' en 'the best ever orchestrated response'.

Verworvenheden cyberdomein breder trekken

Ik ben van mening dat bovenstaande laat zien dat we twee lessen kunnen trekken uit de mogelijkheden die het cyberdomein biedt: we hoeven bij serieus 'terugslaan' niet meer te denken aan conventioneel-militaire actie en je móét op een gegeven moment terugslaan om je grenzen aan te geven. Effectief terugslaan kan zonder geweld; zie de trollenfabriek die geheel in virtueel puin lag of de persconferentie van minister Bijleveld, die voor het oog van de wereld het Kremlin ter verantwoording riep. Dat moeten we vaker doen. Daarom is het goed dat, na de schaamteloze vergiftiging van de Russische oppositieleider Navalny, in Duitsland en daar-

Een van de lessen uit het cyberdomein: je móét op een gegeven moment terugslaan om je grenzen aan te geven

buiten de discussie nu echt is losgekomen over sancties tegen Poetin door het gasleidingproject Nord Stream 2 op te schorten of helemaal te stoppen. Als Poetin ergens gevoelig voor is, is het voor harde maatregelen die de Russische belangen direct en hard treffen. Of, zoals de voorzitter van de Buitenlandcommissie van de Bondsdag, Norbert Röttgen, zo treffend zei: 'Die einzige Sprache, die Putin versteht, ist eine der Härte'.⁵

Laten we de verworvenheden van het jonge cyberdomein breder trekken. Dus meer persconferenties graag waar met overtuigend bewijs man en paard wordt genoemd, en consequent (persistent) serieuze tegenmaatregelen (engagement) onder de drempel van gewapend conflict. Veel meer opties heeft Europa helaas niet om niet vermorzeld te worden door de wereldmachten. ■

4 Zie onder meer *The Washington Post*, 'U.S. Cyber offensive aimed to safeguard November elections', 27 februari 2019.

5 Zie onder meer: *Welt.de*, 'Nord Stream 2 muss unbedingt fertig gebaut werden', 3 september 2020: <https://www.welt.de/politik/ausland/article214938854/Fall-Alexej-Navalny-Nord-Stream-2-muss-unbedingt-fertig-gebaut-werden.html>.

Herbewapen het Korps Nationale Reserve

Mr. S.A. Wiegman*

Stel dat een groep luchtmobiele collega's wordt opgeleid tot het operationeel kunnen bemannen van een Leopard 2A6. Ongetwijfeld zal die groep militairen de opleiding succesvol afronden, waarna deze tank kan worden toegevoegd aan het luchtmobiele arsenaal. Bij een *air assault*-inzet ontstaan echter direct praktische problemen. Hoewel het 120mm-kanon indrukwekkend oogt en verbluffende vuurkracht kan leveren, zit het danig in de weg bij de uitvoering van een luchtmobiele opdracht. Sterker nog: het kan de uitvoering van de opdracht belemmeren. Niet voor niets verkiest de Luchtmobiele Brigade daarom een Luchtmobiel Speciaal Voertuig (LSV)¹ boven een tank: wendbaarheid verhoogt de slagkracht van een *air assault*-inzet meer dan vuurkracht. Voor een soortgelijke afweging staat het Korps Nationale Reserve (Natres).

Allereerst moet ik een illusie uit de wereld helpen. De Natres is niet opgeleid op een LSV of een gevechtstank; dat zou ook niet passen bij de taakstelling van reservisten. De primaire taakstelling van de Reservist Militaire Taken vat ik gemakshalve samen met het bewaken en beveiligen van wat ons dierbaar is. Het wapen waarmee hij of zij dat moet doen is de Colt C7, dat als persoonlijk wapen aan de reservist is gekoppeld. Maar wat de gevechtstank is voor een *air assault*-operatie, is de C7 voor een bewakings-

en beveiligingstaak: ongeschikt. Ik zal dat toelichten.

Korte afstand

Doorgaans is de inzet van de Natres in een laag geweldsspectrum en met een intensief contact met burgers. Daar ligt ook de kracht van reservepersoneel: zij komen uit de dagelijkse maatschappij en kunnen daarmee dus excellent communiceren. Omdat optreden soms bewapend is, vergt het reservistenoptreden wel een zekere doortastendheid en daarvoor zijn onder meer geweldsmiddelen noodzakelijk. Een persoonlijk wapen is daarvoor een geschikt instrument. Maar mijn pijnpunt is het (enkele) soort wapen. De C7 kan tot op honderden meters nauwkeurig schade aanrichten en past daarom niet bij het directe contact dat de Natres onderhoudt met burgers. Dat directe c.q. onderlinge contact is namelijk veelal op fysiek korte afstand van elkaar. Die korte afstand is relevant. In andere situaties, waarin eventueel gebruik van het wapen noodzakelijk lijkt, zal de reservist zich terugtrekken. Een grotere afstand, van laten we aannemen driehonderd meter, past immers niet in de bewakings- en beveiligingstaak. De crux zit daarin dat als de reservist in het uiterste geval gericht vuur moet uitbrengen, dat alleen kan met het persoonlijke wapen. En dat wringt met de eis van subsidiariteit.²

Karabijn en pistool

Het subsidiariteitsbeginsel houdt in dat het subversieve element wordt geneutraliseerd met een zo min mogelijk schadelijk middel. Daar hangt het proportionaliteitsbeginsel mee samen: het geweld wordt gestopt zodra het doel bereikt is.³ In dat tweede beginsel wordt de reservist continu getraind, maar bij het eerste heeft de reservist niet of nauwelijks keuze. Op het

* De auteur is als geweerbeschutter werkzaam bij het Korps Nationale Reserve en in zijn civiele functie jurist bij de Rijksoverheid. Deze column is op persoonlijke titel geschreven.

1 Luchtmobiel Speciaal Voertuig: een speciaal voor de genoemde brigade ontwikkeld open en licht terreinvoertuig, geschikt voor uiteenlopende operationele taken.

2 De juridische fijnproever heeft gelijk dat dit standpunt jegens een eventuele strafbaarstelling van de reservist uiteraard genuanceerder ligt en onder meer zal afhangen van de omstandigheden van het moment. Voor nu is van belang dat, zoals verderop in de tekst wordt betoogd, de reservist geen keuze heeft in het gebruik van een (geschikt) persoonlijk wapen.

moment dat gericht vuur uitbrengen noodzakelijk is, kan de reservist dat enkel met de C7; een geweer met een lange loop. Een wapen dat, op korte afstand, niet noodzakelijkerwijs het minst schadelijk is. Er zijn lichtere vuurwapens die geschikter zijn om de taakstelling van de Natres te ondersteunen. Zo is de Natres volgens mij beter af met een combinatie van een geweer met het Glock-pistool. Als geweertype pleit ik voor de C8-karabijn. Dit compacte geweer biedt meer praktische bewegingsvrijheid, continueert de robuuste uitstraling van de reservist⁴ en is voldoende geschikt voor (vuur)contact op korte afstand. Een stap in de goede richting qua subsidiariteit is de toevoeging van het pistool aan de wapenuitrusting van de reservist. Het pistool biedt namelijk uitkomst voor (vuur)contact op zeer korte afstand.⁵ Door de reservist de keuze te geven en te trainen in het gebruik van deze geweldsmiddelen, kan het beginsel van subsidiariteit worden toegepast. Niet alleen de reservist ter plaatse heeft dan die keuze: bij de bevelsuitgifte kan het kader meer rekening houden met het verwachte dreigingsbeeld, waarop de bewapening van de manschappen kan worden aangepast. Afhankelijk van het soort opdracht de bewapening kunnen bepalen vergroot de inzetbaarheid van de Natres.

Open debat

In de praktijk dragen de karabijn en het pistool bij aan een verhoogde wendbaarheid van de reservist. De Natres zal veelal opereren op korte afstand van burgers en een praktisch voorbeeld hiervan is het bemannen van een verkeerssluis door reservisten. Bij alle aspecten binnen een verkeerssluis is de C7 *too much* en onwerkbaar. Nog afgezien van de krassen die dat wapen veroorzaakt op het voertuig zodra met de bestuurder wordt gesproken – wat niet meewerkt aan het de-escalerend optreden – moet, zodra een dreiging zich voordoet, eerst een significant aantal passen achterwaarts worden gezet om het vuurwapen eventueel te kunnen gebruiken. Hiermee gaat essentiële tijd verloren en dat kan de reservist zich op dat moment niet veroorloven. Het pistool kan hier uitkomst bieden. Daarbij geeft het pistool, als vuurcontact noodzakelijk is, meer kans op een informatief gesprek met het subversief element nadien.

De C8, gecombineerd met het Glock-pistool, biedt de Natres meerdere voordelen

Mijn verwachting is dat uit een grondige analyse zal blijken dat de C7 ook voor de overige taken van de Natres ongeschikt zal zijn.

De C8, gecombineerd met het pistool, biedt de Natres voordelen qua uitstraling, in de praktische uitvoering en op juridisch vlak. De C7 is zoals de gevechtstank: zodra je de capaciteit bij je hebt, zal je deze moeten gebruiken als dat noodzakelijk is; optimaal is het echter niet. Ik hoop dat deze column uitnodigt tot een open debat over de bewapening van de Natres. Volgens mij is er, na een eerlijke, kritische blik, verbetering mogelijk. ■

-
- 3 De genoemde beginselen zijn hier benaderd vanuit het nationaal (militair) strafrecht.
 - 4 Sterker nog: het dragen van het pistool 'op de man', naast de karabijn voor de borst, kan een robuuster voorkomen opleveren dan enkel het dragen van de C7.
 - 5 Het inwisselen van de C7 voor de C8 draagt niet *per se* bij aan de subsidiariteit, want beide geweertypen maken immers gebruik van munitie met hetzelfde kaliber. De toevoeging van het pistool zorgt ervoor dat er keuze is voor gebruik van een minder krachtig vuurwapen. Een uitwerking over de ballistische kenmerken hoe welk vuurwapen omgaat met welke munitie, laat ik over aan een wapenspecialist.

