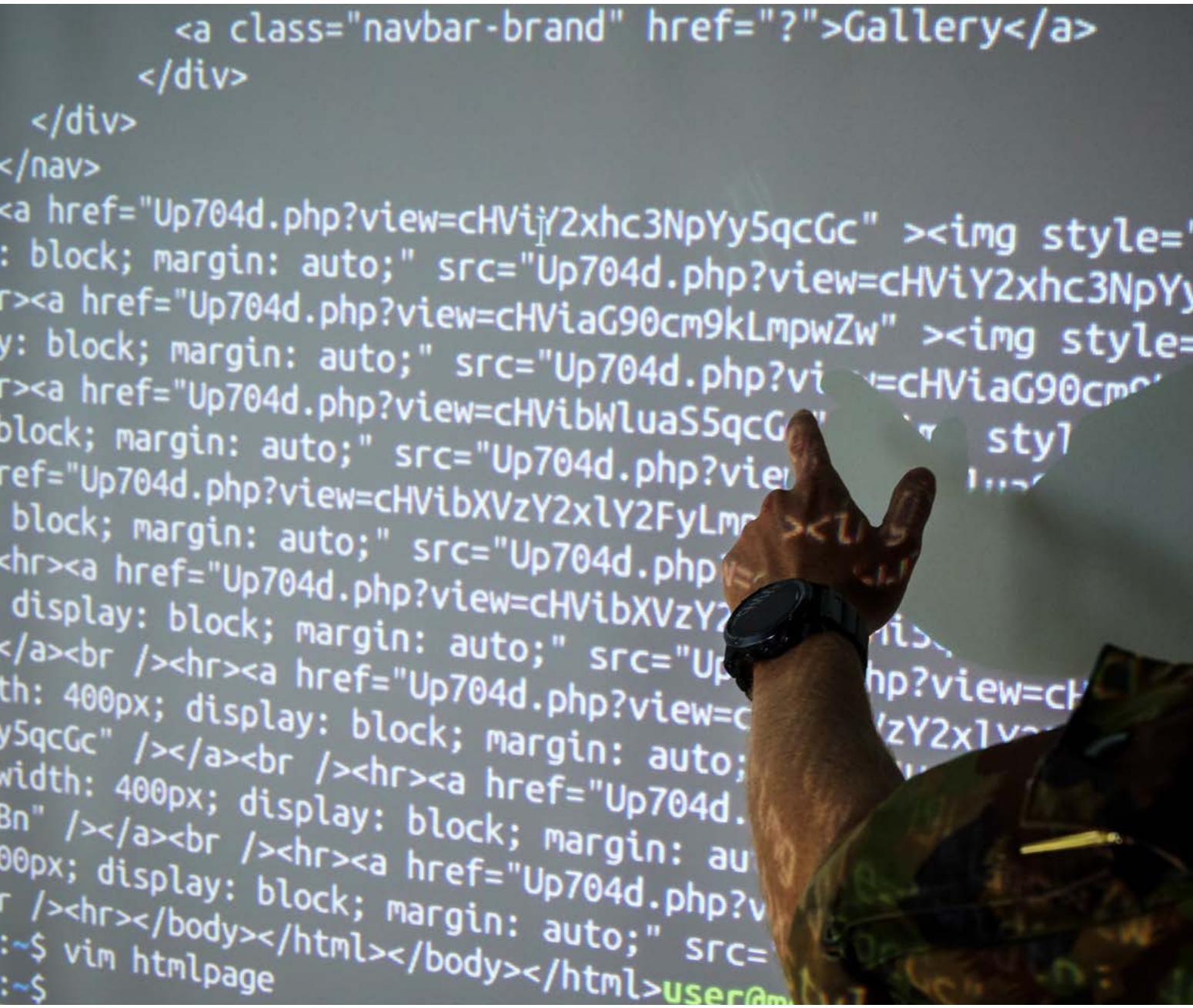
Herausgeber: Chef der Armee

Nr. 2/2018
Beilage zur ASMZ 12/18 und RMS 6/18

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

Chefredaktion ASMZ:
Divisionär Andreas Bölsterli
Verlag ASMZ
Brunnenstr. 7
8604 Volketswil

NATO's Challenges Today: A European Perspective 5

Richard Rossmanith

Erfahrungen und Lehren der Strategischen Führungsübung 2017 (SFU 17) 13

Erika Laubacher-Kubat

Cybersécurité: la première ligne de défense contre l'impact de l'intelligence artificielle 18

Marc-André Ryter

Strategieanalyse: Methodik und Visualisierung 31

Mauro Mantovani
Marcel Berni

Spin Politics – Machtpolitik *anders* lesen 43

Remo Reginold

Ethics in Military Public Affairs: a practical framework 60

Henrique Schneider

Titelbild Die Abwehr gegen Cyper-Angriffe ist eine sicherheitspolitische Hauptherausforderung (VBS/DDPS)

Vorwort

Geschätzte Leserinnen und Leser der Military Power Revue

Begriffe wie Cyber War, Cyber Security, Cyber Defence, Cyber Attacken sind seit geraumer Zeit in aller Munde. Weit weniger bekannt ist, dass die nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken im Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) durch den «Plan d'Action Cyber Défense» umgesetzt wird. Dieser beschreibt die Massnahmen, welche auf Stufe Departement und auf Stufe der Bundesämter respektive der Gruppe Verteidigung im VBS umzusetzen sind.

Im Rahmen dieses «Plan d'Action Cyber Défense» integriert sich die Armee aktiv in das nationale Gesamtdispositiv und arbeitet an verschiedenen Stellen mit den zivilen Behörden und der Wirtschaft zwecks Schutz und Abwehr von Cyber-Bedrohungen zusammen. Für die Schweizer Armee bedeutet dieser Ansatz, dass

- sie ihre Informatiksysteme im In- und Ausland in allen Lagen selbständig vor Cyber-Angriffen schützen muss;
- sie andere Schweizer Akteure subsidiär unterstützen kann, jedoch nicht für deren Cyber-Schutz verantwortlich ist;
- sie einen Beitrag an das nationale Lagebild leistet und eng mit den anderen Akteuren zusammenarbeitet;
- sie nach einem entsprechenden politischen Entscheid Aktionen im Cyberraum selbständig durchführen können muss.

Dazu setzt die Armee Teile der Berufsorganisation der Führungsunterstützungsbasis (FUB) ein, welche durch Milizangehörige der Armee unterstützt werden. Dieses bereits etablierte Vorgehen hat sich durgehend bewährt; aufgrund der sich abzeichnenden Bedrohungsentwicklung ist es jedoch nötig, mehr gut ausgebildetes Personal einsetzen zu können.

Und genau hier setzt unser Cyber-Lehrgang an. Im vergangen August hat ein Pilot Projekt an der EKF S 64 in Jassbach begonnen. Insgesamt 18 Rekruten werden 40 Wochen lang Dienst leisten und geniessen insgesamt 800 fachspezifische Ausbildungsstunden, unter anderem an der ETH in Zürich und an der EPF in Lausanne. Sie beenden den Lehrgang als Wachtmeister.

Ab 2019 wollen wir pro Jahr zwei Lehrgänge mit je 25 Rekruten durchführen; übergeordnetes Ziel ist es, dass wir mit den Absolventen des Cyber LG bis Ende 2020 insgesamt rund 600 Milizangehörige eingeteilt haben, welche die Durchhaltefähigkeit der Profis im Bereich Cyber sicherstellen können.

Konkret bilden wir Spezialisten Computer Network Operations (CNO), Spezialisten militärischen Computer Emergency Response Teams (milCERT) sowie Spezialisten Cyber Defence aus. Damit sind wir in der Lage, Softwarewerkzeuge zu entwickeln, Cyber-Ereignisse und -Attacken zu analysieren sowie Schwachstellen zu erkennen. Wir sind ebenfalls in der Lage, technische und forensische Untersuchungen durchzuführen; und schliesslich können wir auch die Truppen im Felde mittels Lage-Analyse und -Darstellung beraten und ausbilden sowie nachrichtendienstliche Beiträge leisten.

Die anlässlich des Cyber-Lehrgangs vermittelte Ausbildung ist auch zivil anerkannt: Nach Abschluss des Lehrgangs kann dank des engen Schulterschlusses mit dem Berufsverband ICT-Berufsbildung Schweiz die Berufsprüfung zum «Cyber Security Specialist» mit eidgenössischem Fachausweis abgelegt werden.

Es ist nicht übertrieben, hier von einer Win-Win-Situation zu sprechen – weil die Armee das Vertrauen der Bildungslandschaft und der Wirtschaft mit einem Beitrag bezüglich Reduktion des Fachkräftemangels zurückzahlen kann. Mit anderen Worten: Unser bewährtes Milizsystem bietet enorme Chancen für die Bewältigung der Herausforderungen im Cyberraum. In diesem hochspezialisierten Bereich lassen sich die Vorteile des Milizsystems vollständig nutzen. Die Wirtschaft profitiert von den jungen Fachkräften aus dem Cyber-Lehrgang und wir profitieren später in den Wiederholungskursen von den Berufserfahrungen unserer Cyber-Soldaten und -Kader.

Ich möchte es zum Schluss noch einmal unterstreichen: Die primäre Aufgabe der Armee ist es, die eigenen Netze zu schützen. Dafür werden bis 2023 insgesamt 3,4 Milliarden Franken investiert in Rechenzentren VBS / Bund, ins Führungsnetz Schweiz und in die Telekommunikation der Armee. Mit diesen Massnahmen härten wir unsere Systeme, damit die Führungsfähigkeit der Armee über alle Lagen sichergestellt ist.

In diesem Sinne empfehle ich Ihnen in dieser Ausgabe auch den Artikel «Cybersécurité: la première ligne de défense». Ich wünsche Ihnen eine spannende Lektüre.

Chef der Armee
KKdt Philippe Rebord

Editorial

Sehr geehrte Leserinnen und Leser der Military Power Revue

Viele besorgte Beobachter der internationalen Lageentwicklung haben den nicht unbegründeten Eindruck, dass die Welt, aber auch ihre unmittelbare Umgebung sich in eine falsche Richtung bewege. Perzeptionen und Problemerfassungen sind das Eine, solide Lösungen sind das Andere. Diese lassen sich aber eigentlich nur mit dem Einschluss aller Betroffener und damit mit Kompromissen auf allen Seiten erreichen. Die zunehmende Polarisierung auf globaler, euroregionaler und auch nationaler Ebene steht dem aber oft im Wege.

Vor diesem Hintergrund steht auch die für die Schweizer Armee zentrale Frage der künftigen Luftverteidigung vor einigen Herausforderungen. Diese «Grossbaustelle» darf aber nicht von den Herausforderungen und Gefahren ablenken, welche der aktuellen Lage und deren absehbaren Entwicklungen inhärent sind. Dabei wird immer deutlicher, dass die klassischen sicherheitspolitischen Kooperationen und Allianzen unter Druck geraten, hinterfragt werden oder gar mit deren Aufkündigung gedroht wird. Dabei greift leider der traditionelle schweizerische Ansatz nach möglichst unabhängigen und autonomen Lösungsansätzen immer weniger. Von der «Black-Box» im Kampfjet bis zu komplexen Entscheidprozessen auf politischer Ebene nehmen Interdependenzen und auch Abhängigkeiten zu, die zudem durch die gesamte Palette der «Cyber-Dimension» verstärkt und/oder beeinflusst werden.

Die angesprochenen Herausforderungen an Kooperationen und Allianzen im Rahmen der europäischen Sicherheitsarchitektur zeigt Richard Rossmanith am Beispiel der NATO exemplarisch auf. Die Atlantische Allianz sieht sich einer Reihe von Herausforderungen gegenüber, die in ihrer Gesamtheit vermutlich komplexer sind als während des Kalten Krieges. Rossmanith lässt in seiner europäisch ausgelegten Perspektive klar erkennen, dass nicht nur das eigentlich seit 2008 zunehmend aggressivere Auftreten Russlands, sondern auch die unterschiedlichen Auffassungen zur bisher als unverbrüchlich beschworenen transatlantischen Allianz zu kaum mehr zu verbergenden Spannungen innerhalb des Bündnisses geführt haben.

Vor dem Hintergrund der volatilen Weltlage und weiterer möglicher Krisen strategischen Ausmasses stellt die Schulung des nationalen Krisenmanagements und seiner Prozesse ein wichtiges Instrument dar. Die Strategische Führungsübung SFU17 steht in der Reihe zunehmender Anstrengungen des Bundes und Organen der Kantone, die strategische Führungsfähigkeit anhand von konkreten Szenarien zu überprüfen. Erika Laubacher-Kubat zeichnet Aufgaben und Kontext der SFU 17 nach und zeigt die für den Bundesrat wichtigsten Erkenntnisse und Lehren auf. Diese sind bereits in die derzeit laufenden Vorbereitung der für 2019 geplanten Nachfolgeübung eingeflossen.

Gemeinhin nehmen die Nachrichtendienste für sich in Anspruch, die erste Verteidigungslinie eines Staates zu sein. Marc-André Ryter zeigt zurecht auf, dass der erfolgreichen Verteidigung gegen Cyber-Angriffe dieses Prädikat ohne Weiteres auch zuerkannt werden kann und muss. Mit gewisser Erleichterung kann festgestellt werden, dass nun auch die Schweiz dieser Bedrohung mit einigem Aufwand entgegentreten will. Die neue Cyberstrategie des Bundes sowie insbesondere auch die vom CdA im Vorwort aufgezeigten konkreten Massnahmen der Armee gehen sicher in die richtige Richtung.

Der Begriff «Strategie» wird gerne und oft angewandt, ohne sich kritisch zu hinterfragen, ob den beabsichtigten Vorgehensweisen auch wirklich eine Strategie zugrunde liegt und ob die Ziele damit auch wirklich erreicht worden sind. Mauro Mantovani und Marcel Berni stellen einen originellen Ansatz zur Strategieanalyse vor, der anhand der amerikanischen Strategie während des Vietnamkrieges praktisch erläutert wird.

Dem britischen Prime Minister Tony Blair hat man während seiner Regierungszeit vorgehalten, zur wenig transparenten Beeinflussung von Westminster (Parlament), ausländischer Partner und Kontrahenten sowie des eigenen Elektorats in seinem Amtssitz an der Downing Street vorwiegend sogenannte «Spin Doctors» zu beschäftigen. Wie Remo Reginold aufzeigt, ist das Phänomen der Spin Politics heute weiterentwickelt worden und wird unter anderen gerade auch von China sehr gezielt angewandt. Dabei zeigt er auf, dass damit in der politischen und strategischen Lagebeurteilung sowie Entscheidfindung umfassendere und teilweise neue Ansätze angezeigt sind.

Zeit- und inhaltgerechte Information ist eine wichtige Komponente im Krisenmanagement wie in der Führung militärischer Operationen. Zunehmend erfolgt Validierung und Bewertung der Glaubwürdigkeit des Inhalts wie auch der verbreitenden Institution durch Aussenstehende. Henrique Schneider zeigt vor diesem Hintergrund die Rolle und Verantwortung des Public Affairs Officers (PAO) auf. Zurecht weist er darauf hin, dass in diesem Spannungsfeld ethische Grundsätze wie auch die proaktive Interaktion mit relevanten Zielgruppen von wesentlicher Bedeutung sind.

Ich wünsche Ihnen eine anregende und hoffentlich interessante Lektüre und freue mich auf allfällige Rückäusserungen und Anregungen.

Der Chefredaktor der Military Power Revue
Urs Gerber

NATO's Challenges Today: A European Perspective[1]

Europe is currently facing several complex and dynamic security risks at the same time. Europeans are experiencing greater vulnerability and a feeling that the security architecture that they have gradually built over the last decades is more fragile than previously perceived. Never have security and prosperity in Europe depended so much on security and prosperity elsewhere. Geographic distance from a crisis no longer implies distance from its consequences. The terrorist attacks over the last years in Brussels, Paris, Barcelona, London, Berlin and many other places are tragic reminders of this. The role of criminal networks in the migration crisis is another example of the complexity of the security threats Europe is facing.

Richard Rossmanith

The late Eli Wiesel, Nobel Peace Prize Winner, and according to the Nobel Committee, "a messenger to mankind", said just before he died "The winds of madness are blowing". His Holiness Pope Francis said a while ago, "World War Three has started". The world is in a mess, isn't it? In the last decades while serving in the military, I do not remember many moments when so much of the world was in such trouble.

Most of the last five years, in Europe at least, has been taken up with noise, economic and political action against Russia, and some significant changes in NATO's posture because of Ukraine, and latterly with noise and failure to predict, appreciate and deal with the refugee crisis in Europe, and since a while with events in Syria, the Middle East and Northern Africa.

Among the many structural problems of the European Union, one is its lumbering, bureaucratic inefficiency in a crisis.

