Denkwürdigkeiten

Journal der Politisch-Militärischen Gesellschaft

Nr. 100
Juli 2016

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

ISSN 1436-3070

LEADOFF

Liebe Mitglieder,

etwas altbacken kommt das neue „*Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr*" schon daher. Wo ist der große Wurf? Viel Wind um wenig.

Bundeskanzlerin Merkel unterstreicht im Vorwort das strategische Ziel der Bundesregierung, Krisen und Konflikten vorzubeugen. „*Sicherheitspolitik muss vorausschauend und nachhaltig sein. Gleichzeitig müssen wir in der Lage sein, schnell auf gewaltsame Konflikte zu reagieren, zu helfen und zu einer raschen Konfliktbeilegung beizutragen.*" Dafür sei es unerlässlich, dass die zivilen und militärischen Instrumente zusammenwirkten, schreibt die Kanzlerin in ihrem Vorwort. Die Bundeswehr ist hier als Instrument des vernetzten Ansatzes unverzichtbar. Das hat die Bundeskanzlerin bereits im Jahr 2009 beim NATO Gipfel in Kehl festgestellt. Immerhin ist jetzt die gewachsene, globale Verantwortung fixiert. Diese wird sich materialisieren müssen. Auch und gerade vor dem Hintergrund zunehmend „hybrider" Herausforderungen für unsere Sicherheit.

Die Beiträge dieser Denkwürdigkeiten vermitteln einen Eindruck über Themenfelder globaler Verantwortung, die uns schon bald sehr vertraut sein dürften

Ralph Thiele, Vorstandsvorsitzender

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

In dieser Ausgabe

THEMEN

Das Signal von Canberra

Plädoyer für ein rüstungspolitisches „Team Deutschland"

Fußball, Energie und Rüstung – drei in Deutschland emotional diskutierte Themenfelder, die auf den ersten Blick nichts gemeinsam haben. Wie so oft täuscht der erste Blick, doch der Reihe nach.

Die australische Regierung gab am 26. April 2016 bekannt, dass Frankreichs DCNS der bevorzugte Design-Partner für das *Future Submarine Program* ist. Die Entscheidung weckte hierzulande in den letzten Tagen Emotionen; berechtigte Enttäuschung schlug um in Schuldzuweisung an die Industrie und die Regierung. An der Kritik ist etwas Wahres dran, wenn es etwa um die mangelnde Sichtbarkeit politischer Entscheidungsträger aus Deutschland in Australien geht oder moniert wird, der Fokus auf Japan habe den Blick für den französischen Wettbewerber getrübt.

Die Kritik läuft aber auch ins Leere. In seinen projektspezifischen

Zusagen ging Berlin gegenüber Canberra weit über das Gewohnte hinaus etwa mit Blick auf gemeinsame Technologieentwicklung, Ausbildung, Qualitätssicherung, Kostenprüfung und ein „rotes Telefon“ bei möglichen Problemen. Ebenso haben thyssenkrupp Marine Systems (tkMS), Siemens und weitere deutsche Unternehmen Australien nichts weniger angeboten als den Schlüssel zur Revitalisierung der Schwerindustrie mit einem Upgrade ins digitale Zeitalter der Industrie 4.0.

Die eigentliche Bedeutung der Entscheidung Canberras ist das davon ausgehende Doppelsignal. Als wichtigster europäischer Handelspartner der Asien-Pazifik-Region hinterlässt Deutschland hier bislang einen geostrategisch kaum relevanten Fußabdruck. Hinzu kommen die Konsequenzen für die Rüstungskooperation in Europa.

Mitte April 2016 teilte Oslo mit, dass Norwegen mit tkMS und DCNS über sein U-Boot-Programm verhandelt. Auf norwegischer Seite spielt Kongsberg die zentrale Rolle. Seit langem versucht Kongsberg für seine *Naval Strike Missile* einen Erstkunden zu gewinnen. Mit einem robusten Verhandlungsansatz erhoffte man sich von Berlin im Rahmen der U-Boot-Kooperation ein entsprechendes Zeichen, das bislang ausblieb. Frankreich scheint dagegen den Schwung aus Canberra zu nutzen und bietet Kongsberg an, den Lenkflugkörper künftig als *Joint Strike Missile* für die französischen Kampfflugzeuge sowie als *Naval Strike Missile* für die Über- und Unterwasserplattformen zu nutzen. Letzteres wiegt besonders schwer, denn bis heute hat Deutschland keinen eigenen Lenkflugkörper, der von U-Booten verschossen werden kann. Auf dem Umweg über Canberra und Oslo schafft Paris damit Fakten in der europäischen Konsolidierung – justament als Berlin sich entschließt, als einziges EU-Mitglied mit dem Mehrzweckkampfschiff MKS180 ein Rüstungsprogramm im europäischen Wettbewerb auszuschreiben. *Honnit soit qui mal y pense!*

Und damit sind wir beim Eingangsthema: Deutschlands Rüstungspolitik kann vom Fußball (Compliance ist damit nicht gemeint!) und der Energiepolitik lernen. 2014 gewann in Brasilien eine Mannschaft. „Team Deutschland“ ist, was Berlin in der internationalen Rüstungszusammenarbeit fehlt. Und diese Mannschaft gewann, weil sie Wille zeigte. Einen Willen, den die Bundesregierung nach dem Unglück in Fukushima aufbrachte, um die eigene Energiepolitik um 180 Grad zu drehen. Die Bundesregierung kann, wenn sie will, lautet die Botschaft. Daraus ergeben sich vier rüstungspolitische Handlungsfelder:

„Team Deutschland“ beginnt mit dem politischen Bekenntnis zur strategischen Bedeutung der Rüstungskooperation, der rüstungsbezogenen Forschungs- und Technologiezusammenarbeit sowie des Rüstungsexports als Instrumente der deutschen Außen- und Sicherheitspolitik. Deutschland hat ein Interesse daran, dass seine Verbündeten in der Lage sind, alleine und gemeinsam mit Berlin für ihre Sicherheit und damit auch für Deutschlands Sicherheit zu sorgen. Denn davon hängt, denkt man an die Bedeutung wichtiger Handelsbeziehungen mit der Golfregion, Asien, Afrika und Lateinamerika, auch Deutschlands Prosperität ab. Genau hier fehlt aber der entscheidende Teamgeist, denn die Kritik an der Rolle des Wirtschafts- bzw. Verteidigungsministeriums im Australienkontext verläuft auch entlang parteipolitischer Grenzen. Das zeigt: Rüstung ist Spielball parteipolitischer Interessen, nicht getragen von parteiübergreifendem Konsens – das gilt es zu ändern.

Dieses politische Bekenntnis muss konzeptionell geschärft werden. Bislang überwiegt die Einzelfallbetrachtung bei der Frage, welche rüstungspolitischen Schwerpunkte Deutschland mit welchen Partnern aus welchen außen- und sicherheitspolitischen Erwägungen verfolgt. Das greift zu kurz angesichts der strategischen Natur der Rüstungskooperation und des erklärten Willens der Bundesregierung, diese auch zu nutzen, um nationale Kerntechnologien zu erhalten. Künftig sollte Deutschland rüstungspolitisch nicht bloß auf die europäische Karte setzt. Vielmehr zeigt Paris’ Verhalten, dass die außereuropäische Diversifizierung der deutschen Rüstungspolitik unerlässlich ist. Deutschlands Partner wissen, dass der Umgang mit Berlin gerade wegen des harten Ringes um Rüstungsexportentscheidungen nicht einfach ist. Aber im Unterschied zur Konkurrenz steht Deutschland politisch sowie industriell zu seinen Zusagen und wird gerade deshalb geschätzt.