Vage inrichtingsprincipes? Nee, rollende kronen!

Jaus Müller MA*

The road ahead is empty... miles of the unknown', zong de Nederlandse popgroep City to City. In 1999 stond het nummer vier weken op 1 in de Nederlandse hitlijst (parate kennis van de songtest verraadt dat uw columnist zijn jeugd grotendeels beleefde in de jaren 90). De tekst van de ballad schoot door mijn hoofd toen ik half oktober de 64 pagina's van de *Defensievisie 2035* bestudeerde.¹ Ik kon niet anders dan concluderen dat het liedje niet zou misstaan als de *theme song* van deze verse *Defensievisie*. 'Het dreigingsbeeld wordt diverser, complexer en verontrustender', staat er in. Verderop wordt dit nog eens samengevat in een pictogram van een onheilspellend bozig figuurtje met daaronder: 'tegenstander is onbekend'. Dat wordt de komende vijftien jaar rijden op een weg zonder dat we precies weten wie we precies onderweg tegenkomen. Miles of the unknown...

Hier moet ik even een hand in eigen boezem steken. Begin dit jaar, toen corona enkel nog een onschuldige Mexicaans biertje met een schijfje limoen was, schreef ik in een eerdere column al dat de veiligheidssituatie met het wegvallen van de multipolaire wereld na 1989 met het jaar minder goed voorspelbaar was. Het gevolg: het creëren van voorspellend vermogen is nog nooit zo moeilijk geweest als nu. Ga er dus maar eens aan staan om een visie te schrijven voor 2035,

gebaseerd op een dreigingsanalyse die inherent troebel is.

Een antwoord formuleren op die onbekende weg is niet eenvoudig, maar de vraag is of je er mee wekomt door dan maar tien 'inrichtingsprincipes' te formuleren, zoals de *Defensievisie 2035* doet. Als ik met mijn auto de weg kwijtraak en om route-advies vraag, zou ik raar staan kijken als iemand mij tien kanten tegelijk opstuurt.

Kijken we naar die inrichtingsprincipes, dan roepen die toch ook de vraag op hoe vernieuwend en toekomstgericht die werkelijk zijn. Neem het inrichtingsprincipe 5, 'IGO', oftewel informatiegestuurd optreden. Er staat: 'Het verzamelen, snel verwerken en inzetten van betrouwbare informatie, alsmede snellere en betere commandovoering dan de tegenstander, is in de toekomst vanwege de toegenomen dreiging nog doorslaggevend voor succes.' *What's new?* Je vraagt je af wat die informatie-specialisten binnen de krijgsmacht de afgelopen tijd dan gedaan hebben. We hebben toch juist een uitstekende MIVD die al tientallen jaren precies dit werk doet? En wat hebben die landmachtoverstes dan afgelopen jaren zitten doen op de brigadestaven in de G2-secties? Of de inlichtingen-officieren bij de bataljons wiens kerntaak dit is? Waren al de geavanceerde sensorsystemen op de platforms van de marine dan niet goed afgestemd afgelopen tijd? Ik durf te zeggen dat de krijgsmacht al jaren informatiegericht werkt. Wie dat ontkent, veegt het verleden wel erg makkelijk van

* Op deze plaats vindt u afwisselend columns van Jaus Müller MA en drs. Frans Matser.

¹ *Defensievisie 2035. Vechten voor een veilige toekomst* (Den Haag, ministerie van Defensie, 2020).



tafel door iets nieuws te presenteren wat eigenlijk helemaal niet zo nieuw is.

Meer inzetten op informatiedominantie is natuurlijk altijd goed. En natuurlijk moet Defensie investeren in betere netwerkvoorzieningen met de nieuwste software, zoals de visie terecht bepleit. Maar biedt een dergelijk inrichtingsprincipe genoeg handen en voeten om de komende vijftien jaar de vijand uit de tuin te houden? Het valt te betwijfelen.

Om de krijgsmacht toekomstbestendig te maken, moet de defensiebegroting ergens in de toekomst worden verdubbeld. Jaarlijks is tussen de 13 en 17 miljard extra nodig om de dreiging – wat die ook mag zijn – het hoofd te bieden. De gigantische bezuinigingen op Defensie van het eerste kabinet-Rutte dreunen nog altijd na, terwijl de wereld in de tussentijd bepaald geen veiligere plaats is geworden. Defensie minister Bijleveld is in een lastige positie om bij collega Hoekstra van Financiën geld los te peuteren. Het is begrijpelijk dat de minister van Defensie, midden in een pandemie gevolgd door de sterkste economische terugval sinds de Tweede Wereldoorlog, niet helemaal vooraan staat bij het uitdelen van die paar euro's die nog in de schatkist zitten.

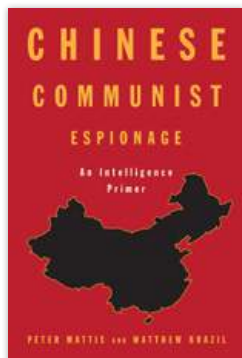
Zitten we klem? Kan het dan niet anders? Misschien wel. In precies dezelfde week dat Bijleveld haar *Defensievisie* presenteerde, deed Peter Hultqvist hetzelfde. Hultqvist is minister van Defensie in het eveneens zwaar door het coronavirus getroffen Zweden. Hij kijkt niet door tot 2035, maar zet in op een middellange-termijnstrategie. Zweden onderkent de dreiging van buurland Rusland, dat om de haverklap het luchtruim en de wateren van het Scandinavische land schendt. Zweden zoekt daarom toenadering tot de NAVO, al blijft het land neutraal. Het blijft niet bij woorden of denkrichtingen. In Stockholm klinken geen vage inrichtingsprincipes en hoopvolle begrotingsprognoses, maar rollen de kronen. Er gaat tussen 2021 en 2025 omgerekend 2,6 miljard euro extra naar Defensie. Zweden, dat iets meer dan tien miljoen inwoners telt, verhoogt de defensiebegroting daarmee met maar liefst 40 procent, tot

'The road ahead is a highway or a dead-end street'

1,5 procent van het bruto binnenlands product. Dat is het hoogste niveau in 17 jaar tijd. Het land krijgt er een gemechaniseerde brigade bij, de luchtmacht Gripen-jachtvliegtuigen met vernieuwde radar, de marine een nieuwe onderzeeër en geld om een nieuw type oorlogsschip te ontwerpen.² Terwijl de Nederlandse visie weliswaar erkent dat de hybride dreiging steeds sterker wordt, ziet Zweden dit ook maar koppelt daar meteen een programma aan vast om cruciale infrastructuur in eigen land weerbaarder te maken tegen cyberaanvallen. Het geheel oogt als een samenhangend programma waar de militair op de grond ook daadwerkelijk wat mee kan gaan doen. Nu wij nog!

Het is niet gek dat er bij het liedje *The road ahead* bij u geen lampje ging branden: City to City beleefde met hun nummer een *one-hit wonder*. Het raakte daarna volledig in de vergetelheid. Laten we hopen dat we medio 2035 niet hetzelfde moeten zeggen van de Nederlandse defensieorganisatie. ■

2 Government Offices of Sweden, 'Substantial investment in total defence' (Stockholm, 16 oktober 2020). Zie: <https://www.government.se/press-releases/2020/10/substantial-investment-in-total-defence/>.



Chinese Communist Espionage

An Intelligence Primer

Door Peter Mattis en Matthew Brazil

Annapolis (Naval Institute Press) 2019

360 blz.

ISBN 9781682473030

€ 36,99

In het jaarverslag van de MIVD over 2019 schreef directeur generaal-majoor Jan Swillens dat 'digitale spionage door statelijke actoren, zoals Rusland en China (...) een van de grootste dreigingen voor Nederland en zijn bondgenoten' vormt. Of de dienst voldoende zicht weet te houden op deze ontwikkeling is volgens Swillens maar de vraag. Inzicht in de intenties en capaciteiten van de Volksrepubliek China, die ernaar streeft in 2049 de belangrijkste wereldmacht te zijn, zal voor de inlichtingen- en veiligheidsdiensten alleen maar belangrijker worden. Beijing laat zich militair, diplomatiek, economisch en op het inlichtingenvlak steeds meer gelden. *Chinese Communist Espionage. An Intelligence Primer* van de Amerikanen Peter Mattis en Matthew Brazil is alleen daarom al een actueel en belangrijk boek. Voormalig CIA-analist Mattis is gespecialiseerd in het hedendaagse handelen van de Chinese diensten, terwijl oud-legerofficier en oud-diplomaat Brazil zich op het verleden richt.

Huidige kennisstand

Sinologen vermijden het onderwerp *intelligence* en studies van inlichtingenexperts over China beperken zich veelal tot economische spionage en

cyber crime. Die nauwe blik kan tot een vertekend beeld leiden van Chinese spionage in het algemeen. In het grotendeels op Chinese bronnen gebaseerde *Chinese Communist Espionage* behandelen Mattis en Brazil daarom zowel de historische wortels van de Chinese diensten als de huidige inlichtingenoperaties van de Volksrepubliek China. Zoals de ondertitel aangeeft is het boek een inleiding in het onderwerp, die de huidige kennisstand weergeeft. Daarmee dient het niet alleen als uitgangspunt voor verder onderzoek, maar ook als handzaam overzicht van de belangrijkste Chinese inlichtingenorganisaties, hun vooraanstaande spionnen en voorbeelden uit de Chinese spionagepraktijk. In de inleiding beschrijven de auteurs enkele constanten in de geschiedenis van de Chinese inlichtingendiensten, zoals de angst voor infiltratie, het meedogenloze optreden bij zuiveringen en de overheersende rol van de krijgsmacht bij het vergaren van buitenlandse intelligence sinds de open-deurpolitiek van Deng Xiaoping (1978-1989). Daarnaast gaan zij in op de opkomst van China als een *global intelligence power*, waarbij de vroege omarming van het cyberwapen in de jaren negentig opvalt. In het

militaire domein zien de auteurs de reorganisatie van de strijdkrachten onder Xi Jinping in 2015 als een keerpunt: waar de nadruk voorheen op strategische inlichtingenvergaring lag, kregen nu operationele en tactische inlichtingen een prominere plaats binnen de krijgsmacht.