It is indefensible that European politicians and leaders took so long and were so indecisive over that crisis. Among the many structural problems of the European Union, one is its lumbering, bureaucratic inefficiency in a crisis. Some would even say that the EU is itself collapsing and that the refugee crisis, the EURO crisis, events in Poland and in Hungary, and British Brexit have all led to this situation.

Figure 1 NATO is faced with multiple challenges (Internet).

At this point in Europe's history, as the continent faces a complex and dynamic security environment, the alternative to closer cooperation appears to be a divided and weaker Europe. In the past, Europe has demonstrated its ability to emerge stronger from crisis. For the sake of Europe's security and prosperity, it is vital that it succeeds this time too. The security challenges posed by fragile and failed states call for a much stronger and better-coordinated European response. Indeed, many of the crisis Europe is facing have their origins in a belt of fragile or failed states on or close to its Southern borders. Europe needs a more strategic and comprehensive policy to address the interlinked issues of security, development, migration, and humanitarian assistance in fragile states.

In terms of stabilization efforts, Europe must seek to do more than eliminate the self-proclaimed Islamic State and other terrorist groups that currently threaten European security. Europe's longer-term goal must be to make sure that the Islamic State's successors, wherever they emerge, do not find fertile ground for their extremist ideologies in fragile or failed states in the future.

1 The text consists of an amended version of a key note talk at the Geneva Centre for Security Policy (GCSP) in early September 2018.

Figure 2 Interception of a Russian aircraft (The Independent).

Figure 3 Paris terror attacks (nytimes.com).

Complex Relationship with Russia

I strongly believe that, in its relationship with Russia, Europe must remain united in upholding respect for international law, democracy, and human rights. Through its actions in Ukraine and currently in Syria, Russia has deliberately contributed to a greater sense of insecurity in Europe. Even so, it will be in Europe's long-term security interests to develop a constructive relationship with Russia. There is no contradiction between safeguarding common interests in cooperation with Russia and standing firm on the commitment to international law and on fundamental principles of international relations.

And indeed, the unlawful annexation of the Crimean Peninsula in 2014 and the support to separatist forces in Eastern Ukraine by Russia unexpectedly brought back the use of military force to change borders as well as the security architecture of Europe. NATO reacted the same year after intensive debate and consultations at the Wales Summit. A substantive package of far reaching measures was decided to improve NATO's ability to cope with the emerging situation. Just about to end combat operations in Afghanistan, NATO started to adjust to the new strategic development heading towards collective defence including the respective military force posture.

It was more than obvious that Russia would become the dominating security challenge to the alliance in the upcoming years. However, terrorist attacks in 2015 and the following years in Paris, Brussels, London, Madrid, Berlin and many other European cities were clear evidence of another substantive threat to our security created by Islamic fundamentalism and terror networks.

For the first time in the history of the European Union's Common Security and Defence Policy, France requested the application of Article 42.7 of the Lisbon Treaty to defend against an armed attack. Article 42.7 is the solidarity clause stating that if a member of the European Union is the victim of "armed aggression on its territory" other states have an "obligation of aid and assistance by all the means in their power." Since then, French forces together with many more are in the fight against the Islamic State at home and abroad. Organized in a coalition of the willing with a strong U.S. lead, the international coalition has been successful in reducing and mainly defeating the Islamic State. Germany is contributing to this fight with reconnaissance aircraft, air-to-air refuelling capabilities and naval forces.

For the first time in the history of the European Union's Common Security and Defence Policy, France requested the application of Article 42.7 of the Lisbon Treaty to defend against an armed attack.

Decisions at the 2016 Warsaw Summit

Thus, at the Warsaw NATO Summit in 2016, two major topics were to be discussed: the situation in the Middle East and Northern Africa generating terrorist threats and the new strategic situation resulting from Russian aggression.

Figure 4 Change of Command at the Enhanced Forward Presence (The Baltic World).

The results of the Warsaw Summit are key to NATO's future:

- The dialogue with Russia was defined as a political objective equal to strengthening defence and deterrence capabilities.
- The heads of states and governments confirmed the measure decided at the Wales Summit and requested their full and timely implementation.
- NATO's missile defence has reached an important milestone; its Initial Operational Capability was declared that provides SACEUR with adequate command and control capabilities, sensors and effective operational means.
- The heads of states and governments emphasized the necessity to strengthen civil and military means for resilience and defence. Considering hybrid threats, critical infrastructure needs to be protected. At the same time national cyber defence capabilities are to be established.
- All measures to strengthen NATO's deterrence and defence capabilities are in line with the NATO-Russia Founding Act which should remain valid despite Russia's aggression.
- NATO Air Policing in the Baltic States will continue to operate on an increased level of forces.
- NATO maritime presence in the Baltic Sea was increased and close coordinated with all other NATO activities in the region.
- The NATO Response Force has increased its state of readiness and strength and has been turned into the "enhanced" NATO Reaction Force (eNRF). The force now encompasses amongst others land forces in division strength.
- The "spearhead" of the eNRF will be the Very High Readiness Joint Task Force (VJTF) composed of a brigade of land forces and elements of air, naval forces and special forces.
- In all eight Eastern NATO nations NATO Force Integration Units (NFIUs) have been established supporting the training of allied forces and supporting the reception and staging of reinforcements from abroad.
- The upgraded Multinational Corps North East in Stettin has become a part of NATO's Force Structure and has been developed into a High Readiness Corps becoming the corner stone for all NATO activities in Northeast Europe. In addition, a Multinational Division was established in Poland and another one in Romania, providing all together additional C2 capabilities supporting the NATO Command Structure with their regional expertise.
- For the southern flank a framework concept was developed to strengthen situational awareness and regional partnerships as well as to improve NATO's capabilities to project stability in this region. In February 2017 at a NATO Ministerial meeting, NATO Secretary General Jens Stoltenberg announced the establishment of an information sharing organization as part of the NATO Strategic Direction South (NSD-S) initiative. This Southern Hub has been established in 2017 at HQ Force Command Naples in Italy.
- NATO's political and military reaction capabilities have been improved through adjustments to decision making processes and military planning.

Additional measures were decided to improve deterrence and strengthen defence capabilities. In the Baltic States and Poland, an "enhanced Forward Presence" capability has been established starting in 2017. In each of the four nations, a multinational Battle Group is deployed on a rotational basis. Were an attack to be waged on one of NA-

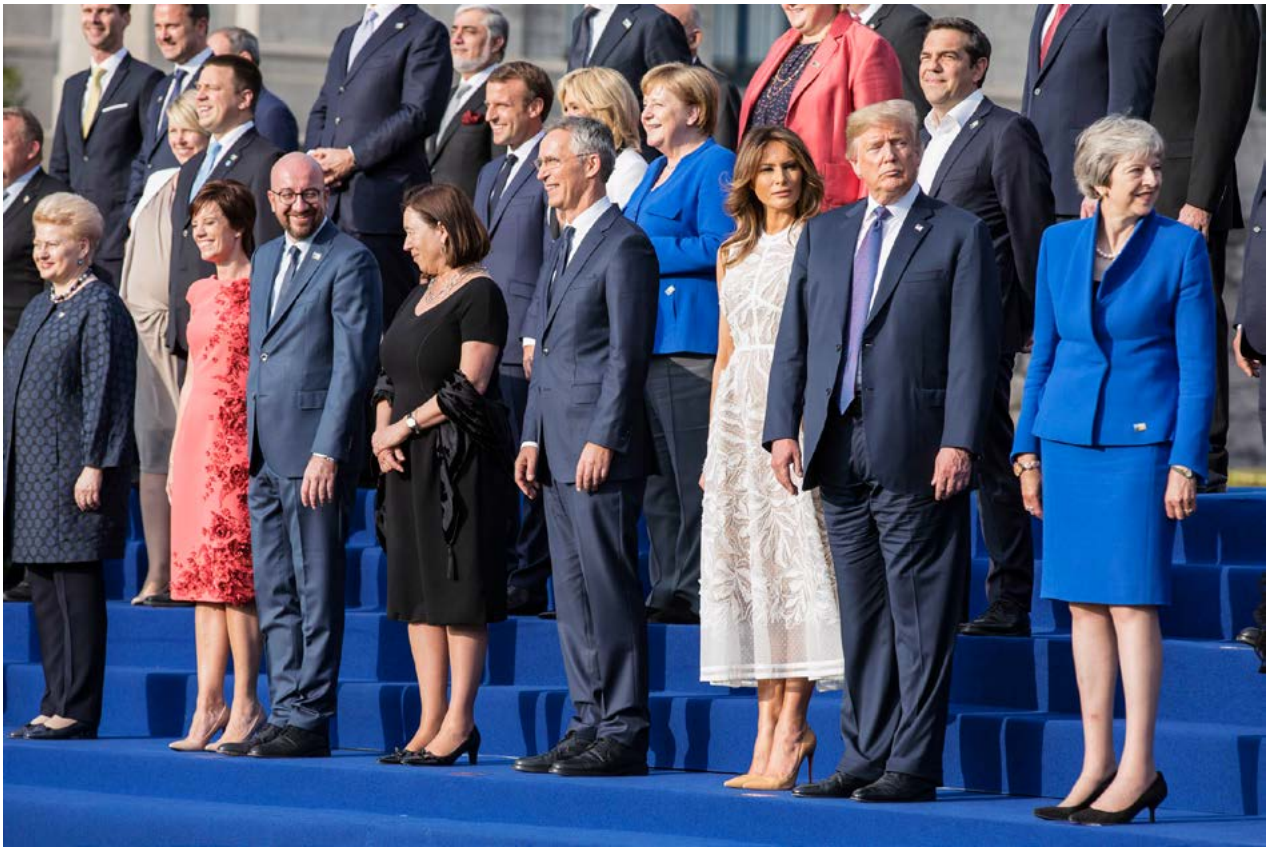


Figure 5 Heads of states at the NATO 2018 Brussels Summit (nato.int).

TO's frontline states, allied presence would more forcefully trigger NATO's Article 5 collective defence clause, where an attack against one is considered an attack against all. The U.S., the UK, Canada and Germany are in lead for the four battle groups. The German Army provides the bulk of a mechanized armoured battalion to Lithuania supported by Belgium, the Netherlands, Norway, Croatia, France, Luxemburg and Iceland. The battle groups are intensively training and exercising in close cooperation with the respective national and other NATO forces.

In Southeast Europe, a dedicated force has been created in accordance with the specific requirements of the Black Sea region. It includes a multinational brigade under Romanian lead reporting to the Multinational Division Southeast, supported by adequate air and naval forces.

At the Southern flank, NATO's objectives include to improve stability of its Southern neighbours. Following the logic "If my neighbours are more stable, we are more secure" the "Project Stability" initiative has been started. First activities have been conducted in Iraq leading towards a train and assist mission of Iraqi security forces. NATO AWACS are supporting the Counter IS operations from Turkish and international air space. Operation SEA GUARDIAN replaces the old article 5 operation ACTIVE ENDEAVOUR.

Structural Changes are in the Offing

Faced by substantive changes to roles, responsibilities and task, the headquarters of the NATO Command Structure are not any longer deemed adequate for the new missions. The heads of states and governments requested the Secretary General to initiate a functional review, to decide on adaptations in 2018.

NATO 3.0 is more than the sum of NATO 1.0 and NATO 2.0! NATO will enter new ground conceptionally, strategically and operationally.

Over the last years, NATO has developed substantially and will continue to do so. In analogy to commerce and industry, we may talk about NATO 3.0 to evolve within the next few years. NATO 1.0 was created for collective defence and to protect nations and NATO against existential threats from the Soviet Union. In the 90ies of the last century starting with the Balkan conflict, we saw NATO 2.0 mainly on operations to separate conflict parties, to establish safe and secure environments, to support, train and assist local security forces, to fight insurgents, and to stabilize fragile states in what we called earlier "out of area". Operations on the Balkans like KFOR or missions in Afghanistan – first ISAF and now RSM since 2014 – are cur-

Figure 6 President Trump and NATO Secretary General Stoltenberg at working breakfast at the Brussels NATO Summit (nato.int).

rently continuing. NATO 3.0 on the one side will be able to provide collective defence and maintain a credible deterrence. On the other side, we must be able to contribute outside NATO territory to stability in our neighbourhood and in regions of strategic interest. NATO 3.0 is more than the sum of NATO 1.0 and NATO 2.0! NATO will enter new ground conceptionally, strategically and operationally. The challenges will become broader and more demanding. At the same time, resources will remain rather limited.

Consequently, at the Wales Summit the heads of states and governments reiterated the already existing goal to provide adequate defence budgets, including the intent to increase budgets up to 2 percent of their Gross Domestic Product by the year 2025. Since then, in many nations we have seen growing defence budgets, even as this may not yet be enough. And indeed, questions like, how much is enough, how to spend the money most effectively, and which capabilities are to be provided in the most meaningful way by whom are delicate and extremely sensitive. Answers on these questions will be key for maintaining solidarity and cohesion in the Alliance.

Implications of a new U.S. Administration on the Alliance

However, nobody in 2014 or 2016 expected such discussions and developments we have seen starting on 20 January 2017. Almost eighteen months into the Trump administration, much of the traditional partnership between the United States and Europe is under severe, and in many ways unprecedented, stress. Up to this point, the relationship has been dominated by the myriad of issues on which Washington and European capitals diverge – whether the Paris climate agreement, the recognition of Jerusalem as the capital of Israel, withdrawal from the Joint Comprehensive Plan of Action with Iran, or more recently steel and aluminium tariffs.

The Trump administration certainly bears primary responsibility for what is perceived in Europe as a highly debateable alliance policy.

The Trump administration certainly bears primary responsibility for what is perceived in Europe as a highly debateable alliance policy. Yet, despite these differences, the United States and Europe are the most natural partners to confront the 21st century challenges facing our democracies. The threats from challengers such as China and Russia will only grow more unmanageable if transatlantic partners retreat into their corners. A way forward on areas of agreement, and areas where mutually beneficial bargains can be carved out, must be found despite the turmoil. Managing ongoing cooperation and avoiding a split over inevitable disagreements will be a key challenge for

Figure 7 NATO exercise in Poland as reaction to major Russian exercises (Breaking Defense).

policymakers on both sides of the Atlantic over the coming months and years.

Yet, there is a need to go beyond just managing ongoing cooperative efforts to also reinvent the transatlantic agenda – it is time for Washington and European capitals to develop a positive agenda that gives new meaning to the transatlantic alliance. This should include stepping up the U.S. engagement within Europe itself, strengthening the U.S. presence and engagement on Europe's periphery, and capitalizing on opportunities to work with Europe on addressing shared global challenges. This will require NATO to overcome two forms of discord – U.S.-European and intra-European – to ensure the future effectiveness of the Alliance.

Yet, there is a need to go beyond just managing ongoing cooperative efforts to also reinvent the transatlantic agenda – it is time for Washington and European capitals to develop a positive agenda that gives new meaning to the transatlantic alliance.

NATO summits are typically a forum for allies to move the dial on policy issues of mutual importance. The 2018 summit at Brussels was no different. There were many important initiatives on the table, including increasing Alliance readiness in the face of Russian aggression to NATO's east, implementing long-overdue military command structure reform, introducing a new training mission in Iraq, providing counterterrorism support to Afghanistan; and a new Black Sea regional security initiative. We have seen agreement and progress on several fronts, but there are real concerns about the long-term impact of fractures within the Alliance itself. Disunity within NATO not only prevents congruence around specific goals, it more seriously sends harmful signals to global challengers and competitors, such as Russia and China.

Defence spending was the key topic at the summit. Prior to and since taking office, President Trump has blasted European allies for not meeting their defence spending goals. In June, President Trump sent sharply-worded letters to leaders of Canada, Belgium, Denmark, Norway, and notably Germany, in which he wrote "continued German underspending on defence undermines the security of the Alliance." The letters, which follow similar formats, go on to state that "it will, however, become increasingly difficult to justify to American citizens why some countries continue to fail to meet our shared collective security commitments."

President Trump is not the first U.S. leader to come down hard on allies on defence spending, but the tone and timing of the letters has raised alarm among European leaders, with some reading them as a veiled threat that the United States might adjust its military presence in Europe if allies don't step up. Such a development could signal a shift to a more confrontational transatlantic relationship. It would also raise questions over the future of U.S. commitments to European security at a time of increased military and hybrid forms of Russian aggression.

Figure 8 German frigate «Schleswig Holstein» on operation in the Mediterranean Sea (n-tv).

