Denkwürdigkeiten

Journal der Politisch-Militärischen Gesellschaft

Nr. 97
Juni
2015

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

ISSN 1436-3070

LEADOFF

Liebe Mitglieder,

die Auseinandersetzung des Westens mit Putins Russland bestimmt weiter die außen- und sicherheitspolitische Tagesordnung. Der G7 Gipfel in Oberbayern vom vergangenen Wochenende kam rasch zur Sache. Was treibt Putin für ein Spiel? Warum zündelt er weiter in der Ukraine? Was hat er vor? Selbstkritische Fragen wurden eher nicht gestellt.

Obama machte die amerikanische Position deutlich: Die G7-Gruppe müsse sich gemeinsam der "Aggression in der Ukraine" entgegenstellen. Allerdings – so unterstrich die deutsche Kanzlerin – gebe es auch Fragen, bei denen russische Unterstützung gebraucht wird, beispielsweise mit Blick auf die Verhinderung des Nuklearprogramms im Iran und die Beendigung des Bürgerkriegs in Syrien. Dennoch hält auch sie eine Rückkehr Russlands in den Kreis der G8 derzeit für nicht möglich. Mit der Annexion der Krim hätte sich Russland gegen die gemeinsamen Werte gestellt und damit eine Barriere errichtet, die sich nur schwer überwinden lassen wird. Entsprechend rief EU-Ratspräsident Donald Tusk die sieben führenden Industriestaaten auf, sich geschlossen hinter die Sanktionspolitik zu stellen.

Wohin diese Ansätze führen, wird man sehen. Bisher hat sich der Konflikt schleichend ausgeweitet und mittlerweile in einer Cyber-Ausprägung möglicherweise auch den Bundestag erreicht. Nach Spiegel-Online liegen den deutschen Sicherheitsbehörden inzwischen Indizien vor, die auf eine Urheberschaft russischer Cyberspione hinweisen. Was gibt uns eigentlich die Gewissheit, dass der Ukrainekonflikt sich dort begrenzen oder gar lösen lässt und wie gut sind wir hier in Deutschland auf eine weitere Eskalation vorbereitet – außen- und wirtschaftspolitisch, militärisch und in der inneren Sicherheit oder etwa in der Cybersicherheit?

Ralph Thiele, Vorstandsvorsitzender

In dieser Ausgabe

THEMEN

Rüstung: Anders oder gar nicht

Deutschlands sicherheits- und verteidigungspolitische Rolle ist kein Feld, auf dem sich Politiker, Soldaten und Kommentatoren Anerkennung verdienen könnten. Wer bemerkt, dass Soldaten kriegsnah ausgebildet werden müssen, wird entsorgt. Wer nach einsatzfähigen Waffen ruft, ist der Kriegstreiberei und Verschwendung schuldig. Wer Kriegseinsätze für absehbar oder gar sinnvoll hält, wird als amerikanischer Agent denunziert.

Dabei würde es die Bundeswehr als eines der bewundernswertesten Produkte des deutschen Neuanfangs nach 1945 durchaus verdienen, wenn man sie und die in ihr dienenden Menschen bei Ihrer schwierigen Aufgabe ernst nehmen und wirksam unterstützen würde.

Bei der Ausrüstung und Ausrichtung der Bundeswehr liegt Manches im Argen. Die heutigen Anforderungen unterscheiden sich von denen der Vergangenheit. Nach den Regeln der Kunst empfiehlt sich eine Analyse der strategischen Lage - wohl wissend, dass es ebenso so viele Bilder von der strategischen Lage gibt wie Menschen, die sich darüber strukturierte Gedanken machen. Aber irgendwo muss man ja anfangen, damit eine professionelle Debatte in Gang kommt.

Im Folgenden wird aus einem Aufriss der strategischen Ausgangsbedingungen ein grundlegender Neuansatz hergeleitet, der wesentlich besser für die Bereitstellung der notwendigen zukunftsorientierten Wehrfähigkeiten sorgen kann als das existierende Rüstungswesen.

Strategische Lage, Teil 1: Russland

Das nach zeitweilig jämmerlichen Jahren des Umbruchs wieder stabilisierte Russland knüpft an traditionelle sicherheitspolitische Konzepte an und nutzt das Vakuum an der Peripherie der EU, im Schwarzmeerraum und im Nahen Osten, um sich mit einem Glacis von Gangsterstaaten und -territorien zu umgeben.

Diese Strategie der kulturellen Einigelung Russlands dient dem Machterhalt der Ex-KGB-Eliten, gegenwärtig geleitet von Wladimir Wladimirowitsch Putin, die den Wandel von der moralisch und finanziell bankrotten Sowjetunion zum neuen Russland vorgedacht und inszeniert haben. Sie geht einher mit einer wohldosiert erneuerten Drohkulisse gegenüber NATO-Staaten, um Mittel in Europa zu binden und euro-atlantische "Weltpolitik" im Krisenraum vom Mittelmeer nach Ostasien zu schwächen.

Strategische Lage, Teil 2: Kulturkampf

Die radikale, aggressive Abkehr weiter Teile Europas sowie der amerikanischen Medieneliten von traditionell etablierten sittlichen Werten menschlichen Zusammenlebens ist – so alternativlos sie uns selbst aus europäischer Sicht erscheinen mag - für die breite Mehrheit der Menschheit außerhalb Europas existentiell so befremdlich und abstoßend, dass von Bewunderung und "soft power" Europas keine Rede mehr sein kann.

Kombiniert mit der ostentativen Arroganz des mitteleuropäischen Reichtums und der allzu offensichtlichen Aporien unserer vorgeblichen europäischen Vorbildrolle - wie z. B. in der menschenverachtenden Flüchtlingspolitik - hat dies weltweit zum einem Verlust des Respekts für europäische Politik geführt. Wann immer ein Europäer irgendwo zu irgendeinem Thema den Mund aufmacht, wird von Vielen zunächst ein Aufguss bigotten, aufdringlichen Gewäschs erwartet - egal ob in Russland, USA, Iran, China, Nigeria oder Israel. Auch einige kleinere Länder innerhalb der EU haben schon diese Erfahrung gemacht.

Europa muss sich daher darauf gefasst machen, sich in einer Position zunehmender Schwäche und Isolation dem wachsenden Hass der Außenwelt ausgesetzt zu sehen. Der körperliche Kampf gegen Europa und das, wofür es steht, ist zu einem Identifikationsfaktor männlicher Jugend geworden, insbesondere in islamisch geprägten Gemeinschaften außerhalb und innerhalb Europas.

Strategische Lage, Teil 3: Krieg im Nahen Osten

Im Nahen und Mittleren Osten und am Horn von Afrika hat ein zumindest Dreißigjähriger Krieg epischen Ausmaßes begonnen, der sich einerseits um das sunnitisch-schiitische Schisma strukturiert, andererseits die Vision vom neuen Kalifat gegen die Realität der Herrscherhäuser auf der arabischen Halbinsel, und vor allem gegen die saudische Kontrolle der heiligen Stätten und des Öls richtet.

Neben diesen propagandistischen Leitideen geht es - wie in jedem solchen Krieg aller gegen alle - vor allem um die Aufstiegschancen, die das erzeugte Chaos den "Tüchtigen" eröffnet, und um die Lust an der Macht über Leben und Tod.

Dieser vielschichtige, zutiefst gewalttätige Konflikt hat bereits zur Vernichtung des orientalischen Christentums geführt und wird aller Wahrscheinlichkeit nach zum wesentlichen bestimmenden Faktor der kommenden Entwicklungen in der Weltwirtschaft und weltweiten Rüstung der nächsten beiden Jahrzehnte werden.

Die USA hatten in den Jahren von Präsident Carter bis Präsident George W. Bush den großangelegten strategischen Versuch unternommen, die USA als Ordnungsmacht in Westasien zu etablieren, um diesem seit den 70er Jahren erkennbaren Trend entgegenzuwirken.

Europa ist von dieser zeitweiligen gemeinsamen Strategie im zweiten Irak-Krieg abgefallen. In der Folge haben sich die USA auf Dauer aus dieser exponierten, kostspieligen Rolle zurückgezogen und den Kampf um Frieden in der Region so weitgehend wie möglich den Akteuren vor Ort überlassen.

Aus europäischer Sicht kann es in dieser Lage über schöne Worte hinaus nur zwei relativ bescheidene Ziele geben: sich gegen schädliche Auswirkungen absehbarer Verzerrungen des Erdölmarktes abzusichern und die Anrainer des östlichen Mittelmeers möglichst vor Verwüstung und Massenmord zu schützen, einschließlich Israel, Libanon, Türkei und Ägypten. Die fehlgeschlagenen Ansätze zur Intervention in Libyen und Syrien haben jedoch bereits gezeigt, dass für letztere Ambition die Grundvoraussetzungen in jeder Hinsicht fehlen.

Es bleibt somit die Option, durch gesteuerte Waffenlieferungen in die Konfliktregion und in die bedrohten angrenzenden Länder die für Europa relativ am wenigsten gefährlichen Kräfte zu stärken - und zugleich auf diese Weise dem Absterben der europäischen Rüstungswirtschaft ein wenig entgegenzuwirken.

Es ist in diesem Zusammenhang absehbar, dass die arabische Vorliebe für teure Edelwaffen im Stil des ehemaligen Ost-West-Wettrüstens in den praktischen Bedarf an großen Mengen billiger Abnutzungswaffen im Verbund mit erschwinglicher mobiler elektronischer Vernetzung übergehen wird.