Rüstungspolitische Zusammenarbeit muss auch strukturell besser abgebildet werden. Entscheidungskompetenzen sind auf verschiedene Ministerien verteilt. Das führt in der Koalitionslogik zwangsläufig zu Blockaden, die nur mit großen internen Reibungsverlusten überwunden werden können. Die Hauptlehre aus Canberra ist, dass „Team Deutschland“ eine leistungsfähige Struktur braucht, um internationale rüstungspolitische Kampagnen aus einer Hand zu fahren. Dazu bedarf es der besseren Abstimmung zwischen den Ministerien genauso wie mehr Gemeinschaftlichkeit statt Rivalität auf der Industrieseite. Unerlässlich sind auch Kampagnenstrategien, die gemeinsame und individuelle Rollen festlegen.

Alle diese Anstrengungen müssen kommunikativ vorbereitet und begleitet werden. Mit der Forderung nach mehr Transparenz hat die Opposition der Bundesregierung einen Steilpass aufgelegt, den sie noch verwerteten muss. Nichts ist besser geeignet, den parteiübergreifenden Konsens herzustellen, als ein regelmäßiger rüstungspolitischer Dialog zu den Grundsatzfragen, wo Deutschland und seine Industrie welche Interessen verfolgen, ob diese kongruent oder divergierend sind und wie Kräfte gebündelt werden können. Dieser Dialog darf kontrovers sein, doch er sollte so geführt werden, dass sich alle an eine einmal gemeinsam definierte Linie halten.

Canberras Entscheidung war ein Weckruf für Berlin. Bleibt dieser ungehört, zeichnet sich in Norwe-

gen ein vergleichbarer Ausgang an. Die Folge wäre eine weitere Schwächung der Unterwasserindustrie, einer der letzten strategisch bedeutenden Technologiekerne, mit dem Deutschland internationalen Gestaltungsanspruch erheben kann. Daher ist klar: Schaun'm mer mal war gestern. Jetzt gilt: Auf geht's, „Team Deutschland"!

Dr. Heiko Borchert

Dr. Heiko Borchert ist Inhaber eines sicherheits- und verteidigungspolitischen Beratungsunternehmens.
Erstmalig erschienen im griephan Brief 21/16, 23.05.2016.
Der Beitrag gibt die persönliche Auffassung des Autors wieder.

THEMEN

Maritime Security: New perspectives of a familiar subject

The role of Navies, Coast Guards and NGOs in today's maritime domain

Artificial islands are challenging maritime nations with a new and unknown situation. Examples have been established in the South China Sea and the implications have many aspects, two most important have legal and strategic characteristics.

We have almost forgotten that artificial islands are not new phenomena and that many nations are responsible for such islands. Mostly they are located inside territorial waters where their purpose is to host maritime infrastructure such as the Gulf oil terminals. Today global changes have created new challenges, risks and indeed threats to maritime security. Although we are focused on the regional situation in South China Sea, we know it would be a crucial mistake to look at the situation from a purely regional perspective.

It is the intention of this brief paper to draw attention to some more traditional as well as some newer perspectives of the maritime domain, which will continue to have or to gain more awareness in future.

A key consideration is to establish what are the constant and variable factors?

In principle we can understand maritime security as either a condition or as an enduring task. As a condition, action is required if the status quo is challenged or threatened. As an enduring task, presence and a well-balanced mix between quality and quantity in capabilities has to be maintained. So a maritime security policy can be to be reactive or pro-active.

The choice between these options has an impact on research and technology, on training and education and, not least, on how all the various maritime services cooperate with each other.

The ultimate challenge is to combine initiatives and innovation at the strategic, technological and organisational levels. One way to help understand the complexity of today's maritime domain is to divide it into four dimensions:

Considering the maritime domain as...

A Habitat
- What are the consequences of global climate change? The development of artificial islands to advance a claim for extending sovereignty is an indirect consequence of climate change. Are they otherwise in danger of disappearing as a consequence of rising sea-levels?
- Almost 80 per cent of the world` s population lives within 100 km of the coast,

A Resource
- What is the impact of overfishing and exploiting mineral and energy resources?
- What kind of balance between economic and environmental interests is required to reach a regional consensus? What is the role of the growing responsibility of the International Seabed Authority in this context? Are artificial islands introducing a new dimension into UNCLOS?

A Highway (transport)
- What are the consequences of insecure global sea-lanes?
- What about the prospect of attacks on the global seabed cable network?

A Domain for Power Projection
- How is good governance at sea to be achieved?
- What are the Global and Regional Maritime Strategies?
- What existing and future capabilities are needed?
- What are (or should be) the consequences of violating UNCLOS?
- Who has the authority, the political will and the means to enforce the Law of the Sea?
- Do we need to consider a new maritime force, which is focused on civilian-military security operations?
- Is there a role for NGOs in this context?

Having considered these dimensions, it is then necessary to define the role of a navy, independently of the region, from a joint and/or combined force perspective and also establish whether operations are purely military or a civilian-military.
- **Maritime Deterrence and Defence** – deterring by demonstrating decisive maritime presence based on operational readiness and capability; protecting and defending national sovereignty and integrity, as well as the United Nations Convention of the Law of the Sea and its ambition to ensure good governance at sea. Chapter VII states: "Actions with respect to threats to the peace, breaches of the peace and acts of aggression". Articles 39 to 51 provide the necessary justification. This is and will remain a naval responsibility, but potentially supported by other maritime services.
- **Crisis Response** – participating in specific operations ranging from peacekeeping, peace enforcement and conflict prevention to humanitarian assistance, disaster relief and non-combatant evacuation. Improving operations by exercising civilian-military cooperation. Co-

ordinating and cooperating with NGOs when appropriate.

- **Naval Diplomacy** – providing a visible symbol of national, international commitment and support to political objectives as in conflict prevention and stabilization. This can be achieved by port visits and joint exercises or even by the mere presence of a warship (i.e. a show of force).
- **Maritime Capacity Building –** Maritime Capacity Building measures can be seen either as a subordinate mission of Maritime Diplomacy or as a task in its own right. Current examples are demonstrating the growing importance and success of such activity conducted by coast guards, navies, maritime services and NGOs in particular

Specific roles cover the whole spectrum from low intensity to war-fighting tasks, so an interim conclusion must be that we need a broad mix of maritime and joint capabilities to be prepared for a rapid shift from a low intensity capability to a high-end capability. The question must therefore be posed: what kind of capabilities are needed? This is a crucial policy and strategic level decision.

A more recent consideration for all maritime security contributors is the option to act in support of another service or to be supported by them. Non-Combat Evacuation Operations are an example. These involve among other aspects: providing security, life support for evacuees and evacuators, understanding the legal implications and working with the media. It will also look at relationships and co-ordination with embassies, host nation governments, other government departments, Non-Governmental Organisations (NGOs) and other nations engaged in a concurrent NEO of their own entitled nationals.

Areas of actions: examples for Maritime Security Operations

Nations differ in how they protect their national strategic maritime security interests. In some countries these tasks are the responsibility of civilian surveillance and law enforcement authorities such as coast guards; in others navies have this responsibility. Therefore enhancing civil-military cooperation is essential regardless of their internal national organisation. A Maritime Security Operations (MSO) Concept is necessary to provide options for how maritime forces can contribute to achieve, enhance and execute maritime security in a comprehensive intergovernmental approach. In essence it establishes specific tasks aimed at deterring, preventing and countering unlawful activities. From the MSO derive the different missions, activities and operations:

- **Surveillance of the Global and Regional Maritime Domain**.
  Acquiring and sharing surveillance information with other military and civilian agencies and relevant actors in order to improve situational awareness of the global maritime domain and ensuring early warning. Information sharing is a fundamental task which is a vital enabler for all maritime forces' roles and tasks, and it is a key factor for success in operations in support of maritime security.
- **Maritime Protection.**
  Protecting sea lines of communication, choke points, merchant traffic, fishing industry, maritime critical infrastructure for energy, transport, research and strategic communications sites and ports by conducting maritime operations such as: counter piracy, mine countermeasures, special operations and support to law enforcement activities combating illegal migration, trafficking and organised crime.
- **Maritime Interdiction/Control.**
  Conducting specific operations such as ensuring sea control and/or sea denial within a given area, boarding and inspection of suspicious ships and imposing maritime embargos as required.
- **Maritime Counter-Terrorism and Counter-Proliferation of Weapons of Mass Destruction.**
  Preventing, deterring, detecting and disrupting terrorist activities and counter-proliferation of WMD, including CBRN, and protecting citizens and their interests against criminal activities at sea by means of specific capabilities and through close collaboration with the international community**.** In addition, maritime forces, civilian and military, may be required to perform operations such as:

  ▪ **Maritime Presence.**
  Conducting maritime diplomacy; demonstrating the political will to support all activities enforcing the freedom of navigation on the high seas which enables early deployment and forward presence.