In his farewell address in 2011, U.S. Defence Secretary Robert Gates criticized NATO allies for not spending enough on defence and warned of a "dim if not dismal future" unless more members contributed their fair share. Burden-sharing has remained a key sticking point in the Alliance, with the United States emphasizing valid concerns about chronic European underspending and its impact on credible defence. President Trump is not wrong to call out European allies whose defence spending is less than ambitious, but his caustic tone and singular focus on this one metric misses the mark on more valuable ways of measuring nations' contributions to collective defence. Allies such as Norway and Denmark, who currently do not meet the 2 percent mark, channel their funds directly into large-scale and impressive defence modernization plans, including procuring high-end capabilities such as U.S.-made F-35s and P-8 aircraft, that help fill Alliance capability gaps. Efforts on this front demonstrate the importance of going beyond the 2 percent metric to look, more importantly, at how and where money is spent. For instance, few nations spend 2 percent on defence, but their defence budgets go largely toward personnel costs rather than enhancing important wartime capabilities. To understand allied contributions to collective defence in totality, it is crucial to look at other important areas such as defence procurement, investment in research and development (R&D), and participation in NATO missions. At the summit in Brussels, European allies wanted to have a more nuanced and constructive conversation about defence expenditures. They more or less failed to make the case to broaden understanding around what it means to contribute to NATO.

Efforts on this front demonstrate the importance of going beyond the 2 percent metric to look, more importantly, at how and where money is spent.

Fortunately, other topics had a better fate at the summit. The U.S.-proposed Readiness Initiative was a major proposal that was up for discussion in Brussels. As already described, following Russia's annexation of Crimea in 2014, NATO placed rotational multinational battalions in the three Baltic States and Poland as a means to deter and defend against potential Russian aggression. Today's enhanced Forward Presence is an important first step, but the forces are small in number. To ensure credible defence and rectify slow deployments in a contingency, NATO must work to improve readiness across the Alliance. It is in this context NATO defence ministers agreed in June to support the "Four Thirties" initiative. In a nutshell, this initiative is a military readiness plan that would see the Alliance have by 2020 30 land battalions, 30 air squadrons, and 30 navy vessels, ready for deployment in 30 days or less. The initiative will support U.S. priorities in stepping up readiness to ensure that the Alliance is equipped to rapidly reinforce when and where it may need to. The multi-domain approach to territorial defence is an important feature and would likely aim to respond to some of the threats posed more recently by Russia in the air and maritime domains, as demonstrated during its ZAPAD 17 military exercise. As the initiative is adopted, next steps will include designating troops, establishing a reporting mechanism, and planning for readiness exercises.

Alongside readiness, the Alliance aims to advance long-overdue command structure reform with the creation of two new commands – one in Norfolk, Virginia, to ensure U.S. maritime access across the Atlantic, and the other called Joint Support and Enabling Command in Ulm, Germany, focused on logistics in Europe and ensuring allied forces can get to where they need to go. The agreement on command structure reform were critical to securing improved military readiness for the Alliance and will help ensure the United States' ability to reinforce European forces.

Reports of a Pentagon study exploring the cost of withdrawing U.S. troops from Germany set off alarm bells in European capitals over the potential repositioning of U.S. troops across or out of Europe. Such a move would not only have military ramifications, but political ones as well. Although the White House has emphasized that the Pentagon assessment of U.S. troop deployments is routine, it has added to Germany's sense of unease following hostilities with President Trump at the recent G-7 meeting in Canada, and the tense relationship between the U.S. president and the German chancellor – Angela Merkel.

A fundamental misalignment in threat perceptions now exists within the Alliance, and this inability to agree on what the threat is makes it harder for NATO allies to collectively grapple with and adapt to the array of complex security challenges they face.

Future Challenges

Tension between U.S. and European leaders is not the only point of friction within the Alliance. Emergency European Council meetings in June and July 2018 demonstrated ongoing disagreements among European Union members of the Alliance over what to do about flows of refugees and migrants to Europe. The meetings saw EU leaders rush through a bunch of measures to strengthen external borders and internal controls over migration after pressure from Italy's new government and Germany's rather fragile coalition. Although French President Emmanuel Macron praised the "European cooperation" that enabled a deal to come together, Southern European states remain frustrated by what they see as unfair burden-sharing on migration issues, and a lack of will by other allies to carry more weight by taking in greater numbers of refugees. Europe's migration issue is illustrative of a larger and more concerning linchpin for NATO. While northern and eastern allies are concerned about Russian aggression to the east, southern allies are focused on migration and border concerns.

A fundamental misalignment in threat perceptions now exists within the Alliance, and this inability to agree on what the threat is, makes it harder for NATO allies to collectively grapple with and adapt to the array of complex security challenges they face. If this misalignment cements, it will make it very difficult for NATO to act together in the face of an immediate and direct threat, which risks undermining the collectivity and credibility underpinning NATO's defence clause.

Richard Rossmanith

Lieutenant General ret., German Army. He held several NATO posts in Brussels, Karup/ Denmark, SHAPE and Heidelberg. In three operational tours, he served in Bosnia-Hercegovina, Kosovo and at ISAF HQ in Afghanistan. In his last assignment, he was in command of the Multinational Joint Headquarters of the German Armed Forces with possible commitments to NATO, the European Union or the United Nations.

E-Mail: Richard.Rossmanith@t-online.de

Erfahrungen und Lehren der Strategischen Führungsübung 2017 (SFU 17)

Am 16. und 17. November 2017 führte die Bundeskanzlei im Auftrag des Bundesrates eine Strategische Führungsübung (SFU 17) durch. Das Thema der Übung war ein Terrorangriff auf die Schweiz. Die Übung wurde in enger Kooperation mit dem Kanton Genf durchgeführt. Evaluiert wurden die Reflexion auf strategischer Ebene, die Arbeit der Krisenstäbe, die Koordination, das Vorgehen und die Kommunikation. Der Bundesrat hat im Mai 2018 die Auswertung und die Empfehlungen aus der SFU 17 verabschiedet.

Erika Laubacher-Kubat

Szenario

Die Szenarien für eine SFU gehen von Risiken aus, die in unserer Gesellschaft tatsächlich bestehen. Die Krise muss so gewichtig sein, dass strategische Massnahmen auf Stufe Bundesrat zu deren Bewältigung nötig sind, und eine Krise nicht nur auf lokaler oder kantonaler Ebene bewältigt werden kann. Angesichts der aktuellen Bedrohungslage lag es auf der Hand, für die SFU 17 das Thema Terrorismus zu wählen. Die Vorgabe an das Szenario war, dass dieses realistisch sein musste und keine «Künstlichkeiten» (zum Beispiel ein Pestkranker läuft an einer Schule entlang und gleichzeitig stürzt in der Nähe ein Flugzeug ab) enthalten sollte. Startschuss für die Übung war am 16. November 2017 kurz nach 7 Uhr, als ein Strommast in unmittelbarer Umgebung des Kernkraftwerks Mühleberg gesprengt wurde und es in der Folge zu einem Anlagenotfall im Werk kam. Zeitgleich wurde am Flughafen in Genf eine Bombe entdeckt, die anschliessend entschärft werden konnte. Die Ereignisse überschlugen sich ab 9.30 Uhr mit einem Terroranschlag im unterirdischen Bahnhof CEVA Eaux-Vives in Genf und einer Geiselnahme im Gebäude der Vereinten Nationen in Genf.

Alle Angriffe wurden von der fiktiven Terrororganisation Global Liberation Front (GLF) durchgeführt. Unter der Führung der sog. «Triade der Erleuchteten» vereint die GLF konfessions- und kulturübergreifend Personen, die von den etablierten Weltreligionen und dem kapitalistischen System enttäuscht sind. Nach Ansicht der GLF tragen die Grossmächte, das globalisierte Finanzsystem und die internationalen Organisationen als deren Handlanger die Schuld daran, dass die Welt zu einem «gottlosen Ort des Mammons» verkommen sei. Die fiktive Terrororganisation war im Herbst 2017 gemäss Szenario mit Anschlägen in europäischen Hauptstädten medienwirksam in Erscheinung getreten. Drohungen in allgemeiner Form wurden gegen internationale Institutionen und Organisationen ausgesprochen. Somit rückte die Schweiz als Sitzstaat der UNO – insbesondere Genf – ebenfalls in den Fokus der GLF.

Diese Anlage erlaubte es, die Koordination und die Absprachen zwischen den verschiedenen Krisenstäben zu testen, ebenso die Fähigkeit, ein umfassendes Lagebild zu schaffen.

Anspruchsvoll war für die Teilnehmenden die gleichzeitige Bewältigung mehrerer Ereignisse: eine potenzielle radioaktive Verstrahlung im Raum Bern, Terroranschläge und eine anhaltende Geiselnahme in der UNO in Genf. Diese Anlage erlaubte es, die Koordination und die Absprachen zwischen den verschiedenen Krisenstäben zu testen, ebenso die Fähigkeit, ein umfassendes Lagebild zu schaffen. Die einzelnen Ziele der Übung waren: a) Überprüfung der Mechanismen der Zusammenarbeit zwischen Bundesrat und Kantonsregierung, b) Klärung der Zusammenarbeit und der Schnittstellen zwischen operativen und strategischem Krisenmanagement auf Stufe Bund, c) Prüfung der Arbeit der verschiedenen Krisenstäbe und d) Prüfung der internen und externen Krisenkommunikation von Bund, Kantonen und Partnern.

Die SFU 17 als Teil der Gesamtplanung Grosser Übungen

Der Bundesrat hat im Januar 2016 eine von der Bundeskanzlei und vom Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) vorgelegte

Abbildung 1 Regieraum SFU 17, Kaserne Bern. Das integrale Projektteam am Regietisch während der Übung (BK).

Abbildung 2 Regieraum SFU 17, Kaserne Bern. Stabsoffiziere aus dem Stab Operative Schulung verfolgen den Verlauf der Übung und erstellen die Lage zuhanden der Regie bzw. der Übungsleitung (BK).

Abbildung 3 Regieraum SFU 17, Kaserne Bern. Besprechung der Projektleiterin mit dem Chef Regie dem Chef Beobachtung und dem Chef Lage mit dem Ziel der Synchronisierung der nächsten Übungsphase (BK).

Abbildung 4 Die Chefin Kontakt Stab (stehend) mit ihrem Team aus dem EDA. Der Kontaktstab Ausland simulierte den Druck des Auslands auf die Schweiz in der Übung (BK).

Gesamtplanung für die Grossen Übungen in der Schweiz bewilligt. Kern dieser Planung ist, dass künftig Strategische Führungsübungen (SFU) und Sicherheitsverbundsübungen (SVU) in Planung und Durchführung aufeinander abgestimmt werden. So sollen diese beiden Übungen innerhalb einer 4-Jahres-Periode ein zusammenhängendes Szenario haben.

Das Ziel dieser Verknüpfung ist es, eine verbesserte Koordination zwischen den Übungen bezüglich Organisation, Inhalt und Methodik herbeizuführen sowie Ressourcen optimal zu nutzen. Ziel ist auch, aus den Resultaten der SFU 17 Lehren zu ziehen, Empfehlungen für die Krisenbewältigung zu formulieren und diese in der SVU 19 nochmals zu behandeln. Die SFU 17 als Teil der Gesamtplanung durchzuführen, bedeutete, dass die Konzepte der SFU 17, der SVU 19 und der Gesamtnotfallübungen (GNU) 17 und 19 zu verknüpfen waren, was sich konkret in der Erarbeitung eines zusammenhängenden Szenarios sowie der Planung, Umsetzung und Auswertung der vierjährigen Übungssequenz manifestierte. Diese Planung erlaubt auch grosse Armeeübungen und teilweise grössere interkantonale Übungen zu integrieren.

Die Qualität des Szenarios und der Übungsumwelt (Kontaktstelle, Medien, soziale Medien, Website) sowie die Funktionalität von Beobachtung und Regie waren dank der Expertise hoch.

Die Bundeskanzlei leitete das integrale Projektteam der SFU 17. Dieses setzte sich aus Expertinnen und Experten aus dem Generalsekretariat des VBS, dem Bundesamt für Bevölkerungsschutz (BABS), der Armee (Operative Schulung), dem Bundesamt für Polizei (fedpol), dem Nachrichtendienst des Bundes (NDB), dem Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) dem Führungsstab Polizei und dem Kanton Genf zusammen. Dieses Team mit Expertinnen und Experten aus verschiedenen Fachbereichen hat zur Akzeptanz der Übung beigetragen. Die Qualität des Szenarios und der Übungsumwelt (Kontaktstelle, Medien, soziale Medien, Website) sowie die Funktionalität von Beobachtung und Regie waren dank der Expertise hoch.

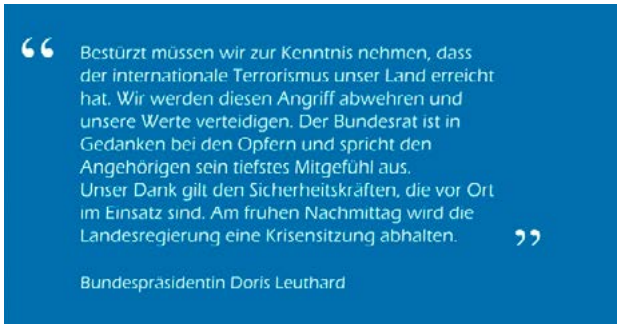


Abbildung 5 Ein Tweet von Bundespräsidentin (2017) Doris Leuthard während der Übung (BK).

Abbildung 6 Die Mitarbeitenden der Medienzelle SFU 17 bei der Arbeit (BK).

Eine etwas andere SFU

Die SFU 17 wurde als zweitägige Stabsübung konzipiert. Übungsleiterin war Bundespräsidentin Doris Leuthard und die Generalsekretärenkonferenz (GSK) agierte als operatives Aufsichtsgremium. Die Übung war realitätsnahe angelegt und es fanden keine vorbereitenden Veranstaltungen statt. Die Übung wurde ohne Unterbruch während 29 Stunden gespielt. Die Ereignisse der SFU 17 wurden per E-Mail und Telefon oder auf der Übungswebsite mit eigens kreierten Radio-, Presse- und Social-Media-Beiträgen sowie offiziellen (Medien-) Mitteilungen eingespielt. Die Teilnehmenden reagierten in eigenem Ermessen auf die gespielten Ereignisse.

Die Medienzelle bereitete für die SFU 17 fast 5 000 Posts vor, ein Bruchteil, von dem, was in der Realität passieren würde, doch genug, um die Medienwelt der Sozialen Medien abzubilden.

Die SFU 17 bemühte sich um einen intensiven Einbezug von Sozialen Medien: Ein Team simulierte auf einer Website die Social Media Community # Terror in Bern und Genf und forderte die Teilnehmenden der SFU 17 zum Reagieren heraus. Diese konnten via die Übungswebsite auch ihre Stellungnahmen und Tweets abgeben. Ein Wirrwarr aus Emotionen, Gerüchten und Berichten von Augenzeugen wurde über die Übungswebsite geschaffen:

07.15 Der erste Post: @Tourdumonde: «Ruban de police et plusieurs policiers à #GeneveAeroport #GVA»

09.11 Die Terroristen kommunizieren auch über die Sozialen Medien: Bösartig melden sie: «GVA you got lucky today. YOUR TIME WILL COME. rainofFIRE»

14.30 @Alertswiss: Lage in #Mühleberg weiterhin stabil. Die UserInnen glauben's nicht: @Ferdinandli_32: «Ich trinke kein Wasser mehr aus dem Hahn!»

05.04 Im Drehbuch wurde doch noch eine Geisel umgebracht. Die ganze Welt ist entsetzt! #FightTerror

Die Medienzelle bereitete für die SFU 17 fast 5 000 Posts vor, ein Bruchteil, von dem, was in der Realität passieren würde, doch genug, um die Medienwelt der Sozialen Medien abzubilden. Zusätzlich zu den Sozialen Medien wurden stündliche Radiosendungen produziert und ebenso wurde die nationale und internationale Presse abgebildet.

Auswertung SFU 17

Die Daten für die Auswertung wurden während des gesamten Übungsverlaufs gesammelt. Insgesamt waren während der SFU 17 ca. 60 instruierte Beobachterinnen und Beobachter in Bern und in Genf in Einsatz. Je ein Beobachterteam, bestehend aus jeweils drei Personen – zwei verwaltungsinternen Personen und einem Vertreter des Stabes Operative Schulung – beobachtete jeweils einen Krisenstab. Insgesamt verfassten die Beobachterteams 24 Berichte. Als Quellen der Auswertung standen dem Auswertungsteams zusätzlich zu den Berichten der Beobachtenden die in der Übung erstellten Produkte zur Verfügung wie Bundesratsanträge, Sitzungsprotokolle, die Inhalte der elektronischen Lagedarstellung (ELD), Medienmitteilungen oder Social-Media-Beiträge und die E-Mails der Teilnehmenden.

