Denkwürdigkeiten

Journal der Politisch-Militärischen Gesellschaft

Nr. 114
Dezember 2019

Herausgegeben vom Vorstand der Politisch-Militärischen Gesellschaft e.V. (pmg) in Berlin

ISSN 1436-3070

LEADOFF

Liebe Mitglieder,

Die Hoffnung auf globalen Frieden steht traditionell im Mittelpunkt von Weihnachtsbotschaften. Frieden wollen ist wichtig. Doch man wird den Frieden kaum bewahren können, wenn man nicht bereit ist, ihn auch zu schützen. Hierauf zielt der bekannte lateinische Spruch: „Si vis pacem, para bellum“, auf deutsch: „Wenn Du den Frieden willst, bereite den Krieg vor.“ Oder etwas weniger zugespitzt: „Wenn Du den Frieden willst, musst Du Angriffe auf Dich und die Deinen abwehren können.“

Vor wenigen Tagen überraschte in Berlin der vormalige Inspekteur der japanischen Marine Admiral Tomohisa Takei die Zuhörer seines Vortrags *Reexamining National Security Policies in the New Era of Competing Great Powers* mit der Feststellung, dass wir uns derzeit in einer Zwischen-Kriegsphase befinden.

Tatsächlich spricht viel dafür, dass großmächtige, aber auch kleinere und ebenso irreguläre und privatwirtschaftliche Akteure derzeit ausloten, welches Maß an Angriffen auf etablierte Strukturen, Wirtschaften und Gesellschaften unterhalb der Schwelle des offenen Krieges möglich sind.

Admiral Takei argumentierte, dass eine neue Ära konkurrierender Großmächte begonnen hat, die seiner Ansicht nach das Ende der 28 Jahre dauernden Ära nach dem Kalten Krieg markiert. Hieraus resultieren nach seiner Auffassung Anforderungen an demokratische Staaten, die nur durch eine Überprüfung ihrer aktuellen Sicherheitspolitik in den Bereichen Diplomatie, Wirtschaft, innere und äußere Sicherheit möglichen Kriegsrisiken wirksam begegnen können.

Wir haben letzteren Aspekt in den vergangenen beiden Mitgliederveranstaltungen der pmg intensiv diskutiert. Diese Denkwürdigkeiten zeigen u.a. am Beispiel der Ardennenoffensive vor 75 Jahren, wie wichtig es ist Frieden zu schützen und warum Frieden auch heute engagierten Schutz braucht.

Der Vorstand der Politisch-Militärischen Gesellschaft wünscht Ihnen ein frohes Weihnachtsfest und ein gesundes, erfolgreiches Neues Jahr

Ralph Thiele, Vorstandsvorsitzender

In dieser Ausgabe

THEMEN

75 Jahre Ardennenoffensive 1944/45 der Wehrmacht

Der Albtraum des Großherzogtums Luxemburg

Am 16. Dezember 2019 gedenken allen voran Luxemburger, Belgier und Amerikaner den Beginn der Ardennenoffensive der Wehrmacht vor 75 Jahren. Dazu haben der König der Belgier und der Großherzog Luxemburgs die Staatsoberhäupter der beteiligten Länder ins ostbelgische Bastogne und auf den amerikanischen Soldatenfriedhof in Luxemburg-Hamm eingeladen. Aus den USA wird eine große Delegation aus Regierungsvertretern, Militär und Kongressmitgliedern erwartet. Aus Deutschland werden Bundespräsident Frank-Walter Steinmeier und sein Vorgänger Joachim Gauck teilnehmen.

Am 10. Mai 1940 überfiel Nazi-Deutschland das neutrale Luxemburg, hielt es bis September 1944 besetzt und gliederte es unter Gauleiter Simon zusammen mit Trier und Koblenz in den Gau Moselland ein.

Nach der erfolgreichen Landung in der Normandie am D-Day (6. Juni 1944) erreichten amerikanische Truppen am 9. September 1944 Petingen in Luxemburg. Sie stießen hier und auch in den folgenden Tagen nur auf vereinzelten Widerstand kleinerer deutscher Einheiten. Die deutsche Zivilverwaltung hatte sich bereits vor der sich hinter dem Westwall[1] zurückziehenden Wehrmacht das Großherzogtum verlassen.

Am 11. September war Luxemburg weitgehend befreit und bei Stolzenburg betraten erstmals amerikanische Soldaten deutschen Boden. Am 14. September 1944 überwand eine US-Panzereinheit den Westwall bei Wallendorf und stand schon zwei Tage später nur noch acht Kilometer vor Bitburg. Als die Deutschen Truppen aus der ganzen Region heranführten, um diesen Einbruch zurückzuschlagen, erhielt die US-Einheit den Befehl den verlustreichen Vorstoß zu beenden und sich hinter Sauer und Our zurückzuziehen.[2]

Die überwältigende Mehrheit der Luxemburger begrüßte die amerikanischen Befreier auf das Herzlichste und mit ihnen Prinz Félix und Erbgroßherzog Jean, die zusammen mit den US-Truppen in der Hauptstadt eintrafen.

Mit den US-Soldaten kamen auch amerikanische Zivilisten nach Luxemburg wie Ernest Hemingway und Marlene Dietrich. Nach Auftritten vor amerikanischen Truppen in Frankreich trat sie auch vor US-Soldaten und Offizieren in Luxemburg auf und dinierte mit General Bradley, dem Befehlshaber der 900.000 Mann starken 12. US-Heeresgruppe in seinem Hauptquartier im Hotel Alfa in Luxemburg-Stadt.[3]

Ein Höhepunkt der Feiern war Thanksgiving, das amerikanische Erntedankfest, an dem US-Einheiten ihre mitgebrachten Truthähne mit dankbaren Luxemburgern teilten. Doch die wiedergewonnene Freiheit sollte für viele Luxemburger leider nur von kurzer Dauer sein.

Am 16. Dezember 1944 griff Nazi-Deutschland mit drei Armeen und den letzten Reserven an Kriegsmaterial unter dem Codenamen „Wacht am Rhein“[4] die US-Streitkräfte in Luxemburg und Belgien an und überraschte damit die Amerikaner, die keinen Angriff in den Ardennen erwarteten. „*Die Alliierten sonnten sich in kaum zu überbietender Siegeseuphorie*“.[5] Hitler persönlich hatte diesen in Luxemburg „Rundstedt-Offensive“[6] genannten letzten großen Angriff befohlen, für den alle verfügbaren Reserven und modernes Kriegsmaterial (u.a. die berüchtigten „Königstiger“-Panzer) der Wehrmacht und der Waffen-SS zwischen Bonn und Trier zusammengezogen wurden.

Auf einem schmalen Angriffsstreifen von 130 Kilometern standen 17 deutsche Divisionen mit über ca. 200.000 Soldaten (darunter allerdings viele 16- bis 18- und über 60-Jährige) mit ca. 600 Panzern und Sturmgeschützen nur ca. 83.000 US-Soldaten gegenüber.

Nazi-Deutschland setzte damit alles auf eine letzte Karte. Das Ziel war die Eroberung des alliierten Nachschubhafens Antwerpen, über den inzwischen ein Drittel des gesamten alliierten Nachschubs lief, womit auch gleichzeitig sowohl ein militärischer als auch politischer Keil zwischen die nördlich davon operierenden britischen und kanadischen Truppen, und den amerikanischen Streitkräften südlich davon getrieben werden sollte. Dabei dürfte Hitler die Operationspläne von 1940 vor Augen gehabt haben, als die deutschen Truppen in hohem Tempo durch Belgien und Luxemburg bis zur französischen Kanalküste bei Abbéville vorstießen, um Briten und Franzosen in Dünkirchen einzuschließen.[7] Doch die Ausgangslage war kaum vergleichbar. Im Gegensatz zu 1940 besaßen die Alliierten die Luftherrschaft und auf der deutschen Seite herrschte akuter Treibstoffmangel – nur für die ersten 60 der insgesamt über 200 Kilometer bis Antwerpen reichte der Treibstoff. Zudem waren die Eliteeinheiten (in der Normandieschlacht) abgekämpft und die neu aufgestellten Truppenteile schlecht ausgebildet. Doch Hitler setzte sich über die Bedenken seiner Generäle hinweg[8] und als Mitte Dezember dichter Nebel einsetzte und die alliierte Luftwaffe zwang am Boden zu bleiben, war am 16.12.1944 der Zeitpunkt für den Angriff gekommen.

Mit einem Trommelfeuer aus ca. 3.400 Artilleriegeschützen zwi-

[1] Von den Alliierten in Anlehnung an eine deutsche Abwehrstellung an der Westfront im Ersten Weltkrieg „Siegfried Line“ genannt.