Case study's

In zeven hoofdstukken behandelen Mattis en Brazil verschillende facetten van moderne Chinese spionage, vanaf de oprichting van de Communistische Partij in 1921 tot heden. In hoofdstuk 1 en 2 bespreken zij verscheidene Chinese inlichtingen- en veiligheidsdiensten en het leiderschap van de diensten. In de inleiding benoemde trends worden hier van voorbeelden voorzien: zo voerde het ministerie van Publieke Veiligheid (1949-heden) begin jaren vijftig 700.000 executies uit tijdens een campagne tegen 'contrarevolutionairen' en wordt de loyaliteit van de diensten aan Mao Zedong geïllustreerd door het optreden tijdens zuiveringen als het Futian-incident (1930), de Rectificatiecampagne (1943) en de Culturele Revolutie (1966-1976). Hoofdstuk 3 tot en met 6 behandelen spionage-operaties in en door China tijdens de Chinese Revolutie en de vroege Volksrepubliek, loopbanen van de belangrijkste spionnen tijdens die periode, gevallen van economische spionage en spionage tijdens de recente opkomst van China (1989-heden). De hoeveelheid case study's die Mattis en Brazil aanvoeren is ontzagwekkend: van de moorden op nationalist die de communistische agent Gong Changrong in het Shanghai van de jaren dertig vanaf zijn fiets pleegde, de rol die Hong Kong vanaf 1921 als spionnest speelde, de gevangenneming van de CIA-agenten John

Downey en Richard Fecteau in 1952 en economische spionage via onder meer genaturaliseerde Chinezen in de VS tot het lekken van informatie door kolonel James Fondren van het U.S. Pacific Command tussen 2004 en 2008.

De passage over de nationalistische generaal en dubbelagent Mo Xiong illustreert dat sommige verhalen niet zouden misstaan in Hollywood-films. Toen hij in oktober 1934 intelligence over de aanstaande vernietiging van het Chinese Rode Leger door de troepen van Chiang Kai-shek in handen kreeg, wilde hij die aan de communisten lekken. Omdat alleen landlopers Shanghai konden verlaten, verzon hij een list: 'He knocked out four of his front teeth with a stone, sullied his clothing, and made himself appear like a roughed-up beggar. (...) When challenged, Xiong told of being beaten and chased by dogs at a rich man's house. It was enough for the Nationalist sentries to allow him through without a search that might have changed the course of modern Chinese history'. Tot slot laat hoofdstuk 7 zien hoe de diensten in China ingezet werden en worden om de

binnenlandse veiligheid te verzekeren. Daarbij komen onder meer inspanningen op het gebied van (militaire) contra-inlichtingen en de geraffineerde methoden die het ministerie van Staatsveiligheid toepast bij het bespioneren van de eigen bevolking en buitenlanders aan bod.

Twee boeken in één

Hoewel Mattis en Brazil hun boek als inleiding op het onderwerp typeren, doen zij het daarmee tekort; *Chinese Communist Intelligence* is in feite twee boeken in één, over de geschiedenis en over het heden van Chinese intelligence. De keuze voor de deels overlappende hoofdstukken leidt evenwel regelmatig tot herhalingen. Verder is het jammer dat de auteurs enkele lijnen uit de verschillende hoofdstukken niet hebben samengebracht in een epiloog. Thema's die zich daar goed voor lenen zijn de macht van militaire attachés bij het vergaren van intelligence in en over het buitenland, de gevolgen van maoïstisch taalgebruik binnen de Chinese diensten en het spanningsveld tussen partijbelangen en de

inlichtingengemeenschap. Het is daarbij de vraag in hoeverre *telling truth to power* opgaat in China, zeker nu Xi Jinping 'has returned to Mao's policy of demanding personal loyalty from his security services' (blz. 58). Daarnaast zou het bij een tweede versie interessant zijn om meer Europese voorbeelden te zien bij het hoofdstuk over economische spionage. Ondanks deze kanttekingen is *Chinese Communist Espionage* een fantastisch boek voor geïnteresseerden in de handelwijze van de Chinese inlichtingengemeenschap in het verleden en het heden. Hoewel het tjokvol feiten staat en de informatiedichtheid hoog is, hebben Mattis en Brazil een goed leesbaar boek geschreven dat niet verveelt. Zij tonen de noodzaak van het gebruik van Chinese bronnen en de meerwaarde van een historische aanpak. Vanwege de breedte en de diepgang zal *Chinese Communist Espionage* een standaardwerk zijn voor historici, Chinadeskundigen en analisten bij inlichtingen- en veiligheidsdiensten. ■

T.A. Onderwater MA, Nederlands Instituut voor Militaire Historie

MEDEDELING

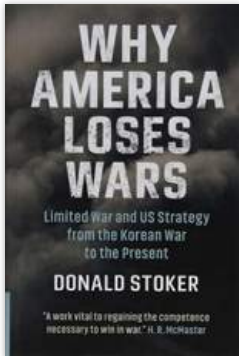
Voordrachten gevraagd voor de Kooy Prijs 2021

Het Koninklijk Instituut van Ingenieurs (KIVI) kent jaarlijks de Kooy Prijs toe voor de beste scriptie over defensie- of veiligheidstechnologie geschreven aan een technische universiteit of hogeschool.

Voordrachten voor de Kooy Prijs 2021 kunnen tot en met 23 december 2020 worden ingediend. Meer informatie over de voordrachtprocedure is te vinden op www.kivi.nl/dv onder prof. Kooy afstudeerprijs.

De prijs, tweeduizend euro en een certificaat, is genoemd naar prof. Johan Kooy, in de vorige eeuw een internationaal bekende hoogleraar in de rakettechniek. De uitreiking vindt plaats op het Kooy Symposium op 3 juni 2021 in Stroe.

In 2020 ging de prijs naar ir. Laurent Declerck van de TU Delft voor zijn onderzoek naar de prestaties en vliegeigenschappen van compoundhelikopters. Als het te lang is mag de oranje alinea er af.



Why America Loses Wars

Limited War and US Strategy from the Korean War to the Present

Door Donald Stoker

Cambridge (Cambridge University Press) 2019

332 blz.

ISBN 9781108479592

€ 25,-

Donald Stoker stelt in *Why America Loses Wars* aan de orde waarom in zijn visie de Verenigde Staten sinds de Korea-oorlog geen conflict of oorlog meer hebben kunnen winnen. De oorzaak hiervan herleidt Stoker naar de ruimte die opeenvolgende presidenten sinds Harry Truman zoeken om de Amerikaanse strijdkrachten in te zetten zonder hierbij gehinderd te worden door het Congres. Dit kan alleen wanneer een formele oorlogsverklaring achterwege blijft. Termen als *low intensity conflict*, *fourth/fifth generation warfare*, *hybrid war*, et cetera komen in zwang om een conflict het stempel 'beperkt' te geven en zo de noodzaak van een formele oorlogsverklaring te omzeilen. Stoker brengt al deze conflictvormen onder één noemer, namelijk 'limited war'. Dit is volgens de auteur een met vaagheid omkleed begrip, waarover verderop meer. Om de beperking 'tastbaar' te maken, worden bewust grenzen gesteld aan de middelen en mogelijkheden waarover commandanten kunnen beschikken. Dit werkt door in het formuleren van de te voeren strategie. Deze wordt niet langer gedomineerd door de politieke doelstelling, maar door de politiek haalbare geachte inzet van midde-

len. Een omdraaiing van de klassieke doel-middelen relatie.

Zelf opgelegde beperkingen

Stoker analyseert uitvoerig tot welke ongewenste effecten het omdraaien van de doel-middelenrelatie leidt. Hij gebruikt Clausewitz als theoretisch kader voor zijn analyse. Vervolgens wijst hij niet alleen met een beschuldigende vinger naar de beleidsmakers maar bekritiseert ook tal van bekende wetenschappers en theoretici die onderbouwing leveren voor limited war als alternatief voor Clausewitz' gedachtengoed. Beleidsmakers zijn in zijn visie vooral politici en hoge ambtenaren. Hij verwijt militaire commandanten soms te 'gehoorzaam' te zijn geweest, hoewel we deze kritiek meer tussen de regels door moeten oppikken.

Met Clausewitz in de hand wijst Stoker op het gegeven dat een conflict, vanwege allerlei fricties en factoren die we niet kunnen beheersen of beïnvloeden, sowieso veel beperkingen kent: bijvoorbeeld 'basale' zaken als tijd en geografie, maar ook publieke of internationale steun. Maar, zo stelt hij, een intelligente flexibele geest kan binnen een deugdelijk geformuleerde strategie omgaan met dit soort beperkingen.

Het risico zit in de politiek opgelegde beperkingen. Hij noemt deze 'zelf opgelegde beperkingen'. Zij leiden ertoe dat 'beperking' omslaat in 'onvoldoende'. Zo onvoldoende, met name in termen van de hoeveelheid in te zetten personeel en materieel, dat het conflict onmogelijk nog tot een goed einde gebracht kan worden. Stoker beschuldigt de beleidsmakers er zelfs van dat zij het niet winnen van een conflict als zelf opgelegde beperking inmiddels acceptabel vinden. Aan de hand van voorbeelden uit de conflicten waarbij de VS sinds Korea betrokken zijn geweest, beschrijft Stoker welke dure consequenties deze opgelegde beperkingen voor de VS hebben. Hij wijst op de langdurige en blijvende betrokkenheid van de VS bij conflicten. Deze gaan gepaard met al maar oplopende kosten en bovenal met onnodig veel bloedvergieten. Een heilloze weg, volgens Stoker, die het tegengestelde bewerkstelligt van wat het begrip limited impliceert. Is Stokers pleidooi dus om alle beperkingen maar te laten varen? Dat duidelijk ook niet.