Das Szenario der SFU 17 hat die beteiligten Krisenorgane und Verwaltungseinheiten gefordert. Es hat die Stärken der Bundesverwaltung bei einer Krisenbewältigung aufgezeigt, aber auch, dass in gewissen Bereichen Verbesserungspotential besteht.[1]

Erkenntnisse und Empfehlungen

Der Bericht zeigt auf, dass der Bundesrat und die Krisenstäbe sich intensiv und engagiert mit der Bewältigung der Krisenszenarien auseinandersetzten. Während der Übung wurden tausende E-Mails von den Teilnehmenden in den verschiedenen Verwaltungseinheiten ausgetauscht, 26 Krisenstäbe waren im Einsatz, und die Beobachtenden lobten die «positiv ernsthafte» Stimmung in den Krisenstäben. Der Bundesrat kam im Laufe der Übung zu zwei

1 Der gesamte Bericht zur Auswertung SFU 17 finden Sie unter: https://www.bk.admin.ch/bk/de/home/dokumentation/fuehrungsunterstuetzung/strategische-fuehrungsuebung--sfu-.html

ausserordentlichen Sitzungen zusammen und beschloss die Wiedereinführung der Grenzkontrollen und die Unterstützung der zivilen Behörden durch Angehörige der Armee. Um 14.30 Uhr am ersten Übungstag wandte sich Bundesrätin Simonetta Sommaruga in Genf mit einem Statement ein erstes Mal an die Öffentlichkeit. Nach der ersten Bundesratssitzung fand die erste offizielle Medienkonferenz mit Bundespräsidentin Doris Leuthard in Bern statt.

Beispielsweise gab es Unklarheiten über die Zuständigkeiten bei der Bewältigung der Geiselnahme der UNO zwischen der Zentrale EDA, der Mission Schweiz in Genf, der Einsatzorganisation fedpol/SOGE und der Kantonspolizei in Genf.

In der SFU 17 fand mit dem Kanton Genf eine enge Koordination auf politischer und operativer Stufe statt. Die Kontakte wurden genutzt, um Informationen zu erhalten, Handlungen zu koordinieren und Zuständigkeiten zu klären. Trotzdem gab es Unklarheiten bezüglich Zuständigkeiten und Prozessen, die immer wieder diskutiert wurden. Fachwissen war zwar vorhanden, gelangte aber nicht auf die Entscheidungsebene. Beispielsweise gab es Unklarheiten über die Zuständigkeiten bei der Bewältigung der Geiselnahme der UNO zwischen der Zentrale EDA, der Mission Schweiz in Genf, der Einsatzorganisation fedpol/SOGE und der Kantonspolizei in Genf. Weitere Unsicherheiten herrschten beim Antrag für militärische Unterstützung vor oder auch bei der Vorgehensweise und den Begrifflichkeiten für eine Grenzschliessung respektive Grenzkontrolle. Aufgrund unterschiedlicher Auffassungen bezüglich Zuständigkeiten und Prozesse ging in Bern wie in Genf viel wertvolle Zeit verloren.

Als Empfehlung aus der SFU 17 sollen die Departemente und die Bundeskanzlei deshalb Prozesse und Zuständigkeitsregelungen klären, die in der Übung zu Unsicherheiten geführt haben. (z. B. Grenzschliessung / Einführung von Grenzkontrollen, Antrag auf militärische Unterstützung, Verantwortlichkeiten bei Zusammenarbeit mit internationalen Organisationen). In der Kommunikation hingegen funktionierten die Absprachen im Führungsstab Polizei mit den kantonalen Polizeikorps und fedpol gut.

Des Weiteren hat der Bundesrat die Bundeskanzlei beauftragt, die Organisation des Krisenmanagements auf Stufe Bund zu überdenken, insbesondere eine mögliche Reduktion der Anzahl Stäbe und das Zusammenwirken sowie die Besetzung der jeweiligen Stäbe zu überprüfen.

Als für die Krisenbewältigung wirksames Instrument erwies sich die Einsetzung eines interdepartementalen Ad-hoc-Krisenstabs, welcher von der Bundespräsidentin geleitet wurde und dem Schlüsselpersonen aller Departemente angehörten. Der Ad-hoc Krisenstab trug dazu bei, die Informationen der verschiedenen Behörden zu vervollständigen und ihr Vorgehen aufeinander abzustimmen. Als eine Empfehlung aus der SFU 17 gilt es nun, das Verfahren zur Einberufung des Ad-hoc-Krisenstab, die Anforderungen an diesen und seine Zusammensetzung besser zu definieren, sodass er seine koordinierende Rolle effizient und zeitgerecht ausführen kann. Des Weiteren hat der Bundesrat die Bundeskanzlei beauftragt, die Organisation des Krisenmanagements auf Stufe Bund zu überdenken, insbesondere eine mögliche Reduktion der Anzahl Stäbe und das Zusammenwirken sowie die Besetzung der jeweiligen Stäbe zu überprüfen. Das dezentrale System des Krisenmanagements mit seinen vielen Stäben bedeutet auch, dass einige Schlüsselpersonen mehrere Hüte tragen. Hier gilt es die Zusammensetzung der jeweiligen Stäbe zu überprüfen und koordinierende Stellen zu berücksichtigen, so dass Überkreuz-Vertretungen vermieden werden. Der Bundesrat wünscht explizit keinen permanenten Krisenstab, sondern will die Verantwortung den jeweiligen Krisenstäben aus den Departementen (und Kantonen) überlassen. Diese Stäbe sind ausgelegt um ein definiertes und spezifisches Problem rasch zu lösen, ohne den Rest der Verwaltung über Gebühr zu belasten. Die Herausforderung in der SFU 17 war, dass viele Stäbe gefordert waren, was einer zeitgerechten und umsichtigen Koordination bedurfte.

Die Krisenorganisationen gingen die Problemerfassung und Lagebeurteilung sehr unterschiedlich an.

Ein aktuelles, qualitativ gutes und einheitliches Lagebild ist die Grundlage von guten Entscheiden. Bei den sich überschlagenden Ereignissen war es für die Teilnehmenden eine Herausforderung, sich ein umfassendes und für die strategische Ebene zweckmässiges Bild der Krisenlage zu verschaffen. Die Krisenorganisationen gingen die Problemerfassung und Lagebeurteilung sehr unterschiedlich an. Einige Stäbe fokussierten ausschliesslich auf die Lageberichte des NDB, ohne sich ein eigenes Bild der gesamten Lage zu machen. So fehlte oft eine umfassende Lagebeurteilung unter Einbezug der eigenen Fachebene. Wieder andere zählten schlicht Ereignisse auf, ohne sie zu einem gesamtheitlichen Lagebild zu verdichten oder die Lage zu beurteilen. Nochmals andere nahmen zwar nach der Problemerfassung eine Lagebeurteilung in Angriff, aber gingen nicht in die Tiefe und erkannten keine Querverbindungen zwischen den Ereignissen oder konnten keine Auswirkungen auf andere Themenfelder ausmachen.

Verbesserungspotential wurde auch bei der Abwicklung der Stabsarbeit und der Kommunikation festgestellt. Um künftig gegen innen und aussen zielgerichteter und rascher kommunizieren zu können, muss das Krisenkommunikationskonzept der BK konsequent angewendet wer-

den. Die sozialen Netzwerke sollen künftig auch in der Krise stärker als ergänzendes Kommunikationsmittel eingesetzt werden, um die breite Öffentlichkeit schnell und zielgruppengerecht zu informieren. Der Bundesrat hat die BK und die Departemente beauftragt, zu prüfen, ob das aktuelle Krisenkommunikationskonzept alle notwendigen Aspekte der Verwendung der sozialen Medien in einer Krise (mitunter auch das Medien-Monitoring) genügend abdeckt, und ob diese Aspekte auch allen Verantwortlichen bekannt sind.

Rolle der Armee

Die Armee ist ein wichtiger, anerkannter und verlässlicher Partner des Sicherheitsverbunds Schweiz. Der Sicherheitsverbund Schweiz bündelt zivile, militärische sowie staatliche und privatwirtschaftliche Mittel, um die aktuellen und künftigen Sicherheitsbedrohungen der Schweiz zu bewältigen. Über alle Phasen der SFU 17 konnten wir auf die Unterstützung der Armee zählen. So waren Vertreter der Berufs- und auch der Milizkomponente der Operativen Schulung Teil des integralen Projektteams und haben Beiträge in der Planung, Durchführung und Auswertung der SFU 17 erbracht.

So konnte die Projektorganisation vom Wissen bezüglich des Anlegens von Übungen, der Erarbeitung des Szenarios und Drehbuchs sowie des Aufbaus der Regieorganisation profitieren. Während der SFU 17 haben Offiziere der Operativen Schulung die «Mixed»-Beobachterteams ergänzt und mit den Analysen aus den Beobachtungen zur zielgerichteten Auswertung der Übungen beigetragen.

Ausblick

Eine interdepartementale Arbeitsgruppe mit Vertretern aus allen Departementen unter Leitung der Bundeskanzlei befasst sich nun mit den Folgeaufträgen aus der SFU 17. Es gilt, den Schwung der SFU 17 zu nutzen um die Empfehlungen umzusetzen und das Krisenmanagement auf Stufe Bund vor allem bei komplexen Krisen zu stärken.

Der Bundesrat hat entschieden, dass das Szenario der SFU 17 in der SVU 19 fortgeführt werden soll.

Im November 2019 findet die SVU 19 statt, in welcher gewisse Aspekte aus der SFU 17 nochmals vertieft werden können. Es gilt diese Synergiewirkung zu nutzen. Bei einer SVU wird das Krisenmanagement im gesamten Sicherheitsverbund Schweiz getestet, wodurch Bund, Kantone und Dritte ihre Strukturen und Abläufe überprüfen können. Der Bundesrat hat entschieden, dass das Szenario der SFU 17 in der SVU 19 fortgeführt werden soll. Das Thema ist eine anhaltende Terrorbedrohung. Diese erfolgt durch Angriffe gegen kritische Infrastrukturen, erpresserische Forderungen und drohende Anschläge. Die SVU 19 soll unter anderem überprüfen, wie die Schweiz eine länger andauernde Terrorbedrohung bewältigen kann und ob die betroffenen Organisationen rasch einsatzbereit und durchhaltefähig sind. In vier Teilprojekten (Bevölkerungsschutz, Polizei, Armee und Krisenkommunikation) wurden zusätzlich spezifische Ziele festgelegt. Bis zur Stabsrahmenübung im November 2019 stellt die Übungsleitung vier periodische Lageberichte zur Verfügung, mit denen sich die Teilnehmenden innerhalb ihrer Organisation befassen können. Im Anschluss an die SVU 19 wird die erste Übungssequenz (2016–2019) evaluiert und in der Folge dem Bundesrat eine Planung Grosser Übungen für die weiteren acht Jahre vorgelegt werden.

Erika Laubacher-Kubat

Dr. phil., Stellvertretende Leiterin der Sektion Strategische Führungsunterstützung, Bundeskanzlei; Projektleiterin der SFU 17

E-Mail: Erika.Laubacher-Kubat@bk.admin.ch

Cybersécurité : la première ligne de défense contre l'impact de l'intelligence artificielle

Durant les prochaines années, le cyberespace va être confronté au développement de l'intelligence artificielle. Celle-ci va grandement accroître le potentiel d'efficacité des cyberattaques et obligera ainsi tous les utilisateurs du cyberespace à adapter leur protection. Les forces armées en particulier feront face à des défis considérables afin de maintenir leurs capacités opérationnelles, même si elles pourront aussi profiter de l'intelligence artificielle dans de nombreux domaines.

Marc-André Ryter

Introduction

Le but de cet article est de démontrer l'importance de la cybersécurité en tant que protection contre les risques accrus qui vont être générés par le développement et l'intégration de l'intelligence artificielle (IA) dans le cyberespace. L'article se concentre sur la dimension technique de l'évolution en cours, et sur ce qu'elle implique pour les forces armées. Toutefois, certaines considérations éthiques ou concernant la place de l'homme dans un univers de machines au sens philosophique seront inévitables. Ce qui se passe dans le cyberespace peut amener des progrès fantastiques mais peut aussi à tout moment devenir une menace de première importance. Les risques impliqués sont susceptibles de remettre en cause la paix et la sécurité internationales.

L'IA va révolutionner la perception et la mise en œuvre de la cybersécurité, qui va devenir une tâche collective et permanente.

Cette évolution est inéluctable et un retour en arrière est impensable en tant que tel. L'engagement de nouvelles technologies a lieu dans tous les domaines de la vie des individus et des sociétés[1], et les possibilités de l'IA sont telles que les avantages justifieront beaucoup de compromis. Les progrès dans l'informatique sont à la fois porteurs d'espoirs et dangereux. Les nouveaux outils peuvent promouvoir les libertés et le développement, le progrès et le bien-être, mais aussi l'oppression, la fraude, les manipulations et les contrôles. Les progrès technologiques vont profiter à tous, aux puissants comme aux faibles, aux autorités légales comme aux groupes criminels. De ce fait, les hiérarchies et l'autorité peuvent être renforcées ou affaiblies.[2] Ceci aura un impact important sur la nature des conflits futurs. Si l'on veut maîtriser la croissance des nouvelles technologies et surtout leurs applications, il est important d'anticiper et d'intégrer les risques aux opportunités.

L'IA va révolutionner la perception et la mise en œuvre de la cybersécurité, qui va devenir une tâche collective et permanente. Les Etats et les infrastructures critiques sont déjà aujourd'hui victimes d'attaques qui visent à obtenir toutes sortes d'avantages, qu'ils soient politiques, militaires ou économiques. L'espace numérique est donc déjà un véritable espace de confrontation[3] et les cyberattaques sont devenues le lot quotidien d'une sorte de nouvelle guerre froide[4]. Les sociétés dans leur globalité, en raison de leurs interconnections croissantes, deviendront toujours plus vulnérables. Les conflits entre Etats, entreprises ou individus pourraient prendre des formes jusqu'à maintenant ignorées. Mais une chose est sûre, qu'ils soient nationaux ou internationaux, politiques ou économiques, les conflits auront une dimension cyber croissante. L'acteur qui réussira à prendre le dessus dans le réseau prendra le dessus sur son adversaire.[5] Les cyberattaques deviendront à la fois plus précises et plus rapides. La cyber-

1 Ryter, Marc-André: La 4ème révolution industrielle et son impact sur les forces armées, MPR I/17, pp. 50–62.

2 Rid, Thomas: The Rise of the Machines, Scribe Publications, London, 2016, p. 298.

3 Ryter, op. cit., pp. 58–60.

4 Straub, Jeremy: Artificial Intelligence is the weapon of the next Cold War, The Conversation, 29.01.2018, disponible sous https://theconversation.com/artificial-intelligence-is-the-weapon-of-the-next-cold-war-86086, p.2

5 Anil, Suleyman: How to integrate cyber defence into existing defence capabilities, in ANGELI, Franco (Dir.): International Humanitarian Law and New Weapon Technologies, International Institute of Humanitarian Law, San Remo, 2012, p. 152.

Figure 1 Exemple d'un grand centre de stockage de données en Islande, qui montre que le cyberespace se base sur des infrastructures physiques qui peuvent être ciblées (https://www.cio.com/article/2368989/data-center/100152-10-more-of-the-world-s-coolest-data-centers.html#slide8, consulté le 20.07.2018).

sécurité qui doit être élaborée en réponse à cette évolution doit être vue comme une construction de multiples éléments qui se complètent afin de créer une architecture de sécurité globale pour le cyberespace. Les capacités militaires dans ce domaine peuvent et doivent constituer un élément important de cette architecture. La portée des menaces numériques, surtout lorsqu'elles fonctionnent avec de l'IA, n'est pas encore bien comprise. Pour le moment, il faut la plupart du temps extrapoler les risques pour les forces armées des risques pour les domaines civils, afin d'imaginer quelles actions belliqueuses un agresseur pourrait entreprendre.

C'est pourquoi les forces armées, y compris l'armée suisse, doivent être à la pointe de la cybersécurité. Celle-ci peut être considérée comme le premier niveau de la dissuasion, dans le sens d'une prévention d'une invasion du territoire par des forces armées étrangères. Ces dernières pourraient renoncer à leurs actions au sol si elles ont été incapables d'affaiblir ou de paralyser les forces armées du pays ciblé en amont des opérations. La résilience qui vise à une récupération rapide de la capacité d'action, doit permettre l'engagement des moyens après ou malgré le fait d'avoir subi une cyberattaque et d'avoir essuyé certains dommages. Il apparaît donc évident que les forces armées ont un intérêt considérable à contribuer à la cybersécurité. Les nouvelles technologies qu'elles utiliseront dans le futur devront être sécurisées car elles devront être à même de remplir leur mission, même dans un environnement cyber dégradé.