Begleitend muss sich Europa auf Jahre der Flüchtlingsrettung und -aufnahme im Umfang vieler Millionen Menschen vorbereiten.

Strategische Lage, Teil 4: Wirtschaftliche und gesellschaftliche Stagnation

Der Raubbau der Nachkriegsgeneration an den Staatsfinanzen und die langjährige Unterdrückung liberaler Innovationskraft zugunsten einer mit wenigen Ausnahmen ausschließlich am karrierebezogenen Eigennutz orientierten Managementkaste in der Großindustrie mündet in gesamtgesellschaftliche Lähmung.

Die "grüne" Technologiepolitik der letzten dreißig Jahre hat zwar den Absatz der Automobilindustrie durch regulatorischen Zwang verstetigt und der Solar- und Windkraftindustrie zu einem subventionsgetriebenen Boom verholfen, aber andere Innovation auf breiter Front verhindert.

Von den Regierungen begeistert unterstützt wegen der Chance, die Besteuerung und Abgabenbelastung von Energie, Verkehr und anderen umweltrelevanten Faktoren radikal anzuheben, hat diese Politik die direkten und indirekten Mobilitäts- und Transaktionskosten so stark erhöht, das sich Europas enormes Wachstums- und Integrationspotential ins Negative gewendet hat.

Deutschland ist zwar noch in der Illusion des wachsenden Wohlstands und der eigenen Exemplarität befangen, ist aber bereits in eine lange Phase der wirtschaftlichen Stagnation und des Niedergangs eingetreten. Wie eine Generation früher im Fall Japans wird dies den Abschied von den eigenen Überlegenheitsvorstellungen erzwingen.

Die extreme Überalterung der Gesellschaft, das Fehlen wirksamer Leistungsmotivation für die wenigen verbleibenden Jugendlichen, die strukturelle Unfähigkeit, Expertise und Erfahrung der Älteren und der Zuwanderer wirtschaftlich zur Entfaltung zu bringen, sowie der im internationalen Vergleich besonders besorgniserregende Integritätsverfall des deutschen Bankensektors lassen kaum Hoffnung auf Besserung zu.

Anders als Japan genießen Deutschland und seine Nachbarländer nicht das Privileg insularer Distanz. Europa ist ein vergleichsweise offenes Feld für bewaffnete Kräfte. Europas Gesellschaften sind ein weiches, kaum schützbares und gegenwärtig sogar kaum schutzwilliges Ziel für böse Menschen, die für sich selbst Vorteile aus dieser Verletzlichkeit ziehen wollen.

Strategische Lage, Teil 5: Rüstungsnotstand

Für die Verteidigung, noch mehr für die Rüstung, und noch viel mehr für die zukunfts- und praxisorientierte Rüstungsforschung verheißt diese absehbare wirtschaftliche Misere ohne Wenn und Aber: Es ist kein Geld da. Die real existierende Rüstungsmaschinerie ist ein Groschenschlucker, der ohne stete Zufuhr erheblicher Geldmengen in Winterstarre fällt und sich dann plötzlich ins Nichts auflöst. Es geht nicht mehr so weiter bis bisher.

Und das zu einer Zeit, in der sowohl das kolumbianische Szenario territorial ausgreifender Gangsterbanden als auch das biblische Szenario religiös verbrämter Mordzüge bedrohlich nahe an das Europa der Gegenwart herangerückt sind.

An Stelle der abstrakten und manchmal etwas weit hergeholten Bedrohungen der Ost-West-Vergangenheit besteht jetzt die greifbare Gefahr, dass Landesverteidigung nach Steinzeitart wieder notwendig und dringlich wird. Wenn möglich sollten wir uns aber bitte in die Lage dazu versetzen, dieser Gefahr mit geeigneten, unsteinzeitlich überlegenen Mitteln zu begegnen.

Ist Deutschland dafür gerüstet? Trotz einer unendlich scheinenden Kette von "Reformen" ist die Bundeswehr in Kern und Wesen noch immer dieselbe wie in der Zeit des Ost-West-Antagonismus geblieben. Die großen Rüstungsprogramme, die heute abgearbeitet werden, reichen noch in jene längst vergangene Epoche zurück.

Das deutsche Rüstungswesen existiert in einer ganz eigenen Welt der Bestandswahrung, Leisetreterei, Vetternwirtschaft und einem ebenso engstirnigen wie aussichtlosen Insistieren auf nationaler Selbstbehauptung gegen die vermeintliche Rivalität anderer Nationen. Als unlängst nach 30 Jahren gemächlicher Bedenkzeit endlich die Entscheidung zur Gemeinsamkeit mit Frankreich in der satellitengestützten Bildaufklärung fiel, brach sogleich Empörung los, da Deutschland ja bekanntlich alles besser alleine machen kann – es aber halt nicht tut.

Der traditionelle Geheimschutz im Rüstungssektor hüllt Alles in eine zwar sicherheitspolitisch weitgehend sinnentleerte und volkswirtschaftlich kontraproduktive, aber korporatistisch und protektionistisch willkommene Nebelwand ein, hinter der man wie gewohnt unter sich bleibt und neue Konkurrenz gleich gar nicht erst ins Bild rücken kann.

Essentielle Neuerungen wie Vernetzung, Fernwirkung und die entscheidende Rolle von exzellent ausgerüsteten und informierten Kämpfern wurden verschlafen oder auf die lange Bank geschoben. Die nicht in den bequemen Konsens loyal einstimmenden Köpfe wurde abgesägt - natürlich stets auf die feine, unblutige Art.

Nur ein Neuanfang an Haupt und Gliedern kann hier helfen. Es fehlt nicht an Wissen, Können und Wollen. Es fehlen Institutionen, die zeitgemäß zielgerichtet handeln können. Mehr dazu später.

Strategische Lage, Teil 6: Bedrohung

Ein islamistischer Napoleon könnte schon heute weitgehend ungehindert in das Herz Europas vordringen. Der beste einstweilen noch partiell wirksame Schutz dagegen besteht im Moment aus der Durchdringung islamistischer Bewegungen durch Agenten der interessierten Regierungen bzw. Ex-Regierungen der Region, die sich im Streit oft gegenseitig zu neutralisieren scheinen.

Wenn es zu einer wirklichen islamistischen Massenmobilisierung durch eine charismatische Persönlichkeit kommt, können rasch alle Dämme brechen. Alle anderen sinnvollerweise denkbaren Bedrohungen der absehbaren Zukunft lassen sich abhalten, wenn die Fähigkeit zur Abwendung dieser militärischen Hauptbedrohung geschaffen wird.

Neudefinition von Rüstung

Der Modus des Rüstungsbetriebs beruht auf der Grundannahme, dass er separat vom zivilen Technikbetrieb ganz spezielle Fähigkeiten schafft. Dieser Gedanke führt aber heute in fataler Weise die Irre. Militärtechnik ist schon seit zwei Jahrzehnten nicht mehr Vorreiter, sondern hinkt in fast jeder Hinsicht hinter den zivilen Konsummärkten zurück, gerade in einstigen Glanzdomänen wie Elektronik und Materialforschung.
Statt überlegene zivile Technik rasch zu übernehmen und die kurzen Innovationszyklen ziviler Technik zu nutzen, werden weiterhin Rüstungsprogramme mit einem Zeithorizont von 15-30 Jahren bis zur Einführung verfolgt. Statt die Bugwelle überkommener, nicht mehr zeitgemäßer Plattformbeschaffungen ins Leere laufen zu lassen, wird sie gemächlich abgewurstelt, während sich die Soldaten im Einsatz einstweilen mit ihrer mitgebrachten privaten Ziviltechnik ums Überleben bemühen.
Es empfiehlt sich, dieses gescheiterte und perspektivlose Rüstungssystem durch ein neues zu ersetzen, das folgenden Prinzipien folgt:

- Entwicklung und Erprobung neuer technischer Mittel mit möglichem Wehrbezug sind sehr wichtige gesamtgesellschaftliche Aufgaben.
- Es ist nicht die Aufgabe des Rüstungswesens, für die Subsistenz von Grundlagenforschung und industriellen Strukturen bestehender Rüstungsbetriebe zu sorgen.
- Im Normalfall wird greifbare zivile Technik genutzt, um militärisch taugliche Produkte, Systeme, Infrastrukturen und Dienstleistungen zu realisieren.
- Rüstungsforschung und -entwicklung ist integraler Bestandteil der auf unternehmerische Erfindungs- und Umsetzungskraft vertrauenden Innovationspolitik, die vor allem bestehende Hürden für agile, kooperative Innovation aus dem Weg räumt und staatliche Risikoübernahme in kritischen Projektphasen auf möglichst unbürokratische Weise anbietet.
- Dazu gehört die Bereitstellung des möglichst kostengünstigen und barrierefreien Zugangs zu technischen Informationen und zur gemeinsamen Nutzung von Test- und Zertifizierungseinrichtungen.
- Öffentlichkeit und Transparenz der Rüstungsmaßnahmen sind Vorbedingungen für ihren Erfolg. Seltene Ausnahmen mag es geben, wo es um wirklich kriegsentscheidende Neuerungen geht. Der Schutz von Patenten und industriellen Geheimnissen ist nicht Aufgabe der staatlichen Rüstungspolitik und rechtfertigt keinen Geheimschutz-Protektionismus.
- Offene Wettbewerbe und eine Kultur spekulativer Projektinvestitionen zur Entdeckung und Anregung leistungsfähiger Teams sind zentrale Elemente. Die Grundannahme muss sein, dass die wirklich entscheidenden Akteure der zukünftigen Rüstungslandschaft bislang nicht Teil derselben sind.
- Maßnahmen sind in der Regel auf möglichst rasch und frei vergebene Verträge kurzer Laufzeit und relativ niedrigen Einzelwertes zu stützen. Dies dient dazu:
  - Verschwendung durch Scheitern langlaufender Projekte bei Ablauf zu verhindern
  - Verteuerung und Risikoanhäufung durch veränderte Anforderungen während der Laufzeit zu vermeiden
  - die Notwendigkeit laufender intrusiver Projektkontrolle zu minimieren und zeitraubende Ablenkung von der eigentlichen technischen Aufgabe zu vermeiden
  - Festpreiskontrakte und Vorauszahlungen zu ermöglichen, um neue agile Akteure für wehrbezogene Innovationsmaßnahmen zu interessieren und sie dazu wirtschaftlich zu befähigen.
  - Gleichzeitiges Verfolgen unterschiedlicher Lösungsansätze anzuregen und so zu einem lebhaften Innovationsmarkt beizutragen, der einen tragfähigen Ausgangspunkt für rasche Aufwuchsfähigkeit im Ernstfall bereitstellt.
- Maßnahmen sind nicht national, sondern zumindest EU-weit angelegt, um auf eine ausreichend leistungsfähige, breite Basis zugreifen zu können, die sich im Leistungspotential zumindest in Teilaspekten mit den USA messen kann.
- Dies erfolgt (außer in der eigentlichen Beschaffungsphase von Waffensystemen) nicht auf der Basis zwischenstaatlicher Abmachungen, sondern nach den Regeln des europäischen Binnenmarkts unter Beachtung relevanter Begrenzungen staatlicher Beihilfen.
- Das Projektmanagement sollte möglichst unabhängigen, unternehmerisch agierenden kleineren Unternehmen übertragen werden, die im Zusammenwirken mit besser ausgestatteten, aber weniger agilen Partnern eher für greifbare Erfolge sorgen können als das übliche Matrixmanagement in Großunternehmen, das regelmäßig an hinderlichen und schädlichen internen Fehlallokationen leidet.

Wie eine solche neuartige Rüstungspolitik institutionell im deutschen öffentlichen Dienst verankert werden kann, ist nicht erkennbar. Ausbildung und gewohnte Verhaltensweisen sind in der Regel zu weit von den Tugenden entfernt, die diese Politik verlangt.
Als Ausweg bietet sich eine außerhalb der staatlichen Hierarchieordnung angesiedelte gemeinnützige Struktur aus einem Bündel thematisch aufgeteilter Aktionszentren für rüstungsrelevante Innovation an. Diese wird von temporär rekrutierten Mitarbeitern betrieben, welche hohe Einsatz- und Risikobereitschaft und persönliche Verantwortung für die erfolgreiche Umsetzung ihrer gestellten Aufgabe bieten und dafür gut bezahlt werden.

Als zentrales Rekrutierungskriterium sollte gelten, dass vor allem jene sich für diese Aufgabe eignen, denen im bisherigen Rüstungsbetrieb sowohl amtsseitig als auch in der Wirtschaft der Einstieg verwehrt geblieben wäre, weil sie zwar sehr befähigt sind, aber ihr Ausbildungs- und Karriereweg nicht konventionell und geradlinig genug ist.

Im Verständnisses von Rüstung als gesamtgesellschaftliche Aufgabe ist es Sinn und Zweck dieser neuen Struktur, quer durch die deutsche und europäische privatwirtschaftliche, wissenschaftlich-technische und militärische Landschaft fruchtbare Verknüpfungen herzustellen und diese wo sinnvoll gezielt für praktische Zwecke zu ermächtigen und zu alimentieren.
Der beschriebene Ansatz würde Deutschland in die Lage dazu versetzen, dem neuen "Framework-Nation"-Konzept der NATO in der Wehrplanung die nötige Dynamik zu verschaffen, um den angestrebten gemeinschaftlichen Neuanfang im Bündnis als innovativer Vorreiter wirklich mit Leben zu erfüllen.

Neubestimmung des Ausrüstungsbedarfs

Dies ist nicht der Ort, um den tatsächlichen Bedarf an Rüstungsmaterial und –Infrastruktur der näheren und mittleren Zukunft herzuleiten. Exemplarisch lassen sich aber selektiv einige Lücken wie die folgenden nennen, für die es gegenwärtig weder eine Heimat noch ernsthafte Triebkräfte in der Rüstungsmaschinerie gibt:

- leichte bemannte und unbemannte Flugzeuge, die komplett mit Bewaffnung bzw. Ausrüstung, Vernetzung und Systemunterstützung weniger als 5 Millionen Euro pro Stück kosten, mit Schwerpunkt auf der Fähigkeit zum Angriff auf Bodenziele sowie gesicherte Überlegenheit bei der vernetzten Lagebildgewinnung über große Räume. Existierende zivile Plastikflugzeuge könnten sich hier für die Rüstungsbasis der Zukunft als weitaus wichtiger erweisen als elend teure Kampflugzeuge der letzten (oder doch wohl eher vorletzten) Generation.
- eine vervielfachte Anzahl im harten Einzelkampf geschulter und laufend trainierter Männer und Frauen, so gut mit Mobilitätselektronik und ausgerüstet und entsprechend ausgebildet, um im losen Verbund weiträumig vernetzt und flexibel einsetzbar zu sein
- gesicherte schnelle Luftbeweglichkeit von Truppen mit Hilfe einfacher, robuster Luftfahrzeuge unterschiedlicher Art und Größe, einschließlich Luftlandetruppen
- flexibel schaltbare Fernmelde- und IT-Schnittstellen, um bei Bedarf alle verfügbaren Kommunikations- und Vernetzungswege zur Einsatzunterstützung nutzen zu können - egal ob zivil oder militärisch, eigen oder fremd
- geeignete, flexible Mittel in ausreichender Zahl mit optimierten Fähigkeiten gegen unkonventionelle Gegner zum Schutz der Seewege und Küsten in den europäischen Randmeeren (einschließlich maritime Lufthoheit). Dies erfordert andere Schiffstypen und Operationsweisen als bisher angenommen.
- Fähigkeit zur "Befestigung" von Orten und Räumen gegen feindliche Eindringlinge unter intelligenter Nutzung neuer Technologien
- Abwehrfähigkeit gegen relativ primitive Raketen kurzer und mittlerer Reichweite.

Zusammenfassung

Um Deutschland im Verbund mit seinen Verbündeten in EU und NATO angesichts der erkennbaren neuen Bedrohungsformen wehrfähig zu halten, ist ein umfassender, tiefgreifender Umbruch im öffentlichen und privatwirtschaftlichen Rüstungswesen erforderlich.
Als bahnbrechende neue Lösung bietet sich eine außerhalb der hierarchischen Zwänge des öffentlichen Dienstes angesiedelte, thematisch verteilte Gruppe gemeinnütziger Organisationen an, die unternehmerisch die jeweils benötigten, aus anderen Quellen herangezogenen Faktoren zusammenspannen, um so effizient wie möglich selbstgesteckte Aufgaben des rüstungsbezogenen Ingenieurswesens durch agiles Projektmanagement zu lösen.

Eine solche Innovationsagentur wartet nicht als Bedarfsdecker darauf, bis der Bedarfsträger weiß, was er wollen sollte, und dies dann auf ewig festschreibt, ohne dass er weiß, was sinnvollerweise geeignet, machbar und erschwinglich ist. Vielmehr werden Produkte und Systemleistungen geschaffen und angeboten, die dann rasch verfügbar gemacht werden können, wenn sie dringend gebraucht werden. Angebot und Nachfrage erhalten somit eine Chance, sich gegenseitig zu steuern, was als ein Optimierungsrezept für Kosten und Qualität wohlbekannt ist.

Es ist klar, dass ein solcher Neuanfang auch mit Risiken verbunden ist. Die zugrundeliegenden andersartigen Regeln und Werte müssen sich erst durchsetzen. Es wird Fehlschläge und Missbrauchsversuche geben. Der beschriebene Ansatz ist jedoch so gestaltet, dass dies jeweils frühzeitig erkannt und abgestellt werden kann und möglichst wenig bleibenden Schaden zur Folge hat – anders als die Fehlentwicklungen im gegenwärtigen Rüstungssystem.

Der Verfasser ist Gründungsmitglied der pmg. Er leitet seit 2002 sein eigenes Beratungs- und Projektmanagementunternehmen Knowledge & Analysis mit Sitz in Großbritannien. Davor war er als in der Sicherheits- und Strategieforschung bei IISS, SWP und DGAP tätig.

Klaus Becher

Klaus Becher ist Gründungsmitglied der pmg. Er leitet seit 2002 sein eigenes Beratungs- und Projektmanagementunternehmen Knowledge & Analysis mit Sitz in Großbritannien. Davor war er in der Sicherheits- und Strategie-forschung bei IISS, SWP und DGAP tätig.
Der Beitrag gibt die persönliche Auffassung des Autors wieder.

THEMEN

Autonomous Warfare – A Revolution in Military Affairs

Introduction

The world is on the cusp of an epochal shift from an industrial to an information based society and this is having a fundamental impact on the way war is conducted and what technologies are becoming available to the Military.

