Herausgeber: Chef der Armee

Nr. 1/2019
Beilage zur ASMZ 6/19 und RMS 3/19

Military Power Revue

der Schweizer Armee
de l'Armée suisse
of the Swiss Armed Forces

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Schweizer Armee
Armée suisse
Swiss Armed Forces

Der Chef der Armee ist Herausgeber der Military Power Revue.

Die Military Power Revue erscheint zweimal jährlich (Ende Mai und Ende November).

Die Military Power Revue ist Beiheft der Allgemeinen Militärzeitschrift ASMZ und der Revue Militaire Suisse (RMS).
Verlag: ASMZ, Brunnenstrasse 7, 8604 Volketswil.

Herstellung:
Zentrum elektronische Medien ZEM,
Stauffacherstrasse 65/14
3003 Bern
058 464 65 00

Druck:
galledia ag
Burgauerstrasse 50,
9230 Flawil
Tel. 058 344 96 96

Chefredaktion Military Power Revue:
Urs Gerber
Internationale Beziehungen Verteidigung
Papiermühlestrasse 20
3003 Bern
Tel. +41 58 483 82 36
E-Mail: urs.gerber@vtg.admin.ch

Strategic Missile Defence – Quo Vadis? 5

Stefan C. P. Hinz

Die «Gerasimov-Doktrin» und die russischen Militärwissenschaften 13

Hanna Grininger
Christoph Bilban

Défendre la Suisse dans le cyberespace 29

Gérald Vernez

Offset-Geschäfte der Schweiz: Bedeutung für die sicherheitsrelevante Technologie- und Industriebasis 40

Diego Heinen
Christoph Ebnöther

Strategische Kommunikation in den Streitkräften 50

Michael Holenweger

Energiesicherheit von Streitkräften – eine zentrale Verteidigungsfähigkeit! 64

Daniel Krauer
Martin Krummenacher

Buchbesprechungen 75

Titelbild Der Blick in die nächste und übernächste Geländekammer vermindert das Risiko von Überraschungen auf allen Stufen (VBS/DDPS).

Vorwort

Geschätzte Leserinnen und Leser der Military Power Revue

Wie Sie wissen, startete die Umsetzung der Weiterentwicklung der Armee (WEA) am 1. Januar 2018 und dauert bis am 31. Dezember 2022. Einer der vier Pfeiler der Weiterentwicklung der Armee (WEA) ist die Erhöhung der Bereitschaft. Unser Ziel war es, Ende 2018 in der Lage zu sein, mit den Mitteln der ersten Stunde – also Berufsorganisation und Durchdienerformationen – sowie den Milizformationen mit hoher Bereitschaft die vorgegebenen Leistungen zu erbringen.

Unabdingbare Voraussetzungen dazu sind primär das praktische Üben der Mobilmachung, aber auch die ausreichende personelle Alimentierung und Ausrüstung dieser Formationen. Weil mit der Armee XXI die Fähigkeit zur Mobilmachung abgebaut wurde und somit – wie Ihnen sicher bekannt ist – das entsprechende Wissen weitgehend verloren gegangen war, wurde vergangenes Jahr also folgerichtig damit begonnen, das Mobilmachungssystem wiederaufzubauen.

Konkret wurden 2018 unter der Leitung der Territorialdivisionen, der Luftwaffe und der Logistik- und Führungsunterstützungsbrigaden primär mit den Milizformationen mit hoher Bereitschaft Mobilmachungsübungen durchgeführt. Dabei wurde die Zusammenarbeit der Fassungsdetachemente der Milizformationen mit den Armeelogistikcentern geschult und praktisch trainiert. Die Materialfassungen für die Wiederholungskurse erfolgten somit mehrheitlich so, wie sie im Mobilmachungsfall durchgeführt werden würden.

Zusätzlich haben auch zahlreiche Formationen, die erst im Jahr 2019 für Mobilmachungsübungen geplant waren, bereits 2018 die Gelegenheit genutzt, die Mobilmachung im Rahmen eines Eigentrainings zu üben.

Das deckt sich mit jenen Erfahrungen, die ich mit der Truppe in Bezug auf die Mobilmachung gemacht habe und noch immer mache: Die Miliz ist neugierig, wissbegierig, lernwillig und leistungsbereit; sieht sie den Sinn einer Sache ein, so verbeisst sie sich richtiggehend in die Materie und lässt nicht locker.

Die Erfahrungen aus diesen ersten Mobilmachungsübungen zeigen, dass das Konzept richtig ist. Die entsprechenden Prozesse bedürfen bislang keiner Anpassungen. Hingegen wurden beim Dispositiv der Mobilisierung aufgrund von gewissen Umbasierungen der Logistikbasis der Armee und den gemachten Erfahrungen kleinere Anpassungen bei den Standorten eingeleitet.

Die ersten Schritte für das Wiedererlangen der Fähigkeit zur Mobilmachung sind also gemacht. Die technische Fähigkeit zur elektronischen Alarmierung mittels SMS ist vorhanden und überprüft. Das System eAlarm funktioniert, und die Qualität der erfassten Daten der Angehörigen der Mittel der ersten Stunde sowie der Milizformationen mit hoher Bereitschaft wird laufend überprüft und verbessert.

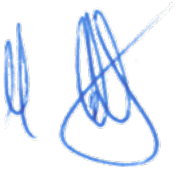
Ab 2019 soll zusätzlich auch mit jährlichen Testalarmen die Erreichbarkeit der Angehörigen der Armee überprüft werden. Auch die Alarmierung des im Mobilmachungsfall erforderlichen Berufspersonals ist vorbereitet und wird ebenfalls laufend überprüft.

Wir dürfen uns jedoch nichts vormachen: Wir sind punkto unserer Fähigkeiten zur Mobilmachung noch weit davon entfernt, die nötige Routine zu besitzen – es ist also zwingend, regelmässig zu trainieren. Anders formuliert: Wir müssen üben, üben und nochmals üben.

Die Situation ist digital: Wir sind verpflichtet zu erfüllen, weil die Bereitschaft das zentrale Element des Leistungsprofils unserer Milizarmee ist. Dieses Leistungsprofil ist quasi ein «contrat operationnel» mit der Politik; es gibt vor, welche Leistungen wir in welchem Zeitraum zu erbringen haben. Bei unvorhergesehenen Ereignissen ist es unser erklärtes Ziel, innert zehn Tagen bis zu 35 000 vollständig ausgerüstete Angehörige der Armee aufbieten und einsetzen zu können.

Auch dafür müssen wir noch üben, üben, üben. 2019 und in den folgenden Jahren wird es deshalb darum gehen, die Mobilmachungskompetenzen der bereits 2018 beübten Truppen weiter zu vertiefen. Bei den übrigen Truppenkörpern, welche nicht zur Miliz mit hoher Bereitschaft zählen, werden die entsprechenden Mobilmachungsübungen ab 2020 durchgeführt.

Wir bleiben dran. Wir sind verpflichtet, zu erfüllen.



Chef der Armee
KKdt Philippe Rebord

Editorial

Sehr geehrte Leserinnen und Leser der Military Power Revue

Der renommierte U.S. Think Tank *Center for Strategic and International Studies* CSIS hat kürzlich eine Aufdatierung der fünf grössten (globalen) Risiken für 2019 vorgenommen:

1. Yes, we have no certainty.
2. U.S. alliances are breaking.
3. Pressure to fragment global supply chains is intensifying.
4. Alternatives to capitalism are trending.
5. Designer babies are here.

Auf den ersten Blick mag sich die geneigte Leserschaft fragen, ob und in welchem Umfang diese Thesen für die schweizerische Sicherheitspolitik und die Armee überhaupt von Interesse oder gar Relevanz sind, zumal es sich um eine eher U.S.-amerikanische Sichtweise handelt. Wenn man aus der militärstrategischen Optik gleichzeitig die derzeitigen und absehbaren strategischen sowie technologischen Entwicklungen und Trends berücksichtigt, erscheint eine zumindest indirekte Relevanz auch für uns gegeben zu sein. Vor dem Hintergrund der zunehmenden Ausweitung der Operationssphären (z. B. Outer Space) wie auch der erkennbaren Neubeurteilung der Bedeutung und Möglichkeiten von Nuklearwaffen scheint diese Relevanz eher noch zuzunehmen, auch und vielleicht gerade wegen des Umstandes, dass unser Land hier kein eigenständiger Akteur ist und realistischerweise nicht sein kann. Fügt man hier noch die laufenden Aktivitäten und Entwicklungen im Cyber-Bereich oder die sich abzeichnenden Implikationen durch die Errungenschaften der künstlichen Intelligenz hinzu, verstärkt sich die Erkenntnis, dass Sicherheitspolitik und Streitkräfte, auch die schweizerischen, sich obigen Herausforderungen in Zukunft noch vermehrt zu stellen haben werden. Dabei ist den anderen Risiken und Bedrohungen wie insbesondere diejenige durch die verschiedensten Formen von Terror oder den Auswirkungen von Machtpolitik weiterhin mit der nötigen Entschiedenheit entgegenzutreten. Dafür existieren auch mit Unterstützung aller technologischer Neuerungen nach wie vor keine politischen oder militärischen Patentrezepte. Eine Schlüsselfähigkeit scheint aber immer mehr herauszuragen: eine möglichst robuste und trotzdem flexible Führungsfähigkeit, welche zeitverzugslos und nahtlos von der lokalen zur strategischen Stufe sichergestellt ist.

Im Umfeld eher zunehmender Unsicherheit, sich verändernder Risiken und Bedrohungen sowie volatilen Lagebildern dürften klassisch-lineare, möglichst auf Autonomie ausgerichtete Führungsansätze kaum mehr erfolgsversprechend sein. Es erscheint offensichtlich, dass ein national und international möglichst robust vernetztes Risikomanagement eher angezeigt ist, zumal es auf die Volatilitäten in einem von Unsicherheit geprägten Umfeld wahrscheinlich flexibler reagieren kann. Robuste Vernetzung erfordert aber auch bei aller Berücksichtigung neutralitätsrelevanter Rahmenbedingungen möglichst stabile Partnerschaften, die unter anderem Zugang zu strategisch relevanten Entscheidgrundlagen oder gar Einwirkmöglichkeiten garantieren. Deshalb sind die oben erwähnten Risiken des Zerfalls von U.S. Allianzen wie auch der Fragmentierung globaler Handelsströme auch für die Schweiz von (strategischer) Relevanz.

Die MILITARY POWER REVUE hat sich seit jeher zum Ziel gesetzt, derartige Trends aufzunehmen und im Sinne des Denkanstosses sowie der Erkenntnis- oder Erfahrungserweiterung einer interessierten Leserschaft anzubieten. Auch diese Ausgabe fühlt sich diesem Grundsatz verpflichtet. Das gilt für die Zukunftsperspektiven der strategischen Raketenabwehr, der Bedeutung der strategischen Kommunikation in den Streitkräften wie auch die Implikationen der Energiesicherheit für die Streitkräfte. Das Konzept und die Umsetzung der Cybersicherheit für das Land und die Armee sowie die sicherheitspolitische Relevanz von Offset-Geschäften für die schweizerische Industrie- und Technologiebasis sprechen aktuell im Fokus stehende Herausforderungen im nationalen Kontext an. Die Aufarbeitung der «Gerasimov-Doktrin» im Spannungsfeld zwischen Absicht und Perzeption lässt klar werden, dass vor lauter Fokussierung auf künftige Herausforderungen Basisarbeit bezüglich klassischem militärischen Denkens und Doktrin weiterhin unabdingbar bleibt. Der genuin militärische Beitrag zur Meisterung aller dieser Herausforderungen wird immer komplexer. Er kann in einer Milizarmee aber nur erbracht werden, wenn die Mobilisierung der Angehörigen der Armee zeit- und inhaltsgerecht gelingt, was gemäss dem Chef der Armee auf guten Wegen, aber noch nicht am Ziel ist.

Damit wünsche ich Ihnen eine anregende und hoffentlich interessante Lektüre.

Der Chefredaktor der Military Power Revue
Urs Gerber

Strategic Missile Defence – Quo Vadis?

It is argued that it would be expedient to apply the overarching criterion of whether a significant strategic[1] missile defence capability is a real "stability gain" or not. For this purpose, it could be helpful to be aware of the consequences, which includes the risks and side effects when considering the net balance of a possible or planned strategic missile defence capability. However, it becomes questionable as soon as missile defence exceeds a certain capability level and thus significantly weakens or even neutralises the strategic deterrence potential of an opponent, at least in the context of complementary counterforce capabilities.[2]

Looking prominently to the United States as a superpower, it is as evident as undisputable that missile defence is *one* tool in the toolbox aiming to maintain and expand its comprehensive claim to superiority vis-à-vis *all* other powers.[3] From the perspective of Washington, it can be deducted that missile defence capabilities *must* be dispersed not only as a national defence, but also in both "vital peripheries"[4] on the Eurasian continent, in Europe and East Asia. United States' allies must be protected in the best possible way, not least from blackmail. Moreover, from the U.S. perspective, missile defence activities provide opportunities for burden sharing and defence cooperation – but also to sell U.S. products.

Stefan C.P. Hinz

Setting the scene

The "Missile versus missile defence" process had started in World War II. The allies had no defence capabilities against the world's first ballistic missile, the A-4 (in Nazi terminology the "V[5]-2", the "Mother" of all subsequent SCUD missiles and their enhancements), when in flight. This made it all the more important to engage the missile before being launched, i.e. on the ground[6], or even better, to attack the production lines.

Although such an extreme operational scenario has not repeated itself since that time (apart from the "War of the Cities" between Iran and Iraq in the 1980s, in which hundreds of ballistic missiles were employed), some basic principles have remained unchanged to this day. Strategic (long-range) missiles are more likely to be employed at the end of a "hot" conflict. The party to the conflict which is (or deems itself) at the losing end, will strive to bring about a change. It will at least want to defend itself as fiercely as possible. In an era, where weapons of mass destruction are readily available, there is the additional option of mounting nuclear, biological or chemical warheads. As we have learned from both Gulf Wars, the *option* of employing weapons of mass destruction alone creates strategic effects, not least in the sense of terrorising the population that may be affected. This makes the following points all the more important: The missiles and/or launchers must be searched and destroyed *before* they are employed.[7] Above all, the principle of deterrence applies. Especially in the Levante, all parties involved were and are aware that, if weapons of mass destruction were actually employed against Israel, this would have "existential consequences" for the attacker.

In general, one could argue, that for all nations with a small surface area, such as Switzerland or Israel, a threat posed by missiles has the potential to be existential, i.e. strategic. In the case of nations with a greater surface area, or alliances, a differentiation must be made between tactical (protection of peripheries, deployed troops, objects) and strategic (protection of territory, capital, centre of gravity) missile defence. An in-depth discussion about the

1 In this analysis, "strategic" is defined as a capability which could cover the territory of a whole nation / region / alliance.
2 Cf. Peter Rudolf, US-Geopolitik und nukleare Abschreckung in der Ära neuer Grossmachtrivalitäten, May 2018 and Aporien atomarer Abschreckung, July 2018, available in German at <https://www.swp-berlin.org/>
3 Most current update: Missile Defense Review (MDR) 2019, Office of the Secretary of Defense, January 2019, <https://media.defense.gov/2019/Jan/17/2002080666/-1/-1/1/2019-MISSILE-DEFENSE-REVIEW.PDF>, in this analysis referred to shortly as "MDR 2019".
4 As defined by Zbigniew Brzezinski, The Grand Chessboard. American Primacy and its Geostrategic Imperatives, New York, 1997, p.32
5 V= Vergeltung (= retialiation)
6 Exactly this "the earlier, the better" is a main narrative of the MDR 2019, especially because of new hypersonic threats.
7 Coalition SCUD Hunting in Iraq 1991

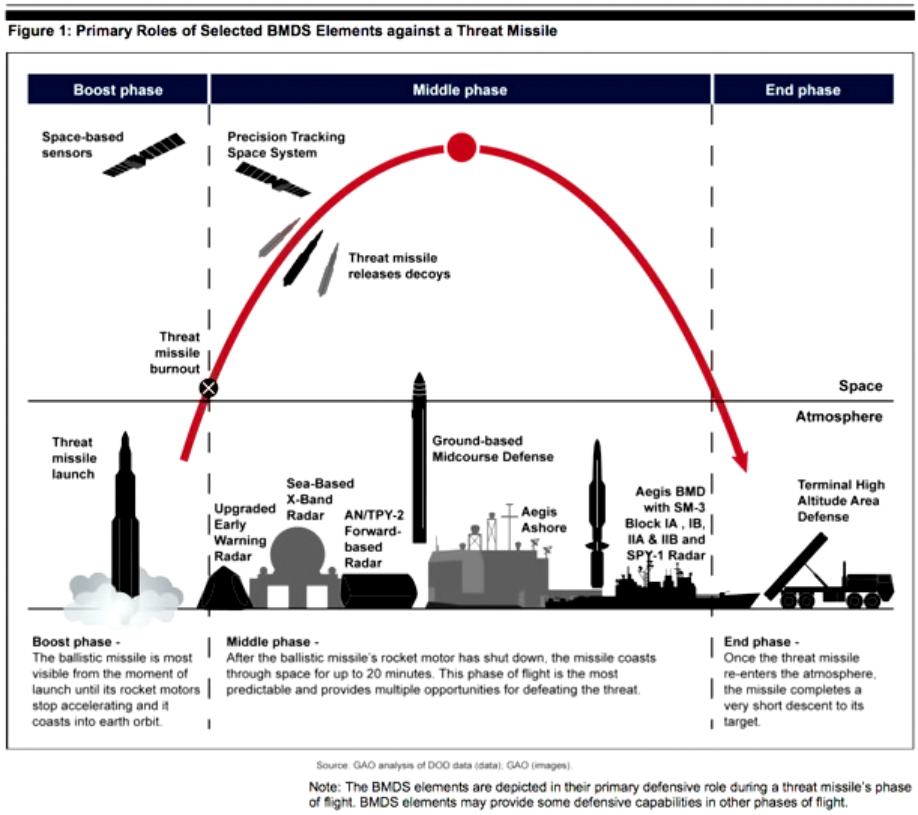


Figure 1 Primary role of selected BMDS elements against a missile threat. (https://www.cfr.org/backgrounder/ballistic-missile-defense)

division between "strategic" and "tactical" would go beyond the framework of this analysis.

In general, one could argue, that for all nations with a small surface area, such as Switzerland or Israel, a threat posed by missiles has the potential to be existential, i.e. strategic.

Strategic missile defence systems affect global and/or regional stability. This was the reason why the Anti-Ballistic Missile (ABM) Treaty was signed 1972, granting both parties to the treaty (the United States and the Soviet Union/Russia) only a fig leaf, i.e. a limited number of strategic interceptor missiles.[8] The underlying rationale was to put a stop to the nuclear-strategic arms race in the field of defence. Otherwise, there would have been the threat of an open-ended arms race with the respective interplay of defensive and offensive measures.[9]

A triad ensures a best possible deterrence, i.e. a second-strike capability, through redundancies, which means that at least a part of the attack potential will survive under all circumstances.

Having said this much, it is undisputed that long-range missiles, including the relevant risks and threats as well as a potential defence against these missiles, must be regarded in a comprehensive manner. Since the Cold War, the United States and Russia have had a fully established nuclear-strategic triad, i.e. land-, sea- and air-based nuclear arms. China, India as well as Pakistan in the foreseeable future, are in the process of developing the required capabilities. Israel is likely to already possess the relevant capabilities. A triad ensures a best possible deterrence, i.e. a second-strike capability, through redundancies, which

8 Finally, both parties were allowed to deploy 100 interceptors each. These could be based as a protection of the capital (so the Sowjetunion decided, the system is still operational) or of a missile launch silo area (so the US did, but only for a few years); find the treaty at <https://www.state.gov/t/avc/trty/101888.htm>.

9 Cf. Michael Krepon, Cooperative Threat Reduction, Missile Defense and the Nuclear Future, New York, Houndmills, 2003, pp. 85ff

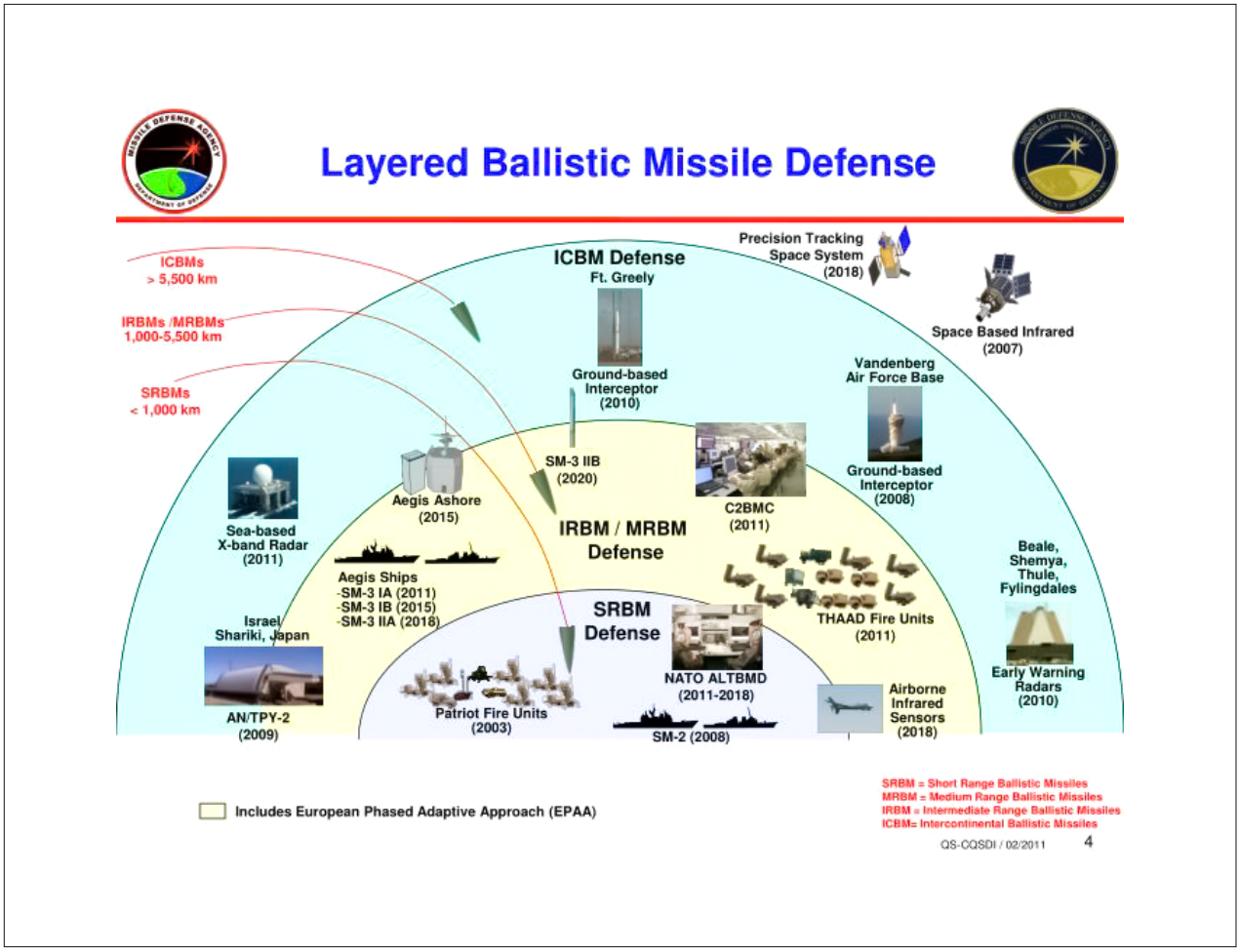


Figure 2 An overview on layered ballistic missile defense.
(https://image.slideserve.com/270253/layered-ballistic-missile-defense-n.jpg)

means that at least a part of the attack potential will survive under all circumstances.

The discussion of missile defence is generally strongly focused on ballistic missiles. Such weapons can be fired from the land or from the sea. Cruise missiles, however, can also be launched from aircraft (long-range aviation forces[10]). Occasionally, it is mentioned that the *critical* discussion is limited to defence capabilities against ballistic missiles whilst neglecting long-range aviation. However, when analysing the balance of strategic deterrence, the focus is justifiably on land- and sea-based assets, because they make up the main deterrent capability. As a rule, only these assets are permanently operational (in the much-quoted "hair-trigger alert"[11]), mostly in hardened silos and/or in concealed emplacements or under water (at least some). In critical situations, aircraft-based deterrents must be able to take off and then reach their theatre of operations. With a view to the permanent, revived practice of Russia's long-range aviation forces, these assets primarily perform a visible warning function in times of peace and tension, due to their ostentatious muscle flexing above the Atlantic Ocean, the North and Baltic Seas. Such a function cannot be performed by land-based systems (apart from test launches which naturally have to be carried out on Russian territory), but rather by sea-based systems which are visible above the water surface and invisible below. Operations and operational planning in that field, particularly of strategic submarine forces, are probably among the best-kept secrets on this globe.

Missile defence as a promise

Terms such as "missile defence" or even "missile defence shield" insinuate a defensive, if not peaceful, character. At the same time, they hold the hardly verifiable promise that it may be possible to ward off a strategic attack. An analysis and subsequent political consultancy must go deeper. What are the interrelationships between strategic defensive and offensive? What is the net balance of strategic missile defence capability, considering all the consequences and side effects?

In 2002, the United States unilaterally terminated the Anti-Ballistic Missile (ABM) Treaty due to the development of a *National* Missile Defence (NMD), i.e. a defense against limited ballistic missile attack, whether intentional, acciden-

10 These cruise missiles are often similar to the related ground-or sea-launched variants.

11 Cf. David Wright/Eryn MacDonald/Lisbeth Gronlund, Reducing the Risk of Nuclear War. Taking Nuclear Weapons Off High Alert, January2016, <http://large.stanford.edu/courses/2018/ph241/misra1/docs/ucs-jan16.pdf>

Figure 3 BMEWS solid-state phased-array radar at RAF Fylingdales, UK. (https://commons.wikimedia.org/wiki/File:Radar_RAF_Fylingdales.jpg)

tal, or unauthorized.[12] This was preceded by some years of intensive discussions with Russia as well as the allies about the possibility of maintaining the treaty or at least saving it in a modified form. The Clinton Administration had already made every effort to convince its European allies of the necessity to develop a missile defence capability by showing off the range of current and future Iranian long-range missiles. Germany, at least the German ministries, were not really convinced, and the same was true for the majority of the German public, as far as it was interested at all. Already at that time, Berlin was of the opinion that it was important to not neglect but rather include the effects of new missile defence capabilities on Moscow. As far as we know, the European NATO partners, in particular, had been informed by the Russian side at an early stage that the installation of a far-reaching missile defence capability, practically on Russia's doorstep, would cost them "something". This may very well also have been an attempt to drive a wedge between the allies. In the end, Moscow refused to compromise and negotiate any further. The buck was thus passed to Washington which then (in 2002) consequently terminated the bilateral ABM Treaty.[13]

The prominent example of Iran and North Korea shows that the main U.S. concern has been and still is not least *escalation dominance*. All cards against "rogue states" are on the table, including offensive ones. Missile defence thus works, preventing certain *response* options. To put it in the words of the MDR 2019 (p. IX): It is about "Enabling Regional and Transregional Military Operations".

The prominent example of Iran and North Korea shows that the main U.S. concern has been and still is not least *escalation dominance.*

Allies play a *certain* role in the national security strategy of the United States, depending not least on the depth of the bilateral relationship. In Europe, these are primarily Great Britain and Denmark, where the radar stations in Fylingdales and Thule have been a defensive element of missile defence architecture for a long time. With their decision in favour of a European Phased Adaptive Approach (EPAA) at the NATO Summit in Lisbon in the autumn of 2010, all NATO members endorsed a kind of missile defence intended to protect the territory and the population in the long term. The components were distributed in Germany (Missile Defence Headquarters Ramstein, operational), Romania (Defence Station Deveselu, operational), Poland (De-

12 On "Reducing the Risk of Inadvertent or Unauthorized Launch" cf. a presentation at Stanford University: <http://faculty.publicpolicy.umd.edu/sites/default/files/fetter/files/Presentations/2002-08-18-Stanford.pdf>

13 Similar to what is going to happen now with the INF-Treaty.

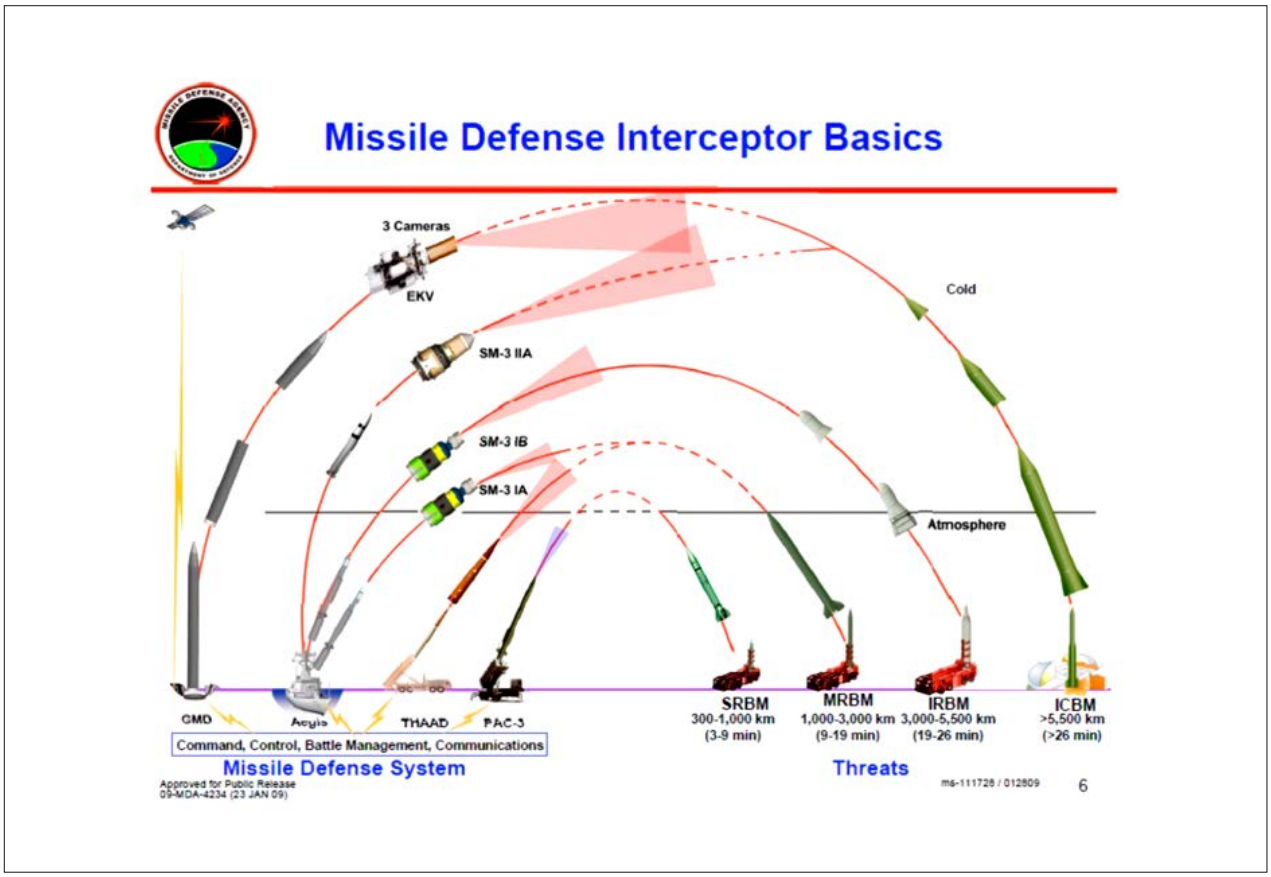


Figure 4 Spectrum of current U.S. ballistic missile defense interceptors. (https://www.quora.com/Does-the-US-have-a-missile-defense-system-capable-of-shooting-down-an-ICBM-launched-from-North-Korea)

fence Station Redzikowo, not yet operational[14]) and at European waters (missile defence enabled AEGIS cruisers).

Dynamic international situation developments: The suspension of the INF-Treaty

The international situation has developed dynamically in the last four years, to put it mildly. Today, the Russia we are dealing with is a completely different country. For years (since 2014 officially), there have been good reasons to believe that Russia has been violating the Treaty between the United States of America and the Union of Soviet Socialist Republics on the Elimination of their Intermediate-Range and Shorter-Range Missiles (INF Treaty) by introducing new ground-based medium-range cruise missiles.[15] After the announcement by President Trump of October 20, 2018, to withdraw from INF, "the United States suspended its participation in the treaty and submitted its official notice of withdrawal February 2, 2019. Russia responded by suspending its participation on February 2, 2019, as well".[16]

NATO is thus faced with difficult issues. The Lisbon consensus stipulates that missile defence would not be directed against Russia's "strategic potential of deterrence". However, no consideration is given to the fact that – from Moscow's perspective – this also means putting European centre of gravity at risk. Yet, NATO's new missile defence capabilities may very well cause some "irritation" in Moscow.

The European Phased Adaptive Approach (EPAA) will retain its inherent adaptive character. In this context, it has to be mentioned that

a. the originally planned Phase IV of the EPAA which was cancelled in 2013 considering more powerful interceptor missiles would have included intercontinental ballistic missile defence systems[17];
b. the plans of the G.W. Bush Administration for a strategic early-warning radar deployment in the Czech Republic, which would have looked far into Russia.

Defence against Russia's missiles has so far by no means been an operational level of ambition of a NATO European Missile Defence capability (EPAA).

14 On the delay see Paul Mc Leary, 23Mar2018, <https://breakingdefense.com/2018/03/crucial-polish-missile-defense-site-delayed-two-years-mda/>

15 An always current comprehensive summary is provided by Amy F. Woolf, Russian Compliance with the Intermediate Range Nuclear Forces (INF) Treaty: Background and Issues for Congress, CRS report, Washington, last update 08February2019, <https://fas.org/sgp/crs/nuke/R43832.pdf>

16 Ibid, Summary, p1

17 See below, footnote 23.

If the cooperation options with Russia, being accepted and envisaged in Lisbon, are dropped, NATO must address the question as to what extent the EPAA shall be adapted to Russian missiles. It is foreseeable that two opposing positions will be facing each other. One side sees it as completely undisputed that in the new (old) world of Article V *any* defence capability, i.e. including missile defence, must be focussed on Russia. The other side[18] will remain steadfast, pointing to the cooperative orientation of the Lisbon Treaty (which has been adapted continuously since its entry into force), and possibly also to Russia's "overwhelming" long-range and short-distance missile capabilities. Defence against Russia's missiles has so far by no means been an operational level of ambition of a NATO European Missile Defence capability (EPAA). However, the problem will be that the already established architecture, at least on Russia's doorstep in Romania and then Poland, will naturally suggest itself as a good basis for developments and adjustments. A kind of worst-case scenario is that the respective perceptions and actions of Russia and NATO will goad each other in some kind of vicious circle.

Summing up, the following can be stated: The missile defence dossier is surely not the most urgent problem facing the relationship between Russia and NATO – but it is a significant stumbling block. Recent studies such as from Peter Rudolf of *Stiftung Wissenschaft und Politik*[19] have demonstrated convincingly that there are many stumbling blocks: The renewed emphasis on nuclear weapons with low explosive power[20], the progress made in the field of cyber warfare, precise long-range (conventional) weapons[21], anti-satellite weapons and autonomous weapon systems in connection with the development of missile defence may well raise the question as to how a solid "relationship of deterrence" (Rudolf) between the United States and Russia and between the United States and China can be maintained in future. The term of "Counterforce Revolution" has been circulating in the American discussion also in the sense of new possibilities of neutralising adversary nuclear weapons. All this does not really convey the impression of solid relationships of deterrence.

The term of "Counterforce Revolution" has been circulating in the American discussion also in the sense of new possibilities of neutralising adversary nuclear weapons.

18 Presumably, Germany and France will be the main voices of this side.
19 See footnote 2.
20 Cf. Robert W. Nelson, Low-Yield Earth-Penetrating Nuclear Weapons, Jan/Feb2001, <https://fas.org/faspir/2001/v54n1/weapons.htm> and several pieces by Michael Krepon, Stimson Center, Washington, 2017/2018, e.g. <www.armscontrolwonk.com/archive/1206289/the-highly-questionable-case-for-new-low-yield-options/><www.armscontrolwonk.com/archive/1202952/low-yield-nuclear-weapons-again/> <https://www.armscontrolwonk.com/archive/1205546/tom-schelling-mini-nukes-and-the-nuclear-taboo/>, see also Amy F. Woolf, A Low Yield, Submarine-Launched Nuclear Warhead: Overview of the Expert Debate, March 21, 2019, <https://fas.org/sgp/crs/nuke/IF11143.pdf>
21 Cf. Amy F. Woolf, Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues, CRS Report, Washington, 8January2019, <https://fas.org/sgp/crs/nuke/R41464.pdf>

It is currently assessed that the United States is unlikely to grant North Korea a relationship of nuclear strategic deterrence at eye level. Ideally, this kind of new engagement network described above would deny such an opponent the realistic option of (successfully) employing nuclear weapons. However, two important questions still need to be answered:

a. How would *the / a* new "integrated" US engagement network[22] (together with its allies) look like?
b. What position would Russia and China respectively take?[23]

Solid relationships of deterrence? United States – Russia and China – India

Although the second-strike capabilities of Russia and China are not at risk *for the time being*, it is undisputed that the question of "Quo vadis USA?" is of great relevance to global stability. President Trump is certainly not the / our preferred communicator in this matter. However, he is not causally responsible for the security dilemma, i.e. requirement to ensure security under nuclear deterrence. Already Ronald Reagan had missile defence visions, the realisation of which were to offer a way out of the security dilemma. Space forces played an important role in these visions. By establishing a national space force as of 2020, Trump is ultimately following this tradition. It remains to be seen what this means exactly.[24] As the Missile Defence Review (MDR) 2019 shows, it will include missile defence – sensors, so far. The discussion about weapons in space is again gaining momentum.[25] In this case, the following applies as well: "Open-end level of ambition". MDR 2019 is putting it pretty clearly: "Consequently, the United States will not accept any limitation or constraint on the devel-

22 "In the longer term, it is the aim of the US administration to build a global network of mobile interceptors and sensors", Götz Neuneck/Christian Alwardt/Hans Christian Gils, Ballistic Missile Defense in Europe, A Study of the „Forum Friedens und Konfliktforschung" of the Science Academy in Hamburg in cooperation with the Institute for Peace Research and Security Policy at the University of Hamburg, November 2010 (!), p.3, <http://www.unidir.org/files/medias/pdfs/executive-summary-g-neuneck-eng-0-324.pdf>
23 "Assuming that the Aegis system has the proposed reliability and ability to work under realistic conditions, it can, at least from the Russian and Chinese perspective, again pose a threat to the strategic nuclear arsenals of both countries. This would be a serious obstacle for further disarmament", ibid., p.3; on Aegis vs. ICBMs see also George N. Lewis, update 05Jun2018, <https://mostlymissiledefense.com/2018/06/05/update-on-aegis-sm-3-block-iia-against-icbms-june-5-2018/>, beginning with: "In a post nearly two years ago, I argued that the SM-3 Block IIA interceptor, scheduled to begin deployment on U.S. (and Japanese) ships and Aegis Ashore sites in the next few years, would almost certainly be capable of intercepting ICBMs (at least in the absence of effective countermeasures). Moreover, they could cover the entire United States from a relatively small number of locations. I further argued that since these interceptors would likely be deployed in large numbers, and often on mobile platforms, their deployment could pose a severe threat for any possible reductions in nuclear forces by the United States and Russia." Fulfilling this prediction, the MDR 2019 now states: "Congress has directed DoD to examine the feasibility of the SM-3 Blk IIA against an ICBM-class target. MDA will test this ... capability in 2020. ... Land-based sites in the United States with this ... missile could also be persued "(p. 55); and here we are: <https://nationalinterest.org/blog/buzz/navy-vs-nukes-us-navy-plans-test-missile-defenses-against-icbm-47942>, by Kris Osborn, 18March2019.
24 Cf. Ledyard King, 23October2018, <https://eu.usatoday.com/story/news/politics/2018/10/23/space-force-trump-administration-details-trajectory-pentagon-plan/1739251002/>
25 "As rogue state missile arsenals develop, the space-basing of interceptors may provide the opportunity to engage offensive missiles in their most vulnerable initial boost phase of flight, before they can deploy various countermeasures" (MDR 2019, p. XI).

Figure 5 The First ever test of the Indian Advanced Air Defence (AAD) Missile, conducted on 6 December, 2007. (https://upload.wikimedia.org/wikipedia/commons/6/6d/AAD_Launch_Crop.jpg)

opment of missile defense capabilities needed to protect the homeland against rogue missile threats".[26]

Russia and China are working on developing new national engagement networks. This explicitly includes missile defence and, in the sense of an asymmetric approach, primarily the cyber domain and space. From an external perspective, a realistic assessment on the likelihood of such capabilities remains difficult. A lot of information remains hidden and some tests cannot be carried out in peacetime under realistic conditions. In principle, however, the three rivals are not at eye level. Only the United States is pursuing the declared goal of a sustained comprehensive military superiority. China knows that it would not stand a chance if directly challenging this superiority. Therefore, it is pursuing a different and softer strategy. Acting in the spirit of the ancient Chinese strategists, the goal is to be reached without a fight. This is illustrated by the activities in the South China Sea. Proceeding tenaciously, Beijing is obviously planning to establish a sinocentric world order by the middle of the 21st century.

The nuclear powers China, India and Pakistan are in a triangular relationship, in which strategic armaments efforts of one side are almost automatically followed by cascading measures of the other two sides.

26 MDR 2019, p. IX

At this point, the "Asian Cascade"[27] should be briefly touched upon. The nuclear powers China, India and Pakistan are in a triangular relationship, in which strategic armaments efforts of one side are almost automatically followed by cascading measures of the other two sides. To put it simply: If China modernises and expands its strategic nuclear weapons potential (most recently by equipping its long-range missiles with cluster warheads), particularly due to the United States' missile defence, India will feel threatened and react accordingly. This, in turn, will evoke a reaction from Pakistan (with Chinese support by the way). Hence, the fact that both India and Pakistan are working to develop strategic missile defence capabilities is logical from a military perspective. Whether this is the right way to help promote stability in this arena, is highly doubtful. India and Pakistan do not have an established relationship of deterrence. The war on Kargil 1999 did show that the threshold of a "nuclear-armed face-to-face" could be reached quite quickly.[28]

Unlimited arms races are not conducive to stability, neither in this volatile region, nor elsewhere. Generally, it is assumed that offensive armaments are in most cases preferred to defensive ones based on the perception that their acquisition is comparatively easier and often cheaper.

And Europe?

Finally, let us take a look at Europe, beginning with some short remarks about Switzerland. The development of a new ground-based missile defence system ("BODLUV") will help Switzerland to complete its capabilities in the field of air-breathing target engagement. Additionally, Switzerland de facto benefits from being protected by the (virtual) screen of the EPAA. Within the legal boundaries of Swiss neutrality, this raises the issue of a possible Swiss participation in EPAA's information processes.

Within the legal boundaries of Swiss neutrality, this raises the issue of a possible Swiss participation in EPAA's information processes.

NATO Europe is involved in the relationship of deterrence between the United States and Russia. The European public likes to avoid this issue. Nuclear participation with tactical nuclear weapons stationed in Germany, Italy, Belgium, the Netherlands and Turkey is an issue one does not like to talk about. Missile defence with its defensive connotation seems less unpleasant.

27 Krepon, 2003, pp. 131ff

28 Krepon, 09July2018, <https://www.armscontrolwonk.com/archive/1205441/the-holy-grail-of-deterrence-stability/>, quote: "The Pakistan-India strategic competition constitutes a far different case. These 'middle powers' in the global nuclear order have outstanding grievances that have only been magnified by the acquisition of nuclear weapons. Their limited conventional war in the heights above Kargil and subsequent crises ratcheted up the nuclear competition on the subcontinent. China's strategic modernization programs and history of supporting Pakistan's nuclear ambitions, both civil and military, pose another significant complication. A triangular strategic competition is inherently unstable when all three of its legs are of different size, and two legs are conjoined at the expense of the third."

The situation appears different for the traditional European nuclear powers Great Britain and France. Any power that possesses nuclear weapons must at least be interested in strategic early-warning information. As mentioned before, the United Kingdom with its station in Fylingdales has been an integral part of the western missile defence architecture for a long time. Although this is not the case with France, it is safe to assume that resilient early-warning channels exist in the direction of the "Grande Nation". For the time being, there is no question of both nations making strategic contributions to *active* missile defence. Their territories, at least, are not very well suited due to their "rearward" position.

However, the following question remains: Which capabilities, apart from those in the tactical-operational area (e.g. PATRIOT and its successors)[29], are to be ultimately included in a new strategic missile defence capability and which not? It seems difficult to imagine and would financially not be feasible, at least in the foreseeable future, for nations like Germany to establish a missile defence screen that would significantly protect the entire country.

… a comprehensive and reliable protection against the abundance of Russian missiles can never be achieved, especially not against (very fast) cruise missiles.

The important fact remains that Moscow would not remain passive in the event of a substantial change in the relationship of deterrence. Russia, as our close neighbour, has a great variety of offensive airborne, sea- and land-based missile options. A main argument of this analysis is that a *comprehensive* and *reliable* protection against the abundance of Russian missiles can never be achieved, especially not against (very fast) cruise missiles. Russia's alleged breach of the INF Treaty, which most presumably will lead to its termination, is not least one of the late effects to follow the termination of the ABM Treaty. Cruise missiles, in particular, are an effective and relatively inexpensive option against missile defence and its components.[30]

Instead of getting caught up in expensive and, in our view, nonsensical arms races, it is more advisable to undertake arms-control efforts[31] at global and regional level, aimed at establishing a ruled-based order. For this purpose, it seems appropriate to regard the strategic offence *and* defence, thus taking a holistic-combined approach. The main finding of this analysis is that unlimited strategic missile defence and / or unrealistic ambitions with regard to comprehensive "protective shields" most likely will fail to demonstrate that they really do help to promote stability and security.[32]

The British and French nuclear-strategic offensive approach, including in the field of Europe's defence, seems expedient: providing a limited set of capabilities, which are *sufficient* to achieve the defined objectives. Translated into missile defence, this would mean the following: Establishing a limited capability that makes it possible to intercept a limited number of long-range missiles. As long as we will have to live with nuclear weapons, from a specific threshold, nuclear deterrence must be employed, particularly vis-à-vis Russia. The hope remains that, contrary to current trends, dialogue and trust will not entirely be lost.

Stefan C. P. Hinz

Colonel (GS) Dipl-Kfm (univ), German Air Force. He is currently seconded from the German Armed Forces to the Geneva Centre for Security Policy (GCSP). With a background in Military Politics, he has been serving in Extended Integrated Air Defence as well as at the German Ministry of Defence and Ministry of Foreign Affairs respectively.

E-Mail: s.hinz@gcsp.ch

29 These are undisputed elements of pre-deployment preparations and planning at the periphery of the NATO Alliance, i.e. also of exercises such as the most recent Trident Juncture.

30 Krepon, 07 March 2018, <https://www.armscontrolwonk.com/archive/1204843/the-belated-consequences-of-killing-the-abm-treaty/>, quote: "A *second* consequence [of killing the ABM Treaty], long anticipated, is renewed emphasis on cruise missile penetration capabilities.", further: "A *third* consequence is renewed freaked out behavior by the Kremlin and the somewhat revived Russian military industrial complex. …. A *fourth* consequence, I regret to surmise, is the renewal of freaked out behavior by the U.S. missile defense complex, which will be encouraged by the usual precincts on Capitol Hill to explore space-based interceptors once again. A *fifth* consequence (not to be a complete downer) might be the demise of new U.S. low-yield warhead options previously championed in Trump's Nuclear Posture Review. The notion of escalating to de-escalate, which low-yield options were presumably designed to counter, seems downright silly after Putin's new laundry list of nuclear overkill. … A *sixth* consequence of killing the ABM Treaty — and one that is worth dwelling on here and elsewhere — is the prospective demise of a numerically-based system of U.S.-Russian strategic arms control and reductions. …."

31 "Given the still unsolved technical challenges, the reliability of missile defense will not be guaranteed. Consequently, politicians and military will never rely completely on such a system. This implies that diplomatic means, a common realistic threat assessment, improved early warning and effective arms export controls and regional arms con-trol initiatives will continue to be necessary and should be expanded. This includes for example the reactivation and emphasis on the "Hague Code of Conduct", Neuneck et al., 2010; their comprehensive update in: Schriften der Akademie der Wissenschaften in Hamburg, Raketenabwehr in Europa, Baden-Baden 2015, elaborating on the utopy of an impenetrable Missile Defence shield

32 Quite harsh: Oliver Meier, SWP Berlin: "Well, if … Trump intended to fuel Russian paranoia with his MissileDefenseReview speech, I think he did a good job: US wants to be ready to destroy any missile anywhere, before and after launch. That is called a first-strike capability", see https://twitter.com/meier_oliver 17January2019

Die «Gerasimov-Doktrin» und die russischen Militärwissenschaften

Die sogenannte «Gerasimov-Doktrin» sorgte ab 2014 auf beiden Seiten des Atlantiks in Politik und Fachkreisen für Aufregung. Viele Analysen übersahen gewissermassen Gerasimovs Verankerung in den russischen Militärwissenschaften und interpretierten sie als den Plan zur Annexion der Krim und der Unterstützung der Separatisten in der Ostukraine. Betrachtet man jedoch den Entstehungskontext der Rede sowie vorhergehende und darauffolgende sicherheitspolitische Entwicklungen, kann die Existenz einer «Gerasimov-Doktrin» als Grundlage «hybrider Kriegsführung» angezweifelt werden. Wir stellen uns in unserem Beitrag der Frage, warum eine Beschäftigung mit Gerasimov dennoch sinnvoll sein kann.[1]

Hanna Grininger, Christoph Bilban

Ab Mitte 2014 wurde die Rede des russischen Generalstabschefs Valerij Gerasimov, die er im Jänner 2013 vor der Generalversammlung der Russischen Akademie der Militärwissenschaften (AMW) gehalten hatte[2], im Westen als Grundlage der «hybriden Kriegsführung» Russlands bzw. dessen aussen- und sicherheitspolitischen Handelns bekannt. Die als «Gerasimov-Doktrin» bezeichneten Ausführungen bekamen besonders vor dem Hintergrund der Annexion der Krim und der Kämpfe in der Ostukraine viel Aufmerksamkeit.[3] In seiner Rede betonte Gerasimov u. a. das Verschwimmen der Grenzen zwischen Krieg und Frieden und die gestiegene Rolle nicht-militärischer Mittel in aktuellen und zukünftigen Konflikten. Die von Gerasimov angesprochene Relevanz von Spezialeinsatzkräften und die Nutzung des Protestpotenzials der Bevölkerung liessen sich gedanklich leicht den Ereignissen auf der Krim zuordnen. Besonders zwei grafische Darstellungen zu Verlauf und Charakter moderner Konflikte konnten ausserdem mit dem damals sehr populären Diskurs über hybride Kriegsführung verbunden werden (siehe Abbildungen 1 und 2). Viele westliche Analysen wollten in Gerasimovs Rede eine «Handlungsanleitung für die russische Militäroperation»[4] in der Ukraine sehen, und deuteten die Inhalte der Rede entsprechend dieser Erwartungshaltung. In unserem Buch zum *Mythos «Gerasimov-Doktrin»* argumentieren wir, dass wenige Elemente aus dem ersten Teil der Rede besonders viel Aufmerksamkeit bekamen, während der Rest der Ausführungen eher ignoriert wurde. Ebenso betrachteten viele Analysen die Rede meist isoliert und ausserhalb des russischen sicherheitspolitischen Diskurses. Die «Gerasimov-Doktrin» fand dabei in verschiedenen europäischen Ländern eine quantitativ und qualitativ unterschiedliche Verbreitung.[5] Eine Auseinandersetzung mit ihren Inhalten kann dabei auch für die Einschätzung der heutigen Politik Russlands relevant sein.