[2] General Eisenhower hatte als Oberkommandierender der alliierten Streitkräfte in Europa entschieden, den größten Teil des Nachschubs dem britischen Generalfeldmarschall Montgomery für seine Luftlandeoperation „Market Garden“ am 17. September 1944 bei Arnheim und seinen Vormarsch durch den Süden Hollands zur Verfügung zu stellen. Montgomery wollte mit einem Überraschungsangriff über Maas, Waal und Niederrhein Richtung Ruhrgebiet vorstoßen. Die entscheidende Brücke von Arnheim konnte er aber nicht nehmen und die Stadt blieb in deutscher Hand. Der schnelle Vormarsch der Alliierten durch Ostfrankreich hatte zudem wachsende Engpässe beim Nachschub zur Folge, so dass der Vorstoß in Richtung Mittelrhein bis März 1945 warten musste.

[3] Einer ihrer größten Bewunderer war General Patton, der ihr ein paar Pistolen mit Perlmuttgriff schenkte.

[4] Später erhielt die Operation den Namen „Herbstnebel“.

[5] Antony Beevor, Die Ardennenoffensive 1944. Hitlers letzte Schlacht im Westen ((Originaltitel: Ardennes 1944. Hitler´s Last Gamble, London 2015), C. Bertelsmann, München 2016, S. 11.

[6] Auch die Amerikaner sprachen zunächst von „Rundstedt-Offensive“, was den betagten Generalfeldmarschall irritierte, da die Offensive nicht sein Plan war und er sogar erst spät darüber informiert worden war. Rundstedt (und Model) erhielten die ausdrückliche Weisung, dass ihre Aufgabe nur darin bestehe, die Befehle der OKW an die unterstellten Einheiten weiterzuleiten.

[7] Hitler glaubte mit zwei Panzerarmeen die Westalliierten auseinanderdividieren zu können, die Kanadier aus dem Krieg zu drängen und den Briten vielleicht sogar ein neues „Dünkirchen“ zu bereiten. Auch sollte dadurch die Bedrohung der Rüstungsindustrie im Ruhrgebiet abgewendet werden.

[8] Als Hitler am 16. September aus dem täglichen Lageberichts General Jodls erfuhr, dass die zuvor stark bedrängten deutschen Truppen in der Eifel eine Verschnaufpause erhalten hatten und rund 100 Kilometer Front in den Ardennen nur von vier amerikanischen Divisionen gehalten würden, stand sein Entschluss fest im Westen zum Gegenangriff überzugehen, um durch die Ardennen über die Maas nach Antwerpen vorzustoßen.

schen Monschau und Echternach an jenem Samstagmorgen vor dem vierten Advent gegen 5:30 Uhr wurde das Vorrücken der 6. SS- und der 5. Panzerarmee gegen 7:00 Uhr vorbereitet. Weiter südlich hatte die 7. Armee den Auftrag, die Flanke zu schützen. Generaloberst Jodl hatte Hitler allerdings überzeugen können, die Stadt Luxemburg nicht ebenfalls als Ziel der „Operation Herbstnebel“ anzugreifen.

Nach dem Trommelfeuer blieb allerdings schon der erste Angriff der 6. SS-Panzerarmee unter SS-Oberstgruppenführer Dietrich, die als stärkste der drei Armeen der Heeresgruppe B im Norden den Hauptstoß führen sollte, rasch stecken. Die US-Truppen im Nordteil des Operationsgebietes leisteten deutlich länger Widerstand als erwartet. Frühzeitig mussten Reserven herangeführt werden, um das Momentum nicht zu verlieren. Ein Luftlandeunternehmen mit ca. 1200 Fallschirmjägern im Rücken des Gegners bei Eupen scheiterte völlig.

Weiter südlich im Abschnitt Dasburg-Gemünd setzten die 2. Panzerdivision, die 26. Volksgrenadierdivision (26.VGD) und die Panzer-Lehr-Division (PLD) der 5. Panzer-Armee unter General von Manteuffel über die Our, allerdings deutlich langsamer als geplant, was vor allem den schwierigen Anfahrten und den Wasser – und Uferverhältnissen geschuldet war.[9] Aber auch innerhalb Luxemburgs verlief der Vormarsch in Richtung Bastogne deutlich langsamer als erwartet. Die Invasoren trafen im Großherzogtum auf die Soldaten des 110. Regiments der 28. US-Infanteriedivision[10], die sich in ihren Orten einigelten und diese bis zum 18. Dezember 1944 tapfer verteidigten, ehe sie der deutschen Übermacht weichen mussten.[11] Die heftige Gegenwehr mehrerer US-Einheiten – Hemingway war als Zeitzeuge dabei[12] – und das nur langsame Vorankommen der deutschen Panzerverbände aufgrund des aufgeweichten Bodens führte dazu, dass die Amerikaner Zeit hatten, mehrere Einheiten am strategisch wichtigen Verkehrsknotenpunkt Bastogne zusammenzuziehen und so den Verteidigungsring um Bastogne zu schließen bevor die Spitzen der deutschen Angreifer am frühen Morgen des 19. Dezember 1944 den belgischen Grenzort von Norden und von Süden erreichten.

Bastogne war zwar nunmehr von deutschen Truppen umzingelt, denen es aber nicht gelang die Stadt einzunehmen. Die Aufforderung zur Kapitulation durch General Lüttwitz wurde am 22. Dezember 1944 von dem Befehlshaber der 101-US Luftlandedivision, Brigadegeneral Anthony C. McAuliffe, der die Verteidigung von Bastogne leitete, mit dem legendären „Nuts!“ (Unsinn) zurückgewiesen. Die Aufforderung zur Kapitulation war kaum mehr als ein Bluff, da die deutschen Kräfte für eine Einnahme der Stadt nicht ausreichten.[13]

Am 23. Dezember 1944 standen die Spitzen der 2. Deutschen Panzerdivision[14] aber immerhin sechs Kilometer vor Dinant kurz vor der Maas – doch weiter sollten die Deutschen nicht mehr vordringen was vor allem an den fehlenden Treibstoffvorräten lag.

Nördlich von Bastogne wurden die deutschen Einheiten in heftige Kämpfe verwickelt, an denen auch der 21-jährige Henry Kissinger als Mitglied einer Aufklärungseinheit teilnahm.

Am 23. Dezember 1944 klarte zudem das Wetter auf und die Alliierten konnten nun mit ihren Jagdbombern die deutschen Verbände angreifen.[15]

Bereits am 24. Dezember 1944 erkannte Generalfeldmarschall von Rundstedt, dass die Ardennenoffensive gescheitert war, doch Hitler befahl eine Fortsetzung der Kämpfe, die sich nunmehr auf die Eroberung Bastognes konzentrierten.

Im Süden gelang es General Patten, der in Lothringen einen Angriff auf das Saargebiet und Richtung Rhein vorbereitete, seine dritte Armee binnen 48 Stunden um 90 Grad zu drehen, um sie nach Luxemburg und Ostbelgien in Marsch zu setzen. Über Arlon stieß er mit seiner 4. Panzerdivision Richtung Bastogne vor, die am 26. Dezember 1944 gemeinsam mit den Verteidigern der Stadt den deutschen Belagerungsring sprengen konnte. Seine 26. Panzerdivision stieß gleichzeitig in Richtung Wiltz und die 80. US-Panzerdivision in Richtung Ettelbrück vor.

Nach dem Durchbruch Pattons durch den deutschen Belagerungsring befahl von Rundstedt das sofortige Heranführen aller Reserven, doch der Ring konnte nicht wieder geschlossen werden, ganz zu schweigen die Eroberung der Stadt, wie von Hitler ausdrücklich befohlen.

---

[9] Da die Brücke in Gmünd erst am späten Abend fertig wurde, wurde ein Teil der PLD über die Brücke bei Dasburg geleitet, was dort einen gewaltigen Stau verursachte, so dass von Manteuffel sich gezwungen sah, höchstpersönlich den Verkehr zu regeln.

[10] Die 28. Infanteriedivision hatte zuvor im Hürtgenwald beim erfolglosen Vorstoß zur Rur in Richtung Rhein schwere Verluste erlitten und über 5.600 Mann verloren. Insgesamt verlor die US-Army in diesem Feldzug von 120.000 Beteiligten 33.000 Mann. Die 4. und die 28. Infanteriedivision wurden danach zur Erholung in die südlichen Ardennen geschickt, in die „Luxemburgische Schweiz“, „ein ruhiges Paradies für müde Soldaten“.