Enjeux liés au développement de l'intelligence artificielle

L'enjeu central sera donc de savoir gérer l'évolution en cours ainsi que ses conséquences pour les forces armées, puisque cette évolution est inéluctable. Il faut identifier les changements de paradigmes, ce qui va effectivement changer la nature de la vie sociétale et des rapports entre les pays. Les caractéristiques du monde de demain seront la volatilité, l'incertitude, la complexité et l'ambiguïté. La puissance sera vraisemblablement projetée d'une nouvelle manière et les conflits armés conventionnels tels qu'on les connait aujourd'hui ne seront à l'avenir plus que des phénomènes périphériques. Le défi sera de trouver le moyen de tirer un profit maximal de l'introduction des nouvelles technologies tout en se protégeant des risques majeurs qu'elles engendrent. Dans ce contexte, la cybersécurité deviendra une responsabilité globale de l'Etat et de tous les autres acteurs pouvant potentiellement bénéficier d'opportunités dans le cyberespace, ou profitant du bon fonctionnement de celui-ci.

Globalement, la principale menace vient du fait que toutes les actions lancées dans le cyberespace peuvent déboucher sur des dommages concrets dans les espaces physiques et affecter la population civile, voire même causer des victimes. Il faut identifier des menaces qui n'existent pas encore et qui résulteront du développement des nouvelles technologies et de l'IA. La cybermenace doit être placée au même niveau que la menace émanant des missiles balistiques ou du terrorisme international, sans oublier que ces menaces peuvent être combinées. Les acteurs non-étatiques vont disposer des capacités à produire les mêmes effets que les acteurs étatiques. Toutefois, il faut garder à l'esprit le fait que des attaques qui ont le potentiel de remettre en cause la sécurité nationale et la stabilité d'un Etat nécessitent des moyens considérables.

La cybermenace doit être placée au même niveau que la menace émanant des missiles balistiques ou du terrorisme international, sans oublier que ces menaces peuvent être combinées.

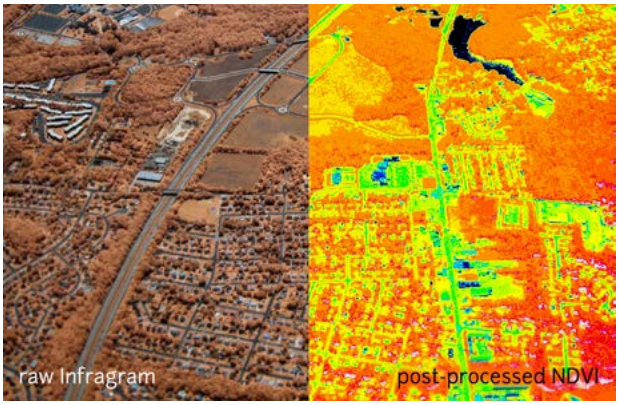


Figure 2 Des possibilités améliorées d'analyse des images grâce à l'IA, qui permettront une meilleure préparation des opérations (https://publiclab.org/wiki/near-infrared-camera, consulté le 30.05.2018).

Figure 3 Amélioration des possibilités de création d'images de synthèse pour de la désinformation. L'original est à gauche, l'image créée à droite (https://interestingengineering.com/ai-software-generate-realistic-fake-videos-from-audio-clips, consulté le 30.05.2018).

Les systèmes doivent être protégés dans leur globalité. Sans une protection, un attaquant peut perturber ou interrompre un grand nombre de services essentiels pour la population, comme la distribution d'eau ou d'électricité, ou la vente en général. Ceci peut rapidement conduire à des troubles sociaux importants. Il n'est dès lors pas étonnant que les cyberattaques russes en Ukraine en 2014 ont visé des centrales électriques, des banques, des hôpitaux et des systèmes de transport, ainsi que le déroulement des élections. Les théoriciens des systèmes partent du principe que si 37 % d'une infrastructure est détruite, elle ne fonctionne plus.[6] Selon la « Revue Stratégique », il est possible d'évaluer la gravité d'une attaque en fonction de 4 critères.[7] En premier lieu, il s'agit (1) d'évaluer les préjudices pouvant être portés aux intérêts fondamentaux du pays avant (2) d'analyser les atteintes à la sécurité intérieure qui en résulteraient. Il faut ensuite (3) estimer les dommages à la population et à l'environnement et finalement (4) ceux portés à l'économie.

Il est possible de dire à l'heure actuelle que l'IA va à coup sûr jouer un rôle important dans la sécurité, à la fois en ce qui concerne les capacités de défense et celles nécessaires pour l'attaque. Pour certaines tâches sécuritaires, l'IA va très certainement dépasser les capacités des humains et permettre de nouvelles percées. L'IA sera aussi capable de contrôler certaines nouvelles technologies dans une mesure qui dépasse les capacités des humains. Le rôle de l'IA pour l'apprentissage automatisé (machine learning / deep learning) est essentiel. Des progrès rapides et dans un spectre très large d'applications se font par le biais de l'apprentissage automatique, bien plus que par la programmation. L'IA va permettre une fusion des mondes réels et virtuels en vue d'obtenir une meilleure représentation de l'environnement. Cela ouvre des possibilités d'entrainement nouvelles qui se baseront sur les capacités augmentées à collecter des données, à les analyser très rapidement et à les utiliser immédiatement.

Il faut s'attendre à ce que l'IA accroisse les menaces de 3 différentes manières: elle va étendre et diversifier les menaces existantes, elle va introduire de nouvelles menaces et elle va modifier le caractère et la nature des menaces connues.[8] Les attaques seront plus efficaces, plus précises, plus difficile à attribuer et exploiteront systématiquement toutes les vulnérabilités. Elles fournissent aussi des capacités pour les forces armées, comme l'identification de cibles humaines (commandants militaires) ou la navigation autonome. Il sera possible de créer des campagnes de désinformation à des échelles et avec une vraisemblance encore inconnues.

En conséquence, l'augmentation de l'efficacité sera l'une des caractéristiques majeures des futures attaques dans le cyberespace. Cela veut aussi dire qu'elles seront mieux et très soigneusement préparées.[9] Grâce à l'engagement de l'IA, les attaques seront personnalisées et faites sur mesure afin d'atteindre le but recherché. Face à ce potentiel nouveau, l'interopérabilité entre les humains et les machines sera un enjeu considérable. Un défi important sera de trouver la meilleure combinaison entre l'homme et la machine. Pour le moment, il faut garder un certain niveau de simplicité afin que l'information puisse être utilisée rapidement par l'humain. Trop d'informations peuvent à un certain moment se révéler contre-productives, à tous les niveaux, dans toutes les fonctions, donc aussi pour les militaires. Une sorte de guerre des machines, systèmes contre systèmes, n'est pas de la science-fiction dans le domaine de la cybersécurité. Les machines qui attaquent devront simultanément être capables de se défendre face à des contre-attaques extrêmement rapides de la part des systèmes préalablement ciblés. Trois facteurs principaux concernant les robots sont pertinents pour la sécurité.[10] D'abord, le déve-

6 Anil, op. cit., p. 149.
7 Revue Stratégique de Cyberdéfense, Secrétariat Général de la Défense et de la Sécurité Nationale, Paris, 12.02.2018, disponible sous http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf, p. 81.
8 Brundlage, Miles (et al): The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation, February 2018, 99 p., disponible sous: https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf.
9 Ibid, p. 21.
10 Ibid, p. 39.

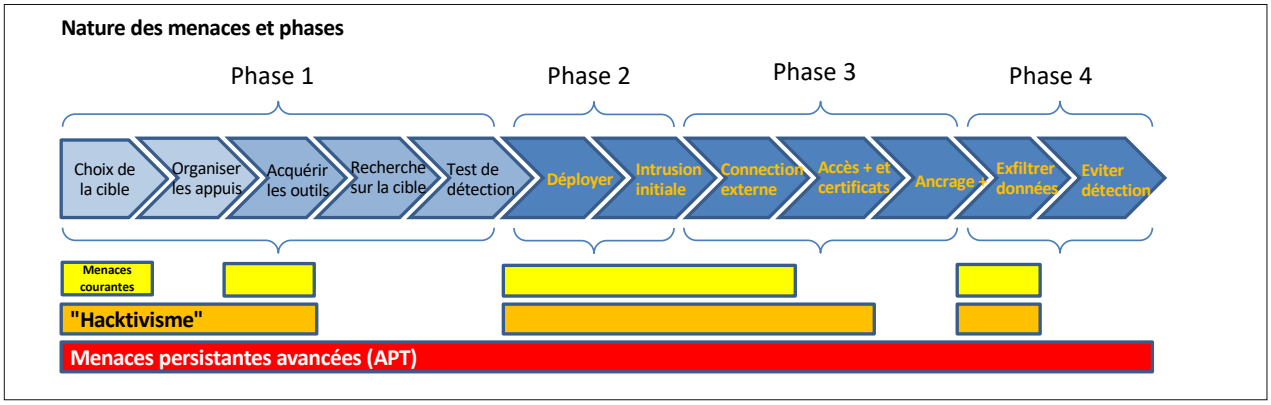


Figure 4 Evolution de la complexité de la menace grâce aux APT, avec leurs composantes et phases (ASTAB ; DDPS).

loppement et le déploiement des robots qui se généralisent et deviennent un phénomène global. Ensuite, l'adaptabilité des robots pour les utilisations les plus variées, qui représente un vrai problème pour la sécurité, et finalement l'autonomie, qui est le facteur comportant le plus de risques. Il est en effet possible que la machine veuille s'affranchir du contrôle du soldat, et vouloir accomplir la mission de la manière qui lui semble la plus rationnelle. Le contrôle par des humains pourrait dès lors apparaître comme l'élément perturbateur et dangereux, qu'il faut éliminer pour remplir la mission. L'un des plus grands dangers de cette évolution est que certaines décisions nécessitant des réactions très rapides et sans hésitation pourraient être déléguées à de l'IA, comme pour l'engagement de missiles ou d'armes nucléaires.[11]

L'IA va aussi accroître l'efficacité des cyberattaques de type APT (Advanced Persistent Threats), qui sont les plus utilisées pour l'espionnage industriel. Ces outils sont très utiles pour l'espionnage des réseaux classifiés des forces armées car ils sont difficiles à repérer. Grâce à ces APT, les acteurs non-étatiques vont de plus en plus disposer des capacités à produire les mêmes effets que les acteurs étatiques dans le domaine de l'espionnage. Mais l'IA a aussi un impact positif pour l'accroissement de la sécurité. Elle ouvre de nouvelles perspectives quant aux capacités à détecter, à contrer et à répondre aux cyberattaques, même lorsque le vecteur des attaques est inconnu jusqu'alors. Elle est aujourd'hui déjà engagée dans la détection d'anomalies et de maliciels dans le cyberespace.

Impact sur les forces armées

Face à la menace potentielle considérable constituée par l'utilisation de l'IA dans le cyberespace, les forces armées devront être prêtes à appuyer les autorités civiles en cas de déstabilisation importante de la société. La plupart du temps, les risques pour les forces armées doivent être extrapolés des risques pour les domaines civils, afin d'imaginer quelles actions malveillantes un agresseur pourrait entreprendre. Un environnement sûr dans le cyberespace sera nécessaire pour que les développements positifs puissent être intégrés et que leur potentiel ne génère pas de catastrophes. Si l'on considère le potentiel d'opportunités et de risques, il s'agit de définir la meilleure manière pour les forces armées de profiter des opportunités tout en se protégeant des risques. Elles doivent en effet en premier lieu assurer leur bon fonctionnement afin de fournir les prestations de sécurité au profit de l'Etat.

Un nouveau débat va certainement débuter. En ce qui concerne les conflits et le combat, l'évolution en cours ainsi que les nouvelles technologies vont apparaître comme des moyens permettant de provoquer plus de dégâts grâce à une meilleure précision et une plus grande efficacité au but. Ces nouveaux systèmes permettront de détruire les moyens de l'adversaire avec plus d'efficacité. Dans cette logique, les nouvelles technologies ne sont utilisées qu'en tant que vecteurs améliorant ce qui est possible aujourd'hui déjà. Si l'on change de paradigme, il est évident qu'il faut se demander si un ennemi pourra être défait sans même le combattre, par d'autres moyens.

Pénétrer un réseau pourrait même se révéler plus bénéfique que d'introduire un nouveau système d'arme. La destruction physique de l'adversaire ne serait ainsi ni une nécessité ni une fin en soi et la nature même de la guerre va non seulement évoluer, mais complètement changer. L'IA et les armes cyber ont une grande flexibilité qui permettra leur engagement en vue de produire un très large spectre d'effets. La puissance sera projetée d'une nouvelle manière et les conflits tels qu'on les connait tendront à devenir des phénomènes périphériques, le plus souvent menés par des intermédiaires. Dans ce genre de nouveau combat, les conséquences possibles pour les populations civiles ne sont pas encore claires.

11 Straub, op. cit., p. 3.

Evolution de la nature des conflits et des forces armées

Dès lors, de nombreuses questions se posent à propos de l'évolution de la nature des conflits. La plus fondamentale est celle de savoir si la cyberguerre deviendra la guerre du futur, encore plus que l'affrontement de systèmes d'armes robotisés. Ceci aurait des conséquences très importantes sur la doctrine. L'adversaire pourrait être défait par des actions dans le cyberespace qui le priveraient de l'utilisation de toute son infrastructure critique et l'empêcheraient d'agir. Ensuite, il n'est pas sûr que les armes nucléaires et les systèmes d'armes aux effets les plus dévastateurs gardent encore une quelconque utilité. Il pourrait être possible de bloquer la capacité d'engager ces armes via le cyberespace, respectivement de les rendre inefficaces. De même, les armes cyber pourraient en cas de besoin infliger des dégâts aussi importants que les armes nucléaires. Dans un tel cas, la capacité à développer des actions dans le cyberespace deviendra la clé du succès, une sorte de dissuasion du futur. Ceci implique que l'intimidation d'un adversaire et la démonstration de force se feront via le cyberespace, et via des actions qui dans une première phase au moins n'impliqueraient sans doute pas ou peu de conséquences pour les populations civiles. Mais dans le cas de paralysies de pans complets de l'économie d'un pays, de déclanchement volontaire de catastrophes technologiques ou écologiques, avec de nombreuses victimes, ou même lors de manipulations crasses du processus démocratique, il sera vraisemblablement question d'actes de guerre.

La plus fondamentale [question] est celle de savoir si la cyberguerre deviendra la guerre du futur, encore plus que l'affrontement de systèmes d'armes robotisés.

La défense dans le cyberespace doit donc faire partie de la panoplie de toutes les forces armées pour qu'elles puissent remplir leur mission de défense et de protection des populations civiles. La dimension cyber est une dimension croissante de tous les engagements des forces armées, de la planification à la conduite en passant par les infrastructures et les processus utilisés. Tous les éléments du cyberespace jouent un rôle de démultiplicateurs des forces engagées.[12] Le fait que les cyberattaques soient non seulement précises, mais également très rapides (vitesse de la lumière) est particulièrement intéressant. Les forces armées occidentales, qui utilisent largement les nouvelles technologies et sont déployées sur toute la planète, sont constamment confrontées aux risques liés à l'utilisation de technologies qui se basent sur le cyberespace. Cette utilisation est souvent une condition sine qua non à la réalisation de leurs opérations, y compris des engagements de promotion de la paix ou humanitaires dans des régions éloignées.

L'importance du cyberespace dans la planification et la conduite des opérations est souvent sous-estimée malgré le fait que de nombreux objectifs militaires peuvent y être atteints. En premier lieu, il est possible de perturber et

Figure 5 Exemple de soldats spécialistes cyber des forces armées israéliennes (IDF) (https ://www.blick.ch/storytelling/2018/zukunft/index5.html, consulté le 08.08.2018).

d'interrompre les échanges de données (communications en tous genres), d'empêcher l'accès à des données, de corrompre des données ou de les détériorer en les infectant ou en les rendant inutilisables. Mais l'objectif peut être plus simplement de détruire certaines données dans des ordinateurs ou même des banques de données complètes ou de bloquer des réseaux. De manière générale, il est possible de considérer l'implantation de maliciels dans les systèmes informatiques d'un adversaire comme une assurance en cas d'attaque, respectivement comme une préparation à long terme pour des cas de différends ou de disputes. Il y a dans ce cas un grand intérêt à ce que l'attaque ne soit pas détectée. Par contre, si un Etat utilise des armes à grande échelle dans le cyberespace, avec l'intention de causer des dommages importants à son adversaire, il le fait avec une certaine intention, et donc n'a pas forcément intérêt à rester camouflé. Au contraire, il se dévoilera afin d'obtenir ce qu'il recherche.[13]

L'intelligence artificielle comme défi pour les forces armées

Les attaques dans le cyberespace vont de plus en plus être utilisées car le temps, la distance, la vitesse et le tempo ne jouent plus de rôle majeur, ne constituent plus des contraintes, et car elles peuvent de surcroit être automatisées. Il est possible que les effets produits par des actions dans le cyberespace contre des adversaires non-conventionnels soient plus difficiles à réaliser, respectivement plus limités, si ces adversaires ne basent pas leur conduite et leurs systèmes d'armes sur des réseaux informatiques. Dans le cas de l'Ukraine en 2014, le maintien de certaines commandes manuelles a permis de réagir plus facilement après une cyberattaque contre l'infrastructure de production d'électricité. Les cyberattaques qu'on subi l'Estonie, la Géorgie et l'Iran n'ont pas été perçues par ces pays comme une attaque militaire en tant que telle et n'ont ainsi pas eu de conséquence pour leurs forces armées. Mais ceci est une question d'interprétation, puisque la destruction de capacités jugées clés, peut apparaître comme une attaque contre le pays tout entier. Il faut aussi se demander si l'importance du cyberespace diffère tout au long des phases d'un conflit ou si, au contraire, cette importance persiste, éventuellement même après la fin des hostilités. Il serait

12 Arquilla, John et Ronfeldt, David: Cyberwar is coming!, Comparative Strategy, vol. 12, no 2, 1993, p. 39.

13 Dannreuther, Roland: International Security: the Contemporary Age, Cambridge, Polity Press, 2013, p. 266.

faux de considérer le cyberespace comme un espace d'opération utilisé uniquement ou principalement durant les phases initiales d'un conflit, et de penser que les opportunités et donc l'importance du cyberespace diminuent au cours du conflit.