De oplossing kan volgens Stoker ook niet gevonden worden in het formuleren van de (enig) juiste limited war-strategie. Die is namelijk niet te formuleren, want limited war is een subjectief en (daardoor) ondefinieerbaar begrip. Met name op dit punt bekritiseert hij de theoretici die het tegenovergestelde beweren. Het juiste antwoord is volgens Stoker dat beleidsmakers in de VS weer moeten inzien en begrijpen dat een limited war gewonnen moet worden. In het verlengde hiervan moet in de te volgen strategie de politieke doelstelling weer leidend zijn in plaats van de middelen. Tot zover is Stoker overtuigend. Maar hoe zit het met de

haalbaarheid van zijn pleidooi? Deze manier van denken over limited war manifesteert zich nu al zo lang, die draai je niet zomaar terug. Stoker rept er met geen woord over hoe hij dit denkt te bewerkstelligen. Zijn pleidooi is dus eigenlijk niet af.

Politiek, bevolking en krijgsmacht

Waar ik benieuwd naar ben, is tot welke oplossingen of conclusies Stoker zou zijn gekomen indien hij Clausewitz' drie-eenheid als analytisch raamwerk had meegenomen in zijn overwegingen. Clausewitz beschrijft met behulp van deze drie-eenheid de onlosmakelijke relatie tussen politiek, bevolking en krijgsmacht. Stoker richt zijn kritische pijlen op één element van deze driehoek, namelijk de politiek. De andere elementen van de driehoek en hun onderlinge relatie blijven nagenoeg onbesproken. Hierin schuilt een belangrijk gevaar, stelt bijvoorbeeld Bart Schuurman die het thema dat Stoker aansnijdt jaren geleden al eens analyseerde in een artikel in de *Militaire Spectator*.¹ Onderbelichting van een van de drie elementen van de driehoek of het leggen van onbewezen

relaties daartussen, zo beschrijft Schuurman, leidt ertoe dat de uitkomst van de analyse volledig los komt te staan van de realiteit en dus onbruikbaar is.

Andere voorbeelden van een pleidooi voor een meer integrale analyse van de driehoek en de verhoudingen daarbinnen verschenen, eveneens in de *Militaire Spectator*, in een editoriaal en een artikel van KTZ Henk Warnar.² Het editoriaal wijst op rol en belang van 'politieke cultuur'; KTZ Warnar wijst op 'cultuur' in bredere zin. Met een beter en dieper besef van de (politieke) cultuur om ons heen, zijn we binnen de driehoek waarschijnlijk beter in staat tot de gewenste strategische kwaliteit te komen, dan door haar of elementen daarbinnen te 'bevechten'. Dit laatste is namelijk wat Stoker doet, waarmee hij ons mogelijk een betere oplossing onthoudt.

Samenvattend: waarom het in Stokers visie in de VS fout is gelopen met het concept van limited war legt de auteur mede dankzij zijn heldere en directe schrijfstijl op overtuigende wijze uit. Stokers pleidooi is onderbouwd vanuit de theorieën van Clausewitz, aangevuld vanuit een rijke bibliografie waarin ook werk van de Nederlandse auteurs Kees Homan, Ger Teitler en Rob de Wijk te vinden is. Dit is overigens niet de enige Nederlandse inbreng: Samuel Kruijzinga van de Universiteit van Amsterdam becommentarieerde het manuscript. De oplossing zoals Stoker die ziet, overtuigt echter niet. Lawrence Freedman lijkt hier eveneens op te duiden in zijn korte, maar twijfelende beoordeling van Stokers boek in *Foreign Affairs*.³ ■

LtKol KLu b.d. drs. Jan-Leendert Voetelink

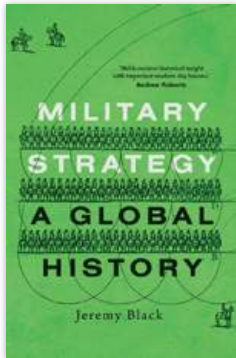
- 1 B.W. Schuurman, 'Clausewitz en de new wars denkers. Een nieuwe kijk op het trinitaire concept en de critici', in: *Militaire Spectator* 179 (2010) (1) 33-43.
- 2 'Normatieve discussie in strategievorming', editoriaal in: *Militaire Spectator* 188 (2019) (12) 578-579; Henk Warnar, 'Van wereldmacht tot 'braafste jongetje'', in: *Militaire Spectator* 188 (2019) (12) 633-636.
- 3 Lawrence D. Freedman, 'Why America Loses Wars: Limited War and US Strategy From the Korean War to the Present', in: *Foreign Affairs* 98 (2019) (5) 228.

Schrijft u een gastcolumn in de *Militaire Spectator*?

De redactie van de *Militaire Spectator* biedt lezers de mogelijkheid een gastcolumn te schrijven van maximaal duizend woorden. Het thema is vrij, maar moet passen in de formule van het tijdschrift. Een gastcolumn bevat een relevante boodschap voor de lezers, een gefundeerde eigen mening en juiste en verifieerbare feiten in een logisch opgebouwd betoog. U kunt uw gastcolumn sturen naar de bureauredactie (zie colofon) of aanbieden via de website. De redactie wacht uw bijdrage met belangstelling af.

De hoofdredacteur





Military strategy

A Global History
 Door Jeremy Black
 New Haven (Yale University Press) 2020
 306 blz.
 ISBN 9780300217186
 € 30,-

Een boek van Jeremy Black recenseren is altijd leuk. De Britse veelschrijver heeft een eigenzinnige kijk op militaire geschiedenis en zijn argumentatietrant zet je doorgaans aan het denken. Bij zijn recente boek over de geschiedenis van militaire strategie, uitgegeven bij het prestigieuze Yale University Press, is dat niet anders. Al vroeg in het boek (blz. xi) neemt Black stelling tegen diegenen die beweren dat er tegenwoordig een tekort bestaat aan strategisch denkvermogen. Strategie is niet een *lost art* die mensen vroeger beter beheersten, want het succes van een bepaalde strategie is contextgebonden. Wat werkte in de ene situatie, werkt niet noodzakelijkerwijs in de andere. Strategie draait om handelen, al dan niet met militaire middelen, en de afwegingen en ideeën die daaraan ten grondslag liggen. Er is geen recept voor succes en ‘generalisaties op basis van *specifics*’ (theorievorming dus) bevatten, soms ernstige, tekortkomingen (blz. 2). Politieke en militaire leiders laten zich niettemin vaak door theorievorming leiden, terwijl ‘(...) understanding the nature of a particular conflict, rather than theorizing about war in general, is crucially necessary’ (blz. 21). Ik kom hierop nog terug.

Black behandelt in vogelvlucht de strategieën van de continentale Euraziatische mogendheden vanaf omstreeks 1450, en betreft daarbij ook nadrukkelijk China. Hij besteedt vervolgens meer aandacht aan de Britse strategieën vanaf de late 17e eeuw. De Amerikaanse Onafhankelijkheidsoorlog en de Napoleonische oorlogen komen daarna aan de orde, gevolgd door hoofdstukken over de Amerikaanse Burgeroorlog, de Eerste Wereldoorlog, de Tweede Wereldoorlog, de Koude Oorlog en het huidige tijdsgewricht. Hij wijst daarbij op een aantal continuïteiten, maar benadrukt ook dat de omstandigheden in elke periode anders waren, wat generalisaties lastig maakt.

Geveinsde verbazing

Deze werkwijze leidt tot een inzichtrijk boek, waarbij de lezer op bijna elke pagina wordt uitgedaagd diepgewortelde overtuigingen terzijde te leggen. Black bindt bijvoorbeeld de strijd aan met de sinds Geoffrey Parker gangbare opvatting dat technologische innovaties veranderingen op het slagveld inluiden. Dat technologie een *game changer* kan zijn, bestrijdt Black niet, maar hij ziet vooral driften, ideeën en politiek als

drijfveer: de zucht naar eer, de honger naar territorium en buit. De vanaf begin 16e eeuw toegenomen effectiviteit van vroegmoderne krijgsmachten moet primair toegeschreven worden aan betere organisatie en administratie. Effectiviteit door efficiency, in plaats van door innovatie, derhalve. Prikkelend is ook zijn terloops vermelde (blz. 127) – en zonder twijfel geveinsde – verbazing over de aandacht waarin Duitse strategen zich in studies over strategie mogen verheugen: dat land werd immers tot twee keer toe verslagen, in 1918 en 1945. Terecht plaatst hij ook kanttekeningen bij het mechanische en rationalistische idee dat een keuze voor strategie x automatisch leidt tot uitkomst y. Die opvatting miskent immers de menselijke factor, terwijl oorlog (en politiek) mensenwerk zijn, waarin angsten, vooringenomenheden en onzekerheid het vaak winnen van rationaliteit. De vraag wat de ‘beste’ strategie is, laat zich dus niet zonder meer beantwoorden, en brengt Black er ook toe in het voorbijgaan (blz. 258) kanttekeningen te plaatsen bij het gebruik van speltheorie en *serious gaming* om scenario’s te testen.