The fundamental nature of war remains immutable. As Carl von Clausewitz characterized it "war is essentially an interactive clash or two-sided due (Zweikampf)l between independent, hostile, sentient wills dominated by friction, uncertainty, disorder and highly nonlinear interactions". Nothing alters the fact that war is a human endeavor, with decidedly deadly consequences for all involved. New technology does not make war more clinical, it makes it more deadly. What technology does do is to make the battlefield more complex.

Public debate is heating up over the future development of lethal autonomous weapon systems. Some advocate a complete ban on any further development, others a more gradual development and evolution of codes of conduct based on traditional legal and ethical principles governing weapons and warfare. On the other hand, there will always be those who will develop and deploy such future systems with scant regard of ethics and legality.

Previous Revolutions in Military Affairs

The systematic study of technology's' impact on war is a relatively new phenomena. The definitive work is perhaps van Creveld`s "Technology and War: From 2000BC to the Present". In his book van Creveld divides military history into four eras: "Age of Tools", "Age of the Machine", Age of Systems" and "Age of Automation". During the "Age of Tools", which lasted until around 1500 AD, most technology was driven primarily by muscles of humans or animals. The "Age of the Machine" was defined by greater professional skills and the substitution of firepower mass rather than manpower mass. In the "Age of Systems" the emphasis shifted to the integration of technology (machines) into complex networks. This era culminated in World War 2 with the innovative application of aviation, ground forces and communication technology.

Since 1945 the importance of systems has taken a great leap forward and has culminated in the Age of Automatisation. This era culminated in the Persian Gulf War, where the United States and her allies overwhelmed the world`s fourth largest army in remarkably short time with insignificant casualties and loss of equipment. That conflict was dominated by the use of guided munitions and unmanned systems. Many of the deployed system were automated, but all required human input during at least one stage of deployment. All the deployed systems had been around in one form or another for a good period of time and were - simply put - further developments of legacy systems. Aircraft used in the conflict were 4th rather than 3rd Generation, the Main Battle Tanks improvements on those developed to counter the Soviet threat, much as the Artillery was a refinement of a similar development dating back to the 1950s.

The Age of Autonomous Systems

We are now entering an entirely new era of Warfare which will be dominated by unmanned and autonomous systems. Such systems will replace existing unmanned air, sea and ground vehicles in all physical operating domains and across the full range of military operations. Such a regime has the potential to change the concept of defense strategy and will have a profound impact on how decision makers consider decisions about the use of force. It is sure to trigger debates regarding operational concepts, the relationship between offensive and defensive military strategies and the ethical and moral implications of deploying such systems. The debate over the use of armed UAVs continues to dominate discussions about the future of Warfare. Only few nations have deployed such systems and many Governments and political parties reject the use of such systems on moral grounds. Future systems will not only be unmanned, they will have no human in the decision making loop at all. It is understandable, that the use of autonomous UAVs and other systems such as autonomous land and sea systems is divisive in the extreme.

The principles of "Just War" are the basis of ethics and law that govern armed conflict and they can accommodate the use of such autonomous systems currently under development. Under the laws of war, appropriate use of force is judged not only by assessing the results of force, but also by the proportionality of employing that force. A UAV might kill a non-combatant on the battlefield, which is tragic. However, if such force had been deemed to be proportional according to the situation and threat, the death would be both morally and legally acceptable. If autonomous systems are programmed to act according to the laws of war, such systems pose no new ethical dilemma if deployed on the battlefield.

The Drivers of Autonomous Systems

The main drivers of this Age of Autonomous Systems is the recognition that the dominance enjoyed by the United States up until the early 2000s in the area of high-end sensors, guided weaponry battle networking, cyberspace systems and stealth technology has started to erode. The reason for this development is the shift from government-directed security research and development to the private sector. Companies focused on producing consumer goods and business-to-business services are driving key enabling technologies such as advanced computing, big data handling, autonomy, artificial intelligence, miniaturization, nano technology and high density power systems. All these developments can be exploited by clients to build increasingly sophisticated and capable weapons systems. Some of the clients are defense companies outside the US.

A further driver is the continued development of guided munitions. Such weapons trace their origin back to the Second World War and came in the form of guided conventional weapons that actively corrected their trajectories after release. In 1943 German submarines first used passive acoustic homing torpedoes sinking several merchant ships in the process. For the first time such weapons demonstrated accuracy regardless of the range and could be fired beyond the range of the defenders counter measures. A parallel development was the concept of battle networks as demonstrated in 1940 during the Battle of Britain. The development of Radar and the establishment of a rudimentary command, control and coordination network took surprise and chance out of the equation and allowed the outgunned and outnumbered RAF to effectively counter German attacks.

Following World War Two the combination of guided weapons and battle networks spurred tactical and technological improvements in all operating domains. This culminated in the development of bombs and missiles with reliable Global Positioning System and internal navigating systems which could be deployed day or night and in all weather conditions. During Operation Iraqi Freedom the percentage of guided weapons rose to nearly 65%of all munitions expended.

This development has not gone unnoticed by countries such as China and Russia. They too have developed state of the art munitions and systems and are exporting these to their client states. At the same time they are also developing advanced cyber warfare tools and counter-stealth technologies designed specifically to exploit perceived vulnerabilities in existing western systems. Such countermeasures are designed to cut lines of communication between operator/controller and weapon, be it manned or unmanned. It is this threat which is leading to the development of autonomous systems.

A driver in the development of autonomous systems which should not be ignored is demographic changes in the West which will result in fewer recruits being available to join the armed forces. German population, for example, is set to decline from 82 Million to 75 Million by 2050 and the average age of the population will be 50. This trend (fewer and older) has already had an impact on the cost of personnel. In the United States the average pay and benefits for the armed forces has risen from $ 44.200.- in 2001 to $ 81.600.- in 2013 – an increase of 85%. It is estimated that some 50% of the total defense budget of the US is wage related. Clearly the introduction of autonomous systems will serve to reduce the proportion of money spent on employing and retaining personnel.

The final driver of autonomous systems is the rapid advancements in computing, big data management and miniaturization. The fusion of advanced computing and data management with sensor technology has enabled platforms to become more aware of their environment and interact with it in the absence of human control.

Current Autonomous Weapons

Current autonomous weapon systems have autonomous modes, and therefore only operate autonomously for short periods. They are also constrained in the tasks they are used for, the types of targets they attack and the circumstances in which they are used.

The development of the Brimstone air to ground missile is a good illustration of how autonomous weapons evolve. Brimstone was originally designed as a “fire and forget” weapon against formations of armored vehicles using a millimetric wave active radar homing seeker to ensure accuracy against moving targets. Experience in Afghanistan led to the addition of laser guidance thus allowing the operator to distinguish between targets in in order to reduce the possibility of civilian casualties. Brimstone can be programmed by the operator to adapt to specific mission requirements and thus gives the weapon the ability to distinguish between targets and to self-destruct if it is unable to find a target in the designated area. Brimstone has an autonomous target selection capability once released from the aircraft and has the capability to determine where on a target best to impact causing the most damage.

Brimstone was used extensively during Operation Ellamy over Libya in 2011 and currently by the Royal Air Force over Iraq. In all over 120 missiles were fired over Libya with a success rate of 98%. The missile has been tested on a MQ-9 Reaper, the first time an autonomous weapon has been fired from a remotely guided platform.

In April 2015 the Office of Naval Research in Arlington announced that it had tested its LOCUST UAV Swarming Technology programme. The LOCUST programme includes a tube-based launcher that can launch low-cost UAVs in rapid succession. The breakthrough technology then utilizes information-sharing between the UAVs, enabling autonomous collaborative behavior in either defensive or offensive missions. The demonstrations took place in multiple locations in the spring of 2015 during which up to 9 UAVs worked together completely autonomously in synchronized flight. The LOCUST programme uses three-foot long Coyote drones made by BAE Systems which are electrically powered and weigh around 15 pounds. The UAV has a cruising speed of 60 knots and a dash speed of 85 knots and can operate at altitudes of up to 20.000 feet. The Navy is now planning a ship-based demonstration in 2016 using up to 30 swarming UAVs.

There are today a wide range of missile defensive systems which can be described as operating autonomously. The Phalanx close in weapon system is in active service with 25 navies and was first deployed in 1980. The Aegis combat system was introduced in 1983 and Patriot in 2002. There are furthermore a number of ground vehicle active protection systems in operation or under development. Such systems are designed to detect and intercept missiles, rockets (RPGs) or artillery rounds before they impact on the target. Such systems are out of the loop of human control given the extremely short response times required to neutralize the threat. The SHARK Active Protection System developed by Thales and IBD Deisenroth Engineering is a good example of such systems. A combination of radar and optronic sensors detects threats at very short ranges and destroys incoming fire by releasing a pyrotechnical charge. The incoming round disintegrates and the remaining energy is absorbed by the armor of the vehicle. Similar systems have been developed by KBP Instrument in Russia, Artis and Raytheon in the United States and Rafael in Israel.

The Definition Problem

There is no internationally agreed-upon definition for an autonomous weapon which complicates the debate on this topic. From a common sense perspective, it makes sense to define an autonomous weapon as one that selects and engages targets on its own, and a semi-autonomous weapon as one where a human is selecting the specific targets for engagement. Given that definition it becomes clear, that there are today only very few truly autonomous systems in operation. Such systems are currently defensive and can be described as being human-supervised with physical access to the system if necessary.