En ce qui concerne le déroulement d'un conflit, il faut se représenter un saut qualitatif au moins équivalent à celui survenu avec l'apparition de l'aviation.

Malgré les considérations qui précèdent, il y a encore des auteurs qui pensent que la menace de cyberguerre n'est pas une menace très sérieuse pour les forces armées. Ils perçoivent les actions menées dans le cyberespace plutôt comme des mesures parallèles au conflit traditionnel voire au conflit hybride, les échanges dans le domaine cyber étant qualifiés d'escarmouches. C'est pourquoi il est nécessaire de se pencher en détail sur l'impact que l'IA va certainement avoir sur les forces armées. Les conséquences révolutionnaires de l'IA dans le domaine de la sécurité obligeront les forces armées à faire un saut adaptatif. Elles ne pourront plus se contenter d'évolutions qualitatives pour s'adapter à de nouveaux produits. En particulier, l'IA et l'apprentissage automatique auront des implications décisives pour la cybersécurité et la cyberguerre. En ce qui concerne le déroulement d'un conflit, il faut se représenter un saut qualitatif au moins équivalent à celui survenu avec l'apparition de l'aviation. Plus que dans la conduite du combat dynamique, les forces armées qui disposeront de l'assistance de l'IA auront un avantage important pour accomplir leur mission de sécurité de la société. L'IA permettra d'analyser et de fusionner l'immense volume de données. Dans le domaine du renseignement en particulier, des activités qui requièrent pour le moment de nombreuses personnes pourront être automatisées. Les forces armées disposeront d'une capacité augmentée à collecter des données, à les analyser très rapidement et à les utiliser immédiatement. La lutte pour disposer d'une supériorité dans l'espace de l'information deviendra féroce, car elle sera décisive.

La lutte pour disposer d'une supériorité dans l'espace de l'information deviendra féroce, car elle sera décisive.

L'IA générera des possibilités d'entrainement dans des mondes qui mêlent des informations réelles et des éléments virtuels et permettra un niveau inégalé de préparation aux opérations, ceci pouvant être fait également à distance. L'IA peut ainsi se révéler un instrument précieux dans la phase initiale des conflits, ou lorsqu'un acteur ne veut pas ou ne peut pas engager de troupes pour atteindre son objectif. L'espionnage des systèmes adverses, en tant que mesure préparatoire au combat, va gagner en importance et sera la première étape d'une guerre. Cette récolte d'informations servira de base à des activités de subversion, comme la mobilisation à des fins politiques et la prise d'influence sur l'opinion, y compris en manipulant l'information. Elle servira aussi à la préparation au sabotage d'installations, de systèmes d'armes, d'infrastructures critiques, et à la perturbation ou à la modification de la nature des communications[14], autant d'actions d'affaiblissement de l'adversaire et donc de préparation du champ de bataille. Par contre, il serait faux de prédire que toutes les guerres débuteront systématiquement par une phase de cyberguerre puisque des acteurs isolés pourront toujours agir directement en ayant recours à des actions violentes.

Dans le domaine des matériaux et des équipements en général, l'IA va aussi avoir un impact. Elle permettra de contrôler les nouvelles technologies bien mieux que ne le feraient des humains. Les nouvelles capacités des robots combinées à l'intelligence artificielle permettront des frappes au centimètre près.[15] La programmation des capteurs, surtout lorsqu'ils peuvent ensuite déclencher une réponse automatique, sera améliorée et deviendra cruciale et sensible. L'automatisation couplée à l'IA permettra un développement du « fire and forget » avec des applications à un très grand nombre de systèmes, d'où la nécessité de développer parallèlement les possibilités de contrôle par les humains sur l'engagement de ces armes. Les forces armées vont vouloir mettre pleinement à profit les avantages des machines dans la conduite du combat. En parallèle, il est aussi question de matériaux qui sont non seulement plus légers et plus isolants, mais qui pourraient aussi changer de forme et de couleur. Si on couple ces matériaux à l'intelligence artificielle, on voit apparaître un grand potentiel d'utilisation, notamment dans le domaine du camouflage, mais aussi afin d'améliorer les performances des soldats.

Les possibilités de l'intelligence artificielle dans la conduite des opérations militaires

La combinaison de la masse de données disponibles et de l'IA dans le cyberespace permettra d'affaiblir la volonté de résistance d'un point de vue psychologique. Cette capacité sera utile à la fois pour la défense et pour l'attaque. De manière générale, la conception d'attaques se fera de plus en plus de manière précisément adaptée à l'objectif de façon à en garantir l'efficacité. Ainsi, dans le domaine de la désinformation, les possibilités seront accrues et la diffusion se fera à une vitesse très rapide. C'est pourquoi l'IA deviendra un appui indispensable à la conduite des opérations, principalement en raison de son potentiel d'analyse élevé. L'IA ouvre de nouvelles dimensions à ces améliorations potentielles, en particulier pour la recherche des vulnérabilités des systèmes adverses.

Elle permettra aussi de développer l'appui aux combattants par des systèmes autonomes. L'extension de la capacité à effectuer des missions de manière autonome sera une caractéristique de la future forme des combats. L'humain, grâce à l'IA, essaiera de réagir aux changements plus rapidement et mieux que l'adversaire, ce qui lui amènerait un gain substantiel sur le champ de bataille.

14 Brundlage, op. cit., p. 43.
15 Rid, op. cit., p. 296.

Figure 6 Interprétation plus précise et automatisée de photos de reconnaissance militaire (https://www.38north.org/2017/10/udmh102517/, consulté le 30.05.2018).

Mais l'IA peut aussi soutenir les troupes dans des aspects moins techniques, par exemple dans le domaine de la psychologie, avec l'analyse de contenus violents, qui minent le moral des troupes.

L'IA permettra de combattre simultanément une multitude de systèmes, dans les mondes réel et virtuel, et de parer une succession d'attaques rapprochées et de différente nature. Elle pourra coordonner les défenses, prioriser et agir extrêmement rapidement. En fonction des objectifs, l'IA permettra une meilleure analyse des cibles potentielles, principalement par recoupement d'informations. Ceci est aussi valable pour l'analyse d'image connectée à d'autres données pour, par exemple, reconnaître les infrastructures critiques ainsi que le meilleur moment pour les attaquer, par des cyberattaques ou par des attaques conventionnelles. Mais l'IA peut aussi soutenir les troupes dans des aspects moins techniques, par exemple dans le domaine de la psychologie, avec l'analyse de contenus violents, qui minent le moral des troupes. Dans le domaine de la protection physique, elle diminue les risques, notamment pour la reconnaissance en zone ennemie ou pour le déminage, qui peut être effectué par des robots. Il sera possible de préserver les êtres humains en confiant les tâches 3D (dirty, dull, dangerous) à des machines dotées d'IA. La prise de décision peut aussi être améliorée avec l'IA, tout comme la connexion des différentes unités, la simulation opérationnelle pour la préparation des opérations, l'augmentation de l'efficacité et des performances des systèmes de combat et la facilitation des fonctions de soutien logistique, surtout dans la maintenance. De ce fait, les ordinateurs dotés d'IA vont de plus en plus devenir des systèmes d'armes en tant que tels. Les armes cyber deviendront ainsi des sortes de super-armes de perturbation[16] et d'affaiblissement.

Il y aura cependant toujours une grande différence entre la sécurité qui peut être améliorée dans les zones urbaines ou certaines infrastructures comme les gares ou les aéroports, où de très nombreux capteurs comme des caméras de surveillance sont installés et dont les images sont disponibles et peuvent être analysées, et le combat dynamique dans un environnement où aucun capteur fixe n'est disponible. Lors d'une opération, la mise en place à large échelle de capteurs va continuer à représenter un obstacle au vu de l'envergure de l'action, ce qui laissera toujours une place à la surprise.

En raison de l'intégration croissante de l'IA dans les systèmes des forces armées, le champ de bataille subira plusieurs évolutions. D'abord, il y aura un remplacement à grande échelle des humains par des robots autonomes, dans tous les domaines, allant de la logistique aux robots de combat. Bien sûr, ces robots auront des degrés d'autonomie différents en fonction de leurs tâches. Il s'agira de fixer pour chaque tâche quel degré minimal de contrôle humain sera nécessaire. A long terme, les avions de combat deviendront partiellement obsolètes et pourront être rem-

16 Douzet, Frédérick: Cyberguerres et cyberconflits, dans Badie, Bertrand et Vidal, Dominique: Nouvelles Guerres, L'état du monde 2015, La Découverte, Paris, 2014, pp. 111–117.

placés par des essaims de drones pour certaines tâches. Cette évolution sera favorisée par la forte baisse du coût des drones. Pour les forces engagées au sol, il faudra trouver une parade pour qu'elles puissent réagir à une attaque par des centaines ou des milliers de drones. De même, les charges explosives improvisées deviendront des armes de précision, démultipliant le potentiel de n'importe quel groupe terroriste, par exemple avec une voiture kamikaze se déplaçant de manière autonome. Le potentiel de groupes armés visant la déstabilisation d'une société dans le cadre d'une stratégie hybride sera également démultiplié. Ces groupes pourraient recourir à l'assassinat automatisé à large échelle de cadres militaires, politiques, économiques, grâce à des robots. L'IA pourra toutefois aussi appuyer la mise hors de combat de ces groupes en identifiant des transactions douteuses et de manière plus générale permettre de repérer des terroristes potentiels grâce à l'analyse des faisceaux d'indices. On peut aussi améliorer les défenses passive et active des cibles de haute valeur comme les infrastructures critiques (blindage, défenses actives, radar anti-drone, etc.).

… l'IA nous obligera à donner plus d'autonomie aux machines, afin de leur permettre d'utiliser leur potentiel, spécialement en ce qui concerne la rapidité de leurs réactions.

L'apprentissage, plus ou moins automatisé, de l'IA est un sujet central, qui peut s'avérer être une grande vulnérabilité, dès lors qu'un agresseur arriverait à provoquer un apprentissage erroné. Il suffit pour cela d'ajouter des éléments perturbateurs, comme de fausses informations sur lesquelles l'apprentissage se base ou de modifier légèrement la perception de l'environnement par les machines pour provoquer des comportements différents, potentiellement dangereux. On peut par exemple inverser la reconnaissance ami-ennemi dès la phase d'apprentissage ou apprendre aux systèmes d'armes autonomes à cibler spécifiquement les civils. L'apprentissage automatisé va devenir une cible en tant que telle, car il sera intéressant de saboter le potentiel de l'adversaire dès cette phase, de freiner les capacités d'amélioration des systèmes d'armes autonomes et d'espionner ou d'empêcher la prise en charge de plus en plus de fonctions importantes par des robots disposant d'IA.[17] Malgré cela, l'IA nous obligera à donner plus d'autonomie aux machines, afin de leur permettre d'utiliser leur potentiel, spécialement en ce qui concerne la rapidité de leurs réactions. En ce sens, l'humain va devenir un facteur ralentissant. Si on limite l'autonomie et la vitesse des machines pour garantir un meilleur contrôle, on prend le risque que l'adversaire soit plus rapide. Il n'y aura donc plus de choix et le risque est réel que l'humain ne devienne le spectateur des interactions entre machines, jusqu'à et y compris des combats entre machines. L'exemple des drones est révélateur. La multiplication exponentielle de leur nombre pour les tâches les plus diverses est problématique car elle va accroître le risque d'actions non contrôlées. Au final, il va s'agir d'identifier les systèmes d'armes qui ne peuvent fonctionner sans appui de l'IA, afin de prendre les mesures de protection adéquates et d'assurer la redondance de ces systèmes.

Les vulnérabilités impliquées par l'intelligence artificielle

L'intégration croissante de l'IA dans les systèmes et dans les processus de conduite des forces armées soulève aussi de nombreuses questions quant aux effets négatifs possibles et aux mesures nécessaires afin de garder les risques sous contrôle. Il s'agit en fin de compte d'éviter que des systèmes ou processus militaires puissent être détournés de leur usage primaire. De manière très générale, il s'agit de se demander comment un environnement cyber dégradé peut interférer avec la capacité de forces armées à accomplir leur mission, de la mobilisation jusqu'au combat. Il est possible que les évolutions technologiques, respectivement leur intégration dans les forces armées, puissent être freinées en raison des risques encourus. Dès que l'on parle d'armements et de conduite plus ou moins automatisés, il faut pouvoir garantir le maintien du contrôle, respectivement qu'une prise de contrôle ou une reprogrammation par l'adversaire soit exclue. Il faudra donc particulièrement renforcer la sécurité et la protection des systèmes.[18]

La capacité de l'IA à réagir et à résoudre des situations nouvelles et inattendues, qui est essentielle pour les forces armées, constituera un axe de développement prioritaire.

Les vulnérabilités seront activement recherchées et immanquablement attaquées. Il y aura des contraintes importantes mais inévitables lors de l'intégration de systèmes utilisant l'IA dans les forces armées. Un défi important sera de trouver la meilleure combinaison entre l'homme et la machine, afin d'utiliser le potentiel de l'IA et les synergies de la meilleure manière possible. Il s'agit de combiner de la manière la plus rapide possible l'identification d'opportunités et la décision concernant la meilleure option pour l'action, en tous les cas plus rapidement que l'adversaire, et ceci de manière répétée.[19] Il faut surtout éviter que la machine ne neutralise l'humain ou ses fonctions de contrôle si elle n'est pas d'accord, qu'elle qu'en soit la raison, avec la décision de l'humain. Ceci ne sera certainement pas toujours facile, surtout dans les domaines dans lesquels l'IA dépassera l'intelligence humaine. L'humain devra s'efforcer de garder la sécurité des populations au centre des préoccupations de l'IA, et ceci en toutes circonstances. Pour le moment, l'IA dépend encore de facteurs d'apprentissage qui sont au minimum initiés par les humains. La capacité de l'IA à réagir et à résoudre des situations nouvelles et inattendues, qui est essentielle pour les forces armées, constituera un axe de développement prioritaire. Ceci montre toutefois qu'il faudra développer

17 Allen, Greg et Chan, Taniel: Artificial Intelligence and National Security, Harvard Kennedy Scholl, Belfer Center for Science and International Affairs, July 2017, p. 46.

18 Villani, Cédric: Donner un sens à l'intelligence artificielle: pour une stratégie nationale et européenne, Mission parlementaire du 8 septembre 2017 au 8 mars 2018, Paris, mars 2018, p. 221, disponible sous aiforhumnaity.fr.

19 Rid, op. cit., p. 300.

Figure 7 Des radars permettent de suivre en permanence les activités, y compris les attaques dans le cyberespace (https://www.journaldugeek.com/2015/01/16/pal-la-cyberguerre-cest-pour-demain/, Consulté 15.08.2018).

un nouveau système spécifique de contrôle des armements pour les armes autonomes, surtout pour celles qui ont des effets létaux. Il faut s'assurer que les humains puissent d'urgence désactiver un système autonome qui s'écarterait de sa mission. L'IA pourrait occasionner des problèmes inattendus en raison d'effets non prévisibles générés par la vitesse et la cumulation des interactions. Dans le cadre de cette évolution inéluctable, il faut que la responsabilité finale de l'engagement d'armes autonomes reste en tous les cas chez les humains, qu'il n'y ait pas de déresponsabilisation.[20]

Une guerre qui se déroule au moyen de missiles à guidage autonome, de chars de combats sans équipages et de drones armés, éventuellement guidés à distance est une option qu'il faut envisager. On pourrait assister à une sorte de « déshumanisation » des guerres du futur.