Nadelen brede definitie

Hoewel ik als historicus veel sympathie kan opbrengen voor het idee dat strategie eigenlijk niets anders is dan een poging om specifieke historische ervaringen te veralgemeniseren in ‘lessen’ en ‘principes’, en dat daarbij een zekere pad-afhankelijkheid optreedt (‘strategische cultuur’), voelde ik me tijdens het lezen van dit boek bij tijd en wijle toch ongemakkelijk. Dat heeft een aantal redenen. De brede definitie van strategie die Black voorstaat, oogt aantrekkelijk,

maar heeft ook een aantal nadelen. Als alles wat een land inzet om een doel te bereiken *strategie* is, verdampt het verschil met politiek, terwijl de inhoudelijke overlap met het begrip *strategische cultuur* tot verwarring leidt. Dat begrip is immers zelf ook problematisch: volgens Black verklaart strategische cultuur de continuïteit in de wijze waarop landen politieke doelen nastreven, al dan niet met militaire middelen. Maar waarom dat soort continuïteiten bestaan, wordt eveneens verklaard aan de hand van dat begrip. Zo ontstaat een cirkelredenering: de onderliggende aanname dient als bewijs dat de aanname klopt. Als strategie synoniem is aan strategische cultuur, is alles strategie en valt er ook geen onderscheid meer te maken tussen bedoelde en onbedoelde effecten van de keuzes. *Alles* wordt dan immers strategie: het plan, het proces en zelfs de uitvoering. Dat lijkt me uit analytisch

oogpunt een onaanvaardbaar hoge prijs. Black ziet dat zelf ook, want hij grijpt in de meeste hoofdstukken terug op een engere definitie. Ik sluit echter niet uit dat zijn aanvankelijke keuze is ingegeven door een – begrijpelijke – zorg over de trend om ‘strategie’ los te zien van ‘politiek’, waarbij strategie dan het exclusieve domein van de militaire professional is (vgl. blz. 272), een trend die Black vooral ziet in Groot-Brittannië en de Verenigde Staten. Het was misschien verstandig geweest om het boek daarmee te openen.

Denkwerk

Daarnaast presenteert Black zijn ideeën vrij stellig en is het aantal bronvermeldingen beperkt. Beide zijn beslist geen unicum in Angelsaksische geschiedschrijving, maar sommige stellingen, zoals dat er een rechte lijn loopt van tsaar Alexej (1629-1676) naar Vladimir Poetin,

zijn zonder verdere argumentatie echt te kort door de bocht. Voor een boek dat niet alleen grote lijnen trekt, maar ook waarschuwt tegen het naar hartenlust uit hun historische context lichten van ‘lessen’ uit het verleden (bijvoorbeeld op blz. 270), is dat opmerkelijk. Opvallend is ook dat de *conclusions* aan het eind van de meeste (niet eens alle) hoofdstukken maar weinig te maken hebben met de inhoud van het betreffende hoofdstuk. Mislukt zou ik het boek echter allerminst willen noemen, al is Black er niet in geslaagd een werkelijke *global history* te schrijven. Zijn centrale punt overtuigt echter: strategie is niet het mechanisch heen en weer schuiven van blokjes over een kaart. Het vereist denkwerk. ■

Dr. Floribert Baudet, Faculteit Militaire Wetenschappen/Nederlandse Defensie Academie

MEDEDELING

Vernieuwing website en tijdschrift

De website van de Militaire Spectator, www.militairespectator.nl, wordt in het voorjaar van 2021 vernieuwd. Het archief, dat teruggaat tot 1832, krijgt een uitgebreidere zoekfunctie en rubrieken zullen sneller vindbaar zijn. Het gedrukte tijdschrift krijgt vanaf januari 2021 nieuwe, moderne vormgevingsaccenten.

De hoofdredacteur



‘Oorlog tegen waanbeelden’

In zijn boek *Onvoorspelbaar Verleden* beschrijft oud-militair Nikko Norte zijn ervaringen als inlichtingspecialist in de Afghaanse provincie Uruzgan in 2006-2007. Hij plaatst kanttekeningen bij de internationale interventie van de International Security Assistance Force (ISAF) en bij het Nederlandse optreden.

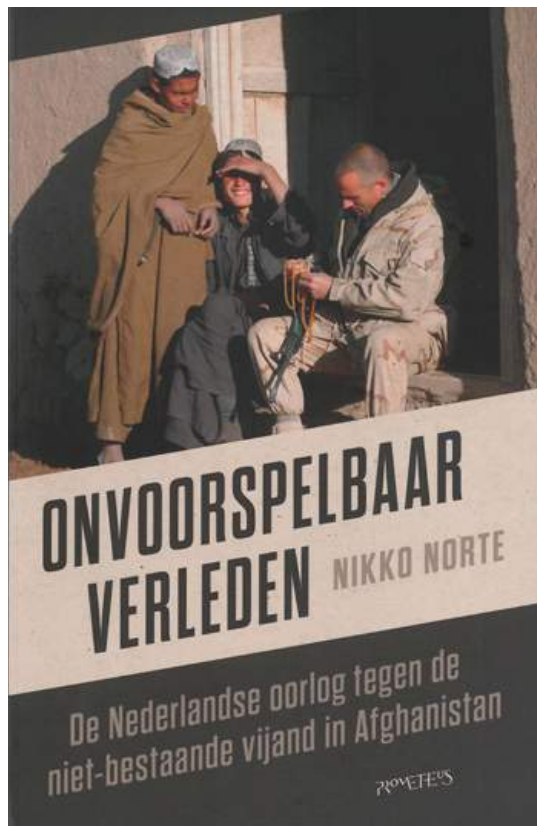
Arthur ten Cate en Frans van Nijnatten

***Onvoorspelbaar verleden* gaat over uw tours als inlichtingsonderofficier bij de eerste twee Battlegroups van de Task Force Uruzgan (TFU). De strekking van uw verhaal is dat ISAF-troepen daar hun eigen vijand creëerden?**

Afghanistan zijn geen bange en zeker geen laffe mensen. Macht der gewoonte maakt dat zij het gebied waarin zij wonen tegen kwaadwillende indringers beschermen en kwaadwillend is iedere indringer tot het tegendeel is bewezen. Daarnaast werkte de Nederlandse manier van optreden, door bijvoorbeeld te opereren in SUA's [*smallest unit of action*] die de omvang hadden van ten minste een peloton, als de bekende rode lap op een stier. Dat optreden straalde angst uit, die er ten onrechte was, en spoorde jonge Afghaanse mannen aan af en toe wat schoten op SUA's te lossen of er een RPG op af te vuren. De barrage van Nederlands vuur die doorgaans op een paar schoten of een afgevuurde RPG volgde, leidde tot onvrede onder de bevolking en daarmee was een negatieve spiraal ingezet.

Los van het voorgaande had het ingraven van IED's en het afschieten van 107-millimeter-raketten in het relatief kleine Nederlandse inzetgebied voorkomen kunnen worden. Kleine eenheden, één groep, die zich doorlopend door nederzettingen verplaatsten en niet erlangs, hadden het respect van de bevolking kunnen

Kapitein b.d. Nikko Norte (Rotterdam, 1964) is een Nederlandse schrijver en blogger. Hij verbleef het grootste deel van zijn volwassen leven in conflictgebieden, is vliegtuig- en helikopterpiloot en bracht in dienst van de Nederlandse krijgsmacht in diverse intelfuncties twee jaar door in de Afghaanse provincie Uruzgan.



¹ Nikko Norte, *Onvoorspelbaar Verleden. De Nederlandse oorlog tegen de niet-bestaande vijand in Afghanistan* (Amsterdam, Prometheus, 2020, 304 blz.).

winnen – ook dat van naar roem dorstende jonge mannen – en hadden die bevolking er als vanzelfsprekend van overtuigd dat zij geen kwaadwillende indringers waren.

U reisde zomer 2006 van Kandahar Airfield naar Tarin Kowt, Uruzgan, in een zwaar-bewapend konvooi met gevechtsvoertuigen en Apache-gevechtshelikopters erboven. U noemt dat ‘onzinnig en een verkeerd signaal’. Wat was dat signaal en aan wie?

Iedere Afghaan die de konvooien zag passeren, begreep dat slechts een handvol transportvoertuigen door een enorme troepenmacht werd beschermd op een weg waar nauwelijks gevaar dreigde. Zoals ik schrijf, reed ik het traject tweemaal met slechts twee Amerikaanse humvees. Overbeveiligde konvooien gaven een signaal van angst af en dat is in Afghanistan niet verstandig, omdat het iets dappers wakker roept bij mensen die zich onder andere omstandigheden niet tot vijandelijkheden hadden laten verleiden. Hetzelfde signaal werd afgegeven met de bouw van een gepantserde stad, waarvan de bouw door overbeveiligd vervoer vertraging opliep. De transporten werden uiteindelijk overgelaten aan Afghaanse vrachtwagenchauffeurs en hun onbeveiligde konvooien werden logischerwijze staande gehouden en geplunderd. Niet per se door taliban of door een vijand van Nederlandse troepen, maar door iedereen die daar zin in had.

Een typische situatie: u beschrijft uw eerste ontmoeting met een militie, bij Spinkechah bij Tarin Kowt, als u op pad bent met Afghaanse militairen. Die militie was een soort drugsbende?

Tijdens deze ontmoeting liet ik me door mijn Afghaanse vriend Wahdat uitleggen dat we op een militie stuitten. Wat voor militie dat was, was iedereen, ook mij, onduidelijk. Milities hadden linksom of rechtsom altijd iets met drugs te maken, om de eenvoudige reden dat de hele Afghaanse economie daarom draait. Welke partij die milities in de drugshandel kozen was onduidelijk, want er was niemand die ook maar een vaag idee had van de structuur van die handel.

‘Overbeveiligde konvooien gaven een signaal van angst af en dat is in Afghanistan niet verstandig’

Het leggen van berm bommen, dat is toch bepaald geen spelgoed in handen van hooligans, zoals u ze noemt?