[11] Die 28. US-Division kämpfte weiter auch als ihr Frontabschnitt längs der „Skyline-Drive“ genannten Straße durchbrochen war. Am Ende des ersten Tages hatte die deutsche 5. Panzerarmee keines ihrer gesetzten Ziele erreicht. Die hartnäckige Verteidigung von Hosingen hielt bis zum späten Vormittag des zweiten Tages an. Auch in Heinerscheid und Marnach verteidigten einzelne US-Kompagnien wichtige Straßenkreuzungen, die den ganzen Vorstoß um entscheidende anderthalb Trage verzögerte. (Vgl. Beevor, S. 138).

[12] Ernest Hemingway war offiziell als Frontberichterstatter bei der US-Army akkreditiert, aber bei vielen Offizieren als Fronttourist verschrien. Er wollte natürlich die große Schlacht nicht verpassen und traf am 17.12. 44 mit Fieber aus Paris kommend in einem Privatkonvoi in der Stadt Luxemburg ein, von wo aus er sich direkt nach Rodenburg zum Befehlsstand der 22. US-Infanterieregiments begab. Am 22.12. beobachtete er von den Höhen bei Breitweiler in der Nähe von Condorf den Kampf der US-Armee, die dort trotz hoher Verluste den Durchbruch der Wehrmacht verhinderte. In Dickweiler geriet er selbst unter Beschuss, dem er nur mit knapper Not entkam. Sein zynischer und zugleich schonungsloser Artikel über die Kämpfe in Echternach, Berdorf, Lantenborn, Osweiler und Dickweiler erschien im Januar 1945 in „Time & Life“.

[13] Beevor, S. 252.

[14] In der 2. deutschen Panzerdivision kämpften auch zwangsrekrutierte Elsässer und Luxemburger, von den sich die meisten bei erster Gelegenheit den Amerikanern ergaben. (Beevor, S. 301).

[15] Angriffe wurden auch auf Trier und dessen Rangierbahnhof geflogen.

General Patton besuchte an diesem Heiligabend die Kirche in Luxemburg-Stadt, wo er auf der Bank Platz nahm, von der aus Kaiser Wilhelm II während seines Luxemburgaufenthalts während des 1. Weltkriegs den Gottesdienst verfolgt hatte.

Südöstlich von Bastogne kam es ab dem 27. Dezember zu den „*wohl mörderischsten und verlustreichsten Kämpfe der Ardennenoffensive auf Luxemburger Boden*“[16] am Schumanns Eck, einem Verkehrsknotenpunkt in der Nähe von Wiltz, der Luxemburger Gemeinde, die am heftigsten unter der Ardennenschlacht zu leiden hatte.[17] Bis zum 10. Januar 1945, als große Teile der 5. Deutschen Fallschirmjägerdivision der deutschen 7. Armee eingeschlossen wurden und in Gefangenschaft gerieten, waren allein in diesem Abschnitt mehrere tausend Soldaten gefallen oder verwundet worden. Bei seiner etwas vollmundigen Ankündigung gegenüber Bradley „*Der Kraut hat seinen Kopf in den Fleischwolf gesteckt, und ich halte die Kurbel in der Hand*“, hatte Patton das Wetter, das Gelände und den entschlossenen Widerstand unterschätzt, den die Einheiten der deutschen 7. Armee bei der Verteidigung der Südflanke des Frontbogens leisteten. Er hatte die Stärke des deutschen Gegners unter- und die eigene überschätzt.[18]

Am 16. Januar 1945, genau einen Monat nach Beginn des deutschen Angriffs gelang es den amerikanischen Verbänden den deutschen Frontbogen, den Churchill später „the bulge“ (Beule, Ausbuchtung) nannte, abzuschneiden. Deshalb ging die Ardennenschlacht im englischsprachigen Raum als „Battle of the Bulge“ in die Geschichtsbücher ein.

Am 18. Januar 1945 griff General Patton die Deutschen an der Sauer von Dahl bis Wallendorf an, um den deutschen Vorsprung in den Ardennen an der Ausgangsbasis abzuschneiden. In den folgenden Tagen konnten alle Gemeinden des Öslings (nördlicher Teil Luxemburgs) von US-Verbänden befreit werden. Am 29. Januar 1945 waren die deutschen Verbände wieder dorthin zurückgedrängt, von wo aus sie sechs Wochen zuvor den Angriff gestartet hatten. Als letzte Gemeinde wurde am 12. Februar 1945 Vianden an der Our befreit – damit war endlich ganz Luxemburg und sein Norden ein zweites Mal von amerikanischen Soldaten befreit.

Die Ardennenoffensive ließ den ganzen Norden Luxemburgs zerstört zurück. Über 300 luxemburgische Zivilisten waren zwischen die Fronten geraten und hatten dabei ihr Leben verloren.[19] Im Großherzogtum brach eine Nahrungsmittelkrise aus. Das lag an den Kriegsschäden und daran, dass die Deutschen den Norden des Landes ausgeplündert hatten. Es dauerte Jahrzehnte, bis die tiefen Wunden die den Ortschaften des Öslings insbesondere durch den Artilleriebeschuss zugefügt worden waren, verheilten. Die Erinnerung an diesen Alptraum wird in Museen und mit Gedenkstätten und zahlreichen Gedenkveranstaltungen am Leben gehalten – insbesondere in diesem Jahr, dem 75.Jahrestag der ersten Befreiung und dem Beginn der Ardennen-Offensive.

Der Kampf wurde insbesondere von deutscher Seite und dort vorwiegend von den Einheiten der Waffen-SS mit größter Brutalität geführt – auch gegen die Zivilbevölkerung. Besonders hatten die Ortschaften zu leiden, in denen lokale Resistenzler die einige Monate zuvor aus Frankreich über Belgien und Luxemburg zurückweichenden Einheiten angegriffen hatten. Insbesondere in Ostbelgien fielen zahlreiche Zivilisten Racheakten zum Opfer. In Luxemburg mussten insbesondere die leiden, bei denen man US-Flaggen oder andere Anzeichen für eine pro-amerikanische Einstellung fand.

Wie zuvor vor allem an der Ostfront kam es nunmehr auch im Westen zu zahlreichen Kriegsverbrechen. In Malmedy in Ostbelgien erschoss eine Einheit der Waffen-SS 84 amerikanische Kriegsgefangene[20], was sich auch an anderen Stellen der Front wiederholte. Da dieses der US-Seite nicht verborgen blieb, kam es auch auf amerikanischer Seite zu einzelnen Gefangenenerschießungen als Vergeltungsmaßnahmen. „*Bei den Kämpfen in den Ardennen wurde ein für die Westfront beispielloser Grad an Brutalität erreicht. Das Erschießen von Kriegsgefangenen war dort stets in viel stärkerem Maße üblich, als Militärhistoriker in der Vergangenheit zuzugeben bereit waren, besonders wenn sie über ihre eigenen Landsleute schrieben*.“ … „*es muss schockieren, dass eine Anzahl Generale, bei Bradly angefangen, das Erschießen von Gefangenen als Vergeltungsmaßnahme offen billigten*“, so der britische Historiker Antony Beevor in seinem Werk über die Ardennenschlacht, für das er ausgiebig in amerikanischen Archiven recherchieren konnte .[21]

Die letzte deutsche Großoffensive des Zweiten Weltkriegs scheiterte in einem großen Desaster mit Verlusten von fast 82.000 Soldaten – über 12.500 Toten, über 30.500 Vermissten und über 38.000 Verwundeten.

Die Ardennenoffensive verzögerte den alliierten Vormarsch zum und über den Rhein in Richtung Berlin. Erst am 6. März 1945 erreichten die Alliierten Köln. Am 7. März 1945 konnten die Amerikaner die Rheinbrücke bei Remagen im

[16] Frank Rockenbrod, Mörderische Kämpfe am „Schumanns Eck“ (Dezember 1944-Janaur 1945), in: Schumanns Eck 1944-1945, Inauguration des 1944-1945 Liberation Memorial le 11 juin 1994, S. 57-132, S. 61.

[17] Daher trägt Wiltz auch den Ehrennamen „Märtyrerstadt“.

[18] Beevor, S. 317.

[19] Man geht davon aus, dass etwa ein Drittel bei Luftangriffen der Alliierten ums Leben kam.

[20] Der Leiter der Einheit, SS-Obersturmbannführer Peiper, wurde im Juli 1946 im sog. Malmedy-Prozess wegen dieser Vorgänge zusammen mit 42 weiteren Soldaten als Kriegsverbrecher zum Tode verurteilt. Der Oberbefehlshaber der US-Streitkräfte in Europa, Thomas T. Handy, begnadigte Peiper am 31. Januar 1951 zu lebenslanger Haft. Nach der vorzeitigen Entlassung aus dem Kriegsverbrechergefängnis Landsberg 1956 arbeitete er zunächst in Deutschland bis er sich in den 1960er Jahren in Frankreich ansiedelt, wo er im Juli 1976 einem Anschlag zum Opfer fiel, der nie aufgeklärt wurde.