Viele westliche Analysen wollten in Gerasimovs Rede eine «Handlungsanleitung für die russische Militäroperation» in der Ukraine sehen, und deuteten die Inhalte der Rede entsprechend dieser Erwartungshaltung.

1 Dieser Beitrag stellt einen eigenständigen Aufsatz dar, der auf der von der Autorin und dem Autor herausgegebenen Publikation basiert, welche in dieser Ausgabe unter den Buchbesprechungen rezensiert wird.

2 Gerasimov, Valerij: Cennost' nauki v predvidenii. In: Voenno-Promyšlennyj Kur'er, 27.02.2013, S. 1–3.

3 Vgl. z. B. Freedman, Lawrence: Ukraine and the Art of Limited War. In: Survival, 6/2014, S. 7–38, hier: S. 15.; Kuster, Matthias: Die Ukraine-Krise 2014/2015 aus militärstrategischer und operativer Sicht. In: Military Power Revue, 2/2015, S. 15–26, hier: S. 25.

4 Bilban, Christoph/Grininger, Hanna/Steppan, Christian: Gerasimov – Ikone einer tief verwurzelten Denktradition. In: Bilban, Christoph/Grininger, Hanna (Hrsg.): Mythos Gerasimov-Doktrin. Ansichten des russischen Militärs oder Grundlage hybrider Kriegsführung? Schriftenreihe der Landesverteidigungsakademie, 2/2019, Wien, S. 15–56, hier: S. 47.

5 Vgl. Bilban, Christoph/Grininger, Hanna: Die Regionalstudien im Vergleich. In: Bilban, Christoph/Grininger, Hanna (Hrsg.): Mythos Gerasimov-Doktrin. a.a.O., S. 325–342, hier: S. 327ff.

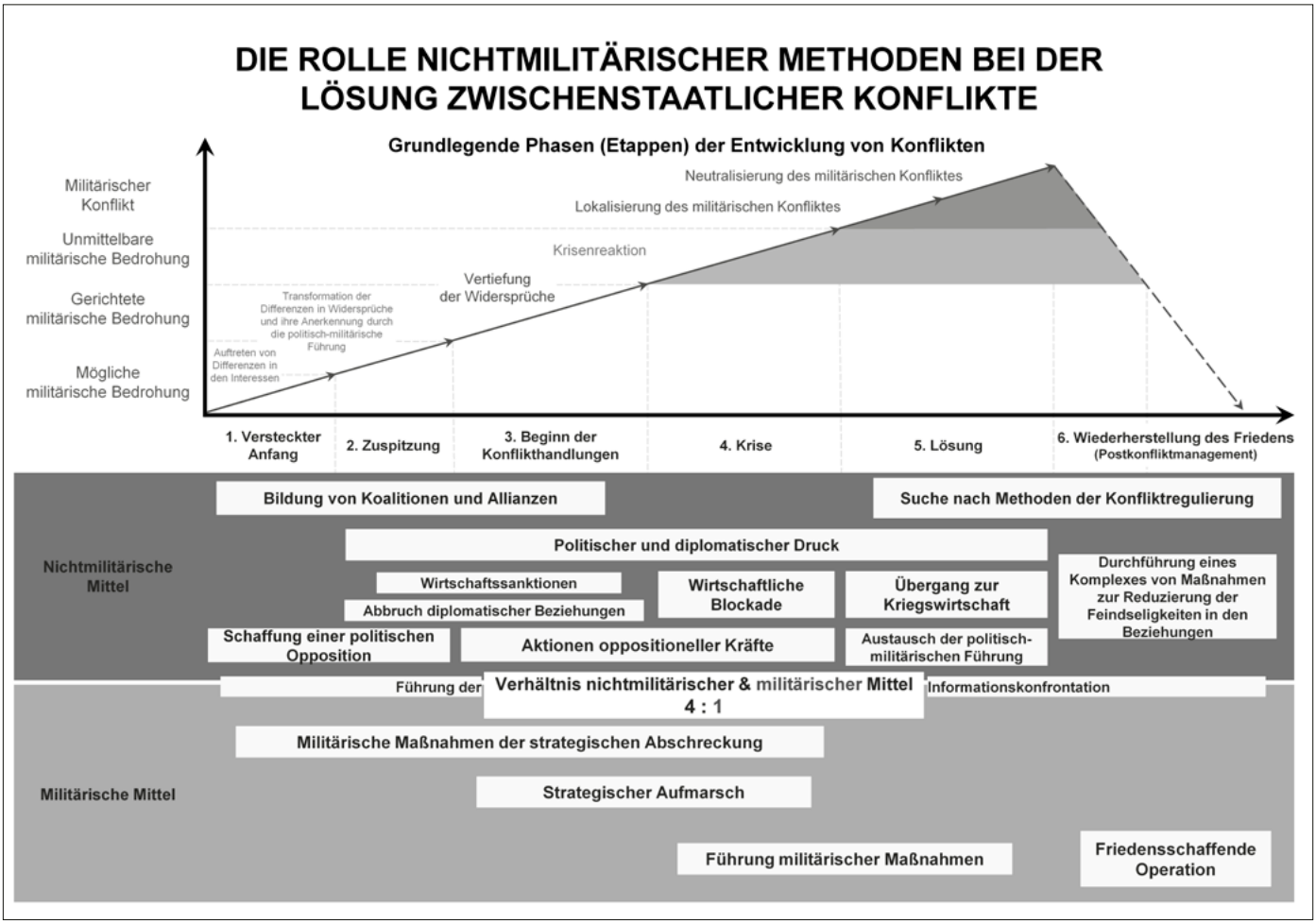


Abbildung 1 Verlauf moderner Konflikte nach Gerasimov.
(Vestnik Akademii Voennych Nauk 1/2013, S. 25; eigene Übersetzung)

Die «Gerasimov-Doktrin»

Betrachtet man die Rede des russischen Generalstabschefs genauer, lässt sich diese in vier Abschnitte gliedern: (1) die Darstellung des modernen Konfliktbildes, (2) Aufgaben der Militärwissenschaften, (3) die Notwendigkeit einer Territorialverteidigung und (4) die Rolle der Militärwissenschaften heute.

Der erste Abschnitt – so wie dies auch in den weiteren Reden Gerasimovs der Fall ist – stellt einen Abriss des aktuellen Bedrohungsbildes aus Sicht des Generalstabs dar. Kriege würden nicht mehr erklärt und verliefen auch nicht mehr nach bekannten Mustern, merkt Gerasimov gleich in seinem Eröffnungsstatement an. Diese Einschätzung ist geprägt von den Ereignissen des «Arabischen Frühlings» und den sogenannten «Farbrevolutionen»:

«Die Erfahrung kriegerischer Konflikte, einschliesslich jener im Zusammenhang mit den sogenannten Farbrevolutionen in Nordafrika und dem Nahen Osten, bestätigen, dass sich ein vollkommen gutsituierter Staat in wenigen Monaten und sogar Tagen in eine Arena heftiger bewaffneter Kämpfe verwandeln, zum Opfer einer ausländischen Intervention werden, in den Abgrund des Chaos, einer humanitären Katastrophe und eines Bürgerkriegs versinken kann.»[6]

In diesem Zusammenhang spricht Gerasimov die «Nutzung des Protestpotenzials der Bevölkerung» als Teil der «weitreichenden Anwendung politischer, militärischer, wirtschaftlicher, informationeller, humanitärer und anderer nicht-militärischer Massnahmen»[7] an. Im Vergleich zu den traditionellen Formen der Kriegsführung übertreffen diese nicht-militärischen Mittel sogar militärische in ihrer Effektivität zur Erreichung der politischen und strategischen Ziele, so Gerasimov.

Ohne den Einsatz des Militärs kommt jedoch auch Gerasimovs Ansatz nicht aus. So werden die oben genannten Massnahmen durch den Einsatz von Spezialeinsatzkräften und als Friedenstruppen getarnter militärischer Formationen ergänzt. Begleitet werden alle getroffenen Massnahmen durch Informationsoperationen. Diesem neuen Kon-

6 Gerasimov: Cennost' nauki, S. 2.
Die Übersetzungen stammen aus der deutschen Übersetzung der Rede in Bilban, Christoph: Mythos «Gerasimov-Doktrin». Eine strategieorientierte Diskursanalyse ausgewählter US-Thinktanks und des NATO Defense College. Korrigierte Version. Masterarbeit, Universität Wien 2019, hier: S. 119ff. online unter <http://bit.ly/gerasimov_de>.

7 Gerasimov: Cennost' nauki, S. 2.

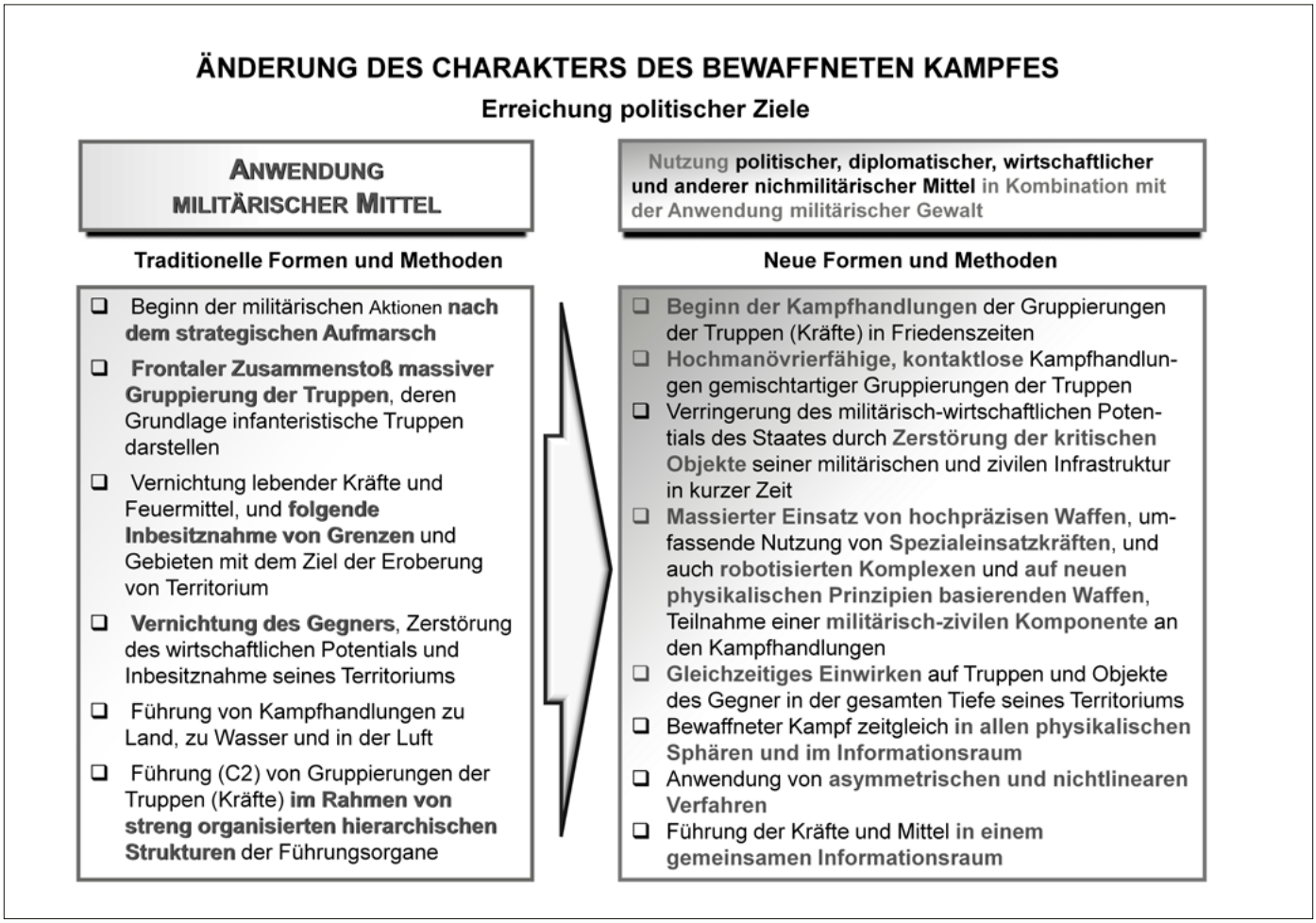


Abbildung 2 Änderungen des Charakters moderner Kriegsführung nach Gerasimov.
(Vestnik Akademii Voennych Nauk 1/2013, S. 25; eigene Übersetzung)

fliktbild begegne die russische Armeeführung mit «nichtstandardisierten» Verfahren, wie sie Gerasimov nennt. Dabei handelt es sich um die Einführung verbesserter C2-Systeme, hochmobilen und gemischtartigen Truppen, verbesserter Aufklärung und dem Einsatz präziser und weitreichender Waffensysteme. Im Grunde spricht Gerasimov hierbei von den Prinzipien netzwerkzentrierter Kriegsführung (NCW), welche in der russischen Militärtheorie schon seit 2004 intensiv diskutiert wurden.[8] Dass sich «Gerasimov-Doktrin» und die westlichen Konzepte NCW, *comprehensive approach* und *effects based operations* stark gleichen, zeigte bereits Söhnke Marahrens.[9]

Die USA, so Gerasimov weiter, würden diese neuen Methoden der Kriegsführung bereits in ihren Kriegen (z. B. Desert Storm 1991, Irak 2003) und ihren Doktrinen (z. B. *Joint Vision 2020, Global Strike*) umsetzen. In Libyen habe Washington durch den Einsatz privater Militärfirmen, einer Flugverbotszone und einer Seeblockade neue Mittel zur Unterstützung der bewaffneten Oppositionellen angewandt.

Am Rande und im Westen kaum erkannt, spricht Gerasimov hier auch die Schaffung spezialisierter Verbände für Friedensmissionen an.

Eine Antwort auf diese asymmetrischen Bedrohungen solle die Akademie der Militärwissenschaften finden. Dabei stellt Gerasimov im zweiten Abschnitt seiner Rede klar, dass die Vorbilder nicht im Ausland zu suchen seien, sondern dass Russland eigene Erfahrungen u. a. aus dem Krieg in Afghanistan (1979–1989) vorzuweisen habe. Zudem müssten sich die Militärwissenschaften mit der Rolle von Robotik und künstlicher Intelligenz in den Kriegen der Zukunft beschäftigen. All dies beeinflusse die Struktur und den Einsatz der russischen Streitkräfte, so der General weiter. In diesem Abschnitt der Rede geht Gerasimov ausserdem auf den Einsatz der Streitkräfte ausserhalb Russlands ein. Die rechtlichen Grundlagen seien bereits

8 Vgl. Vorobyov, I. N./Kiselyov, V. A.: The Role of Military Science in Russia's Changing Armed Forces. In: Military Thought, 1/2011, S. 70–79, hier: S. 75f.; Siehe auch den Hinweis auf die Artikelserie bei Kazar'yan, B. I.: Operations, Combat Actions, and Network-Centric Warfare. In: Military Thought, 1/2010, S. 82–98, hier: S. 82.

9 Vgl. Marahrens, Soenke: The Gerasimov «Doctrine». The day the West started to fight its own shadow. Canadian Forces College 2018, hier: S. 14ff.

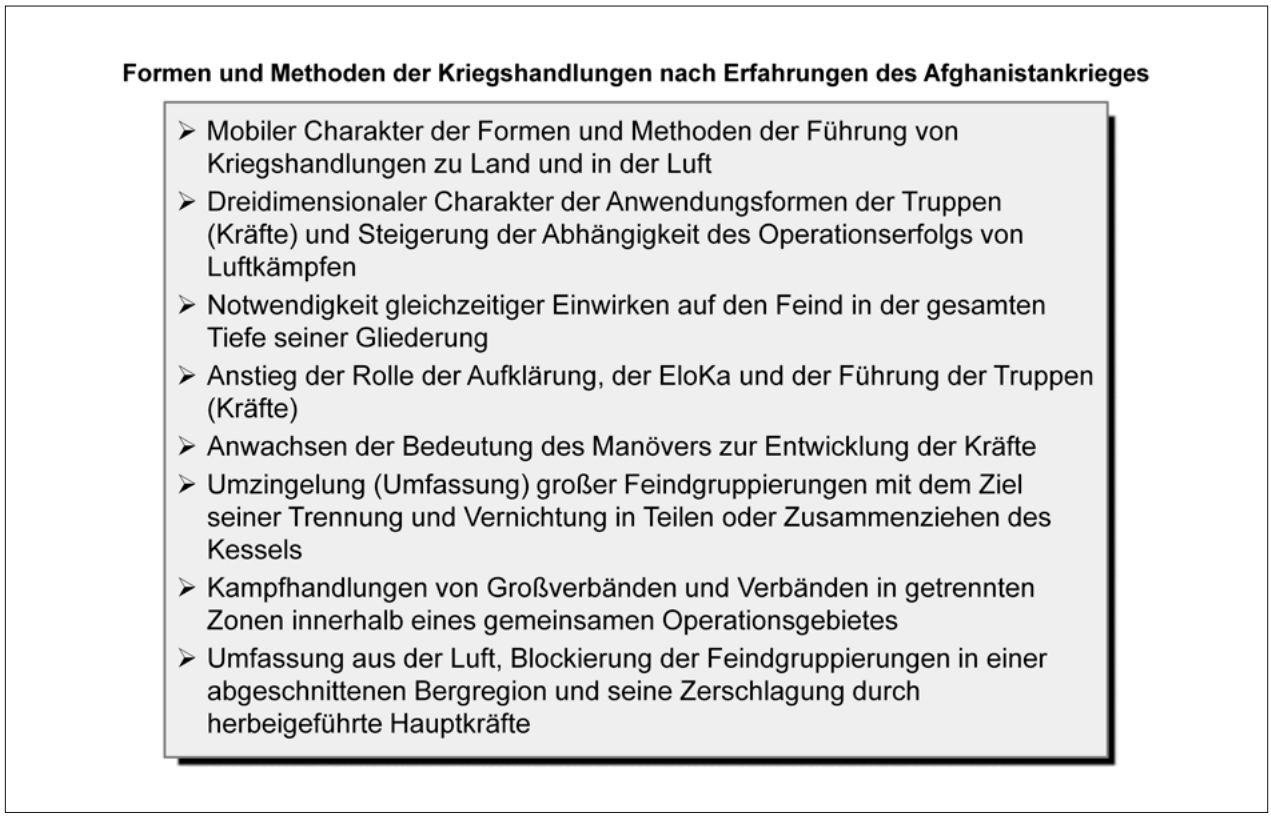


Abbildung 3 Lehren für die russische Kriegsführung am Beispiel des sowjetischen Krieges in Afghanistan. (Vestnik Akademii Voennych Nauk 1/2013, S. 26; eigene Übersetzung)

2009 geschaffen worden, aber die militärischen Verfahren müssten noch an die Bedingungen moderner Kriegsführung angepasst werden. Am Rande und im Westen kaum erkannt, spricht Gerasimov hier auch die Schaffung spezialisierter Verbände für Friedensmissionen an.

Im dritten Teil seines Vortrags fordert Gerasimov den Aufbau einer effizienten Territorialverteidigung. Durch die Reduktion der Personalstärken könnten die Streitkräfte nicht mehr die «Abwehr von Sabotage und Terroristen» sicherstellen. Daher bedürfe es Regelungen, wie die Truppen und Kräfte anderer Ministerien (z. B. Nationalgarde, Katastrophenschutz, etc.) im Krisenfall mit den Streitkräften zusammenarbeiten. Hier beansprucht Gerasimov bereits eine koordinierende Rolle des Generalstabs in Friedenszeiten, die in Form des Nationalen Führungszentrums der Verteidigung[10] *(Nacional'nyj Centr Upravlenija Oboronoj)* seit 2015 auch umgesetzt wird. Die wissenschaftlichen Grundlagen für die (Weiter-)Entwicklung der Territorialverteidigung solle die AMW beitragen, so Gerasimov 2013.

Im letzten Abschnitt seiner Rede kritisiert der Generalstabschef den schlechten Zustand der russischen Militärwissenschaften. Es fehle an grossen Denkern wie z. B. Aleksandr Svečin und Georgij Isserson aus den 1920ern. So habe bereits Isserson erkannt, dass Kriege lange vor den ersten Kampfhandlungen mit der Mobilisierung der Streitkräfte beginnen. Diese Anfangsphase des Krieges *(initial period of war)* muss folglich auch von den heutigen Wissenschaftlern erkannt werden, impliziert Gerasimov. Sein Hinweis auf die Missachtung von Issersons Warnungen durch die sowjetische Führung zeigt, wie sehr der deutsche Überfall auf die Sowjetunion 1941 für das russische Militär bis heute ein Trauma darstellt.[11] Auch moderne Theoretiker wie Sergej Čekinov und Sergej Bogdanov warnten schon in einem Artikel von 2012, dass die Anfangsphase in den «Kriegen neuer Generation» entscheidend sein werde. Dem könne Russland nur durch eine glaubhafte Abschreckung – friedlich oder mit militärischen Mitteln – begegnen.[12] Diese militärische Abschreckung solle, so Gerasimov in seiner Rede 2013, durch eine Mobilisierung des Staates auf allen Ebenen vor Beginn des Krieges sichergestellt werden.[13] Ausserdem sollen die Militärwissenschaften die Schwachstellen des Feindes erkennen und somit einen Vorteil generieren. Jeder Krieg folge seiner speziellen Logik, weshalb es umso wichtiger sei, möglichst genau vorherzusehen, in welche Kriege Russ-

10 Das Nationale Führungszentrum der Verteidigung wurde 2014 in Betrieb genommen. Es dient vor allem als gesamtstaatliches Lagezentrum und soll in Friedenszeiten vor allem eine Koordinierungsfunktion übernehmen. In Krisenzeiten soll es die Führung über die Truppen anderer Ministerien übernehmen. Laut *The Military Balance 2019* (S. 171) bestehen drei Führungszentren mit unterschiedlichen Aufgaben. Die tatsächliche Effektivität wird jedoch von Experten u. a. wegen der Rivalitäten zwischen den verschiedenen Sicherheitsbehörden unterschiedlich bewertet.

11 Vgl. dazu Cimbala, Stephen J.: Russian Threat Perceptions and Security Policies: Soviet Shadows and Contemporary Challenges. In: The Journal of Power Institutions in Post-Soviet Societies, Issue 14/15/2013, <https://pipss.revues.org/4000>, abgerufen am 12.07.2017, hier: S. 28.

12 Vgl. Chekinov, S. G./Bogdanov, S. A.: Initial Periods of Wars and Their Impact on a Country's Preparations for a Future War. In: Military Thought, 4/2012, S. 14–28, hier: S. 25f.

13 Vgl. Gerasimov: Cennost' nauki, S. 3.; Monaghan, Andrew: Russian State Mobilization: Moving the Country on to a War Footing. London 2016, hier: S. 28.

Abbildung 4 Vom Nationalen Führungszentrum aus leitet die oberste Führung der russischen Streitkräfte nicht nur den Einsatz in Syrien, sondern überwacht auch z. B. die Übernahme von neuem militärischem Gerät: Auf dem Bild das Fliegerabwehrraketensystem SA-13 Gopher (russisch 9K35 Strela-10).
(mil.ru, https://syria.mil.ru/images/upload/2018/MIL_0612.jpg)

land «hineingezogen werden könne». Die Vorausschau sei die Kernaufgabe der Militärwissenschaft, stellt Gerasimov am Ende seines Vortrags fest. Er merkt an: «Bei der Bewältigung der zahlreichen Probleme, vor denen die Militärwissenschaften heute steht, zählt der Generalstab auf die Hilfe der AMW, welche in ihren Reihen die führenden Militärwissenschaftler und angesehene Spezialisten versammelt.»[14]

Die Akademie der Militärwissenschaften

Um Gerasimovs Ausführungen richtig einordnen zu können, sollten der konkrete Entstehungskontext, sowie das sicherheitspolitische und militärische Denken Russlands betrachtet werden. Bei der «Gerasimov-Doktrin» handelt es sich, wie bereits angesprochen, um den Vortrag «Grundlegende Tendenzen der Entwicklung der Formen und Methoden der Anwendung von Streitkräften, aktuelle Aufgaben der Militärwissenschaft für ihre Umsetzung», den der russische Generalstabschef anlässlich der Generalversammlung und zugleich jährlichen militärwissenschaftlichen Konferenz der Russischen Akademie der Militärwissenschaften am 26. Jänner 2013 hielt. Knapp einen Monat nach der Versammlung erschien im *Voenno-Promyšlennyj Kur'er* (VPK, dt. *Militär-Industrieller Kurier*) am 27. Februar 2013 das journalistisch adaptierte Manuskript des Vortrags unter dem Titel «Der Wert der Wissenschaft liegt in der Vorausschau».[15]

Um Gerasimovs Ausführungen richtig einordnen zu können, sollten der konkrete Entstehungskontext, sowie das sicherheitspolitische und militärische Denken Russlands betrachtet werden.

Der VPK ist eine wöchentlich erscheinende russische Fachzeitung zu vorwiegend militärischen und sicherheitspolitischen Themen aus ökonomischer, politischer und historischer Perspektive. Er gehört einem Konsortium mehrerer Rüstungskonzerne, darunter Almaz Antej[16]. Zwei Russlandforscher, Roger McDermott und Charles Bartles, zeigten hinsichtlich des Publikationsmediums Verwunderung. Nach Meinung von McDermott hätte der «inhärent militärwissenschaftliche» Artikel sein Zielpublikum besser in der offiziellen Zeitschrift des Generalstabs, *Voennaja Mysl'* (dt. *Militärischer Gedanke*), erreicht.[17] Bartles hingegen meinte, dass Gerasimov durch die Veröffentlichung im

14 Gerasimov: Cennost' nauki, S. 3.

15 Vgl. Bilban: Mythos «Gerasimov-Doktrin», S. 44.
16 Vgl. Voenno-Promyšlennyj Kur'er: O gazete. <https://vpk-news.ru/about>, abgerufen am 28.01.2019.
17 Vgl. McDermott, Roger N.: Does Russia Have a Gerasimov Doctrine. In: Parameters, 1/2016, S. 97–106, hier: S. 100.

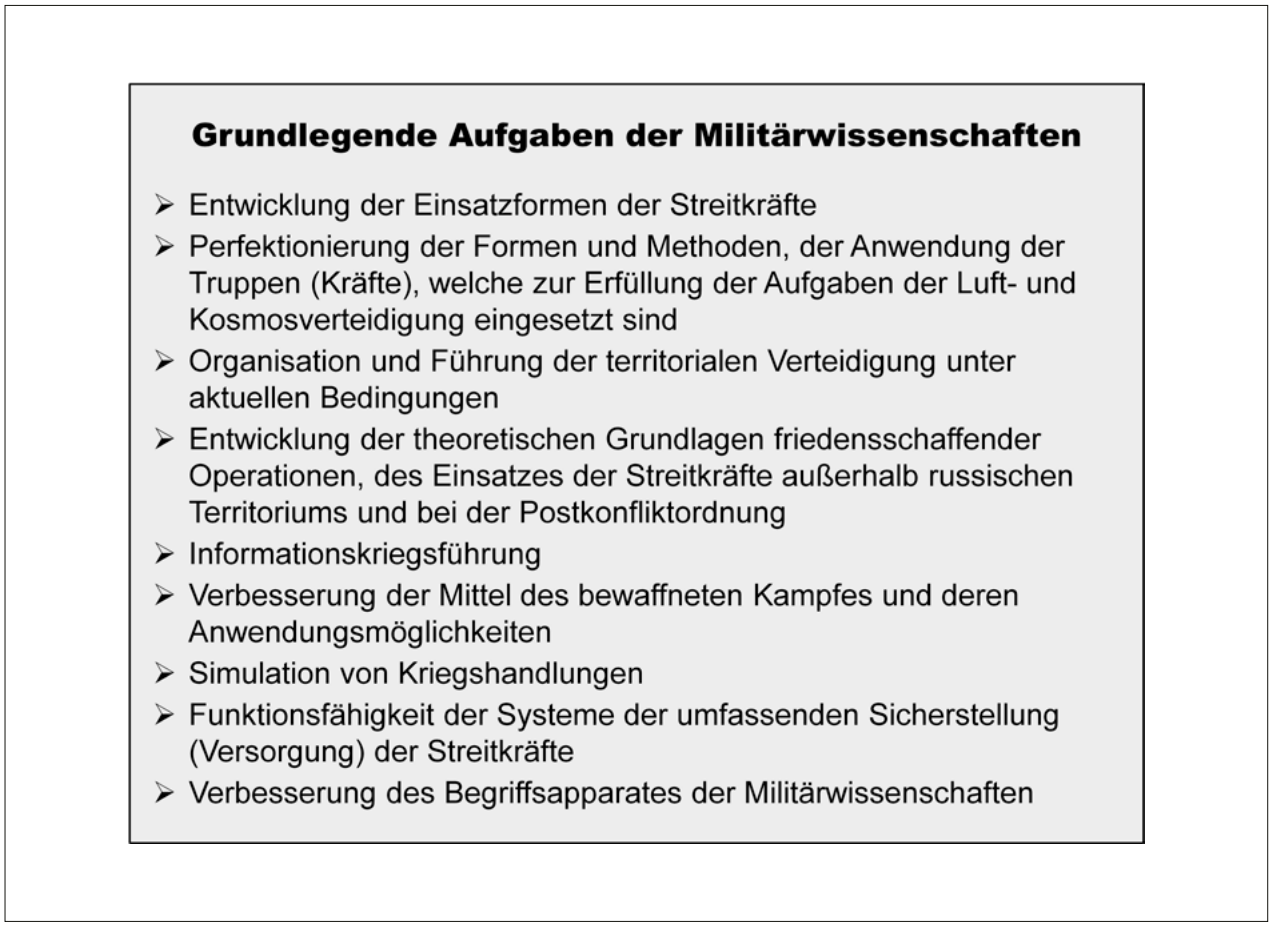


Abbildung 5 Auflistung der Aufgaben für die Militärwissenschaften nach Gerasimov. (Vestnik Akademii Voennych Nauk 1/2013, S. 28; eigene Übersetzung)

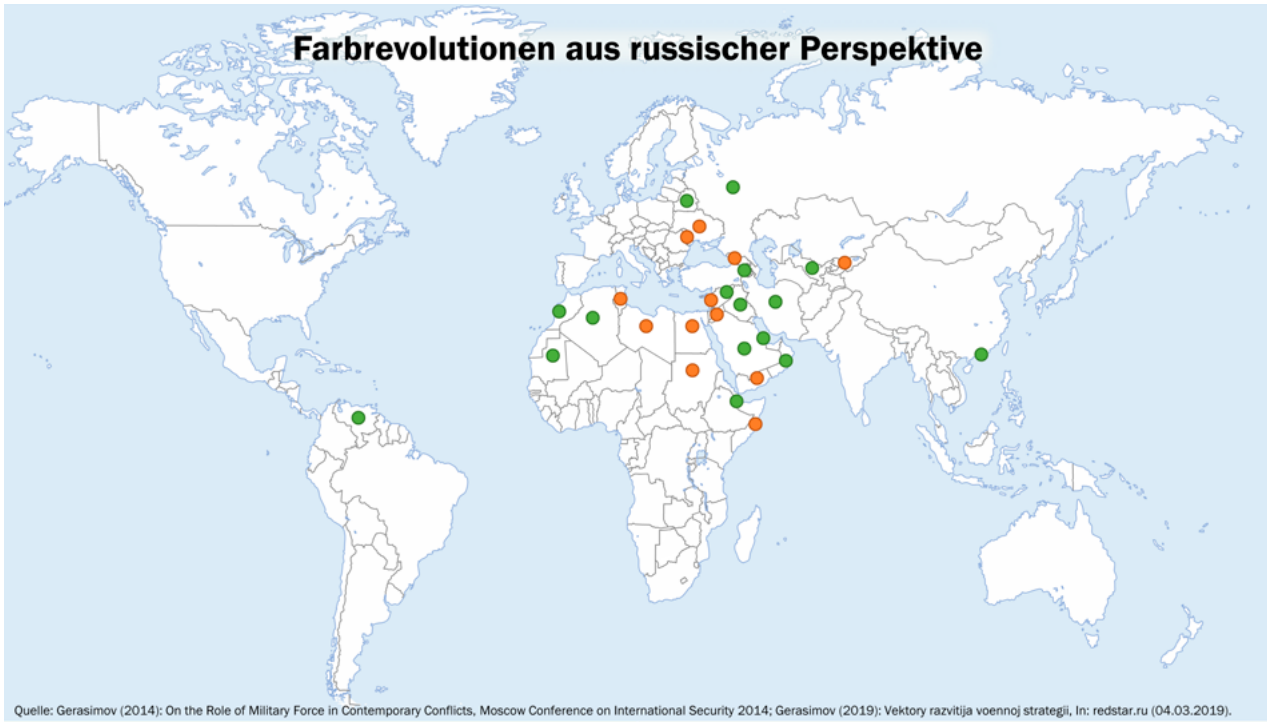
VPK die politische Führungsspitze ansprechen wollte.[18] Zu beachten ist jedenfalls, dass schon die Vorträge von Gerasimovs Vorgängern und alle seine seit 2013 jährlich gehaltenen Reden immer im VPK erschienen. Die Fachzeitung ist ausserdem ein Partner der Russischen Akademie der Militärwissenschaften[19] und berichtet jedes Jahr von der Generalversammlung.

Die weniger bekannte Originalversion des Redemanuskripts findet sich im *Vestnik Akademii Voennych Nauk* (dt. *Anzeiger der Akademie der Militärwissenschaften*). Diese Version unterscheidet sich vom Abdruck im VPK durch zusätzliche Abbildungen über die Aufgaben der Militärwissenschaften (siehe Abbildung 5), die Lehren aus dem sowjetischen Afghanistankrieg, die gesetzlichen Grundlagen zum Einsatz der Armee im Ausland, die US-amerikanischen Entwicklungen robotisierter und automatisierter Waffensysteme, sowie Bilder der bedeutendsten russischen Militärtheoretiker des frühen 20. Jahrhunderts und die Darstellung des Verfahrens der «Tiefen Operationen» nach Triandafillov und Tuchačevskij.[20] Durch die zusätzlichen Grafiken wird das Thema Militärwissenschaften in Gerasimovs Vortrag deutlicher unterstrichen als in der VPK-Version.

Klima der Angst: Massenproteste und Arabischer Frühling

Für die Interpretation der «Gerasimov-Doktrin» muss auch der spezifische Zeitpunkt der Rede beachtet werden. Anstatt Gerasimovs Rede durch den Bezug auf die Ukrainekrise zu erklären, lohnt sich ein Blick in die Zeit der Jahre davor. Anders als im Westen beruht Russlands sicherheitspolitisches Denken, so einige Forscher, nicht auf einem post-2014-Szenario; vielmehr lebt Moskau in einer «post-2011/12-Welt».[21] Gerasimovs Ausgangspunkt sind die Lehren des Arabischen Frühlings im Speziellen und die sogenannten Farbrevolutionen im Allgemeinen. Diese Art des zwischenstaatlichen Konflikts werde, so der Generalstabschef, den typischen Krieg des 21. Jahrhunderts ausmachen.[22]

18 Vgl. Bartles, Charles K.: Getting Gerasimov Right. In: Military Review, 1/2016, S. 30–38, hier: S. 31.
19 Vgl. <http://avnrf.ru/index.php>, abgerufen am 09.04.2019.
20 Vgl. dazu Gerasimov, Valerij V.: Osnovnye tendencii razvitija form i sposobov primenenija vooružennych sil, aktual'nye zadači voennoj nauki po ich soveršenstvovaniju. In: Vestnik Akademii Voennych Nauk, 1/2013, S. 24–29.
21 Vgl. Monaghan, Andrew: Ukraine Crisis in Hybrid Warfare Context with a Historical Perspective (06.08.2016). <http://www.ccw.ox.ac.uk/blog/2016/6/8/ukraine-crisis-in-hybrid-warfare-context-with-a-historical-perspective>, abgerufen am 12.07.2017; Siehe auch Giles, Keir: Moscow rules: what drives Russia to confront the West. London 2019, hier: S. 46f.
22 Vgl. Gerasimov: Cennost' nauki, S. 2.



Quelle: Gerasimov (2014): On the Role of Military Force in Contemporary Conflicts, Moscow Conference on International Security 2014; Gerasimov (2019): Vektory razvitija voennoj strategii, In: redstar.ru (04.03.2019).

"Farbrevolutionen", die zu einem Regimewechsel führten			"Farbrevolutionen", die zu keinem Regimewechsel führten		
Ägypten, 2011	Libanon, 2005	Sudan, 2011	Armenien, 2008	Kuwait, 2011	Saudi-Arabien, 2011
Georgien, 2003	Libanon, 2011	Tunesien, 2010	Bahrain, 2011	Mauretanien, 2011	Syrien, 2011
Jemen, 2011	Libyen, 2011	Ukraine, 2004	Belarus, 2005	Marokko, 2010	Usbekistan, 2005
Jordanien, 2010	Moldau, 2009	Ukraine, 2013/14	Djibouti, 2011	Oman, 2011	Venezuela, seit 2014
Kirgisistan, 2005	Somalia, 2011		Irak, 2011	Russland 2011/12	

Abbildung 6 Farbrevolutionen seit 2000 aus russischer Perspektive. Grüne Punkte markieren Farbrevolutionen ohne Regimewechsel; orange Punkte mit Regimewechsel.
(Bilban/Grininger)

Russische Forscher und Politiker verstehen unter Farbrevolutionen grundsätzlich Regierungsumstürze durch Massenproteste, wie sie z. B. 2000 in Serbien, 2003 in Georgien und 2004/5 in der Ukraine stattfanden. Auch der Arabische Frühling ab 2011 und der «Euromaidan» 2014 werden zu den Farbrevolutionen gezählt. Verallgemeinert werden diese Ereignisse im Westen meist positiv und als Zeichen für Demokratisierung wahrgenommen, während sie in Russland als Bedrohung definiert werden.[23] Farbrevolutionen gelten als Technologien des Westens, vor allem der USA, mit deren Hilfe in die inneren Angelegenheiten eines souveränen Staates eingegriffen wird.[24] Besondere Gefahr liegt in der potenziellen Vorbildwirkung von Massenprotesten in benachbarten Ländern. Dies ist vor allem im Kontext der grossen Proteste vor den Parlaments- und Präsidentschaftswahlen 2011/12 in Russland zu sehen. Aus Sicht einiger russischer Forscher werden Farbrevolutionen seit 2013/14 immer mehr als Teil der (hybriden) Kriegsführung des Westens gegen Russland interpretiert und bezeichnet.[25] Bereits seit Mitte der 2000er-Jahre forderten auch führende Militärtheoretiker, dass Russland «militärische Antworten auf nicht-militärische Bedrohungen» durch Farbrevolutionen finden müsse.[26] Folglich reichen die gedanklichen Grundlagen der «Gerasimov-Doktrin» tiefer, als es die Geschehnisse in der Ukraine 2014 aussehen liessen.[27]

Aus Sicht einiger russischer Forscher werden Farbrevolutionen seit 2013/14 immer mehr als Teil der (hybriden) Kriegsführung des Westens gegen Russland interpretiert und bezeichnet.

23 Vgl. Präsident der Russländischen Föderation (2015): Ukaz Prezidenta Rossijskoj Federacii ot 31 dekabrja 2015 goda N 683 «O Strategii nacional'noj bezopasnosti Rossijskoj Federacii».

24 Vgl. Bilban/Grininger/Steppan: Gerasimov – Ikone einer tief verwurzelten Denktradition, S. 25ff.; Zur westlichen Sicht auf Farbrevolutionen siehe Stykow, Petra: «Bunte Revolutionen» – Durchbruch zur Demokratie oder Modus der autoritären Systemreproduktion? In: Politische Vierteljahresschrift, 1/2010, S. 137–162; Cordesman, Anthony H.: Russia and the «Color Revolution» (28.05.2014). <https://www.csis.org/analysis/russia-and-%E2%80%9Ccolor-revolution%E2%80%9D>, abgerufen am 09.08.2018.

25 Vgl. Bouchet, Nicolas: Russia's «militarization» of colour revolutions. Policy Perspectives Vol. 4/2, Center for Security Studies ETH Zurich. Zürich 2016, hier: S. 2.; Manojlo, Andrej V.: Gibridnye vojny i cvetnye revoljucii v mirovoj politike. In: Pravo i Politika, 7/2015, S. 918–929 besonders Kapitel 5.

26 Vgl. Gol'c, Aleksandr: «Doktrina Gerasimov» — novyj variant. In: Eždnevnyj Žurnal, 04.03.2019, <http://ej.ru/?a=note&id=33501>, abgerufen am 10.04.2019; Galeotti, Mark: Russian Political War: Moving Beyond the Hybrid. Routledge Focus, London/New York, NY 2019, hier: S. 29ff.

27 Vgl. Monaghan: Ukraine Crisis.

Gerasimovs Bedeutung für die Militärdoktrin 2014

Ein weiterer wichtiger Aspekt des zeitlichen Kontexts ist die Bestellung Gerasimovs als Generalstabschef nur wenige Monate bevor er die berühmte Rede hielt. Es kann davon ausgegangen werden, dass er in dieser kurzen Zeit keine «Doktrin» entwickelte, ohne dabei auf bereits bestehende Ideen und Konzepte zurückzugreifen.[28] Das vorgestellte Bedrohungsbild und die Entwicklungsfelder der russischen Streitkräfte wurden, so Galeotti, wahrscheinlich von mehreren Personen entwickelt.[29]

So ist beispielsweise 2014 als Merkmal moderner militärischer Konflikte von der «komplexe[n] Anwendung von militärischer Gewalt, von Massnahmen politischen, ökonomischen, informationellen und anderen nicht-militärischen Charakters, die unter breiter Nutzung des Protestpotenzials und der Kräfte für Spezialoperationen realisiert werden» die Rede.

Der Vergleich zwischen Gerasimovs Rede und der russischen Militärdoktrin 2010 zeigt bereits, dass der Generalstabschef dem Diskurs der letzten Jahre folgt. Gerasimovs Charakteristika militärischer Auseinandersetzungen im 21. Jahrhundert und die Auflistung derselben in der Militärdoktrin von 2010 gleichen sich teils stark. Gerasimovs Rede brachte aber auch neue Elemente auf, die schliesslich Eingang in die präzisierte Militärdoktrin von 2014 fanden.[30] So ist beispielsweise 2014 als Merkmal moderner militärischer Konflikte von der «komplexe[n] Anwendung von militärischer Gewalt, von Massnahmen politischen, ökonomischen, informationellen und anderen nicht-militärischen Charakters, die unter breiter Nutzung des Protestpotenzials und der Kräfte für Spezialoperationen realisiert werden»[31] die Rede. Bereits 2010 wurde die «komplexe Anwendung militärischer und nicht-militärischer Kräfte und Mittel»[32] genannt, aber nicht näher bestimmt. In der Militärdoktrin 2010 wird auch die «Verstärkung der Rolle des Informationskampfes»[33] angemerkt. Die Erwähnung des Protestpotenzials der Bevölkerung fehlt 2010 im Gegensatz zu 2014 – hier macht sich möglicherweise das geänderte Bedrohungsempfinden durch die Anti-Putin-Proteste 2011/12 und den Arabischen Frühling bemerkbar.[34] Zudem gab es 2014 weitere Neuerungen, wie beispielsweise die «Teilnahme irregulär bewaffneter Formationen und privater Sicherheitsunternehmen»[35] in modernen Konflikten.[36]

Gerasimovs Aussagen von 2013 geben folglich die Entwicklung des russischen sicherheitspolitischen Diskurses wieder, sind jedoch nicht Beginn von etwas fundamental Neuem. Seine Ausführung stellten keine Grundlage für eine komplett neue Form der Kriegsführung, wohl aber einen wichtigen Denkanstoss für die Weiterentwicklung der russischen Militärdoktrin aus dem Jahr 2010 dar. Gerasimov machte in seiner Rede implizit darauf aufmerksam, dass eine Adaptierung der Militärdoktrin notwendig sei, und von anderen Ländern zu diesem Zeitpunkt schon vorgenommen worden war.[37]

Gerasimovs Aussagen von 2013 geben folglich die Entwicklung des russischen sicherheitspolitischen Diskurses wieder, sind jedoch nicht Beginn von etwas fundamental Neuem.

Wiederaufbau der russischen Militärwissenschaften

Gerasimovs Rede von 2013 kann im Nachhinein als Wendepunkt einer seit 2008 laufenden russischen Debatte darüber, ob die Militärwissenschaften noch über einen zeitgemässen Wissens- und Theorievorrat für die Kriegsführung der Zukunft verfügen[38], gesehen werden. Die militärtheoretischen Debatten verliefen parallel zur Streitkräftereform unter Minister Anatolij Serdjukov. Nach den vergleichsweise schlechten Leistungen der Streitkräfte gegen die zahlenmässig weit unterlegene georgische Armee im «Fünf-Tage-Krieg» 2008 wurden diese radikal umstrukturiert, was vor allem im Offizierskorps – darunter auch viele Angehörige der AMW – negativ aufgenommen wurde.[39] Schon vor Gerasimovs Rede, kritisierten die beiden Militärtheoretiker Ivan Vorob'ëv und Valerij Kiselëv in einem Artikel aus dem Jahr 2011 die «schlechte theoretische Begründung»[40] der Militärreform. Dem wirkte der Generalstab durch die Schaffung mehrerer Schnittstellen zwischen Forschung und Verteidigungsministerium entgegen.

28 Vgl. Pester, Kristian: Russlands Militärreform: Herausforderung Personal. SWP-Studie, 21/2013, Berlin, hier: S. 19.; McDermott: Does Russia Have a Gerasimov Doctrine, S. 100.
29 Vgl. Galeotti, Mark: The mythical «Gerasimov Doctrine» and the language of threat. In: Critical Studies on Security, 1/2018, S. 1–5, hier: S. 2.
30 Vgl. Bilban/Grininger/Steppan: Gerasimov – Ikone einer tief verwurzelten Denktradition, S. 37f.
31 DSS, Dresdner Studiengemeinschaft Sicherheitspolitik e.V. (Hrsg.): Militärdoktrin der Russischen Föderation. Präzisierte Redaktion 12/2014. DSS-Arbeitspapiere, 113/2015, Dresden, hier: S. 16f.
32 DSS, Dresdner Studiengemeinschaft Sicherheitspolitik e.V. (Hrsg.): Militärdoktrin der Russischen Föderation. Bestätigt durch Erlass Nr. 146 der Präsidenten der Russischen Föderation vom 5. Februar 2010. DSS-Arbeitspapiere, 99/2010, Dresden, hier: S. 12.
33 Ebd., S. 13.
34 Vgl. Bilban/Grininger/Steppan: Gerasimov – Ikone einer tief verwurzelten Denktradition, S. 39.
35 DSS (Hrsg.): Militärdoktrin 2014, S. 17.
36 Damit wurde scheinbar auch die Anfang 2014 von den Theoretikern Ivan Vorob'ëv und Valerij Kiselëv geäusserte Forderung nach einer Ausweitung der Liste möglicher Bedrohungen in der Militärdoktrin umgesetzt. Vgl. Vorobyov, I. N./Kiselyov, V. A.: Strategies of Destruction and Attrition: A New Version. In: Military Thought, 1/2014, S. 127–141, hier: S. 139.
37 Vgl. Bilban/Grininger/Steppan: Gerasimov – Ikone einer tief verwurzelten Denktradition, S. 48f.
38 Vgl. Eklund, Niklas: Vision Impossible? Some Aspects of the Current Russian Debates about the Military Sciences. In: Journal on Baltic Security, 1/2015, S. 71–84, hier: S. 71.; Persson, Gudrun: Security Policy and Military Strategic Thinking. In: Hedenskog, Jakob/Vendil Pallin, Carolina (Hrsg.): Russian Military Capability in a Ten-Year Perspective – 2013. Stockholm 2013, S. 71–88, hier: S. 80.
39 Vgl. Truffer, Patrick: Ein weiter Weg: Die russische Militärreform – Teil 1. In: Offiziere.ch, 18.01.2019, <https://www.offiziere.ch/?p=35170>, abgerufen am 09.04.2019; Golts, Alexander: Die Militärreform in Russland und ihre Folgen. In: Russland-Analysen, 306/2015, S. 5–9, hier: S. 6ff.; Pester: Russlands Militärreform, S. 5ff.
40 Vorobyov/Kiselyov: The Role of Military Science, S. 72.

Abbildung 7 Ein wesentlicher Teil des Personals der wissenschaftlichen Kompanien wird durch Wehrdienstleistende («herausragende» Absolventen ziviler Universitäten) gestellt. Hier präsentiert sich die wissenschaftliche Kompanie der Militärakademie der Fernmeldetruppen auf einer Messe.
(mil.ru; http://vas.mil.ru/upload/site39/document_images/6-1200.JPG)

Bereits 2009 wurde beim Generalstab das militärwissenschaftliche Komitee eingerichtet, um die Forschungsaktivitäten des Ministeriums und die Zusammenarbeit mit externen Stellen zu koordinieren.[41] 2011 und 2012 wurden noch zwei Institutionen geschaffen, um sowohl militärtheoretische wie technologische Innovationen voranzutreiben.[42] Unter Gerasimov wurden schliesslich die Kompetenzen des Generalstabs im Bereich der Militärwissenschaften erweitert. Durch die «Verordnung über den Generalstab der Streitkräfte der Russischen Föderation»[43] beauftragte Putin im Juli 2013 den Generalstab mit der «Leitung des militärwissenschaftlichen Komplexes und der Organisation der wissenschaftlichen Arbeit in den Streitkräften».[44] Zum militärwissenschaftlichen Komplex gehören die militärischen Hochschulen (z. B. Akademie des Generalstabs), die Forschungszentren der Streitkräfte und auch sieben wissenschaftliche Kompanien. Diese Einheiten wurden seit 2013 bei den verschiedenen Hochschulen der (Teil-)Streitkräfte aufgestellt und betreiben angewandte Forschung für die jeweiligen Bedarfsträger.[45] In Zukunft, so äusserte Gerasimov seine Vorstellung 2014, soll der militärwissenschaftliche Komplex in einem Verbund mit der AMW, der Russischen Akademie der Militärwissenschaften und anderen zivilen Forschungseinrichtungen zusammenwirken und somit die Verteidigungsfähigkeit und Sicherheit Russlands gewährleisten.[46]

Der westliche Diskurs der letzten Jahre konzentrierte sich auf das scheinbar Offensichtliche: Russlands «Doktrin» einer hybriden und/oder Informationskriegsführung.

Viele westliche Experten sahen in der «Gerasimov-Doktrin» von 2013 nicht den Beginn eines «Wiederaufbaus» der am Boden liegenden russischen Militärwissenschaften.[47] Dabei stellen gerade die Militärwissenschaften das Bindeglied zwischen den technischen und moralisch-politischen Fähigkeiten eines Staates dar. Die konzeptuellen Fähigkeiten der Militärwissenschaften sollten auch Einfluss in die Bewertung der militärischen Möglichkeiten eines Staates finden, argumentiert Niklas Eklund.[48] Im Fall Russlands nimmt die Militärwissenschaft diesbezüglich eine bedeutende Stellung ein.[49] Vor dem Hintergrund der Annexion der Krim und der Intervention in der Ukraine,

41 Vgl. Eklund: Vission Imposiible?, S. 73.
42 Vgl. Persson: Security Policy, S. 80.; My budem dumat' o buduščem. Interview mit Kokoškin, Andrej. In: Nezavisimoe Voennoe Obozrenie, 20.05.2011, <http://nvo.ng.ru/realty/2011-05-20/1_kokoshin.html>, abgerufen am 08.04.2019.
43 Ukaz Prezidenta Rossijskoj Federacii ot 23 ijulija 2013 goda N 631 «Voprozsy General'nogo štaba Booružennych Sil Rossijskoj Federacii» [Erlass des Präsidenten der Russischen Föderation vom 23. Juli 2013 Nr. 631 «Belange des Generalstabs der Russländischen Föderation»].
44 Vgl. Gerasimov, Valerij V.: Rol' general'nogo štaba v organizacii oborony strany v sootvetstvii s novym položeniem o general'nom štabe, utveržděnnym prezidentom Rossijskoj Federacii. In: Vestnik Akademii Voennych Nauk, 1/2014, S. 14–22, hier: S. 18.
45 Sie z. B. die Aufgaben der 5. Wissenschaftlichen Kompanie, welche an der MVOKU in Moskau disloziert ist und u. a. dem Nationalen Verteidigungsmanagement Zentrum zuarbeitet: Programmieren, Visualisierung und Darstellung von Informationen, Automatisierung der Datensammlung und -analyse, Ausarbeitung eines Systems zur Unterstützung der Entscheidungsfindung, Schaffung einer Datenbasis und 3D-Modellierung. – Vgl. <https://recrut.mil.ru/for_recruits/research_company/companies/sv.htm>, abgerufen am 09.04.2019.
46 Vgl. Gerasimov: Rol' general'nogo štaba, S. 19–21.; Bilban: Mythos «Gerasimov-Doktrin», S. 63.
47 Vgl. als eine rezente Ausnahme: McDermott, Roger: Gerasimov Appeals for Military Science to Forge New Forms of Combat. In: Eurasia Daily Monitor, 12.03.2019, <https://jamestown.org/program/gerasimov-appeals-for-military-science-to-forge-new-forms-of-combat/>, abgerufen am 09.04.2019.
48 Vgl. Eklund: Vission Imposiible?, S. 71.
49 Vgl. Persson: Security Policy, S. 80.