  ▪ **Maritime Capacity Building.**
  Contributing to and supporting the strengthening of the maritime safety and security capacity of a fragile state through the provision of advice and training across a wide spectrum of maritime activities of which training and education are the key elements.

  ▪ **Law Enforcement.**
  Conducting operations under constabulary authority in international waters, regulated by a regional or national legal regime – such as the Contiguous Zone (CZ) or the Exclusive Economic Zone (EEZ) – as well as on the high seas beyond those zones, in respect of foreign merchant vessels or vessels without nationality, which are suspected of being involved in illegal activities.

Today`s focus is on South China Sea and the challenges emanating from the deteriorating situation in this region.

A brief look into China´s maritime ambitions and aspirations could help to understand and to reflect on appropriate and successful responses to the growing tensions.

The publication of the "Unrestricted Warfare" strategy in China in 1999 changed the Chinese Military outlook. How did it influence the rise of PLA Navy and what is the link between the rebirth of China's "blue water" navy ambitions and the concept?

In 1982, Deng Xiaoping implemented an important shift in strategy. Until then it had been the classical Mahanian view of sea power that guided the early years of Chinese Navy's rebirth. The strategy was founded on the principles of a strong commercial fleet with a Navy capable of securing its trade routes. The end of the 1990s saw another crucial shift in Chinese strategic thinking, marking the beginning of the new millennium. In response to the country's burgeoning economic development there was a need to adapt the PLA Navy's focus on coastal and brown water to the high seas or blue water. Intellectually, this shift can be traced back to the growing influence of Corbett rather than Mahan in China's strategic naval thinking.

Since 2000, China's strategic thinkers have successfully linked this new approach with the country's traditional strategies. This intellectual step forward was achieved by taking into account new technologies on the one hand and the concept of "Unrestricted Warfare" on the other. Therefore we should ask: What are the roles and tasks of the PLA Navy in relation to this strategy? We do not know the whole answer, but we have witnessed the fact of redefining naval forces into maritime forces, which are able to perform an escalating role while staying just short of adopting a fighting mode.

Conclusions

The new trends and developments include:

- The increasing demand for comprehensive approaches and inter-agency interaction.
- Smooth integration between civilian and military capabilities.
- Defense and security operations: developing a high-low capabilities mix.

There is an increasing need to:

- Change mindsets in order to adapt a more transparent attitude in information sharing: Move from "need to know" to "need to share" and then to "responsibility to share".
- The need to assess new concepts and modes of war fighting (e.g. cyber warfare, hybrid warfare, air-sea/joint campaign, sea basing, anti-access/are denial).
- Coming to terms with the impact of new – commercial and military – technology in maritime security (e.g. use of unmanned systems in all domains).
- Do we consider sea-borne activity by non-state actors as maritime operations?
- How do we engage with non-state navies such as the Sea Shepherd Conservation Society or Mercy Ships?
- How do we deal with maritime border disputes?
- Do they require both low and high-end capabilities?
- Is there a need for new inter-agency approaches?

An option to answer at least some of the questions could be a Combined Maritime Force, a CMF.
The unique characteristic of the CMF is that participation is purely voluntary. No nation is asked to carry out any duty that it is unwilling to conduct. The contribution by each country varies depending on its ability to contribute assets and the availability of those assets at any given time. The nations that comprise a CMF are not bound by either a political or military mandate, which makes the CMF a very flexible organization. Contributions can vary from the provision of a liaison officer at CMF HQ, wherever it might be located, to the supply of warships or support vessels in task forces to maritime reconnaissance aircraft based on land. The CMF can also call on warships not explicitly assigned to the coalition to give associated support, which is assistance they can offer if they have the availability and capacity to do so whilst undertaking national tasking.

Coalitions are founded on the principle that forces will never be asked to do anything that their governments are unwilling to have them do. As such, the legal basis for CMF operations is based on the United Nations Convention on the Laws of the Sea and the authority of United Nations Security Council Resolutions. In this way, each warship in the coalition has to abide by its own domestic law. There are no coalition Rules of Engagement but a "Set of Permissions" to which all countries agree. While there are national mandates that limit the participation of some of coalition partners, the CMF remains a cooperative, multinational effort, a true coalition of the willing.

The formation of such a CMF with a rotating leadership between the contributing nations would be a most impressive answer of solidarity, political will and naval and maritime capabilities in the South China Sea and beyond.

Lutz Feldt

Vice Admiral (rtd) Feldt served in the German Navy for 41 years and retired in 2006 as Chief of the German Naval Staff in Bonn and Berlin. He was president of the German Maritime Institute until June 2012 and is now a member of its board. Since August 2011, Vice Admiral Feldt, in his function as a Director of the Wise Pens International, is working on studies dealing with future maritime safety, security and defence. Since November 2013 Vice Admiral Feldt has been President of EuroDefense Deutschland e.V.
This paper was presented on the occasion of the VI. Joint Conference of the Konrad Adenauer Foundation (KAS) and the Sea Lanes of Communication (SLOC) Study Group Korea "The Legal, Economic, and Strategic Implications of China's Artificial Island-building Projects for the South China Sea and Beyond" on May 17, 2016 in Seoul, South Korea.
First published in ISPSW Strategy Series: Focus on Defense and International Security, Issue No. 425, June 2016.

THEMEN

Migration – A new form of "Hybrid Warfare"?

Preliminary Remarks

It is a great pleasure and honor for me to attend, now for the sixth consecutive occasion, the strategic dialogue organized by the Research Institute for National Security Affairs (RINSA), the Korea National Defense University (KNDU), and the Konrad Adenauer Foundation, in Seoul.

I would also like to take this opportunity to thank the representative of the Konrad Adenauer Foundation in South Korea, Stefan Samse, for inviting our German team to this high-level conference.

While migration has many facets I shall focus here on its utilization as an instrument of "hybrid warfare".

Let me begin by giving two definitions. The Federal Office for Migration and Refugees in Germany defines migration thus:

"*Migration occurs when a person changes the location of their usual place of residence. International migration occurs when this movement crosses national boundaries*".

Hybrid warfare is defined by the European Parliament as follows:
Hybrid war is a situation in which a country resorts to the overt use of armed forces against another country or a non-state actor, in addition to a mix of other means (i.e. economic, political, and diplomatic).

I personally find the following, in-depth definition more persuasive:
"*Hybrid Warfare is 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, terrorists, and criminal elements*".

'Hybrid threats', Ladies and Gentlemen, are often involved, for example, in the ongoing conflict in the Ukraine and the campaign by the so-called "Islamic State" in Iraq and Syria.

I would like to turn to Russia's hybrid warfare in the Ukraine. In his analysis *Crisis in the Ukraine – The Emergence of Hybrid Warfare,* Colonel Thiele – who regrets that he will be unable to join us this year in Seoul – makes reference to 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.