It is also becoming apparent, that the above common sense definition is not sufficient in setting exactly where the line is between autonomous and semi-autonomous weapon systems. In order to define more clearly, a further definition might sharpen the distinction between autonomous and semi-autonomous systems, a human-supervised autonomous system. Thus the above described Brimstone missile would fall into this category, as the operator makes a decision to engage a specific target or not. In the case of an autonomous system, however, the operator makes a decision to launch a weapon to seek out and destroy a general class of target over a wide area, but is not taking a decision about which specific targets are to be engaged. The LOCUST project would seem to fit the definition of a truly autonomous system.

Conclusion

Rapid technological advances and changing threats mean that capabilities that today seem impossible will come to fruition much sooner than we realise. Remotely controlled vehicles on ground in the air or in water will soon be replaced by increasingly autonomous operating systems. The Franco-German plans to develop a “new” MALE-UAV for operational use in around 10 years’ time is a step in the wrong direction, unless such a system can perform its intended operations in an autonomous mode. The current political view, at least in Germany, is however to ban autonomy in future weapons without any clear evidence that such systems are harmful. In fact, human- supervised autonomous systems such as Brimstone have actually reduced civilian casualties in war. Brimstone was developed precisely with this in mind.

In the heat of battle, technical indicators have, at times, proven more reliable than human judgment. In 1988, for instance, the USS Vincennes shot down an Iranian airliner after the crew believed the aircraft was descending to attack. In fact, computers on board accurately indicated it was ascending to pass-by harmlessly. In the case of the USS Vincennes the human operators overrode the automatic Aegis system and created a human and diplomatic disaster.

The incremental development and deployment of autonomous weapon systems is inevitable, and any attempt at a global ban will be ineffective in stopping their use by those states whose acquisition of such weaponry would be most dangerous. For this reason, the United States and some other Western allies will continue to develop and increasingly deploy autonomous weapon systems. Some view this emergence of autonomous weapon systems as a crisis for the law and for the ethics of war. Provided we start now to incorporate legal and ethical norms adapted to weapons that incorporate emerging technologies of automation and autonomy, the incremental movement to autonomous weapon systems can both be regulated and made to serve the ends of law on the battlefield of the future. Autonomous systems both in civilian life and on the battlefield are here to stay, as uncomfortable that fact might be to the general public.

Maxim Worcester

Maxim Worcester is Managing Director of German Business Protection GmbH (GBP), a Berlin-based security consultancy. He has previously worked for the Economist Intelligence Unit, Frankfurter Allgemeine Zeitung, Control Risks and KPMG.
Opinions expressed in this contribution are those of the author.

THEMEN

Crisis in Ukraine – The Emergence of Hybrid Warfare

1. A Black Swan has emerged

„Europe has never been so prosperous, so secure nor so free. The violence of the first half of the 20th Century has given way to a period of peace and stability unprecedented in European history.“[1] These opening sentences of the European Security Strategy of 2003 have become history. A black swan has emerged. The crisis in Ukraine has altered the security status quo. Suddenly, the rivalry between East and West is back.

When on Sunday March 2, 2014, in the Crimea soldiers without insignia – whom Ukrainians referred to as ‘little green men’ – began to occupy important buildings, including barracks and town halls NATO ambassadors of the 28 Member

[1] European Security Strategy, Brussels 2003

States in Brussels would sit for hours and ask themselves: Who are these *"green men"* setting up roadblocks on the Ukrainian peninsula? What is happening to the Russian military bases? What is happening in the Crimea? The smoke disappeared. The *"green men"* turned out to be Russian soldiers. Vladimir Putin announced before Parliament in Moscow the return of the Crimea to the homeland.

The Russian general staff has been preparing for Ukraine-type hybrid operations for years. Long before the Ukraine crisis there were manoeuvres in several military districts. Particularly the Russian military's *ZAPAD 2013* exercise[2] involving more than 75,000 troops proved to be a kind of rehearsal for parts of the Ukraine campaign. Consequently, the Russian military played its well-orchestrated role.

In Mid February 2015 there were approx. 15,000 Russian troops on Ukrainian territory backing up approx. 30,000 illegally armed formations of separatists in eastern Ukraine. These units were well equipped with superior body armour and body armour piercing ammunition, which can easily defeat normal infantry when combined with night vision and snipers. Artillery and multiple-rocket launchers utilize advanced munitions, which in combination with RPV/UAV target acquisition caused 85% of all Ukrainian casualties and can take battalion size units out of action in one strike.

Russian modern overlapping dense air defence drove opponent Close Air Support and Attack Helicopters off the battlefield, particularly as sophisticated ECM and air defence suppression was not available for the Ukrainian troops. UAVs, drones & RPVs ensure front-end operational intelligence and tactical targeting. Electronic warfare means – including high-power microwave systems – jammed not only the communications and reconnaissance assets of the Ukrainian armed forces but to also disabled the surveillance unmanned aerial vehicles operated by monitoring teams from the Organisation for Security and Co-operation in Europe (OSCE).

Former NATO Secretary General, Anders Fogh Ramussen sees Russia engaged in a hybrid war and has warned that "*Russia has adopted this approach and it is a mix of very well-known conventional warfare, and new, more sophisticated propaganda and disinformation campaigns including efforts to influence public opinion through financial links with political parties within NATO and engagement in NGO's…"*[3]

Russia's hybrid campaign in the Ukraine appears to be achieving Moscow's desired results.[4] Flooding the region with illegal weapons, using mercenaries to destroy regional infrastructure, weakening local economy, blocking state functions, in particular law enforcement, justice, social welfare, causing a refugee crisis, exploiting social media & information warfare and introducing own peace keeping forces proved to be effective. The core message that has come along with the hybrid campaign is: While traditional combat still remains a possibility, it will no longer be the primary means to victory on the battlefield of the 21st century.[5]

2. Hybrid War

"Hybrid warfare has been defined as a combination of conventional, irregular, and asymmetric means, including the persistent manipulation of political and ideological conflict, and can include the combination of special operations and conventional military forces; intelligence agents; political provocateurs; media representatives; economic intimidation; cyber attacks; and proxies and surrogates, paramilitaries, terrorist, and criminal elements."[6] Hybrid war involves multi-layered efforts designed to destabilise a functioning state and polarize its society.

Hybrid war appears vaguely connected. In fact, the pieces are a part of a whole. It is a war that appears to be an incomprehensible sequence of improvisations, disparate actions along various fronts – humanitarian convoys followed by conventional war with artillery and tanks in Eastern Ukraine, peacekeeping operations in Transnistria, cyber-attacks in Estonia, vast disinformation campaigns on mass media, seemingly random forays of heavy bombers in the North Sea, submarine games in the Baltic Sea, and so on. Hybrid tactics reflect an order behind the spectrum of tools used. That makes it incumbent upon political leaders and strategic thinkers to fit such activities accurately within the political objectives discussed by Carl von Clausewitz, who underlined that war was an extension of politics by other means. In thinking through the ongoing hybrid campaigns, it is important to understand that "*hybrid*" refers to the means of war opposed to the principles, goals, or nature.

Clausewitz sees war as a chameleon and such a chameleon is hybrid war. It is a potent, complex variation of warfare. What is making it so dangerous is the rapidity with which one can escalate a conflict in the digital world. Consequently, a broad politico-military debate has started, whether a new form of warfare appears to have been born.

a. The "ISIS" model

When ISIS made its way across western Iraq, observers described it as "*hybrid warfare*". The same happened, when Ukrainian rebels seized control of Crimea and various cities throughout south-

[2] Pauli Järvenpää, Zapad-2013, A View From Helsinki, Washington, DC August 2014, www.jamestown.org/uploads/media/Zapad_2013_View_From_Helsinki_-_Full.pdf (Accessed: 17 May 2015)

[3] Damien Sharkov. Russia Engaging in 'Hybrid War' With Europe, Says Former Nato Chief. Newsweek. April 15, 2015 8:01 AM ED www.newsweek.com/2015/04/24/former-nato-chief-says-europe-hybrid-war-putin-322293.html

[4] Reuben F Johnson: Russia's hybrid war in Ukraine 'is working', - IHS Jane's Defence Weekly, Kiev, 26 February 2015

[5] Jordan Bravin. Getting behind Hybrid Warfare. CICERO Magazine. July 17, 2014. ciceromagazine.com/essays/getting-behind-hybrid-warfare/

[6] Robert A. Newson, Counter-Unconventional Warfare Is the Way of the Future. How Can We Get There? In: Janine Davidson Blogspot: Defense in Depth. October 23, 2014. blogs.cfr.org/davidson/2014/10/23/counter-unconventional-warfare-is-the-way-of-the-future-how-can-we-get-there/ (Accessed: 17 May 2015)

eastern Ukraine. In the past months in Europe there has been a split on which kind of hybrid challenges to focus on. Within NATO and the European Union, Northern members such as the Baltic States, Poland and German think with view to hybrid warfare immediately of the "Russian" model. Whereas Italians, French, Greeks or Spanish see the "ISIS" model at least as threatening.