Abbildung 8 Informationskriegsführung besteht nach russischem Verständnis aus einer psychologischen und technischen Komponente. Die russischen Streitkräfte verfügen über umfangreiche Kräfte zur elektronischen Kriegsführung, für Cyberoperationen und psychologische Kriegsführung. Auf dem Bild das Störsender-System Borisoglebsk-2.
(mil.ru, https://upload.wikimedia.org/wikipedia/commons/4/4c/ElectronicWarfareExercise2018-01.jpg)

Abbildung 9 General Valerij Gerasimov hält seinen jährlichen Vortrag bei der Generalversammlung der Russischen Akademie der Militärwissenschaften 2018.
(mil.ru, http://vagsh.mil.ru/upload/site17/document_images/6HlxpThWpk.jpg)

blieb dieser wesentliche Aspekt aber verborgen. Der westliche Diskurs der letzten Jahre konzentrierte sich auf das scheinbar Offensichtliche: Russlands «Doktrin» einer hybriden und/oder Informationskriegsführung.[50]

Militärtheoretische Ursprünge der «Gerasimov-Doktrin»

Da die «Gerasimov-Doktrin», wie bereits gezeigt wurde, nicht im luftleeren Raum des russischen sicherheitspolitischen Denkens entstand, ist es aufschlussreich, sie auch in einen militärwissenschaftlichen Kontext zu setzen. An den Reden ehemaliger Generalstabschefs vor 2013 wird ersichtlich, dass viele Themen der «Gerasimov-Doktrin» bereits vor 2013 angesprochen wurden. Besonders relevant sind die Reden General Nikolaj Makarovs, des direkten Vorgängers Gerasimovs. Dies gilt beispielsweise für den vielzitierten Einsatz politischer, ökonomischer, informationeller, humanitärer und anderer nicht-militärischer Mittel, die schon 2009 in der Zeitschrift *Voennaja Mysl'* diskutiert wurden.[51] Makarov sprach dieses Thema in seiner Rede 2010 ebenfalls an.[52] Auch die Idee der Entgrenzung des Krieges ist im russischen Diskurs nicht neu.[53] Besonders Informationsoperationen würden zu dieser Entgrenzung beitragen, so Gerasimov in seiner Rede von 2013.[54]

Der Stellenwert von Information wurde bereits vor Gerasimovs thematisiert, u. a. in Zusammenhang mit dem Konzept der «Kriege neuer Generation» *(vojny novogo pokolenija)*. Dabei handelt es sich um eine russische Adaption der US-Erfahrungen mit netzwerkzentrierter Kriegsführung. Das Konzept wurde bereits seit Mitte der 2000er u. a. von den Militärtheoretikern Sergej Čekinov und Sergej Bodganov weiterentwickelt.[55] Kern des Konzeptes ist die Überwältigung des Gegners durch Informationskriegsführung noch vor Beginn offener Kampfhandlungen.[56] Die Überlegungen Čekinovs und Bogdanovs bauen auf ihren Vorarbeiten zu Asymmetrie und Informationskriegsführung auf. Schon 2010 betonen sie, dass durch Informationsoperationen (militär)strategische Ziele erreicht werden können.[57] Im Jahr 2011 fordern sie: «Given the current reality, it appears expedient for Russia to map out and eventually also implement a *strategy of indirect approach* as its state strategy without an alternative.»[58] Zentrales Element ist die Anwendung der schon beschriebenen nicht-militärischen Mittel und insbesondere informationeller Massnahmen.[59] Auch General Makarov spricht bereits 2010 und 2012 von asymmetrischen Handlungen und Einflussnahme im informationell-kommunikativen Bereich, um das Kampfpotenzial des Feindes zu verringern.[60]

Weitere Kernelemente der «Gerasimov-Doktrin» wie die wachsende Rolle subversiver Handlungen, der Einsatz von Spezialeinsatzkräften in der Tiefe des feindlichen Territoriums, und der Einsatz gemischter und hochmobiler Kampfgruppen, neuer Technologien und hochpräzisier Waffensysteme, finden sich auch in den Reden der Generalstabschefs vor 2013 und bei Theoretikern wie Vorob'ëv und Kiselëv.[61]

50 Vgl. dazu Fridman, Ofer: Russian «Hybrid Warfare»: Resurgence and Politicisation. London 2018, vor allem S. 107–125.
51 Vgl. z. B. Lutovinov, V. I.: Development and Use of Nonmilitary Measures to Reinforce the Military Security of the Russian Federation. In: Military Thought, 2/2009, S. 26–30, hier: S. 28.
52 Makarov, Nikolaj E.: Charakter vooružennoj bor'by buduščego, aktual'nye problemy stroitel'stva i boevogo primenenija vooružennych sil RF v sovremennych uslovijach. In: Vestnik Akademii Voennych Nauk, 2/2010, S. 18–26, hier: S. 19.
53 Vgl. Bilban, Christoph/Grininger, Hanna: Was bleibt von der «Gerasimov-Doktrin»? In: Bilban, Christoph/Grininger, Hanna (Hrsg.): Mythos Gerasimov-Doktrin. a.a.O., S. 263–302, hier: S. 269.
54 Vgl. dazu insbesondere die Durchführung von Informationsoperationen an der Grenze von militärischen und nicht-militärischen Mittel über den gesamten Konfliktverlauf in Abbildung 1.
55 Vgl. Bilban/Grininger: Was bleibt von der «Gerasimov-Doktrin»?, S. 266ff.
56 Vgl. Chekinov, S. G./Bogdanov, S. A.: The Nature and Content of a New-Generation War. In: Military Thought, 4/2013, S. 12–23, hier: S. 19.
57 Vgl. Chekinov, S. G./Bogdanov, S. A.: Asymmetrical Actions to Maintain Russia's Military Security. In: Military Thought, 1/2010, S. 1–11, hier: S. 6f.
58 Chekinov, S. G./Bogdanov, S. A.: Strategy of Indirect Approach: Its Impact on Modern Warfare. In: Military Thought, 3/2011, S. 1–13, hier: S. 12.
59 Vgl. ebd., S. 3ff.
60 Vgl. Makarov: Charakter vooružennoj bor'by, S. 26. und auch seinen Beitrag in Vestnik Akademii Voennych Nauk, 2/2012, S. 20–26.
61 Vgl. Bilban/Grininger: Was bleibt von der «Gerasimov-Doktrin»?, S. 290f.; Vorobyov/Kiselyov: The Role of Military Science, S. 75f.

In der «Gerasimov-Doktrin» finden sich jedoch auch einige Elemente, die von den bisherigen Generalstabschefs vor der Akademie der Militärwissenschaften noch nicht angesprochen wurden. Darunter fällt insbesondere der Begriff der Farbrevolutionen und die Nutzung des Protestpotenzials der Bevölkerung zur Destabilisierung von Staaten, sowie die Bedeutung von friedensstiftenden Operationen u. a. als Deckmantel für ausländische Militärinterventionen und der Schutz russischer Interessen ausserhalb der Russischen Föderation. Gerasimov spricht ausserdem von einem gesamtstaatlichen Ansatz in der Landesverteidigung und nimmt Bezug auf sowjetische Militärtheoretiker, besonders auf Svečin, der meint, dass es für Kriege keine Schablone gebe und jeder individuell sei. Auch das Verwischen der Grenzen zwischen Krieg und Frieden spricht Gerasimov als erster Generalstabschef in dieser Deutlichkeit an.[62]

Im Vergleich zu den vorhergehenden Jahren ist Gerasimovs Rede von 2013 eher allgemein gehalten. Während zuvor konkrete Themen wie Militärreform, Umstrukturierung oder die Ausrüstung der Streitkräfte im Detail besprochen wurden, geht es bei Gerasimov 2013 stärker um die allgemeinen Charakteristika moderner Kriege. Vielleicht lässt sich die Beliebtheit dieser Rede auch dadurch erklären.[63]

Auch 2017 stellt Gerasimov fest, dass das Konfliktpotenzial der Welt gestiegen sei, weswegen die Kapazitäten zur strategischen Abschreckung durch die nukleare Triade in den kommenden Jahren modernisiert und ausgebaut werden sollen.

Die Reden, die Gerasimov nach 2013 jährlich vor der Generalversammlung der Akademie der Militärwissenschaften hielt, wurden von der wissenschaftlichen Öffentlichkeit weit weniger rezipiert. 2014 ging Gerasimov beispielsweise auf die Rolle von NGOs und privaten Militärfirmen in Konflikten ein, und sprach viel über einen gesamtstaatlichen Ansatz und die Rolle des Generalstabs im Bereich der Landesverteidigung. In der Rede von 2015 behandelte er das 70-jährige Jubiläum des Sieges im Grossen Vaterländischen Krieg und die Einheit von politischer und militärischer Führung, die diesen Sieg ermöglicht hatte. Gerasimov stellt hier auch eine Querverbindung zum Nationalen Führungszentrum her. Zentrales Thema der Rede von 2016 sind die militärischen Lehren aus dem Krieg in Syrien. Gerasimov bezeichnet diesen explizit als «hybrid» und übernimmt somit die westliche Terminologie. Hybride Kriege würden jedoch nur vom Westen geführt, so Gerasimov. Farbrevolutionen, neue Waffensysteme, Präzisionswaffen, Informationskrieg und Nutzung des Protestpotenzials der Bevölkerung sind nach 2013 wiederum wichtige Elemente seiner geopolitischen Lagebeurteilung in der Rede von 2016. Er legt zudem einen «neuen» Fokus auf nukleare Abschreckung. Auch 2017 stellt Gerasimov fest, dass das Konfliktpotenzial der Welt gestiegen sei, weswegen die Kapazitäten zur strategischen Abschreckung durch die nukleare Triade in den kommenden Jahren modernisiert und ausgebaut werden sollen. Er plädiert ausserdem für eine Stärkung der Verbindung zwischen Armee und Gesellschaft und merkt an, dass der Sieg auch von der Moral der Bevölkerung abhänge. Auch 2018 folgt Gerasimov seinen Einschätzungen der geopolitischen Lage der letzten Jahre. In der Rede geht es jedoch vor allem um innere Entwicklungen, die Umstrukturierung der russischen Armee und die Zusammenarbeit zwischen Generalstab und Akademie der Militärwissenschaften.[64]

Zwischen der «Gerasimov-Doktrin» und den vorhergehenden und nachfolgenden Reden der Generalstabschefs bzw. Gerasimovs ergeben sich also einige thematische Überschneidungen. Es wird klar, dass hier eine «Evolution» des russischen militärischen Denkens stattfindet. Betrachtet man die Anknüpfungspunkte zu den Arbeiten von Theoretikern wie Čekinov/Bogdanov und Kiselëv/Vorob'ëv, fallen viele Gemeinsamkeiten auf. Diese zwei Autorenpaare haben scheinbar Gerasimov schon bei seiner Rede 2013 beeinflusst.[65]

Gerasimov 2019: Moderne Strategie braucht Theorie und Praxis

Die aktuellste Rede Gerasimovs vom 2. März 2019 könnte eine neue Etappe des russischen militärischen Denkens auf Grundlage der Erfahrungen in Syrien andeuten. McDermott argumentiert, dass diese Rede wiederum Einfluss auf die von Putin Ende 2018 angeordnete Ausarbeitung einer neuen Militärdoktrin haben wird.[66] Der Vortrag bei der Versammlung der AMW beginnt in fast schon traditioneller Weise mit der Feststellung, dass die USA ihre Konzepte *Global Strike* und *Multi-Domain Battle,* sowie die Technologien der Farbrevolutionen und *soft power* nutzen, um unliebsame Länder zu «liquidieren». Mit der «Strategie der aktiven Verteidigung» habe Russland mittlerweile durch die Arbeit der Militärwissenschaftler und des Generalstabs eine Antwort auf diese Bedrohung gefunden. Der passende Komplex von Massnahmen finde sich bereits in der Militärdoktrin 2014, so der Generalstabschef.[67]

Ein wesentlicher Teil des Vortrags behandelt auch die Relevanz der nuklearen Abschreckung, besonders vor dem Hintergrund des Endes des INF- und New START-Vertrag. Russland werde sich aber nicht in ein neues Wettrüsten drängen lassen, merkt Gerasimov an. Durch die russischen Erfahrungen aus Syrien sei es zudem gelungen, eine «Strategie der begrenzten Aktionen» ausserhalb der Landesgrenzen zu perfektionieren. Die Streitkräfte hätten nun Verfahren für die Durchführung von «humanitären Ope-

62 Vgl. Bilban/Grininger: Was bleibt von der «Gerasimov-Doktrin»?, S. 291f.
63 Vgl. ebd., S. 273.
64 Vgl. ebd., S. 273ff.
65 Vgl. dazu auch Galeotti: Russian Political War, S. 29ff.; Fridman: Russian «Hybrid Warfare», S. 127ff.
66 Vgl. McDermott, Roger: Gerasimov Unveils Russia's «Strategy of Limited Actions». In: Eurasia Daily Monitor, 06.03.2019, <https://jamestown.org/program/gerasimov-unveils-russias-strategy-of-limited-actions/>, abgerufen am 08.04.2019.
67 Vgl. Gerasimov, Valerij V.: Vektory razvitija voennoj strategii. In: Krasnaja Zvezda, 04.03.2019, <http://redstar.ru/vektory-razvitiya-voennoj-strategii/>, abgerufen am 10.04.2019.

Abbildung 10 Die Luft- und Weltraumstreitkräfte Russlands trugen die Hauptlast des Einsatzes in Syrien. (mil.ru, http://syria.mil.ru/images/upload/2015/SAVX7322-1.jpg)

rationen» erarbeitet. Damit erfüllt Gerasimov eine Forderung aus dem Jahr 2013. Jedoch verweist er kurz darauf auf die Notwendigkeit, die C4ISTAR-Fähigkeiten technologisch wie konzeptionell weiter auszubauen. Ebenso hätten die Streitkräfte Nachholbedarf im Bereich des Schutzes kritischer Infrastruktur als Massnahme der Landesverteidigung. Zuletzt bekommt auch die strategische Bedeutung der Informationssphäre wieder Raum.[68]

Im Unterschied zur Rede von 2013 fällt auf, dass den tatsächlichen militärischen Möglichkeiten Russlands viel Platz eingeräumt wird. So hebt Gerasimov hervor, dass die Personaloffensiven Wirkung zeigen und bis 2025 rund 475.000 Zeitsoldaten verpflichtet werden sollen. Damit werde die Zahl der eingezogenen Wehrpflichtigen noch weiter sinken. Schon heute besitze die russische Armee einen hohen Professionalisierungsgrad. Gerasimov betont: «Alle Kommandeure der Militärbezirke, der Armee und Korps der Land-, Luft-, Weltraum- und Luftverteidigungsstreitkräfte, sowie auch 96 Prozent der Kommandanten von Divisionen, Brigaden, Regimentern und selbständigen Bataillonen verfügen über Kampferfahrung.»[69] Auch in *The Military Balance 2019* wird diesbezüglich festgehalten: «Since the mission [in Syria, Anm.] began in late 2015, more than 500 Russian generals have rotated through the country on deployment.»[70]

Gerasimov betont: «Alle Kommandeure der Militärbezirke, der Armee und Korps der Land-, Luft-, Weltraum- und Luftverteidigungsstreitkräfte, sowie auch 96 Prozent der Kommandanten von Divisionen, Brigaden, Regimentern und selbständigen Bataillonen verfügen über Kampferfahrung.»

Gerasimov unterstreicht zudem erneut die Relevanz der Militärwissenschaften, denn ohne Theorie sterbe die Strategie. Ebenso brauche es die Wirtschaft, um das richtige Material bereitzustellen. Er betont eine notwendige «Abstimmung» von Verteidigungsministerium und dem militär-industriellen Komplex, was er mit einem Svečin-Zitat besonders unterstreicht: «Die Wirtschaft versteht es, sich dem Charakter der Kriegshandlungen zu unterwerfen.»[71] Gerasimov schliesst seine Rede 2019 mit einem Lob für die Arbeit der Militärwissenschaften. Im Zentrum steht nun aber der vom Generalstab geführte militärwissenschaftliche Komplex der Streitkräfte, und die AMW scheint über den gesamten Vortrag hinweg eher eine untergeordnete Rolle zu spielen.

68 Vgl. ebd.
69 Ebd.
70 IISS (Hrsg.): Chapter Five: Russia and Eurasia. In: The Military Balance 2019. London 2019, S. 166–221, hier: S. 168.
71 Gerasimov: Vektory razvitija voennoj strategii.

Abbildung 11 Der T-72B3 (hier bei der Übung Zapad-2017) und der BMP-2M werden auf absehbare Zeit das Rückgrat der russischen Panzerstreitkräfte bilden. Von den modernen Fahrzeugen der Armata-Plattform (T-14, T-15) werden nur etwa 130 Stück in den nächsten Jahren beschafft. Diese sind zu teuer (vgl. dazu The Military Balance 2019, S. 177).
(mil.ru, http://mil.ru/images/upload/2017/Tanki-1200.jpeg)

Überlieferungsgeschichte: Wie aus der Rede eine «Doktrin» wurde …

Die Rede von 2019 zeigt, dass sich das russische militärische Denken wieder in Richtung «strategischer Abschreckung» und «begrenzter, konventioneller Interventionen» weiterentwickelte, während im Westen immer noch von der «Gerasimov-Doktrin» gesprochen wird.[72] Es stellt sich also die Frage, wie die Rede Gerasimovs von 2013 eine solche Bekanntheit erreichen konnte. Die Überlieferungsgeschichte gibt Aufschluss darüber, in welchen thematischen und geografischen Kontexten dies geschah.[73]

Nur zwei wenig beachtete Publikationen aus den USA und Schweden verwiesen schon 2013 auf Gerasimovs Rede.[74] Gemäss unseren Recherchen war Jānis Bērziņš von der lettischen Verteidigungsakademie der erste Autor, welcher Gerasimovs Rede in einen Zusammenhang mit der Annexion der Krim und einer «neuen Art der russischen Kriegsführung» setzte.[75] Er stellte auch Teile der Rede einem breiten westlichen Publikum in englischer Sprache vor.

Die Rezeption der Rede Gerasimovs wurde aber besonders durch Übersetzungen ins Englische angeregt. Am 21. Juni 2014 veröffentlichte Robert Coalson, damals Journalist bei Radio Free Europe/Radio Liberty, auf seinem Facebook-Profil eine Übersetzung der Rede. In seinen einleitenden Anmerkungen verknüpfte er die Ausführungen Gerasimovs mit den «russischen Strategien und Taktiken in der Ukraine».[76] Coalsons Übersetzung wurde zur Grundlage eines häufig zitierten Beitrags von Mark Galeotti auf seinem privaten Blog *In Moscow's Shadows,* in dem er die übersetzte Rede mit eigenen Kommentaren versieht. Galeotti trug massgeblich zur Schaffung des Begriffs «Gerasimov-Doktrin» bei; einerseits durch den Titel des Beitrags, andererseits durch die einleitenden Worte:

«Nonetheless, it represents the best and most authoritative statement yet of what we could, at least as a placeholder, call the ‹Gerasimov Doctrine› (not that it necessarily was his confection).»[77]

Anfang 2017 fügte Galeotti seinem Blog-Beitrag nochmals ein Vorwort hinzu, in dem er bemerkt, dass er den Begriff «Gerasimov-Doktrin» nicht verbreiten wollte, da es sich nicht um eine Doktrin im eigentlichen Sinn handelt:

72 Vgl. z. B. Clark, Mason/Harris, Catherine/Cafarella, Jennifer: Russia in Review: The Gerasimov Doctrine Is Here To Stay. In: ISW Blog, 30.10.2018, ‹http://iswresearch.blogspot.com/2018/10/russia-in-review-gerasimov-doctrine-is.html?m=0›, abgerufen am 13.01.2019.

73 Siehe die detaillierte Beschreibung bei Bilban/Grininger/Steppan: Gerasimov – Ikone einer tief verwurzelten Denktradition, S. 15ff.

74 Vgl. McDermott, Roger: Gerasimov Links Russian Military Modernization to the Arab Spring. In: Eurasia Daily Monitor, 05.03.2013, ‹https://jamestown.org/program/gerasimov-links-russian-military-modernization-to-the-arab-spring/›, abgerufen am 13.07.2017; Persson: Security Policy, S. 82.

75 Vgl. Bērziņš, Jānis: Russia's New Generation Warfare in Ukraine: Implications For Latvian Defense Policy. Policy Paper 02, National Defence Academy of Latvia, Center for Security and Strategic Research. Riga 2014.

76 Vgl. Coalson, Robert: Russian Military Doctrine article by General Valery Gerasimov (21.06.2014). ‹https://www.facebook.com/notes/robert-coalson/russian-military-doctrine-article-by-general-valery-gerasimov/10152184862563597/›, abgerufen am 21.11.2016.

77 Galeotti, Mark: The «Gerasimov Doctrine» and Russian Non-Linear War. In: In Moscow's Shadows, 06.07.2014, ‹https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/›, abgerufen am 21.02.2017.

«When using the term ‹Gerasimov Doctrine›, I was just going for a snappy title. I really didn't expect (or want) it to become a more generally used term.»[78]

Die Veröffentlichung der übersetzten «Gerasimov-Doktrin» passte zeitlich genau zum ersten Höhepunkt der Kämpfe in der Ostukraine im Frühsommer 2014 und der Annexion der Krim. Diese Handlungen Russlands kamen für die meisten westlichen Beobachter überraschend und trafen die Expertengemeinschaft unvorbereitet.[79] Die Gründe dafür lassen sich u. a. auf fehlende sicherheitspolitische Russland-Expertise und Russland-Forschung zurückführen, da diese nach Ende des Kalten Krieges vernachlässigt wurde.[80] Viele Forscherinnen und Forscher hätten, so Andrew Monaghan, zudem gar nicht versucht, russischsprachige Quellen oder die Sichtweise Moskaus heranzuziehen, und stützten sich auf Behauptungen und Annahmen zur russischen Strategie.[81] In der «Gerasimov-Doktrin» fanden einige Analystinnen und Analysten also ein leicht zugängliches Erklärungsmuster für die Ereignisse in der Ukraine. McDermott merkte vor dem Hintergrund der damals spärlichen analytischen Kapazitäten treffend an: «It [the «Gerasimov doctrine»] may well mark a modern example of blue assessing red, and seeing a reflection of blue.»[82] Insgesamt kann wohl von einer selektiven Wahrnehmung in Bezug auf Gerasimovs Rede und ihre Inhalte gesprochen werden.

Die Veröffentlichung der übersetzten «Gerasimov-Doktrin» passte zeitlich genau zum ersten Höhepunkt der Kämpfe in der Ostukraine im Frühsommer 2014 und der Annexion der Krim.

… und warum es keine «Gerasimov-Doktrin» gibt

Ab 2016 wurden in der wissenschaftlich-sicherheitspolitischen Debatte immer mehr kritische Stimmen laut, die die Existenz einer «Gerasimov-Doktrin» in Frage stellten. Zu Beginn des Jahres 2018 prägte Galeotti den Diskurs zur «Gerasimov-Doktrin» durch zwei Artikel nochmals in besonderem Masse.[83] Darin argumentiert er gegen den Begriff der «Gerasimov-Doktrin» und übt Selbstkritik für seine Beteiligung an der Schaffung des Begriffs:

«[This article] is a polemic against the use of the term the ‹Gerasimov doctrine› to describe a supposed dramatic turn in Russian strategic thinking. It is a polemic against the way that pseudo-technical terms and jargon can be mobilized and appropriated not simply to obscure the truth but also to drive a hawkish political security agenda. It is also an apologia, because to a degree, it is all my fault.»[84]

Auch Michael Kofman hatte sich zuvor bereits kritisch gegenüber der «Gerasimov-Doktrin» geäussert und meinte Mitte 2018:

«The image of Putin sitting in the Kremlin pulling knobs and levers, or the mythical Gerasimov Doctrine (a linguistic invention that its author has forsworn), have become tragic caricatures on the current zeitgeist.»[85]

Im russischen Diskurs findet sich der Begriff einer «Gerasimov-Doktrin» kaum. Meist wird er nur verwendet, um seine Existenz zu bestreiten und das Unverständnis des Westens anzuprangern.[86] Nichtsdestotrotz bleibt die Idee einer «Gerasimov-Doktrin» nach diesen kritischen Bezugnahmen sowohl bei Praktikern aus Politik und Diplomatie, als auch in Medien und Wissenschaft weiter bestehen.[87]

Es lohnt sich ausserdem, sich mit dem Begriff der «Doktrin» genauer auseinanderzusetzen. Im Russischen, so Galeotti, bezeichnet das Wort «Doktrin» ein «grundlegendes strategisches Dokument».[88] Im Militärisch-Enzyklopädischen Wörterbuch des russischen Verteidigungsministeriums findet sich aber kein Eintrag unter «Doktrin».[89] In einem Wörterbuch des NATO-Russland-Rats aus dem Jahr 2011 wird Doktrin als «Prinzipien des Einsatzes der Streitkräfte»[90] übersetzt. Russische zivile enzyklopädische Wörterbücher verstehen unter einer Doktrin eine «systematische Lehre»[91] von etwas. Je nach Herkunft und Hintergrund wird somit Unterschiedliches unter einer Doktrin verstanden. Der Begriff «Doktrin» klinge im Englischen aber bedrohlich und fremd, was seine Anziehungskraft erklären könne, so Galeotti.[92]

Für die «hybride» Machtprojektion gegenüber dem Westen zeichnen sich vielmehr Präsidialadministration und Nationaler Sicherheitsrat verantwortlich.

Die Kriterien für eine Doktrin laut Definition der NATO erfüllt erst die Militärdoktrin von 2014, da sie die Grundätze für den Einsatz des Militärs darlegt und ein verbindliches Dokument ist; nicht aber Gerasimovs Rede von 2013.[93] Nun könnte man die «Gerasimov-Doktrin» noch auf eine

78 Ebd.
79 Vgl. Monaghan: Ukraine Crisis.
80 Vgl. Fridman: Russian «Hybrid Warfare», S. 166ff.
81 Vgl. Monaghan: Ukraine Crisis.
82 McDermott: Does Russia Have a Gerasimov Doctrine, S. 105.
83 Vgl. Galeotti: The mythical «Gerasimov Doctrine».; Galeotti, Mark: I'm Sorry for Creating the «Gerasimov Doctrine». In: Foreign Policy, 05.03.2018, ‹https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/›, abgerufen am 03.07.2018.
84 Galeotti: The mythical «Gerasimov Doctrine», S. 1.
85 Kofman, Michael: Raiding and International Brigandry: Russia's Strategy for Great Power Competition. In: War on the Rocks, 14.06.2018, ‹https://warontherocks.com/2018/06/raiding-and-international-brigandry-russias-strategy-for-great-power-competition/›, abgerufen am 03.07.2018.
86 Vgl. Bilban: Mythos «Gerasimov-Doktrin», S. 41f.; Galeotti: The mythical «Gerasimov Doctrine», S. 2. 2
87 Vgl. Bilban/Grininger: Was bleibt von der «Gerasimov-Doktrin»?, S. 283.; Bilban: Mythos «Gerasimov-Doktrin», S. 42, 73ff.
88 Vgl. Galeotti: The mythical «Gerasimov Doctrine», S. 1–3.
89 Verteidigungsministerium der Russischen Föderation: Voennyj énciklopedičeskij slovar'. ‹http://encyclopedia.mil.ru/encyclopedia/dictionary/list.htm›, abgerufen am 03.07.2018.
90 NATO-Russia Joint Editorial Working Group (Hrsg.) (2001): NATO-Russia Glossary of Contemporary Political and Military Terms. Brussels: NATO, Distribution Unit.
91 Academic.ru: Doktrina. ‹https://bit.ly/2tSUt3X›, abgerufen am 03.07.2018.
92 Vgl. Galeotti: The mythical «Gerasimov Doctrine», S. 3.
93 Vgl. Bilban/Grininger: Was bleibt von der «Gerasimov-Doktrin»?, S. 286.

Abbildung 12 «Führungstrio» der militärischen Macht der Russischen Föderation – Verteidigungsminister Šojgu, Präsident Putin und Generalstabschef Gerasimov.
(mil.ru, https://structure.mil.ru/images/upload/2018/SAVX2546-1.jpg)

Stufe mit allgemeinen, politischen Erklärungen stellen (wie z. B. der Truman-Doktrin als Beginn der US-«Containment»-Politik), dem widerspricht aber die Regelmässigkeit und thematische Kontinuität der Reden russischer Generalstabschefs. Keine dieser Reden stellte bisher eine grundlegende Neuausrichtung russischer Militärpolitik dar. Dies ist schon grundsätzlich äusserst unwahrscheinlich, da diese nur zu einem kleinen Teil vom Generalstab und dem Verteidigungsminister bestimmt wird.[94] Für die «hybride» Machtprojektion gegenüber dem Westen zeichnen sich vielmehr Präsidialadministration und Nationaler Sicherheitsrat verantwortlich.

Sprache, Wahrnehmungen, Aufmerksamkeit: Was wir daraus lernen können

Warum spielt es also eine Rolle, ob wir von einer «Gerasimov-Doktrin» sprechen oder nicht? Sprache beeinflusst unsere Wahrnehmung der Realität, und damit unser Verhalten. Wie Galeotti feststellt, «[…] it does matter, because words make worlds, and how we choose to label and discuss a threat defines it.»[95]

Viele Diskursbeiträge gehen nicht im Detail auf die Rede des russischen Generalstabschefs und deren Inhalte ein, und benutzen die «Gerasimov-Doktrin» gewissermassen als Schlagwort.

Am Beispiel der westlichen Debatten über die «Gerasimov-Doktrin» zeigt sich, dass sicherheitspolitische Forschung von Trends geleitet wird und auch in der Wissenschaft das Ziel verfolgt wird, Aufmerksamkeit zu generieren. Viele Diskursbeiträge gehen nicht im Detail auf die Rede des russischen Generalstabschefs und deren Inhalte ein, und benutzen die «Gerasimov-Doktrin» gewissermassen als Schlagwort.[96] Diese Erzeugung von Aufmerksamkeit ist eine von drei Funktionen, die Ina Kraft in ihrer Analyse der diskursiven Eigenschaften des Begriffs der «hybriden Kriegsführung» beschreibt.[97] Weitere sind laut ihr die Vereinfachung komplexer Sachverhalte und die Legitimierung eigener Positionen und Forderungen der Diskursteilnehmer. Diese Funktionen können auch für die «Gerasimov-Doktrin» identifiziert werden.

Durch den Begriff «Gerasimov-Doktrin» erfolgt in der wissenschaftlich-sicherheitspolitischen Literatur eine Kom-

94 Vgl. Konyshev, Valery/Sergunin, Alexander: Military. In: Tsygankov, Andrei P. (Hrsg.): Routledge Handbook of Russian Foreign Policy. London/New York 2018, hier: S. 174ff.
95 Galeotti: The mythical «Gerasimov Doctrine», S. 2.
96 Vgl. Bilban/Grininger: Die Regionalstudien im Vergleich, S. 332f.; Bilban: Mythos «Gerasimov-Doktrin», S. 103f.
97 Vgl. Kraft, Ina: Hybrider Krieg – zu Konjunktur, Dynamik und Funktion eines Konzepts. In: Zeitschrift für Aussen- und Sicherheitspolitik, 3/2018, S. 305–323, hier: S. 314ff.

plexitätsreduktion. Der Begriff wird als ein Synonym für Russlands aussenpolitisches Handeln (z. B. Einflussnahme auf Wahlen, Intervention in Syrien, Unterstützung der Separatisten im Donbass) verwendet. Dabei beschreiben weder die «Gerasimov-Doktrin» noch der ebenfalls häufig gebrauchte Begriff «hybride Kriegsführung» die russischen aussenpolitischen Intentionen vollumfänglich.[98]

Als Beispiel für die dritte Funktion nach Kraft – die Legitimierung der eigenen Positionen und Forderungen – sei hier die Rückkehr der NATO zur Bündnisverteidigung, die Stationierung der Enhanced Forward Presence im Baltikum und Polen und die Erhöhung der nationalen Verteidigungsausgaben vieler NATO-Staaten genannt.[99]

Was bleibt somit von den Debatten über die «Gerasimov-Doktrin»? Um das russische militärisch-strategische Denken zu verstehen, und um nicht wieder wie 2014 vom Tagesgeschehen überrascht zu werden, muss sicherheitspolitische Forschung auch Grundlagenforschung beinhalten.[100] Dabei reicht es jedoch nicht, sich auf Verteidigungsministerium und Generalstab zu fokussieren.

Auch wenn Gerasimov mit seiner Rede keine «Anleitung» für das russische aussenpolitische Handeln lieferte, lässt sich aus dem Umgang mit seiner «Doktrin» einiges lernen: über die russischen Streitkräfte sowie vor allem über unsere eigenen Einstellungen und Erwartungen.

In Zukunft noch von einer «Gerasimov-Doktrin» zu sprechen, könnte den Blick für die für Europa relevanten Entwicklungen im russischen Militär trüben, welche durchaus konventionelle Kriegsführung und eine «Eskalation zur De-Eskalation» betonen.[101] Es scheint, dass die russischen Streitkräfte nach einer «qualitativen Phase» mit Fokus auf Theorie- und Doktrinbildung, die (praktischen) Erkenntnisse der letzten Jahre nun in ihren Strukturen, der Ausbildung und einer neuen Militärdoktrin umsetzen werden. Auch wenn Gerasimov mit seiner Rede keine «Anleitung» für das russische aussenpolitische Handeln lieferte, lässt sich aus dem Umgang mit seiner «Doktrin» einiges lernen: über die russischen Streitkräfte sowie vor allem über unsere eigenen Einstellungen und Erwartungen.

Hanna Grininger

MA MA, Studium Interdisziplinäre Osteuropastudien, Slawistik und Romanistik in Wien und Moskau. 2017–2018 Gastforscherin am Institut für Friedenssicherung und Konfliktmanagement an der Landesverteidigungsakademie des Österreichischen Bundesheeres.

hanna.grininger@hotmail.com

Christoph Bilban

MA BA, Studium Politikwissenschaften und Slawistik in Wien und Moskau. Milizoffizier (Oblt) im Stab eines Jägerbataillons. Seit 2016 am Institut für Friedenssicherung und Konfliktmanagement an der Landesverteidigungsakademie des Österreichischen Bundesheeres.

christoph.bilban@bmlv.gv.at

98 Vgl. Galeotti: Russian Political War, S. 47f.
99 Vgl. Fridman: Russian «Hybrid Warfare», S. 118ff.; Bilban: Mythos «Gerasimov-Doktrin», S. 109.
100 Vgl. Bilban/Grininger: Was bleibt von der «Gerasimov-Doktrin»?, S. 286ff.
101 Vgl. Galeotti: Russian Political War, S. 44f.; Truffer, Patrick: Ein weiter Weg: Die russische Militärreform – Teil 3. In: Offiziere.ch, 11.02.2019, <https://www.offiziere.ch/?p=35192>, abgerufen am 09.04.2019.

Défendre la Suisse dans le cyberespace

Notre société vit depuis les années '80 une transformation radicale due aux technologies de l'information et de la communication (TIC). Cette ère a conduit à la création d'une nouvelle dimension nommée « cyberespace ». Que signifie cette évolution pour la sécurité et la défense de la Suisse, à quels développements et quelles formes de conflictualités liés à cet espace faut-il se préparer ? Les réflexions qui suivent souhaitent dépasser les considérants encore dominants de la sécurité informatique et de la réaction aux cyberincidents courants. Ces lignes se veulent un plaidoyer pour un « continuum sécurité-défense agile, dans la profondeur et en réseau [1] » qui permette de tenir compte de la multitude de facteurs interagissants et de leur rapide évolution.

Gérald Vernez

Définir le cyberespace

Trouver une formule précise pour appréhender un milieu aussi complexe et en constante évolution est un exercice difficile. On peut le définir – même si cela s'avère rapidement insuffisant – comme « *une dimension composée d'éléments tangibles et intangibles dans laquelle sont produites, transformées, transportées*[2] *et stockées des données indispensables aux systèmes et infrastructures assurant le fonctionnement de notre société* ». La fin de cette définition indique qu'il ne s'agit pas seulement d'un espace virtuel. En effet, bien que non défini par des frontières géographiques ou temporelles, cet espace est intimement lié au monde physique duquel il dépend et dans lequel il induit des effets mesurables. Il suffit de considérer nos activités quotidiennes entre transports, travail, santé, information, etc. pour mesurer combien le cyberespace est à la société humaine ce que l'oxygène est à nos poumons. Imaginons seulement ce qui cesserait de fonctionner sans Internet.

Les données sont le « sang » circulant dans les artères du cyberespace et qui permettent aux appareils de produire des effets, de réaliser des actions (voir figure 1) dans le champ virtuel et physique. Ces données sont hébergées sur des supports de stockage et traitées par des algorithmes exécutés par des composants matériels qui dépendent à leur tour de toute une série de services, d'infrastructures complexes et d'énergie. Que l'un de ces éléments dysfonctionne, que la disponibilité, l'intégrité, la confidentialité ou la traçabilité des données et des services les traitant soit affecté et toute action qui en dépend le sera aussi. L'action n'aura pas lieu (ou trop tard) ou pas comme cela était prévu ; l'adversaire ou le concurrent sera alors en mesure d'anticiper ou de gêner nos mouvements, de nous subtiliser des parts de marché ou de nous défaire. Que se passerait-il si des dysfonctionnements étaient provoqués dans des systèmes par des données erratiques. Que resterait-il de notre confiance dans cet espace ?[3]

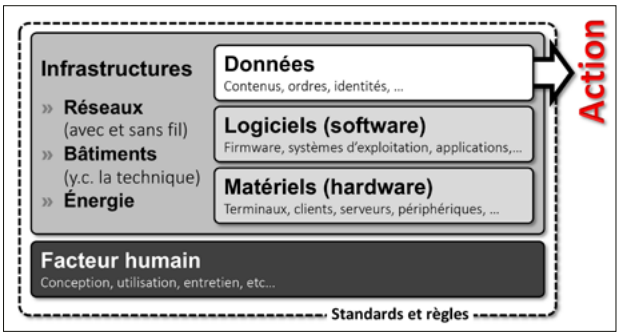


Figure 1 Description du cyberespace. (Vernez)

Il s'agit de réduire l'exposition des infrastructures et systèmes TIC devant être protégés à un niveau acceptable, car vouloir éliminer tous les risques et produire une sécurité à 100% n'est en effet pas un but atteignable.

1 Dans le sens du mot allemand «Verbund» ou du «pas de cyberdéfense sans cyberalliance» du Général Bonnet de Paillerets, Commandant de la cyberdéfense des Armées françaises.

2 Au moyen de fils ou de fibres, mais également d'ondes ; l'espace électromagnétique devient ainsi indissociable du cyberespace et les doctrines de ces deux dimensions tendent à se rapprocher, voire même à se confondre. https://www.hsdl.org/?abstract&did=807334

3 https://actu.epfl.ch/news/l-epfl-s-engage-pour-creer-la-confiance-numerique

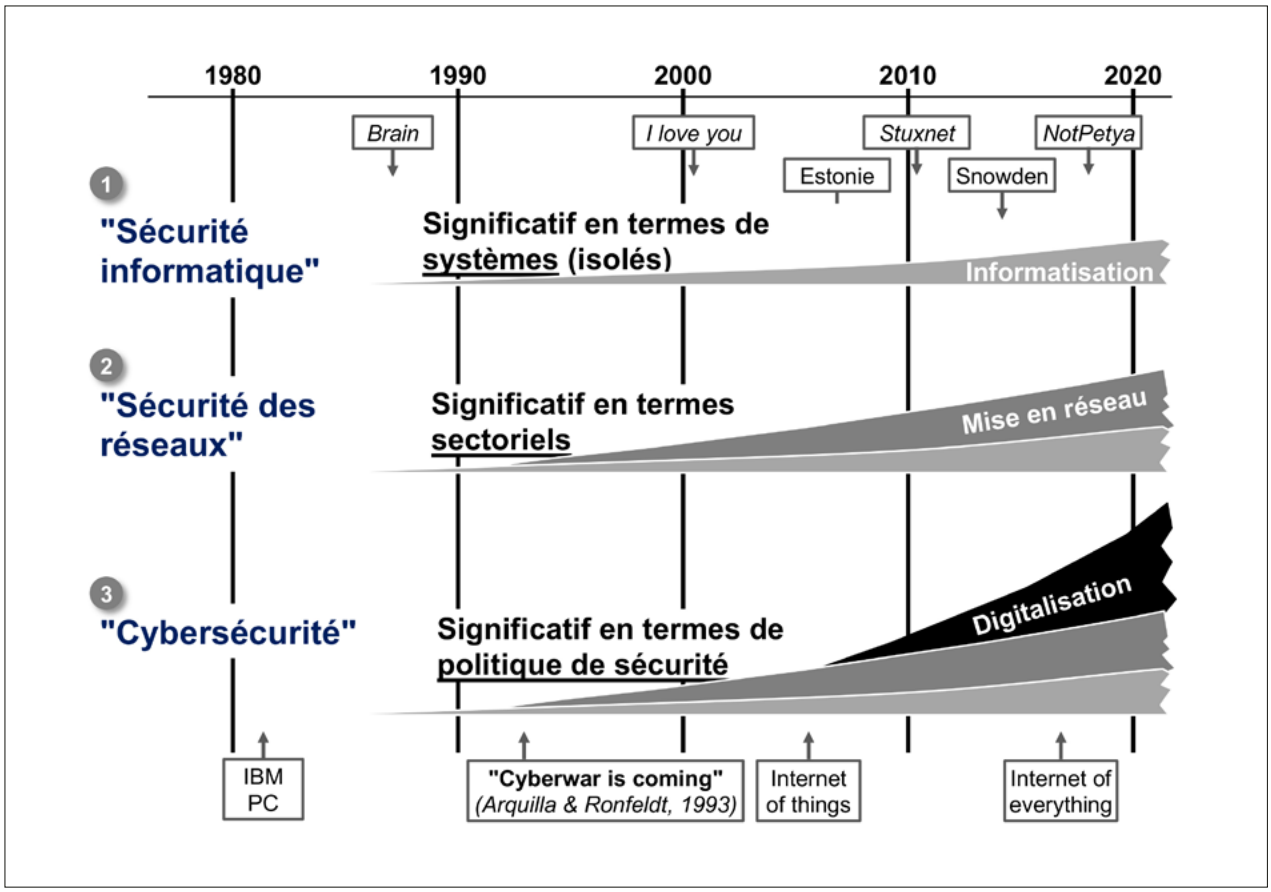


Figure 2 De la sécurité informatique à la cybersécurité. (Vernez)

Quand on considère l'entrelacs complexe et fragile de nos infrastructures et des multiples services dépendants du cyberespace, on réalise combien il est facile pour un adversaire déterminé et compétent d'infliger des dommages à une entité qui dépend de cet espace. On mesure aussi combien il est difficile pour les défenseurs de remplir leur mandat. La dissymétrie existante entre des attaquants qui n'ont besoin que d'un trou pour entrer dans un réseau et les défenseurs qui sont censés le sécuriser et le défendre intégralement impose en effet à ces derniers une approche de type « gestion des risques ». Il s'agit de réduire l'exposition des infrastructures et systèmes TIC devant être protégés à un niveau acceptable, car vouloir éliminer tous les risques et produire une sécurité à 100% n'est en effet pas un but atteignable. Si l'attaquant parvient tout de même à réaliser son attaque, alors le défenseur doit être en mesure de la détecter, de la contenir, de la contrer, voire même de la combattre. Il doit par ailleurs s'assurer que les fonctions et services touchés recouvrent le plus rapidement possible un niveau de service acceptable, celui-ci devant donc être défini au préalable. C'est la notion de résilience.

Tout comme pour les dimensions sol, air, mer, espace et espace électromagnétique, de nombreux acteurs avec des intérêts et des moyens différents sont actifs dans le cyberespace. A la différence des équipements physiques souvent peints en différents tons de vert chez les militaires, la distinction civil – militaire est impossible à établir dans le cyberespace. Un bit ne se laisse pas appliquer une couleur spécifique et dans un vecteur de transport (physique ou onde), ce qui distingue les paquets de données, c'est leur utilisation.

Evolution du cyberespace et des notions de sécurité y relatives

Le cyberespace est une construction humaine dont l'évolution peut[4] être représentée en trois étapes (voir figure 2).

La première étape a vu se développer des systèmes isolés dédiés à des tâches précises et géographiquement déterminées. Cette « informatisation » des débuts visait avant tout à améliorer la performance d'équipements et de services qui n'avaient alors que peu ou pas de liaisons entre eux. Une bonne stratégie d'isolation suffisait à les protéger des rares menaces connues et lorsque survenaient des incidents, leur portée était limitée et ils ne se propageaient guère. On peut simplifier en disant qu'alors est née la ***sécurité informatique,*** une discipline réservée à de rares techniciens spécialisés, souvent relégués dans une cave obscure de l'entreprise par un management qui n'avait même pas conscience de l'existence de ce type de problème ni des métiers requis pour les maîtriser.

4 Michael Bartsch et Stefanie Frey, « Cybersecurity Best Practices, Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden », Article 15 de Adolf Dörig et Gérald Vernez, « Erfahrungselemente erfolgreicher Strategie-Entwicklung und –Umsetzung im Umgang mit existentiellen Risiken im Cyberraum », (Springer, 2018).

La seconde étape se caractérise par l'arrivée et la généralisation de l'Internet et donc de la mise en réseau. Les acteurs de ce domaine ont alors dû apprendre à gérer une forme supplémentaire de sécurité résumée dans la figure 2 par la notion de ***sécurité des réseaux.*** La forte croissance et l'optimisation économique de cette époque ont vu de nombreuses infrastructures – sans que leurs responsables aient vraiment conscience des conséquences de cette évolution – être soudainement reliées au monde extérieur alors que le concept de leur cybersécurité était inexistant au moment de leur déploiement dans les années 60 à 80 du fait de l'absence des cybermenaces telles que nous les connaissons aujourd'hui.

Rapidement est ainsi née la discussion de la sécurité des SCADA[5], puis celle des OT – *Operational Technology* – c'est-à-dire l'ensemble des dispositifs techniques permettant de conduire des opérations de production industrielle, telles que la logistique ou la gestion et la production d'énergie. En termes de sécurité, ce domaine est venu s'ajouter à la sécurité du monde de l'IT – *Information Technology* – avec laquelle elle converge de plus en plus vers l'IIoT – I*ndustrial Internet of Things*. Par-dessus, il faut encore prendre en compte la CT – *Consumer Technology* ou l'électronique grand public – qui comprend l'ensemble des appareils acquis et utilisés par les particuliers (téléviseurs, téléphones portables, montres, caméras, console de jeu, etc.) permettant d'accéder à des services. Cette évolution de la mise en réseau a fait sortir les responsables de la sécurité – pour la plupart des techniciens – de leur isolement et on commence à leur confier des fonctions de direction.

C'est alors de *cybersécurité* de tout un espace complexe et dynamique dont il est question, nous faisant entrer dans des considérations de politique de sécurité, que ce soit au niveau des entreprises, des organisations ou des Etats.

Aux deux premières étapes – essentiellement de nature technique et qui n'ont cessé de prendre de l'ampleur et un cyberespace qui a conquis toutes les activités humaines – vient s'en ajouter une troisième. On passe désormais à la phase de « digitalisation » qui est une transformation en profondeur de la société. Les modèles économiques[6], la circulation de la connaissance, les relations et comportements sociaux, la consommation, les processus de travail et de production sont en train de changer fondamentalement. Désormais ce ne sont plus des systèmes que nous devons protéger mais des prestations et *in fine* il s'agit de l'écosystème sociétal dans son ensemble. C'est alors de ***cybersécurité*** de tout un espace complexe et dynamique dont il est question, nous faisant entrer dans des considérations de politique de sécurité, que ce soit au niveau des entreprises, des organisations ou des Etats. Les techniciens et

Figure 3 Les cités hyperconnectées et « intelligentes ». (shutterstock 578845732-3-1)

spécialistes sont plus utiles et précieux que jamais, mais les tâches de gestion et de conduite sont devenues essentielles à tous les niveaux hiérarchiques et la cybersécurité se décline désormais également en termes et en actions non techniques et politiques.

C'est cette dimension qui a été développée au sein de l'armée pour ses propres besoins depuis la première conception de sa cyberdéfense en 2013 (voir figure 5) et qui a également été mise en place au niveau stratégique du DDPS depuis la crise de RUAG.[7] Avec la décision du Parlement à fin 2017 de créer un Centre de compétences pour la cybersécurité[8] et celle de fin janvier 2019 du Conseil fédéral pour sa mise en œuvre et la création simultanée de structures fédérales de conduite, on peut se réjouir de voir se multiplier l'établissement des domaines de « gouvernance » et de « pilotage ».[9]

Dépendances et complexité: le besoin impératif de «cartographies»

Nombreux sont ceux qui l'ignorent, ne veulent pas l'admettre ou qualifient encore les questions stratégiques liées au cyberespace de « hype » (exagération), mais le constat est implacable : les individus, entreprises, administrations publiques et même les forces armées dépendent intimement du cyberespace, le plus souvent déjà de façon critique et irréversible. Cet espace a gagné une importance que personne n'a vraiment anticipée et nous a littéralement « mangés ». Et avec le développement de la communication mobile à haut débit[10], de l'intelligence artificielle, des technologies quantiques, de la robotique, … ce n'est pas terminé, loin s'en faut. Nous invitons donc le lecteur à s'arrêter un instant sur la figure 3 et à réfléchir à la signification de cette évolution, notamment en termes d'organisation, de comportements, de ressources, de compétences et

5 *Supervisory Control And Data Acquisition,* ou Systèmes de contrôle et d'acquisition de données.

6 Dans une interview accordée à Le Matin le 31 mars 2019, le CEO de Swisscom indique que 70% du chiffre d'affaire de son entreprise provient de produits qui n'existaient pas il y a 10 ans et que la transformation des métiers historiques des PTT l'oblige à trouver de nouveaux produits pour une valeur de 200 millions CHF par an pour remplacer ceux devenus désuets.

7 https://www.parlament.ch/centers/documents/fr/bericht-gpk-n-cyberangriff-ruag-2018-05-08-f.pdf

8 https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173508

9 Pour l'échelon fédéral cet aspect est exposé au chapitre « Dispositif national », pour le DDPS au chapitre « Plan d'action cyberdéfense du DDPS ».

10 https://allinwebblog.wordpress.com/2017/01/25/evolution-of-mobile-communication-from-1g-to-4g-5g-6g-7g

Figure 4 « Pour faire voler un avion il faut toute une armée » (slogan de la campagne de recrutement de l'Armée de l'air française pour le métier de mécanicien sur avions).

en particulier en cas de perturbations, spécifiquement en milieu urbain dense.