His speech is, indeed, significant and very helpful for an understanding of Russia's approaches to hybrid warfare. I restrict myself here to citing three short passages from the above lecture:

"*The very 'rules of war' have changed. The role of non-military means of achieving political strategic goals has grown, and, in many cases, has exceeded the power of the armed forces with respect to effectiveness….*

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

Asymmetrical action has become widespread, enabling the nullification of an enemy's advantages in armed conflict. Among such actions is 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 informational action, devices, and means that are constantly being perfected…"

In short, three stages of Russia's hybrid warfare have been identified:
- Destabilizing a country by way of inciting domestic conflict;
- Causing the collapse of the state by way of ruining an economy and destroying its infrastructure;
- Replacing local political leadership with one's own operatives as "invited saviour".

At one point during the Ukrainian crisis, Russia had more than 55,000 troops positioned along the Ukrainian border. When it came to sowing instability in Ukraine, it was not conventional forces that were used but a range of unorthodox methods.

While the rebels directly engaged the Ukrainian army in the Donbass, the Russian military conducted training manoeuvres just across the border within Russian territory. These exercises included the use of space, missile and nuclear forces, special forces and conventional military units, as well as psychological operational teams and political operatives. All branches of the Russian military and security services were pulled in, as well as civilian leadership.

Closer analysis of Russia's hybrid warfare strategies requires prior knowledge of President Putin's objectives in the Ukraine, in Europe and in international politics. The President of the Federal Academy of Security Policy (BAKS), Dr Karl-Heinz Kamp, succinctly expressed the matter in a BAKS publication, in April 2016:

"*Russia has undergone a fundamental transformation in its foreign policy. Putin understands his country as an anti-Western power. He thinks in Cold War categories, namely, in spheres of influence, and thus along expansionist lines. In so doing, he does not shrink from occupying sovereign states. This is demonstrated by the annexation of the Crimea and armed conflict in the eastern Ukraine.*

For Putin, the USA is the root of all evil. From his point of view, the USA was the reason for the fall of the Soviet Union – a situation he continues to deplore to the present day. His goal is to divide the USA and Europe, to question the legitimacy of their institutions, such as NATO and the UN, and to weaken the EU as a political and economic union. To this end, almost any means is justified".

Roderich Kiesewetter, foreign and security policy expert for the CDU in the German parliament, also shares Dr Kamp's view. In an interview with *Deutschlandfunk* in February 2016, Kiesewetter observed that Russia's strategic objective is the destabilization of the EU. Furthermore, Putin finances extremist rightwing networks in Europe.

He also accused Putin of exacerbating the crisis in Syria, and seeking to intensify the refugee crisis. A further refugee scenario is imminent in the Ukraine should agreements for a ceasefire in the East of the country fail.

A fact sheet issued by the German Bertelsmann Foundation in January 2016, entitled *Facts on the European Dimension of Displacement and Asylum: Ukraine,* shows that 1.8 million internally displaced persons (IDPs) were registered by UNHCR, the UN refugee agency, in December 2015. According to UNHCR, at least 800,000 IDPs live in areas under the Ukraine government control alone. Ukraine also has:

- a substantial number of non-registered IDPs
- some 600,000 people living in IDP-like conditions
- 7,100 displaced persons and asylum seekers from other countries.

According to UNHCR, another 1.1 million refugees fled the Ukraine. The main destinations were Russia (858,000 disputed), Belarus (127,000 disputed) Germany 6,540.

The chief reasons for Ukraine's migration flows are as follows:

1. Forced migration as IDPs and refugees from the war in Donetsk and Luhansk, and the annexation of Crimea;
2. Emigrating as a means to avoid the military draft and
3. Leaving to find work and/or for educational purposes.

The Russian government continues to blame the Ukrainian government for causing the migration crisis. This is not the whole story, however. In my estimation, Putin's hybrid warfare campaign – the provision of weapons to Ukrainian rebels, the use of mercenaries for destroying regional infrastructure, the weakening of local economy, blocking state functions, causing a refugee crisis, exploiting social media and information warfare etc. – has already proved successful. He has destabilized the Ukraine and will continue to do so. This is closely aligned with his concept of combined foreign and security policy and hybrid warfare.

The so-called "Islamic State" – Migration and "Hybrid Warfare"

Let us now take a brief glance at Bakr's "Master Plan" for the so-called Islamic State.

Samir Abd Muhammad al-Khlifawi, known by his nom de guerre as Haji Bakr, was the strategic head of the rebel group "Islamic State of Iraq and the Levant (ISIL) and was former colonel in Saddam Hussein's Intelligence Services. He later joined the rebel group al-Qaida in Iraq and took part in the Iraqi insurgency.

In late 2012, he relocated to the small Syrian town of Tell Rifaat, north of Aleppo. From there he helped organize the capture of parts of Syria by the IS, which would, in turn, be used as a base for invading Iraq.

Under the guise of Islamic missionary centers, the IS opened bases and recruited informers by using hybrid warfare tactics. Khlifawi's plans aimed at gathering information on:

- The leading families and individuals in villages or towns
- The sources of the latter's income, weaknesses and secrets which would make them susceptible to blackmail.
- The rebel groups in villages or towns, their leaders and ideological orientation

All such information was very helpful for expanding IS influence in Syria and Iraq.

Haji Bakr was killed by rival rebels on January 6, 2014.

The civil war in Syria has been responsible for the deaths of over 250,000 people over the past five years. More than half the population, approximately 13.5 million people, are on the move – 8.7 million of whom within Syria, and 4.7 million within the neighboring countries Turkey, Lebanon, Jordan, Iraq, Egypt and Libya. More than 900,000 Syrians have filed an asylum request in Europe.

The Assad regime, in particular, along with the so-called "Islamic State" is chiefly responsible for this humanitarian catastrophe. Their war strategy includes the deliberate killing and starving of the civilian population, the widespread destruction of residential areas, and the systemic displacement of ethnic and religious groups considered potential trouble-makers or adversaries, namely, the use of hybrid warfare tactics. But what we are also witnessing here is a proxy war among such contestants as Saudi-Arabia, Qatar, Iran, Turkey, the US, Russia and others.

The above-mentioned figures also demonstrate why so many migrants have been forced to leave their homes and their country.

Last month (April 2016), the President of the German domestic intelligence agency (BfV), Dr Hans-Georg Maaßen, admitted in an interview that security authorities wrongly evaluated the so called "Islamic State" strategies to infiltrate Germany. Security officials initially believed it was unlikely that "Islamic State" terrorist would use the recent influx of refugees to enter the country and that the risk was too high. Although they did not need to covertly insert their people among the refugees, they did, in fact, do this", referring to the strategy as "a show of force".

Among the one million refugees entering Germany last year, around 70 per cent of them held no valid passport and were registered on the basis of information they provided.

Maaßen also claimed that the BfV and partner agencies may, in fact, have information about dangerous individuals in their databases, but may well fail to notice their presence here due to their entry with false identity papers.

Radical Islamists in Germany are also actively trying to win over newly arrived refugees. Maaßen said the BfV was aware of around 300 attempts from conservative Salafists and other Islamists to recruit refugees.

When asked how many Islamists in Germany were considered "highly dangerous", he said around 1,100 individuals have been classified as possible terrorists. In the interview he went on to point out that he is particularly concerned about the many unaccompanied minors, and that this group is being deliberately targeted.

There have also been several cases where Germans returning from Syria were connected to recently disclosed attack plans, and that the danger of German jihadists remains "virulent".

Here are three examples showing how the IS sends terrorists to Europe in the guise of refugees.

On Friday, November 13, 2015 the IS tasked a killer-commando to the streets of Paris. Three suicide bombers struck near the *Stade de France*, followed by suicide bombings and mass shootings at cafés, restaurants and a music venue. One hundred and thirty people were killed, and a further 368 injured. Prior to their attack in Paris, two of the suicide bombers had been registered on the Greek island of Leros, where they registered as Syrian refugees. The IS claimed responsibility for the attacks.