Het bouwen en ingraven van IED's in Uruzgan was initieel het werk van amateurs. Een duidelijke reactie van Nederlandse troepen op de dreiging bleef uit – mijn voorstel was de wegen die gevoelig waren voor het ingraven van IED's onder permanente waarneming te houden, wat eenvoudig mogelijk was geweest – en dus boekten de bouwers en de ingravers van IED's successen die betere bommenbouwers en ingravers aantrokken. IED's, zeker in de eerste twee jaar van de Nederlandse inzet in Uruzgan, waren dus spelgoed in handen van hooligans en om dat in perspectief te plaatsen: u en ik knutselen veel van de in Uruzgan ingegraven IED's met weinig moeite in elkaar. Voor zulke IED's was geen organisatie nodig. Alle materialen waren vrij voorhanden en de kennis om een IED te bouwen kon overal worden opgedaan. Meer en meer mengsels van diesel en kunstmest werden gebruikt, wat aangeeft – maar niet per se bewijst – dat er geen aanvoer van gedegen hoofdvladingen voor IED's was, zoals in andere provincies.

U was ook in Ali Sherzai, de hoofdbazaar van het district Chora in het noorden van de Baluchivallei, vlak na de eerste aanval daar, in juni 2006. Was het geen aanval van de Taliban, maar drugsgerelateerd?

Wat ik in juni 2006 leerde over de ‘aanval’ op Chora was dat er twee pick-uptrucks met gewapende mannen het dorp in waren gereden, dat een aantal politieagenten – voor zover de mensen onder het bevel van politiecommandant Gul die naam waardig waren – klappen had gekregen en dat er was geprobeerd

brand te stichten in een door de Amerikanen neergezet gebouw dat zij (de Amerikanen) 'school' noemden. Uiteraard was een en ander drugsgelateerd, maar hoe precies, was onduidelijk. De mensen die van een pak slaag een aanval maakten, werden door de lokale bevolking gekscherend 'dolari' genoemd: mensen die hun moeder voor een paar dollar zouden verkwanselen. Het opwaarderen van 'dolari', die doorgaans een paar woorden Engels spraken, tot informant had verstrekkende gevolgen.

Het narratief was altijd, onder meer door dergelijke gevechtsacties in districtscentra, dat het in Zuid-Afghanistan wemelde van de Talibanstrijders (georganiseerd Talibanverzet). Ook de Amerikanen, Australiërs en Emiraten vochten in Uruzgan behoorlijke veldslagen uit voordat Nederlandse troepen in 2006 arriveerden.

Ik zie het als een groot waanbeeld. Uruzgan was voor westerse troepen de provincie bij uitstek om roem te vergaren, juist omdat het er structureel aan een werkelijke vijand ontbrak en het er wemelde van de 'dolari'. Ik nam deel aan twee elkaar opvolgende acties in de Baluchivallei, Operation Perth en een operatie die door het Nederlandse KCT werd uitgevoerd. Iedereen die die acties als juist of noodzakelijk beoordeelt, nodig ik uit om samen met mij een uurtje op Google Earth naar de Baluchivallei te staren. Een kinetische actie in de Baluchivallei tegen een niet als zodanig identificeerbare vijand is onmogelijk te rechtvaardigen en had dus ook niet mogen worden uitgevoerd, waarmee ik terugkom op mijn stelling dat bijvoorbeeld de Baluchivallei de plek bij uitstek was om roem te vergaren en niet om tot oplossingen van problemen te komen. De Australiërs noemden Operatie Perth hun 'eerste veldslag sinds Vietnam'. Dat er op troepen die de Baluchivallei

*Groene zone bij de Baluchipas
overgang tussen de Derafshan- en
Baluchivallei*

FOTO BEELDBANK NIMH (AVDD, JUUL PLATENBURG)



introkken werd geschoten, is logisch, maar dat wil niet zeggen dat er een vijand was.

Bij uw eerste vuurgevecht in Surk Murgab (Derafshanvallei) met het Afghan National Army en de Amerikanen vroegen jullie je af: tegen wie vechten we eigenlijk?

Het was mij tijdens mijn eerste vuurgevecht onduidelijk tegen wie we vochten. Daar kwam bij dat we elkaar al na een paar minuten kwijt waren en iedereen feitelijk individueel aan het knokken was tegen een vijand die, zoals dat altijd is in landen als Afghanistan, onzichtbaar was. Pas een dag later kwam ik er achter wat de oorzaak van dat bewuste gevecht was. Veel mannen in de strijdbare leeftijd waren vanwege Operatie Perth de Baluchivallei ontvlucht en hielden zich schuil in nederzettingen ten noorden en zuiden van de vallei. Ten zuiden van de vallei had een Nederlands peloton in pantservoertuigen een heuveltop bezet zonder dat wij daarvan op de hoogte waren. Zoals ik in mijn boek schrijf, waren dat waarschijnlijk de eerste rupsvoertuigen sinds lange tijd in de regio en dat hun aanwezigheid tot onvrede leidde, laat zich raden. De YPR's – tanks in de ogen van de lokale bevolking – vormden een te geduchte tegenstander om aan te vallen; wij vormden dat niet.

In oktober 2006 trekken Nederlandse SF door de Baluchivallei en raken diverse malen in gevecht, met de inzet van zwaar kaliber-wapensystemen. U observeert weer: 'hooligans', die 'geen idee hadden wat ze over zich afriepen', losten wat schoten en de Nederlandse commandotroepen vochten overweldigend terug.

Als ik in de Baluchivallei had gewoond, had ik niet anders gereageerd dan de bevolking daar deed tijdens de inval van Nederlandse SF. Als Nederlandse psychologen bij de planning van die actie waren betrokken, hadden zij waarschijnlijk dezelfde conclusies getrokken als ik, en zij hadden die mogelijk in een waarschuwing verpakt. Operatie Perth werd uitgevoerd door een bataljon, de Nederlandse SF-operatie door een kleine eenheid. Voor die kleine eenheid ging niemand in de Baluchivallei op de vlucht en

'Een kinetische actie in de Baluchivallei tegen een niet als zodanig identificeerbare vijand is onmogelijk te rechtvaardigen'

geen bewoner van de Baluchivallei kon weten dat het een SF-eenheid was, met alle moderne middelen om met overweldigend geweld te reageren op ieder (logisch) schot dat de bevolking loste.

U spreekt consequent van oppositie en hooligans, niet van vijand. Hebben politiek en media een verkeerd beeld geschetst van de situatie in Afghanistan, en vanuit welk belang?

De politiek, in het geval van Uruzgan, was er slechts in geïnteresseerd een vlaggetje op de kaart van de wereld te plaatsen. Een vlaggetje dat aangaf dat Nederland militair present was in Afghanistan. De troepen die daadwerkelijk in Uruzgan waren gelegerd, kregen de vrijheid naar eigen goeddunken te handelen. Journalisten, die een en ander hadden moeten bewaken, werden om de tuin geleid. Het boek van journalist Joeri Boom is in dat opzicht verontrustend verhelderend. Maar de pers focpte ook zichzelf door te focussen op de controverse wederopbouw-missie/gevechtmissie.

U benoemt in uw boek niet echt de hoofdbazen van de drugsbendes, maar Amerikanen, Australiërs en Nederlandse commando's vochten reeds ver voor de zomer van 2006 en de aankomst van de TFU ten gunste van bijvoorbeeld oud-gouverneur Jan Mohammed, naar verluidt een grote speler in het lokale drugsnetwerk. Waren het onder meer zijn milities waar u op doelt?

Ik benoem geen hoofdbazen van drugsbendes omdat ik die niet ken en een gedegen structuur van de drugshandel, zoals wij die graag zien, in Afghanistan ook niet bestaat. Het is een drugs-

2 Joeri Boom, *Als een nacht met duizend sterren. Oorlogsjournalistiek in Uruzgan* (Amsterdam, Uitgeverij Podium, 2010).

handel van opportunisten, met uitzondering van de boeren die verantwoordelijk zijn voor de verbouw van het basisproduct. Ook in Nederland is de drugshandel er een van en voor opportunisten: wie vandaag de baas is, kan morgen buitenspel gezet zijn. Het verschil is dat Nederlandse drugshandelaars niet door onze overheid of door een buitenlandse macht worden ondersteund. Daarbij moet worden opgemerkt dat in Uruzgan zelfs mensen werden ondersteund die initieel niets met de drugshandel te maken hadden, maar die de Nederlanders onbewust in het zadel hielpen omdat de verhalen die deze mensen ('dolari') opdisten – half begrepen vanwege de taalbarrière – te makkelijk voor waar werden aangenomen. Militieiders – als de mensen die zich als zodanig presenteerden dat al waren – wilden geld en wapens. Wat zij daar vervolgens mee deden, werd bepaald door opportunisme, niet door de idealen die zij predikten.

Een ander voorbeeld: buitenpost Martello in Noord-Kandahar. U schrijft dat uw compagnie de geschiedenis inging als de eenheid die in september 2006 een Talibanaanval op Martello afsloeg. Maar het was eigenlijk geen aanval van de Taliban?

Ik kreeg tot ongenoegen van de commandant ter plekke de vrijheid er iedere dag op uit te trekken met een groep soldaten. Al de eerste dag kon ik ontkrachten dat een aanval was uitgevoerd vanaf de mij aangewezen locaties. De dagen die volgden vond ik de locaties die gebruikt waren om vuur uit te brengen op Kamp Martello, dat niet was aangevallen, maar beschoten, een groot verschil. De Taliban zou Kamp Martello onder geen beding hebben aangevallen; er was geen motief. Zestig militairen die zich opsluiten in een kamp! Geen Taliban is zo dom die militairen daar niet rustig te laten zitten. Zelfs eer was er

met een aanval op Kamp Martello niet te behalen en vertaald naar Afghaanse normen was er dus geen belang. Kamp Martello vormde geen bedreiging voor de drugshandel of voor Talibanstrijders – als die al in het gebied aanwezig waren geweest – en was dan ook beschoten door hooligans, met precies de reactie waarop zij hoopten: paniek. Er waren overigens weinig Nederlandse militairen in Kamp Martello die mijn mening in dezen niet deelden.