Les deux premières phases de développement évoquées dans le dernier chapitre provoquent un biais important qui, fort heureusement, se résorbe graduellement. En effet, ces questions sont encore souvent appréhendées sous l'angle technique, donc du « comment on va régler les problèmes ». L'expérience montre cependant que la question du « quoi » est prioritaire afin de déterminer l'état final recherché et d'identifier les « objets » (physiques ou virtuels) devant être protégés. Les actions qui en découlent ont certes souvent une composante technique, mais de nombreux autres domaines sont également concernés, comme les finances, l'organisation, la diplomatie, la formation et les aspects juridiques.

Cette question du « quoi » est d'une grande complexité car elle implique de devoir comprendre comment fonctionne notre société hyperconnectée et de définir « qui » se trouve dans la chaîne d'approvisionnement et y poursuit quels intérêts. En effet, les optimisations fiscales, techniques, financières, logistiques, etc. des administrations publiques et des entreprises conduisent de nombreux acteurs à déléguer tout ou partie de leurs tâches à des tiers. Si par exemple Apple est bien une entreprise étasunienne, son iPhone est un produit « made in monde ».[11] En fonction donc de l'utilisation que l'on fait d'une technologie ou d'un service, ne considérer que ses avantages est insuffisant et il est désormais impératif de se poser de nouvelles questions. D'où vient tel composant, qui a vérifié et certifié son origine et sa compatibilité avec les systèmes en place ? Les normes sont-elles respectées, … si norme il y a ? Est-on sûr que telle application fait bien ce pour quoi elle est prévue et rien d'autre ?

La *« Supply Chain Security »* n'est pas simplement une nouvelle notion à la mode ; c'est un défi supplémentaire que les pratiques commerciales et managériales exacerbent rapidement et qui concerne également les forces armées soumises à des pressions budgétaires importantes.

Cette dernière interrogation illustre le phénomène des *« easter eggs »*, ces jeux cachés à notre insu dans de nombreuses applications[12], ou des « portes dérobées » supposées[13] ou avérées[14] qui pourraient permettre à un acteur mal intentionné de manipuler (espionnage, chantage, sa-

11 https://www.micmag.be/8-pays-minimum-l-iphone-un-produit-made-in-monde-par-excellence

12 http://www.topito.com/top-10-des-easter-eggs-caches-dans-vos-logiciels-et-sites-internet-favoris

13 https://www.tdg.ch/monde/Pekin-rejette-les-soupcons-norvegiens-sur-Huawei/story/28176289

14 https://fr.wikipedia.org/wiki/Révélations_d%27Edward_Snowden

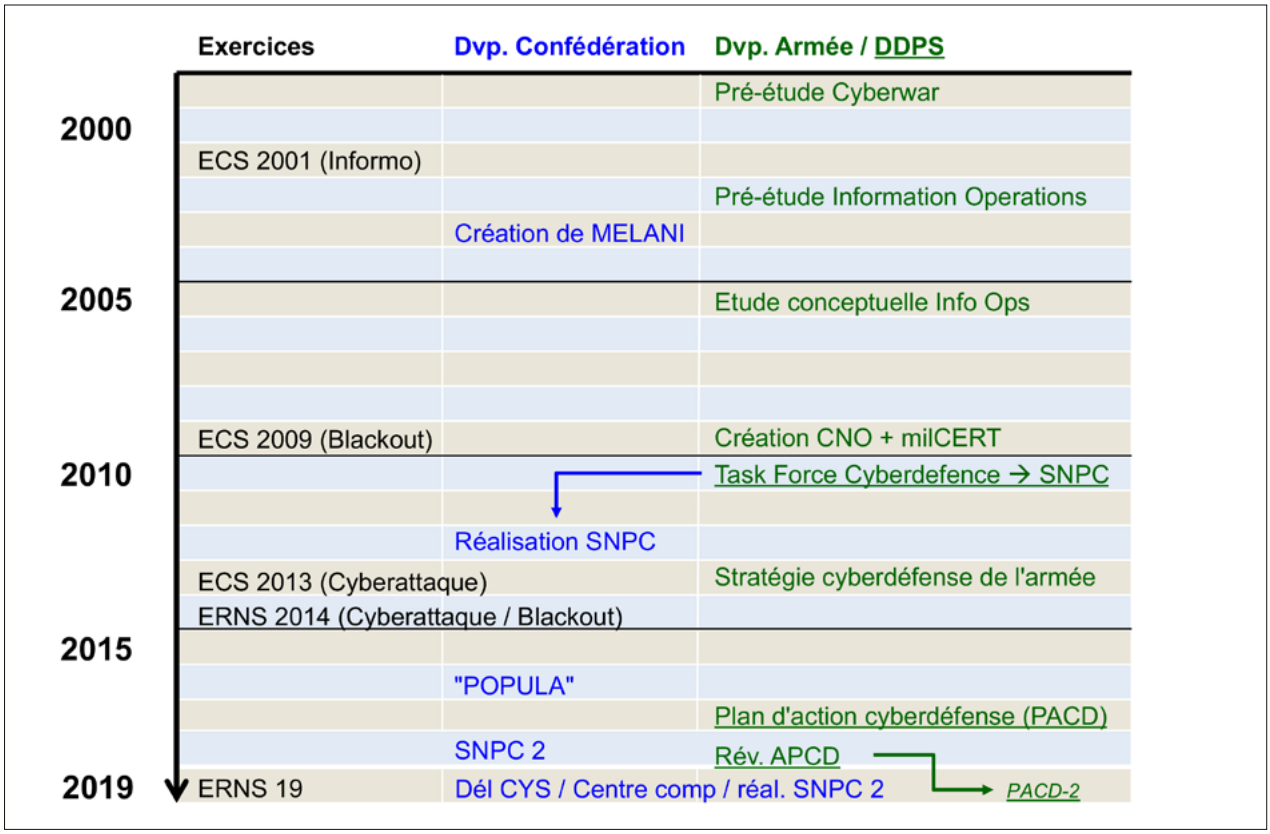


Figure 5 Historique du développement des compétences et capacités de cybersécurité / cyberdéfense en Suisse. (Vernez)

botage, etc.) des infrastructures. L'étendue des compétences requises pour maîtriser toutes les facettes de ce domaine est donc vaste et elle s'ajoute aux multiples aspects existants de qualité du code source[15], d'implémentation, de configuration, d'exploitation, etc. le tout sur fond de documentations souvent défaillantes voire même inexistantes. La « *Supply Chain Security* » n'est pas simplement une nouvelle notion à la mode ; c'est un défi supplémentaire que les pratiques commerciales et managériales exacerbent rapidement et qui concerne également les forces armées soumises à des pressions budgétaires importantes.

La complexité va donc croissant alors que la connaissance de nos infrastructures reste très partielle. Comment dans ces circonstances protéger et défendre nos futures « *smart cities* » ? Qui doit faire ce travail et qui doit l'encadrer et le contrôler ? Comment distinguer entre prestataires compétents et « cybercharlatans » ? Ces questions montrent combien il est important de disposer de « cartographies » à jour[16] pour être en mesure de découvrir et de réduire les risques et de lutter contre toutes les formes de criminalités et d'attaques. La figure 4 illustre la notion de système et la nécessité pour chaque rouage de connaître et d'intégrer les autres.

Développement de l'appréhension des cyberrisques en Suisse

Pour qualifier l'état de développement des moyens de cybersécurité en Suisse, les commentaires du type « nous ne sommes nulle part » ne sont pas rares. Reflètent-ils la réalité ? Non, mais eu égard à la nature des cyberrisques nous devrions être plus avancés. Comme représenté à la figure 5, les défis du cyberespace ne sont pas nouveaux et leur prise en compte remonte même à l'exercice de conduite stratégique (ECS) de 1997. Cet exercice avait pour thème « Les défis d'origine autre que politico-militaire devant être relevés par la Suisse au seuil du XXIe siècle » et une des huit recommandations[17] traitait en particulier la révolution de l'information. Les autres principaux jalons ont été le passage à l'an 2000, la cyberattaque contre l'Estonie en 2007, l'opération Stuxnet de 2010 contre le programme iranien d'enrichissement d'uranium, les révélations de Snowden en 2013 et la cyberattaque contre RUAG découverte en 2016. Ce n'est donc pas fortuit que la dimen-

15 On parle ici d'erreurs involontaires mais que de nombreux acteurs recherchent activement pour les vendre sur le marché des « zero days » et permettre ainsi à leurs détenteurs de disposer d'avantages inconnus des défenseurs, une sorte de joker https://fr.wikipedia.org/wiki/Vulnérabilité_zero-day

16 https://www.satw.ch/fileadmin/user_upload/documents/02_Themen/03_Cyber/SATW-Le-partage-d-information-en-cybersecurite_FR.pdf

17 http://www.alexandria.admin.ch/bv01337269.pdf

sion cyber appartienne désormais a tout grand exercice et ce sera à nouveau le cas lors de l'ERNS[18] en novembre 2019.

Dans le domaine militaire, de nombreux concepts ont fleuri dès la fin des années '90 en relation avec la dimension informationnelle : RMA – *Revolution in Military Affairs,* EBAO – *Effect Based Approach* to Operation, CCW – *Command and Control Warfare,* IW – *Information Warfare,* IO – *Information operations,* etc. Afin de comprendre la signification des changements apportés par cette dimension, le DDPS a réalisé plusieurs chantiers pour les besoins de la défense représentés en vert dans la figure 5. En 2010, le Conseil fédéral l'a également chargé de développer la « Stratégie nationale pour la protection de la suisse contre les cyberrisques » (SNPC) dont la mise en œuvre durant la période de 2012–2017 a été confiée au Département fédéral des finances (DFF). L'armée a alors poursuivi ses travaux et élaboré une propre stratégie de cyberdéfense en 2013.

… le chef du DDPS a ordonné l'établissement du Plan d'Action Cyberdéfense du DDPS (PACD) qui a été approuvé en 2017, puis déjà révisé à fin 2018, alors que sa prochaine refonte est déjà agendée pour 2020.

La cyberattaque contre RUAG survenue en 2016 a cependant rapidement exigé un pilotage au niveau stratégique et la crise a été conduite depuis le Secrétariat général qui s'est doté à cet effet d'une unité organisationnelle conduite par l'auteur de ces lignes. Le besoin de disposer d'une stratégie couvrant l'ensemble des offices composant le DDPS s'est alors rapidement imposé et le chef du DDPS a ordonné l'établissement du Plan d'Action Cyberdéfense du DDPS (PACD) qui a été approuvé en 2017, puis déjà révisé à fin 2018, alors que sa prochaine refonte est déjà agendée pour 2020. Parallèlement, en avril 2017, le Conseil fédéral a chargé le DFF de réviser la première SNPC. Il l'a approuvée en avril 2018 et sa mise en œuvre est en cours et s'étalera jusqu'en 2022.

Dispositif national

En janvier 2019, le Conseil fédéral a défini les domaines « cybersécurité », « cyberdéfense » et « lutte contre la cybercriminalité » et les responsabilités de leur prise en charge au sein de l'administration fédérale. La figure 6 illustre ces domaines ainsi que leurs intersections et élargit la vue aux autres acteurs clés. Le DDPS – tout en assurant sa propre cybersécurité – est spécifiquement responsable du domaine « défense ».

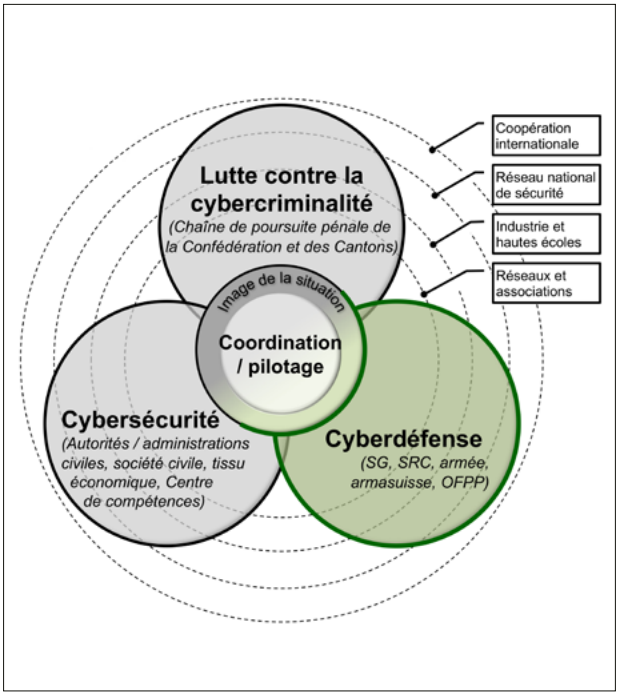


Figure 6 Dispositif national de cybersécurité. (Vernez)

Le centre du dispositif – et c'est cela qui est particulièrement nouveau depuis les récentes décisions du Conseil fédéral – met en évidence deux tâches centrales auxquelles le DDPS participe aussi de manière prépondérante :

- ***l'image de situation*** où le Service de renseignement de la Confédération (SRC) joue déjà un rôle clé, également en matière d'appréciation des cyberrisques ;
- la ***coordination et le pilotage,*** défini par la récente décision du Conseil fédéral[19] au sujet de la création du Centre de compétences pour la cybersécurité sous la direction d'un Délégué à la cybersécurité, des éléments essentiels pour assurer à l'ensemble sa cohérence, tant en termes d'amélioration générale de la sécurité et de la résilience du « système Suisse » que pour la coordination des mesures en cas d'incidents significatifs.

Derrière ces cercles principaux, il y en a quatre autres tout aussi importants :

- la ***coopération internationale*** avec par exemple la prochaine participation de la Suisse au centre de compétence sur la cyberdéfense de l'OTAN à Tallinn[20], un développement qui vient compléter les nombreux échanges existants ;
- le ***réseau national de sécurité*** co-dirigé par la Confédération et les cantons et qui permet d'assurer la cohérence des décisions concernant leurs moyens et mesures ;

18 Exercice du Réseau National de Sécurité 19, https://www.vbs.admin.ch/fr/themes/politique-securite/exercice-reseau-national-securite-2019.html. Il est intéressant de noter que le scénario de l'ERNS 14 démarré au printemps 2014 et joué en novembre de la même année débutait par une cyberattaque touchant l'Europe occidentale et qu'en juillet de la même année la presse se faisait l'écho d'une cyberopération touchant 48 pays et visant des systèmes de contrôle industriels (ICS) en particulier dans les domaines énergétiques ; le groupe responsable, baptisé notamment DRAGONFLY, est actif depuis 2011 https://www.bbc.com/news/technology-28106478 et ses méfaits ont fait encore récemment en 2018 l'objet de diverses résurgences (cf. MELANI, chi. 5.3.1, https://www.newsd.admin.ch/newsd/message/attachments/52183.pdf).

19 https://www.efd.admin.ch/efd/fr/home/dokumentation/nsb-news_list.msg-id-73839.html

20 https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184000

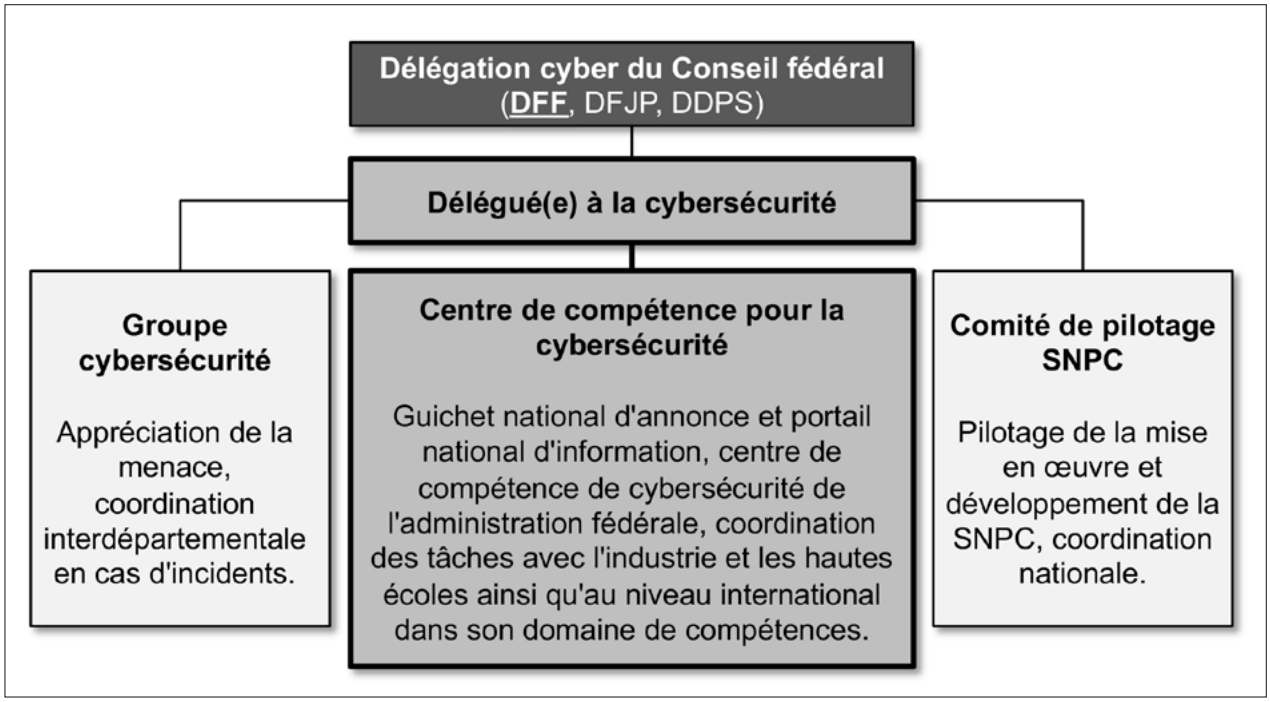


Figure 7 Structure de conduite du domaine cybersécurité de la Confédération. (Vernez)

- ***l'industrie et les hautes écoles*** qui forment le personnel et développent des solutions et disposent de compétences très larges, d'où le besoin d'une connaissance la plus détaillée possible à leur sujet ;
- les ***réseaux et associations*** qui sont un important vivier de savoir et d'échange et qui jouent un rôle politique central.

Le Centre de compétences sera piloté par un(e) délégué(e) à la cybersécurité qui disposera de deux instruments de coordination, l'un opérationnel pour les acteurs institutionnels (y compris les cantons) chargés de la sécurité et de la défense, le second se concentrant sur le développement continu des mesures de protection de la Suisse, en collaboration notamment avec les hautes écoles et l'industrie.

Cet article laisse délibérément de côté le volet de la lutte contre la cybercriminalité. Mentionnons toutefois – sous l'impulsion notamment du Procureur fédéral, de fedpol, de la Conférence des directrices et directeurs cantonaux de justice et police, de la Conférence des procureurs de Suisse ainsi que du Délégué du réseau national de sécurité – les progrès substantiels en cours pour unifier les efforts de la lutte contre la cybercriminalité. Ainsi est en train de croître une structure appelé « CYBERBOARD »[21], un développement d'autant plus important que les formes classiques de criminalité se réduisent au « profit » de la cybercriminalité, sans qu'il soit toutefois possible de mesurer ce phénomène avec précision.

21 https://www.jv-aargau.ch/jwa/vfs/web/2015.jv-aargau.ch/media/publikationen/PDF/Cybercrime.pdf

Plan d'action cyberdéfense du DDPS (PACD)

Comme précédemment mentionné, la cyberattaque subie par RUAG a contribué à une prise de conscience au plus haut niveau et il est devenu clair que l'évolution des cybermenaces nécessitait au DDPS une révision du dispositif et des moyens consacrés. Le chef du DDPS a en conséquence ordonné en juillet 2016 l'établissement du PACD.

La seconde étape a, quant à elle, permis de définir la stratégie et d'identifier les trois missions clés « se protéger », « agir », et « aider » et d'inscrire le tout dans une « architecture » claire et consistante.

La première étape des travaux résumés à la figure 8 a consisté en la réalisation d'un état des lieux pour s'assurer que tous les acteurs avaient la même compréhension des faits. La seconde étape a, quant à elle, permis de définir la stratégie et d'identifier les trois missions clés « se protéger », « agir », et « aider » et d'inscrire le tout dans une « architecture » claire et consistante. La troisième étape a été celle de l'élaboration d'un plan de réalisation où ont été fixés les processus, les responsabilités, les moyens, le calendrier et la conduite du projet. Lors de la révision de ce plan à fin 2018, ont été en outre définis les éléments relatifs aux compétences et dont la réalisation des premiers éléments (Cyber-Lehrgang et CYD-Campus ; voir plus bas) a entretemps débuté. Ces progrès doivent beaucoup à l'intensification de la collaboration avec les écoles polytechniques et aux apports du Groupe d'experts qui accompagne les travaux du DDPS depuis 2013.

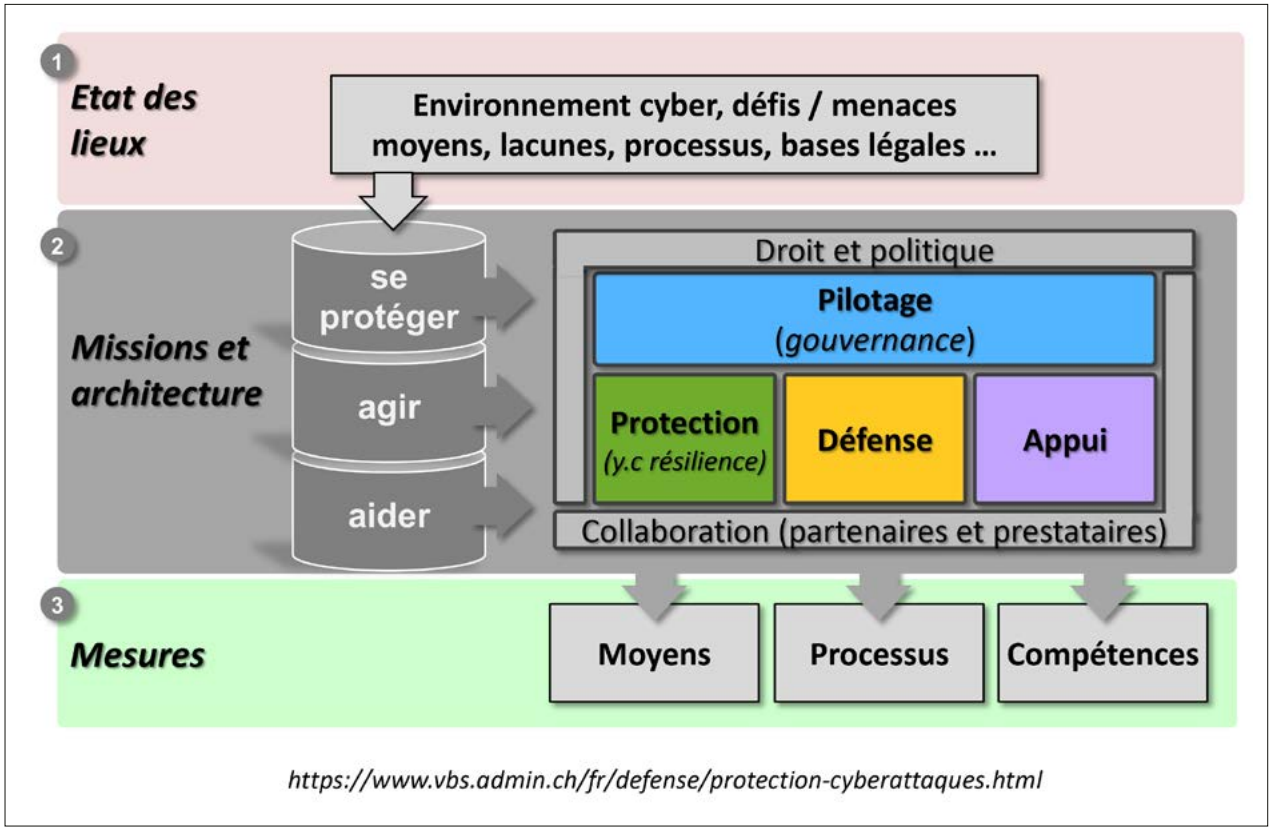


Figure 8 Le Plan d'Action Cyberdéfense du DDPS en bref. (Vernez)

Avec son PACD, le DDPS s'est fixé les buts stratégiques suivants :

« Le DDPS est un ***pôle*** *reconnu en matière de cyberdéfense. En étroite collaboration avec ses partenaires, l'économie et les hautes écoles, il dispose des moyens suffisants en quantité et qualité, afin de :*

- *protéger, défendre*[22] *et assurer la résilience en tout temps et toute circonstance de ses systèmes et infrastructures TIC contre les cybermenaces et cyberattaques ;*
- *conduire les opérations militaires*[23] *et de renseignement*[24] *dans le cyberespace ;*
- *prêter assistance aux autorités civiles en cas de cyberattaques*[25] *contre les infrastructures critiques.*

Avec la motion[26] 17.3507 « Création d'un commandement de cyberdéfense dans l'armée suisse », du Conseiller aux Etats Josef Dittli, le Parlement a donné au volet militaire du PACD une reconnaissance politique qui est venue compléter celle que lui confèrent l'article 100 de la Loi militaire et son ordonnance d'application pour la cyberdéfense. Ainsi, le PACD dispose de bases solides et ses objectifs seront atteints d'ici à fin 2020, notamment grâce aux ressources accordées par l'armée. Comme présenté à la figure 6, la cyberdéfense mise en place par le DDSP fait partie intégrante du dispositif national et la coordination du PACD avec la SNPC 2 (2018–2022) est en bonne voie.

Ce plan a déjà permis de mettre en place de nombreuses mesures, parmi lesquelles les deux initiatives phares suivantes brièvement mentionnées plus haut :

- Le ***« Cyber-Lehrgang »***[27]
  Ce stage de formation permet à des jeunes hommes et femmes ayant réussi les tests d'entrée, d'accomplir une formation de 41 semaines à l'issue de laquelle ils peuvent réaliser un examen de brevet fédéral de « spécialiste en cybersécurité » qui attise d'ores et déjà les convoitises de nombreuses entreprises en recherche de personnel qualifié.

  Le Cyber-Lehrgang comprend une école de recrue, une école de sous-officiers et un stage pratique ou « paiement de galons » (avec son cours de cadres préalable) durant une seconde école de recrue. En tout ces militaires accomplissent ainsi près de 800 heures de formation et d'entraînement technique, éthique, juridique et de conduite. Le premier cours pilote a été lancé à l'été 2018, le second en janvier 2019 et ce programme poursuit sa montée en puissance.

22 Loi fédérale sur l'armée et l'administration militaire, art. 100, al. 1, lit. c, https://www.admin.ch/opc/fr/classified-compilation/19950010/index.html et l'Ordonnance sur la cyberdéfense militaire, https://www.admin.ch/opc/fr/official-compilation/2019/565.pdf

23 Il y a globalement consensus pour reconnaître l'application du droit international en cas de conflit. http://www.unidir.org/files/publications/pdfs/faire-face-aux-cyberconflits-en-473.pdf

24 Loi fédérale sur le renseignement, art. 26, al. 1, lit d-1 et art. 37, al.2, https://www.admin.ch/opc/fr/classified-compilation/20120872/index.html

25 Loi fédérale sur le renseignement, art. 26, al. 1, lit d-2 et art. 37, al.1

26 https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173507

27 https://www.vtg.admin.ch/fr/actualite/themes/cyberdefence.html#Instruction-cybernetique

Le Cyber-Lehrgang comprend une école de recrue, une école de sous-officiers et un stage pratique ou « paiement de galons » (avec son cours de cadres préalable) durant une seconde école de recrue.

Le Cyber-Lehrgang prépare les militaires à devenir des spécialistes dans l'un des domaines suivants :

- *Computer Network Operations* avec des tâches dans le développement d'outils logiciels ainsi que de l'analyse de cyberincidents, de cyberattaques et de vulnérabilités ;
- *milCERT*[28] avec des tâches de détection de cybermenaces contre des systèmes informatiques et de communication de l'armée, de gestion des incidents et d'investigations techniques et d'analyse forensique ;
- *Cyberdéfense* avec des tâches d'analyse de la situation et de sa représentation, de support technique et forensique, de conseil et de formation des troupes.

– Le ***« CYD-Campus »***[29] (campus cyberdéfense)
La division Sciences et Technologie (S+T) d'armasuisse ayant son siège et ses laboratoires à Thoune, s'est rapidement avérée comme le pilier par excellence de la concrétisation de la partie « appui » de l'architecture du PACD. Avec ce CYD-Campus il ne s'agit pas de construire une nouvelle infrastructure, mais de mettre en place un réseau fort de quatre missions principales : 1) établir une plateforme d'anticipation, 2) renforcer les compétences et capacités technico-opératives, 3) attirer, créer et gérer les vocations et talents, 4) renforcer l'interopérabilité des acteurs.

Avec ce CYD-Campus il ne s'agit pas de construire une nouvelle infrastructure, mais de mettre en place un réseau fort de quatre missions principales : 1) établir une plateforme d'anticipation, 2) renforcer les compétences et capacités technico-opératives, 3) attirer, créer et gérer les vocations et talents, 4) renforcer l'interopérabilité des acteurs.

S+T – sur certains sujets en coopération aussi avec l'Académie Suisse des Sciences Techniques, SATW – dispose déjà d'outils de premier plan tel que le programme de veille technologique DEFTECH[30] pour apprécier les développements technologiques. Récemment, S+T a également mis en place un système automatisé de « Surveillance des technologies et des marchés » (STM) qui explore les sources publiques d'information comme par exemple les registres du commerce et les sites Internet d'entreprises.

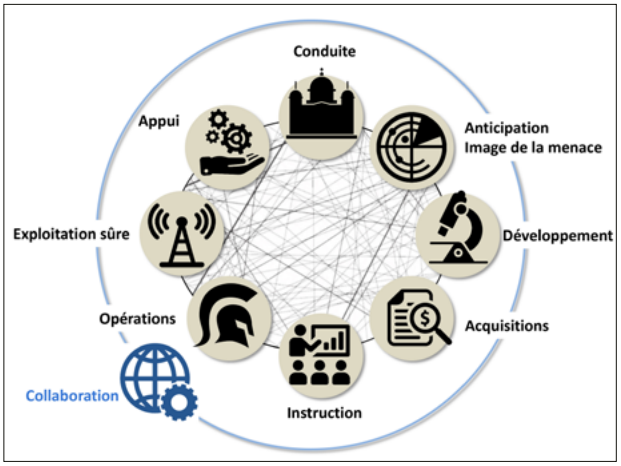


Figure 9 Le DDPS, une « entreprise générale » de la cybersécurité. (Vernez)

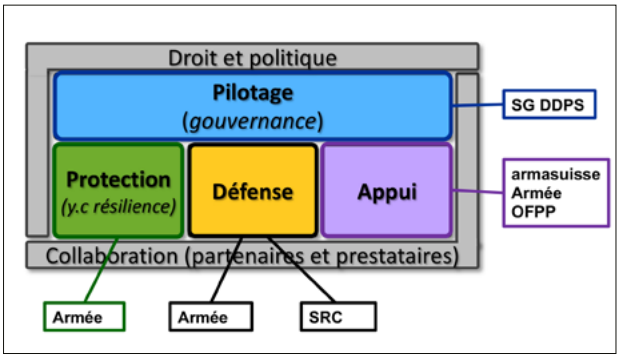


Figure 10 Répartition des tâches PACD au sein du DDPS. (Vernez)

En comparaison internationale les moyens dont dispose la Suisse pourraient en première apparence apparaître modestes. Nous sommes en effet loin des milliers de postes annoncés par certains de nos voisins. Il faut cependant y regarder de plus près. Quel pays de 8.5 millions d'âmes place deux institutions aux 8ème (EPFL) et 9ème (ETHZ) rangs mondiaux[31] en matière de « *computer science & information systems* » ? C'est là juste un exemple qui tend à montrer que les problèmes de la Suisse en matière de cybersécurité semblent relever avant tout d'un manque de confiance en ses capacités qu'elle n'a pas encore identifiées et de la coordination encore insuffisante pour les engager de manière efficiente. La récente décision du Conseil fédéral au sujet de la nomination prochaine d'un(e) délégué(e) à la cybersécurité devrait à cet égard être essentielle.

Au sein du DDPS, ces aspects de conduite sont réglés et le PACD a conduit à la mise en place d'une gouvernance efficace que l'expérience permettra encore d'améliorer. Avec le PACD, le DDPS est désormais assimilable à une « entreprise générale » de la cybersécurité capable d'offrir une palette complète de « produits » (figure 9). Ici également des progrès sont encore nécessaires, notamment en termes de capacité à durer lors d'incidents de grande ampleur auxquels nous devons impérativement nous préparer.

28 Military Computer Emergency Response Team
29 https://www.ar.admin.ch/fr/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.html
30 https://www.ar.admin.ch/en/armasuisse-wissenschaft-und-technologie-w-t/forschungsmanagement-w-t/forschungsprogramm7.html
31 https://www.topuniversities.com/university-rankings/university-subject-rankings/2019/computer-science-information-systems#sorting=rank+region=+country=+faculty=+stars=false+search=

Comme représenté à la figure 10, cinq unités administratives du DDPS sont impliquées et le Secrétariat général assure la coordination de l'ensemble. Avec sa division S+T, armasuisse joue un rôle central pour le développement et l'anticipation technique. On peut dire en forçant le trait que le DDPS dispose ainsi d'une sorte de « mini-DARPA[32] » avec des liens forts avec les milieux de la recherche et déjà nombre de projets concrets tels que récemment encore la protection de récepteurs GPS contre les cyberattaques.[33]

L'observateur non avisé pourrait y voir une fragmentation. Dans les faits le DDPS dispose d'une boîte à outils complète qu'il peut, grâce au « pilotage », mettre en œuvre de manière situative et agile en concentrant et priorisant les effets que peuvent délivrer ses acteurs.

Dans les faits le DDPS dispose d'une boîte à outils complète qu'il peut, grâce au « pilotage », mettre en œuvre de manière situative et agile en concentrant et priorisant les effets que peuvent délivrer ses acteurs.

Développements futurs

En matière de cybersécurité, la Suisse a résolument démarré. Il pleut littéralement des initiatives – nécessitant comme précédemment relevé une intensification significative de la coordination – avec par exemple l'annonce récente du chef du Département de l'économie, de la formation et de la recherche (DEFR) de la création conjointe de l'EPFL et de l'ETHZ d'un master en cybersécurité[34] ou encore les *Swiss Cyber Security Days* qui viennent de se dérouler à Fribourg avec un succès dépassant toutes les attentes et une prochaine édition déjà prévue les 12 et 13 février 2020[35].

Il serait erroné de penser que ces développements tombent dans un désert car beaucoup de choses existent déjà (aussi par exemple à l'université de Lausanne[36]). Dans l'autre sens il serait tout aussi faux de se contenter d'un satisfecit sur la base de ces succès, car les défis sont immenses. Pensons seulement au marché du travail qui va se trouver avec un déficit croissant de personnel qualifié, ICT-Switzerland annonçant[37] pour 2026 un trou de près de 40 000 professionnels dans la branche des TIC, soit près de 18% de l'effectif requis à l'échelle de tout le pays. La sécurité des objets connectés – qui vont devenir toujours plus nombreux et performants avec la 5G et les évolutions suivantes – ainsi que le thème de la *Supply chain security* – seront à n'en point douter des enjeux majeurs.

Aux nombreux défis discutés plus haut il faut ajouter les tensions géopolitiques autour des relations houleuses entre les grandes puissances ou encore les questions énergétiques (Internet consommant bientôt plus de 20% de l'électricité produite[38]), de ressources minérales consommées par cette branche (notamment lithium, silicium, cobalt, terres rares), de domination de certains produits et donc de souveraineté.

D'importantes réflexions sont encore nécessaires, mais il apparaît déjà à ce stade et à la lumière de diverses attaques récentes qualifiables de *« proof on concept »* subies notamment par l'Ukraine, que l'enjeu principal est désormais la sécurité des infrastructures vitales dont dépendent notre société.

A quelles formes et intensités de conflits d'avenir faut-il donc se préparer dans le cyberespace ? D'importantes réflexions sont encore nécessaires, mais il apparaît déjà à ce stade et à la lumière de diverses attaques récentes qualifiables de *« proof on concept »* subies notamment par l'Ukraine[39], que ***l'enjeu principal est désormais la sécurité des infrastructures vitales*** dont dépend notre société.

Pour assurer une défense efficace, quatre éléments-clés semblent s'imposer.

- Mettre en place une ***« défense en profondeur »***. La sécurité ne consiste pas en quelques barrières techniques ; elle comprend l'anticipation, des produits et prestations *« secure by design »*, la protection, la recherche et l'élimination des vulnérabilités, la détection d'incidents et d'anomalies, la recherche et le suivi des menaces, la capacité de résilience en cas d'impact et enfin l'amélioration continue comprenant l'instruction et l'entraînement du personnel à tous les niveaux. Sans ces mesures, la défense sera submergée d'incidents et c'est donc bien un « continuum sécurité – défense » qui doit être établi.
- Se doter de ***« cartographies »*** de l'ensemble des paramètres et de leurs interdépendances. Ces informations sont cruciales pour disposer en tout temps d'une analyse dynamique des risques permettant de définir avec sûreté les priorités et d'assurer une capacité décisionnelle élevée en milieu complexe. Comment assurer une conduite efficace et une bonne coordination avec les autres domaines de la sécurité sans ces informations ? Un proverbe chinois qui trouve ses racines loin dans l'histoire humaine mais qui reste valable aux temps de la digitalisation et que chacun devrait connaître par cœur et appliquer est « Connais ton ennemi et connais-toi toi-même, tu vaincras cent fois sans péril ».[40] Tout cela n'est

32 https://fr.wikipedia.org/wiki/Defense_Advanced_Research_Projects_Agency
33 https://www.ar.admin.ch/fr/home.detail.news.html/ar-internet/news-2018/news-w-t/protection-de-recepteurs-gps-contre-des-cyberattaques.html
34 https://actu.epfl.ch/news/l-epfl-et-l-epfz-lancent-un-master-conjoint-en-c-2
35 https://swisscybersecuritydays.ch/fr
36 https://www.unil.ch/dcs/home.html
37 https://www.ict-berufsbildung.ch/fr/themes/news/details/n-n/372/
38 https://www.rtbf.be/info/economie/detail_internet-bientot-premier-consommateur-mondial-d-electricite?id=9889099
39 https://www.newsd.admin.ch/newsd/message/attachments/52184.pdf
40 Issu de L'art de la guerre de Sun Tzu chapitre III, vers 18. La version originale dit « Connais ton ennemi et connais-toi toi-même ; eussiez-vous cent guerres à soutenir, cent fois vous serez victorieux. Si tu ignores ton ennemi et que tu te connais toi-même, tes chances de perdre et de gagner seront égales. Si tu ignores à la fois ton ennemi et toi-même, tu ne compteras tes combats que par tes défaites. »

pas nouveau et la cybersécurité ne fait pas exception, il est bon de le rappeler.
- Le ***« partage d'information »***: les incidents et anomalies doivent être le plus rapidement portés à la connaissance des autres acteurs afin qu'ils puissent agir avant d'être eux-mêmes touchés. On peut donc espérer que le principe de « l'obligation d'annoncer » finira par s'imposer en Suisse comme le prévoit d'ailleurs la SNPC 2 et qu'ainsi les responsabilités seront clairement établies. Il est impératif de comprendre que le cloisonnement de l'information profite uniquement aux agresseurs. Les vieux principes du maintien du secret doivent impérativement être dépoussiérés.
- La ***« coopération et la coordination »***: à l'ère de la digitalisation, vouloir centraliser les moyens semble être un concept dépassé par la transversalité et la rapide évolution du cyberespace qui se trouve ainsi réparti dans des domaines d'activité et des régimes légaux différents. Même les unités disposant de moyens conséquents ne parviennent plus à disposer au bon moment de toutes les compétences et il s'avère bien plus rentable – aussi en termes d'agilité – de savoir où les chercher et de concentrer leurs effets là où cela est requis.

Pour conclure

Le nombre de variables et d'inconnues est important et évolutif; il ne permet pas d'établir des pronostics précis et la réalisation du PACD est avant tout une affaire de conduite où il faut jongler avec la pénurie de spécialistes, les dimensions rapidement croissantes du problème et relever sans cesse de nouveaux défis. La SNPC 2, le PACD et le Cyberboard de la chaîne de poursuite pénale ne sont pas des aboutissements; ce sont uniquement les étapes d'une évolution qui nous est imposée par la marche du monde et à laquelle nous devons nous adapter et de laquelle nous devons tirer le meilleur au profit de la population suisse et de l'attractivité de notre pays. Le terme sur lequel repose le monde numérique est « confiance »; dès lors que nous confions nos vies à cette dimension, il est vital d'en maîtriser les éléments-clés.

Le terme sur lequel repose le monde numérique est « confiance »; dès lors que nous confions nos vies à cette dimension, il est vital d'en maîtriser les éléments-clés.

A la vue des récentes décisions, des nombreuses actions qui se mettent en place, on constate que la Suisse prend – encore trop lentement il est vrai – graduellement acte des défis et menaces du cyberespace, qu'elle se met en ordre de bataille pour y faire face et qu'elle prend conscience de la dimension des défis et menaces du cyberespace en termes de politique de sécurité. Ces premiers succès et l'absence d'attaques majeures subies jusqu'ici ne sauraient cependant être des excuses pour différer nos efforts. Ils doivent être poursuivis, étendus et renforcés sans aucune concession. Rappelons-nous que le cyberespace est à la société humaine moderne ce que l'oxygène est à nos poumons et sans lui... Il s'agit donc d'assurer notre sécurité dans le cyberespace et au besoin de nous y défendre.

Gérald Vernez

col EMG, Délégué du DDPS pour la cyberdéfense,

E-Mail: gerald.vernez@gs-vbs.admin.ch

Offset-Geschäfte der Schweiz: Bedeutung für die sicherheitsrelevante Technologie- und Industriebasis

Die Fähigkeiten der Industrie müssen die Bedürfnisse der Armee mit Blick auf das gesamte Gefahrenspektrum abdecken können. Dazu wird der Aufbau einer sicherheitsrelevanten Technologie- und Industriebasis (STIB) angestrebt. Offset-Geschäfte umfassen hingegen Verpflichtungen gegenüber den Lieferanten bei Beschaffungen im Ausland. Mittels eines Modells werden die wichtigsten Elemente und die komplexen Interaktionen der beiden Bereiche dargestellt sowie praxisrelevante Schlussfolgerungen gezogen.

Diego Heinen, Christoph Ebnöther

Industriebeteiligungsgeschäfte im Bereich der Sicherheitspolitik sind Kompensationsgeschäfte bei Rüstungsbeschaffungen im Ausland, für welche in der Regel der Begriff Offset-Geschäft verwendet wird. Welche Aspekte, Zusammenhänge und Herausforderungen sind in der Praxis zu beachten, damit ein Offset-Geschäft möglichst wirksam ausfällt und welche Rolle spielt dabei die STIB? Ein zu dieser Frage entwickeltes theoretisches Modell, welches die bestimmenden Elemente aufzeigt, basiert auf diversen theoretischen Hintergründen aus den Bereichen Offset und STIB.[1]

Rüstungspolitik

Den aktuellen Gesamtrahmen für Offset-Geschäfte und für eine STIB Schweiz bieten die Grundsätze des Bundesrates für die Rüstungspolitik des VBS.[2] Gemäss Bundesrat ist das Ziel der Rüstungspolitik, im Sinne der staatlichen Sicherheit festzulegen, welche Bedürfnisse minimal abzudecken sind, um die nötige Handlungsfreiheit zu gewährleisten.[3] Dabei ist stets ein Gleichgewicht zwischen Aufgabenerfüllung und Ressourcenverfügbarkeit zu erhalten.[4] Der Umgang mit länderübergreifenden Abhängigkeiten wird im Rahmen der Rüstungspolitik durch den Bundesrat festgelegt, ebenso welche relevanten Kapazitäten trotz wirtschaftlicher Einschränkungen, wie zum Beispiel der geringen zu produzierenden Stückzahl von Systemkomponenten, weiterhin in der Schweiz zu fördern sind.[5]

Sicherheitsrelevante Technologie- und Industriebasis

Damit die vom Bundesrat im Bereich der Rüstungspolitik festgelegten Kapazitäten in der Schweiz durch eine verbesserte Zusammenarbeit mit Unternehmen gefördert werden können, wird von armasuisse eine STIB-Datenbank geführt, welche den aktuellen Bestand der involvierten Unternehmen erfasst.[6] Allgemeines Ziel der STIB Schweiz ist es, wissenschaftliche und technische Kernkompetenzen sicherzustellen, damit die Fähigkeiten der Industrie im Bedarfsfall und je nach Lage die Bedürfnisse der Armee mit Blick auf das gesamte Risiko- und Gefahrenspektrum abdecken können.[7] Dazu gehört die Fähigkeit der Schweizer Industrie, die betriebenen Systeme zu warten, deren Werterhalt oder Wertsteigerung sicherzustellen und im Bedarfsfall Nachbeschaffungen zu ermöglichen.[8] Die STIB Schweiz umfasst jedoch nicht nur die Industrieun-

1 Obschon es in der Schweiz erfolgreiche Beispiele, wie das Offset-Geschäft in Zusammenhang mit der F/A-18 Kampfjetbeschaffung, gibt, wurde zu Gunsten einer allgemein gültigen Aussage sowie Analyse auf die explizite Nennung sämtlicher Beispiele verzichtet.

2 Bundesrat (2010). *Grundsätze des Bundesrates für die Rüstungspolitik des VBS*. Bern: Bundesrat. Am 24. Oktober 2018 wurden die aktualisierten «Grundsätze des Bundesrates für die Rüstungspolitik des VBS» in Kraft gesetzt. Der Artikel – basierend auf einer im Juli 2018 abgeschlossenen wissenschaftlichen Arbeit – referenziert noch auf die Grundsätze aus dem Jahr 2010, dennoch gibt es keinen Widerspruch zu den aktuellen Grundsätzen des Bundesrates. Teilweise finden sich in den aktuellen Grundsätzen für die Rüstungspolitik bereits Teile aus dem Fazit des Artikels.

3 ebd.

4 ebd.

5 ebd.

6 armasuisse (2018). *Sicherheitsrelevante Technologie- und Industriebasis*. Abgerufen von: https://www.ar.admin.ch/de/beschaffung/sicherheitsrelevante-technologie-und-industriebasis-stib.html

7 ebd.

8 ebd.

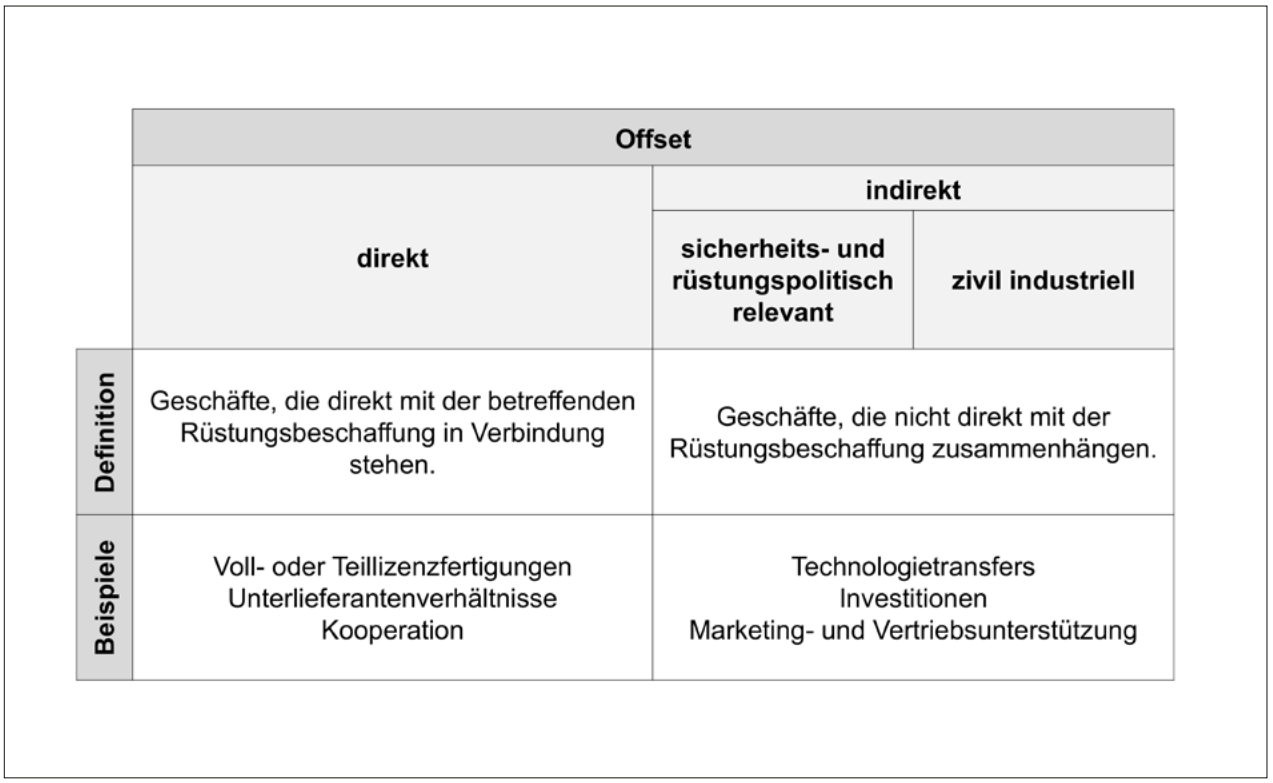


Abbildung 1 Übersicht direkter und indirekter Offset-Geschäfte gemäss Industriebeteiligungsstrategie des Bundesrates. (Heinen/Ebnöther)

ternehmen, welche sicherheitsrelevante Güter oder Teile davon herstellen, sondern auch Forschungseinrichtungen wie Hochschulen, welche einen Beitrag zur Entwicklung und zum Kompetenzaufbau für sicherheitsrelevante Technologien leisten.[9]

Allgemeines Ziel der STIB Schweiz ist es, wissenschaftliche und technische Kernkompetenzen sicherzustellen, damit die Fähigkeiten der Industrie im Bedarfsfall und je nach Lage die Bedürfnisse der Armee mit Blick auf das gesamte Risiko- und Gefahrenspektrum abdecken können.

Offset

Die STIB ist gemäss dem Offset-Management-Modell der armasuisse die Basis für Offset-Geschäfte, soll aber im Umkehrschluss auch durch Offset-Geschäfte gestärkt werden können.[10] Offset-Geschäfte umfassen dabei gemäss Industriebeteiligungsstrategie des Bundesrates alle Arten von Kompensationsgeschäften in Zusammenhang mit Rüstungsbeschaffungen im Ausland.[11] Wie in Abbildung 1 dargestellt, gilt in der Schweiz die Aufteilung in direkte und indirekte Offset-Geschäfte. Der sich aus der Aufteilung ergebende Hauptunterschied liegt darin, dass indirekte Geschäfte entgegen den direkten Geschäften nicht mit dem beschafften Rüstungsgut per se in Verbindung stehen müssen.[12]

Aus der Aufteilung in direkte und indirekte Offset-Geschäfte lässt sich schliessen, dass lediglich die direkten Geschäfte eine gewisse Unabhängigkeit im Betrieb und Unterhalt der Systeme mit sich bringen, da diese im Gegensatz zu den indirekten explizit mit der Rüstungsbeschaffung zusammenhängen. Einheimische Unternehmen erhalten zum Beispiel die Möglichkeit, in die Lieferantenkette des Herstellers aufgenommen zu werden und dadurch gewisse Komponenten eigenständig zu produzieren. Eine andere Variante ist, dass Schweizer Unternehmen das Rüstungsgut selber in Voll- oder Teillizenz herstellen können. Indirekte Geschäfte dienen vornehmlich der Stellung und Positionierung von Schweizer Unternehmen im internationalen Markt.