L'un des plus grands dangers inhérent à cette évolution est que certaines décisions qui nécessitent des réactions très rapides et sans hésitations pourraient être déléguées à de l'IA, comme pour l'engagement de missiles ou d'armes nucléaires.[21] L'IA pourrait ainsi entraîner une nouvelle course aux armements, car tous les acteurs voudront améliorer leurs systèmes d'armes avec le potentiel de l'IA. Le recours de plus en plus courant à l'IA sera donc une évolution inéluctable, pour ses bénéfices en premier lieu, mais aussi avec toutes les conséquences dans le domaine de la protection. Les humains deviendront moins déterminants, et dans le même temps, les machines dicteront le tempo des combats dans tous les espaces d'opération et surtout influeront directement sur le résultat. Les humains devront trouver un moyen de garder le contrôle sur le déroulement des opérations et éventuellement poser des limites aux machines ou à leur assistance. Une guerre qui se déroule au moyen de missiles à guidage autonome, de chars de combats sans équipages et de drones armés, éventuellement guidés à distance est une option qu'il faut envisager. On pourrait assister à une sorte de « déshumanisation » des guerres du futur.

Dans la conduite des opérations, empêcher les communications a de tout temps joué un rôle essentiel. Mais ceci n'a d'impact positif que si l'on peut dans le même temps assurer ses propres communications. On peut donc penser que l'élimination des forces de l'adversaire afin d'emporter la décision va encore perdre de l'importance au profit de la capacité à atteindre le cœur du système adverse, ses centres de gravité, ou à le désorganiser pour le paralyser. La capacité à reconnaître les fenêtres d'opportunité sera toujours plus importante et décisive.

Des fenêtres d'opportunité peuvent être créées en « aveuglant » l'adversaire ou en l'induisant en erreur. Les systèmes de communication des forces armées adverses seront donc de plus en plus des infrastructures critiques essentielles. Leur attaque et leur destruction permettraient sûrement de paralyser et donc de vaincre l'adversaire dans un monde où la maîtrise de l'information et la capacité à la manipuler représenteront la puissance. La supériorité dans l'espace de l'information sera atteinte grâce à une capacité augmentée à collecter des données, à les analyser très rapidement et à les utiliser immédiatement sur le champ de bataille. Il y aura plus de sources et il sera plus facile de diffuser de fausses informations ou d'influencer les décisions de l'adversaire. La propagande, la tromperie et l'ingénierie sociale, soit la manipulation psychologique à grande échelle, seront améliorées. Ceci servira aussi à semer la confusion chez l'adversaire en perturbant sa perception de l'image de la situation plus sûrement qu'en détruisant ses équipements et systèmes d'armes. Les structures de commandement verticales laisseront de plus en plus la place à des structures en réseau, très flexibles, permettant d'intégrer la coopération, permanente ou tempo-

20 Brundlage, op. cit., p. 42.
21 Straub, op. cit., p.3.

raire, avec de nouvelles composantes. Il y aura donc à coup sûr également des changements importants dans l'analyse des centres de gravité et dans la planification du targeting.

Les systèmes de communication des forces armées adverses seront donc de plus en plus des infrastructures critiques essentielles.

Il faudra aussi, dans le domaine des armes cyber et de l'appui par l'IA, un certain équilibre qui permettra, à l'image de la dissuasion nucléaire, une nouvelle forme de dissuasion cyber. La période de transition entre le développement de nouvelles capacités et l'équilibre des moyens sera une période à risques. Il faut prendre en compte que les applications militaires de systèmes civils d'IA ne sont pas si faciles à réaliser. La nature de double emploi de ces technologies sera un facteur important, éventuellement aussi limitatif. Une des dimensions importantes avec l'engagement de systèmes d'armes autonomes est celle des dommages collatéraux qu'ils pourraient causer. Il y a souvent dans ce domaine une question de mise en balance des intérêts en jeu, dans un contexte qui peut évoluer de seconde en seconde. C'est n'est donc pas qu'une question de précision des informations à disposition, mais bien une évaluation d'un système global, avec une action unique qui peut avoir un impact stratégique. La question de l'autonomie comprend aussi la dimension de la responsabilité en fonction du déroulement et des conséquences des engagements de systèmes d'armes autonomes. On peut au final s'imaginer que dans le cadre d'une défense active, un Etat puisse réagir avec une réponse seulement partiellement militaire, cyber et non-cyber, à des cyberactions agressives contre ses intérêts. De facto, une cyberprotection et des cybercapacités qui fonctionnent permettent aux forces armées de remplir leurs missions, et donc de mener les opérations, éventuellement même de manière plus efficace et moins coûteuse.[22]

L'importance de la cyberdéfense pour l'armée suisse

Le fait de disposer d'une cyberdéfense efficace et de protéger les systèmes deviendra dans les années à venir la pierre angulaire de l'effet dissuasif de l'armée suisse. Un adversaire qui ne parviendrait pas à l'affaiblir par des cyberattaques réfléchira à deux fois avant de s'engager plus avant, respectivement d'engager ses moyens au sol et dans les airs. La cybersécurité est essentielle comme première ligne de défense, dans la mesure où elle peut constituer une forme de dissuasion contre des attaques dans les espaces physiques. Mais elle ne doit pas être confondue avec le concept de dissuasion nucléaire. Il s'agit ici de convaincre un adversaire de renoncer à une attaque en contrant ses opérations préparatoires dans le cyberespace et dans l'espace de l'information. Il faut donc activement promouvoir les mesures qui contribuent à cette conviction. Ceci est particulièrement valable dans le cas où un adversaire choisit une stratégie hybride, qui commencerait par un affaiblissement ciblé de l'Etat et de ses forces armées par des mesures dans le cyberespace. Il faut rendre la vie d'un potentiel agresseur difficile en augmentant les moyens nécessaires à un succès. La Suisse, n'ayant plus d'armée de masse pour dissuader un adversaire potentiel, se doit d'être à la pointe de la cybersécurité pour protéger ses systèmes d'armes et ses infrastructures critiques, afin de ne pas être affaiblie en amont d'un conflit. Le fait de disposer de systèmes qui recourent à l'IA peut aussi constituer un facteur de dissuasion.[23]

La cybersécurité est essentielle comme première ligne de défense, dans la mesure où elle peut constituer une forme de dissuasion contre des attaques dans les espaces physiques.

La dépendance de l'armée suisse à l'égard d'infrastructures civiles, en particulier des réseaux de communication, est un facteur qui justifie pleinement le développement de la sécurité militaire dans le cyberespace. Il est essentiel pour l'armée que ces infrastructures soient elles aussi bien protégées. A partir de là, il est important d'intégrer la problématique de la cyberdéfense dans tous les exercices militaires ou de gestion de crise, spécialement dans ceux qui impliquent aussi les partenaires civils. De plus en plus, les relations entre les forces armées et les institutions civiles s'intensifient dans les deux directions, ce qui veut concrètement dire que les forces armées, dans le contexte de l'architecture de cybersécurité, peuvent aussi bénéficier du soutien d'entreprises civiles, dans la mesure où elles n'en sont pas dépendantes. La recherche au sein de armasuisse W+T doit aussi consacrer plus de ressources à l'étude, au développement et à l'intégration de l'IA, ceci afin d'être à même de contrer celle de l'adversaire. Par ailleurs, en ce qui concerne le personnel, il ne faut pas oublier que les entreprises civiles et les forces armées seront en compétition pour les mêmes spécialistes. Il faudra faire du système de milice un avantage, et non pas un handicap.

Il faudra à l'avenir pour l'armée suisse une structure de commandement très flexible, envisagée dans le cadre d'un système de systèmes, où la conduite verticale cède la place à une conduite thématique, horizontale et adaptable.

Les possibles affrontements dans le cyberespace créeront des attentes et des contraintes plus importantes pour les chefs à tous les échelons, qui devront être capables d'agir de manière autonome dans un schéma global donné. Celui qui utilisera la « conduite par ordres » (Befehlstaktik) avec les nouvelles technologies, par exemple en tant qu'instrument de contrôle permanent pour imposer une vision, sera perdant. Les Task Forces modulables, très flexibles, avec un spectre très large d'emplois possibles, et qui pourront s'adapter à un adversaire en permanente évolution, sont

22 Revue Stratégique de Cyberdéfense, op. cit., p. 52.

23 Straub, op. cit., p. 5.

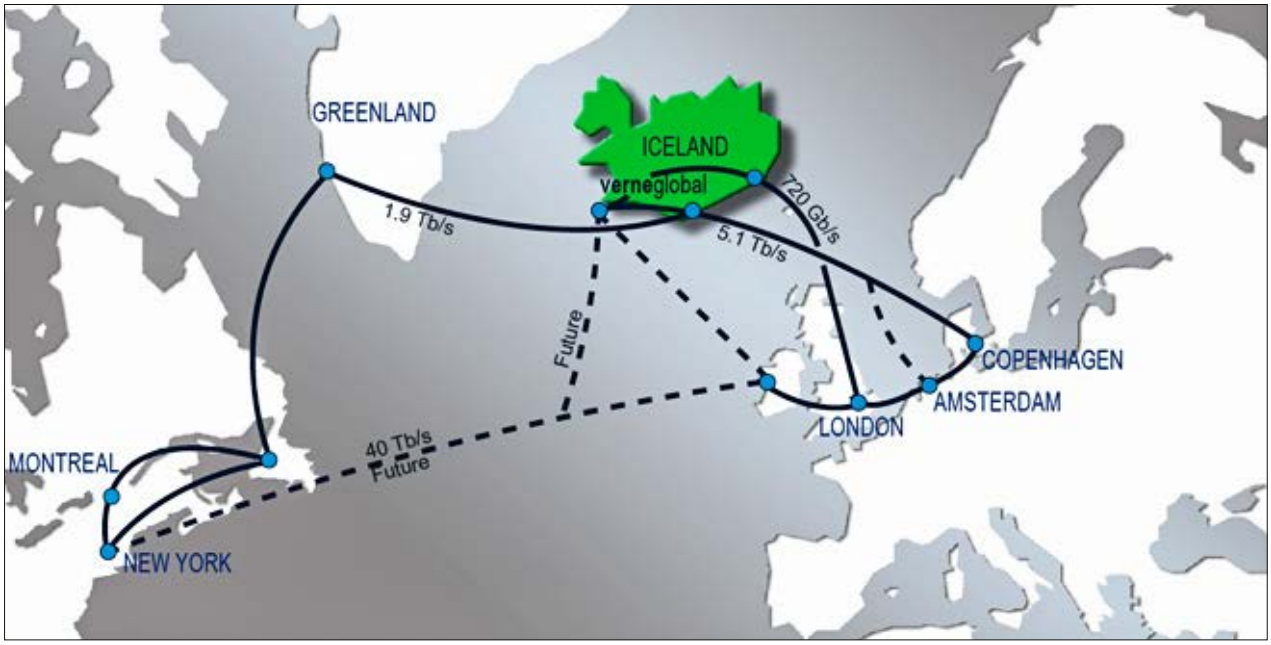


Figure 8 Importance des infrastructures pour le bon fonctionnement du cyberespace, à l'image des réseaux transitant par l'Islande (https://askjaenergy.com/2013/02/11/data-centres-in-iceland/, consulté le 20.07.2018).

les forces du futur. Il faudra à l'avenir pour l'armée suisse une structure de commandement très flexible, envisagée dans le cadre d'un système de systèmes, où la conduite verticale cède la place à une conduite thématique, horizontale et adaptable. Il est probable que l'accroissement de l'importance du cyberespace signifie une diminution de l'importance de la domination du terrain et des espaces physiques en général. Cette évolution n'est donc pas anodine et devra être intégrée dans les futurs développements de l'armée, car la notion de terrain a jusqu'ici toujours eu une importance considérable dans la doctrine.

La cyberguerre va aussi rendre l'analyse des centres de gravité de l'adversaire encore plus importante, et doit conduire à un effort principal sur la protection des propres centres de gravité et sur la capacité à agir sur les centres de gravité adverses. L'assistance que l'IA peut générer pour la conduite du combat en zone urbaine, qui est la zone d'engagement principale de l'armée suisse, sera importante et pourra être un avantage décisif. En raison du renouvellement de nombreux systèmes d'armes dans les 10 à 15 années à venir, et du fait que ces systèmes d'armes sont prévus en général pour une durée d'utilisation d'une trentaine d'années, les défis pour la planification des acquisitions seront bien réels et ne pourront être sous-estimés. Des questions telles que la future utilité de chars d'assaut ou d'autres moyens lourds comme l'artillerie devront être abordées. Mais il faudra toujours intégrer, dans les processus d'acquisition de ces systèmes, la dimension de la cybersécurité et de la redondance en cas de cyberattaques. L'armée suisse devra disposer des moyens cyber adéquats à une préparation optimale du champ de bataille, ou au blocage de la préparation du champ de bataille par un éventuel adversaire. En raison des engagements de l'armée suisse à l'étranger, il faudra aussi identifier les possibilités et les limites d'actions dans le cyberespace contre des adversaires non-conventionnels. Il faudra aussi trouver la meilleure manière possible d'assurer la cybersécurité des troupes à l'engagement dans des environnements peu favorables. En résumé, il y a 8 évolutions principales, avec les implications du cyberspace et de l'IA, qui vont toucher l'armée suisse et qu'il faudra donc suivre et intégrer dans les planifications de développement des forces armées: (1) l'augmentation du nombre de robots, dans tous les domaines, (2) l'abandon de certains systèmes d'armes, remplacés par de nouvelles technologies, (3) les nouvelles méthodes de combat qui découlent des nouvelles technologies, (4) les nouvelles armes, (5) les nouveaux critères et instruments de puissance, (6) l'autonomie croissante des machines, (7) les nouveaux problèmes liés aux machines, et finalement (8) les nouvelles cibles.

Conclusions

La cyberdéfense est devenue une nécessité absolue en vue de protéger non seulement la population et les infrastructures, mais aussi la vie sociétale et démocratique. Les cyberattaques constituent la menace principale, même si cette menace a pour l'instant été masquée par la visibilité du terrorisme. Les nouvelles vulnérabilités apparaissent plus vite que les anciennes ne sont éliminées. Un des problèmes majeurs sera le coût nécessaire pour une protection à large spectre.

Les cyberattaques constituent la menace principale, même si cette menace a pour l'instant été masquée par la visibilité du terrorisme.

Les développements dans le cyberespace et l'utilisation croissante de l'IA dans cet espace d'opération, vont changer les paramètres auxquels nous sommes habitués. Ceci sera vrai autant pour les aspects civils que pour les forces armées. Les nouvelles menaces dans le cyberespace ne remplacent pas les anciennes, mais s'ajoutent à celles déjà connues qui vont subsister en tant qu'instruments possibles dans la palette d'actions, en priorité de la part des acteurs non-étatiques, comme des attentats en tout genre, des détournements d'avions, de bateaux, etc. Mais les forces armées ne sont que l'un des partenaires parmi les autres et peuvent contribuer à la gestion d'une cybercrise avec leurs moyens, dans la mesure où les dispositions légales le permettent. Elles n'ont donc pas un rôle de premier plan dans ce domaine, respectivement ne devraient pas en avoir si les organes civils remplissent leur rôle. Ceci ne diminue en rien la nécessité pour elles de garantir leur aptitude à fournir les prestations attendues grâce une protection efficace de leurs systèmes et donc de rapidement reconsidérer les priorités en ce qui concerne l'allocation des ressources.

La révolution engendrée par les nouvelles technologies diffusera et redistribuera la puissance, le plus souvent au profit d'acteurs plus petits et actuellement plus faibles

Le niveau de sécurité des systèmes de l'Etat, y compris ceux des forces armées, est un enjeu central. Un haut niveau est indispensable. L'IA créera de nouvelles possibilités, les rendra abordables pour plus d'acteurs. Les caractéristiques géopolitiques comme l'étendue du territoire, la population et les ressources naturelles ne seront plus les seuls attributs de puissance d'un pays. La révolution engendrée par les nouvelles technologies diffusera et redistribuera la puissance, le plus souvent au profit d'acteurs plus petits et actuellement plus faibles.[24] Les petits Etats à la pointe de l'IA pèseront plus lourd dans la balance. Le danger principal sera sans doute un déséquilibre dans les moyens, qui pourrait pousser un Etat à une attitude agressive s'il est presque certain de l'emporter ou de disposer d'une supériorité dans le cyberespace. Il faudra aussi dans le domaine des armes cyber et de l'appui par l'IA un certain équilibre qui permettra, à l'image de la dissuasion nucléaire, une nouvelle forme de dissuasion cyber. Une régulation du cyberespace est donc indispensable afin de favoriser la coopération et de permettre la répression des abus. Il faudra que les Etats se donnent les moyens de jouer un rôle normatif dans le cyberespace, ce qui semble pour le moment plutôt difficile. Si le fossé entre les Etats riches et les Etats pauvres continue à s'accroître, des crises majeures sont à prévoir. Les pays pauvres auront de plus en plus les moyens de réagir contre les abus du système économique mondial et pourront avec des moyens relativement limités lancer des actions agressives dans le cyberespace contre ceux qui sont perçus comme des oppresseurs ou des profiteurs. Ceci pourrait générer d'importants risques de déstabilisation et de conflits.