On January 12, 2016 a suicide attack occurred near the Blue Mosque in Istanbul. Turkish authorities identified the attacker as Nabil Fadli. Coming from Syria, he entered Turkey on January 5, 2016, where he had been registered and fingerprinted as a refugee. In Istanbul he then furtively mingled among a group of tourists before then detonating his explosives. Thirteen people were killed, including eleven Germans; with a further nine injured tourists. Fadli was a Syrian member of the IS and the IS claimed responsibility for the attack.

Mid-December 2015: Austrian media reported that police had arrested two people suspected of involvement in the terror attacks in Paris on November 13, 2015. The two people in question arrived on the Greek Island of Leros in October 2015, at about the same time as the two men who launched the November attacks in Paris. The twenty-eight-year-old Algerian and thirty-four-year-old Pakistani applied for asylum in Austria and had their fingerprints taken. They had purportedly been in contact with Abdelhamid Abaaoud, one of the ring-leaders of the Paris attacks who had been subsequently killed in a shootout.

Recommendations

Ladies and Gentlemen, as you will note, I have placed a question mark behind the title of my presentation *Migration – A New Form of "Hybrid Warfare"?.* I am now convinced of the facts and no question now remains. To conclude, I would like to present five recommendations:

1. Although the EU and NATO have identified Russia's hybrid warfare activities, its capabilities and the threats, double-track policies seem to be the best way forward. These include:
   a) continued dialogue with Moscow by way of various channels, such as the NATO Russia Council, the OSCE and several other open and secret channels;
   b) a strong political and military signal, which should be given at the NATO Summit in Warsaw on July 8-9, 2016.
2. NATO and EU Member States should increase their situational awareness, covering political, economic and social influence of hybrid actors which could threaten NATO and the EU.
3. The European Union should increase the staff of its EU East STRATCOM Task Force and provide an appropriate budget as soon as possible.
4. NATO should strengthen its Center of Excellence in the Latvian capital Riga, where strategies in the propaganda war are analyzed and countermeasures developed.
5. When planning combat strategies against the hybrid warfare campaigns of Russia and the so-called "Islamic State", the words of NATO Secretary General Jens Stoltenberg are instructive: "Our goal is to bring the truth to light. We believe that critical journalism and an open political debate are the best ways to counteract propaganda."

Dr. Peter Roell

Dr Peter Roell has been President of the Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) in Berlin since January 2006.

This paper was presented on the occasion of the VI. Joint Conference of the Konrad Adenauer Foundation (KAS) and the Research Institute for National Security Affairs (RINSA) of the Korea National Defense University (KNDU) "Emerging Transnational Risk Assessment and Responses: Europe and Asia" on May 16, 2016 in Seoul, South Korea.
First published in ISPSW Strategy Series: Focus on Defense and International Security, Issue No. 422, May 2016.

"... und der Nachschub an Chips könnte besser sein. Kartoffelchips!"

THEMEN

Cyber an die Front

Zur Handlungsfähigkeit der Bundeswehr im Cyber- und Informationsraum

Tagtäglich finden Cyberangriffe auf die Bundeswehr statt. Im ersten Halbjahr 2015 wurden bei Einsätzen über 100.000 sicherheitsrelevante Ereignisse bei den Rechnern der Bundeswehr registriert. Zum Teil sind dies gezielte, individuell zugeschnittene Angriffe. Sie werden mit hohem Aufwand geplant, vorbereitet und durchgeführt. Nicht immer werden sie sofort erkannt und abgewehrt. Statistisch dauerte es 2015 selbst bei schwerwiegenden Attacken im Schnitt 205 Tage, bis Cyberangriffe überhaupt erkannt wurden. Die Lösung der daraus resultierenden Probleme dauerte dann durchschnittlich noch einmal 32 Tage. Diese Statistiken geben Anlass zur Sorge. Und das hat auch die Bundesregierung erkannt.

Deshalb gründen jetzt auch die deutschen Streitkräfte ein eigenes Kommando für die Operationsführung im Internet, im Militärjargon Cyberraum genannt. Mit ordentlichem Medien-Auftrieb hat Ministerin von der Leyen angekündigt, mit dem Kommando Cyber- und Informationsraum bis zum April 2017 eine neue Teilstreitkraft der Bundeswehr aufzubauen.

Besonders perfide für die nationale und internationale Sicherheit sind sogenannte *hybride Bedrohungen* unterhalb der Schwelle eines militärischen Angriffs. Hierzu zählen Operationen im Cyberraum für Spionage, Informationsmanipulation, mögliche Cyber-Terrorakte bis hin zu groß angelegten Sabotage-Attacken zum Beispiel auf kritische Infrastrukturen wie die Netze der Energieversorger. Die russischen Cyber-Attacken im Kontext der Georgien-Krise 2008, der Ukraine-Krise, aber auch beim Hacker-Angriff auf das Netz des Deutschen Bundestages geben erste Eindrücke über das Spektrum der Möglichkeiten. Aber Russland steht hier nicht allein. Die USA, Israel, China, Nordkorea, Taiwan, England und Frankreich sind ebenfalls schlagkräftig aufgestellt.

Während die Bundeswehr mit der Entwicklung nicht Schritt halten konnte, behandeln die NATO und etliche Partnerländer den Cyber- und Informationsraum schon länger als einen eigenen Operationsraum. Sie bauen konsequent eigene Cyber-Fähigkeiten aus. Die USA haben schon vor sechs Jahren ihr Cyber-Kommando eingerichtet. Das Atlantische Bündnis begreift Cyber-Fähigkeiten geradezu als *Game Changer*, also als eine Fähigkeit, die etablierte Macht- und Kräfteverhältnisse zwischen Staaten auf den Kopf stellen kann.

In Abstimmung mit der Europäischen Union (EU) entwickelt die NATO zur Abwehr der hybriden Bedrohungen gerade eine neue Strategie. Wir werden beim bevorstehenden NATO-Gipfel in Warschau mehr darüber hören. Die EU hat ihre diesbezüglichen Vorstellungen bereits veröffentlicht. Dazu zählt insbesondere der Schutz kritischer Infrastrukturen wie Energie und Telekommunikation. Man sorgt sich insbesondere vor Cyberangriffen, die zu erheblichen Störungen einer zunehmend vernetzten Wirtschaft und Gesellschaft führen. Für den digitalen Binnenmarkt gilt es deshalb, die Resilienz der Kommunikations- und Informationssysteme in Europa zu stärken. Inzwischen zeichnet sich auch eine Intensivierung der Zusammenarbeit zwischen EU und NATO ab. Diese konzentriert sich absehbar neben der Verbesserung des Bewusstseins für hybride Bedrohungen auf die Stärkung der Resilienz sowie auf Prävention, Krisenreaktion und Rückkehr zur Normalität.

Handlungsfähig werden

Noch mehr Sorge muss bereiten, dass nicht nur die Administration und Büroorganisation der Streitkräfte bedroht sind. In alten und neuen Waffensystemen finden sich zahllose Prozessoren, Interfaces, Chips und Computer. Viele dieser Systeme wurden bereits oder werden derzeit vom informationstechnischen Fortschritt überrollt und sind professionellen Cyber-Angriffen hilflos ausgesetzt. Im Umkehrschluss lassen sich hochentwickelte Cyber-Fähigkeiten auch zur Unterstützung der Einsätze der Bundeswehr einsetzen. Bits und Bytes können nicht nur die Kommunikation und Entscheidungsfindung eines Gegners beeinflussen, sondern ggf. den Einsatz kinetischer Kampfkraft klassischen Zuschnitts ermöglichen, verstärken oder auch ersetzen. Wenn ich ein Raketensystem auch ohne Waffenwirkung ausschalten kann, vermeide ich die sowohl die Gefährdung eigener Kräfte im Zuge eines erforderlichen Einsatzes wie auch denkbare Kollateralschäden.