In der Schweizer Rüstungspolitik ist zudem festgehalten, dass bei Rüstungsbeschaffungen im Ausland die Investitionssumme zu 100 Prozent durch den Lieferanten in der Schweiz zu kompensieren ist.[13] Ausserdem dürfen Offset-Geschäfte nicht als Strukturerhaltungsprogramm für Firmen dienen.[14]

9 VBS (2017). *Luftverteidigung der Zukunft – Sicherheit im Luftraum zum Schutz der Schweiz und ihrer Bevölkerung.* Bern: VBS.
10 armasuisse (2016). *Offset-Policy.* Bern: VBS.
11 Bundesrat (2010). *Industriebeteiligungsstrategie.* Bern: Bundesrat.
12 ebd.
13 Bundesrat (2010). *Grundsätze des Bundesrates für die Rüstungspolitik des VBS.* Bern: Bundesrat.
14 ebd.

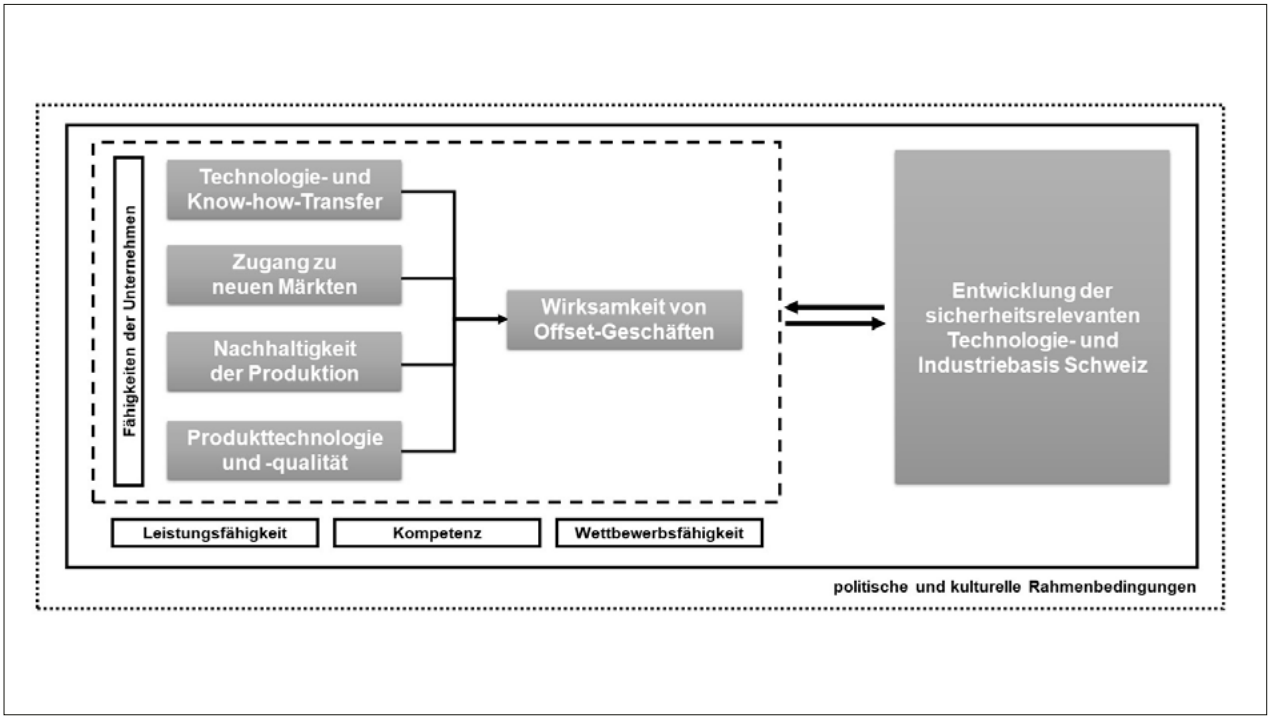


Abbildung 2 Theoretisches Modell von Offset-Geschäften. (Heinen/Ebnöther)

Theoretisches Modell

Die Schweizer Industrie muss also aus sicherheitspolitischen Überlegungen befähigt sein, die Schweizer Armee im Bedarfsfall mit den benötigten Ressourcen zu unterstützen. Dazu bedarf es einer STIB, welche mit den entsprechenden Fähigkeiten ausgestatteten ist. Um diese Fähigkeiten aufbauen und erhalten zu können, verweist die Offset-Policy der armasuisse auf Offset-Geschäfte.[15] Um die effektive Relevanz des Einflusses von Offset-Geschäften in Bezug auf die STIB Schweiz erklären und deuten zu können, muss zunächst die grundsätzliche Frage beantwortet werden, welche Auswirkungen Offset-Geschäfte auf die Entwicklung der STIB Schweiz haben können. Hierzu bedarf es eines umfassenden Modells, das nicht nur die verschiedenen Einflussfaktoren berücksichtigt, sondern auch Interaktionen zwischen Offset-Geschäften und der STIB aufzeigt. Der hier vorgestellte Ansatz ist ein Beitrag zur Lösung dieser Problemstellung.[16] Er fasst die bisher geleitstete Forschung zusammen und erweitert diese zu einem kohärenten Modell.

Das Modell für den Bereich STIB basiert primär auf Keith Hartley's *The Economics of Defence Policy.*[17] Seine zentralen Überlegungen zu den Indikatoren «Leistungsfähigkeit», «Kompetenz» sowie «Wettbewerbsfähigkeit» zur Evaluation der Stärke einer STIB wurden in das Modell übernommen. Diese Indikatoren können als Grundpfeiler der Wirksamkeitsmessung von Offset-Geschäften betrachtet werden.

Zum anderen bezieht sich das Modell im Problemkreis der Wirksamkeit von Offset-Geschäften auf Stéphane Rapaz, der in seiner Dissertation *Swiss Defence Offsets: The Case of Aerospace* diesen Teilbereich untersucht hat.[18] Rapaz zieht zur Analyse von Offset-Geschäften die Faktoren «Technologie- und Know-how-Transfer», «Zugang zu neuen Märkten», «Nachhaltigkeit der Produktion» und «Produkttechnologie und -qualität»[19] heran. Sie eignen sich als Faktorengruppe sehr gut, um die Wirksamkeit von Offset-Geschäften zu erfassen, die in einem direkten Zusammenhang mit der Entwicklung der STIB stehen.

Das bedeutet, dass die in Offset-Geschäften involvierten Unternehmen bestimmte Anforderungen erfüllen müssen, damit der gewünschte Output an Wirksamkeit überhaupt erreicht werden kann.

Die Erkenntnisse aus den Forschungen von Hartley und Rapaz bezüglich bestimmender Faktoren ergänzen sich und können widerspruchsfrei in ein Modell übernom-

15 armasuisse (2018). *Rüstungspolitik des Bundesrates.* Abgerufen von: https://www.ar.admin.ch/de/beschaffung/ruestungspolitik-des-bundesrates.html

16 Heinen, Diego (2018). *Offset-Geschäfte der Schweiz – Bedeutung für die sicherheitsrelevante Technologie- und Industriebasis.* Masterarbeit: ZHAW, S. 14–20.

17 Hartley, Keith (2011). *The Economics of Defence Policy.* Abingdon (UK): Routledge.

18 Rapaz, Stéphane (2004). *Swiss Defence Offsets: The Case of Aerospace.* MDA Dissertation: Cranfield University.

19 Beim Faktor Produkttechnologie und -qualität ist aufgrund des hohen Qualitätsstandards der Schweizer Industriebranche primär auf die Produkttechnologie zu fokussieren. Die Produktqualität kann dahingegen als befähigend angesehen werden, indem das Unternehmen aufgrund seines hohen Qualitätsstandards zu neuem Wissen und neuen Aufträgen kommen kann.

men werden. Die Faktorengruppen von Hartley und Rapaz alleine reichen jedoch noch nicht aus, um dem Anspruch eines umfassenden Ansatzes gerecht zu werden. Als ergänzender Indikator, welcher für alle vier Wirksamkeitsfaktoren von Relevanz ist, muss die den Unternehmen zugrunde liegende Fähigkeit ins Modell aufgenommen werden.[20] Das bedeutet, dass die in Offset-Geschäften involvierten Unternehmen bestimmte Anforderungen erfüllen müssen, damit der gewünschte Output an Wirksamkeit überhaupt erreicht werden kann. Eine weitere, in der bisherigen Forschung zu wenig berücksichtigte Relation ist, dass nicht nur Offset-Geschäfte einen Einfluss auf die Entwicklung der STIB haben können, sondern dass ein Einfluss auch in entgegengesetzter Richtung, das heisst von der STIB auf Offset-Geschäfte festgestellt werden kann.[21] Den äusseren Rahmen des Modells bilden dabei die politischen und kulturellen Rahmenbedingungen. Sie wurden bei der Entwicklung des Modells vorläufig als statisch betrachtet. Bei einer allfälligen Weiterentwicklung des Modells ist es unabdingbar, die Einflüsse, die aus der Politik und des kulturellen Umfelds auf das Modell wirken, ebenfalls zu untersuchen.

Das theoretische Modell wurde einerseits anhand Interviews mit Expertinnen und Experten aus den Bereichen Politik und Verwaltung sowie aus Verbänden, KMU und Grossunternehmen, welche aufgrund ihrer Tätigkeit mit Offset-Geschäften und der STIB zu tun haben, auf seine Konsistenz hin überprüft. Andererseits wurden Erkenntnisse aus den Experteninterviews in das theoretische Modell aufgenommen, wodurch dieses in bestimmten Bereichen erweitert werden konnte.

Das Modell weist durch die gleichzeitig, aber in unterschiedlicher Intensität wirkenden Faktoren eine hohe Komplexität auf. Die Erfassung der Aus- und Rückwirkungen innerhalb des Modells sowie die daraus entstehende Dynamik bleibt Gegenstand der Forschung. Im Folgenden geht es darum, die Zusammenhänge der einzelnen Faktoren und die dazugehörigen Herausforderungen sowohl für die Verwaltung wie auch für die Industrie ausführlich zu erläutern. Ziel ist es dabei, darzustellen, wie die verschiedenen Faktoren aus dem theoretischen Modell interagieren und auf welche Bereiche der Interaktion ein Fokus zu legen ist.

Wirksamkeitsfaktor Technologie- und Know-how-Transfer

Der Einfluss von Technologie- und Know-how-Transfers zeigt sich unter anderem in der Initialisierung von neuen Projekten, welche dank des zusätzlich generierten Wissens akquiriert werden können und der damit einhergehenden Bereitstellung von neuen Arbeitsplätzen. Ein weiteres wichtiges Element ist der Eintritt in die *supply chain* des Herstellers.[22] Als Chance kann auch die Reduktion der Abhängigkeit vom Hersteller angesehen werden, was mit einer Stärkung der STIB einhergeht. Zusätzlich bietet ein Technologie- und Know-how-Transfer einen Vorteil betreffend Verständnis des zu beschaffenden Systems, welches erst mit dem nötigen Wissen vertieft getestet und beurteilt werden kann. Unternehmensintern bereits vorhandenes Know-how wirkt unterstützend für die Erlangung eines Auftrages im Rahmen von Offset-Geschäften.

Bei einem frühzeitigen Einstieg in ein Projekt kann aufgrund der Zusammenarbeit auch der Hersteller bei sorgfältiger Auswahl der Lieferanten von einem Transfer profitieren. Dennoch geben Unternehmen nur ungern systemrelevantes Wissen weiter, folglich regelt der freie Markt, wer in den Bereichen Technologie und Wissen führend ist. Jedoch können Offset-Geschäfte den Prozess unterstützen und insbesondere für kleinere Unternehmen den Zugang zu grossen ausländischen Unternehmen ermöglichen und somit den Zugang zu neuen Technologien und neuem Wissen vereinfachen. Für einen Technologie- und Know-how-Transfer sind Offset-Geschäfte nicht zwingend, können aber eine entscheidende initiale Rolle spielen.

Offset-Geschäfte dienen dank eines Technologie- und Know-how-Transfers auch der Bekanntheit eines Unternehmens. Mittels zusätzlich erlangtem Wissen können neue Aufträge eingeholt werden, welche wiederum als Referenz gegenüber potentiellen Neukunden dienen. Gleichzeitig können Fähigkeitslücken mittels gezielten Transfers geschlossen werden, was für die Entwicklung der STIB einen relevanten Faktor darstellt. Wichtig dabei ist, dass Unternehmen ihre Fähigkeitslücken erkennen und bewusst angehen. Wird dies konsequent umgesetzt, erlangen Offset-Geschäfte die benötigte Nachhaltigkeit.

Zusätzlich sind Partnerschaften mit grossen und international tätigen Unternehmen immer auch Empfehlungen gegenüber potentiellen neuen Kunden.

Wirksamkeitsfaktor Zugang zu neuen Märkten

Ein zentraler Aspekt beim Zugang zu neuen Märkten ist, dass der Zugang zur *supply chain* bei bereits existierenden Systemen praktisch nur mittels Offset möglich ist. Ein System-Hersteller ist auf eine gut organisierte und zuverlässige Lieferantenkette angewiesen. Da der Prozess zur Gewinnung von passenden Lieferanten langwierig und aufwändig ist, nehmen Hersteller nur ungern Änderungen vor. Mittels Offset-Geschäften kann der Hersteller aber verpflichtet werden, gewisse Bereiche der Produktion in die Schweiz zu verlagern. Dies ermöglicht Schweizer Unternehmen, insofern diese über die nötigen Fähigkeiten verfügen, den Zugang zu internationalen Herstellern. Ist ein Unternehmen entsprechend vorbereitet, erfüllt es die Kriterien und bewährt sich längerfristig in der Zulieferkette, besteht die Möglichkeit, dass sich dieses beim Hersteller als vertrauenswürdiger Partner etabliert und dadurch weitere Aufträge auch ausserhalb des Offset-Geschäftes erhält. Zusätzlich sind Partnerschaften mit grossen und international tätigen Unternehmen immer auch Empfehlungen gegenüber potentiellen neuen Kunden.

20 Heinen, Diego (2018). *Offset-Geschäfte der Schweiz – Bedeutung für die sicherheitsrelevante Technologie- und Industriebasis.* Masterarbeit: ZHAW, S. 58–60.
21 ebd.
22 Weitere Details dazu werden beim Element «Zugang zu neuen Märkten» aufgezeigt.

In Zusammenhang mit Offset-Geschäften und dem Zugang zu neuen Märkten wird häufig auf die Funktion als *door-opener* verwiesen. In diesem Kontext ist ein *door-opener* eine Eintrittsmöglichkeit in einen neuen Markt, welche bei richtiger Umsetzung durch das Unternehmen unterstützend beim Verbleib im Markt wirken kann. Die Tatsache, dass der Eintritt mittels Offset-Geschäft ermöglicht wurde, reicht aber nicht aus. Das Unternehmen muss zwingend selber in der Lage sein, die dadurch gebotene Chance zu nutzen. Wird diese Chance von den Unternehmen wahrgenommen, kann in die Lieferantenkette eines grossen Herstellers eingedrungen werden, in welche insbesondere kleinere Unternehmen unter normalen Bedingungen faktisch keinen Zugang finden würden. Ausländische Unternehmen kommen auf der Suche nach Lieferanten nicht primär in die Schweiz, daher stellen Offset-Geschäfte eine Möglichkeit für die Schweizer Industrie dar, sich zu präsentieren. Ein zusätzlicher Effekt besteht darin, dass durch neue Kunden potentiell auch neue Bereiche erschlossen werden können und das Unternehmen damit sein Portfolio auf dem Markt erweitern kann. Offset-Geschäfte können aber auch für politische Kampagnen genutzt werden. Einerseits kann mittels Verpflichtungen gegenüber dem Hersteller und einem präzisen Konzept zu Offset-Geschäften eine regionale Verteilung der Aufträge sichergestellt werden. Andererseits können Schweizer Firmen, wenn diese Offset-Verpflichtungen im Ausland eingehen müssen, mittels proaktiver Lieferantensuche politische Unterstützung für den Kauf ihres Systems erlangen. Es kann also festgehalten werden, dass Offset-Geschäfte einen direkten industriellen und einen indirekten politischen Nutzen als *door-opener* haben können.

Der direkte Einfluss eines möglichen Zugangs zu neuen Märkten auf die Wirksamkeit von Offset-Geschäften hängt stark von den potentiellen Lieferantenunternehmen und deren Zielen ab. Der Einfluss kann nur positiv ausfallen und einen wirksamen Effekt entfalten, wenn das Unternehmen auch bereit ist, in neue Märkte vorzustossen. Ist ein Unternehmen nicht gewillt, diesen Schritt in Zusammenhang mit einem Offset-Geschäft zu vollziehen, kann sich der Auftrag nach Ende des Offsets in ein Strukturerhaltungsprogramm wandeln, was nicht gewollt ist und langfristig einen negativen Einfluss hätte. Weiter können Offset-Geschäfte auch ein *door-opener* für ausländische Firmen sein, wenn diese in der Schweiz Fuss fassen möchten. Dieser Faktor ist aber aufgrund des eingeschränkten Schweizer Marktes als untergeordnet zu betrachten.

Wirksamkeitsfaktor Nachhaltigkeit der Produktion

Langfristige Partnerschaften sind ein wichtiger Faktor bei der Nachhaltigkeit der Produktion und aus diesem Grund explizit anzustreben. Es ist zu beachten, dass Offset-Geschäfte aufgrund der Dauer grundsätzlich Langzeitpartnerschaften bedingen, welche jedoch nach Ende der Offset-Verpflichtung weitergeführt werden sollten. Entsprechend wichtig ist der Aufbau einer Langzeitpartnerschaft, für welche sich Unternehmen zunächst innerhalb der etablierten *supply chain* des Herstellers platzieren müssen. Dazu bedarf es der Wettbewerbsfähigkeit, welche als Grundlage für die Nachhaltigkeit dient. In diesem Zusammenhang ist auch ein Rückgang des dank Offset-Geschäften erhaltenen Auftragsvolumens zu vermeiden. Ein Unternehmen muss fähig sein, sich während der Zeitdauer, in der ein Offset-Geschäft abgewickelt wird, so zu positionieren, dass die Aufträge nach Ende des Projektes im gleichen Rahmen weiterlaufen. Ist dies nicht möglich oder von einem Unternehmen nicht angestrebt, würde das Offset-Geschäft nicht die gewünschte Wirkung entfalten.

Kann sich ein Schweizer Unternehmen in der *supply chain* eines grossen Herstellers festsetzen, kann daraus auf lange Sicht ein Mehrwert für die gesamte STIB Schweiz geschaffen werden.

Es muss explizit das Ziel sein, geeignete Unternehmen für die Offset-Geschäfte zu identifizieren, ansonsten besteht ebenfalls die Gefahr eines Strukturerhaltungsprogrammes. Kann sich ein Schweizer Unternehmen in der *supply chain* eines grossen Herstellers festsetzen, kann daraus auf lange Sicht ein Mehrwert für die gesamte STIB Schweiz geschaffen werden. Möglich wäre auch, dass mittels Offset-Geschäften Partnerschaften immer wieder erneuert werden. Dies wird aber aufgrund des geringen Beschaffungsvolumens zunehmend schwieriger, da Neubeschaffungen jeweils zeitlich äusserst exakt gesteuert sein müssten. Ein weiterer zu beachtender Faktor bei Langzeitpartnerschaften, welche sich spezifisch auf ein System beziehen, ist die Lebens- beziehungsweise Betriebsdauer. Wird ein System ausser Dienst gestellt, werden auch die Zulieferteile nicht mehr benötigt. Dementsprechend ist die rechtzeitige Neuausrichtung innerhalb des Angebots des Herstellers wichtig.

Die Nachhaltigkeit eines Offset-Geschäfts verweist auf dessen Wirksamkeit. Idealerweise kann sich ein Unternehmen aus einem Offset-Geschäft heraus weiterentwickeln, sein Wissen multiplizieren und als zuverlässiger Partner festsetzen. Zur effizienten Umsetzung ist ein Monitoring nötig, anhand welchem festgestellt werden kann, ob von ausländischen Unternehmen auch relevante Informationen weitergegeben werden und den Schweizer Unternehmen die Möglichkeit geboten wird, Nachhaltigkeit zu erreichen. Analog müssten die Schweizer Unternehmen bei Bedarf gesteuert und so auf das Ziel der Nachhaltigkeit ausgerichtet werden können.

Das relevanteste Element in Bezug auf Nachhaltigkeit ist die Wettbewerbsfähigkeit von Schweizer Unternehmen. Ein Unternehmen muss in Zusammenhang mit Offset-Geschäften fähig sein, sich international behaupten zu können und die dafür notwendigen Investitionen zu tätigen. Insbesondere für kleine Unternehmen kann dies zu einem kritischen Erfolgsfaktor werden. Stimmt für den Hersteller seitens Lieferanten der Preis, die Qualität und die termingerechte Lieferung nicht, wird die Partnerschaft am Ende der Offset-Verpflichtung mit grosser Wahrscheinlichkeit beendet. Zur Erhaltung seiner Wettbewerbsfähigkeit darf ein Unternehmen nie still stehen und muss sich laufend neu erfinden, um im (internationalen) Wettbewerb zu bestehen. Eine weitere Möglichkeit besteht darin, dass sich

Lieferanten auf Nischenprodukte spezialisieren und dadurch für den Hersteller zu einem kritischen Teil der Lieferkette werden.

Wirksamkeitsfaktor Produkttechnologie und -qualität
Die Entwicklung von Fähigkeiten und Kompetenzen eines Unternehmens bezüglich Produkttechnologie und -qualität haben einen positiven Einfluss auf die Wirksamkeit. Kleine Firmen profitieren von der Einführung neuer Standards, der schriftlichen Festhaltung von Prozessen und der Möglichkeit auf dem internationalen Markt Fuss zu fassen. Grössere Firmen, welche die aufgeführten Faktoren bereits erfüllen, können die Flexibilität verbessern, mit welcher auf Veränderungen reagiert wird. Da die Schweiz grundsätzlich über einen gut entwickelten Technologiestandard verfügt, ist es möglich, dass die Entwicklung mehrheitlich im Bereich der Methodik stattfindet. Ein Grund für diese Verschiebung des Transferfokus kann sein, dass bei Rüstungsbeschaffungen aufgrund der politischen Vorgaben eher ältere Technologien involviert sind. Dies ist begründbar mit dem Grundsatz, dass bewährte Systeme beschafft werden und daher deren Entwicklungsstart bereits einige Jahre zurückliegt. Insbesondere im Bereich der Informationstechnologie ist dies eine grosse Herausforderung, da sich heutzutage der zivile Bereich mindestens so rasch entwickelt wie der militärische.

Gelingt es dann einem Unternehmen, anlässlich des Offset-Geschäftes Referenzen von anerkannten Herstellern zu erlangen, unterstützt dies die Suche nach weiteren Aufträgen.

Die Wettbewerbsfähigkeit kann durch eine verbesserte Produkttechnologie und -qualität ansteigen, insofern die Chance entsprechend genutzt wird. Dies verweist wiederum auf die Fähigkeiten und den Willen eines Unternehmens, welche bei Offset-Geschäften unabdingbar sind. Auch wenn internationale Wettbewerbsfähigkeit zu Beginn schwierig ist, haben gut vorbereitete Unternehmen die Chance, dank einem Offset-Geschäft in den internationalen Markt einzusteigen und sich zu bewähren. Alle Unternehmen, welche in Offset-Geschäfte involviert sein möchten, müssen sich mit dem internationalen Markt auseinandersetzen, um die entsprechenden Vorgaben zu erfüllen. Bereits dieser Schritt bringt einen Vorteil im Bereich der Professionalisierung. Gelingt es dann einem Unternehmen, anlässlich des Offset-Geschäftes Referenzen von anerkannten Herstellern zu erlangen, unterstützt dies die Suche nach weiteren Aufträgen. Es kann argumentiert werden, dass das Offset-Geschäft per se keinen Einfluss auf die Wettbewerbsfähigkeit hat, da diese, wie dargelegt, bereits vorgängig erlangt werden muss. Das Offset-Geschäft funktioniert daher eher als Anreiz für Unternehmen, welche sich international ausrichten möchten. Auch geben die potentiellen Offset-Partner erste Hinweise, welche Fähigkeiten und Kompetenzen für den internationalen Markt relevant sind. An diesen kann sich ein Unternehmen orientieren. Idealerweise würden Hersteller von sich aus wettbewerbsfähige Lieferanten in der Schweiz suchen. Eine verbesserte Wettbewerbsfähigkeit bringt den Unternehmen nicht nur international einen Mehrwert, sondern auch auf nationaler Ebene.

Nicht nur die Industriebasis, sondern auch die Hochschulbasis, welche neues Wissen aufbauen und weiterentwickeln kann, hat die Möglichkeit von Offset-Geschäften zu profitieren. Die Industriebasis – insbesondere die STIB – kann bei korrekter Umsetzung laufend von Expansionsmöglichkeiten und potentiellen Know-how-Transfers profitieren. Es werden zusätzliche Kompetenzen und relevantes Prozesswissen aufgebaut, wodurch neue Partner und Aufträge akquiriert werden können. In einem weiteren Schritt können dadurch wiederum neue Arbeitsplätze geschaffen und folglich die Gesamtwirtschaft gestärkt werden. Da die Schweizer Industrie über einen hohen Qualitätsanspruch verfügt, profitiert der Standort vornehmlich von verbesserten Technologien und neuem Wissen. Die Produktqualität ist ein unterstützender Faktor, dank welchem Schweizer Unternehmen in gewissen Bereichen erst zum nötigen Know-how gelangen. Der Transfer muss aber in Zusammenhang mit der STIB Entwicklung auch einen positiven Effekt aufweisen, das heisst Know-how ist im Bereich von komplexen und *high added value* Produkten aufzubauen. Dies geht unterstützend mit dem bereits erwähnten hohen Qualitätsanspruch der Schweiz einher. Die Wirksamkeit von Offset-Geschäften kann durch die Herstellung von Nischenprodukten und mittels internationaler Zertifizierungen noch verbessert werden. Letzteres ist im Bereich der Wettbewerbsfähigkeit ein zusätzlicher Vorteil. Der primäre Fokus muss somit auf der Erlangung von Kompetenzen liegen, welche in einem weiteren Schritt für die Herstellung von spezialisierten Produkten verwendet werden können. Die Schweiz bewegt sich in einem Bereich der Kosten pro Arbeitsstunde, in welchem die Herstellung einfacher und billiger Produkte im internationalen Vergleich zu teuer ist. Dadurch werden komplexe Systeme und Verfahren, welche dank der vorhandenen Qualität herstell- beziehungsweise durchführbar sind, für die Schweizer Industrie interessant.

Da die Schweizer Industrie über einen hohen Qualitätsanspruch verfügt, profitiert der Standort vornehmlich von verbesserten Technologien und neuem Wissen.

Indikator Fähigkeiten von Unternehmen
Unternehmen müssen die Fähigkeit und Bereitschaft mit sich bringen, den hohen Aufwand vor dem Eintritt in die *supply chain* eines internationalen Herstellers aufzubringen. Dazu gehört unter anderem die Fähigkeit zur Etablierung neuer Prozesse, zur Anpassung an internationale Standards oder zur Erlangung geforderter Zertifikate, was mittels aufwändiger Audits erfolgt. Weiter muss sich ein Schweizer Unternehmen im internationalen Wettbewerb behaupten können, damit Nachhaltigkeit erreicht werden kann. Zudem müssen die finanziellen Rahmenbedingungen gegeben sein, damit die nötigen Investitionen getätigt

werden können. Die Erfüllung der benötigten Fähigkeiten kann insbesondere für kleinere Unternehmen eine beträchtliche Herausforderung sein, da zahlreiche und teils neue Vorgaben gleichzeitig aufkommen. Eine Analyse der Fähigkeiten der Unternehmen ist ausserdem für die Vorgabestelle von Relevanz, da damit eine erste Abwägung vorgenommen werden kann, ob das Unternehmen für die STIB im Zusammenhang mit Offset-Geschäften einen Mehrwert generieren kann oder nicht.

Politische und kulturelle Rahmenbedingungen

Die politischen und kulturellen Rahmenbedingungen zeigen auf, dass sich sowohl die Offset-Geschäfte, wie auch die STIB in ein weitreichendes Framework einzugliedern haben. Die politischen Vorgabestellen definieren den Rahmen von Beschaffungsvorhaben und leisten damit einen wesentlichen Beitrag zum Gesamtkonstrukt. Würde zum Beispiel auf politischer Ebene gegen Offset-Geschäfte entschieden, wäre das gesamte Modell obsolet und ein Einfluss auf die STIB wäre zwangsläufig nicht mehr möglich. Die kulturellen Rahmenbedingungen beziehen sich vornehmlich auf die Zusammenarbeit mit ausländischen Partnern. Je nachdem wo ein Hersteller oder ein Lieferant seinen Hauptsitz hat, sind kulturell geprägte Eigenschaften ebenso wie der Stand der Technologisierung wichtig. Die Kultur und Gewohnheiten des Partnerlandes müssen bekannt und respektiert werden. Ändern lassen sich diese Rahmenbedingungen jedoch nicht, daher müssen sich die Schweizer Unternehmen entsprechend darauf vorbereiten.

Interaktion zwischen Offset-Geschäften und der Entwicklung einer Schweizer STIB

Offset-Geschäfte sind für Unternehmen im Rüstungsbereich relevant, da durch diese ein Kompetenzerhalt innerhalb der STIB möglich wird. Als Grundlage dienen, wie bereits anhand der Wirkungsfaktoren aufgezeigt werden konnte, die Fähigkeiten der Unternehmen, die durch Offset gegebenen Möglichkeiten gezielt und nachhaltig umzusetzen. Mittels Offset-Geschäften, welchen ein ausführliches und langfristig ausgerichtetes Konzept zu Grunde liegen sollte, können spezifisch ausgewählte Fähigkeitslücken innerhalb einer STIB geschlossen werden. Dadurch kann die Unabhängigkeit der Schweiz und der Schweizer Armee in einem Krisenfall vergrössert werden. Dies ist aber nicht zwingend gleichbedeutend mit der Eigenproduktion aller Systeme. Minimales Wissen im Bereich des Unterhalts, der Reparatur und betreffend Werterhalt eines Systems sind jedoch erstrebenswert. Wird dieses spezifische Systemwissen mittels Offset in die Schweiz geholt, können gleichzeitig zusätzliche Arbeitsplätze für Fachleute innerhalb der STIB und ökonomische Wertschöpfung generiert werden. Um den Einfluss von Offset-Geschäften auf die Entwicklung der STIB Schweiz detaillierter erfassen zu können, ist auf die Unterscheidung von direktem und indirektem Offset zurückzugreifen. Beide Varianten des Offsets sind gleichwertig, jedoch trägt indirekter Offset nur marginal zu einer STIB bei, wohingegen direkter Offset den Aufbau einer STIB fördern kann. Aufgrund des direkten Bezuges zwischen dem zu beschaffenden System und den Aufträgen, welche aus direkten Offset-Geschäften hervorgehen, kann der gewünschte Technologie- und Know-how-Transfer besser gesteuert werden. Für eine entsprechende Umsetzung muss dies jedoch bereits beim Beschaffungskonzept des gewünschten Systems explizit festgehalten und bei Vertragsabschluss seitens Hersteller eingefordert werden. Eine Alternative zu den klassischen Offset-Geschäften könnte der Abschluss eines *life-cycle*-Vertrages sein, welcher die Wartung explizit in der Schweiz vorsieht. Dadurch würde die STIB ebenfalls gestärkt, ob aber mittels eines solchen Vertrages ein nachhaltiger Wissenstransfer stattfindet, welcher zu Folgeaufträgen führen kann, müsste vertieft analysiert werden.

Zusätzlich sollte eine STIB zu definieren versuchen, welche Produkte der Schweizer Armee in einem Krisenfall ohne ausländische Abhängigkeit zur Verfügung gestellt werden müssen.

Nicht nur der Einfluss eines Offset-Geschäfts auf die STIB ist möglich, sondern auch, dass mittels STIB-Vorgaben die Wirksamkeit der Offset-Geschäfte gesteuert werden kann. So gibt die STIB Hinweise auf Fähigkeitslücken, welche in der Schweizer Industrielandschaft existieren. Weiter kann mittels einer expliziten Definition der STIB festgehalten werden, welche Bereiche erhalten beziehungsweise aufgebaut werden sollen. Offset-Geschäfte können aufgrund des beschränkten Marktes der Schweiz diesen Prozess, mittels Forderungen an die ausländischen System-Hersteller, unterstützen. Zusätzlich sollte eine STIB zu definieren versuchen, welche Produkte der Schweizer Armee in einem Krisenfall ohne ausländische Abhängigkeit zur Verfügung gestellt werden müssen. Das in der Schweiz nicht vorhandene Know-how für die Herstellung solcher Produkte, könnte wiederum mittels Offset-Geschäften eingefordert werden. Idealerweise wird dies direkt bei der Ausschreibung festgehalten. Nachträglich ist es praktisch unmöglich, die Lücken bei spezifischen Systemen zu schliessen. Eine klare Definition der sicherheitsrelevanten Technologien, welche die Schweizer Industrie selbstständig herstellen können muss, ist elementar.

Herausforderungen bei wirksamen Offset-Geschäften

Bezüglich der Wirksamkeit von Offset-Geschäften existieren diverse Herausforderungen, welche bei der Analyse und der Betrachtung des theoretischen Modells bekannt sein müssen. Im Folgenden werden jene Herausforderungen aufgezeigt, die für die Praxis von hoher Relevanz sind.

In der Schweiz stellen die Vorgaben im Bereich der Exporte eine Herausforderung dar.

In Bezug auf einen Technologie- und Know-how-Transfer sowie den Zugang zu neuen Märkten ist die Wettbewerbsfähigkeit der Unternehmen ein kritischer Faktor. Kleine Unternehmen haben es generell schwerer, im Ausland Aufträge zu erhalten, da eine gewisse Ausdauer, die nötigen Finanzen und eine langfristige Planung verlangt werden. Dazu kommt die Fähigkeit neue Prozesse zu etablieren und

die dazugehörige Anpassungsfähigkeit inklusive dem Willen zur Anpassung. Weiter nimmt die Komplexität der zu beschaffenden Systeme laufend zu, wodurch es schwieriger wird, ein Gesamtsystem zu verstehen. Dieser Effekt wird in der Schweiz durch den international vergleichsweise geringen Bedarf an Rüstungsgütern noch verstärkt. Idealerweise sind Voraussetzungen zu schaffen, welche für alle in einem Offset-Geschäft involvierten Partner eine *win-win* Situation generieren. Dazu bedarf es aber eines Konzepts und einer klaren Zielsetzung, welche von Beginn weg allen Parteien bekannt ist und entsprechend gemeinsam umgesetzt werden kann. In der Schweiz stellen die Vorgaben im Bereich der Exporte eine Herausforderung dar. Relevant ist dabei insbesondere, dass die Exportbeschränkungen variabel sind und auch bereits abgeschlossene Verträge von Schweizer Unternehmen aufgrund von weltpolitischen Entwicklungen und entsprechenden Entscheidungen der Schweizer Regierung nicht mehr erfüllt werden dürfen. Weiter sind die aus Langezeitpartnerschaften entstehenden Abhängigkeiten eine Herausforderung. Werden über Jahre hinweg mit einem Hersteller gute Erfahrungen gemacht, wird möglicherweise ein nahezu blindes Vertrauen aufgebaut, wodurch bei weiteren Produktbestellungen die Konditionen weniger detailliert kontrolliert werden. Denkbar ist auch, dass durch Partnerschaften ein etwas höherer Preis bezahlt wird, da man als Konsument grundsätzlich mit dem Produkt zufrieden ist und weniger aggressiv in die Preisverhandlungen einsteigt.

Bringt ein Unternehmen nicht die nötigen Voraussetzungen – wie die Anpassung an internationale Standards – und eine entsprechende Vision mit, können keine Verbesserungen im Bereich der Produkttechnologie und -qualität erreicht werden. Die Schweizer Industrie muss allerdings im internationalen Vergleich insbesondere in den Bereichen Technologie und Know-how konkurrenzfähig bleiben, zumal andere Ressourcen wie zum Beispiel Land rar und teuer sind. Die Zusammenarbeit zwischen der Industrie und den Hochschulen ist ein weiterer relevanter Faktor. Mögliche gemeinsame Projekte sollten vermehrt initialisiert werden, damit beide Seiten vom jeweiligen Wissen, der internationalen Vernetzung und den besten Fachkräften profitieren können.

Vor dem Hintergrund der Interaktion von Offset und STIB sieht sich ein Hersteller mit der Anforderung beziehungsweise Konsequenz konfrontiert, dass spezifisches Know-how bei einer Beschaffung an Schweizer Unternehmen übergehen wird.

Aus Sicht von Unternehmen, welche Offset-Verpflichtungen unterstehen, stellt die Erfüllung der vom Bestellerland aufgestellten Forderungen eine Herausforderung dar. Durch diese gehen ein Teil nationaler Wertschöpfung und Bereiche des aufgebauten Technologiewissens des Unternehmens in ein anderes Land über. Je nachdem, wie weit dabei das Importland entwickelt ist, kommen für das Unternehmen noch zusätzliche Investitionskosten hinzu, damit das System mit dem in der Schweiz angestrebten Standard produziert und vertrieben werden kann.

Vor dem Hintergrund der Interaktion von Offset und STIB sieht sich ein Hersteller mit der Anforderung *beziehungsweise* Konsequenz konfrontiert, dass spezifisches Know-how bei einer Beschaffung an Schweizer Unternehmen übergehen wird. Da Hersteller gewisse systemrelevante Informationen nicht teilen wollen, muss dies vertraglich geregelt und eingefordert werden. Daraus lässt sich erkennen, dass die dafür notwendigen Verhandlungen bereits in einem frühen Stadium des Beschaffungsprozesses zu führen sind. Auch müssen Offset-Geschäfte herausfordernde Arbeit beinhalten, welche einen Mehrwert generiert. Werden zum Beispiel lediglich Montagearbeiten ausgeführt, ohne dass das System als Ganzes bekannt ist, bringt dies die STIB nicht oder nur sehr eingeschränkt weiter. Eine zusätzliche Herausforderung stellt die nicht gegebene Transparenz von Rüstungsbeschaffungen dar, welche in der Regel auf sicherheitsrelevante Themenbereiche zurückzuführen ist und damit vertraulich zu behandeln sind. Minimal ist aber eine transparente Kontrolle der Zielerreichung von Offset-Geschäften und der STIB nötig, um gegenüber der Bevölkerung und der Regierung Glaubwürdigkeit zu vermitteln. Ferner ist eine solche Kontrolle relevant für eine gezielte Beurteilung der in Offset involvierten Unternehmen und der daraus entstehenden Möglichkeit, aus Fehlern zu lernen.

Fazit

Das dargestellte theoretische Modell weist auf einen Einfluss wirksamer Offset-Geschäfte auf die Entwicklung der STIB Schweiz hin. Im Zusammenspiel zwischen Rüstungspolitik, Offset-Geschäften und STIB sind einige wertvolle Aspekte erkannt worden, von welchen die relevantesten im Folgenden zusammengefasst dargestellt werden.

Standpunkt des Akteurs bei Offset-Geschäften
Initial ist wichtig, dass bei einer Analyse und bei Diskussion betreffend Offset-Geschäften zwingend der Standpunkt des Akteurs bekannt sein muss. Je nachdem, ob der Akteur Offset-Verpflichtungen erfüllen muss oder ob er dank diesen die Möglichkeit erhält, bei einem Hersteller als Zulieferer einzusteigen, herrschen von Grund auf unterschiedliche Ansichten. Verpflichtungen werden nur ungern eingegangen, da diese mit einem Wissenstransfer ins Ausland gekoppelt sind. Daher sind diese eher negativ konnotiert. Offset-Verpflichtungen können jedoch auch eine Chance sein, denn durch proaktives Verhalten können geeignete ausländische Zulieferer gefunden und allenfalls auch politische Unterstützung für den Verkauf des eigenen Produktes aufgebaut werden. Unternehmen, die dank Offset Zugang zum internationalen Markt erhalten, betrachten Kompensationsgeschäfte konsequenterweise als positiv und unterstützend.

Bei Kompensationsgeschäften mit internationalen Herstellern ist der Fokus auf komplexe Teile des Systems, Nischenprodukte oder *high added value* Produkte zu legen.

Voraussetzungen des Standortes Schweiz nutzen

Bei Kompensationsgeschäften mit internationalen Herstellern ist der Fokus auf komplexe Teile des Systems, Nischenprodukte oder *high added value* Produkte zu legen. Ein Technologie- und Know-how-Transfer in diesen Bereichen ist um einiges effizienter und nachhaltiger, als die Produktion einfacher Bauteile in der Schweiz. Analog dazu ist auch die reine Endmontage von Systemen wenig geeignet beziehungsweise ungeeignet, um systemspezifisches und relevantes Wissen aufzubauen. Weiter besteht die Gefahr, dass wenn nicht nachhaltige Arbeiten übernommen werden, das Offset-Geschäft zu einem von der Regierung nicht gewünschten Strukturerhaltungsprogramm verkommt. Können jedoch für das Gesamtsystem relevante Bauteile in der Schweiz produziert werden, lohnt sich für den Lieferanten auch der Einstieg in die *supply chain* des Herstellers, da sich ihm die Möglichkeit bietet, sich für eine langfristige Partnerschaft über die Offset-Verpflichtung hinaus zu empfehlen. Zusätzlich kann international eine Reputation aufgebaut werden, welche zu potentiellen Aufträgen von anderen Herstellern führen kann.

Eine vollständige Unabhängigkeit ist aufgrund des kleinen Rüstungsmarktes der Schweiz weder erstrebenswert noch möglich. Deshalb ist der Fokus auf relevante und spezifisch ausgewählte sicherheitsrelevante Technologien und Industriebereiche zu legen, anhand welcher die STIB ausgerichtet werden soll. Das Ziel dabei muss sein, die Armee mit den limitierten Ressourcen in der Auftragserfüllung möglichst zweckdienlich zu unterstützen. Ebenfalls aufgrund des kleinen heimischen Rüstungsmarktes sollten der Rüstungsindustrie möglichst umfangreiche Exportchancen geboten werden. Dies würde dem Einsatz von Technologien und dem Erhalt von Know-how dienen, da von den Unternehmen ein grösserer Markt bedient und das Auftragsvolumen stabiler gehalten werden könnte. Zu berücksichtigen ist jedoch, dass mittels Kompensationsgeschäften eingeholtes Wissen aufgrund von Vorgaben der Hersteller vielfach auf die Nutzung zu Gunsten des Eigenbedarfs beschränkt ist. Folglich dürfen gewisse Produkte und Dienstleistungen aufgrund von vertraglichen Einschränkungen nicht exportiert werden.

Umfang von Offset-Geschäften

Aktuell werden in der Schweiz bei umfangreichen Rüstungsbeschaffungen seitens der Regierung Kompensationen im Umfang von 100% der Beschaffungskosten gefordert. Diese verteilen sich auf direkte sowie indirekte Offset-Geschäfte[23], wobei insbesondere die direkten Offset-Geschäfte für die Entwicklung einer STIB Schweiz relevant sind. Sollen mit der Beschaffung eines neuen Systems gleichzeitig die Fähigkeitslücken der STIB geschlossen werden, vorausgesetzt diese sind bekannt, könnte möglicherweise ein geringerer Gesamt-Prozentsatz, mit Fokus auf den direkten und STIB-relevanten indirekten Offset, denselben Effekt erreichen. Der Prozentsatz wäre dabei zwangsläufig bei jedem Rüstungsgeschäft anhand der vorhandenen Fähigkeiten der STIB neu zu beurteilen. Parallel zur Reduktion des kompensationspflichtigen Betrages könnten zum Beispiel *life-cycle*-Verträge abgeschlossen werden, welche die nicht-STIB-relevanten Arbeiten dennoch an Unternehmen in der Schweiz binden. Weitere zu berücksichtigende Faktoren sind die Möglichkeiten und Kapazitäten der Schweizer Industriebasis, welche fähig sein muss, den vorgegebenen Prozentsatz der Kompensationsgeschäfte aufzufangen. In diesem Zusammenhang ist die in der Analyse nicht erforschte Möglichkeit des Einsatzes von Multiplikatoren zu erwähnen. Diese ermöglichen, dass der von Investitionen durch Offset-Geschäfte generierte volkswirtschaftliche Nutzen, welcher höher ausfallen kann als die eigentliche monetäre Transaktion, adäquat erfasst wird.[24] Durch eine gezielte Steuerung könnten somit potentielle Kapazitätsengpässe der Industrie aufgefangen werden.

Werden jedoch relevante Bereiche einer STIB definiert, kann mittels intensiver und vielseitiger Zusammenarbeit zwischen der Schweizer Armee, der Privatwirtschaft und den Hochschulen eine gewinnbringende Partnerschaft aufgebaut werden.

Wirksamkeit von Offset-Geschäften mit Blick auf die STIB

Die Rüstungsindustrie und die Armee sollten gemeinsam festhalten, welche Bereiche eine STIB Schweiz in Krisensituationen und im Sinne der Unabhängigkeit eigenständig abdecken können muss. Ist dies nicht explizit definiert, besteht keine Möglichkeit, die Entwicklung der STIB bewusst mit gezielten Offset-Geschäften zu beeinflussen. Werden jedoch relevante Bereiche einer STIB definiert, kann mittels intensiver und vielseitiger Zusammenarbeit zwischen der Schweizer Armee, der Privatwirtschaft und den Hochschulen eine gewinnbringende Partnerschaft aufgebaut werden. Die private Industrie dient auch in Krisensituationen als Zulieferer von Dienstleistungen sowie als Produzent sicherheitsrelevanter Güter. Hochschulen können zusätzlich mittels Forschung, Dienstleistungen sowie der Ausbildung von Fachkräften einen relevanten Beitrag zur STIB leisten. In der Schweiz sollten aus den genannten Gründen gemeinsame Ziele der Partner definiert sein, für welche frühzeitig gegenseitige Erwartungen geklärt werden müssen. Gelingt eine solche Partnerschaft, wäre es denkbar, dass Offset-Geschäfte explizit auf STIB Unternehmen ausgerichtet und die Industriebasis dadurch gestärkt werden kann. Offset-Geschäfte können in diesem Zusammenhang eine *door-opener* Funktion übernehmen, wodurch die Unternehmen die Gelegenheit er-

23 Die Offset-Policy der armasuisse sieht dabei einen Anteil von mindestens 20% direkter Offset-Geschäfte vor und strebt eine regionale Verteilung der Aufträge in die drei Sprachregionen der Schweiz (65% deutsch, 30% französisch und 5% italienisch) an.

24 VBS (2018). *Anforderungen an die Beschaffung eines neuen Kampfflugzeugs (NKF) und eines neuen Systems der bodengestützten Luftverteidigung (BODLUV)*. Bern: VBS.

halten, sich nachhaltig auf dem Weltmarkt zu präsentieren und sich mit guten Leistungen dort festzusetzen. Bei potenziellen langfristigen Partnerschaften ist die personelle Kontinuität ein weiterer wichtiger Faktor. So sollten die Ansprechpartner möglichst während der Laufzeit eines spezifischen Projektes nicht ausgetauscht werden. Ein personeller Wechsel kann eine Verzögerung auslösen, da zunächst Wissen und Verständnis für den Gesamtzusammenhang des neuen Mitarbeiters oder Verantwortlichen aufgebaut werden müssen.

Kommunikation von Offset-Geschäften

Die aktuell in der Schweiz angewandte Definition der Aufteilung in direkten, indirekten sicherheits- und rüstungspolitisch relevanten und indirekten zivil-industriellen Offset wurde während der Analyse vereinzelt als veraltet und nicht adäquat aufgeführt. Zielführender könnte zum Beispiel eine Unterteilung in STIB-relevanten[25] und nicht-STIB-relevanten[26] Offset sein. Dadurch würde eine vereinfachte und klare Definition der für die STIB relevanten Geschäfte ermöglicht. Ausserdem ist in der Öffentlichkeit und der Politik der Begriff Offset eher negativ besetzt, obwohl es sich um einen international bekannten und verwendeten Begriff handelt. Dies verweist darauf, dass in der Schweiz allenfalls eine bessere und proaktive öffentliche Kommunikation in Zusammenhang mit Offset-Geschäften und Rüstungsbeschaffungen angebracht wäre. Dies muss bis auf die lokalpolitische Ebene erfolgen, so dass der allfällige Mehrwert für eine Region zum Beispiel durch zusätzliche Arbeitsplätze, bekannt gemacht wird. Fehlt eine breite Abstützung in der Bevölkerung, haben Offset-Geschäfte langfristig gesehen einen schweren Stand.

Dies verweist darauf, dass in der Schweiz allenfalls eine bessere und proaktive öffentliche Kommunikation in Zusammenhang mit Offset-Geschäften und Rüstungsbeschaffungen angebracht wäre.

Offset-Konzept als Grundlage

Wird anlässlich einer anstehenden Beschaffung entschieden, mittels Kompensationsgeschäften einen nachhaltigen Know-how-Transfer und den Zugang zu neuen Märkten zu ermöglichen, ist eine frühzeitige Ausarbeitung eines beschaffungsspezifischen Offset-Konzeptes von grosser Bedeutung. Existiert das Offset-Konzept zu einem Rüstungsgut zum Beispiel bereits bei der Ausschreibung, wären allen potentiellen Herstellern die Rahmenbedingungen von Beginn an bekannt. Nachträglich Offset-Verpflichtungen in spezifischen Bereichen einzubringen, erweist sich als schwierig. Zusätzlich zu einem Offset-Konzept muss ein Controlling Mechanismus implementiert werden, mit Hilfe dessen kontrolliert werden kann, ob die Verpflichtungen eingehalten werden. Sollten Verstösse erkennbar sein, müssten konsequenterweise Sanktionen eingeleitet werden.

Vereinzelt wird darauf hingewiesen, dass sich Beschaffungen beim Einsatz von Kompensationsgeschäften verteuern könnten. Anlässlich der durchgeführten Analyse wurde dieser Faktor nicht vertieft untersucht, daher kann keine abschliessende Aussage gemacht werden. Dennoch soll erwähnt sein, dass im Gesamtrahmen die Frage gestellt werden sollte, ob sich ein potentieller Mehrpreis bis zu einem gewissen Betrag lohnen würde. Der erwartete Ertrag aus der Investition müsste dabei exakter und wohl von Fall zu Fall analysiert werden. Dieser Abklärungsaufwand könnte sich mit Blick auf zusätzliche Arbeitsplätze und lokale Wertschöpfung lohnen und zudem in ein Offset-Konzept einfliessen.

Abschliessend kann festgehalten werden, dass Offset-Geschäfte durchaus Einfluss auf die Entwicklung der STIB nehmen können. Dazu braucht es eine klare Definition und Zielvorgaben für die STIB, eine klare Konzeption bei Offset-Geschäften sowie Schweizer Unternehmen mit den entsprechenden Fähigkeiten. Offset-Geschäfte und die Entwicklung der STIB können zusammenfassend als interagierendes System betrachtet werden, welches für die Sicherheit der Schweiz gewinnbringend eingesetzt werden kann.

Diego Heinen

MSc BA in Public and Nonprofit Management, Chef militärstrategische und politische Geschäfte, Armeestab, Hptm

E-Mail: diego.heinen@vtg.admin.ch

Christoph Ebnöther

Dr., Dozent ZHAW School of Management and Law, Oberst

E-Mail: ebch@zhaw.ch

25 STIB-relevanter Offset = direkter Offset sowie indirekter sicherheits- und rüstungspolitisch relevanter Offset

26 Nicht-STIB-relevanter Offset = indirekter zivil industrieller Offset

Strategische Kommunikation in den Streitkräften

Das Konzept der strategischen Kommunikation im Rahmen der militärischen Aktivitäten entwickelte sich im Zuge des Afghanistan-Krieges und gewann an Bedeutung im Rahmen der Ukraine-Krise. Einerseits soll mittels strategischer Kommunikation die lokale Bevölkerung in den Krisen- und Kriegsgebieten vom Narrativ des Westens überzeugt werden und andererseits soll die Bevölkerung der truppenstellenden Staaten informiert werden, um Akzeptanz für den Streitkräfteeinsatz zu schaffen. Heute findet in Europa eine stärkere Kooperation auf der Ebene der strategischen Kommunikation statt, wie der Austausch der East StratCom Task Force mit dem NATO Exzellenzzentrum für strategische Kommunikation und der entsprechenden Abteilung für strategische Kommunikation im NATO-Hauptquartier beweist. Die Entwicklung des Konzeptes der strategischen Kommunikation verläuft in Richtung einer integrierten Kommunikation für die Streitkräfte, bei denen eine eindeutige und durchdachte Kommunikationsstrategie und daraus abgeleitete Ziele formuliert werden. Die militärischen Einsätze sollen dabei als Handeln von supranationalen Organisationen oder Nationalstaaten wahrgenommen werden.