[21] Beevor, S. 396. Beevor zitiert General Pattern aus dessen Tagebuch: „Unglücklicherweise kam es zu einigen Erschießung von Gefangenen. Ich hoffe, dass wir das unter dem Deckel halten können.“

Handstreich nehmen und einen Brückenkopf auf der anderen Seite errichten. Stalin startete den Angriff durch Polen auf das Reich vorzeitig schon am 12. Januar 1945.[22] Da Hitler Kampfverbände aus dem Osten an die Westfront verlegt hatte und diese dort verheizt wurden, führte die sowjetische Großoffensive sehr schnell zum Zusammenbruch der deutschen Ostfront. Der schnelle Vormarsch von der Weichsel bis zur Oder ist zumindest zum Teil auf Hitlers Ardennenoffensive zurückzuführen. Das brachte Stalin auf der Konferenz von Jalta (4.-11. Februar 1945), wo es insbesondere um die „Westverschiebung" der späteren polnischen Grenzen ging, einen großen Verhandlungsvorteil gegenüber Roosevelt und Churchill. Ohne Ardennenoffensive – so kann zumindest spekuliert werden – wären große Teile Deutschlands und womöglich auch Berlin nicht in die Hände der Roten Armee gefallen. Das hätte wiederum die Ausganglage für den bald beginnenden Kalten Krieg fundmental verändert.

Für die USA war die „Battle of the Bulge" die größte und blutigste Landschlacht des Zweiten Weltkrieges. Der hart erkämpfte amerikanische Sieg hat neben der erfolgreichen und blutigen Landung in der Normandie und die glückliche Einnahme der Brücke von Remagen am 7. März 1945 das amerikanische Bild vom Zweiten Weltkrieg in Europa geprägt.

Die US-Verluste lagen mit fast 81.000 Soldaten nur geringfügig unter den deutschen – über 10.000 Tote, über 23.000 Vermisste und über 47.000 Verwundete wurden beklagt.

„*Mit dem Überraschungseffekt und der Brutalität waren mit Hitlers Ardennenoffensive die Schrecken der Ostfront im Westen angekommen*."[23]

Daher ist es sehr verständlich, dass die Erinnerung an diese Schlacht in den USA sehr viel stärker ausgeprägt ist als in Deutschland.[24]

Auf dem amerikanischen Soldatenfriedhof in Hamm nahe der Hauptstadt Luxemburg haben über 5000 gefallene GIs ihre letzte Ruhestätte gefunden, unter ihnen General Patton.[25] Im belgischen Henri Chapelle wurden weitere 8.000 US-Soldaten beigesetzt.[26]

Auf dem deutschen Soldatenfriedhof in Sandweiler – keine 500 Meter vom US-Friedhof in Hamm entfernt – sind fast 11.000 deutsche Soldaten beerdigt – weitere 6.800 sind auf dem Soldatenfriedhof im belgischen Recogne beigesetzt – ganz in der Nähe von Bastogne.

Anfang April 2019 fanden zwei holländische Studenten, die mit Metalldetektoren in den Wäldern am Schumanns Eck unterwegs waren die sterblichen Überreste eines Soldaten, die einige Tage später von Mitarbeitern der Deutschen Kriegsgräberfürsorge aus Sandweiler sowie der Luxemburger Armee und Polizei geborgen werden konnten. Es handelte sich zweifelfrei um einen sehr jungen Soldaten der Wehrmacht, der leider mangels Personenmarke nicht namentlich identifiziert werden konnte. Er wird am diesjährigen Volkstrauertag ihm Rahmen einer von der Botschaft organisierten Beerdigungsfeier auf dem deutschen Soldatenfriedhof in Hamm seine letzte Ruhestätte finden.

Für Luxemburg waren der erneute deutsche Überfall am 16.12.1945 und die schweren Winterkämpfe 1944/45 eine Katastrophe, die umso schwerer wog, weil das Land bereits befreit worden war und sich auf die Friedenszeit vorbereitete. Die Befreiung durch die Amerikaner prägt bis heute die enge Freundschaft zwischen dem Großherzogtum und den USA. Dieses dürfte auch dazu beigetragen haben, dass Luxemburg 1945 entschied, sich von Anfang an in die multilateralen Nachkriegsstrukturen zu Integrierern. So ist das Land u.a. Gründungsmitglied der Vereinten Nationen, der NATO sowie der EU und steht fest zu seinen internationalen Verpflichtungen.

Dr. Heinrich Kreft

Dr. Heinrich Kreft ist deutscher Botschafter in Luxemburg.
Der Beitrag gibt die persönliche Auffassung des Autors wieder.
Eine längere Fassung des Textes ist im Jahrbuch Trier-Saarburg erschienen.

[22] Vgl. Peter Lieb, Unternehmen Overlord. Die Invasion in der Normandie und die Befreiung Westeuropas, , C.H. Beck, S. 210
[23] Beevor, S. 401

[24] Es ist daher auch nicht verwunderlich, dass sich Hollywood des Themas annahm und „Battle of the Bulge (deutsch: „Die letzte Schlacht")u.a. mit Henry Fonda, Charles Bronson und Telly Savalas 1965 in die Kinos brachte.
[25] Bezeichnend für die Bedeutung der Battle of the Bulge für die Amerikaner ist auch, dass General Patton auf dem Sterbebett verfügte, nicht in der amerikanischen Heimat, sondern bei seinen in den Ardennen gefallenen Soldaten beigesetzt zu werden. Er starb am 21.12.1945 in einem Heidelberger Militärhospital an den Folgen eines Verkehrsunfalls.
[26] Im Oktober 1947 brachte man die sterblichen Überreste von 6300 Soldaten in die USA zurück. Über 60 Prozent der gefallenen US-Soldaten wurden schließlich auf Wunsch ihrer Angehörigen in die Heimat überführt.

THEMEN

Hybrid Warfare: Challenges for Intelligence Services

Interview Ralph D. Thiele with Dr. Peter Roell

Thiele: Dr. Roell, you recently presented the European Centre of Excellence for Countering Hybrid Threats in Helsinki with a comprehensive analysis entitled *Hybrid Warfare: Challenges for Intelligence Services*. How did you proceed in structuring this analysis?

Roell: Based the various definitions of hybrid warfare, I initially treated the present threat situation, above all, how it is perceived by the USA and the Peoples' Republic of China. I then followed this up with further analyses of various aspects of the problem, such as China's espionage, Huawei and the challenges for intelligence services, hybrid warfare – terrorism – countermeasures, Germany's perception of the terrorism threat, Germany's counter measures, the role of the EU Intelligence Analysis Centre (INTCEN) in Combating International Terrorism, the importance of electronic warfare, electronic warfare in action with some examples, A2/AD

and technology and, finally, five recommendations.

Thiele: Which of the definitions did you settle for?

Roell: I also find the definition "hybrid warfare" very useful for describing the combination of conventional, irregular and asymmetric means; such means include the persistent manipulation of political and ideological conflict, the combination of special operations and conventional military forces, intelligence agents, political provocateurs, media representatives, economic intimidation, cyber-attacks, proxies and surrogates, paramilitaries, terrorists, and criminal elements.

Thiele: The international threat scenarios are widely known. But how do the United States of America and the Chinese leadership in Beijing perceive such threat scenarios?

Roell: In 2018, former Secretary of Defence, General Jim Mattis, described the threat from a US perspective as follows:

"*We are emerging from a period of strategic atrophy, aware that our competitive military advantage has been eroding. We are facing increased global disorder, characterized by decline in the long-standing, rules-based international order – creating a security environment more complex and volatile than any we have experienced in recent memory. Inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security.*

China is a strategic competitor which uses predatory economics to intimidate its neighbours while at the same time militarizing parts of the South China Sea. Russia has violated the borders of nearby nations and pursues veto power over the economic, diplomatic, and security decisions of its neighbours. Meanwhile, North Korea's breaches of international law and reckless rhetoric continue despite United Nation's censure and sanctions. Iran continues to sow violence and remains the most significant challenge to Middle East stability. Despite the defeat of ISIS' physical caliphate, threats to stability remain as terrorist groups with long reach continue to murder the innocent and threaten peace more broadly."

Thiele: And how does the Chinese leadership in Beijing perceive the threat potential?

Roell: To analyse the Chinese perception, one must first see things from the perspective of the Chinese Politbureau. Like the Europeans, the Chinese have understood that there is obviously only one topic in Washington, in Congress, in the Pentagon, and in think tanks: China, China, China.