Vor diesem Hintergrund ist das Grundrational der Verteidigungsministerin durchaus überzeugend: „*Staat, Wirtschaft und Gesellschaft sind in einer zunehmend vernetzten, digitalisierten Welt für Angriffe im Cyber- und Informationsraum (CIR) verwundbarer geworden. Diese digitale Verwundbarkeit der Gesellschaft haben sich in den letzten Jahren staatliche und nichtstaatliche Akteure – insbesondere im Rahmen der hybriden Kriegsführung – zu Nutze gemacht. ... Die zunehmend komplexeren Angriffe erfordern den Ausbau der staatlichen Handlungsfähigkeit zum Schutze unseres demokratischen Systems und seiner wirtschaftlichen Grundlagen.*“

Bereits zum Oktober 2016 wird im Verteidigungsministerium eine eigenständige Abteilung eingerichtet. Der vormalige Thyssen Krupp-Manager Klaus-Hardy Mühleck übernimmt hier als Chief Information Officer mit Budgethoheit die Verantwortung für die Themen Cyber und IT. Als IT-Architekt der gesamten Bundeswehr soll er zunächst einmal die bislang verzettelte materielle und personelle IT-Infrastruktur unter ein Dach bringen und die Bundeswehr-Informationstechnikgesellschaft als eigenständige IT-Organisation (Systemhaus) steuern. Ob dann noch Zeit, Kraft und zielführende Vision für die zukunftsweisende Gestaltung der Netze des militärischen Nachrichtenwesens, für die recht komplexe Waffensystem IT sowie die leistungsfähige Ausprägung einer neuen Teilstreitkraft mit ganz neuen Fähigkeiten bei rechtlich unübersichtlichen Rahmenbedingungen bleibt?

Bis Anfang April 2017 wird zudem ein Kommando für den Cyber- und Informationsraum (CIR) aufgestellt mit den Aufgaben Cyber, Informationstechnologie, militärisches Nachrichtenwesen, Geoinformationswesen, operative Kommunikation und elektronische Kampfführung. Insgesamt 13.500 Dienstposten werden hierzu von den anderen Teilstreitkräften und Organisationsbereichen in die neue Struktur wechseln – 12.800 davon allein aus der Streitkräftebasis.

Die Ministerin will mit diesen Maßnahmen die IT-Kompetenz in der Bundeswehr bündeln und effektiver zu nutzen. Zugleich sollen Effizienz und Schlagkraft der Bundeswehr im dynamisch wachsenden Feld der Informationstechnologie verbessert werden, ebenso der Schutz der Truppe – auch im Einsatz – und gegebenenfalls auch der Schutz der Bevölkerung. Denn die Bundeswehr stellt sich darauf ein, bei Cyber-Angriffen von katastrophalen Ausmaßen an der Seite der Spezialisten von der Polizei und vom Bundesamt für die Sicherheit in der Informationstechnik in die Abwehr einzugreifen. Eingebettet in einer Ressortübergreifenden Gesamtstrategie der Bundesregierung sollen dann die Cyber-Fähigkeiten der Bundeswehr in enger Abstimmung vor allem mit dem Bundesinnenministerium agieren.

In diesem Kontext stellt sich natürlich die Frage, welche Rahmenbedingungen – faktisch und rechtlich – im internationalen Einsatz sowie beim Schutz von Bevölkerung, Wirtschaft und der verletzlichen Infrastruktur der Heimat auf dem digitalen Gefechtsfeld gelten. Welcher Mix aus defensiven und offensiven Fähigkeiten ist notwendig? Welcher ist erlaubt? Wo sind rechtliche Grenzen gesetzt?

In der Bundeswehr erwartet man, dass solche Fragen im Falle eines Auslandseinsatzes durch ein Bundestagsmandat geklärt werden. Einsatzmöglichkeiten jenseits der Firewall eines fremden Servers kommen für sie – außer im Verteidigungsfall – nur infrage, wenn sie für den jeweiligen Einsatz vom Bundestag mandatiert sind. Bei Angriffen auf die eigenen Computersysteme im Inland, darf sich die Bundeswehr zwar schützen. Sie überlässt die erforderlichen Gegenmaßnahmen jedoch dem im Inland zuständigen Bundesamt für Sicherheit in der Informationstechnik. Ob das in der Praxis gut geht?

Die nächste Großbaustelle der Bundeswehr

Man könnte die Ministerin für ihre Weitsicht in Sachen Internet loben. Allerdings wurden die bedrohlichen Cyber-Herausforderungen in der Bundeswehr doch bemerkenswert spät wahrgenommen. Wer die Details der deutschen Planung prüft, entdeckt viele gute Absichten und viel weniger gute Taten. Was die Ministerin inhaltlich verspricht, trifft frühestens 2020 ein, vermutlich erst viel später. Das Geld reicht nicht. Das Personal reicht nicht. Die Strukturüberlegungen geben in erster Linie bestehenden Organisationen einen neuen Namen und eine neue Unterstellung – alter Wein in neue Schläuche.

Bereits jetzt sorgt sich der Wehrbeauftragte des Bundestages vor einem flächendeckenden Burnout in der Bundeswehr. Das Weißbuch 2016 spricht im gegenwärtigen Entwurfsstand selbstkritisch von „*schleichender Überalterung des Materials*“ und von Streitkräften, die im Grundbetrieb vermehrt aus der Substanz leben müssten. Dies ist eine freundliche Umschreibung für die Kannibalisierung von Ersatzteilen aus Waffensystemen, Fahrzeugen, Flugzeugen und Schiffen, früher ein klassifizierendes Merkmal von Drittweltstaaten. *„Aufgaben, Kräfte und Mittel befinden sich nicht mehr in einer ausgewogenen Balance“*. Gemeint sind Panzer die nicht fahren, Flugzeuge die nicht fliegen, Kompanien ohne Personal.

Die bestehende Planung hat sich bereits ohne die Cyber-Herausforderungen als überholt und ineffizient erwiesen. Nun kommt also das Thema *Cyber* hinzu. Will man hier keine bösen Überraschungen im Einsatz erleben, müsste man die laufenden Rüstungsplanungen, natürlich auch die im Dienst befindlichen Rüstungsgüter, dringend auf ihre Cyberverwundbarkeit prüfen und entsprechend anpassen. Da dies absehbar teuer wird und zudem die bestehende Planung weiter kompliziert, vermied man bislang selbstkritische Analysen und stellt sich dieser Aufgabe erst in der Zukunft.

Nun ventiliert man derzeit die Überlegung, den Problemen der Gegenwart durch eine beschleunigte Beschaffung von IT nach dem Grundsatz – *IT schneller als Rüstung – zu enteilen. Es ist sicherlich gut gemeint,* dass IT-Beschaffung nicht hinter den Innovationszyklen in der Computerindustrie hinterherhechelt. U*nd zugleich ist es realitätsfremd. IT ist Bestandteil von Rüstung. Zunehmend prägt sie erst die Wirksamkeit hochkomplexer Waffensysteme. IT muss insbesondere auch der einsatzbezogenen Nutzung von Rüstungsgütern dienen*. Wenn der IT-Bereich mit der sogenannten *2-speed-IT* eine zusätzliche Überholspur erhält, wird ein Fokus auf die *weiße IT* erkennbar, die sich um die Bürokommunikation bis hin zum Druck von Broschüren dreht. Das ist die Welt, aus der von außerhalb der Bundeswehr hinzugezogene IT-Experten kommen und in der sich diese zu Hause fühlen. Der Bund stellt aber keine Streitkräfte auf, damit deren Bürokommunikation funktioniert. Wenn die *weiße IT* die den Einsatz prägende *grüne IT* überholt, sind die Streitkräfte in Gefahr. Ein einziger Eurofighter fliegt beispielsweise mit hundert Kilometer Kabel an Bord, damit seine 80 Computer das Fliegen und Feuern beherrschen.