A decade ago ISIS emerged as a small Iraqi subgroup of Al Qaeda specialized in suicide bombings. Today ISIS has conquered cities and wide territories in both Syria and Iraq. The movement draws its strength from Sunni Arab communities opposed to the Shiite-led government in Baghdad and the regime in Damascus. Former U.S. defence secretary Chuck Hagel called ISIS "*as sophisticated and well funded as any group that we have seen … beyond anything we have seen*" as it includes former military officers who can fly helicopters, spot artillery, and manoeuvre in battle. ISIS is increasingly a hybrid organization, on the model of Hezbollah – part terrorist network, part guerrilla army, part proto-state.[7]

In fact, Hezbollah – the mother of hybrid battle – clearly demonstrated the ability of non-state actors to study and deconstruct the vulnerabilities of Western-style militaries and devise appropriate countermeasures in the war with Israel in 2006. Hezbollah effectively fused militia forces with highly trained fighters and anti tank guided missile teams. It mastered the art of light infantry tactics against heavy mechanized forces. It even demonstrated its ability to hit Israeli naval assets. Also during subsequent operations such as Operation Cast Lead in 2008 and Operation Pillar of Defence in 2012, Gaza groups successfully run a hybrid warfare-type strategy.

With the Syrian Civil War another hybrid warfare case showed up. But, not only has the armed opposition been conducting hybrid concepts. Also the Baathist dictatorship has shaped its violent strategy by utilizing a broad spectrum of hybrid warfare means. A further scene of hybrid warfare has been the Sahel region. A key characteristic of the violent groups in the Sahel region is the fluidity of their leadership and organisational structures. Interpersonal relationships are holding these groups together. Particular complex is the mixed pursuit of the key actors' political agenda with criminal activities. In Somalia, al-shabaab derives a large part of its income from widespread extortion and commission on seizures affected by pirates. In Mauritania and Mali, the battalion led by Mokhtar Belmokhtar has largely financed its activities through cigarette, cocaine and weapons smuggling. In between, hostage taking has become a lucrative activity.

Particular in the Sahel region hybrid war blends the lethality of state conflict with the fanatical and protracted fervour of irregular warfare. In such conflicts, future adversaries such as states, state-sponsored groups, or self-funded actors exploit access to modern military capabilities, including encrypted command systems, man-portable air-to-surface missiles, and other modern lethal systems, as well as promote protracted insurgencies that employ ambushes, improvised explosive devices (IEDs), and coercive assassinations. This could include states blending high-tech capabilities such as anti satellite weapons with terrorism and cyber warfare directed against financial targets. The more non-state actors' access to game changer weapons increases, the more likely it is that hybrid conflicts will spread.

And in fact, ISIS has already arrived at the Mediterranean shores opposing the European Union. In Libya between 1,000 and 3,000 militants are now fighting for the Islamic State cause. The new ISIS affiliates in Libya are the IS Barqa Province, IS Fezzan Province and IS Tripoli. Since the start of 2015, ISIS has carried out a number of attacks and has captured the Mabruk oilfield south of Sirte. The militants also beheaded 21 Egyptian Coptic Christians earlier this year.[8]

Scott Jasper and Scott Moreland conclude in their article on the Islamic State[9] with the observation that "*... the Islamic State is a formidable, but not unassailable hybrid threat...*" and identify six characteristics of hybrid threats:

- Blended tactics: ISIS forces include traditional military units as well as smaller, semi-autonomous cells, combining both conventional and guerilla warfare tactics. They possess a wide array of weaponry, from improvised explosive devices (IEDs) and mines to rocket-propelled grenades (RPGs), drones, and chemical weapons.
- Flexible and adaptable structure: ISIS quickly absorbs and deploys new resources. Whether new recruits, weaponry, or territory, ISIS constantly incorporates new acquisitions into its strategy and structure.
- Terrorism: Through acts of grotesque and exaggerated violence, ISIS communicates its ideology to a wider audience. The slaughter of Yazida and Chaldean Christian minorities, the destruction of religious and cultural icons such as the tomb of the prophet Jonah, and the widely publicized beheadings of Western aid workers and journalists all provoke terror among the Iraqi populace and the world at large.
- Propaganda and information war: ISIS' social media campaigns highlight clear and careful messaging. Each tweet, video, and blog post aiming to glorify and recruit for the ISIS cause. High quality films in multiple languages bring the conflict from the battlefields of Iraq to the viewer's screen. This has clearly contributed to

[7] Steve Coll. In Search of a Strategy. The New Yorker. September 8, 2014 issue. www.newyorker.com/magazine/2014/09/08 (Access: 17 May 2015)

[8] State Department. ISIS capitalizes on Libya security vacuum, establishes 'legitimate foothold'. rt. March 21, 2015. rt.com/usa/242809-isis-threat-libya-security/ (Accessed: 17 May 2ß15)

[9] Scott Jasper and Scott Moreland The Islamic State is a Hybrid Threat: Why Does That Matter?
Small Wars Journal. Dec 2 2014. smallwarsjournal.com/printpdf/18345 (Accessed: 17 May 2ß15)

ISIS' success in recruiting of foreign fighters.

- Criminal activity: ISIS employs a variety of methods to fund its endeavours as it boasts a diverse investment portfolio: black market sales of oil, wheat, and antiquities; ransom money; and good old-fashioned extortion. While donations account for a portion of their funds, ISIS' criminal enterprises ensure that the group is financially solvent.
- Disregard for international law: ISIS has no respect of humanitarian and legal norms. Based on their extreme interpretations of Sharia law, ISIS inflicts violence against women and minorities, including barbaric punishments such as stoning and amputations etc.

b. The "*Russian*" model

The "*Russian*" model of hybrid war is different. Three stages have been identified[10]:

- Destabilizing a country via inspiring domestic conflict;
- Causing state collapse via ruining economy and destroying infrastructure;
- Replacing local political leadership with own operatives as "*invited saviour*".

At one point during the Ukrainian crisis, Russia had more than 55,000 troops lined up on the Ukrainian border. But when it came to sowing instability in Ukraine, it was not conventional forces that were used, but rather unorthodox and varied techniques. The Russian military hierarchy has been remarkably open in describing how it has been applying hybrid warfare in the Ukraine. While the rebels directly engaged the Ukrainian army in the Donbass, the Russian military engaged in training exercises just inside Russian territory. These exercises include the use of space, missile and nuclear forces, Special Forces and conventional military units, and psychological operations teams and political operatives. All branches of Russia military and security services were pulled in, as well as the civilian leadership.

It is amazing how well these non-military instruments of Russia's hybrid concept have been brought to fruition[11]:

- Investments in key sectors of European economies;
- The use of Russian investments, trade, and capital to bribe and influence key economic and political elites;
- Buy up media, support anti-integration and pro-Russian political parties;
- Arms sales to gain influence over military decision-making;
- Large-scale intelligence penetration of European organizations;
- Forging of links between Russian organized crime and local criminal elements;
- Establishment of ties among religious institutions, exploitation of unresolved ethnic tensions and campaigns for "minority rights";
- Large-scale supports for Russian information outlets abroad;
- And massive coordinated cyber strikes on selected targets.

Although the specific features of Crimea and the Donbass may not be replicable elsewhere, it becomes clear that this repertoire of instruments allows Russia in general enormous flexibility in orchestrating relentless hybrid attacks. Russia has learned how to "*tailor*" forces and non-military instruments to the requirements of the theatre or targets, e.g. targeting British finance in the City of London, French arms sales, German oil, gas, and electricity or Balkan media.

As the world's media concentrates on Russia's conventional and nuclear military capabilities, Russia's on-going propaganda element of their 'Hybrid' war in order to silence independent voices has received less focus. Kremlin controlled radio, television and the printed press have become dominant players in Russian life as they greatly shape public opinion and are used to reinforce resentment of the west. The Sputnik News Channel, which is used to spread Russian propaganda, has begun recruiting Estonian journalists. Russia Today has replaced the state owned RIA Novosti along with the Kremlin's international radio station, Voice of Russia. Russian media is once again owned by the state and all communications are shaped according to Putin's political agenda through editors and journalists loyal to the Kremlin.

Apart from controlling news services throughout Russia the Kremlin has also recognize the power of social media to win hearts and minds of young Russians. VK, which was originally named VKontakte, is the largest Russian social network and is available in 17 languages. Launched in 2003, by 2006 it had a revenue in excess of $ US 121.4 million and by 2012 had over 209 million users. Once owned by Maluru.org, this popular social network for users living in Eastern Europe is now owned and controlled by the Kremlin. Many of the account holders who regularly contribute to these pages are either fighting in Ukraine or have recently returned from the conflict. 'Freedom Fighters' discuss their combat experiences in Ukraine and post graphic images of their activities. Since the start of the Proxy war against Ukraine there has been a dramatic increase in the number of account holders living in Russia.

The Russian controlled media show Putin as a masculine, aggressive, clear-language, strong leader. Related imagery, his deliberate poses and photo-shoots can be found on VT, Facebook, Twitter and other social media networks and go down well with his supporters. They go alongside comments about his strength of leadership and capabilities of re-

[10] Karber, Dr. Phillip A. Russia´s Hybrid War Campaign, Implications for Ukraine & Beyond, Washington CSIS 1o March 2015, fortunascorner.com/wp-content/uploads/2015/03/hybridwarfarebrief.pdf (Accessed: 17 May 2015)

[11] Stephen Blank. Russia, Hybrid War and the evolution of Europe. Second Line of Defense. 2015-02-14. www.sldinfo.com/russia-hybrid-war-and-the-evolution-of-europe/ (Accessed: 17 May 2015)

storing the Russian Empire.