The *Global Times* has accurately pinpointed the dispute with the US, and what the Chinese leadership thinks: "*The recent row between the two major economies is not just about trade. In fact, all of the US requirements target issues beyond trade, which is actually meant to contain China's development in an all-round way. By curbing our development in the high-tech field, the US seeks to manage China's future development in the way they design, which thus poses serious challenges to us… More importantly, they do not wish to see China develop high-tech industries, nor better their technology. That is to say, according to their design, changes must be made to the Made in China 2025 initiative and to the reform of State-owned enterprises so as to contain China's development*."

And the *Global Times* claims that while the PRC is ready to compromise on trade and other issues it cannot relinquish the right to develop and its national sovereignty.

Thiele: And what of China's cyber espionage in Germany?

Roell: In December 2017, the German Federal Office for the Protection of the Constitution (BfV), Germany's domestic intelligence service, issued a public warning about Chinese Intelligence Service having created thousands of fake profiles on the online platform Linkedin. Following a nine-month investigation, the BfV identified 10.000 German citizens who had been contacted by members of a Chinese intelligence service masquerading as employees of headhunting agencies, consulting firms, think-tanks or as scientists.

Recruitment targets were chiefly members of the German and European parliaments, but also senior diplomats, members of the armed forces, lobbyists, researchers in private or government think-tanks and political foundations. As former BfV President, Hans-Georg Maaßen, pointed out: "*These individuals were all targeted as a broad attempt to infiltrate parliaments, ministries and administrations*."

It is quite understandable – given the importance attached to keeping face in Asia – that the Chinese Government dismissed the German allegations by claiming that the BfV's investigation was based on "complete hearsay" and was thus "groundless", before going on to urge German intelligence officials to "speak and act more responsibly".

According to BfV information, over 90% of the initial contacts failed in their desired objective; at over five percent, however, the number of continued first-contacts is thoroughly alarming. Even with a few successful operations in the targeted sectors, such as in politics and government administration – but also in other affiliated fields, such as in the economy, industry and the military – this could result in enormous damage to the Federal Republic of Germany.

Thiele: On 27 June 2019, the Federal Minister of the Interior, Horst Seehofer, and the President of the German Federal Office for the Protection of the Constitution (BfV), Thomas Haldenwang, presented the 2018 Annual Report on the Protection of the Constitution – Facts and Trends to the public, which included aspects of China's espionage activities. What, then, is the focus of Chinese intelligence activities in Germany?

Roell: The focus of Chinese intelligence activities is shifting towards political espionage. Chinese intelligence services are now making great efforts to obtain information on supranational entities, such as the EU, and on international conferences like the G20 summit. Moreover, the country is particularly interested in policy positions on China, e.g. recognition as a market economy or territorial disputes in the South China Sea.

Intelligence targets continue to be business and industry, research, technology and the military. The same applies to the popular movements which the Chinese authorities call the "Five Poisons" – including the independence movement of the Uyghur and Tibetan ethnic minorities, the anti-regime Falun Gong movement, the democracy movement and proponents of sovereignty for the island of Taiwan – fearing that these threaten national unity and the Communist Party's monopoly on power.

In 2018, China continued to acquire medium-sized companies in the high-tech sector in order to close gaps in technology and carry out its ambitious high-tech programme "Made in China 2025", which is aimed at making China a global leader among industrialised nations. With this in mind certain sectors and innovative technologies are targeted for support, including new energy sources and engines, medical technology, industrial robotics, information technologies and space and aviation technology.

The export of German high-tech could harm the German economy in the long-run. Nor can it be ruled out that by acquiring security-relevant German businesses China may obtain sensitive data and information which it could use to the detriment of German security interests.

Thiele: Besides HUMINT activities, are the Chinese Intelligence Services also involved in Cyber activities in or against Germany?

Roell: The increase in Chinese cyber-attacks, as witnessed in 2017, continued into 2018. Meanwhile, attacks have become increasingly difficult to detect. This development in the methods and techniques used by Chinese APT cyber attackers in combination with a high level of resources, signifies a growing threat which is also more difficult to identify.

As measured by its visible activities, the Chinese AP10 group is currently considered the most active group and is currently focusing on targets in Japan and the USA, particularly in the telecom sector. The attacks are carried out in three stages: The initial attacks, which are difficult to detect, are followed by tactical reconnaissance on infected systems. The reloading of permanently usable harmful malware can then occur at any time, sometimes months after the initial infection. Methodology and software are individually adapted to the target spectrum or developed entirely from scratch.

Furthermore, as the BfV Annual Report 2018 indicates, so-called supply chain or managed service provider attacks are regarded as particularly effective and sophisticated. The aim is not to attack the target computer itself, which is usually well-secured, but to identify a detour via third parties installed within the target system and interfaces from service providers (e.g. for remote maintenance). Thus, by infecting presumably trustworthy programs and communication channels, malware can be smuggled through selected victim systems, whereby spyware can be reloaded at a later point in time.

Finally, the BfV states that the current world political situation and China's related political and economic ambitions lead one to expect a further intensification of espionage activities, as well as attempts to exert influence. Protecting German companies against cyber threats is the shared responsibility of government and industry. Thus, the BfV continues to participate in the *Economic Security Initiative,* a forum for cooperation among security authorities and industry coordinated by the Federal Ministry of the Interior, Building and Community. This alliance is in an ongoing dialogue with those responsible for security in industrial associations and their member companies to prevent attacks against German industry.

Thiele: In his speech at the Munich Security Conference (MSC) on February 16, 2019, U.S. Vice President Mike Pence urged allies to turn their backs on Huawei technologies, painting the Chinese telecommunications equipment supplier as a severe security threat. Furthermore, in a letter to Federal Minister for Economic Affairs and Energy, Peter Altmaier, US Ambassador Grenell stressed that Huawei is obliged under Chinese law to serve Chinese security interests and that it will not be possible to minimise the risk of information being passed on to Chinese secret services through controls. Can this accusation be substantiated?

Roell: Indeed, it can. Article 28 of the Chinese cyber security law states the following: "*Network operators shall provide technical support and assistance to public security organs and national security organs which safeguard national security and investigating criminal activities in accordance with law*."

Thiele: What is Germany's position on allowing Huawei Technologies to participate in building the country's 5G Network?

Roell: Already in March this year Chancellor Dr. Angela Merkel pointed out that Germany does not wish to ban Chinese telecoms equipment-maker Huawei from building 5G networks; and when Peter Altmaier, Federal Minister for Economic Affairs and Energy, visited China in June 2019, he pointed out that telecommunication security is top priority, and that all operators must fulfil Germany's security requirements. This directive applies no less to Huawei.

Thiele: And what is your assessment of the problem of permitting

Huawei to participate in constructing the German 5G network?

Roell: I share the view of BND President, Bruno Kahl, as stated in a public hearing on 29 October 2019 before the Parliamentary Control Committee of the German Parliament. In the areas in which core security interests are affected Huawei should not be permitted to participate in the grid construction. Since it is impossible to check all single components for "backdoor" access, it is imperative to establish legal or technical criteria to guarantee the requisite security.

The Federal Government is now confronted with the difficult task of safeguarding Germany's core security interests while at the same time developing its economic ties to the PRC.

Thiele: You mention five recommendations listed in your analysis. Perhaps, you would elaborate on these in further detail?

Roell:

1. As the crisis potentials outlined in the threat situation continue, foreign and domestic intelligence services confront specific challenges. Whereas the Federal Government has established thousands of new positions and financial resources for the relevant services, staffing requirements will only be gradually achieved. Suitable personnel must first be identified, recruited and trained.

   In order to successfully deal with the interim period, it is advisable to extend retirement age by several years – with employees' consent – or to hire retired employees. Some foreign and domestic intelligence services have been very successful, especially when drawing on existing employees' many years operational expertise.

   The geopolitical ascent of the People's Republic of China and the shifting of the international balance of power from the standpoint of politics, economics and the armed forces from West to East, should result in Western intelligence services' ability to account for these developments in intelligence-gathering and analysis.

   Since NATO is not only a military but also a political organization, it should pay more attention to developments in the Asia-Pacific region. The EU must reorganize itself such as to be adaptable to effective common foreign policy.

   As far as intelligence-gathering in the Middle Kingdom is concerned, this is of strategic interest to Germany and Europe in all areas – in politics, economics, science, military, technology. Here it is necessary to build first-class sources – so-called inside agents – which, though requiring time and patience can prove particularly effective.

2. The Federal Republic of Germany and the EU will continue to be the focus of Chinese intelligence services. Economics, science, technology and the armed forces are among the focal points of Chinese intelligence-gathering.

   There is also a tangible shift in intelligence-gathering towards political intelligence-gathering, such as gaining knowledge of supranational institutions like the EU or international conferences (G20 summit). Furthermore, political positions concerning territorial disputes in the South China Sea or the trade dispute with the US, for example, are of great interest to Beijing and essential to strategic decision-making.