Michael Holenweger

Einleitung

Die heutigen militärischen Operationen finden in einem zunehmend dynamischen, unsicheren und risikobehafteten Umfeld statt. Der Einsatz der Streitkräfte nimmt viele unterschiedliche Formen an und erfordert ein hohes Mass an Flexibilität. Die Kriege und Konflikte des 21. Jahrhunderts verbinden unter anderem Elemente der militärischen, politischen, wirtschaftlichen, sozialen und kulturellen Dimension. Für die Schweiz liegt die besondere Herausforderung für die Sicherheit in einer Kombination oder Verkettung der verschiedenen Bedrohungen und Gefahren. Viele der derzeitigen Herausforderungen, welche den Frieden, die Sicherheit oder den Wohlstand der Schweiz in Frage stellen, sind durch die Instabilität in der unmittelbaren Nachbarschaft und die sich wandelnden Bedrohungen bestimmt. Vor allem im Zuge der Ukraine-Krise und der völkerrechtswidrigen Annexion der Krim verschlechterte sich das Verhältnis zwischen dem Westen und Russland, die Verschärfung der Bedrohung durch den dschihadistischen Terrorismus sowie das Ausmass an illegalen Aktivitäten und Missbräuchen im Cyberraum. Der als «hybrider» Krieg bezeichnete Konflikt zwischen Russland und der Ukraine ist auch ein Konflikt, in dem neben der strategischen Kommunikation auch verdeckte militärische Operationen fallen.[1]

Abbildung 1 Die kleinen grünen Männchen auf der Krim. Bewaffnete Soldaten – wie sich später herausstellte Mitglieder russischer Spezialeinheiten – ohne Hoheitsabzeichen an ihrer Uniform auf Patrouille am Flughafen Simferopol auf der Halbinsel Krim, Ukraine.
(Wikimedia Commons 2019)

Diese militärischen Aktionen sind kein neues Phänomen unserer Zeit. Jedoch ist die Informationssphäre inzwischen ein geeigneter Ort, um asymmetrische Aktionen vorzubereiten und durchzuführen. Bei der hybriden Kriegsführung geht es um eine Kombination von zivilen, diplomatischen, wirtschaftlichen, technologischen und militärischen Mitteln mit dem Ziel, ein Land zu destabilisieren oder sein Verhalten zu beeinflussen. Die hybriden

1 Die NATO fasst unter dem *Comprehensive Approach* verschiedene Aspekte der hybriden Kriegsführung zusammen wie z. B. Cyberangriffe, zivil-militärische Zusammenarbeit oder strategische Kommunikation.

Strategien können unterschiedliche Formen annehmen wie z. B. Truppenbewegungen an der Grenze eines Nachbarstaates, Luftraumverletzungen, grosse Militärmanöver oder im Informationsbereich wird mittels Desinformationskampagnen, Cyberattacken, Manipulationen und Behinderung von Wahlen und Abstimmungen versucht, Verwirrung, Chaos und Schaden anzurichten. Durch die gezielte Propaganda und Desinformation wird versucht, die Grundlagen und Grundsätze der europäischen und westlichen Demokratien und deren Souveränität zu untergraben oder ausser Kraft zu setzen, Wahlen zu beeinflussen und extremistische Bewegungen zu unterstützen. Die Annexion der Krim durch Russland und die anschliessende Destabilisierung der Ostukraine zeigt auf, wie militärische und zivile Mittel ineinandergreifen.

Der Erfolg von militärischen Einsätzen hängt weniger vom Ergebnis taktischer Operationen in den Einsatzgebieten ab, sondern vielmehr davon, ob der Zweck, der Verlauf und das Verhalten während des Krieges von der öffentlichen Meinung zu Hause und im Einsatzgebiet wahrgenommen und akzeptiert werden.

Die oben genannten Merkmale scheinen die jüngsten Konflikte in Osteuropa, aber auch im Nahen und Mittleren Osten stark zu prägen. Durch den Wandel im Informationszeitalter sind die heutigen Entscheidungsträger in Politik und Militär gezwungen, Massnahmen hinsichtlich des Informations- und Kommunikationsumfeldes zu ergreifen. Der Erfolg von militärischen Einsätzen hängt weniger vom Ergebnis taktischer Operationen in den Einsatzgebieten ab, sondern vielmehr davon, ob der Zweck, der Verlauf und das Verhalten während des Krieges von der öffentlichen Meinung zu Hause und im Einsatzgebiet wahrgenommen und akzeptiert werden. Das Konzept der strategischen Kommunikation (StratCom) ist eine angemessene Antwort auf die neuen sicherheitspolitischen Herausforderungen für die militärischen und politischen Entscheidungsträger. Nach den Anschlägen vom 11. September 2001 hat das StratCom-Konzept enorm an Bedeutung gewonnen, weil terroristische Organisationen und Aufstände grossen Erfolg im Bereich der Kommunikation erzielt haben, nicht nur in ihren jeweiligen Heimatländern, sondern auch im Westen. General Stanley McChrystal sprach als damaliger Oberkommandierender der ISAF-Mission von einem «Krieg der Ideen», bei dem der Westen einen Kommunikationskampf um die politische Glaubwürdigkeit und Legitimität in den Einsätzen führen müsse. Um der Beeinflussung der Öffentlichkeit durch Terroristen und Aufständische mittels Taten, Bildern und Worten etwas entgegenzusetzen, ergriffen diverse Staaten im Bereich der strategischen Kommunikation proaktiv Massnahmen, um gegen derartige Propaganda und Desinformation vorzugehen und diese zu widerlegen. Ein grundlegendes Problem in Afghanistan war, dass sich die Kommunikationsstrategie der ISAF und der NATO nicht mit den militärischen Aktivitäten der Terrorismus- und Aufstandsbekämpfung deckte. Die propagierten Botschaften von Hoffnung auf ein freies und selbstbestimmtes Leben in einer demokratischen Gesellschaft standen im starken Widerspruch z. B. zur Bombardierung von Zivilisten in Afghanistan, dem Missbrauch von Gefangenen im Abu Ghraib Gefängnis im Irak oder den Koranschändungen im Gefangenenlager von Guantanamo Bay auf Kuba. Diese Vorkommnisse führten nicht nur zu starker Kritik bei der lokalen Bevölkerung, sondern sie waren auch ein Instrument für die Rekrutierung von weiteren Terroristen und führten bei den westlichen Nationen dazu, dass die Unterstützung des Einsatzes in Frage gestellt wurde und sich die Negativspirale in Kombination mit den steigenden Opferzahlen und dem fehlenden Missionserfolg weiter drehte.

Seit dem ISAF-Einsatz wurde die StratCom ständig weiterentwickelt, die Führungssysteme in zahlreichen Streitkräften entsprechend angepasst und die bestehenden Informations- und Kommunikationskapazitäten neu strukturiert, zentralisiert und in einem ganzheitlichen Informationskonzept integriert.

Theoretischer Rahmen von strategischer Kommunikation

Das Konzept der strategischen Kommunikation erfuhr eine zunehmende Aufwertung und zeigte sich in einer grossen Vielfalt von Publikationen aus den Sozialwissenschaften, welche von politischer Kommunikation, Public Relations, Public Affairs, Informations-, Kampagnen-, Change-Kommunikation über Management bis zu interner Kommunikation von Organisationen reichen. Dabei stehen primär soziale Interaktionen mit anderen Organisationen, Unternehmen und der Öffentlichkeit im Vordergrund.

Militärische Organisationen kommunizieren durch ihr Handeln, beziehungsweise handeln auch durch ihre Informations- und Kommunikationspolitik sowohl nach innen als auch nach aussen. Ihre Aktivitäten sind insofern «strategisch» als sie auf ihre Umwelt wirken. Die StratCom in den Streitkräften ist somit nicht einzig und allein auf die Ebene der Strategiefindung innerhalb der Organisation zu beschränken und ist auch nicht von den Handlungen der Organisation zu trennen, weil sämtliche militärischen Aktionen im Einsatz eine kommunikative Wirkung entfalten. Durch den Irakkrieg fand ein Umbruch in der Kommunikationswahrnehmung statt, da dieser Krieg den Zusammenhang zwischen öffentlicher Meinung und Aussenpolitik aufzeigte und im berühmten Konzept des «Gewinnens von Herzen und Verstand» mündete.[2]

Die Konzeptualisierung der strategischen Kommunikation basiert auf folgenden Überlegungen:

1. Die StratCom ist der gezielte Einsatz von Kommunikationsressourcen durch eine Organisation oder ein Unternehmen, um seine Ziele zu erreichen.
2. Alle Arten von Organisationen kommunizieren, um mehr Einfluss in ihrer Arena zu gewinnen. Der öffentliche Sektor agiert in einem zunehmend komplexen und

2 Gelpi et al. (2009).

Abbildung 2 Was beinhaltet strategische Kommunikation? (Holenweger)

vernetzten Umfeld und muss strategische Entscheidungen treffen und diese strategisch kommunizieren, um Aufmerksamkeit auf seine Dienstleistungen und Produkte zu lenken, sich eine gute Reputation zu erarbeiten und Legitimität bei seinen wichtigsten Interessengruppen erlangen zu können.

3. Die Kommunikation einer Organisation ist aus einer integrativen Perspektive zu betrachten. Die konzeptionellen Ansätze wie z. B. Öffentlichkeitsarbeit, politische Kommunikation, Public Relations oder Informationskampagnen unterscheiden sich zwar in Bezug auf die Taktik und das Personal, haben aber gemeinsame Ziele und Strategien. Dabei versucht die StratCom über diese unterschiedlichen Kommunikationsansätze hinauszugehen und Gemeinsamkeiten hervorzuheben und diese in einer gesamtheitlichen Strategie zu integrieren.
4. Die Kommunikation muss fünf grundlegende Komponenten beinhalten:
   a. Identifikation und Segmentierung der Stakeholder;
   b. die Auswahl der Kommunikationskanäle für die Botschaften;
   c. die angestrebten Verhaltensänderungen;
   d. Management von Reputation;
   e. den Einsatz von Kommunikationsprofis.

   Die Ergebnisse der StratCom stehen dabei in direktem Zusammenhang mit den im Planungsprozess ausgewählten Zielen.
5. Elementarer Bestandteil der StratCom ist die Strategie. Strategie wird dabei als mehrdimensionales Konzept verstanden, in welches viele alternative Erkenntnisse einfliessen.

Im militärischen Kontext darf die StratCom nicht als untergeordnetes oder zweitrangiges Mittel betrachtet werden, sondern muss bereits zu Beginn in die Planung der Operationen miteinbezogen werden, um die möglichen strategischen und kommunikativen Wirkungen der militärischen Handlungen zu berücksichtigen und in die Strategie miteinfliessen zu lassen.

Im Rahmen der StratCom werden die verschiedenen Elemente miteinander koordiniert, um Synergien herzustellen und um die zuvor angestrebten militärischen und politischen Ziele zu erreichen. Ein wichtiger Bestandteil der StratCom ist dabei die Koordination zwischen den Massnahmen der zivilen Behörden und den Aktionen der Streitkräfte. Im militärischen Kontext darf die StratCom nicht als untergeordnetes oder zweitrangiges Mittel betrachtet werden, sondern muss bereits zu Beginn in die Planung der Operationen miteinbezogen werden, um die möglichen strategischen und kommunikativen Wirkungen der militärischen Handlungen zu berücksichtigen und in die Strategie miteinfliessen zu lassen. Durch die Einsparungen und ungenügende finanzielle Alimentierung der Verteidigungsetats kommt es auch in den Kommunikationsabteilungen zu Einschnitten und der Frage, wo die Mittel am effizientesten eingesetzt werden sollen, um die Organisations- und Missionsziele zu erreichen. Daher bildet die Evaluation den Grundstein für eine erfolgreiche StratCom,

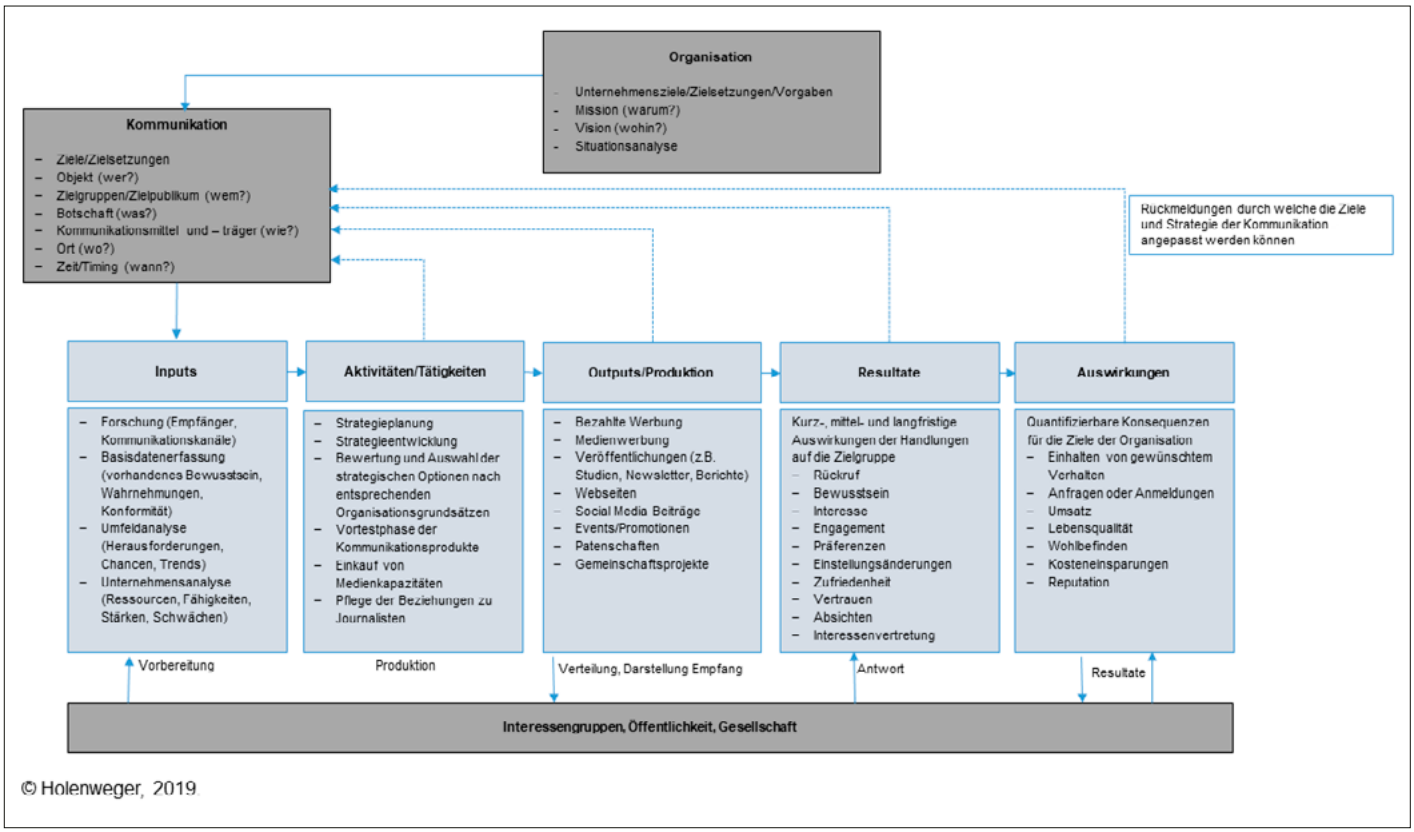


Abbildung 3 Evaluationsmodell der strategischen Kommunikation. (Holenweger)

aufgrund derer beurteilt werden kann, ob und wie eine zielgerichtete Nutzung der Kommunikation zur Stärkung, Erfüllung der Mission, Strategie und Zielerreichung der Organisation beiträgt sowie welche Faktoren die Kommunikationsstrategie beeinflussen.

Das Informations- und Kommunikationsumfeld ist aufgrund der hohen Anzahl von unterschiedlichen Empfängern komplex, vor allem seit der Verfügbarkeit des Internets und der global schnellen Verbreitung von Nachrichten. Der Umgang mit Social Media hat nicht nur bei spontan entstandenen Bewegungen, wie beispielsweise in Nordafrika im Zuge des Arabischen Frühlings zu politischen Veränderungen geführt. Sie ist auch in den Streitkräften zu einem immer grösseren Thema geworden und findet zunehmend auch in den Militärdoktrinen ihren Platz. Vor diesem Hintergrund erfordert die Aufrechterhaltung einer effizienten und effektiven StratCom grosse Anstrengungen, damit unerwünschte Nebenwirkungen, die zur Unterbrechung oder zum Abbruch der Kommunikationsbeziehungen zwischen den Empfängern und den Streitkräften führen könnten, nicht eintreten.

Das einheitliche Auftreten seitens der Kommunikationsträger ist Voraussetzung dafür, dass Klarheit, Glaubwürdigkeit, Transparenz und dadurch Legitimität sowohl vor Ort in den Einsätzen als auch zu Hause bei der Bevölkerung hergestellt werden können.

Die StratCom bemüht sich bei der Vermittlung der Botschaften um eine einheitliche Kommunikation sowohl intern als auch extern durch ihre Kommunikationsträger und versucht dabei die Kohärenz der Kernbotschaften zu wahren. Die interne Kommunikation hat gegenüber den eigenen Soldaten eine wichtige Funktion, indem sie den Sinn der Mission erläutert und die Motivation und Leistungsbereitschaft für den Auftrag herstellt. Militärische Operationen erfüllen zudem einen politischen Auftrag. Dementsprechend ist die Kommunikation von Streitkräften gegenüber den politischen Akteuren auf der nationalen und internationalen Ebene nach Möglichkeit Teil der zivilen Regierungskommunikation und ist daher auf die Belange, Bedürfnisse und Ziele dieser Akteure abzustimmen. Das einheitliche Auftreten seitens der Kommunikationsträger ist Voraussetzung dafür, dass Klarheit, Glaubwürdigkeit, Transparenz und dadurch Legitimität sowohl vor Ort in den Einsätzen als auch zu Hause bei der Bevölkerung hergestellt werden können. Mit Hilfe des oben aufgeführten Evaluationsmodells kann die Effektivität der StratCom hinsichtlich der erzielten Ergebnisse bewertet werden, was wiederum Auswirkungen auf die entsprechende Kommunikationsstrategie hat, die entsprechend angepasst oder neu ausgerichtet werden kann.

Die Entwicklung der strategischen Kommunikation

Im nachfolgenden Abschnitt soll die Entwicklung der strategischen Kommunikation seit ihrer Einführung in die Streitkräfte erläutert werden. Die amerikanische Regierung bestätigte in einem Bericht im Jahr 2004, dass sie

den Krieg in Afghanistan im Kommunikationsbereich verloren habe. Dabei stellten die Autoren fest, dass die Berichte über die psychologischen Operationen nicht mit den nationalen Themen und Vorgaben übereinstimmten und in erster Linie Reaktionen auf die feindliche Propaganda darstellten.[3] 2004 äusserte sich das Defense Science Board sehr kritisch gegenüber der StratCom, wobei das Problem nicht darin bestand, die richtige Botschaft oder den passenden Kommunikationskanal zu finden, sondern sie stellten fest, dass es die mangelnde Glaubwürdigkeit im Einsatz war. Die militärischen Operationen stimmten nicht mit den Botschaften überein und dies führte unweigerlich zu einem Glaubwürdigkeitsverlust.[4]

Im Jahre 2006 wurde das Konzept der StratCom im Rahmen der NATO vor allem durch die USA vorangetrieben. Das US-Aussenministerium definierte die StratCom als «fokussierte Prozesse und Bemühungen der Vereinigten Staaten, welche darauf abzielen, die wichtigsten Zielgruppen zu verstehen und einzubeziehen, um günstige Bedingungen für die Förderung der nationalen Interessen und Ziele durch den Einsatz koordinierter Informationen, Themen, Pläne, Programme und Aktionen, die mit den anderen Elementen der nationalen Macht synchronisiert werden, zu schaffen, zu stärken oder zu erhalten».[5]

Ein Meilenstein in der Weiterentwicklung des Konzeptes war die im September 2009 veröffentliche NATO Strategic Communications Policy.[6] Die StratCom wurde als integraler Bestandteil der Bemühungen der Allianz zur Erreichung ihrer politischen und militärischen Ziele anerkannt. In dem Dokument wurden vier Hauptelemente der strategischen Kommunikation erwähnt:

– Information, Beeinflussung und Überzeugung;
– klare und effektive Zielsetzung;
– Konfliktentschärfung;
– Kommunikation der Aktionen.

Zusätzlich soll die StratCom folgendes aufweisen:

– Schutz und Verbesserung der organisatorischen Glaubwürdigkeit;
– Ausrichtung von Aktionen, Bildern, Signalen und Wörtern zur Informationsplanung und zur Unterstützung von Entscheidungen;
– Klare Identifikation einer Führungskraft, welche für die StratCom verantwortlich ist;
– Verständnis schaffen für die Informationsumgebung, in der die NATO-Streitkräfte tätig sind, insbesondere für das Publikum, das von den Kommunikations- und Informationsaktivitäten beeinflusst werden soll sowie dessen Verhalten.

Diese Richtlinien sollen dazu dienen, die Beziehungen zu den Partnern oder Gleichgesinnten zu stärken, die Tätigkeiten der verschiedenen Einheiten besser zu koordinieren und die Verbindung zwischen den politischen Zielen und gewünschten Kommunikationsoperationen zu verbessern. Diese Leitlinien waren nicht rechtsverbindlich, d. h. justiziabel, sondern sie waren als politische Vorgaben anzusehen.

Insgesamt gibt es ein hohes Mass an Überschneidungen zwischen der NATO StratCom Policy (2009) und den allgemeinen Prinzipien der Public Affairs. Nach dieser Strategie soll die NATO moderne Technik und Technologie einsetzen, um die öffentliche Meinung auf allen Ebenen beeinflussen zu können, auch auf bereits vorhandene öffentliche Stellungnahmen (sofern dies angemessen ist und dabei die grösste mögliche Transparenz in Bezug auf die Verbreitung der Nachrichten angestrebt wird, um gleichzeitig Verständnis und Vertrauen in Bezug auf die Durchführung der Politik, der Operationen und der Missionen der NATO zu erzeugen). Dabei werden folgende Ziele genannt:

a. die Verbesserung der Kohärenz der zivilen und militärischen Kommunikationsmechanismen;
b. die Verbesserung der Kommunikation mit den Zielgruppen/verschiedenen Öffentlichkeiten sowie mit anderen internationalen Akteuren und Organisationen;
c. die bestmögliche Nutzung der vorhandenen Ressourcen.

Diese Massnahmen der StratCom sollen in alle Aktivitäten und Missionen der NATO integriert werden und dies aufgrund der folgenden Grundsätze und Schlüsselprinzipien[7], welche bei der Entwicklung einer Kommunikationsstrategie berücksichtigt werden müssen:

a. Konsistenz und Kohärenz der Nachrichten auf allen Ebenen der Befehlskette;
b. aktives Engagement in der Informationsumgebung, einschliesslich der öffentlichen elektronischen Kommunikation, mit Schwerpunkt auf möglichst hoher Geschwindigkeit und Reaktionsfähigkeit;
c. Gewährleistung der Glaubwürdigkeit der NATO-Kommunikation durch die Förderung der Beziehungen zu Medienvertretern auf Basis von gegenseitigem Vertrauen;
d. eine Vielzahl von Anstrengungen mit maximaler Reichweite, die Einbeziehung aller Kommunikationsfunktionen und aller verfügbaren Kommunikationsplattformen;
e. die Stärkung der Verbreitung von Botschaften im Einklang miteinander, d. h. dass die Botschaften widerspruchfrei sein sollen;
f. das Einholen der öffentlichen Meinung und die Anpassung der Aktivitäten, falls dies erforderlich ist.

Der Leitgedanke der NATO StratCom Policy war es, die Kohäsion zwischen den zivilen und militärischen Kommunikationsmechanismen zu erhöhen, die Kommunikation mit den Stakeholdern zu verbessern und die vorhandenen Ressourcen optimal einzusetzen. Dabei wurden die neuen technologischen Entwicklungen wie beispielsweise der Gebrauch von Social Media berücksichtigt. Die NATO StratCom Policy war der Ursprung für weitere Veränderungen, wie zum Beispiel die ACO Strategic Communication Richtlinie[8], welche Massnahmen im Bereich der Pla-

3 United States Department of Defense (2003).
4 Defense Science Board (2004), 3, 41, 46.
5 QDR (2006).
6 NATO Strategic Communication Policy (2009A).
7 NATO Strategic Communications Policy (2009A), 1-2 ff.
8 NATO, AD 95-2 (2009B).

Abbildung 4 Informationsoperation der US Army in der Khowst Provinz, Afghanistan. U.S Navy Hospital Corpsman Christopher Hogans verteilt während einer Patrouille Flugblätter an lokale afghanische Kinder. Die U.S. Marines führten in der Provinz Khowst, Afghanistan, eine Sicherheits- und Stabilisierungsoperation zur Unterstützung der Operation Enduring Freedom durch. (Wikimedia Commons 2019)

Abbildung 5 Austausch zwischen zivilen Regierungsstellen und Militär. Der Bezirksgouverneur von Chakrez, der Bezirkspolizeichef und der Sicherheitsbeauftragte des Bezirks treffen sich mit afghanischen Beamten während eines Shura in der südafghanischen Provinz Kandahar. Der Bezirksgouverneur äussert seine Besorgnis und seine Ideen für Operationen der afghanischen Nationalarmee und den internationalen Streitkräften gegen die Taliban in seiner Provinz. (Wikimedia Commons 2019)

nung und Durchführung von StratCom aufstellte. Diese Richtlinie verdeutlichte, dass Kommunikation als Waffe eingesetzt werden kann, um Ziele zu erreichen. Gemäss der Richtlinie spielt die StratCom eine zentrale Rolle bei der öffentlichen Meinungsbildung sowohl in den Einsatzländern als auch zu Hause. Durch die ACO Richtlinie soll eine Koordination der Kommunikation zwischen der operativen Planung, der Planung des NATO-Hauptquartiers und den durchgeführten Aktivitäten stattfinden.

Diese Richtlinie verdeutlichte, dass Kommunikation als Waffe eingesetzt werden kann, um Ziele zu erreichen.

Das umfassendste Konzept, welches sich mit StratCom beschäftigte, war das 2010 veröffentlichte NATO Military Concept for Strategic Communications[9], welches die zuvor entwickelten strategischen Kommunikations-Dokumente integrierte. In diesem Dokument wird deutlich, dass die Informationsoperationen koordiniert werden müssen, gleichzeitig aber unabhängig von den Public Affairs Angelegenheiten durchgeführt werden sollen. Weiter wird darauf hingewiesen, dass die Planung und Durchführung der StratCom ein integraler Bestandteil der militärischen Operationen ist. Dabei wurde nochmals die Bedeutung der militärischen Führung hinsichtlich der Kommunikation mit den Zielgruppen auf allen Ebenen hervorgehoben. Um das vorliegende Konzept in den Streitkräften zu implementieren, bedarf es jedoch struktureller Anpassungen und Änderungen bei den Organisations- und Kommunikationsstrukturen. Die wesentlichste Änderung, die vorgeschlagen wurde, war die Delegation der Befugnisse im Bereich der StratCom – die Verbreitung von Informationen auf der Grundlage von Worten, Tönen und Bildern – auf die unterste mögliche Ebene der Befehlskette. Dies deshalb, weil aus den Einsätzen schnell klar wurde, dass die unteren Chargen eine Schlüsselrolle bei der Erfüllung der Aufgaben einnehmen, zentral sind bei der einheitlichen Kommunikation mit den ausgewählten Zielgruppen und wesentlich dafür verantwortlich, dass die strategischen Ziele und Interessen der vorgesetzten Stufe erreicht werden können.

Aus allen oben aufgeführten Dokumenten für die StratCom resultiert eine Kombination aus öffentlichen Angelegenheiten[10], militärischen öffentlichen Angelegenheiten[11], öffentlicher Diplomatie[12], Informationsoperationen[13] und psychologischen Operationen[14], die mit anderen militärischen Aktionen koordiniert werden.

Die öffentlichen Angelegenheiten – *Public Affairs* – bezeichnen die Einflussnahme auf politische Entscheidungsprozesse zwischen Politik, Wirtschaft und Gesellschaft und organisieren dabei die externen Beziehungen einer Organisation z. B. zu Regierungen, Parlamenten, Behörden, Verbänden, Institutionen und der Gesellschaft selbst. Public Affairs bedient sich dabei der Mittel und Instrumente der klassischen Public Relations und setzt zusätzlich spezifische Instrumente der Kommunikation ein, um die relevanten Entscheidungsträger und Meinungsbildner zu informieren.

Die militärischen öffentlichen Angelegenheiten – *Military Public Affairs* – zielen daher darauf ab, möglichst vorteilhafte Beziehungen zwischen den Streitkräften, den Medien und den Regierungsbehörden aufzubauen. Dabei soll eine Arbeitsbeziehung aufgebaut werden, die auf einem regelmässigen Informationsaustausch beruht und sich mit den zuständigen Behörden abstimmt und die Informationen, welche an die Medien weitergegeben werden, koordiniert. Die Military Public Affairs Abteilung stellt mittels Pressemitteilungen, Events, Fotos, Radio, Fernsehen und Internet-Beiträgen Informationsmaterial zur Verfügung mit Bezug zu Militäroperationen oder Ereignissen, bei denen Militärangehörige betroffen sind.

9 NATO, Military Concept for Strategic Communications (2010).

10 NATO Allied Command Operations & Allied Command Transformation (2014).
11 NATO (2011).
12 Vgl. dazu NATO Committee on Public Diplomacy (2014A).
13 NATO Standardization agency (2009)
14 NATO Standardization agency (2007B).

Mittels öffentlicher Diplomatie – *Public Diplomacy* – wird versucht, das Image eines Landes in der Wahrnehmung der anderen Länder zu verbessern. Das US-Aussenministerium umschreibt Public Diplomacy wie folgt: «Public Diplomacy umfasst Aktionen der US-Regierung, die darauf abzielen, ausländische Öffentlichkeiten zu verstehen, zu informieren und zu beeinflussen durch internationale Austauschprogramme, internationale Informationsprogramme, Medienforschung und Umfragen sowie Unterstützung für Nichtregierungsorganisationen. Public Diplomacy festigt die Beziehungen zu Amerikas Verbündeten, sucht andere mit amerikanischen Werten zu impfen und fördert gegenseitiges Verständnis zwischen den Vereinigten Staaten und anderen Gesellschaften. Richtig betrieben, verringert Public Diplomacy das Potenzial für militärische, politische und wirtschaftliche Konflikte und zerstreut negative Vorstellungen über die Vereinigten Staaten. Public Diplomacy ist ein kostengünstiges, aber sehr wirksames Mittel um amerikanische Grundsätze und Interessen im Ausland zu fördern.»[15] Mit der öffentlichen Diplomatie soll «Verständnis für die Vorstellungen und Ideale des eigenen Landes, der eigenen Kultur, aber auch dessen nationalen Zielen und aktuellen politischen Leitlinien»[16] geschaffen werden.

Die Informationsoperationen – *Information Operations* (Info Ops) – sind eine militärische Funktion, welche zur Beratung und Koordinierung militärischer Informationsaktivitäten und zur Unterstützung der militärischen Operationen in anderen Einsatzbereichen dient. Dabei soll die Entscheidungsfindung von (potentiellen) Gegnern beeinflusst, gestört, unterbrochen, korrumpiert oder usurpiert werden und gleichzeitig soll die eigene Informationstätigkeit geschützt werden.[17] Durch die Informationsoperationen soll ein entscheidender Vorteil im Informationsumfeld gegenüber dem Gegner erreicht werden.

Die psychologischen Operationen – *Psychological Operations* (Psy Ops) – sind Massnahmen und Tätigkeiten, welche das Verhalten und die Einstellungen des Gegners oder der Zivilbevölkerung im Einsatzgebiet im Rahmen der politischen oder militärischen Operationen beeinflussen sollen. Dazu haben in der Vergangenheit auch Propaganda und Gaslighting gehört. Bei den psychologischen Operationen werden bewusst gezielte Falschinformationen verbreitet, damit diese in die Beurteilung und Erwägungen des Gegners übernommen werden. Diese Operationen können beispielsweise durch den Betrieb von Radio- und Fernsehsendern, durch Flugblätter und neuerdings auch durch Websites-, E-Mail-, SMS- oder Social Media-Kampagnen durchgeführt werden. Sie sind langfristiger Natur.

Führung in der strategischen Kommunikation

Durch die Zunahme der Übertragungsgeschwindigkeit und Komplexität von Informationen aufgrund der Digitalisierung und Globalisierung stellt sich die Frage, welchen Beitrag die politischen und militärischen Führungskräfte in der Praxis leisten können. Innerhalb der militärischen Kommunikationsabteilungen arbeiten die Mitarbeiter zu einem grossen Teil selbständig an ihren Produkten und daher ist es enorm wichtig, dass diese Mitarbeiter ihren Beitrag im übergeordneten grossen Rahmen kennen. Um die übergeordneten Ziele und die Kommunikationsstrategie zu vermitteln, sind die Führungskräfte gefragt, denn ohne diese Sinngebung kann die StratCom kaum strategisch und die Ressourcen nicht effizient eingesetzt werden.

Abbildung 6 Psychologische Operation der US-Armee in Kirkuk, Irak. Soldaten der 350th Tactical Psychological Operations, 10th Mountain Division werfen am 6. März 2008 Flugblätter über einem Dorf in der Nähe von Jawijah in der Provinz Kirkuk im Irak ab. Die Broschüren sollten die Idee der Selbstverwaltung bei den Bewohnern der Region fördern.
(Wikimedia Commons 2019)

Ohne eine aktive und auf die Zielgruppen fokussierte Kommunikation findet auch keine StratCom statt.

Die militärischen Kommandeure und Entscheidungsträger sollten mit den Schlüsselpersonen der Zielgruppen in Kontakt stehen, um das Verhalten dieser im Sinne des gewünschten (militärischen) Endzieles zu beeinflussen und zu verändern. Diese Schlüsselpersonen können z. B. religiöse Führer, Gemeindeleiter, Clanvorsteher usw. sein. Zentral dabei ist – wie im Evaluationsmodell der strategischen Kommunikation aufgeführt – die Identifizierung und die bestehende Beziehung zu diesen wichtigen Akteuren, welche im entsprechenden Interessenraum für die Erfüllung der Mission entscheidend sind. Sobald die Zielgruppen identifiziert sind, sollten deren Mitglieder hinsichtlich ihrer Persönlichkeit, ihrem Verhalten, ihrer Motive und Ziele analysiert werden. Dies ist dann die Grundlage für die entsprechenden Informationsaktivitäten und die Ausarbeitung eines Plans zur Beeinflussung dieser Schlüsselpersonen unter Berücksichtigung der angestrebten eigenen Ziele, der Beziehung zu diesen Schlüsselpersonen und des situativen Kontextes.

Die Rolle einer militärischen Führungsperson beschränkt sich nicht nur auf die Beeinflussung des externen Umfelds, sondern sie ist auch für die Strategievermittlung, deren Steuerung durch die entsprechenden Ressourcen sowie

15 United States Advisory Commission on Public Diplomacy (2000), 5.
16 Tuch (1990).
17 Vgl. NATO Military Policy on Info Ops (2007); US Joint Chiefs of Staff (2014); NATO Standardization Agency (2014).

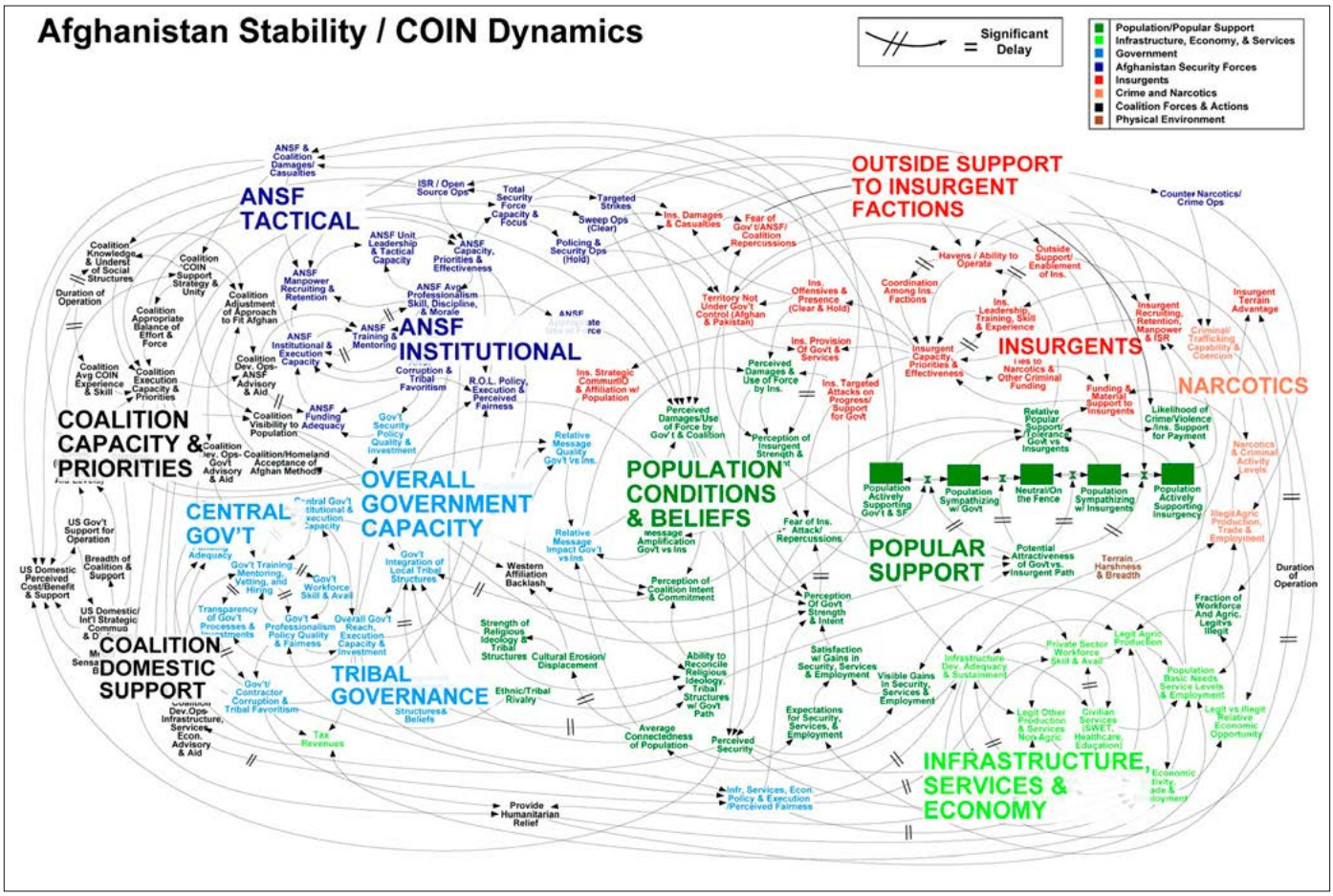


Abbildung 7 US Strategie in Afghanistan Komplexität der US-Strategie in Afghanistan mit den entsprechenden Zielgruppen. (New York Times 2010)

das Wiederholen der Kommunikationsziele und die Ausrichtung auf die Bezugsgruppen verantwortlich. Die direkte Kommunikation und die darin enthaltenen Werte und Prinzipien der Führungsperson bilden ein Grundgerüst für eine effektive StratCom. Dabei ist es wichtig, dass die Werte, welche dem Narrativ der StratCom zugrunde liegen, durch die Mitarbeiter und die Führungspersonen, welche in der StratCom beschäftigt sind, geteilt werden. Durch die Kommunikation der Strategie und die unterstützenden Fact-to-Face Aussagen stellen die Führungspersonen die entscheidende Position für die StratCom dar. Militärische Führungskräfte sind nicht nur formale Vorgesetzte, die die Ziele einer Informationsoperation vorgeben und die Ergebnisse verifizieren, sie stehen auch am Ursprung, der Fortsetzung und der Neu-Entwicklung der zu verbreitenden Botschaften. Durch die Führungskräfte erfahren die Mitarbeiter, wie die Strategie und ihre Botschaften aussehen, wie sie im Gesamtrahmen der Mission zu interpretieren und umzusetzen ist und in welchem Rahmen gehandelt werden soll, obwohl bereits vorher die Strategie den Mitarbeitern in grossen Teilen klar ist. Die militärischen Führer prägen durch ihr Auftreten und ihre Äusserungen einen grossen Teil der StratCom und die involvierten Funktionsbereiche wie zum Beispiel Public Diplomacy und Public Affairs. Erfahrungen und bewährte Verfahren sollten durch die Führungspersonen anhand der Botschaften und Narrative bei militärischen Operationen und Aktivitäten auf jeder militärischen Ebene – strategisch, operativ und taktisch – vermittelt werden. Durch die lessons learned entsteht eine positive Beziehung zwischen der Führungsperson und dem Mitarbeiter der StratCom, weil dadurch ein gemeinsames Verständnis der zu vermittelnden Kernbotschaften, ihrer Form und ihres Inhalts hergestellt werden kann. Durch die Führungskräfte werden die Grundsätze der Kommunikationsstrategie an die Mitarbeiter der Organisation kommuniziert. Ohne eine aktive und auf die Zielgruppen fokussierte Kommunikation findet auch keine StratCom statt.

Im nachfolgenden Abschnitt sollen die Erfahrungen hinsichtlich der StratCom im ISAF-Einsatz und die daraus gewonnenen Erkenntnisse erläutert werden, welche auch für andere Streitkräfte von Relevanz sind, welche strategisch kommunizieren wollen.

Strategische Kommunikation im ISAF Einsatz

Im Rahmen der Mission in Afghanistan gibt es die weit verbreite Annahme, die die NATO als Verliererin im Kommunikationskrieg gegen einen militärisch minderwertigen Gegner darstellten. Im Gegensatz zu den Taliban, die im Einsatzgebiet ihre Kommunikationsstrategien erfolgreich ausgeführt haben, war die Kommunikation der ISAF und der NATO aufgrund heterogener Ziele nicht erfolgreich. Aus dem Einsatz der StratCom in Afghanistan können folgende zentrale Erkenntnisse gezogen werden.

1. Der erforderliche Aufwand und die erforderlichen Kommunikationsressourcen für die Führung der ISAF-Kommunikations- und Informationskampagne auf strategischer Ebene wurde stark unterschätzt. Viele der operativen Risiken, Gefahren und Herausforderungen bei der Ausweitung der Mission waren bekannt, wurden aber nicht genügend antizipiert.
2. Die grösste Schwachstelle der Kommunikation innerhalb der Allianz auf strategischer, operativer und taktischer Ebene war der grundlegende Mangel an personellen Kapazitäten im militärischen Informationsbereich. Als Konsequenz sollten Streitkräfte, um im Bereich der strategischen Kommunikation leistungsstärker zu werden, nur qualifiziertes und geübtes Personal in den Fachgebieten der StratCom einstellen. Zudem sollten kurzfristig einsetzbare militärische Kräfte in allen strategischen Kommunikations-Disziplinen zur Verfügung stehen. Mit der Professionalisierung der Einsatzkräfte im Kommunikations- und Informationsbereich sollen bessere Ergebnisse sowohl auf nationaler als auch internationaler Ebene erzielt werden.
3. Die StratCom war nicht so erfolgreich, wie sie es hätte sein können, war aber bedeutend besser als ihr zugeschrieben wird. Die Politik und die Einsätze müssen besser koordiniert werden, um positive Ergebnisse zu erzielen. Bei der ISAF war die politische und militärische Befehlsstruktur grundsätzlich fehlerhaft, da die ISAF durch ihre Struktur unfähig war, eine einheitliche politisch-militärische Kampagne zu entwickeln und zu leiten. Die StratCom soll unter einem übergreifenden politischen Kommunikationsrahmen stattfinden, der dafür da ist, alle Kommunikationsaktivitäten zu führen. Dabei müssen die militärbezogenen Aspekte der Kommunikation in diesen Rahmen integriert werden. Dabei sollte die Bindung zwischen Operationen und Plänen auf der politischen und militärischen Ebene verstärkt werden. Dies würde zusätzliche Kapazitäten innerhalb der Abteilung für öffentliche Diplomatie erfordern, um eine effizientere Koordination zwischen der StratCom und den politisch-militärischen Aktivitäten zu ermöglichen.
4. Die starke Veränderung des Informations- und Operationsumfeldes in den letzten Jahren hat zu tiefgreifenden Konsequenzen bezüglich der Vorgehensweise der StratCom, vor allem im Bereich der militärischen Operationen geführt. Eine zusätzliche Möglichkeit wäre die Zusammenarbeit mit zivilen Partnern, um beispielsweise die Zielgruppen zu Hause besser zu informieren. Dies könnte beispielsweise in der Form einer Arbeitsgruppe geschehen, wobei erfahrene Fachleute aus den führenden Industrieunternehmen die militärischen Kommunikationsaktivitäten vergleichen und kritisch hinterfragen würden.
5. Ohne die politische und operative Ausführung zu berücksichtigen, können folgende Hauptgründe für die Komplikationen der ISAF-Kommunikation bestimmt werden:
   a. Neun verschiedene Zielgruppen mussten berücksichtigt werden: die NATO-Mitgliedstaaten, die NATO-Partnernationen (insbesondere diejenigen, die die ISAF mit beachtlichen Truppen unterstützen wie zum Beispiel Australien), die drei verschiedenen Gruppen im Einsatzgebiet (die afghanische Regierung, die Bevölkerung einschliesslich ihrer Führungskräfte sowie die Gegner), regionale Akteure (Russland, Pakistan, Indien und Irak), andere Anspruchsgruppen im Verteidigungs- und Sicherheitsbereich (sowie Think Tanks), internationale Organisationen (wie die UNO, die Weltbank und die Europäische Union), Nichtregierungsorganisationen und weitere Institutionen sowie die sich ständig verändernde Zielgruppe der ISAF.
   b. Fünf Disziplinen im Bereich der Kommunikation und Information waren im Spiel: die öffentliche Diplomatie, die militärischen und zivilen Public Affairs, die Psy Ops und Info Ops und die koordinierende StratCom.[18]
   c. Vier verschiedene, konkurrierende aber auch verwandte Kommunikationskampagnen wurden geführt: vom NATO-HQ zu den Nationen, vom NATO-HQ zum afghanischen Volk, von den NATO-Nationen zu deren eigenen Zielgruppen zu Hause sowie von den NATO-Nationen zu den Aufständischen.
6. Es muss klar sein, wer die Verantwortung und Führung des (strategischen) Kommunikationsbereiches innehat. Bei Operationen muss ein Mechanismus vorhanden sein, um sicherzustellen, dass die strategische Kommunikationsgruppe in den Zielkoordinierungsprozess integriert ist.
7. Eine klar definierte Doktrin kann als fundamentales Element für eine sichere Beurteilung im strategischen Bereich gesehen werden. Eine gemeinsame Doktrin aller Beteiligten, welche an immer grösseren und vielfältigeren Koalitionsoperationen teilnehmen, nimmt somit eine grosse Bedeutung ein.
8. Die rasante Entwicklung von Social Media und deren Auswirkungen müssen für die nationalen und internationalen Operationen besser in Betracht gezogen werden. Social Media-Kanäle bringen Risiken und Herausforderungen mit sich, sind aber auch eine Chance für die Streitkräfte. Die Leichtigkeit und die Geschwindigkeit, mit denen sich die Informationen dank diesen Kommunikationsmitteln verbreiten können, sollte insbesondere in den Bereichen der strategischen Kommunikation, der Public Affairs und der Informationsoperationen genutzt werden.

Abbildung 8 Abbildung 8: Eröffnung des NATO Strategic Communications Centre of Excellence. Die litauische Präsidentin Dalia Grybauskaite, der lettische Präsident Raimonds Vejonis und der US-Senator John McCain bei der Eröffnung des NATO Strategic Communications Centre of Excellence am 20. August 2015 in Riga, Lettland.
(Flickr 2019)

18 Ab der NATO StratCom Policy von 2009.

Weiterentwicklung der strategischen Kommunikation

Mit der Ukraine-Krise und der Annexion der Krim durch Russland hat das Konzept der StratCom an Aktualität gewonnen, weil sich der Westen und die NATO durch die russische Berichterstattung bedroht sahen. Daraus resultieren im Bereich der StratCom folgende zentrale Entwicklungen, welche Einfluss auf die Sicherheitspolitik haben:

1. Die NATO hat ihre Bemühungen um eine effektive politische und militärische Kommunikation sichtlich verstärkt, zunächst mit dem erklärten Ziel, russische Propaganda und Falschmeldungen mit Fakten zu widerlegen. Dies macht auch folgender Wortlaut am NATO-Gipfel in Wales deutlich: «Wir werden sicherstellen, dass die NATO in der Lage ist, die spezifischen Herausforderungen hybrider Kriegsführung effektiv anzugehen [...] Dies wird auch eine Steigerung der strategischen Kommunikation einschliessen.»[19]
   Im Jahre 2014 wurde das Strategic Communication Centre of Excellence[20] in Riga in Anwesenheit des inzwischen verstorbenen US-Senators John McCain errichtet, was der strategischen Kommunikation innerhalb der NATO noch zusätzliches Gewicht verschaffte. Der Hauptfokus des StratCom COE liegt auf der Analyse feindlicher Propaganda, vor allem jener von Daesh und von Russland, sowie auf der Erarbeitung eigener Konzepte und Empfehlungen für die Anwendung und Implementierung der StratCom innerhalb der NATO und ihrer Mitgliedstaaten.
2. Auf der EU-Ebene wurde im September 2014 eine Arbeitsgruppe für strategische Kommunikation[21] eingerichtet mit der Aufgabe, russische Falschmeldungen, Propaganda und subversive Informationsoperationen zu kontern und Desinformationskampagnen zu enttarnen. Die wahrgenommene Bedrohung durch die russische Berichterstattung ging schliesslich so weit, dass der Rat der Europäischen Union die Hohe Vertreterin der Europäischen Union für Aussen- und Sicherheitspolitik (entspricht der Funktion des «EU-Aussenministers») im Januar 2015 aufforderte, der russischen Propaganda durch den Ausbau der Kapazitäten im Bereich der StratCom entgegenzuwirken und mit der Errichtung eines Kommunikationsteams zu beginnen. Dieses Team sollte seine Aktivitäten in Länder der östlichen Nachbarschaft, insbesondere nach Armenien, Aserbaidschan, Georgien, die Republik Moldau, Russland, Weissrussland und in die Ukraine ausrichten, wozu es im Ratsbeschluss konkret heisst: «Solche Bemühungen sollten die proaktive Kommunikation von EU-Politiken beinhalten, möglicherweise auftauchende Fehlinformationen korrigieren und die weitere Entwicklung unabhängiger Medien in der ganzen Region unterstützen.»[22]
   Das Eastern Strategic Communications Team[23] ist Teil des Referats für strategische Kommunikation des Europäischen Auswärtigen Dienstes.[24] Mit der EU East Stratcom Task Force sollen folgende Ziele verfolgt werden: «Die drei Ziele [...] sind wirksame Kommunikation und Werben für EU-Politiken und -Werte in der östlichen Nachbarschaft, Stärkung des Medienumfelds insgesamt inklusive Unterstützung für unabhängige Medien und verbessertes öffentliches Bewusstsein von Desinformationsaktivitäten seitens Dritter und verbesserte EU-Reaktionsfähigkeit darauf.»[25]
   Das EU East StratCom Team soll «positive Narrative und Kommunikationsprodukte in russischer Sprache entwickeln und damit ‹russischen Erzählweisen› in Osteuropa die Sicht der EU entgegenstellen».[26] Dieses strategische Kommunikationsteam Ost soll z. B. im Internet aktiv werden und auf Russisch, über Websites und soziale Netzwerke proaktiv über Politik und Werte der EU informieren. Es soll russische Medien auswerten, «offensichtliche Lügen identifizieren»[27] und kommentierte Berichte dazu an die Mitgliedstaaten der EU herausgeben. Die StratCom der EU hat das Ziel, neben der eigenen Bevölkerung auch die EU Nachbarstaaten mittels Pressemitteilungen, Reden, Artikel oder sozialer Medien zu informieren und dort ein positives Bild der EU zu etablieren und konträren Narrativen zu widersprechen. Dafür greift die EU East StratCom auf ein Netzwerk von mehr als 500 Journalisten zurück, die Hinweise auf Falschmeldungen in russischen Medien geben sollen. Der Auftrag der Russland Taskforce ist es aber auch, «unabhängige Medien in Russland zu unterstützen wie z. B. den Europäischen Demokratiefonds oder den Open Neighbourhood Communication Programm.»[28]
   Die Rede ist von proaktiven strategischen Kommunikationskampagnen und «myth-busting». Unter Umständen wird mit «ad-hoc communication» auch auf Meldungen russischsprachiger Medien reagiert, wenn dies aus Sicht der EU tagesaktuell von Nöten ist. Die Aktivitäten umfassen vor allem Kommunikation über das Internet. Es soll über Websites und soziale Netzwerke proaktiv über Politik und Werte der EU auf Russisch informiert werden. Russische Medien werden dabei ausgewertet, um offensichtliche Lügen zu identifizieren und kommentierte Berichte dazu an die Mitgliedstaaten der EU herauszugeben.