Bereits seit langem liefert die Beschaffung nicht, was sie verspricht. Hierfür gibt es viele Gründe. Eine Ursache ist seit Jahrzehnten bekannt: die in Streitkräfte und Bundeswehrverwaltung gespaltene Aufgabenwahrnehmung der Bundeswehr. Es war ein gut gemeinter, aber dennoch struktureller Webfehler bei der Aufstellung der deutschen Streitkräfte, deren Aufgaben grundgesetzlich zu veruneinheitlichen durch die Teilung in Grundgesetz (GG) Art. 87a („Der Bund stellt Streitkräfte zur Verteidigung auf“) und in GG Art. 87b („Die Bundeswehrverwal-

tung wird in bundeseigener Verwaltung mit eigenem Verwaltungsunterbau geführt."). Die durch GG Art. 87a adressierten Streitkräfte erhalten als sogenannte Bedarfsträger von durch Art. 87b adressierten Mitarbeitern der Bundeswehrverwaltung allzu oft Rüstungsgüter, die wesentlich zu spät ausgeliefert werden und zudem auch nicht den Ansprüchen der Truppe im Einsatz genügen. Der Lufttransporter A400M liefert als aktuelles Beispiel immer neue Belege hierfür.

Seit 25 Jahren hat es sich eingebürgert, dass erforderliche Investitionen durch vermiedene Ausgaben erwirtschaftet werden sollen. Zugleich fressen hohe Personalkosten Löcher in Betrieb und Ausrüstungsbedarf. Und natürlich leidet auch die Ausbildung unter dem Geldmangel. Die seit Jahrzehnten mangelhafte finanzielle Unterlegung von Reformen und Innovation hat nicht nur die Substanz der Bundeswehr entkernt, sondern untergräbt zugleich erfolgreichen, rechtzeitigen Wandel.

Das Thema Personal ist ein problematisches Feld. Bislang fehlt der Bundeswehr das hoch qualifizierte Personal, das für den Betrieb und insbesondere für das Erkennen und letztendlich die Abwehr von Cyberangriffen zuständig ist. Insbesondere sind die komplexen Waffensysteme zu schützen und auf aktuellem Stand zu halten. Das ist aufgrund der hohen Innovationszyklen der Informationstechnologie eine große Herausforderung. Demgegenüber verlassen seit Jahrzehnten hochqualifizierte IT-Experten die Bundeswehr in Scharen, weil deren Expertise insbesondere in den ersten Dienstjahren nach deren Studienabschluss ignoriert wird und bei fachfremden Tätigkeiten zu verkümmern droht. Die bisherigen Karriere- und Qualifikationsmodelle lassen eine Förderung der IT-Expertise bislang nur unzureichend zu. Auf der anderen Seite ignoriert man den Bedarf von IT-Kompetenz in operativen Schlüsselverwendungen und schiebt befähigte Allrounder unter dem Hinweis auf nicht besetzte Dienstposten gerne in berufliche IT-Sackgassen. Damit fehlt dann wiederum die adäquate IT-Kompetenz im Umfeld der militärischen und politischen Spitzenentscheider.

Also Experten von außen anwerben? Auch dieser Ansatz stößt auf Hindernisse. Zum einen kann die Bundeswehr den Wettbewerb mit der IT-Industrie um geeignetes Personal nicht gewinnen, da sie nicht mit den Gehältern der Privatwirtschaft mithalten kann. Zum anderen haben die *Nerds* der zivilen Welt nicht selten eine problematische Vergangenheit. Wer in sicherheitsempfindlichen Bereichen arbeitet muss überprüft werden. Die gesuchten Experten wollen aber nicht überprüft werden. Und die Bundeswehr kann schlecht Experten mit Sicherheitsrisiken in sensitive Verwendungen bringen. Die Bundeswehr sucht deshalb nach neuen Wegen. Unter anderem will man eigene Studiengänge aufbauen, um Menschen zu gewinnen und zu halten. Man will zugleich mit Industrie und Universitäten in „Cyber-Clustern" kooperieren, um die nötige Expertise zu bekommen. An der Universität der Bundeswehr München wird dafür ein eigener Studiengang für Cybersicherheit eingerichtet. Schnelle Ergebnisse wird man hier nicht erwarten können.

Ein bisher sträflich vernachlässigtes, aber vielversprechendes Feld sind Cyber-Spezialisten aus dem Reservistenbereich – vormalige Soldaten mit fortgesetzter Affinität zu den Streitkräften. Statt sie nach den bisher angelegten Maßstäben für den Reservistendienst in klassischen militärischen Funktionen einzusetzen, können sie als IT-Fachleute in Deutschland in Rechenzentren und Gefechtsständen mitarbeiten und z.B. Auslandseinsätze im Zuge des sogenannten *Reach-Back* unterstützen. Hier werden Einsatzfunktionen, die nicht unbedingt im Einsatzland wahrgenommen werden müssen, von Deutschland aus ausgeübt. Damit spart man erheblich an Personal in Auslandseinsätzen.

Insbesondere das vorherrschende geistige Maginot-Denken, sich auf die Cyber-Abwehr zu konzentrieren und auf offensive Cybereinsätze weitestgehend zu verzichten, ist im Lande eines Carl von Clausewitz geradezu unfassbar. Bereits vor 200 Jahren lernte man in deutschen Landen zwischen taktischen, operativen und strategisch-politischen Ebenen zu differenzieren. Noch im Kalten Krieg wusste und übte man in Deutschland, wie man einen strategischen Angriff des Warschauer Paktes, durch kleine offensive Gegenangriffe auf taktischer Ebene und Luftangriffe auf die Versorgungs- und Verbindungslinien im Rückraum des angreifenden Gegners ausbremsen konnte. In der Cyber-Domäne ist der Angreifer klar im Vorteil. Sich hier einseitig defensiv auszurichten, bedeutet nichts anderes als sich auf Niederlagen und Großschäden einzustellen.

Will man künftig wirklich immer wieder eigene Informations- und Kommunikationsnetze solange beschädigen lassen, wie es ein Angreifer wünscht? Will man die ausgeprägten IT-Aktivitäten von ISIS und Taliban auch künftig möglichst ungehindert und störungsfrei zur Entfaltung kommen lassen? Wie will man forensisch dem Täter auf die Spur kommen, ohne sein Wirken bis an den Ursprungsort zu verfolgen? Selbstverständlich müssen Mandatierungs- und Rechtsfragen geklärt werden. Dennoch: Wer sich gegen Cyberangriffe effektiv schützen will, muss auch in der Lage sein, einen Angriff auszuführen. Die Fachkenntnis ist ohnehin identisch. Ohne eigene taktische und operative Offensiv-Fähigkeiten macht die Cyber-Truppe keinen Sinn.

Der Weg ins digitale Zeitalter beginnt für die Bundeswehr absehbar mit selbstgemachten Hindernissen. Relevanten Überlegungen stehen strukturelle Mängel, zu kurz gesprungene konzeptionelle Grundlagen, eine Kannibalisierung bestehender Strukturen und unzulängliche Investitionen gegenüber. Drei Empfehlungen sollen diesen Beitrag schließen:

- Eine Vision ohne entsprechende Investition ist eine Halluzination. Die neue Teilstreitkraft Cyber – und Informationsraum braucht eine Mittelausstattung, die es ermöglicht, zentrale Zielsetzungen zu erreichen.

- Die neue Aufstellung im Cyber- und Informationsraum sollte sich mit Priorität daran orientieren, dass die Bundeswehr als eine kombattante Organisation politisch-parlamentarische Zwecke im Einsatz erfolgreich umsetzen soll.
- Alle Teilstreitkräfte – auch das neue Kommando Cyber- und Informationsraum – müssen über einen Mix an offensiven und defensiven Fähigkeiten verfügen. Taktisch und operativ brauchen die Streitkräfte ein den Aufgaben angemessenes Fähigkeitendispositiv, um ihre Einsätze im Sinne der politischen Vorgaben erfolgreich zu gestalten. Dies steht der politisch-strategischen Vorgabe einer strategisch defensiven Ausrichtung der deutschen Streitkräfte im digitalen Zeitalter ebenso wenig entgegen wie zu Zeiten des Kalten Krieges.