   Other intelligence services operating in the Federal Republic of Germany include the Russian Federation, Turkey, Syria, Vietnam etc. Based on the threat situation, the Federal Office for the Protection of the Constitution (BfV) must be so organised as to ensure 360-degree visibility. The same also applies to the activities of Western intelligence services which operate in the Federal Republic of Germany – indeed, as the media has pointed out.

   A common policy should be developed with regard to Huawei's involvement in the development of the 5G network in Germany or the EU, a policy that accounts for security and political aspects.

3. The threat of international terrorism remains, and the cooperation of German services with those of the US is indispensable. In the fight against international terrorism, the EU's Intelligence Analysis Center (INTCEN) is also important. The EU INTCEN has proven its outstanding capabilities in recent years; thus, it clearly makes sense to deal with cyber-threats and fake news.

   Since the Federal Government attaches greater importance to dealing with right-wing extremism, domestic and foreign intelligence services as well as other security agencies are required. Again, the challenge is to be able to provide well-suited staff. The restructuring of the Federal Office for the Protection of the Constitution (BfV), the Federal Foreign Intelligence Service (BND) and the German Federal Office for Military Counterintelligence Service (BAMAD) is underway. The BAMAD will also be increasingly active in the field of operations, which is highly recommended.

   However, this will only be successful if the BAMAD disposes over a sufficiently large number of recruiters/case officers.

4. The diversity of signals within the electromagnetic spectrum, the reallocation of signals, and sharing between commercial and military spheres has presented a myriad of technological hurdles for engineers to overcome. Maintaining the technological edge, orchestrating cooperation between commercial and governmental sectors, and protecting intellectual properties will be key challeng-

es, whereby the intelligence community has an important supportive function.

The closing decades of the last century saw the rise of electronics and software, together with their evolution, penetrating to the heart of military capabilities at all levels, in all domains, and across all services worldwide. This created a modern and very complex battlespace. Meanwhile, Electronic Warfare (EW), i.e. action involving offensive or defensive use of the electromagnetic spectrum (EMS), was also growing in prominence across the armed forces. Disruptive technologies have created threats and opportunities that are changing entirely and thus challenging the way that we have conducted EW in the past.

Electronic Warfare has been an afterthought for a quarter of a century, but the exponential growth of space and cyber technologies that rely, above all, on electromagnetic signals has brought about a renewed sense of urgency with respect to rebuilding and recapitalizing EW capabilities, both offensive and defensive. However, due to the increasing dependencies of modern military systems upon EMS it is imperative that commanders understand the following:

The modern challenges in dealing with the high-end capabilities of opponents, especially in confrontations requiring operations in Anti-Access/Area Denial (A2/AD) environments, have brought EW back to the forefront. This applies, in particular, to hybrid challenges that emphasize ambiguity.

EU and NATO nations would be well-advised to re-invest in modern EW capabilities so as to build their sufficient capacities for meeting respective challenges. Intelligence should support situational awareness about upcoming technologies, capabilities and challenges.

5. It is important to consider anti-access (A2) and area denial (AD) challenges. They are imminent in several regions. Opponents can attack NATO, the EU and its member states in all five key domains – air, sea, land, space, and cyberspace.

   While the focus of high-level discussions is predominantly on sophisticated, longer-range adversary capabilities and methods – such as ballistic missiles, submarines, weapons of mass destruction, and offensive space and cyberspace assets – dangerous, though no less technical methods, may include terrorism, proxy warfare or weaponized social media employed by opponents for opening alternative "hybrid fronts".

   One critical gap to date has been the significant consideration of A2/AD challenges emerging largely from outside the realm of traditional military competition and violence. When opponents effectively combine political, economic, and informational tools with important military capabilities, the A2/AD challenge becomes more acute and potent. When targeted specifically at NATO and EU vulnerabilities, this may induce "warlike" effects on core own values and interests, while precluding the use of military power as a legitimate response.

   Revolutions in information, personal computing, communications, networking and hybrid forms of warfare – when combined with the proliferation of precision weapons and improvised battlefield lethality – substantially widen the universe of effective A2/AD opponents through individuals, loosely organized groups and sophisticated regional powers. Similarly, the networked mobilization of foreign popular, nonviolent resistance may also prove a significant challenge to freedom of action in the future.

   Consequently, it is to be recommended that from the intelligence side the A2/AD challenge be broken down into respective angles so as to include the hybrid spectrum.

Thiele: Dr. Roell, I thank you for this interview, and hope that you will join us in future discussions on Hybrid Warfare with NATO and other EU member states.

Dr. Peter Roell is President of the Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) in Berlin.
Ralph Thiele is Managing Director StratByrd Consulting, Chairman of the Political Military Society (PMG) and President of EuroDefense (Deutschland).
Opinions expressed in this contribution are those of the author.

THEMEN

Hybrid Warfare – Orchestrating the Technology Revolution

The Challenge of Hybrid warfare

Twenty-first century security and prosperity are challenged by complex, trans-regional, all-domain and multifunctional hybrid security threats particularly posed by a combination of state, non-state and pseudo-state actors. In the Nordic and Baltic region and particularly regarding Ukraine, Russia continues to use disinformation, cyber-attacks and military posturing to challenge security. Additionally, an increasingly assertive China is looking to secure access to strategic geographic locations and economic sectors through financial stakes in ports, airlines, hotels, and utility providers, while providing a source of capital for struggling European economies. Russia and China have increased their transactional collaboration to increase their power and influence. Particularly in its neighbourhood, Russia is conducting a campaign of hybrid warfare below the level of openly declared war using various tools of national power in order to advance its strategic interest.

At the same time, Europe's borders, particularly in the south, are wide open. As dividing lines within European societies are growing and deepening, this exposes numerous vulnerabilities that can be exploited by all kinds of hybrid actors from various directions, not only or primarily from Russia. However, military strength provides additional opportunities to exploit hybrid methods, even without the active use of force. Military escalation potential or dominance by its mere existence would support any kind of subversive hybrid activities.

The Ukraine case illustrates an important relationship. The more closely connected and interwoven a country's relations with its adversary, and the more pronounced their mutual dependencies, the more potential starting points there are for hybrid methods of warfare. Consequently, globalization, close international interaction and interconnected societies – as positive and desirable as these developments may be – have the potential to open up additional starting points for hybrid methods of warfare. This could make hybrid warfare a particularly favoured means among former friends such as Ukraine and Russia had been within the framework of intrastate conflicts, and especially in civil wars.

Hybrid warfare of a type e.g. demonstrated on the Ukrainian battlefield, if carried out against European countries, would pose a particular challenge for Europe and the crisis management of both NATO and the EU. Although it may seem unlikely from today's perspective, in an extreme case, NATO's military defence could be bypassed by subversive means in a 'downward escalation mode'. This may include possible military threats from within, for example as a result of long-term subversion, infiltration, propaganda or destabilization. With their security and defence policy primarily oriented towards external threats, neither NATO nor the EU would be prepared, able or ostensibly entitled to protect their member states, as well as themselves as organizations, against such challenges at the blurred interfaces of internal and external security.

Technological trends suggest that the portfolio of hybrid hazards will rapidly expand. While the EU and NATO have stated the high relevance of hybrid threats to include the meaning, possibilities and challenges of emerging, disruptive technologies, knowledge of their true capacities and capabilities is a privilege of the few. It is evident that political, civilian and military decision makers need to become more knowledgeable of the disruptive potential of new technological trends, which may offer new options of violence, as well as of the use of force in a hybrid warfare/conflict context. They also need to become sovereign actors, applying all necessary instruments of power to effectively counter hybrid threats (Schmid 2019a).

Clearly, it is of importance to come to a shared understanding of what is at stake. Yet, if it is time to act, for Europe, for NATO, for our nations – who is to act? If the given technological revolution must be orchestrated – by whom should it be orchestrated? Responsibilities need to be defined. Orchestration in authoritarian states like Russia or China is not a problem – neither legally, not politically, nor ethically speaking. But in democratic nations this is a different matter. In countering hybrid warfare, there is more at stake than "prepare – deter – defend", as NATO is traditionally called upon to do.

Conceptual Considerations

All war is hybrid, but there is also a specific hybrid way of conducting war. In contrast to military-centric warfare, its centre of gravity is not primarily located in the military domain. While far from novel in its essence, the empirical manifestation of hybrid warfare can be surprisingly new and differ from case to case (Schmid 2017a). This hybrid warfare in the narrower sense is of a strategic nature and can be identified by three key characteristics and their hybrid orchestration:

1. Focussing the decision of war/conflict primarily on a broad spectrum of non-military centres of gravity (CoG).
2. Operating in the shadow of various interfaces, such as between war and peace, friend and foe, internal and external security, civil and military domains, state and non-state actors.
3. Utilizing a creative combination, hybrid orchestration and the parallel use of different civil and military, regular and irregular, open as well as covert means, methods, tactics, strategies and concepts of warfare, thereby creating 'ever-new' mixed hybrid forms.