Waren het eigenlijk geen stammengeschillen, zoals ook wel werd gezegd, bijvoorbeeld Popolzai versus Ghilzai, die in Uruzgan speelden?

Uiteraard waren er in Uruzgan stammen-geschillen, maar zoals ik in mijn boek uiteenzet speelden die in het dagelijks leven nauwelijks een rol. 'Dolari' deden desgevraagd graag hun voordeel met die stammengeschillen, maar zolang niemand antwoord kan geven op de vraag wat er in Nederland in het dorp Schubbekutveen zal gebeuren als het CDA ten opzichte van de VVD twee zetels wint in het college van burgemeesters en wethouders heeft het geen zin ons te verdiepen in de stammenverhoudingen in Uruzgan. In een situatie zoals in Uruzgan is er maar één ding om voor op te passen: is er een gebied, onder invloed van een bepaalde stam of niet, waar het opleidingsniveau van mensen hoger ligt dan in andere gebieden? De mensen in zo'n gebied spreken doorgaans beter Engels en kunnen beter met buitenlandse troepen communiceren, maar mogen om die reden niet omarmd worden, moeten juist enigszins gewantwoord worden.

U zegt dat we ons hebben gemengd in een insurgency, met een niet goed onderbouwd plan om als 'zendelingen' via wederopbouw en een *hearts and minds*-campagne democratie te brengen, waar in Afghanistan geen behoefte aan is. Als de 'inktvlekstrategie' niet werkte, hoe hadden we het dan moeten aanpakken?

Iemand – een natie – die Afghanistan wil democratiseren, moet er mijns inziens weg-blijven. Daarnaast was het management van de Nederlandse krijgsmacht in 2006 niet in staat

'Ik kreeg tot ongenoegen van de commandant ter plekke de vrijheid er iedere dag op uit te trekken met een groep soldaten'

een missie zoals in Uruzgan tot een goed einde te brengen en het bewijs daarvan is geleverd. Er was in het geheel geen plan van aanpak en om eerlijk te zijn was dat ook niet per se noodzakelijk. De Nederlandse krijgsmacht had wel moeten weten hoe op te treden in een gebied zoals Uruzgan om het ingraven van IED's en het afschieten van 107-millimetteraketten te voorkomen en om het vertrouwen van de bevolking te winnen: met kleine, zich snel verplaatsende eenheden waarvan de leden links, rechts, overal en vooral onvoorspelbaar hun lachende gezichten laten zien. De krijgsmacht had de flexibiliteit moeten hebben om snel van strategie te wijzigen. Dat was onmogelijk omdat er boven de battlegroups een waterhoofd aan management hing dat te kort diende in Uruzgan om een idee te hebben of te ontwikkelen van wat daar gebeurde. Een man zoals bijvoorbeeld [commandant van de eerste Battlegroup] Piet van der Sar, samen met zijn staf, vormde genoeg management om zekere doelen te bereiken in Uruzgan. De staf van het 12e bataljon had ten minste een jaar in Uruzgan moeten blijven en had deel voor deel moeten worden afgelost.

Het verkeerde vijandbeeld heeft uiteindelijk veel Afghanen het leven gekost, zegt u. Neem bijvoorbeeld wat u het 'spotterdrama' noemt. Wat was dat?

Het spotterdrama beschrijf ik pas in het vervolg op *Onvoorspelbaar verleden*, maar het was gebaseerd op een interessante, voor Afghanen levensgevaarlijke, blinde vlek in de Nederlandse communicatie. Voor het bestempelen van een Afghaan als spotter golden strakke regels. Eenheden te velde noemden iedere Afghaan met een walkietalkie of een radiootje die ze waarnamen een spotter. Via de radio werd de ops om toestemming gevraagd voor het bevuren van de waargenomen spotter. De legad, die daarover zijn veto uitsprak, ging er in vrijwel alle gevallen waarvan ik getuige was vanuit dat de commandanten van eenheden te velde de regels aanhielden voor het aanmerken van een Afghaan als spotter en gaf daarom het advies 'vuren-vrij', zonder te controleren of de te bevuren Afghaan werkelijk aan alle 'spottereisen' voldeed. En die eisen gaan zover dat vrijwel niemand in Uruzgan werkelijk als spotter kon worden aangemerkt.

FOB Martello

FOTO BEELDBANK NIMH (AVDD, PAUL VERHEUL)



U zegt dat u kon ‘leven in de hoofden van de oppositie’ en hebt scherpe kritiek op inlichtingenanalisten van de MIVD, die zouden hebben meegeholpen aan het creëren van een irreëel vijandbeeld. U vindt dat er van tevoren te weinig studie gemaakt is van de politieke, culturele en economische situatie in Uruzgan, waardoor de werkelijke situatie niet in rapporten belandde. Of was die informatie er wel, maar is die genegeerd?

Het was niet nodig van te voren studie te maken van de politieke en algehele situatie in Uruzgan. Nederlanders hadden met vragen de provincie in moeten trekken, niet met antwoorden. Die antwoorden werden ook nog ingegeven door inlichtingenanalisten die van toeten nog blazen wisten, te jong en onervaren waren en zich lieten leiden door wat zij als logisch veronderstelden. Een inlichtingenofficier – ik ben daarin duidelijk in mijn boek – die zich wil indekken voor iedere calamiteit die zich in een inzetgebied kan voltrekken, is geen knip voor zijn neus waard en maakt dat de troepen bang voor hun eigen schaduw het voorterrein in trekken. Dat was precies wat er in Uruzgan gebeurde, met alle gevolgen van dien. ‘Ik weet het niet’, was op veel vragen een goed antwoord geweest. Het was echter een antwoord dat geen medewerker van de MIVD die ik ken ooit durfde geven. Individuele soldaten waren beter in staat een beeld van de situatie in Uruzgan aan hun meerderen door te geven. Als slechts hun ervaringen hadden geteld in Uruzgan en als zij, zoals ik, de vrijheid hadden gehad om die ervaringen onbevekt op te doen, dan had de missie een ander verloop gekregen.

In het late voorjaar van 2007 is er de Slag om Chora. Ook dat was geen Talibanoffensief?

Zoals ik in mijn boek duidelijk stel had de Taliban – als die al bestond in Uruzgan – geen enkele aanleiding voor een offensief tegen Nederlandse troepen in Chora. Voor geen enkele gewapende macht bestond een dergelijk motief. Motieven voor beschietingen van politiestations waren er te over (drugsgelateerd), maar geen Afghaan, wat zijn affiliatie ook was, zou een

offensief hebben overwogen. De Slag om Chora had voorkomen kunnen worden en had voorkomen moeten worden, maar dat was lastig omdat de hoogste bevelvoerders een vijand, van wie het bestaan niet bewezen kon worden, insignificant wilden maken.

In een verklaring van 14 juli 2020 noemt de NAVO het huidige geweld in Afghanistan – ‘driven especially by Taliban attacks against Afghan National Defense and Security Forces’ – onacceptabel en zegt de missie Resolute Support te zullen voortzetten. Gaat de NAVO ten onrechte nog steeds uit van de Taliban als vijand, of is de situatie in Afghanistan intussen toch veranderd?

Het is tot op de dag van vandaag onduidelijk wie of wat de Taliban is en het is onverstandig voor een aanpak in Afghanistan te kiezen gebaseerd op de aanwezigheid van een organisatie die zich Taliban noemt. Afghanistan is een land dat draait op opportunisme en dat de grootste exporteur van opium van de wereld is. Met die laatste twee zaken als uitgangspunt kan worden gezocht naar een manier het land te stabiliseren, waarbij de hoofdvraag luidt: moet een buitenlandse mogendheid zorgdragen voor stabilisatie in Afghanistan of zorgt de aanwezigheid van buitenlandse troepen in Afghanistan al bijna twintig jaar voor destabilisatie? Wat ‘acceptabele vrede’ in de ogen van de bevolking van Afghanistan is lijkt mij een vraag waarop een antwoord moet komen voordat buitenlandse militairen nog een stap zetten in Afghanistan. Het probleem is dat de belangen van landen die zich mengen in het realiseren van vrede in Afghanistan uiteenlopen en weinig te maken hebben met de belangen van de bevolking daar. De Nederlandse wederopbouwmissie in Uruzgan is daarvan een goed voorbeeld. Nederland deed mee! Waaraan wist niemand.

U ging in 2007 terug voor een tweede periode bij de TFU?

Ja, daarover vertel ik in het vervolg op *Onvoorspelbaar verleden*, waarvan het manuscript zo goed als voltooid is. ■



FOTO BEELDBANK NIMH

Militairen van het Regiment Geneeskundige Troepen op oefening tijdens de mobilisatie van 1914-1918

Pandemieën en ‘een miniatuur stukje land als het onze’

In een onderzoek uit 1931 naar de militair-hygiënische dienst tijdens de mobilisatie van 1914-1918 beschrijven J.P. Bijl en H. Peeters in de *Militaire Spectator* de werkwijze van die dienst bij een aantal infectieziekten, uiteenlopend van tyfus tot geslachtsziekten.¹ Die laatste zijn niet direct besmettelijk, maar wanneer militairen dezelfde etablissementen frequenteren kan het hard gaan: ‘Bijzondere moeilijkheden brengt de bestrijding van geslachtsziekten met zich. De wijze, waarop de besmetting tot stand komt, maakt het toch uiterst moeilijk om, zoals bij andere infectieziekten, de bron van besmetting op te sporen. Door het plaatsen van wachten bij bordeelen kon men soms eenigszins in die richting werkzaam zijn. Een enkele maal was bekend, welke vrouw besmetting veroorzaakte. Zij werd dan zoo mogelijk overtuigd van de noodzakelijkheid zich te laten behandelen of kreeg soms een post voor de deur.’