Among the key lessons learned to this point are[12]:

- Mixed ethnic societies are particularly susceptible to mass and social media manipulation.
- Prior to conflict, subtle economic influence and the promotion of corruption serve to establish leverage as well as compromise of key politicians and security organisations.
- Political agents, volunteers and mercenaries provide a variety of low visible inserting, sabotage, training and advisory options.
- Terrorist type techniques include building seizures, infrastructure attack, intimidation of police, cyber disruption, political assassination, kidnapping of children, hostage taking, torture and mutilation.
- Low-intensity conflicts that escalate rapidly to high-intensity warfare unveil unpreparedness of police, border guards, security units and even SOF teams to deal with these challenges.
- A variety of subtle and direct nuclear threats, including nuclear alerts and fly-bys reopen the nuclear debate.

Many elements of the "*Russian*" model are not new. Others, i.e. the use of cyber weapons or the use of social networks for propaganda purposes have only become possible with the Internet. Yet, the core capability comes from the orchestration of all small pieces within a comprehensive concept.

To understand the "*Russian*" model one needs to look both at the small pieces and at the overall concept to understand the character and magnitude of the aggressiveness that has come along with it. A key to understanding has become the speech held by General Valery Gerasimov, Chief of the General Staff of the Russian Federation at the annual meeting of the Russian Academy of Military Science in January 2013.[13]

"In the 21st century we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared, and, having begun, proceed according to an unfamiliar template.

The experience of military conflicts … confirm that a perfectly thriving state can, in a matter of months and even days, be transformed into an area of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war …

In terms of the scale of casualties and destruction – the catastrophic social, economic, and political consequences – such new-type conflicts are comparable with the consequences of any real war.

The very "rules of war" have changed. The role of non-military means of achieving political strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.

The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other non-military measures – applied in coordination with the protest potential of the population.

All this is supplemented by 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.

These days, together with traditional devices, nonstandard ones are being developed. The role of mobile, mixed-type groups of forces, acting in a single intelligence-information space because of the use of the new possibilities of command-and-control-systems has been strengthened. Military actions are becoming more dynamic, active, and fruitful. Tactical and operational pauses that the enemy could exploit are disappearing. New information technologies have enabled significant reductions in the spatial, temporal, and informational gaps between forces and control organs. Frontal engagements of large formations of forces at the strategic and operational levels 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.

The defeat of the enemy´s objects is conducted throughout the entire depth of his territory. The differences between strategic, operational, and tactical levels, as well as between offensive and defensive operations, are being erased. The application of high-precision weaponry is taking on a mass character. Weapons based on new physical principals and automized systems are being actively incorporated into military activity.

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…

Another factor influencing the essence of modern means of armoured conflict is the use of modern automated complexes of military equipment and research in the area of artificial intelligence. While today we have flying drones, tomorrow´s battlefields will be filled with walking, crawling, jumping, and flying robots. In the near future it is possible a fully robotized unit will be created, capable of independently conducting military operations."

[12] Karber, Dr. Phillip A. Russia´s Hybrid War Campaign, Implications for Ukraine & Beyond. Washington CSIS 1o March 2015, fortunascorner.com/wp-content/uploads/2015/03/hybridwarfarebrief.pdf (Accessed: 17 May 2015)

[13] This is a rather lengthy quote, but very telling. See Gerasimov, Valery. The Value of Science Prediction. In: Military-Industrial Courier. Moscow. 2013. vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf (Accessed: 17 May 2015)

Gerasimov observed that these methods and such tactics had been used by the United States for decades. Now Russia would fight in the same way. Because of what Russia perceives as an asymmetry of military capabilities and economic strength between herself and the United States including its Western allies, Russia has to be more aggressive and smarter than its opponents in fighting this new kind of war.

3. A chance for NATO and the EU to work together?

Both Russia and IS are exploiting the implied division between the three pillars of NATO's Strategic Concept – realignment of collective defence, crisis management and co-operative security – by destabilising the home political base of Alliance nations upon which NATO defence solidarity is founded. NATO and the EU need to realign initiatives that have not delivered to this point such as Smart Defence, NATO Forces 2020 and the Connected Forces Initiative.[14] Clearly the concept of hybrid warfare needs to be studied carefully and conceptualized. Threats from both strategic directions „East“ and „South” need to be dealt with, and there may even be a third one in Asia.

Russia's actions in and around Ukraine have reinforced the notion that the security environment in Europe is becoming increasingly unpredictable. The steady decline of defence budgets appears to have stopped. In response to the conflict in Ukraine, NATO member nations have decided to develop a set of tools to deter and defend against adversaries waging hybrid warfare. Up to now the NATO approach countering hybrid warfare has been centred on a rapid military response. This approach has weaknesses that need to be addressed. For example member states need to agree on the source of a conflict. This creates a significant barrier to prompt rapid collective action. And even more important, to counter irregular threats, hard power alone is insufficient.

Consequently, NATO will have to develop a more flexible policy, strive to deter or even counter hybrid adversaries with a wide range of instruments. To realize what are not only the possibilities but also the limits of respective instruments of power is an important requirement for purposeful and effective leadership. As the hybrid scenarios cover a hitherto not known broad spectrum of security challenges, this highlights the need for a broad-based approach, using the full range of hybrid warfare agents as those applied by the other side: rapid deployment and special forces; financial and economic measures; defensive and offensive cyber operations; intelligence operations and police investigations; Information and social media campaigns.

As discussed by Russia in its new doctrine the military instrument per se plays only a limited role. Instead all of the instruments of power are employed: diplomacy, information, military, and economic (DIME). The purpose of using these instruments in this synchronized way is to pressure, influence, and destabilize other countries, i.e. destroying or at least permanently weakening regimes that oppose Russian interests. None of these components is new to Europe, but its societies are more vulnerable than ever before as they are deeply integrated. Everything is connected to everything else: economy, diplomacy, finance, military, intelligence, communications, and cyber space. And everything can be damaged or put out of service via hybrid aggression. It is easy and cheap to launch for external aggressors, but it is costly for the defenders.

The combination and orchestration of different actions creates ambiguity, making an adequate reaction difficult, especially for multinational organizations that operate on the principle of consensus. Undoubtedly, hybrid warfare presents NATO with an institutional challenge. The Alliance will need to strengthen cooperation within the own organisation, but also with international organisations, particularly with the EU. By partnering with the European Union and expanding its set of instruments, the Alliance would be in a much better situation to successfully tackle hybrid threats from all necessary angles with a wide range of both political and military instruments at its disposal. The NATO Summit in Wales has already acknowledged the EU as a strategic partner of the Alliance. And the common threat of hybrid warfare within the Euro-Atlantic area presents a solid opportunity to develop this partnership.

Obviously we need not just to pay attention to conventional weapons and irregular tactics, terrorism and organized crime, but also to *non-violent* actions. These include information operations, economic, financial and subversive political acts. As we look at the scope of hybrid warfare this clearly affects the extent to which various government agencies need to get involved and capable of integrated, networked responses to hybrid challenges to security. Adapting to the threat of 'hybrid warfare' will require governments to invest with view to personnel, training and equipment as well as to concepts of operations in a wider array of capabilities and facilitate the comprehensive interaction between them.

Consequently, the Comprehensive Approach that already has been adopted by NATO and the European Union needs to have a central role in dealing with hybrid challenges as it utilizes all the instruments of power: diplomacy, information, military, and economic. The Comprehensive Approach provides a perspective that explicitly focuses operations on political, military, economic, social, infrastructure, and informational effects by using diplomatic, information, economic and military actions.

The core military capability within the Comprehensive Approach is a superior command and control process which – based on a network of governmental and non-governmental expert's knowledge and instruments of power –

[14] Julian Lindley-French. Hybrid Warfare: NATO needs a Stoltenberg Doctrine. Blogspot: lindleyfrench.blogspot.kr/2015/05/hybrid-warfare-nato-needs-stoltenberg.html (Accessed: 17 May 2015)

makes it possible to project national power at an early stage in order to achieve a maximum effect. As a rule, this approach will employ the means best suited for attaining an objective.

With hybrid warfare unpredictability has become a weapon. Are we still in peace, or we are already at war? According to Article 5 of the NATO treaty all Member States can trust in a guaranteed assistance. Each potential aggressor should know: If I attack a country, then I attack the whole alliance. There must be no grey area here. But obviously, grey is the colour of hybrid warfare. For NATO members article 5 marks the threshold of war, the art of an opponent will be to operate below this threshold.

In order to respond to hybrid challenges below the threshold of traditional collective defence first of all Early Warning and Situational Awareness are of key importance. Given the increasing practice of Russian "snap exercises," NATO and the European Union need to increase their situational awareness. Allies and willing partners should continue to work on improving geographical expertise, updating threat assessments, and facilitating closer intelligence cooperation. These assessments should flow into an easy accessible knowledge base and should cover political, economic, and societal influence of hybrid actors that may limit independent action and threaten governmental stability.

Alexander Vershbow, Deputy Secretary General of NATO stated recently: "*Hybrid warfare isn't new. But we have seen it applied in Ukraine with renewed vigour and ingenuity. Hybrid warfare mixes hard and soft power. And so our response should also be multifaceted. NATO and the European Union each have distinct hard and soft power tools. Our challenge is to bring them together so that we complement each other, and reinforce the essential measures taken by our member states.*"[15]

Steps should be taken to help build the capacity of other arms of government, such as interior ministries and police forces, to counter unconventional attacks, including propaganda campaigns, cyber assaults or home-grown separatist militias. NATO and the European Union now should develop a sense of urgency to make DIME work. By building up pre-crisis capabilities to deal with hybrid security challenges, nations will be better able to assign responsibility to an aggressor nation. Civilian and military leadership needs to be better prepared for comprehensive interagency actions. There is an obvious need to establish policies and technologies, procedures and a common knowledge base with the ability to practically share data in a timely manner for integrated operations and multinational information sharing.