While hybrid warfare actors generally resort to creative and indirect strategies of limited warfare and a limited use of military force, it must be emphasized that hybrid warfare potentially includes all levels of escalation. Friction and uncertainty are always part of the game and the perceived manageable use of force may get out of control. Due to its focus on a broad spectrum of non-military CoGs, a military decision as such is not necessarily required for hybrid warfare actors to achieve their political goals. As happened in Donbas or during the Second Indochina War (Schmid 2017b, 373-390), militarily it may be sufficient for the hybrid warfare actor to prevent his opponent from deciding the war on the military battlefield, while seeking a decision on a non-military centre of gravity. Morale and legitimacy can become strong weapons in this context.

Hybrid warfare generally favours the offensive as it offers a huge potential for surprise and offensive action, even against militarily superior opponents. This builds on the ability to create ambiguity by silently operating in the grey areas of interfaces, while concealing or plausibly denying an actor's intent and role as a party to the conflict, combined with a limited use of force only as a last step. By following a longterm, indirect or masked 'salami tactics' approach or, conversely, by conducting rapid, unexpected offensive operations thus achieving a fait accompli, hybrid actors can create new sets of circumstances that are al-

most impossible to be changed afterwards without undue effort. Hence, the offensive power of hybrid warfare presents the defender with a particular challenge: being taken by surprise without even recognising that one is under hybrid attack until it is too late.

In the face of these developments, hybrid warfare becomes not only the war of choice for the small and poor, such as terrorists, North Korea or Iran. It may also become particularly attractive for larger powers, as they can pursue their political interests with little risk. Against this backdrop, the crux of meeting this challenge will be to identify and understand in due time its ever-changing, multiple and often disguised appearances, as well as the pattern and strategic rationale behind it. It will likely be impossible to respond appropriately unless the strategies and methods of a certain hybrid warfare actor are identified and understood comprehensively and early enough.

Consequently, awareness is the first precondition for addressing hybrid warfare challenges. A multi-domain situational awareness needs to cover the full spectrum of opponents' hybrid activities. Decision makers need to understand the entire set of domains, thus broadening considerably the spectrum of situational awareness requirements. The shifting focus opens up a need for new tools and technologies to fully understand the operating environment, and thus to take valid decisions. Real-time analytics and anomaly detection will serve as elements to uncover hybrid operations. With sensors (Internet of Things), people (social media), systems (Logs), mobiles (locations), etc. generating continuous and/or event driven data, the capability of processing online data streams will be pivotal to a situational awareness, which alerts to certain actions, flags complex events or points out new developments.

While military means and the use of force play an important role in hybrid warfare, and in its respective campaigns – in contrast to military centric/conventional warfare – the strategic CoG of hybrid warfare is not primarily located in the military domain. This has consequences for political, civilian and military elites in democratic societies. The ability to constantly perform in-depth analyses of specific hybrid challenges, related actors and strategies will become a key capability in countering and responding to hybrid methods of warfare. A comprehensive understanding of hybrid warfare and a related education of judgment, not least to prevent overinterpretation and overreaction, are decisive.

Digital Challenges

Today the nation's power – militarily as economically – rests on data. Via data and communication networks, computers and automation come together in a new way with remotely connected robotics. In a world of constant connectivity, data is the new oil. And networks are the new oil rigs. Just as crude oil needs to be refined to create usable products like gasoline, data needs to be refined to deliver actionable information.

The backbone of the Information or Digital Age is the Internet, a global infrastructure for information transfer, a complex and hard to comprehend system of systems. Digital transformation has deeply affected all areas of society, including industry and economy, as well as governmental domains, such as defence and security.

Against this backdrop, armed forces have structured a new business model on modern, interoperable, scalable and service-oriented information and communications technology (ICT). Rapidly increasing complex data volumes, and the capability to make their information actionable have become of decisive importance to military operations. Data may arrive on specialised secure military channels, or it may be so-called open intelligence gathered over the internet or media reports. The sheer diversity of platforms – airborne, satellite, submarine, surface ship, soldier-borne – generating and acquiring data is immense. Connectivity boosts the efficiency of the power instruments non-linearly. Appropriately employed ICT is nowadays decisive for the outcome of war and war-like operations. The cyber world offers a set of hardware and software systems, including data and information processing, globally available broadband data transmission at the speed of light, mass data storage, algorithms and artificial intelligence (AI), precision timing, databases with geo-data, and geolocation services.

The technologies of the digital age have moved us rapidly into the cyber space. Cyber is an abstract realm with its high-speed communication lines, data mountains and processing capabilities not easy to grasp and comprehend. We call it the virtual world as we cannot sense the occurrences in the web and the connected number crunching machines. To most of us the net evades our perceptiveness. We sense results of virtual world processes when they hit the real world often to our surprise or embarrassment.

The tremendous computing power and ubiquitous connectivity have become an everyday feature of our life. Powerful processing and storage devices and global infrastructures providing timing, geolocation and communication changed our political, societal and economic systems. It equally changed warfare. Information and communications technology (ICT) emerged as a key enabler for all human controlled processes. It has opened new ways to collect, store, manipulate, use and distribute data and information and to create knowledge. It even empowers non-military operations to achieve war like effects as demonstrated by the destruction of the centrifuges of the nuclear enrichment facility in Natanz/Iran by malign software in the first decade of this century. It provides access to information and enables influencing individuals, interest groups, and states on a global scale. ICT has become the underpinning of hybrid warfare.

Hybrid warfare happens in the real and in the virtual world. The real-world segment is in principal well observed and understood, while the virtual segment operates

stealthy in the invisible world of computers and networks until showing effects in the real world, often to the surprise of an unprepared target.

Conventional warfare employs Industrial Age technologies, in which mechanical systems embody and deliver the military force. The Industrial Age has been shaped in particular by three revolutions in military affairs (RMAs), i.e. the emergence of disruptive technologies that overtake existing military concepts and capabilities and necessitate a rethinking of how, with what, and by whom war is waged (Wilson 2019, 3).

- RMA I is the method of war fought with combat vehicles and industrial production and it emerged out of the second half of World War I.
- RMA II is the method of war of the insurgent that emerged out of the Sino-Japanese war during the 1930s and led to the successful seizure of power by the Chinese Communist Party (CPP) in 1949.
- RMA III is the method of war via the use or threat of use of nuclear weapons and their long-range means of delivery – a dominating feature of the Cold War.

Currently, the most technologically dynamic method of war is RMA IV, i.e. the method of war fought through the use of silicon and all of the manifestations of the digital age including precision-guided munitions, active and passive sensors, cyberspace, and robotics. It covers the development of guided munitions, Command, Control, Communications, Computer technology, Intelligence (C4I).

The ICT developments of the last three decades have altered the way states pursue their military goals. In the predigital age, information was difficult to collect and to manage. Hierarchically organized structures were the means of choice for information storage and management. This has been a slow system where political and military decisionmakers at the political-strategic and even at the operational level were often several days behind the actual situation in the battle. Today, states and armed forces all over the world have undergone a transformation process to capitalize on the enabling capabilities of the digital world. Concepts of Electronic and Information Warfare emerged and can be considered as a harbinger of hybrid operations.

In this context, the emergence of military technological competitors, such as China and Russia, constitutes a new strategic challenge to the West. China has developed and deployed its armed forces, with modern RMA-I techniques, and it is also exploiting the advances in RMA-IV. In view of this, NATO and the EU face the prospect that a near-peer continental power will soon be able to exploit the tools and techniques of RMA-IV. Against this backdrop, the Anti-Access / Area Denial (A2/AD) challenge has become a centrepiece of Western defence investment. Much of the U.S. response to China and Russia's improved A2/AD capabilities will manifest via the further development and exploitation of the tools and techniques of RMA-IV. This will include significant investments in long-range strike systems to provide large combat platforms with increased survivability and hitting power, enhanced missile defences, and a robust capacity to conduct offensive operations in space and cyberspace. Furthermore, the tools and techniques of nuclear weapons (RMA-III) may see a renaissance.