Een ander, veel dodelijker fenomeen uit die tijd is de mondiale pandemie van de Spaanse griep.

‘Men zal niet kunnen spreken over de infectieziekten, die tijdens de mobilisatie zijn voorgekomen, zonder te denken aan de hevige epidemie van *Spaansche griep*, die in de 2e helft van 1918 heeft geheerscht.’

Toch besteden de auteurs vrij weinig aandacht aan deze griepepidemie, die wereldwijd miljoenen levens heeft gekost, vooral uit onmacht tegenover dit virus: ‘Het aandeel, dat den militair-hygiënischen dienst wordt toegeschreven bij de verspreiding van de *griep*, behoeft nauwelijks besproken te worden. Zelfs de grootste hygiënist zou niet in staat zijn geweest bij een pandemie, die alle werelddelen teisterde, een miniatuur stukje land als het onze vrij te houden.’ ■

¹ J.P. Bijl en H. Peeters, ‘De militair-hygiënische dienst tijdens de mobilisatie’, in: *Militaire Spectator* 100 (1931) (2) 76-95. Zie: <https://www.militairespectator.nl/sites/default/files/bestanden/uitgaven/1931/1931-0076-01-0015.PDF>.

Blind en doof

Linda Polman

Welke koers de EU ging varen wisten we toen de voorzitter van de Europese Commissie, Ursula von der Leyen, bekendmaakte dat de EU zich voornam om de 'European way of life' nog beter te beschermen tegen migranten. Dat was in juli 2019. Sinds die dag hebben we de Europese grensbewakingsorganisatie Frontex zien transformeren tot een *lean and mean* deportatiemachine. Frontex moet voortaan 50.000 migranten en afgewezen asielzoekers per jaar Europa gaan uitzetten. Over dat aantal deden ze pré-Ursula von der Leyen tien jaar.

Volgens de EU is migratie vooral een veiligheidsprobleem. Mensen die naar Europa komen omdat ze vluchten voor oorlog, onderdrukking of armoede worden in de eerste plaats gezien en behandeld als een gevaar voor de Europese veiligheid, onze normen en waarden en – sinds corona – voor de Europese volksgezondheid. De EU is al jaren niet af te brengen van het idee dat we met deportatie en het militariseren van grensbewaking het gevaar moeten bestrijden.

De Europese militaire en veiligheidsindustrie heeft hard gewerkt om dit discours ingang in Brussel te doen krijgen. Wapenfabrikanten smeedden een innige band met Europese beleidsmakers. Ze maken deel uit van de officiële Europese adviesorganen en verkeren in voortdurend overleg met de Europese Commissie en met Frontex. Hun voorstellen worden soms letterlijk overgenomen in EU-beleid en ze kookten vanaf 2015 ook de forse uitbreiding van Frontex voor: de grensbewakers krijgen er duizenden dag en nacht in te zetten Europese militairen en grensbewakers bij en bevoegdheden om eigen satellieten, sensoren, drones, schepen en voertuigen aan te schaffen.

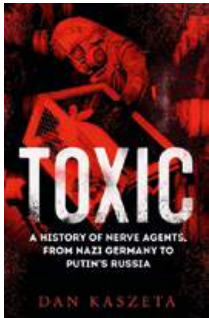
Net als (bijna) alle andere EU-lidstaten doet Nederland mee aan Frontex-grensoperaties. Marechaussee, de nationale politie en Nederlandse patrouillevoertuigen en kustwachtvliegtuigen gingen al op patrouille. In maart dit jaar trad Nederland nog aan bij de Griekse grens met Turkije. De Turkse president Erdogan dreigde de slagbomen voor vluchtelingen omhoog te klappen; 35.000 Syriërs en Afghanen verzamelden zich ervoor. Griekse kogels en rookbommen en Frontex-personeel uit heel Europa hielden de 'vluchtelingeninvasie' tegen. Onder de vluchtelingen vielen ten minste drie doden.

Frontex ligt onder vuur van mensenrechtenorganisaties. Onder de ogen van Frontex-manscapen zouden migranten en vluchtelingen bij de Kroatische grens in elkaar worden getimmerd en in Griekenland worden in het bijzijn van Frontex elk jaar honderden, misschien duizenden mensen zonder de kans te hebben gekregen asiel aan te vragen over de grens gezet, vaak met gebruik van geweld en beroofd van hun bezittingen. En Frontex assisteert bij het onderschepen en terugzenden van vluchtelingen uit Libië. Intussen drijft het mandaat van Frontex steeds verder uit, van controle van Europa's buitengrenzen naar controle op migratiebewegingen tussen EU-lidstaten. Meer mensen worden gearresteerd, gedetineerd en uitgezet voordat ze asiel kunnen aanvragen. Maar terwijl Frontex steeds meer mag, staat het geen externe controle toe: Frontex controleert zélf of het de Europese mensenrechtenwetten respecteert. Uit die interne onderzoeken blijkt dat Frontex puik werk levert, omdat er geen bewijzen zijn dat Frontex dat níét doet.

Op tv zien we met eigen ogen beelden van vluchtelingen die door Griekse autoriteiten op onbestuurbare rubbervlootten retour naar Turkije worden geduwd zonder een asielaanvraag te hebben kunnen doen. Dat druist in tegen Europese mensenrechten, maar Frontex ziet geen kwaad en hoort geen kwaad en de EU-lidstaten spreken er geen kwaad van, ook al weet iedereen dat het Europese mensenrechtenbeleid steeds verder ontspoot. ■



SIGNALERINGEN



Toxic

A History of Nerve Agents, From Nazi Germany to Putin's Russia
Door Dan Kaszeta
Londen (Hurst) 2020
408 blz.
ISBN 9781787383067
€ 28,-

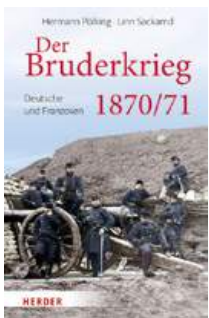
Na de Eerste Wereldoorlog waren militaire denkers overtuigd dat zenuwgas onvoorspelbare aantallen slachtoffers in de eigen rangen aanrichtte en geen beslissend middel was om veldslagen mee te winnen. Maar door de vooruitgang die Duitse onderzoekers in de Tweede Wereldoorlog boekten konden latere regimes strijdgassen gericht inzetten, zegt journalist Dan Kaszeta in *Toxic*. Kaszeta gaat onder meer in op de Iran-Irakoorlog van de jaren tachtig en de oorlog in Syrië. Hij behandelt tevens de inzet van zenuwgas door niet-staatelijke actoren, zoals de Aum Shinrikyo-sekte in Japan, en het gebruik van gas als middel om politieke tegenstanders uit de weg te ruimen door Rusland.



De oorlog tegemoet

Nederlanders en de strijd om Spanje (1936-1939)
Lodewijk Petram en Samuël Kruizinga
Amsterdam (Atlas Contact) 2020
240 blz.
ISBN 9789045032559
€ 22,99

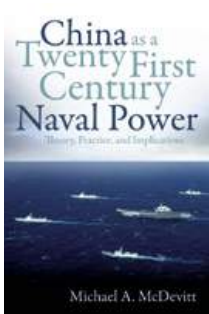
In *De oorlog tegemoet* volgen Lodewijk Petram en Samuël Kruizinga Nederlanders die in de Spaanse Burgeroorlog (1936-1939) meevochten aan de kant van de Republikeinen tegen de Nationalisten van Franco. De auteurs gaan via archieven op zoek naar beweegredenen van deze vrijwilligers en schetsen de discussie die destijds in Nederland woedde en waarin de strijders werden afgeschilderd als communisten die zich mengden in een buitenlands conflict met de bedoeling een Stalin-getrouwe regering aan de macht te helpen. Naast ideologie en motieven komen gevechten aan bod waarbij Nederlandse Spanjegangers betrokken waren en is er aandacht voor wat er van sommigen van hen werd na de oorlog.



Der Bruderkrieg

Deutsche und Franzosen 1870/71
Door Hermann Pölking-Eiken en Linn Sackarnd
Freiburg (Verlag Herder) 2020
688 blz.
ISBN 9783451384561
€ 38,-

De Duits-Franse Oorlog van 1870-71 is een van de belangrijkste gebeurtenissen in de Europese geschiedenis, die onder meer door te weinig aandacht in het onderwijs uit het collectieve geheugen verdwenen is. Dat concluderen Hermann Pölking-Eiken en Linn Sackarnd in *Der Bruderkrieg*. In het boek komen de verschillen tussen de Franse en Duitse cultuur aan bod, de rol van Pruisen in de militaire krachtsverhoudingen en verschillende veldslagen. Uiteindelijk volgde na de Franse nederlaag het uitroepen van het Duitse keizerrijk. Pölking en Sackarnd verrichtten archiefonderzoek en gebruiken ook egodocumenten van officieren, manschappen, politici en burgers om een breed beeld te schilderen.



China as a Twenty-First-Century Naval Power

Theory, Practice, and Implications
Door Michael McDevitt
Annapolis (U.S. Naval Institute) 2020
320 blz.
ISBN 9781682475355
€ 35,-

De Chinese president Xi Jinping heeft duidelijke ambities voor uitbreiding en versterking van de strijdkrachten en de marine lijkt in ieder geval op weg de gestelde doelen te halen. Dat zegt schout-bij-nacht b.d. Michael McDevitt in *China as a Twenty-First-Century Naval Power*. McDevitt legt Xi's strategische visie uit en wijst op de afhankelijkheid van China van de buitenlandse handel, die grotendeels over zee gaat. Daarnaast heeft China met het Belt and Road-initiatief veel belangen in het buitenland gekregen en die moeten veiliggesteld worden, waarbij een *blue water navy* kan helpen, ook verder weg dan de Zuid-Chinese Zee en de Indische Oceaan.