4. Dealing with "*grey*" – the new colour of war

Irregular tactics and protracted forms of conflict have mostly be marked as tactics of the weak, employed by non state actors who do not have the means to do better. Instead of weakness, future opponents may exploit hybrid opportunities because of their effectiveness. As we have seen, unlike conventional warfare, the "*centre of gravity*" in hybrid warfare is people – a target population. The adversary tries to influence key policy- and decision-makers by combining kinetic operations with subversive efforts. The aggressor often resorts to clandestine actions, to avoid attribution or retribution. Thus hybrid war is subversive. It is warfare particularly dangerous to multi-ethnic societies. The art of hybrid warfare is not found on front line manoeuvres but rather in the grey zones of security. Grey is the new colour of war.

It could be observed with ISIS and Russia that exploitation of modern information technology has enhanced the learning cycle of hybrid opponents, improving their ability to transfer lessons learned and techniques within theatres and from one theatre to another. Insurgents have swiftly acquired and effectively employed tactical techniques or adapted novel detonation devices found on the Internet or observed from a different source. To successfully meet hybrid challenges will require that decision-makers and first responders, societies and media modify their mind-sets. Success in hybrid wars requires all political, military and civil echelons leaders with decision-making and cognitive skills that enable them to recognize or quickly adapt to the unknown. It requires smart leaders and smart responders with innovative thinking. Organizational learning and adaptation is of importance, also investment in training and education. Knowledge building and situational awareness need to become focus areas – knowledge and situational awareness about the different political, military, economic, social, infrastructure and information domains within the relevant theatre of operations.

Generally, networking national, regional and global knowledge would provide an ideal base to effectively deal with hybrid situations already from the outset. Integrating knowledge-centric architectures, organizations and people would empower innovative learning and leader development for complex security cooperation on a national, regional and global basis. Networking knowledge would promote interoperability empowering security collaboration with friends and partners around the globe.

Of course, organisations such as NATO or the EU need not to start from scratch. The problem is that information or knowledge often resides isolated in the heads and offices of internal or even external subject matter experts. This information and knowledge is not fused, de-conflicted nor shared. Very often it is not available in an electronically retrievable format. Consequently, there is a need to "*connect*" or "*fuse*" existing information, and the processes that are used to develop it, so that decision-makers of all echelons are

[15] Alexander Vershbow, ESDP and NATO: better cooperation in view of the new security challenges
Speech by NATO Deputy Secretary General Ambassador Alexander Vershbow at the Interparliamentary Conference on CFSP/CSDP, Riga, Latvia, 5 March 2015. www.nato.int/cps/en/natohq/opinions_117919.htm (Access: 17 May 2015)

presented with a clear holistic understanding, as early as possible in the decision-making process.

A process of permanent knowledge development would cover the full spectrum from collection, analysis, storage and distribution of information that helps to contribute to a common and shared understanding of the operational environment. This very process needs to provide political, civilian and military decision-makers and their staffs exactly with the broad scope of comprehensive understanding they need with view to complex hybrid challenges, including the relationships and interactions between systems and actors. As hybrid conflicts normally have a pre-history they can principally be recognized at an early stage and are – to an extent – predictable. The crucial problem, however, is the correct assessment of a multitude of information and drawing timely conclusions. Knowledge development needs to provide indications and warning of an emerging hybrid security problem.

Networking knowledge would help organizations to better prepare and operate together against a wide variety of challenges. This would strengthen situational awareness, support collaborative planning[16], and, in particular, help to determine the most appropriate responses. It would provide more comprehensive and adaptive perspectives based upon shared trust[17] in contrast to the compartmentalized thinking of today. It would systematically capture knowledge in ways that support leaders and organizations to work better together. It would make knowledge persistent to organizations and less reliant on temporary access to subject matter experts. And in particular, it would support improved interoperability between actors across a wide spectrum of tasks using agreed-on information formats. In sum, such a dynamic, collaborative federated network of people, ideas and processes would make knowledge actionable in order to address current and emerging challenges such as hybrid threats.

5. Impacts on Asia

Stephan De Spiegeleire and Eline Chivot have described in their study about the assertiveness of Russia and China[18] – assertiveness, defined broadly as either a rhetorical or behavioural increase in the way a country asserts its power in the international system – that both powers have displayed increasing assertiveness over the past decade, with Chinese assertiveness increasingly more noticeable than Russian. The study highlights a rising Chinese power that is increasingly asserting its military muscle. Over the past decade, China appears to have increased its rhetorical and its factual assertiveness significantly more than Russia has. A second serious finding of the study is that in both countries factual assertiveness has increased more than rhetorical assertiveness.

With China's steep rise in the share of total Asian defence spending in the last five years, and other countries investing largely in maritime and aerial capabilities, it is little wonder that strategists and governments alike have begun thinking seriously about how this might play out amidst the region's "growing militarization". Particularly the Japanese have concerns about 'grey-zone' contingencies with the Senkaku/Diaoyu Islands as one concern.[19] Singapore Minister for Defence Dr Ng Eng Hen stated recently[20] that in face of hybrid warfare the Singapore Armed Forces must restructure to be "*leaner, more potent and versatile*".

Of course, North Korea should be mentioned. What could North Korea learn from the Russian model? Is there perhaps Russian interest in developing North Korean hybrid capabilities? Is it possible that North Korea will become a close ally of Russia, perhaps even playing China and Russia against each other? As Moscow loses traction with the international community it aims to antagonise the U.S. as payback for what it sees as its meddling in Russia's backyard over Ukraine. North Korea and Russia have already announced they will be holding joint military drills later in 2015. Their growing closeness is a likely scenario. As Russia and North Korea grow closer, the U.S. and South Korea will certainly do the same. This comes on top of South Korea's growing need to cope with a series of emerging hybrid national security challenges[21] such as networked terrorism, accelerating cyber attacks, securing long-term energy supplies, and deepening maritime competition in the Indo-Pacific oceans. The prospects for increased hybrid challenges in the region are considerable. The danger of unmanageable escalation has increased.[22]

In sum, the growing hybrid shape of security challenges has complicated the security situation on a global scale.[23] Hybrid challenges have become reality. Hybrid warfare will be a defining feature of the future security environment. This should widen our perspective and our interest to cooperate in particular via adopting our respec-

[16] Allied Command Operations Comprehensive Operations Planning Directive COPD. Available at: publicintelligence.net/nato-copd/ (Access: 17 May 2015)

[17] Paul T. Bartone and Albert Sciarretta, Human Dimension Issues in Distributed and Virtual Teams. *Small Wars Journal*. Available at: smallwarsjournal.com/jrnl/art/human-dimension-issues-in-distributed-and-virtual-teams (Access: 17 May 2015)

[18] The Hague Centre for Strategic Studies. Assessing Assertions of Assertiveness: The Chinese and Russian Cases. June 2014. www.hcss.nl/reports/assessing-assertions-of-assertiveness-the-chinese-and-russian-cases/145/ (Access: 17 May 2015)

[19] Prashanth Parameswaran. Are We Prepared for 'Hybrid Warfare? The Diplomat, February 13, 2015, thediplomat.com/2015/02/are-we-prepared-for-hybrid-warfare/ (Access: 17 May 2015)

[20] Dr Ng Eng Hen, Minister for Defence, Speech at Committee of Supply Debate 2015, 06 Mar 2015, /www.mindef.gov.sg/imindef/press_room/official_releases/sp/2015/05mar15_speech.html#.VQyLpLpSGRg (Access: 17 May 2015)

[21] Lee Chung Min. South Korea's Strategic Thinking on North Korea and Beyond. The ASAN Forum. Special Forum October. 07, 2013. www.theasanforum.org/south-koreas-strategic-thinking-on-north-korea-and-beyond/ (Access: 17 May 2015)

[22] The Hague Centre for Strategic Studies. Assessing Assertions of Assertiveness: The Chinese and Russian Cases. June 2014. http://www.hcss.nl/reports/assessing-assertions-of-assertiveness-the-chinese-and-russian-cases/145/ (Access: 17 May 2015)

[23] Hoffman, Frank G. Hybrid Warfare and Challenges. Joint Force Quarterly, Issue 52, 1st Quarter 2009 / JFQ 34 – 39

tive security concepts and instruments of power and via networking global knowledge of relevance to meeting hybrid threats.

Ralph Thiele

Ralph D. Thiele is Chairman of the Political-Military Society (pmg), Berlin, Germany and CEO at StratByrd Consulting.

This paper was presented on the occasion of the V. Joint Conference “Crisis Management in Asia and Europe” by the Konrad Adenauer Foundation (KAS) and the Research Institute for National Security Affairs (RINSA) at the Korea National Defense University (KNDU) in Seoul, South Korea on May 6, 2015.

Opinions expressed in this contribution are those of the author.

IMPRESSUM

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

Herausgeber
Der Vorstand der **pmg**

Redaktion
Ralph Thiele (V.i.S.d.P.)
Tel.: +49 (221) 8875920
E-Mail: info@pmg-ev.com
Webseite: www.pmg-ev.com

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

pmg