Meanwhile, RMA V is lurking around the corner, as the technological revolution unfolds (Thiele 2019, 6). Artificial intelligence, autonomous systems, ubiquitous sensors, advanced manufacturing, and quantum science is about to transform warfare radically. Emerging technologies will enable new battle networks of sensors and shooters to rapidly accelerate the process of detecting, targeting, and striking threats, what the military call the "kill chain." More incredible still, so-called brain-computer interface technology is already enabling human beings to control complicated systems, such as robotic prosthetics and even unmanned aircraft, with their neural signals alone (Atherton 2019). Obviously, it is becoming possible for a human operator to control multiple drones simply by thinking of what they want those systems to do.

Hybrid Warfare will engage a creative mix of all these RMAs. In particular we must expect stealthy operations such as clandestine operations to influence, coerce, sabotage, and other actions. The information and communications technologies are the key enabler of clandestine operations as an element of hybrid warfare. As the advances of information technologies are faster than the development of mechanical systems in a broad sense, we should expect a shift towards virtual threats.

Dealing adequately with hybrid warfare in all relevant domains requires understanding the tools of hybrid warfare. This implies understanding the complexity of the digital world and the need to include the abstract cyberspace in our security thinking. Here systems of systems thinking is key as hybrid actors fuse military and non-military means. Hybrid warfare applies strategies that seek superiority by systemic capabilities to boost efficiency. ICT enables a systemic approach to combine military operations with various means to destabilize a state and polarise the society by employing diverse combinations of power instruments to target an adversarial society, economy, infrastructure, and the military and to collect information. These power instruments have two prime functions: inflict selective damage and support of decision making: Superior decisions on the own side and misguided decisions on the adversary's part. The power available to political, civilian and military decision-makers and the quality of their decisions will ultimately decide the outcome of every contest.

We can expect hybrid warriors to develop models of their perceived targets and to use them to make an attack. Aggressors will find much of the information needed for the design of own tools openly

available on the internet to include information about critical infrastructures, personal information from social media accounts, corporate data, and information about politics and administration. This increases NATO´s, the EU´s and member nations' vulnerability. This is why we need to model own vulnerabilities and design response functions, a defence system in the virtual world. This requires high system engineering skills and a highly qualified team of engineers, computer scientists, psychologists, and social scientists. We need a new approach to safeguard our security, now and in the future (Theile, 1-6).

Trends and Technologies

While digital challenges pose enormous change requirements, the world is already rapidly moving towards a post-digital era (Accenture 2019, 5). Governmental and non-governmental organizations have made enormous strides to realize the benefits of new digital business models and processes. With every business and organization investing in digital technologies, the next disruption is coming as the power of cloud and artificial intelligence continue to advance. Combined with technologies such as distributed ledger, extended reality, and quantum computing, new technologies will reshape not only prosperity and security, but also relationships – man-machine, between individuals, an entire ecosystem.

Computers are becoming faster and ubiquitous. Machines are getting smaller and more powerful each day. Fundamental breakthroughs include robotics, nano- and biotechnology, artificial intelligence, distributed ledgers, sensor technology, and 5G. Additive manufacturing methods provide for prototypes, parts for weapons and vehicles. The enormous potential of artificial intelligence (AI) is playing an ever-important role. People are adopting new technology with alacrity: customers and employees, governmental officials and criminal actors. We can expect a broad spectrum of technologies to contribute to hybrid warfare and its objectives (Callinan 2019, 44). The further development and integration of artificial intelligence in conventional weapons platforms, and the robotization of battlefields will progress rapidly.

How far can we realistically look into the future? How far must we look into the future? Certainly, researching trends and upcoming disruptive technologies is indispensable. Yet the focus should be on shorter timelines than in the past.

Three lines of thought need to be explored in particular:

- Where is the development of disruptive technologies going, and how fast? Who is driving this development, and in whose interest is it?
- What are the strategic and military implications? What kind of capacities are needed and how are they to be procured and funded? What kind of training and education is needed? What are the implications for the nature of military command and control?
- What is the political and ethical impact of these disruptive technologies on our democratic systems? What is the impact on the political control of armed forces and parliamentary oversight? - on international law? - on the value of human control in regard to AI, etc.?

NATO and Europe are at a crossroads. Hybrid warfare is threatening member nations and NATO´s and the EU`s neighbourhood. Countering hybrid warfare requires the ability to protect vulnerable interfaces and to operate in their grey areas by adopting a truly comprehensive approach. Against the backdrop of hybrid attacks primarily on non-military CoGs, the importance of high professional (particularly also) civilian leadership, civil preparedness, an educated public, and an effective legal framework cannot be overstated.

As hybrid threats put peace and prosperity, social cohesion and security at risk, responses need to include a whole-of- government approach, a whole-of-society approach, as well as international cooperation and coordination. The interfaces between internal and external security are of particular relevance. It is high time for the NATO, EU and the member states to improve their common and comprehensive awareness and understanding of hybrid warfare and related strategies as a precondition for common and comprehensive action in defence and response.

The given technological revolution must be orchestrated, for technical and operational reasons, but also with a view to the fundamental values represented by NATO and EU member nations. Three dimensions need to be tackled.

Conceptually, strategy, concepts and concrete initiatives need to enable successfully resisting and fighting hybrid aggression, as new technologies are fundamentally challenging politics and society, economy and production, prosperity and democracy, security and defence. They should guide stakeholders towards increased resilience against hybrid shock and stress and also towards comprehensive active measures. Each nation and organisation has to develop its own understanding of the kind of hybrid threats/warfare that can be directed against it and is required to thoroughly familiarise itself with its own vulnerabilities. This applies also to NATO, and the EU. All are well advised to develop a common understanding of how to deal with hybrid threats/warfare, so as to pull in the same direction (Hagelstam 2018).

Technologically, the possibilities of the technological revolution need to be exploited, their misuse limited. As technology meets doctrine and organization, training and material, leadership and education, personnel and facilities this constitutes an enormous challenge and must be managed well. Disruptive innovation can lead to new opportunities, or exacerbate existing conflicts, it can promote prosperity, or strengthen radicalisation. This is precisely why this technological revolution must be orchestrated in such a way that all benefit: people and societies, security and defence. The overlap between military and civilian capabili-

ties of the technology revolution can serve as an early indication about what we might see in future security challenges (APA 2019).

Organisationally, as the technology revolution unfolds, there is reason for urgency in orchestrating and accelerating innovation in Europe. It needs to invest not just more manpower and money, but also to push focussed research and thought to achieve innovation acceleration, thus promoting:

- Its own capabilities for enhancing situational awareness as the precondition for viable action when it comes to hybrid threats;
- C4I infrastructures, providing the backbone to act comprehensively with all available instruments of national and international power on all levels of escalation;
- Real-time analytics and anomaly detection as elements to uncover hybrid operations; and
- Edges of our security and defence networks, thus enabling superior network enabled capabilities.

Both, hybrid warfare and disruptive technology constitute serious challenges to NATO, the EU and member states. Meeting these calls indeed for a determined, holistic and collaborative approach. Open, democratic societies that lack strategic vigilance are particularly vulnerable to hybrid methods of warfare (Schmid 2019b).

Dr. Johann Schmid & Ralph Thiele

Dr. Johann Schmid is Director COI Strategy & Defense, Hybrid COE. Ralph Thiele is Managing Director StratByrd Consulting, Chairman of the Political Military Society (PMG) and President of EuroDefense (Deutschland).
Opinions expressed in this contribution are those of the authors.
First published in: STRATPOL: NATO at 70: Outline of the Alliance Today and Tomorrow, Special Edition of Panorama of Global Security Environment 2019. (p. 211-225).

References

Accenture. 2019. "The Post-Digital Era is Upon Us. Are you ready for what´s next? Accenture Technology Vision 2019." May 17. Accessed May 29, 2019. www.accenture.com/t20190201T224653Z__w__/us-en/_acnmedia/PDF-94/Accenture-TechVision-2019-Tech-Trends-Report.pdf.

Die Presse. 2019. "BMW-Chef: Kommende Jahre unklar - 10 oder 10.000 Elektroautos." January 20. Accessed May 29, 2019. https://diepresse.com/home/Economist/Wirtschaftsnachrichten/5565742/BMWChef_Kommende-Jahre-unklar-10-oder-10000-Elektroautos.

Atherton, Kelsey D. 2019. "In this league, drone races are won by brainwaves alone. C4ISRNET." April 26. Accessed May 29, 2019. https://www.c4isrnet.com/unmanned/2019/04/26/league-racesdrones-by-brainwaves-alone/.

IMPRESSUM

Denk*würdigkeiten*
Journal der
Politisch-Militärischen
Gesellschaft e.V.

Herausgeber
Der Vorstand der **pmg**

Redaktion
Ralph Thiele (V.i.S.d.P.)
E-Mail: info@pmg-ev.com
Webseite: www.pmg-ev.com

Die **Denk*würdigkeiten*** erscheinen mehrfach jährlich nach den Veranstaltungen der **pmg**.