Das EU East StratCom Team soll «positive Narrative und Kommunikationsprodukte in russischer Sprache entwickeln und damit ‹russischen Erzählweisen› in Osteuropa die Sicht der EU entgegenstellen».

3. Ein weiterer Schritt in der Weiterentwicklung des StratCom-Konzeptes ist die Implementation in den Streitkräften wie zum Beispiel in den britischen Streitkräften mit der Joint Doctrine Note 1/12[29]. Neben einer Beschrei-

19 NATO (2014B).
20 NATO Strategic Communications Centre of Excellence (2019).
21 Europäische Rat der Europäischen Union (2015).
22 Europäische Rat der Europäischen Union (2015).
23 EU StratCom Task Force (2019).
24 EU Europäischer Auswärtiger Dienst (2019).
25 Deutscher Bundestag (2015), 3.
26 EU StratCom Task Force (2019).
27 EU StratCom Task Force (2019).
28 Das Open Neighbourhood Communication Programm ist ein Kommunikationsprogramm der EU, dass im europäischen Nachbarschaftsraum für die Politik der EU in der entsprechenden Region wirbt und zusätzlich Training für Journalisten anbietet.
29 Das Open Neighbourhood Communication Programm ist ein Kommunikationsprogramm der EU, dass im europäischen Nachbarschaftsraum für die Politik der EU in der entsprechenden Region wirbt und zusätzlich Training für Journalisten anbietet.

bung der Grundlagen der strategischen Kommunikation geht das Konzept detailliert auf das momentane Kommunikationsumfeld ein. Das Konzept erarbeitet eine Lösung, welche auf den Lehren aus der Kommunikationsarbeit der britischen Armee in den Auslandseinsätzen vor allem im Irak und in Afghanistan beruht. Die wichtigsten Lösungsansätze umfassen erstens die Ausarbeitung einer zentralen, übergeordneten Botschaft, welche zweitens als Vorlage für die militärische Strategie und Ausarbeitung der Medienkampagnen dient und drittens auf die spezifischen Zielgruppen ausgerichtet werden soll, um maximale Kommunikationseffekte zu erzielen.[30]

Die militärische StratCom ist integriert in eine gesamtstaatliche Kommunikation, welche nicht nur innerhalb von Grossbritannien und deren nationalen Kommunikationskampagnen wirkt, sondern auch die behördenübergreifende Zusammenarbeit beispielsweise in Notfall- und Kriseneinsätzen festlegt. Der integrierte Kommunikationsansatz bezieht sich darauf, dass Regierungsmitarbeiter aus verschiedenen Institutionen und Departementen auf mehreren Ebenen zusammenarbeiten, um gemeinsam die Ziele zu erreichen. Durch den integrierten Ansatz verfügt beispielsweise das Verteidigungsdepartement über kein Informationsmonopol, wenn es um die Beantwortung von Fragen und Herausforderungen in den Konflikt- und Kriegsgebieten geht. Mit Hilfe dieses Ansatzes wird versucht, das breite Spektrum an Wissen, Fähigkeiten und Ressourcen innerhalb der Departemente optimal zu nutzen und Synergien zu schaffen durch einen multidisziplinären, abteilungsübergreifenden Ansatz bei der Planung, Durchführung, Bewertung und Evaluation der StratCom. Durch die Bündelung der Kommunikation sollen einerseits die vorhandenen Ressourcen effektiv genutzt und andererseits die Wirkung der Kommunikation verbessert werden.[31]

Schlussfolgerungen

Innerhalb der ISAF-Mission hat die Einführung der strategischen Kommunikation vielen Einsatzkräften einen massgeblichen Gewinn an Erfahrung im Umgang mit einer neuen Organisationsfunktion ermöglicht sowie ihre Kenntnisse auf strategischer Ebene verbessert. Der Readiness Action Plan[32] bietet dabei umfassende Massnahmen, um auf die Veränderungen im Sicherheitsumfeld erfolgreich zu reagieren. Nicht nur die Schnelligkeit eines Einsatzes, sondern auch dessen internationale Wahrnehmung wird massgeblich zu seinem Erfolg beisteuern. In der heutigen Infosphäre werden die Informations-, Beeinflussungs- und Überzeugungsfunktionen als gleichermassen wichtig empfunden wie die militärischen Missionen.

Nicht nur die Schnelligkeit eines Einsatzes, sondern auch dessen internationale Wahrnehmung wird massgeblich zu seinem Erfolg beisteuern.

Die jüngsten Ereignisse haben auch gezeigt, welche Effekte ein Land erzielen kann, dessen Führungskräfte viele Medien, Kommunikations- und Informationsmittel kontrollieren und auch den Willen haben, diese Fähigkeiten wirkungsvoll zu nutzen. Die russische Kommunikationskampagne[33] auf der Krim und in der Ostukraine bewirkte die Einschüchterung der Bevölkerung, ohne dass die internationalen Streitkräfte eingreifen konnten. Der Ukraine-Konflikt zeigt die Konsequenzen der Nutzung der neuen medialen Möglichkeiten, wenn sie als militärische Strategie eingesetzt werden. Durch die Gerasimov-Doktrin konnten Russland seine Zielgruppen beeinflussen und manipulieren.[34,35]

Die StratCom nimmt bei der Vernetzung der beteiligten sicherheitsrelevanten Akteure und der Abstimmung der zum Teil divergierenden Ziele eine zentrale Rolle ein und stellt zweifelsohne eine grosse Herausforderung dar.

Einige Berichte[36] über die Verteidigungs- und Sicherheitsfragen der Zukunft zeigen, dass Massnahmen jetzt schon ergriffen werden müssen, um genügend vorbereitet zu sein, falls es zu weiteren Krisen kommen sollte. Verteidigungs- und sicherheitsrelevante Themen und Operationen sind komplexer, da es immer mehr Akteure gibt, die berücksichtigt werden müssen. Gemeinsames Merkmal dieses veränderten sicherheitspolitischen Umfeldes ist die Vernetzung der sicherheitspolitischen Akteure auf der staatlichen Ebene (militärische und polizeiliche Sicherheitskräfte, Akteure der Politik, Diplomatie, Entwicklungszusammenarbeit) und der nicht-staatlichen Ebene (Hilfsorganisationen, NGOs, zivilgesellschaftliche Friedenskräfte). Durch die vereinfachte Mediatisierung und Übertragung von Informationen können immer mehr Leute erreicht werden. Die Bevölkerung rezipiert nicht nur die Medieninhalte, sondern kann auch kommentieren und öffentlich am Mediendiskurs teilnehmen. Die StratCom nimmt bei der Vernetzung der beteiligten sicherheitsrelevanten Akteure und der Abstimmung der zum Teil divergierenden Ziele eine zentrale Rolle ein und stellt zweifelsohne eine grosse Herausforderung dar. Die einzelnen Kommunikationsfunktionen wie zum Beispiel Public Relations und interne Kommunikation sollen in ein Kommunikationskonzept integriert werden und setzen eine stringente Kommunikationsstrategie und klar formulierte Kommunikationsziele voraus. Wenn in einer Organisation mehrere Narrative und Ziele vorhanden sind, ist die Wahrneh-

30 Vgl dazu weiter U.K. Government Communication Service (2019A, 2019B) und U.K. Government Digital Service (2019).
31 U.K. Ministry of Defense (2011).
32 Vgl dazu weiter U.K. Government Communication Service (2019A, 2019B) und U.K. Government Digital Service (2019).
33 Wake (2010).
34 NATO (2017).
35 Gerasimov (2013).
36 Chekinov et al. (2013), 18.

Abbildung 9 Chemiewaffenangriff am 7. April 2018 in Douma, Syrien. RT (früher Russia Today) berichtete über den Chemiewaffeneinsatz folgendes: «Der syrische Einsatz chemischer Waffen (Chlorgas) ist fingiert. Mögliche nackte und nasse Kinder zittern aufgrund der Kälte. Einige der Kinder sind vielleicht bewusstlos, vielleicht schlafen sie auch nur. Es ist gut, dass die Fotos der Opfer bloss inszeniert und keine Menschen für dieses Bildmaterial umgekommen sind. Die NGO Swedish Doctors beschuldigen die Weisshelme, Kinder für ein realistisches Foto umgebracht zu haben» und berief sich dabei auch auf Quellen aus dem russischen Verteidigungsministerium und dem russischen Aussenministerium und wollten damit von der Salisbury-Attacke ablenken.
(Flickr [2019])

Abbildung 10 Abbildung 10: Propagandaveranstaltung zur Annexion der Krim. Grossveranstaltung zur Einverleibung der Krim in die russische Föderation mit Präsident Vladimir Putin.
(Wikimedia Commons (2019), Verweis auf http://kremlin.ru/)

mung dieser Organisation heterogen und widersprüchlich. Es ist nicht klar, wofür diese Organisation steht und sie verliert bei den Stakeholdern an Vertrauen. Die Ziele der Organisation, was sie tun will und was nicht, müssen sich in der (strategischen) Kommunikation widerspiegeln, so dass durch den integrierten Kommunikationsansatz ein inhaltlich, formal und zeitlich zusammenhängendes Bild von der Organisation nach innen und nach aussen entsteht. Infolge dessen ist es für die Streitkräfte wichtig, dass mittels des integrierten Kommunikationsansatzes die departements- und multinational-übergreifende Kommunikation stattfindet.[37]

Die bisherigen Ausführungen zeigen, dass die StratCom viele Facetten aufweist und ein vielschichtiges Konzept ist, bei dem jedoch die beabsichtige Wahrnehmung der Kommunikationsinhalte durch die Empfänger auch mittels einer durchdachten Strategie nicht garantiert werden kann. Die Empfänger interpretieren nämlich die Kommunikation nach ihrem eigenen Deutungshintergrund. Somit ist die Botschaft, welche durch die (strategische) Kommunikation vermittelt wurde, nicht unbedingt jene, die beim Empfänger ankommt und welche der Absender übermitteln wollte. Ob die Kommunikation des Absenders die gewünschte und beabsichtigte Wirkung beim Empfänger hat, hängt weniger von der Botschaft selbst oder den Kommunikatoren, sondern vielmehr von kulturellen und gesellschaftlichen Aspekten ab, die beeinflussen, wie der Empfänger die Botschaft interpretiert. Dies verdeutlicht beispielsweise die sehr kontrovers geführte Diskussion über die 90 000 zumeist geheimen amerikanischen Dokumente über den Afghanistan-Krieg, welche Bradley Manning der Organisation Wikileaks[38] zur Publikation im Internet übergab. Ein weiteres Beispiel, dass auch strategische Kommunikation nicht die komplette Kontrolle über die Weiterverbreitung von Informationen hat, ist die Veröffentlichung der Handyfotos von Angehörigen der Bundeswehr, welche mit Totenschädeln posiert haben, sowie deren anschliessende Verbreitung in den sozialen Medien.[39] Die Möglichkeiten, Informationen weiter zu verbreiten, haben mit der Diversifizierung der Medien mittels Facebook, Twitter etc. massiv zugenommen. Damit einher geht auch, dass die Zahl jener zugenommen hat, die Informationen weiterverbreiten und Mitteilungen produzieren können und dies unabhängig davon, ob sie Zugang zu den offiziellen Informationsquellen haben oder nicht.

Die Streitkräfte versuchen deshalb ihre Aktivitäten, Handlungen und die Kommunikation aufeinander abzustimmen. Die Erfahrung mit StratCom hat gezeigt, dass nicht zwischen der Handlung und der Kommunikation unterschieden werden kann, zumal am Schluss alles eine Form der Kommunikation ist. Gerade die Kommunikation in Konflikt- und Kriegsgebieten ist zu einem strategischen Faktor für den Erfolg des Einsatzes geworden.

Die Wahrnehmung der Botschaften und die Ansprüche der betroffenen Zielgruppen beim Kommunizieren und Handeln sollen entsprechend berücksichtigt werden, weil gerade in demokratischen Gesellschaften, in denen Meinungspluralität herrscht, die politische und gesellschaftliche Legitimation der Streitkräfte von grosser Bedeutung ist.

37 Vgl. Gerasimov (2013), Joint chiefs of staff (2014).
38 Wikileaks (2010).
39 Spiegel Online (2010), Zeit Online (2010).

Wie die NATO Policy zur StratCom bekräftigt, soll StratCom in den ganzen militärischen Planungs- und Entscheidungsprozess auf der strategischen, operativen und taktischen Ebene integriert werden mit dem langfristigen Ziel, Vertrauen, Verständnis, Unterstützung und Transparenz bei den relevanten Zielgruppen herzustellen. Dies kann zum Beispiel nicht durch Informationsoperationen oder psychologische Kriegsführung erreicht werden. Durch die StratCom sollen die Worte und Taten der Streitkräfte verbunden und aufeinander abgestimmt werden, damit die Legitimität der zivil-politischen und der militärischen Ziele bei allen Zielgruppen erhöht werden kann. Die Wahrnehmung der Botschaften und die Ansprüche der betroffenen Zielgruppen beim Kommunizieren und Handeln sollen entsprechend berücksichtigt werden, weil gerade in demokratischen Gesellschaften, in denen Meinungspluralität herrscht, die politische und gesellschaftliche Legitimation der Streitkräfte von grosser Bedeutung ist. Zudem ist es wichtig, dass die Redefreiheit, die freie Meinungsäusserung, der nicht eingeschränkte Zugang zu Informationen sowie der Pluralismus der Medien einen Grundstein für eine demokratische Gesellschaft bilden und daher Schutzmassnahmen gegen Desinformationskampagnen und feindliche Propaganda bereitgestellt werden. Durch StratCom soll Desinformation und Propaganda widerlegt und verhindert werden, so dass die auf Regeln beruhenden Grundlagen und Grundsätze der westlichen Demokratien sowie deren Souveränität nicht untergraben, ausser Kraft gesetzt, Abstimmungen und Wahlen[40] beeinflusst oder «Deepfakes» und extremistische Bewegungen unterstützt werden.

Sowohl in Kriegs- als auch in Friedenszeiten bedürfen die Einsätze der Streitkräfte permanenter Informations- und Kommunikationsarbeit, um die Aufgaben und Handlungen gegenüber der Öffentlichkeit kontinuierlich in einem Dialog zu begründen und zu rechtfertigen. Die Streitkräfte haben nicht nur eine Verantwortung gegenüber der nationalen Öffentlichkeit, den zivilen und militärischen Angehörigen der Streitkräfte, ihre Ziele, Zwecke und Mittel zu rechtfertigen, sondern auch gegenüber allfälligen Partnern in multinationalen Operationen und der Bevölkerung in den Konflikt- und Kriegsgebieten. Anhand des strategischen Narrativs durch die StratCom soll die Kommunikation der politischen Ebene mit den kommunikativen Handlungen der Streitkräfte im Einsatz sinnvoll verknüpft werden. Die sicherheits- und verteidigungspolitische Kommunikation darf dabei nicht nur den Interessen und Profilierungsabsichten der Politikerinnen und Politikern überlassen werden, sondern ist auch eine Aufgabe der Angehörigen der Streitkräfte. Durch die Kommunikation der militärischen Führungskräfte mit der Öffentlichkeit und den politischen Akteuren über Aufgaben, Sinn und Zweck von militärischen Organisationen und deren Handlungen können diese die benötigte Legitimität herstellen.

40 New York Times (2018), Reuters (2018).

Literatur

- Aussenministerium der Russischen Föderation (2018). К ситуации в Сирии, 8. April. Online unter: http://www.mid.ru/ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3155552
- Bergsdorf, W. (2002). Imperativ Politik. In: Schatz, H., Rössler, P. & Nieland J.-U. (Hrsg). Politische Akteure in der Mediendemokratie. Politiker in den Fesseln der Medien? Wiesbaden: Springer VS.
- Chekinov, S. G., Bogdavov, S. A. (2013). The nature and content of a new-generation war. In: Military thought. A Russian journal of military theory and strategy, 160 (4), 18. Online unter: http://www.eastviewpress.com/Files/MT_FROM%20THE%20CURRENT%20ISSUE_No4_2013.pdf
- Deutscher Bundestag (2015). Einrichtung einer Arbeitsgruppe der Europäischen Union «Russland Taskforce» für die «Strategische Kommunikation» in Osteuropa, 18/6486. Online unter. https://andrej-hunko.de/start/download/dokumente/689-einrichtung-einer-arbeitsgruppe-der-europaeischen-union-russland-taskforce-fuer-die-strategische-kommunikation-in-osteuropa/file
- Europäische Rat der Europäischen Union (2015). Schlussfolgerungen des Europäischen Rates vom 19./20. März 2015, Online unter: https://www.consilium.europa.eu/media/21870/st00011de15.pdf
- EU Europäischer Auswärtiger Dienst (2019). Online unter: https://europa.eu/european-union/about-eu/institutions-bodies/eeas_de
- EU StratCom Task Force (2019). Desinformation review. Online unter: https://euvsdisinfo.eu/
- Gelpi, C., Feaver, P. D., & Reifler, J. (2009). Paying the human costs of war. American public opinion and casualties in military conflicts. Princeton: Princeton University Press.
- Gerasimov, V. (2013). The value of science in prediction. In: Military Industrial Kurier. Online unter: http://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimo-doctrine-and-russian-non-linear-war
- Gerasimov, V. (2013). «НОВЫЕ ВЫЗОВЫ ТРЕБУЮТ ПЕРЕОСМЫСЛЕНИЯ ФОРМ И СПОСОБОВ ВЕДЕНИЯ БОЕВЫХ ДЕЙСТВИЙ», Военно-Промышленный Курьер, 8. Online unter: https://sslvpn.ethz.ch/+CSCO+0075676763663A2F-2F6A6A6A2E6963782D61726A662E6568++/articles/14632
- Joint chiefs of Staff (2014). Information operations. Joint publication 3-13, 20.11.2014, Online unter: http://dtic.mil/doctrine/new_pubs/jp3_13.pdf
- NATO (2009A). NATO strategic communications policy. NATO international staff, 14. September. Online unter: https://publicintelligence.net/nato-stratcom-policy/
- NATO (2009B). AD 95-2, ACO Strategic communications. Supreme headquarters allied powers Europe, 19. November. Online unter: http://stratcomhellas.weebly.com/uploads/5/1/6/5/51658901/aco_95_3[1].pdf
- NATO (2010). Military concept for strategic communications. Allied command transformation, 27. July. Online unter: https://publicintelligence.net/nato-stratcom-concept/
- NATO (2011). MC 0457/2, NATO military public affairs policy. Online unter: https://www.nato.int/ims/docu/mil-pol-pub-affairs-en.pdf

- NATO (2014A). Committee on public diplomacy (CPD). Online unter: https://www.nato.int/cps/en/natohq/topics_69272.htm
- NATO (2014B). Wales summit declaration. Online unter: https://www.nato.int/cps/en/natohq/official_texts_112964.htm
- NATO (2017). Readiness action plan. Online unter: https://www.nato.int/cps/en/natohq/topics_119353.htm?selectedLocale=en
- NATO Allied command operations & allied command transformation (2014). Public affairs handbook. Oktober 2014. Online unter: https://shape.nato.int/page1494950/public-affairs-handbook
- NATO Standardization agency (2007A). MC 422-34, NATO military policy on information operations. Online unter: https://publicintelligence.net/nato-io-policy/
- NATO Standardization agency (2007B). AJP 3.10.1(A), Allied joint doctrine for psychological operations. Online unter: https://info.publicintelligence.net/NATO-PSYOPS.pdf
- NATO Standardization agency (2009). AJP-3.10, Allied joint doctrine for information operations. Online unter: https://info.publicintelligence.net/NATO-IO.pdf
- NATO Strategic Communications Centre of Excellence (2016). We have met the enemy and he is us. Online unter: https://www.stratcomcoe.org/we-have-met-enemy-and-he-us-analysis-nato-strategic-communications-international-security-assistance
- NATO Strategic Communications Centre of Excellence (2019). Online unter: https://www.stratcomcoe.org/ und NATO StratCom COE Twitter: https://twitter.com/stratcomcoe
- New York Times (2010). We have met the enemy and he is powerpoint, 26. April. Online unter: https://www.nytimes.com/2010/04/27/world/27powerpoint.html
- New York Times (2018). Justice dept. Accuses russians of interfering in midterm elections. Online unter. https://www.nytimes.com/2018/10/19/us/politics/russia-interference-midterm-elections.html
- NTV (2018). Небензя: «химатака в Сирии» сфабрикована для отвлечения внимания от дела Скрипалей, 10. April. Online unter: https://www.ntv.ru/novosti/2002502/?sn
- QDR Execution roadmap for strategic communication (2006). U.S. Department of State, Washington DC. Online unter: http://www.dtic.mil/dtic/tr/fulltext/u2/a495367.pdf
- Spiegel Online (2006). Skandal-Fotos aus Afghanistan. Bundeswehr trennt sich von zwei Totenschändern. Online unter: https://www.spiegel.de/politik/ausland/skandal-fotos-aus-afghanistan-bundeswehr-trennt-sich-von-zwei-totenschaendern-a-445032.html
- Reuters (2018). Russian twitter accounts tried to help opposition in UK election: report. Online unter: https://www.reuters.com/article/us-britain-election-russia/russian-twitter-accounts-tried-to-help-opposition-in-uk-election-report-idUSKBN1I00BB
- RT (2018). No trace of chemical weapons at alleged attack site in Douma – Russian military, 9. April. Online unter: https://www.rt.com/news/423627-russian-military-checks-chemical-douma/
- Tuch, Hans N. (1990). Communicating with the world. US public diplomacy overseas. St. Martin's Press: New York.
- U.K. Government Communication Service (2019A). Strategic communication. Online unter: https://gcs.civilservice.gov.uk/guidance/strategic-communication/
- U.K. Government Communication Service (2019B). Government communication plan 2018/2019. Building a country that works for everyone: A Britain fit for the future. Online unter: https://gcs.civilservice.gov.uk/wp-content/uploads/2018/04/Government-Communication-Plan-2018-19.pdf
- U.K. Government Digital Service (2019). GDS communications strategy: 2018 to 2019. Online unter: https://www.gov.uk/government/publications/gds-communications-strategy-2018-to-2019/gds-communications-strategy-2018-to-2019
- U.K. Ministry of Defence (2011). Joint doctrine note 1/12, strategic communication: The defence contribution. Online unter: https://www.gov.uk/government/publications/joint-doctrine-note-1-12-strategic-communication-the-defence-contribution
- U.S. Department of Defense (2004). Report of defense science board task force on strategic communication, Washington DC. Online unter: https://fas.org/irp/agency/dod/dsb/commun.pdf
- U.S. Advisory Commission on Public Diplomacy (2000). Consolidation of USIA into the state department: An assessment after one year. Diane Publishing: Washington, DC.
- U.S. Joint Chiefs of Staff (2014). JP3-13, Information operations, 20. November. Online unter: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf
- Wake, C (2010). The integrated approach is essential: Lessons identified at the strategic level. London: Stabilisation unit: Online unter. http://www.sclr.stabilisationunit.gov.uk/top-ten-reads/comprehensive-integrated-approach
- Wikileaks (2010). Wardiaries. Online unter: https://wardiaries.wikileaks.org/
- Zeit Online (2006). Deutsche Soldaten mit Totenkopf. Die schockierenden Fotos aus Afghanistan: Was sind die Folgen? Ein Kommentar. Online unter: https://www.zeit.de/online/2006/44/afghanistan-bundeswehr-totenschaedel

Michael Holenweger

Dr. phil., Projektleiter Forschungsprojekt «Führung in Extremsituationen», Dozentur Führung und Kommunikation, Militärakademie an der ETH Zürich.

E-Mail: michael.holenweger@milak.ethz.ch

Energiesicherheit von Streitkräften – eine zentrale Verteidigungsfähigkeit!

Von Beeinträchtigungen der Energieversorgung sind zivile Sektoren und Streitkräfte aufgrund ihrer Vernetzung und gegenseitigen Abhängigkeiten gleichermassen betroffen, was für praktisch alle Nationen der Erde gilt. So beeinflussen Faktoren von aussen die Energiesicherheit, z. B. indem diese als Machtmittel verwendet wird. Andererseits wirken Faktoren von innen, z. B. indem Wirtschafts- und Bevölkerungswachstum die Kapazitäten der Versorgungssysteme überfordern. Weiter kämpft man grenzüberschreitend mit den Wirkungen des Klimawandels, welcher neue Einwirkungen schafft oder bestehende verstärkt: die in den letzten Jahren beobachtete Häufung extremer Wetterlagen reduziert neben der landwirtschaftlichen- auch die Energieproduktion und damit die Versorgungssicherheit einer europaweit wachsenden Bevölkerung. Dies bedroht ganz konkret die Resilienzpotentiale von Staatswesen. Deshalb haben multilaterale Organisationen wie die NATO oder die European Defence Agency (EDA) begonnen, Programme zu initiieren, welche Klima- und Energiesicherheitsaspekte in ihre Verteidigungsüberlegungen einbeziehen. Ein zentrales Element dieser Überlegungen ist, dass Streitkräfte Energie- und Klimaherausforderungen nur mittels Kooperation und Koordination mit dem zivilen Sektor lösen können.

Daniel Krauer, Martin Krummenacher

Primärziel Energieversorgung

Hybride Bedrohungen treten oft als vielschichtiges Phänomen auf, so, wie es sich damals auch in der Ukraine manifestierte. Matthias Kuster[1] beschrieb eindrücklich, wie durch eine Vielzahl einzelner, zeitlich und örtlich versetzter, verschiedenartig geführter Angriffe Krisensituationen herbeigeführt wurden. Entweder wurden Unruhen und Verunsicherung im Inneren provoziert oder Akteure heizten die politische Situation an oder mittels Hackerangriffen und Sabotageakten wurden wichtige Bereiche des täglichen Lebens massiv beeinträchtigt, z. B. Mobilität und Energieversorgung (Erdgas und Elektrizität). Derartige Angriffe auf die Energieversorgung wirkten aufgrund des gewählten Zeitpunktes und gemeinsam mit gezielter Desinformation besonders demoralisierend.

Äussere Einflussfaktoren – Energie als Machtmittel[2]

Schon vor den 90er Jahren und in der beginnenden postsowjetischen Zeit etablierte Moskau Gaslieferstopps als Druckmittel, um politische Ziele zu erreichen. Später, in den Wintern von 2006 und 2009, stellte Russland die Lieferungen an die Ukraine wegen der Spannungen zwischen Gazprom und Kiew über die Gaspreise ein. Der Streit stoppte auch die russischen Gaslieferungen an die EU, da die Pipelines durch ukrainisches Gebiet führten. Die Gaskrise 2009 dauerte 2 Wochen und betraf auch Gaslieferungen in die EU-Mitgliedstaaten Tschechien, Slowakei, Polen, Rumänien, Österreich und Kroatien. Alleine in Polen erfroren damals 10 Menschen, die Temperaturen betrugen Minus 20 Grad Celsius.

Nach der Annexion der Krim und der anhaltenden Aggression in der Ostukraine erhöhte Russland den Preis für das an die Ukraine verkaufte Gas erheblich. Als sich Kiew im Juni 2014 weigerte, für Gas den überhöhten Preis für meh-

1 Matthias Kuster (2015): Die Ukraine-Krise 2014/2015 aus militärstrategischer und operativer Sicht. *Military Power Revue, 2/2015.*

2 Die Darstellungen zur Krise in der Ukraine in diesem Abschnitt wurden zu grossen Teilen dem Bericht «Assessing Energy Dependency in the Age of Hybrid Threats» (January 2019) des European ‹Centre of Exellence for Countering Hybrid Threats' entnommen. Vgl. https://www.hybridcoe.fi/publications/assessing-energy-dependency-in-the-age-of-hybrid-threats/. Zusammenhänge zur Situation in anderen Regionen sowie daraus resultierende Schlussfolgerungen stammen entweder von den beiden Autoren oder den zitierten Quellen.

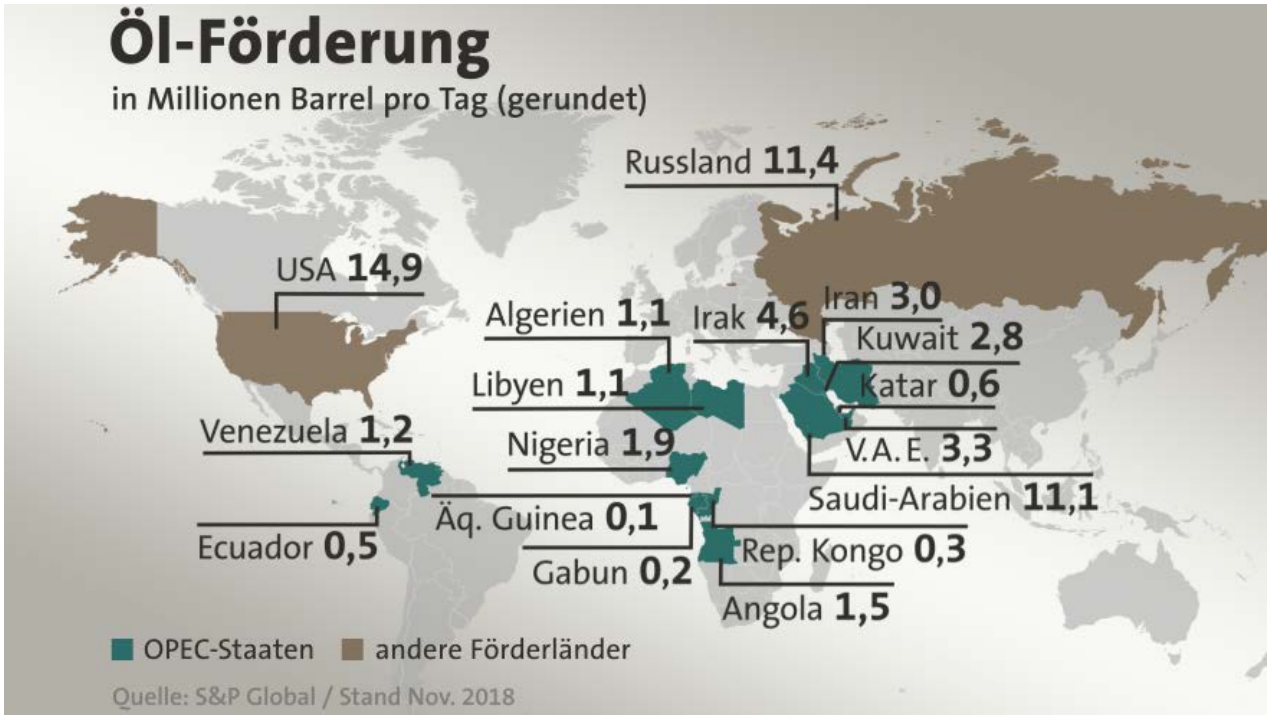


Abbildung 1 Weltweite Ölvorkommen und -Förderung.

rere Monate zu bezahlen, unterbrach Russland die Zufuhr. In der Folge erhielt die Ukraine russisches Gas indirekt von den europäischen Nachbarn und nicht mehr direkt von Russland. Gleichzeitig mit den als Druckmitteln eingesetzten Erdgaslieferstopps haben Russland und sein nationales Kernenergieunternehmen Rosatom um die Vorherrschaft in der Kernenergie gekämpft. Ende 2014, als der Konflikt zwischen Kiew und Moskau eskalierte, beschloss die Ukraine, Kernbrennstoff vom US-amerikanischen Nukleartechnikkonzern und Weltmarktführer Westinghouse zu kaufen. Damit wurde die an eine Monopolstellung anmutende Position des traditionellen russischen Lieferanten Rosatom massiv geschwächt. Da Kernenergie bis heute 60 Prozent der ukrainischen Stromproduktion ausmacht, sind Kernbrennstofflieferungen gleichermassen von strategischer, politischer und wirtschaftlicher Bedeutung.

Die Ankündigung von Brennstofflieferungen für ukrainische Kernkraftwerke durch Westinghouse führte zu vielen kritischen Kommentaren russischer Experten und zu «fake news» in der Richtung, dass ein «zweites Tschernobyl» entstehen könnte. Solche Berichte Russlands, die auf Fehlfunktionen in den Kernkraftwerken hindeuteten, waren bei einer durch die Tschernobyl-Katastrophe traumatisierten Bevölkerung durchaus dazu geeignet, Ängste und Verunsicherung auszulösen. In der vom Kreml gestarteten Propaganda- und Desinformationskampagne erklärte das russische Aussenministerium, dass die Ukraine die Sicherheit in Europa gefährde, indem sie einen US-amerikanischen Lieferanten für sowjetische Kernkraftwerke einsetze: «Die Folgen möglicher Strompannen oder gar Unfälle liegen in der vollen Verantwortung der ukrainischen Behörden und bei den US-Lieferanten des Kernbrennstoffs.» Die Erklärung bezog sich auf die schlimmste nukleare Katastrophe der Welt, die Tschernobyl-Katastrophe von 1986, in der damals noch sowjetischen Ukraine: «Es scheint, dass die Tragödie von Tschernobyl den Kiewer Behörden keine Lektionen erteilt hat.» In dieser panikverursachenden Erklärung des russischen Aussenministeriums wurde verschwiegen, dass Westinghouse seit 2003 auf dem ukrainischen Markt tätig ist und ein Kernkraftwerk in der Südukraine betreibt. Der Kreml versuchte damit, in der ukrainischen Öffentlichkeit Angst zu schüren, da diese nach wie vor unter den Folgen von Tschernobyl litt. In Webblogs erschienen ab dem 12. Januar 2015 Slogans wie dieser: «Oh nein! Kiew plant, (nukleare) quadratische Pflöcke in runde Löcher zu stossen». Bis 2018 lieferte Westinghouse Kernbrennstoff für 7 der 15 nuklearen Kraftwerke der Ukraine, während Rosatom den Rest lieferte.

Europa könnte im Winter keine 30 Tage ohne russisches Gas durchstehen, während Russland sicherlich ein Jahr (wenn nicht sogar Jahre) ohne europäische Gaskäufe, Investitionen und Technologien überstehen dürfte.

Eine grosse Anzahl von EU- und NATO-Ländern ist noch heute auf russische Kernenergie oder Kernbrennstoff angewiesen[3]. Moskau könnte diese Abhängigkeit zukünftig als Zwangsmittel nutzen, um damit eine langfristige strategische Abhängigkeit zu schaffen. Auch die Gaslieferstopps von damals zeigen die heutigen Risiken für die Versorgung Europas, welche auch in Zukunft aufgrund der Abhängigkeit von russischem Gas weiterbestehen werden. Diese Problematik wird sich mit dem Bau der von Gazprom

3 Die Schweiz bezieht das Uran zum Betrieb ihrer Kernkraftwerke auf dem Weltmarkt, so dass der Grad der Abhängigkeit von russischem Kernbrennstoff schwer abzuschätzen ist.

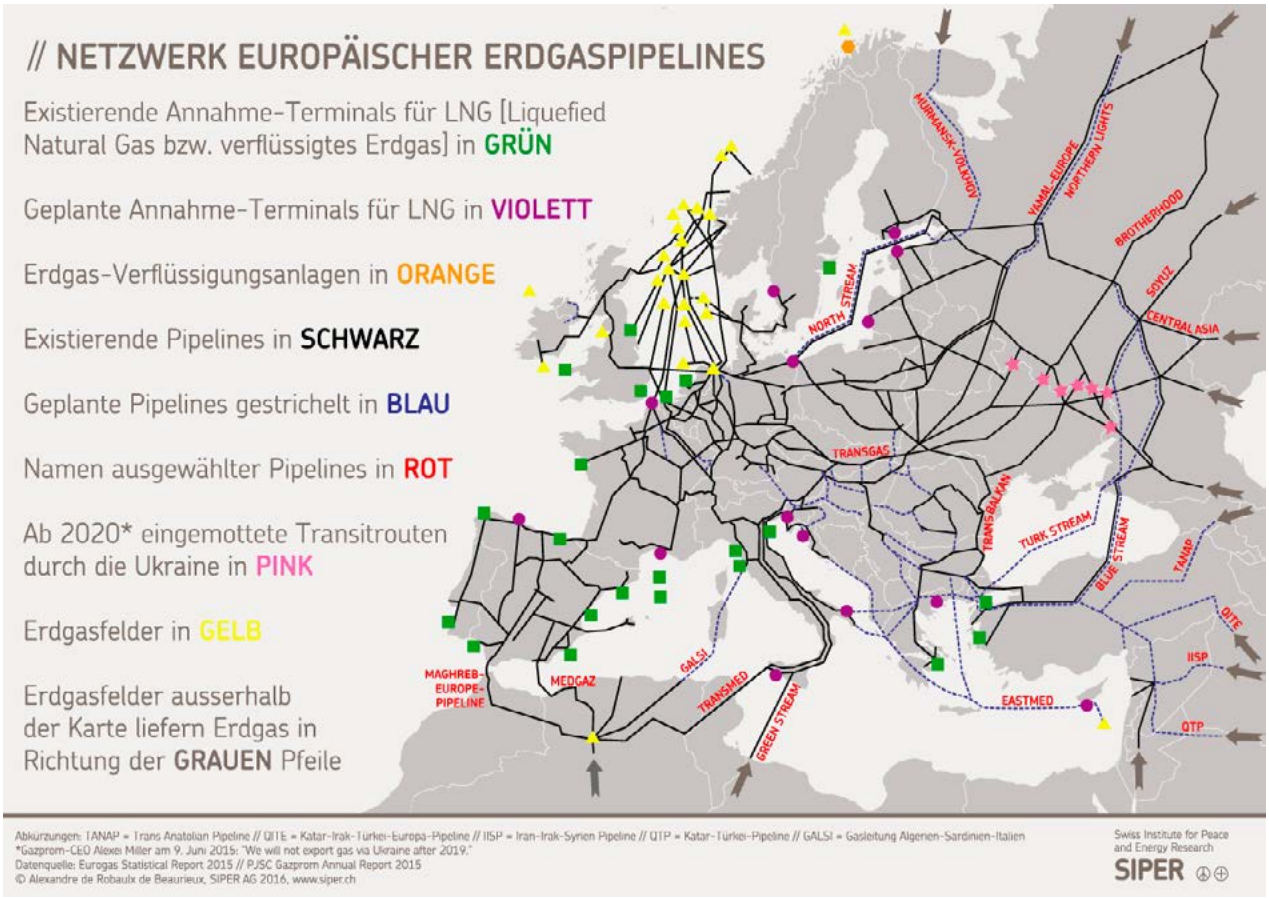


Abbildung 2 US-Fracking-Gas erobert Europa. (SIPER)

geführten Erdgaspipeline Nord Stream 2 verschärfen. Zwei Drittel der russischen Gasexporte nach Europa werden in den parallelen Verbindungsleitungen von Nord Stream 1 und Nord Stream 2 konzentriert. Europa könnte im Winter keine 30 Tage ohne russisches Gas durchstehen, während Russland sicherlich ein Jahr (wenn nicht sogar Jahre) ohne europäische Gaskäufe, Investitionen und Technologien überstehen dürfte. Die Situation wird sich für Europa verschärfen, wenn die russische Gaspipeline Power of Siberia nach China Ende 2019 in Betrieb geht und Russland Alternativen zu den europäischen Märkten erhält. Infolgedessen könnte der Kreml eine «Zuckerbrot-und-Peitschen-Politik» auf die EU und die einzelnen Mitgliedsstaaten anwenden und versuchen, mittels Drosselungen oder Lieferstopps seine Interessen durchzusetzen.

Die Schweiz im Zentrum Europas wäre ebenfalls davon betroffen, da russisches Erdgas gemeinsam mit anderen fossilen Energieträgern für die Energieversorgung hierzulande eine tragende Rolle spielt. Das in der Schweiz bislang benötigte Öl und Gas stammte lange Zeit zur Hauptsache aus Russland, dem nordafrikanischen Raum und Nigeria.

Doch seit einiger Zeit überfluten die USA die Märkte mit billigem, mit Fracking-Methoden gefördertem Erdgas und Erdöl. Dies, weil sie gemäss Einschätzung verschiedener Beobachter des Energiemarktes versuchen, vor allem Russland aus dem europäischen Markt zu verdrängen.[4] Während die USA 2013 erst 100.000 Barrel exportierten, waren es 2016 bereits 1,53 Millionen pro Tag. Seit Februar 2017 wurden über 9 Millionen Barrel täglich produziert, in der ersten Februarwoche 2018 wurde erstmals die 10 Millionen-Marke überschritten. Die US-Energieagentur EIA geht davon aus, dass 2019 bereits mehr als 11 Millionen Barrel täglich gefördert werden.[5] Weiter sind die USA inzwischen zum weltweit grössten Lieferanten von Liquified Natural Gaz (LNG) geworden, was die geplanten Annahmeterminals an den Küsten Europas und die einzumottenden Transitrouten durch die Ukraine eindrücklich veranschaulichen. Diese Fracking-Öl- und -Gas-Schwemme in die Weltmärkte hat wiederum Folgen für die Situation in Europa und insbesondere auch für den nordafrikanischen und arabischen Raum.

Diese Fracking-Öl- und -Gas-Schwemme in die Weltmärkte hat wiederum Folgen für die Situation in Europa und insbesondere auch für den nordafrikanischen und arabischen Raum.

4 Siehe: Oleg Nikiforov, Gunter-E. Hackemesser (2018): Die Schlacht um Europas Gasmarkt, Springer Verlag. Oder: https://www.heise.de/tp/features/Amerikanisches-Rohoel-wird-in-Golfstaaten-exportiert-3964188.html

5 Ebenda.

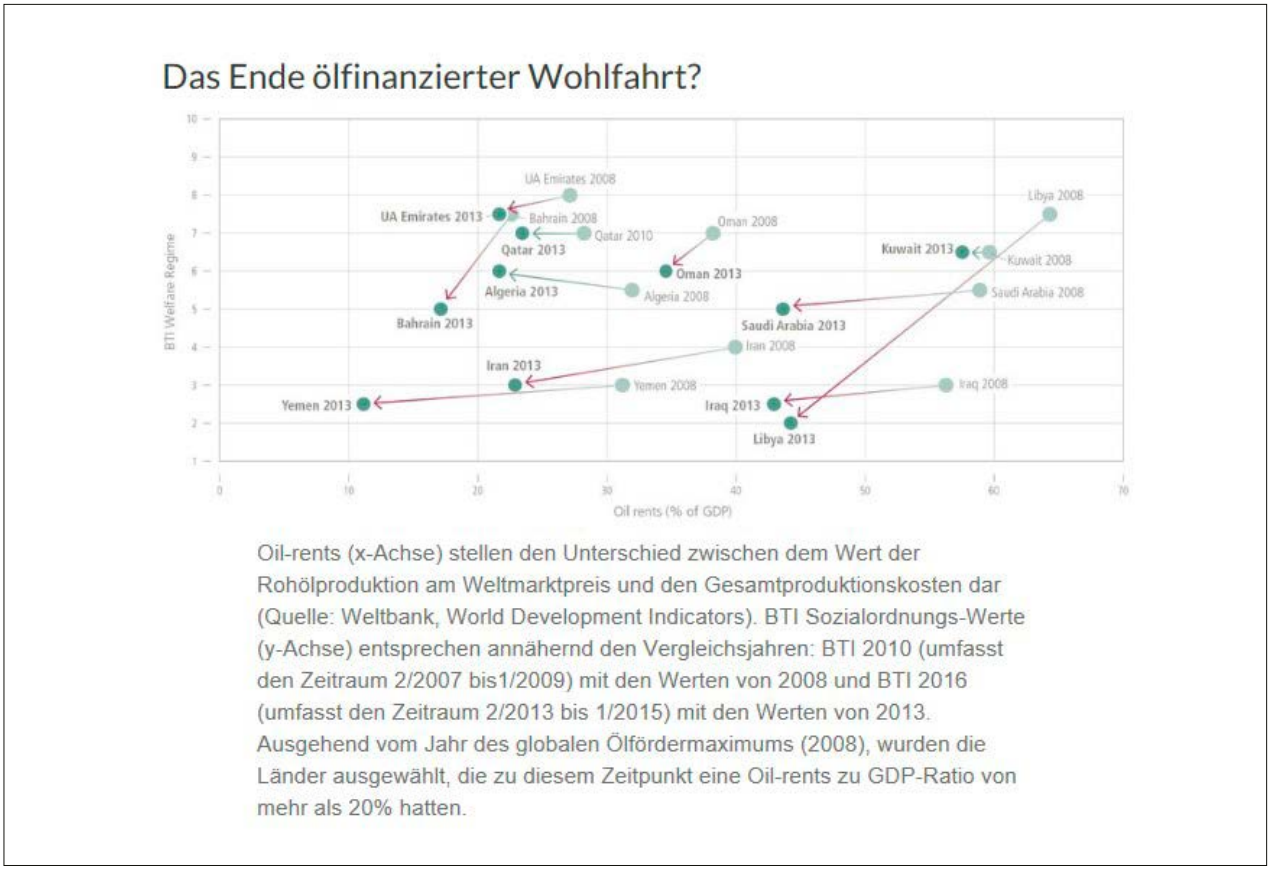


Abbildung 3 Rückgang staatlicher Wohlfahrt im MENA-Raum aufgrund des Preiszerfalls im weltweiten Ölhandel. (Bertelsmann-Stiftung, https://www.bti-project.org/de/berichte/regionalberichte/naher-osten-und-nordafrika/, abgerufen am 12.12.2018)

Neben ethnischen und religiösen Einflussfaktoren wirkte im MENA-Raum (= Mittlerer Osten und Nordafrika) der anhaltende und durch die Fracking-Förderung beschleunigte Preiszerfall im Öl- und Gas-Welthandel destabilisierend. Laut Bertelsmann-Stiftung konnte dieser «Fragilisierungsprozess» lange Zeit abgebremst werden, weil diese Volkswirtschaften auf sichere Einnahmen aus Erdöl- und Erdgasverkäufen zählen konnten.[6] Diese Staaten konnten zwar nur einen kleinen Teil dieser Einnahmen zur «Finanzierung des sozialen Friedens» verwenden, was aber trotzdem lange Zeit half, eine gewisse Stabilität und Lebenssicherheit aufrecht zu erhalten, auch trotz der herrschenden Korruption. Aber die immer tieferen Preise liessen diese Geldquelle überall in der Region versiegen, was ab 2011 gemeinsam mit politischen Fehlentscheidungen und den für diese Bevölkerungen zunehmend schwierigeren Lebensbedingungen zum «arabischen Frühling» führte. Auch kann davon ausgegangen werden, dass sich die Region aufgrund dessen sehr viel langsamer von den Folgen des arabischen Frühlings erholen wird, als wenn die vormals stabilisierenden Finanzen zur Verfügung stehen würden.

Russland hat aller Voraussicht nach wenig Interesse daran, Konkurrenz aus dieser Richtung zu fördern und auch die USA können eine weitere Ausbreitung im Europäischen Markt einfacher realisieren, solange Syrien und die afrikanische Mittelmeerküste nicht zur Ruhe kommen.

Weiter stellt sich vor dem Hintergrund des vorhin beschriebenen «Erdöl- und Erdgaslieferkampfes um Europa» die Frage, ob überhaupt ein Interesse besteht, den Syrienkonflikt zu beenden und damit die geplante Land-Pipeline zu realisieren, welche saudi-arabisches Öl in die Türkei und nach Europa transportieren könnte. Russland hat aller Voraussicht nach wenig Interesse daran, Konkurrenz aus dieser Richtung zu fördern und auch die USA können eine weitere Ausbreitung im Europäischen Markt einfacher realisieren, solange Syrien und die afrikanische Mittelmeerküste nicht zur Ruhe kommen. Dies alles ist für die Versorgungssicherheit Europas und damit auch für die Schweiz mit grossen Risiken und Nachteilen verbunden.

6 Siehe: https://www.bti-project.org/de/berichte/regionalberichte/naher-osten-und-nordafrika/

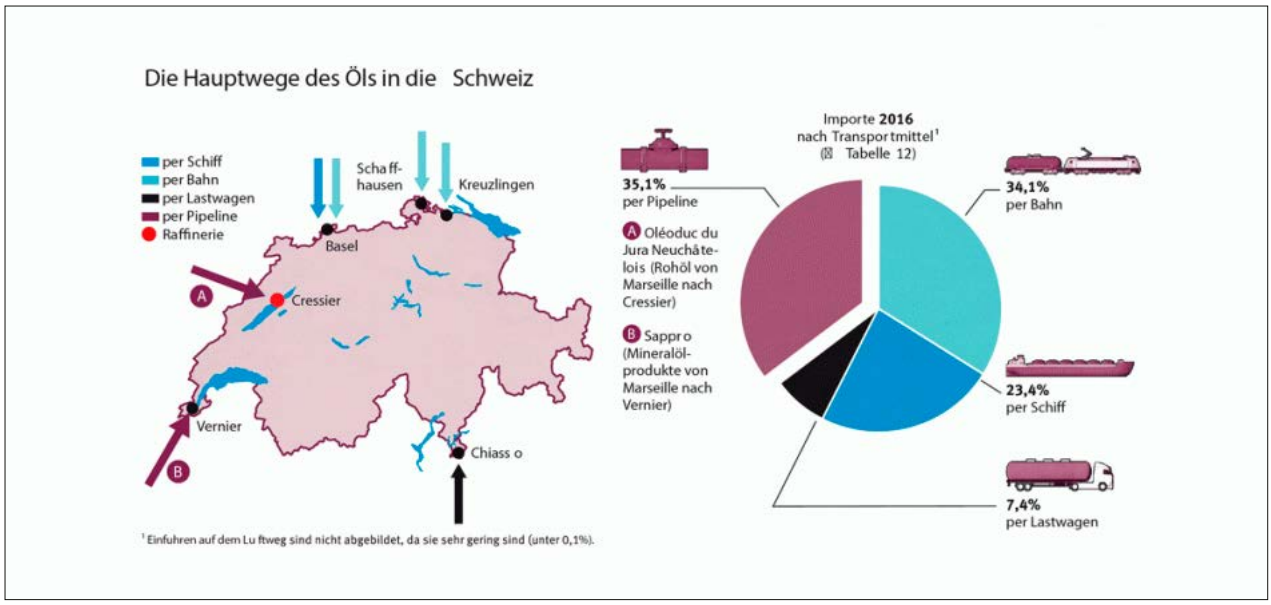


Abbildung 4 Wie gelangt Öl in die Schweiz?
(Jahresbericht 2016 der Schweizerischen Erdölvereinigung)

Ist Energiesicherheit im Bereich fossiler Energieträger möglich?