Ralph Thiele

Ralph Thiele ist Vorsitzender der pmg und geschäftsführender Inhaber von StratByrd Consulting.
Erstmalig erschienen in der Wirtschaftswoche am 17.06.2016
http://app.wiwo.de/unternehmen/it/cyberkrieg-wie-die-bundeswehr-im-netz-aufruestet/13750472.html
Der Beitrag gibt die persönliche Auffassung des Autors wieder.

THEMEN

Risk of war returns to Europe

A century ago this weekend, my great-grandfather – a corporal in the Liverpool-recruited King's Regiment – was waiting to go "over-the-top" at the Somme.

Sent to pick up the company rum ration before the assault, he wound up drinking it and woke up after the action – or at least, that's the story he told the family after World War One was over.

Perhaps his superiors were in an unusually forgiving mood. Or perhaps, like many others, he was just looking for a way to avoid retelling his experiences. By the end of the first day, the Allies had suffered almost 60,000 casualties for precious little ground. By the time the offensive was canceled later in the year, there were more than 800,000, over half of them fatalities.

With the two world wars increasingly passing from living memory, it's becoming easier to forget just how much they dominated the lives of almost every family on the continent.

Quietly, though, that is changing. When NATO states meet in Warsaw at the end of the week for the annual heads of government meeting of the alliance, they will be doing so amid the most serious tensions with Moscow since 1989.

Virtually no one, it must be said, thinks that either side is anything other than very keen to avoid a devastating conflict. Europe remains home to more than half the world's nuclear weapons. No one doubts that should a third major war overwhelm the continent, it would almost certainly be worse than any of those that preceded it.

And yet, a growing number believe, the risk is quietly increasing. In May, retired British General Sir Richard Shirreff – who served as NATO's Deputy Supreme Allied Commander at the time of the Russian annexation of Crimea in 2014 – wrote a book explicitly suggesting all-out war with Russia could happen as soon as next year.

On the surface, the book is a novel – but Shirreff has underlined in multiple interviews, including with this reporter, that he views it a highly plausible scenario. His former NATO boss, U.S. Admiral James Stavridis, underlines the point in a hard-hitting introduction.

In Shirreff's book, all sides are essentially operating from a position of weakness. His unnamed Russian president – clearly modeled on Vladimir Putin – initiates hostilities with both Ukraine and the NATO member Baltic states of Estonia, Lithuania and Latvia to distract from economic woes at home, particularly a falling oil price.

Western leaders, meanwhile, overplay their limited military hand. Politicians on both sides have their eyes as much on their domestic politics as anything else. The result is a chain of errors with potentially devastating consequences.

These real-world tensions have been a long time coming. Even in the 1990s, Russian opinion – both within the military and political elite and wider country – was incensed at what felt like growing Western disdain and encroachment into what Moscow had long seen as its exclusive sphere of influence. Restoring what Russia sees as its self-respect has been at the heart of Vladimir Putin's rule.

In Crimea in particular, Moscow showed itself adept at what military thinkers increasingly call "hybrid warfare", using political manipulation and deniable forces – particularly troops without insignia – to achieve effects without resorting to conventional force. It is an area, some Western officials say, where Russia has developed a considerable lead over the West.

The lesson of the last decade, however, has also been that when it does choose to escalate to all-out military action – as it did in Georgia in 2008, Ukraine in 2014 and Syria last year – it tends to do so with much greater force and speed than Western analysts anticipated.

The problem, of course, is that no one really knows what the best way of avoiding conflict is. For Shirreff and many others, particularly in NATO's more exposed eastern states, the answer is assertive deterrence, putting enough military forces in the region to make any conventional Russian assault difficult.

Much of that is already happening, at least up to a point. The United States has dramatically ramped up its military activity in Europe since 2014, sending tanks, special forces and other personnel to frontline states as well as making high profile deployments of heavy military equipment. That includes the return of U.S. Army tanks to

Europe as well as visits by state-of-the-art F-22 Raptor stealth fighters and aging Cold War-era workhorses such as B-52 heavy bombers and A-10 "tank busters".

Baltic, Nordic and Eastern European nations are ramping up defense spending – albeit several steps behind Moscow, which has poured oil revenue into its military over the last decade with the specific aim of being able to deliver overwhelming force in its very immediate neighborhood. Already, some estimates suggest, Russia has more than enough firepower to swiftly overwhelm local and NATO forces in its immediate neighborhood.

As in Ukraine and Georgia, the most likely flashpoints look to be regions with large ethnic Russian populations – essentially, the border districts of Lithuania, Latvia and Estonia. The governments of those countries have already stepped up development and political efforts in those regions to reduce the risks – but some analysts worry NATO's activities may end up overly militarizing the situation.

As non-NATO members, neither Ukraine nor Georgia could count on Western military support when they wound up fighting Russia in 2008 and 2014. The Baltic states are a different matter – under NATO's founding charter, an attack on one is an attack on all.

During the Cold War, NATO's Supreme Allied Commander Europe [SACEUR] – always the senior U.S. officer who also commands all U.S. forces on the continent – had operational control of European NATO forces facing Russia. That is no longer the case, however, meaning many decisions now also require political authorization from member states. It's the sort of messy situation that would make handling of confrontation much more difficult.

Russia has placed its nuclear arsenal at the center of its strategic approach to this kind of confrontation. According to Western experts, its recent military exercises have relied heavily on what it calls a single "de-escalatory nuclear strike".

It's a very simple – but possibly phenomenally dangerous – concept. The theory is that if Russian forces are engaged with an enemy like NATO, once they have won the conventional battle they would launch a single nuclear strike with the aim of intimidating the West into standing down and accepting the results.

In major exercises in 2013 that simulated an invasion of one or more of the Baltic states, the scenario appeared to end with a nuclear strike on Warsaw, NATO officials say. More recently – perhaps worrying that such an approach might make a NATO nuclear response inevitable – Russian exercises have tended to target a single purely military target, for example a NATO flotilla of warships.

A strike like that could kill thousands if not more – and what would happen next is almost impossible to predict. Putin might well hope such an action might fraction NATO, leaving countries hopelessly divided on how to respond. Already, opinion polls suggest German voters in particular would be reluctant to fight to defend NATO allies, while U.S. presidential contender Donald Trump has explicitly questioned the long-term survival and purpose of the alliance.

In the era of social media and 24-hour news, however, it's equally easy to imagine a furious U.S. electorate demanding a savage retaliation. In the post-Cold War world, after all, the United States has become used to doing what it wishes. Nor, as the UK's referendum has shown, is European politics currently particularly predictable.

Miscalculation is not inevitable. But it is arguably becoming more likely.

Just over a century ago, shortly before the Somme, future Prime Minister Winston Churchill was a battalion commander on the Western Front. He found himself in a briefing on the perceived lessons of the Battle of Loos, a bloody and unsuccessful earlier engagement that used the same tactics.

"I wanted to say 'Don't do it again,'" he wrote to his wife after. "But they will."

Peter Apps

Peter Apps is Reuters global affairs columnist, writing on international affairs, globalization, conflict and other issues. He is founder and executive director of the Project for Study of the 21st Century; PS21, a non-national, non-partisan, non-ideological think tank in London, New York and Washington. Before that, he spent 12 years as a reporter for Reuters covering defense, political risk and emerging markets. Since 2016, he has been a member of the British Army Reserve and the UK Labour Party.
First published at Reuters.com:
www.reuters.com/article/us-europe-war-commentary-idUSKCN0ZL2FM
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**.