Trotz der Entdeckung neuer Vorkommen von Erdöl und Erdgas oder neuer Technologien zu deren Gewinnung ist aufgrund des bisher Dargestellten festzuhalten:

- Diese Vorkommen sind endlich, niemand weiss, wie lange sie noch nutzbar sind;
- sie liegen zu einem grossen Teil in fragilen Regionen oder Konfliktgebieten;
- der Transport des gewonnenen Öls oder Gases erfolgt durch eben solche Gebiete oder ist anderorts z. B. durch Piraterie gefährdet;
- noch zu erschliessende Vorkommen sind schwer zugänglich und liegen in Regionen mit ungeregelten territorialen Ansprüchen (z. B. problematische Tiefseebohrungen in der Arktis);
- Gewinnung und Transport bergen Umweltrisiken mit globalen Dimensionen;
- der Verdrängungskampf im Welthandel der fossilen Energieträger ist ein bedeutender Einflussfaktor auf die globale Sicherheitslage.

Das bedeutet hinsichtlich Versorgungssicherheit:

- Die Preisentwicklung ist potentiell volatil, Entwicklungen sind jederzeit in alle Richtungen möglich, was sich schon in der Vergangenheit wiederholt zeigte.
- Die Nutzung fossiler Energieträger schafft Abhängigkeiten zu einem in verschiedener Hinsicht unzuverlässigen globalen Bezugssystem.

Weiter hat der Klimawandel Folgen für die Versorgungssicherheit mit Erdöl und Erdölprodukten. Laut der Schweizer Erdölvereinigung wird bis zu einem Drittel der jährlich benötigten Erdölmenge durch die Schifffahrt auf dem Rhein in die Schweiz transportiert. Im Sommer 2018 war dies aufgrund der zu tiefen Wasserstände nicht mehr möglich. Erreichen auch die Transporte auf Strasse und Schiene ihre Kapazitätsgrenzen so ist auch in dieser Hinsicht mit Mangellagen zu rechnen und die Versorgungssicherheit nicht lückenlos gewährleistet.

Ersatz fossiler- durch elektrische Energie

Aufgrund dieser multiplen Einflussfaktoren auf die Energiesicherheit des Gesamtsystems, des weltweiten Kampfes gegen den Klimawandel (Reduktion des CO2-Ausstosses) und aufgrund der zunehmenden Verschärfung von Umweltschutzvorschriften findet gegenwärtig global ein Umdenken statt. NATO- und EDA[7]-Energieexperten gehen davon aus, dass erneuerbare Energiequellen und neue Technologien Wirtschaft und Gesellschaft grundlegend verändern werden. Bereits heute wird der Minderverbrauch an fossiler Energie mit einer Zunahme des Verbrauchs von elektrischer Energie erkauft und dieser Trend wird sich verstärken.

Bereits heute wird der Minderverbrauch an fossiler Energie mit einer Zunahme des Verbrauchs von elektrischer Energie erkauft und dieser Trend wird sich verstärken.

7 EDA = European Defence Agency (Europäische Verteidigungsagentur).

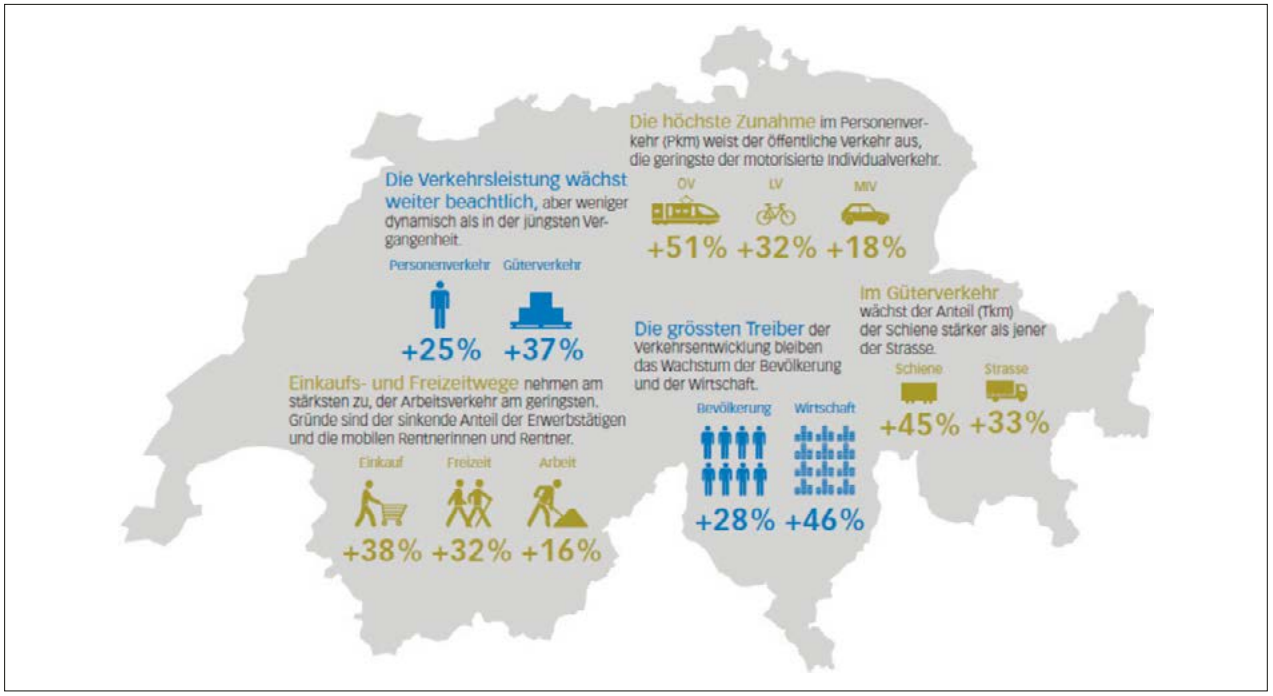


Abbildung 5 Zukunft Mobilität Schweiz: UVEK-Orientierungsrahmen 2040, Bericht vom 15. August 2017. (https://www.are.admin.ch/are/en/home/media-and-publications/publications/transport/zukunft-mobilitat-schweiz.html)

Das zeigt sich beispielsweise daran, dass sich derzeit verschiedene Automobilhersteller dazu entschlossen haben, vermehrt Forschungs- und Entwicklungsaktivitäten im Bereich der Elektromobilität zu betreiben oder keine Autos mehr herzustellen, die ausschliesslich mit klassischen Diesel- oder Benzinverbrennungsmotoren angetrieben werden.[8] Verschiedene Studien[9] prognostizierten, dass Plug-In-Hybridfahrzeuge bis im Jahr 2020 6–8% der gesamten Fahrzeugflotte auf unseren Strassen ausmachen werden. Weiter würden solche Fahrzeuge gemeinsam mit Elektro-, Brennstoffzellen- oder anderen alternativen Antrieben bis im Jahr 2050 die klassischen benzin- oder dieselbetriebenen Fahrzeuge komplett verdrängt haben, was auch die Fahrzeugflotte der Armee entsprechend verändern wird.

Die Kompensation fossiler Energie mit Elektrizität führt aber dazu, dass mehr elektrische Energie produziert oder importiert werden muss. Die Schweiz ist punkto elektrischer Energie stark mit dem europäischen Raum verzahnt und besitzt aufgrund ihrer zentralen geografischen Lage im europäischen Energiehandel eine Drehscheibenfunktion. Im Durchschnitt importieren wir 50% des Eigenbedarfs an elektrischer Energie und exportieren die gleiche Menge, wenn sie andernorts gebraucht wird. Dies wird heute vor allem durch die Pumpspeicher-Kraftwerke in den Alpen ermöglicht, welche überschüssig produzierte Energie speichern und sie Europaweit zur Verfügung stellen.

Die Schweiz ist punkto elektrischer Energie stark mit dem europäischen Raum verzahnt und besitzt aufgrund ihrer zentralen geografischen Lage im europäischen Energiehandel eine Drehscheibenfunktion.

Trotzdem ist längerfristig zusätzlich mit häufigeren Mangellagen zu rechnen, weil die Produktions- und Netzkapazitäten aufgrund technischer Grenzen und fehlender Abkommen mit der EU nicht in dem Tempo und Umfang erhöht werden können, wie es der vorgängig beschriebene Mehrbedarf kombiniert mit dem prognostizierten Wirtschafts- und Bevölkerungswachstum vorgibt. Dies ist Punkto Versorgungssicherheit sehr bedeutend:

«Im Zuge der Umsetzung des 3. Energiepakets wird der europäische Strombinnenmarkt weiter vorangetrieben. Dabei werden bislang privatrechtlich ausgestaltete Vereinbarungen zum Verbundbetrieb durch EU-Recht ersetzt. Die EU-Verordnungen enthalten eine Ausschlussklausel für Drittstaaten, sofern kein Abkommen mit der EU besteht. Dadurch wird die Schweiz bei der Implementierung der markt- und netztechnischen Kodizes zum Teil von versorgungssicherheitsrelevanten Projekten ausgeschlossen. Die Vertretung der Schweizer Interessen ist daher nur noch schwer möglich. Diese Entwicklung ist kritisch, da technische Sachverhalte nur noch am Rande mit der Schweiz besprochen werden. Durch die Implementierung der Kodizes verlieren die EU-Mitgliedsstaaten generell an Souveränität, da bei der Umsetzung ein Kompromiss gefunden werden muss und dieser dann für alle verbindlich ist. Daher ist die Durchsetzung der Schweizer Interessen auch mit einem Stromabkommen nicht selbstverständlich. Die Auswir-

8 z. B.: https://www.nzz.ch/mobilitaet/auto-mobil/e-mobilitaet-volvo-setzt-ab-2019-voll-auf-elektrifizierung-ld.1304395 (abgerufen am 17.01.2018

9 z. B. «Quo Vadis Diesel?», Studie des Verbandes der Automobilindustrie, 2017 oder die «Artemis-Studie» der ETH, 2013.

	Netz-instabilität	Netzüberlast	Ausfall durch Störung	Zerstörung Anlagen/Netz
Häufigkeit Region	alle 1-2 Jahre auch in Europa	jährlich weltweit	jährlich mehrmals auch in EU	kriegsbedingt Krisenzonen
Ursache	Komplexität der dezentralen Stromerzeugung	extremes Wetter + Naturkatastrophen	Unfälle Sabotage Terror	konventionelle oder nukleare Wirkung
Schaden	lokale bis regionale Ausfälle			regionale bis kontinentale Ausfälle
Dauer	Stunden bis Tage		Stunden bis Wochen	Tage bis Wochen

Abbildung 6 Bedrohungsszenarien, gem. Bericht über die Gefährdungen der Landesversorgung 2017, WBF. (Präsentation von Th. Rothacher, armasuisse, vom 17.10.2018)

kungen auf die Versorgungssicherheit der Schweiz sind daher weiter zu beobachten.» [10]

Neben diesen technischen und regulatorischen Grenzen bilden Sabotage und Angriffe aus dem Cyberraum zusätzliche Risiken für die Versorgungssicherheit, was sich z. B. am. 23. Dezember 2015 in der Ost-Ukraine auf verheerende Weise zeigte.

Klimawandel als Problemmultiplikator

Zusätzlich zur Kompensation fossiler Energie durch elektrische wird das Wirtschafts- und das (auch durch Klima-Migration beschleunigte) Bevölkerungswachstum auf der Nordhalbkugel die wesentlichen Anteile dieses Mehrverbrauchs ausmachen. Die Versorgungssicherheit wird durch folgende interagierende Faktoren wesentlich beeinflusst:

- Klimawandel: beeinflusst die jahreszeitliche Produktionskapazität und Nachfrage;
- Bevölkerungs- und Wirtschaftswachstum: erhöhen den Verbrauch;
- Wirtschaftliche und politische Interessen: beeinflussen Verfügbarkeit und Preise und damit den Unterhalt und Betrieb von Produktion sowie Verteilung der Energie.

Wie aus der Grafik in Abb. 7 sichtbar wird, stammt hierzulande gegenwärtig rund 60% unserer selbst produzierten elektrischen Energie aus Wasserkraft, ca. 1/3 aus Kernkraftwerken und der Rest wird mit weiteren Erneuerbaren und Nichterneuerbaren produziert. Im Jahr 2017 teilte sich die Wasserkraftgewinnung auf in 33,7% Speicherkraft und 25,9% Laufkraft. Bei der Speicherkraft werden laut einer durch den Nationalfonds geförderten Studie aufgrund des Klimawandels nicht markante Einbussen erwartet. Hingegen beeinflusst der Klimawandel die Produktion bei der Laufkraft in unseren im Sommer zunehmend trockeneren Flüssen voraussichtlich sehr viel stärker. So berichteten schweizweit Kraftwerksbetreiber Ende Sommer 2018, dass sie verglichen mit den Vorjahren eine bedeutend kleinere Energiemenge produzieren konnten[11], was vor dem Hintergrund der prognostizierten klimatischen Veränderungen künftig Zweifel an der Zuverlässigkeit dieser Energiequelle aufkommen lässt.

Hingegen beeinflusst der Klimawandel die Produktion bei der Laufkraft in unseren im Sommer zunehmend trockeneren Flüssen voraussichtlich sehr viel stärker.

Weiter wird gemäss Bundesamt für Umwelt der Klimawandel sowohl die Energienachfrage als auch die Energieproduktion beeinflussen:

«Die höheren Temperaturen lassen im Winter den Heizenergiebedarf zurückgehen, während im Sommer der

10 Bericht der ElCom zur Stromversorgungssicherheit der Schweiz 2018, S. 59

11 Siehe: – https://www.srf.ch/news/regional/aargau-solothurn/tiefe-flusspegel-kraftwerken-geht-das-wasser-aus, https://www.aargauerzeitung.ch/aargau/kanton-aargau/25-prozent-weniger-strom-aus-aargauer-wasserkraft-auch-die-solarenergie-leidet-unter-der-hitze-132878865, https://www.tagesanzeiger.ch/zuerich/region/wegen-hitze-limmat-liefert-weniger-strom/story/21970895

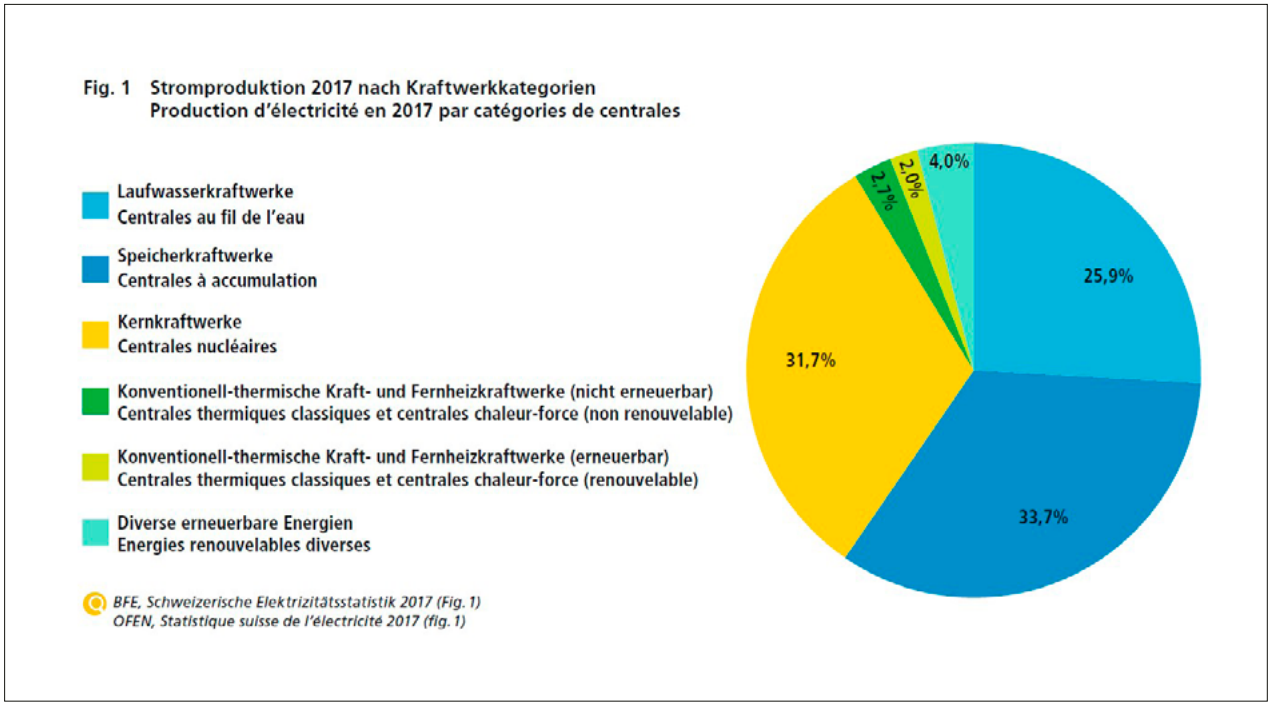


Abbildung 7 Energieproduktion in der Schweiz.
(BFE, Schweizerische Elektrizitätsstatistik 2017, Fig. 1)

Kühlenergieverbrauch steigt. Veränderungen ergeben sich auch für die Erzeugung von Elektrizität in thermischen und Wasserkraftwerken sowie für die Sicherheit von Transportinfrastrukturen».[12]

Mit anderen Worten wird sich in den künftig viel längeren, heissen Sommern[13] die Stromnachfrage gegenüber von heute deutlich erhöhen, gleichzeitig herrscht aber Wasserknappheit und damit eine reduzierte Energieproduktion aus Wasserkraft. Wie vorgängig bereits beschrieben, werden die in absehbarer Zeit an die Kapazitätsgrenzen gelangenden nationalen Verteil- und internationalen Übertragungsnetze aller Voraussicht nach europaweit unterschiedlich schnell und effektiv ausgebaut, wovon die Schweiz wiederum im Zentrum direkt betroffen ist. Die Verteilung lokal und jahreszeitlich anfallender Überkapazitäten wird damit erschwert, die Eintretenswahrscheinlichkeit von Mangellagen irgendwo in Europa – aber dennoch mit Wirkung für die Schweiz – wird vor dem Hintergrund des vorgängig beschriebenen Wirtschafts- und Bevölkerungswachstums erhöht.

Energiesicherheit: eine zentrale Verteidigungsfähigkeit

Die Lösung der Problematik wird für die Schweiz wie für ihre Nachbarstaaten deshalb in einem sukzessiv zu vollziehenden aber im Endeffekt radikalen Umbau von Produktion und Verteilung aller Energieträger und -Formen liegen. Somit besteht ein bedeutendes strategisches Interesse, Abhängigkeiten von fossilen Energieträgern zu minimieren, auf Erneuerbare umzusteigen und möglichst viel Energie aus eigener Kraft zu erzeugen. Ansonsten könnte in Mangellagen oder Notsituationen zukünftig zwischen dem zivilen Sektor und Streitkräften eine Konkurrenzsituation bezüglich der Energieressourcen entstehen. Streitkräfte müssen deshalb analog zum Schutz eigener Kräfte beginnen, Fähigkeiten zu entwickeln, um Energie/Energieträger, die sie zur Erfüllung ihrer zentralen Aufgaben benötigen, aus eigener Kraft zu produzieren oder fähig sein, sie in kurzer Zeit bereit zu stellen. Weiter sind Umwelt- und gesamtgesellschaftliche Resilienzüberlegungen anzustellen und dabei die gegenseitigen Abhängigkeiten von Armee und dem zivilen Sektor zu berücksichtigen.[14]

12 Vgl. https://www.bafu.admin.ch/bafu/de/home/themen/klima/fachinformationen/anpassung-an-den-klimawandel/anpassung-an-den-klimawandel-in-den-sektoren/anpassung-an-den-klimawandel--energie.html

13 Laut Untersuchungen der Weltbank hat sich seit den 1960er Jahren die Häufigkeit und Intensität von Hitzewellen gesteigert. Beispiele für extreme Temperaturen sind die Hitzewellen, die 2003, 2010, 2015 ganz Europa heimsuchten und auch 2018 war es überall in Europa ziemlich heiss. Solche Dürren in unseren Breitengraden kamen laut Weltbank früher durchschnittlich alle 200 Jahre vor. Sie rechnet damit, dass deren Häufigkeit progressiv zunimmt, je nach verwendetem Modell schwanken die Werte. Aber man ist sich einig, dass bis Ende dieses Jahrhunderts alle zwei bis drei Jahre Dürren dieses Ausmasses stattfinden werden, mit Folgen für den Wasserhaushalt und damit für die Energieproduktion mit Wasserkraft.

14 siehe dazu: https://www.eda.europa.eu/what-we-do/activities/activities-search/energy-and-environment-programme

Abbildung 8 Folie aus der Präsentation von Richard Brewin, EDA, an der Conference and Exhibition «Innovative Energy Solutions for Military Applications» (IESMA 2018) vom 13.–15.11.2018, in Vilnius, Litauen.
(European Defence Agency)

Streitkräfte müssen deshalb analog zum Schutz eigener Kräfte beginnen, Fähigkeiten zu entwickeln, um Energie/Energieträger, die sie zur Erfüllung ihrer zentralen Aufgaben benötigen, aus eigener Kraft zu produzieren oder fähig sein, sie in kurzer Zeit bereit zu stellen.

Im Zentrum all dieser Überlegungen steht die Erkenntnis, dass das Erreichen von Energiesicherheit eine zentrale Verteidigungsfähigkeit ist. Ziel muss es laut der European Defence Agency sein, Energieeffizienzmassnahmen besser umzusetzen und erneuerbare Energiequellen im europäischen Verteidigungssektor optimal zu nutzen. Dabei müssen multiple Zusammenhänge berücksichtigt werden, wenn Energiesicherheit für das Gesamtsystem erreicht werden soll.

So gilt der Klimawandel auch bei NATO- Armeen als «risk multiplier», welcher direkt und indirekt alle Aspekte militärischer Fähigkeiten beeinträchtigt. Aufgrund der zunehmenden Technologie- und damit auch Energieabhängigkeit von Armeen zeigt sich dies besonders drastisch. Es ist zu erwarten, dass sich viele Nebenwirkungen des Klimawandels erst noch zeigen werden, welche aber den Energieverbrauch massgeblich beeinflussen, was sich auch am Beispiel künftig steigender Lufttemperaturen zeigen lässt. So wird sich der Treibstoffverbrauch in der Luftfahrt aufgrund steigender Lufttemperaturen und damit sinkender Luftdichte in Zukunft global erheblich erhöhen.

So gilt der Klimawandel auch bei NATO-Armeen als «risk multiplier», welcher direkt und indirekt alle Aspekte militärischer Fähigkeiten beeinträchtigt.

Das Beispiel in Abbildung 9 verdeutlicht zusätzlich die Wichtigkeit von kurz- mittel und langfristigen (50 Jahre und mehr) Betrachtungshorizonten, in welchen der globale Energieverbrauch gemeinsam mit Umweltveränderungen für die militärische Fähigkeitsentwicklung miteinbezogen werden muss. Das Programm der EDA zielt deshalb darauf ab, ein umfassendes Konzept für das Energiemanagement zu schaffen und vollständig integrierte Lösungen zu finden, bei denen sowohl Energieverbrauch als auch Umwelteinwirkungen gemeinsam bewertet werden. Dabei wurde von der EDA folgende Priorisierung vorgenommen:

- Prüfung von Möglichkeiten zur Reduzierung des Kraftstoff- und Energieverbrauchs bei Einsätzen zu Wasser, zu Lande und in der Luft;
- Bewertung der Auswirkungen der künftigen Energiepolitik und neuer Technologien auf die militärischen Fähigkeiten sowie Entwicklung von Anpassungsstrategien;
- Verbreitung bewährter Praktiken für die Entwicklung von Anlagen für alternative Energien an militärischen Standorten;
- Identifikation gemeinsamer Interessen in den Bereichen Energie und Umwelt, die von einem internationalen kooperativen Ansatz (Armee-ziviler Sektor) profitieren würden.

Viele Forschungs-Programme der NATO und der EDA zielen deshalb bereits seit 2006 darauf ab, dass in Zukunft:

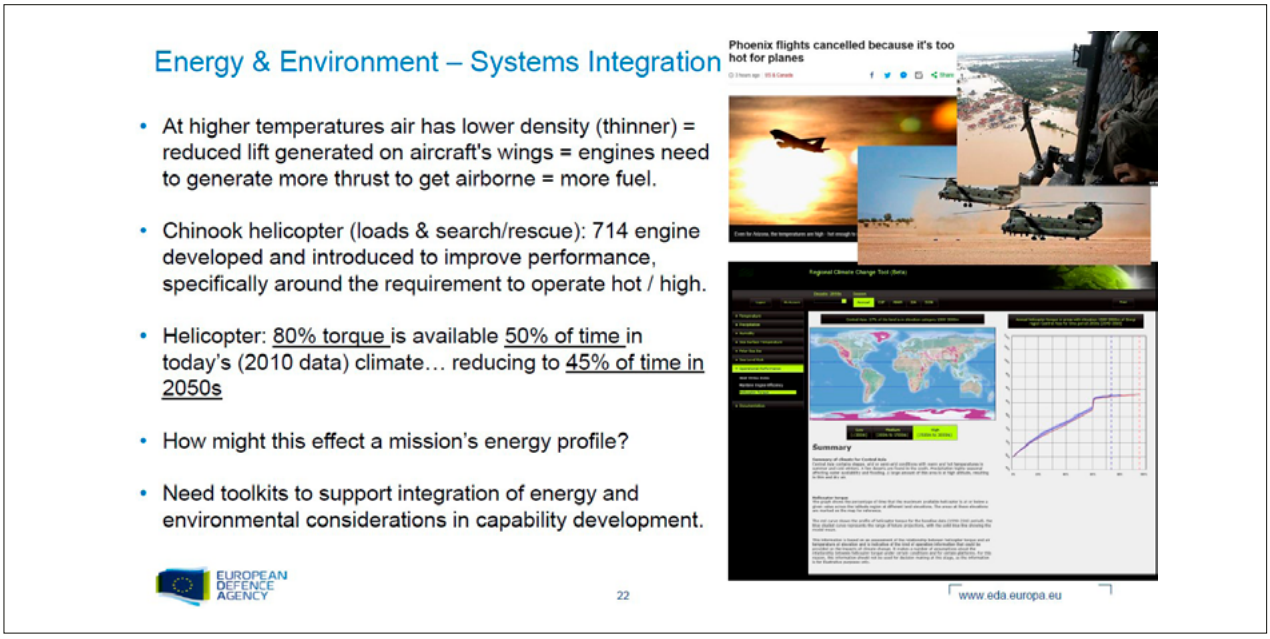


Abbildung 9 Folie aus der Präsentation von Richard Brewin, EDA, an der Conference and Exhibition «Innovative Energy Solutions for Military Applications» (IESMA 2018) vom 13.–15.11.2018, in Vilnius, Litauen.
(European Defence Agency)

– Abhängigkeiten von importierten fossilen Brennstoffen verringert und Energieeffizienz verbessert werden;
– neue Energietechnologien in militärischen Fähigkeiten integriert;
– die Kultur- und Managementfragen verstanden werden, die innerhalb des Militärs bestehen und welche die allgemeine Nachhaltigkeit und Widerstandsfähigkeit beeinträchtigen.

Im Norden Europas wurden diese gesamtgesellschaftlichen Resilienzgedanken auch vor dem Hintergrund neu entstandener Bedrohungen in Verteidigungsstrategien und -Doktrinen festgeschrieben (z. B. Schweden: Resilience: Planning for Sweden's «Total Defence»[15]). Dies ist möglich, weil die Regierungen dieser Länder ihre Armeen als interdependente und interagierende Teile des Wirtschafts- und Gesellschaftsgefüges sehen.

Konklusion

In Nordeuropa, wie auch in der Schweiz, hängen Militär und ziviler Sektor am selben verletzlichen Energie-Netz, woraus sich hinsichtlich Verteidigungsfähigkeiten multiple Herausforderungen ergeben. Man sieht sich mit einer Situation konfrontiert, bei welcher von aussen ein Prozess in Gang gesetzt wurde, der rasant voranschreitet und der das Gesamtsystem Schweiz einige Jahrzehnte beschäftigen wird. Es lohnt sich deshalb für die Armee ihren Handlungsbedarf zu eruieren und dort, wo bereits heute klar erkennbar und notwendig, proaktiv wirkende Massnahmen zu ergreifen, damit existentielle Entwicklungen in Gang gesetzt werden können oder diese zumindest nicht behindert werden. Dabei ist zu beachten:

– Die Armee als Käuferin von Fahrzeugen, Heizungen usw. wird von dieser technologischen Wende betroffen sein und sie wird sich entsprechende Fähigkeiten im Unterhalt wie Betrieb technologisch neuer Systeme aneignen müssen;
– der Aufbau dieser Fähigkeiten ist zeitintensiv und muss frühzeitig begonnen werden, damit diese zeitgerecht zur Verfügung stehen, wenn sie benötigt werden;
– ein Zuwarten generiert heute zwar Einsparungen, wird aber in Zukunft mit Mehrkosten bestraft, wenn die entstandenen Fähigkeitslücken aufgeholt/kompensiert werden müssen.

… besteht aber auch die Chance, Resilienzpotentiale für das Gesamtsystem zukünftig zu erhöhen, wenn es der Armee gelingt, ihren Energiebedarf aus eigener Kraft abzudecken.

Es geht einerseits darum zu verhindern, dass die Armee im Ereignisfall mit dem zivilen Sektor um Energieressourcen konkurriert. Andererseits besteht aber auch die Chance, Resilienzpotentiale für das Gesamtsystem zukünftig zu erhöhen, wenn es der Armee gelingt, ihren Energiebedarf aus eigener Kraft abzudecken. So kann bei Bedarf ein Energieaustausch an den zivilen Sektor geleistet werden, wie wir dies bereits in MPR 2-2016[16] für die Schweiz beschrieben haben. Jedoch muss betont werden:

15 Siehe: https://www.nato.int/docu/review/2018/also-in-2018/resilience-planning-for-swedens-total-defence/en/index.htm (abgerufen am 21.01.2019)

16 Siehe: Krummenacher, Martin und Krauer, Daniel: «Klimawandel und schwindende Ressourcen – interagierende Bedrohungen mit Folgen für die Streitkräfteentwicklung», Military Power Revue, 2-2016. Im damaligen Beitrag haben wir das «Wie» betont und einige Technologien genauer beschrieben, im vorliegenden Artikel steht das «Warum» der Autarkiebemühungen im Vordergrund.

– Innovation entwickelt sich schneller als die Politik.
– Existierende Politik basiert immer auf bereits in kurzer Zeit veralteten Grundlagen.
– Es braucht deshalb ein Denken in langen Zeithorizonten.
– Und: Es muss möglichst rasch ein Anfang gewagt werden.

Einerseits geht es darum, Massnahmen zu treffen, die helfen Energie:

– selber zu produzieren,
– effizient und überdauernd zu speichern,
– zu sparen,
– für die Aufgabenerfüllung der Armee möglichst effizient zu nutzen oder zu verteilen.

Dies deshalb, weil die Schweiz die Wirkung allfälliger Sanktionen/Lieferstopps bei den fossilen Energieträgern stärker spürt als die sie umgebenden Staaten. Obwohl sie im Zentrum des europäischen Verteilnetzes liegt, hat sie kaum Einfluss auf die Verteilungsmodalitäten in Mangellagen. Wie bereits weiter vorne ausgeführt, stellt sich die Situation im Bereich der elektrischen Energie ähnlich dar. Vor diesem Hintergrund sind alle Energieverbraucher in der Schweiz und damit auch die Armee gefordert, die von ihr für die Erfüllung der zentralen Aufgaben benötigte Energiemenge selber ausreichend zu produzieren, zu bevorraten und lagegerecht allfällige Ergänzungen sicherzustellen. Es geht also analog zum Schutz eigener Kräfte darum, Energiesicherheit für die zentralen Aufgaben- und Fähigkeitsbereiche aus eigener Kraft sicherzustellen. Das umfasst alle Handlungsfelder sowie Energieträger und -Formen (Brenn- und Treibstoffe, Elektrizität). In Ergänzung dazu reduzieren Autarkie-Fähigkeiten Abhängigkeiten vom Ausland und schaffen Resilienzpotentiale, welche wie nachfolgend genannt entstehen könnten (Aufzählung nicht abschliessend):

– Kontinuierlicher Aufbau einer Armee-eigenen dezentralen Energieproduktion (d. h. Selbstversorgung und Reduktion/Elimination der Übertragungsverluste);
– Überdauernde Speicherung von überschüssig produzierter elektrischer Energie (z. B. mittels Power to X), was auch dem Mobilitätssektor dienen würde;
– Weitergabe überschüssiger Energie an den zivilen Sektor (zu marktüblichen Preisen, ohne finanzielle Gewinne für die Armee);
– Intelligente Verteilung und sparsame Nutzung der vorhandenen Energie (z. B. durch Netzkonvergenz, Smart Grids usw.);
– Aufbau von Kooperationen mit dem zivilen Sektor im Energiebereich.

Energiesicherheit ist ein strategischer und sicherheitspolitischer Faktor, welchen die Armee massgeblich beeinflussen kann und welcher zur Resilienz des Gesamtsystems Schweiz wesentlich beiträgt.

Abbildung 10 Prototyp der CO-Elektrolyse (10 kW DC): Hier wird überschüssige Sonnen- und Windenergie zur Synthese von Wasser und CO2 zu synthetischem Benzin verwendet (Power to X), mit einem energetischen Wirkungsgrad von 80%. (Sunfire, DEU)

Dadurch tragen die so entstehenden Redundanzen zur Robustheit und Netzstabilität der landesweiten Stromversorgung bei, was bei der Bewältigung von Krisenlagen jeglicher Art bedeutend ist. So könnte die Armee bei regionalen Mangellagen als verlässlicher Partner unterstützend/kompensierend wirken, was auch ihre lokale Verankerung begünstigt. Energiesicherheit ist ein strategischer und sicherheitspolitischer Faktor, welchen die Armee massgeblich beeinflussen kann und welcher zur Resilienz des Gesamtsystems Schweiz wesentlich beiträgt.

Daniel Krauer

Oberst i Gst/MSD/dipl. Bau-Ing., Armeestab, UE V/D, Chef Militärdoktrin

E-Mail: daniel.krauer@vtg.admin.ch

Martin Krummenacher

Dr. phil./dipl. Masch.-Ing., Altkantonsrat, Kanton Luzern, Armeestab, UE V/D, KPM Militärdoktrin

E-Mail: martin.krummenacher@vtg.admin.ch

Mythos «Gerasimov-Doktrin – Ansichten des russischen Militärs oder Grundlage hybrider Kriegführung?

Christoph Bilban und Hanna Grininger (Hrsg.)

344 Seiten, Schriftenreihe der Landesverteidigungsakademie, Band 2/2019, Wien, Jänner 2019.
ISBN: 978-3-903121-57-7

Im Januar 2013 hielt der Chef des Generalstabs der Russischen Föderation, General Valerij Gerasimov, eine programmatische Rede zu Standortbestimmung und Ausrichtung der Streitkräfte Russlands. Spätestens nach der völkerrechtswidrigen Annexion der Krim und dem Ausbruch des bewaffneten Konflikts in der Ostukraine im Verlauf des Jahres 2014 erlangte der Rede und ihre Hauptaussagen den Status «Gerasimov-Doktrin», welche ihrerseits als Ausgangslage eines künftig völlig neuen «Kriegsbilds» zu betrachten sei. Vor diesem Hintergrund boten sich die Aussagen Gerasimovs an, unterstützt durch die Militärdoktrin der Russischen Föderation vom Dezember 2014, dieses neue Bedrohungsbild aus Sicht des Westens auch zu legitimieren. Vom NATO-Generalsekretär bis zu vielen namhaften Militärdoktrin-Experten wurde dieses in der sich entwickelnden Spannungszunahme zwischen dem westlichen Bündnis und Russland perfekt passende Narrativ übernommen und nachhaltig disseminiert.

In einem Zeitgeist, wo political spin zu einem wesentlichen Instrument der Meinungsbildung geworden ist, ist eine unaufgeregte, unparteiliche und wissenschaftlich fundierte Durchdringung solcher vordergründig klaren und simplen Erkenntnisse immer hilfreich. Es ist das Verdienst des Instituts für Friedenssicherung und Konfliktmanagement (IFK) des Österreichischen Bundesheers, sich dieser notwendigen und nützlichen Herausforderung gestellt zu haben. Unter der kundigen und sorgfältigen Schriftleitung durch Christoph Bilban und Hanna Grininger geht es im vorliegenden Band darum, die «Gerasimov-Doktrin» möglichst breit zu kontextualisieren und damit deren Bedeutung für das russische strategische Denken zu verstehen. Zudem soll die angesprochene Entwicklung und Verfestigung sicherheitspolitischer Begriffe und der damit verbundenen Narrative nachgezeichnet und bewertet werden. Dazu ist insbesondere auch die Darstellung der unterschiedlichen Perzeptionen in der Militärpublizistik in ausgewählten Staaten (darunter auch die Schweiz) von Interesse.

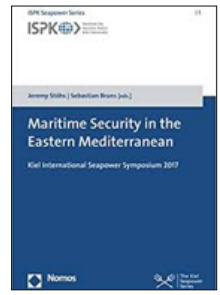
In der breit angelegten Aufarbeitung der effektiven Faktenlage zu dieser Problematik, die in der Entwicklung des Narrativs vielerorts so weit gegangen ist, dass daraus das «neuartige Konzept des hybrid wars» konstruiert worden ist, ist beispielsweise die Feststellung von Relevanz, dass der Begriff resp. das Konzept des «hybrid war» offensichtlich keine genuin russische Erfindung darstellt, sondern 2005 unter anderen vom damaligen Kommandanten des NATO Transformation Commands (ACT) und nachmaligen U.S. Verteidigungsminister James N. Mattis präsentiert worden war.

In der gut strukturierten Publikation der Schriftenreihe der Landesverteidigungsakademie wird die Thematik in zehn Kapiteln aufgearbeitet. Christoph Bilban, Hanna Grininger, Christian Steppan sowie Anna Raas stellen den grundsätzlichen Kontext her und versuchen, Valerij Gerasimov darin einzubetten. Fünf weitere Kapitel sind dem regionalen Diskurs der «Gerasimov-Doktrin» in Nordeuropa (Christian Steppan), im Vereinigten Königreich (Christoph Bilban), in Deutschland, Österreich und der Schweiz (Bilban/Grininger), auf der iberischen Halbinsel (Grininger) sowie bei chinesischen Thinktanks (Doris Vogl) gewidmet. Von besonderem Interesse dürften auch die Erkenntnisse der letzten drei Kapitel aus der Feder von Christoph Bilban und Hanna Grininger sein, die neben der Nachhaltigkeit insbesondere auch die Weiterentwicklung des aufgezeigten Narrativs anhand eines «Zitat-Mapping aufzeigen und diskutieren.

Die Autoren betrachten die Publikation als Beitrag zur Grundlagenforschung und verzichten deshalb bewusst auf direkte Empfehlungen für die europäische Sicherheits- und Militärpolitik, ausser auf diejenige, dass faktenbasierte Politik unabdingbar fundierte und nachhaltige Regionalexpertise – hier zu Russland- erfordert. Dem ist nichts beizufügen! Für eine sicherheits- und militärpolitisch interessierte Leserschaft kann der vorliegende Band vorbehaltlos empfohlen werden. Für Experten mit Anspruch auf thematische Kompetenz wird es als Pflichtlektüre anempfohlen!

GEU

Maritime Security in the Eastern Mediterranean – Kiel International Seapower Symposium 2017



Jeremy Stöhs/Sebastian Bruns (eds.)

84 Seiten, ISPK Seapower Series, Volume 1, Nomos Verlag, Baden-Baden, 2018.
ISBN: 978-3-8487-4530-2.

Seit 2013 führt das Zentrum für Maritime Strategie und Sicherheit des Instituts für Sicherheitspolitik an der Universität Kiel internationale Konferenzen und Anlässe zu maritimen sicherheitspolitischen Herausforderungen und zur Rolle von Seestreitkräften im 21. Jahrhundert durch. Seit 2017 gibt es dazu die sogenannten Kieler Seapower Series.

Die vorliegenden englischsprachige Broschüre enthält die Referatstexte der 2017 unter dem Thema «Maritime Security in the Eastern Mediterranean» Vortragenden. Diesem Thema kommt nicht nur angesichts des seit Jahrzehnten schwelenden Nahostkonfliktes im Allgemeinen, sondern im Besonderen auch angesichts des Syrienkonfliktes, dessen Implikationen und der Verstrickung Russlands mit wieder zunehmender Marinepräsenz im östlichen Mittelmeer eine höchst brisante Bedeutung zu. Das Mittelmeer mit einer reichen Geschichte, als Schmelztiegel zahlreicher Kulturen und Religionen, als Scharnier zwischen drei Kontinenten sowie als Verbindung zu verschiedenen Meeren hat bekanntlich auch eine weit zurückreichende maritime Vergangenheit. Aus der Vielzahl von wichtigen historischen Ereignissen sei nur eines herausgegriffen: Im Yom Kippur Krieg (Oktober 1973) standen sich im östlichen Teil des Meeres über 90 Kriegsschiffe der sowjetischen Mittelmeer-Eskadra und über 60 Einheiten der 6. US Flotte mit drei Flugzeugträgern gefährlich nahe gegenüber. Es war marineseitig die wohl heikelste Zuspitzung im Kalten Krieg. Vor dem Hintergrund des heutigen Syrienkonfliktes und seinen Auswirkungen, der erneuten Verstärkung der russischen Mittelmeer-Eskadra und anderer Akteure sei bloss dieses Ereignis in Erinnerung gerufen.

Sechs Autoren beleuchten die gegenwärtig wichtigsten Fragen zur maritimen Sicherheit in der Region. Sebastian Bruns, der Leiter des Zentrums für Maritime Strategie und Sicherheit, sowie Jeremy Stöhs, amerikanisch-österreichischer Sicherheitsexperte am Institut für Sicherheitspolitik der Universität Kiel, zeichnen als Herausgeber des Bandes.

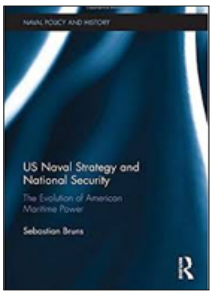
Bruns eröffnet die Textsammlung mit einer Einführung «21st Century Seapower in the Eastern Mediterranean», Chris Parry berichtet über «The Eastern Mediterranean – A Brief Geo-Political Overview», Heiko Borchert über «The Diversity Challenge: Five Perspectives on Eastern Mediterranean Geoeconomics», Shaul Chorev über «Security and Energy in the Eastern Mediterranean: The Israeli Perspective», Sebastian Hamann zu «»Regional Stakeholders in the Eastern Mediterranean and Beyond: Iran, Saudi Arabia and Egypt» sowie Randy Papadopoulos zu «The longue durée: Mediterranean Challenges and Solutions for the U.S. Navy and Marine Corps».

Die Palette der Beiträge ist breit und beschränkt sich nicht bloss auf militärische Aspekte, wobei hier eine russische Stimme durchaus erwünscht gewesen wäre. Im allgemeinen sind die Erkenntnisse über die wirtschaftliche Dimension der Region nicht besonders verbreitet. Umso wertvoller sind die Beiträge dieser Schrift dazu. Als Quasi-Anstösser an die hier behandelte Region müsste die vorliegende Broschüre auch Schweizer Leserinnen und Leser interessieren.

Im Juni 2019 wird die Serie maritimer Konferenzen in Kiel mit dem Thema «The Means of Maritime Strategy in an Era of Great-Power Competition» fortgesetzt. Man darf gespannt sein und hoffen, dass die dort vorgetragenen Texte wiederum einer breiteren Öffentlichkeit zugänglich gemacht werden.

Jürg Kürsener

US Naval Strategy and National Security – The Evolution of American Maritime Power



Sebastian Bruns

270 Seiten, Routledge London and New York, 2018.
ISBN: 9781138651739.

Der Autor leitet das Zentrum für Maritime Strategie und Sicherheit am Institut für Sicherheitspolitik an der Universität Kiel. Das vorliegende englischsprachige Buch ist eine überarbeitete und erweiterte Version seiner Dissertation «U.S. Navy Strategy & American Sea Power from the ‹Maritime Strategy› (1982–1986) to ‹A Cooperative Strategy for 21st Century Seapower (2007): Politics, Capstone Documents, and Major Naval Operations 1981–2011» aus dem Jahre 2014.

Bruns untersucht im Wesentlichen die Entwicklung der amerikanischen Seestrategie zwischen 1981 und 2016. Im ersten Teil geht der Autor unter anderem auf Grundzüge und die Vorgeschichte der Strategie 1945–1980 sowie auf wichtige Begriffe ein, wie beispielsweise auf die feinen Unterschiede zwischen «naval» und «maritime». Es folgen als Kern die vier Kapitel «A naval renaissance through the maritime strategy» (1981–1989), «Managing strategic change and embracing a new world order» (1989–2001), «A sea power rationale for the twenty-first century» (2001–2008) und «Sea change: American national security and U.S. seapower in an increasingly chaotic world» (2009–2016), bevor Bruns seine Schlussfolgerungen zieht.

Das vorliegende Werk über die amerikanische Strategieentwicklung der letzten 30 Jahre ist ein Abbild der jeweiligen Weltlage, der Bedrohungsperzeption, der Strukturen und Bauprogramme der US Navy sowie nicht zuletzt der von den Prioritäten der jeweiligen Administration geprägten Weltanschauung und Maximen. Dass dabei die Bedeutung der Navy immer wieder unterschiedlich beurteilt worden ist, liegt auf der Hand. Entsprechend stellt der Autor wechselnde Gewichtungen der Seestrategie innerhalb der nationalen Sicherheitsstrategie fest. Noch Jahre nach dem Vietnamkrieg und insbesondere unter Carter war die Navy hauptsächlich auf die Projektion von Macht von See auf Landziele fokussiert. Ihre andere, ureigenste Aufgabe, nämlich die Ausübung der Kontrolle bestimmter Seegebiete (sea control), war massiv vernachlässigt worden. Der ehemalige Marineoffizier Carter hat dem maritimen Denken offenbar keine grosse Bedeutung beigemessen. Zählte die Navy 1970 noch einen Bestand von knapp 770 Einheiten, waren es 1977 noch gerademal deren 464. Damit einher ging auch eine Erosion des strategischen Denkens.

Die Einführung ballistischer Lenkwaffen-Unterseeboote (SSBN) befreite die Trägerflotte weitgehend von ihrer bisherigen nuklearen Rolle, der Rückzug der Royal Navy aus dem Mittleren und Fernen Osten, die Rückstufung der amerikanischen Containment Politik, die unter dem sowjetischen Flottenadmiral Gorschkov gross angelegten und weltweiten Manöver der nach der Kubakrise 1962 erstarkten Roten Flotte («Okean 70» und «Okean 75»), die gleichzeitig steigende Bedeutung der konventionellen Konfrontation in Europa und andere wichtige Faktoren förderten in den USA die Erkenntnis auf eine Neugewichtung der Rolle der Navy. Die lange Zeit postulierte Swing-Strategie, die im Konfliktfalle eine Verstärkung der Atlantikflotte durch Elemente des Pazifiks und vice versa vorsah, verlor sukzessive an Rückhalt.

Admiralstabschef Holloway strebte in seiner Amtszeit 1974–78 langfristig einen Wiederaufbau der US Navy auf 500 bis 800 Einheiten an. Bruns zeigt des Weiteren auf, wie die im April 1980 misslungene Operation «Eagle Claw» zur Befreiung der Geiseln aus der US Botschaft in Teheran zu einer Zäsur im Denken der USA geführt hat. Diese Demütigung offenbarte nicht nur das Unvermögen der US Streitkräfte, sondern anerkannte nun wichtige strategische Interessen der USA in der Region. Der Ruf nach einer Weltmachtrolle und starken Seestreitkräften wurde laut. Nicht zuletzt deswegen kamen Präsident Reagan und sein rühriger Marineminister Lehmann ins Amt. Deren Ziel zum Aufbau einer Navy mit 600 Einheiten und mit offensiven Aufgaben bis hin in die Norwegensee (z. B. Seemanöver «Ocean Venture» 1981 und «Ocean Safari» 1985) bzw. den Nordpazifik (zB. «Kernel Potlatch» 1987) zur Entlastung der Zentralfront in Europa, wurde zügig in die Wege geleitet. Die bereits seit langem getätigten Überlegungen zur Stärkung und Rolle der maritimen Komponente der US Militärstrategie mündeten schliesslich ins Dokument «Maritime Strategy» (1986). 1992 folgte als Produkt der veränderten strategischen Landschaft das Weissbuch «...From the Sea», welches dem Ende des Kalten Kriegs und dem anstehenden 21. Jahrhundert Rechnung tragen sollte. Nunmehr sollte sich die Navy nicht bloss mit der globalen Bedrohung auseinandersetzen, sondern – wo erforderlich – auch Mittel und Wege zur Projektion von Macht und zur Einflussnahme bis hin in küstennahe Regionen freistellen.

Eindrücklich erläutert der Autor, wie dieses strategische Konzept 1994 unter der Bezeichnung «Forward...From the Sea» erweitert und angepasst wurde, wobei nun spezifisch auch die Beiträge von Seestreitkräften in friedenserhaltenden Operationen, in der Krisenreaktion, in regionalen Konflikten sowie in Katastrophen berücksichtigt werden sollten. Seither sind zahlreiche weitere Publikationen und Richtlinien für das weltweite Agieren der US Seestreitkräfte publiziert worden, wie der «Fleet Response Plan» (2003), die «Cooperative Strategy for the 21st Cen-

tury» (2007) oder die «Cooperative Strategy for the 21st Century – forward, engaged, ready» (2015), die trotz bestehenden Lücken im Potential alle eine Beibehaltung der Überlegenheit zur See postulieren. Sie sind aber angesichts einer sich schnell verändernden Welt auch Ausdruck eines offensichtlichen Bedürfnisses nach Orientierungshilfe.

Künftige Analysen in der Form des vorliegenden Buches werden sich mit den jüngsten Entwicklungen und den erforderlichen strategischen Konsequenzen weltweit auseinandersetzen müssen. Denn hier werden wieder erstarkte oder potente neue Akteure zur See zu berücksichtigen sein, wie beispielsweise die stark expandierende Marine der Volksrepublik China und die ambitiösen bis aggressiven Aktivitäten Chinas im Südchinesischen Meer.

Bruns ist es hervorragend gelungen, mit einer gut verkraftbaren wissenschaftlichen Chronologie das Wesen, die Bedeutung und Entwicklung der amerikanischen Seestrategie der letzten gut 30 Jahre im Kontext der nationalen Sicherheitsstrategie zu analysieren. Er stellt eine solide Grundlage zur Verfügung, um das maritime Denken und Agieren der USA in der Vergangenheit zu verstehen und um damit das künftige Handeln besser antizipieren zu können.

Jürg Kürsener

Die Military Power Revue ist ein offenes Forum.
Sie fördert das Studium und die Diskussion aktueller sicherheitsrelevanter Themen, insbesondere in Bezug auf die Anwendung militärischer Macht.

Die Military Power Revue leistet Beiträge
– zum sicherheitspolitischen Diskurs,
– zur Förderung des nationalen und internationalen Dialogs,
– bei der Entwicklung von Doktrin und Konzepten.

La Military Power Revue constitue un forum ouvert.
Elle est destinée à encourager l'étude et la discussion sur des thèmes actuels de politique de sécurité, en particulier ceux liés à la mise en oeuvre de la puissance militaire.

La Military Power Revue apporte une contribution
– au débat en matière de politique de sécurité,
– à la promotion du dialogue national et international,
– aux réflexions doctrinales

The Military Power Revue is an open forum. It shall encourage study and discussion on pertinent topics of security related relevance, particularly with regard to the application of military power.

The Military Power Revue is contributing
– to the security policy discourse,
– to fostering national and international dialogue,
– at developing doctrine and concepts.

Military Power Revue der Schweizer Armee – Nr. 1/2019 80.024d 05.2019 18700