La question de la responsabilité doit être résolue le plus rapidement possible. Lors d'un problème majeur, et ceci en raison de la difficulté à identifier un agresseur, il faudra pouvoir attribuer la responsabilité des faits. Cela pourrait être le propriétaire, le programmateur, le constructeur, le diffuseur, voire même éventuellement l'Etat. C'est l'une des questions ouvertes les plus importantes dans un monde qui s'automatise de plus en plus. La difficulté de l'attribution est un problème central, même si elle peut aussi être considérée comme un facteur calmant le jeu, puisqu'elle oblige l'attaqué à rester mesuré dans sa réaction. Toutefois, il faudra aussi pour cela trouver une solution, puisque les attaques seront toujours plus efficaces, plus précises, plus difficiles à attribuer et cibleront toutes les vulnérabilités. Il y aura aussi plus d'acteurs capables d'effectuer de telles attaques. Une sécurité améliorée ne résultera pas seulement de la nécessité de faire les choses mieux, mais aussi de les faire différemment. Une modification du comportement afin de diminuer et éventuellement d'éliminer les risques sera nécessaire. L'expérimentation est une phase qui va gagner en importance, pour vérifier à la fois les gains de sécurité possibles mais aussi rechercher les vulnérabilités en vue de les éliminer. Grâce à ses capacités autonomes d'apprentissage croissantes, l'IA pourrait dans un futur assez proche être capable de développer et d'assurer la cybersécurité d'un système de manière entièrement autonome, c'est-à-dire sans aucun apport nécessaire de la part de l'humain. L'humain gardera toutefois un rôle dans le processus d'apprentissage (« machine learning »). Une absence d'interaction pourrait provoquer un développement des machines dans une mauvaise direction et pourrait ainsi diminuer l'efficacité de la sécurité. L'importance de l'humain, et donc du soldat, ne disparaîtra pas, de même que les nombreuses craintes qui accompagnent le développement de l'IA. Le vrai risque serait de séparer les humains et les machines, ce qui conduirait inévitablement à des conflits.

Grâce à ses capacités autonomes d'apprentissage croissantes, l'IA pourrait dans un futur assez proche être capable de développer et d'assurer la cybersécurité d'un système de manière entièrement autonome, c'est-à-dire sans aucun apport nécessaire de la part de l'humain.

Il sera indispensable que les systèmes militaires deviennent suffisamment sûrs afin de compenser l'accroissement généralisé des possibilités de la menace numérique. Il est impératif que tous les concernés prennent conscience de la gravité de la menace. Le risque dans le cyberespace est un risque systémique et ne se limite pas à de potentielles attaques ciblées ou limitées. Dans ce contexte, la cybersécurité est un élément dissuasif non seulement contre les cyberattaques, mais aussi contre les attaques dans les autres espaces d'opération puisque l'affaiblissement d'un adversaire dans le cyberespace peut aussi être utilisé comme préparation à un conflit ouvert. Il va falloir s'habituer à un environnement où les cyberattaques seront mon-

24 Arquilla et Ronsfeldt, op. cit., p. 26.

naie courante et systématiquement tentées, ce qui pourrait remettre en cause la stabilité de l'ensemble du cyberespace. Il se pourrait donc bien que l'on assiste de plus en plus à des affrontements entre systèmes qui seront tous appuyés par de l'IA, les uns tentant d'exploiter les vulnérabilités des autres. La sécurité dans le monde virtuel constituera la base de la protection du monde réel. Il se pourrait cependant que l'étendue potentielle des dégâts, y compris les dégâts collatéraux, soit telle qu'elle représente un facteur poussant les attaquants à une certaine prudence, spécialement lorsqu'il s'agit d'Etats. Il est en effet très difficile d'estimer les conséquences de cyberattaques qui toucheraient de manière indiscriminée tous les ordinateurs et systèmes d'un pays, et dont les effets collatéraux sont par définition imprévisibles. Ce danger serait tout à fait envisageable avec des armes autonomes qui se baseraient sur l'IA et ne seraient ainsi plus contrôlées par les humains.

La sécurité dans le monde virtuel constituera la base de la protection du monde réel.

Les forces armées et l'armée suisse en particulier n'ont d'autres choix que de se protéger de manière efficace contre les cyberattaques et les dérives des nouvelles technologies si elles veulent conserver leur faculté à remplir leur mission de protection de la population et du territoire national. Il est impossible d'imaginer des forces armées qui ne disposent pas d'une composante cyber. Une prise à la légère des nouveaux défis impliqués par le développement du cyberespace et de l'IA fait peser des risques existentiels sur les sociétés. Des mesures peuvent et doivent être prises, souvent également appuyées par l'IA, pour renforcer la sécurité dans le cyberespace. Il y a six composantes pour une cyberprotection efficace: (1) la prévention, (2) l'anticipation, (3) la protection, (4) la détection, (5) l'attribution et (6) la réaction. La formation des utilisateurs d'internet et des moyens de communication est centrale. L'anticipation implique la connaissance des menaces, afin de pouvoir se préparer à les contrer, alors que la protection implique toutes les mesures afin de compliquer la tâche des attaquants. La détection doit être rendue possible par des mesures prises au sein des systèmes eux-mêmes. Ces mesures gagneront en importance, même si elles pourraient devenir plus compliquées avec le développement de la cryptographie. L'attribution nécessite des moyens spécifiques d'analyse des signaux. Finalement, la réaction concerne surtout les moyens de reprendre et de poursuivre les activités, autant que les mesures contre l'attaquant proprement dites.

Marc-André Ryter

Lic. ès sc. pol./ dipl. en études en politique de sécurité
État-major de l'armée, doctrine militaire

E-Mail: marc-andre.ryter@vtg.admin.ch

Strategieanalyse: Methodik und Visualisierung

Die Dozentur Strategische Studien (DSS) hat eine Analysemethodik für operative Strategie entwickelt, die allgemein anwendbar ist und für sich mehrere Vorzüge beansprucht, insbesondere durch ihren synoptischen Charakter. Die Methodik geht von der Definition von Arthur F. Lykke Jr. aus, der das Zusammenspiel dreier Komponenten – ends, ways und means – betont. Sie unterscheidet nach Deklaration und Aktion sowie nach Einsatz und Reserve und bezieht auch Clausewitz'sche Theorie mit ein. Die Methodik, welche die Analyse und Visualisierung einer tatsächlich verfolgten Strategie einer Partei während eines bewaffneten Konfliktes bezweckt, wird hier erstmals vorgestellt und anhand der amerikanischen Strategie im Vietnamkrieg erläutert.

«[W]hat I do decry is that strategy, which so clearly affects the course of society, is such a disorganized, undisciplined intellectual activity.»
Rear Admiral Joseph Caldwell Wylie, 1967[1]

Mauro Mantovani, Marcel Berni

Einleitung

Der angesehene britische Historiker Hew Strachan beklagt in seinem viel beachteten Artikel «The Lost Meaning of Strategy» von 2005, dass der Begriff Strategie gleichbedeutend zu *policy* geworden sei.[2] Auch Lawrence Freedman, der sich ein Forscherleben lang mit Strategie befasst hat, gelangt in seinem Opus Magnum *Strategy: A History* von 2013 zu einem sehr ähnlichen Verständnis: «[S]trategy is the central political art. It is about getting more out of a situation than the starting balance of power would suggest. It is the art of creating power.»[3] Beide Autoren sehen Strategie also in der politischen Sphäre, beide verzichten jedoch darauf, eine Analysemethodik vorzustellen oder gar Strategie zu visualisieren: Freedmans 751-Seiten-Werk kommt ohne eine einzige Abbildung aus!

Dieser Beitrag will dagegenhalten. Er nimmt die Forderung von J.C. Wylie auf und entwickelt eine Methodik, nach welcher jede Strategie einer Partei in einem zurückliegenden bewaffneten Konflikt systematisch analysiert und nachvollzogen werden kann. Dadurch soll Strategie konkret und fassbar werden.

Methodische Grundlagen

Die hier vorgestellte Methodik der Strategieanalyse basiert auf dem einflussreichen Modell, welches der damalige Dozent für Militärstrategie am US Army War College, Colonel Arthur F. Lykke Jr., 1984 unter dem Titel «Towards an Understanding of Military Strategy» vorlegte.[4] Wie Strachan und Freedman versteht Lykke Strategie umfassend, im Sinne aller Macht-Mittel eines (staatlichen oder nichtstaatlichen) Akteurs, mithin synonym zu «Grand Strategy», einem von Basil Liddell Hart in den 1950 Jahren geschaffenen Konzept, oder zum «*whole-of-government approach*» im aktuellen Sprachgebrauch.

Lykkes Verdienst besteht darin, Strategie auf eine einfache und einprägsame mathematische Formel gebracht zu haben, die für alle Hierarchiestufen gilt: «Strategy equals Ends (objectives towards which one strives), plus Ways (courses of action) plus Means (instruments by which some end can be achieved).»[5] Erfolgreich sei Strategie,

1 J. C. Wylie, *Military Strategy,* Annapolis [2]1989 [New Brunswick 1967], S. 1.

2 «Strategy is a word which has lost its meaning, too often being used as a synonym for policy. Between the late eighteenth century and the end of the First World War, it described the conduct of war as exercised at the level of the military commander. But the scale of the two world wars and the influence of maritime powers, like the United States and Britain, prompted the evolution of ‹grand strategy› to enable the coordination of allies in different theatres of war and to mobilise all national resources for the prosecution of war. Since the end of the Cold War the vocabulary of war-making has lost definition, making lesser conflicts seem larger than they are, ‹militarising› foreign policy and robbing the nation state of an important conceptual tool for adapting military means to political objectives.» Hew Strachan, «The Lost Meaning of Strategy», *Survival,* 47, 2005 (3), S. 33–54 (Abstract). Andernorts schreibt Strachan: «The word strategy has acquired a universality which has robbed it of meaning, and left it only with banalities.» Ders., *The Direction of War: Contemporary Strategy in Historical Perspective,* Cambridge 2013, S. 27.

3 Lawrence Freedman, *Strategy: A History,* New York 2013, S. xii.

4 Arthur F. Lykke, Jr., «Towards an Understanding of Military Strategy», in: ders., *Military Strategy: Theory and Application,* Carlisle Barracks 1984, S. 1–2 – 1–6, hier S. 1–2. Siehe auch den direkt anschliessenden Beitrag von Lykke, «A Methodology for Developing a Military Strategy», ebd., S. 1–7 – 1–9. Der erste Beitrag wurde mehrfach erneut abgedruckt, z. B. in leicht veränderter Form unter dem Titel «Defining Military Strategy» in *Military Review,* May 1989, S. 2–8.

5 Lykke, «Towards an Understanding of Military Strategy» (Fn. 4), S. 1–2. Dabei beruft sich Lykke auf eine Rede von General Maxwell D. Taylor von 1981.

so Lykke weiter, wenn sich diese drei Komponenten im Gleichgewicht befinden. Gleichzeitig weist Lykke auf die Schwierigkeiten der Anwendung seines Modells hin, weil sich die drei Komponenten – Ziele, Methoden und Mittel – im Zeitverlauf verändern und höchstens teilweise offengelegt werden.[6] Die Militärstrategie wiederum ist für Lykke eine Teilmenge der Grand Strategy, da sie nur die militärischen Ziele, Methoden und Mittel umfasst. Der Dreiklang *ends-ways-means* hat in der amerikanischen Militärdoktrin seither fast schon kanonischen Status erlangt; ein jüngeres Beispiel dürfte die *Joint Doctrine Note* 1-18 vom Frühjahr 2018 sein.[7]

Wichtig ist ferner Lykkes Feststellung, dass Strategie – sei es nun Grand bzw. National Strategy oder Military Strategy – sowohl in der Anwendung als auch in der Entwicklung von Macht-Mitteln besteht; ersteres bezeichnet Lykke als «operational strategy», letzteres als «force developmental strategy».[8] Diese Unterscheidung geht im Grunde zurück auf Carl von Clausewitz, der erkannt hatte, dass die «Kriegskunst» eine kriegs- und eine friedensbezogene Dimension besitzt:

«Die Kriegskunst im eigentlichen Sinne wird also die Kunst sein, sich der gegebenen Mittel im Kampf zu bedienen, und wir können sie nicht besser als mit dem Namen *Kriegführung* bezeichnen. Dagegen werden allerdings zur Kriegskunst im weiteren Sinne auch alle Tätigkeiten gehören, die um des Krieges willen da sind, also die ganze Schöpfung der Streitkräfte, d.i. Aushebung, Bewaffnung, Ausrüstung und Übung […]».[9]

Die «Kriegskunst» von Clausewitz entspricht also dem modernen Verständnis von Militärstrategie und sie umfasst – wieder in moderner Terminologie – die Verwendung von Streitkräften im bewaffneten Konflikt sowie die Weiterentwicklung von Streitkräften in Kriegs- oder Friedenszeiten. Auch weitere für die hiesige Methodik zentrale Elemente von Strategie hatte bereits Clausewitz nachdrücklich betont, namentlich die Dynamik des Kriegsgeschehens in dessen Verlauf und den politischen Primat (mit einem politischen «Zweck») gegenüber dem Militär (mit seinen militärischen «Zielen»).[10]

Während die Strategieanalyse der DSS im Sinne der Streitkräfteentwicklung in einem Folgeartikel in der MPR vorgestellt werden soll, geht es hier also um die Analyse von operativen Strategien. Dabei ist der theoretische Ausgangspunkt grundsätzlich das Modell von Lykke, welches zwar wirkungsmächtig, aber durchaus nicht unumstritten ist.[11] Das DSS-Modell nimmt diese Kritik auf und weicht von Lykkes Modell namentlich in drei Punkten ab: Die Methoden (ways) werden nicht mit den *military concepts* gleichgesetzt und sie werden schärfer umrissen (siehe unten). Sodann erscheint die Innenpolitik prominent mit den unverrückbaren Zielen: Machterhalt und Unterstützung für die gewählte Strategie. Schliesslich werden die militärischen Ziele nicht als Teil der Methode verstanden, sondern als eigenständige Ziele, die allerdings darauf ausgelegt sind, die Erreichung der politischen Zielsetzungen zu befördern.

… bei operativen Strategien kann die Verwendung der militärischen Mittel sowohl Anwendung im Gefecht bedeuten oder auch nur Drohung einer solchen Anwendung.

Aber auch bei operativen Strategien kann die Verwendung der militärischen Mittel sowohl Anwendung im Gefecht bedeuten oder auch nur Drohung einer solchen Anwendung. Denn bekanntlich wird oftmals auch mit der Drohung allein versucht, Wirkung auf das gegnerische Verhalten zu erzielen. Dieser Dualismus ist wichtig für das Verständnis der Analysemethodik, welche im Folgenden detailliert erklärt wird, sowohl *in abstractis* wie *in concreto.*

Das Analysemodell *in abstractis*

Das Analysemodell besteht zunächst aus einer Matrix (Abb. 1), welche im Gegenuhrzeigersinn auszufüllen ist, im Nachgang zu intensivem Studium der historischen Ereignisse allgemein und der Strategie der Gegenpartei(en) im Besonderen. Sie unterscheidet zunächst nach zivilen Macht-Mitteln, Methoden und Zielen (blau unterlegt) und militärischen Macht-Mitteln, Methoden und Zielen (grün unterlegt).

Die zentrale «Fixierung» jeder Strategie ist das Ziel, die eigene Machtbasis zu erhalten, mithin die innenpolitische Unterstützung für die Verfolgung der Strategie. Hierbei ist einzig zu fragen, mit welchen Macht-Mitteln und auf welche Art und Weise dies geschieht, wobei durchaus auch aussenpolitische Machtentfaltung diesem innenpolitischen Ziel indirekt dienen kann.

Der Ausgangspunkt der Strategieanalyse wiederum sind die erklärten politischen Ziele (Schritt 1). Sie sind leicht greifbar und in der Regel positiv formuliert, um eine Mehrheit der Machtbasis zufrieden zu stellen. Erklärte politische Ziele werden, wenn immer möglich, in lokale, regionale und globale Ziele aufgeteilt. Diese politischen Ziele werden direkt angestrebt durch eine Reihe von zivilen Mit-

6 «Military strategy may be declaratory or actual. In other words, as stated by our leaders, it may or may not be our real strategy.» Lykke, «Towards an Understanding of Military Strategy» (Fn. 4), S. 1–5.

7 Joint Chiefs of Staff, *Joint Doctrine Note 1-18, Strategy,* 25 April 2018, welche die übergeordneten Reglemente JP 1, Doctrine for the Armed Forces of the United States; JP 3-0, Joint Operations; und JP 5-0, Joint Planning operationalisiert. In der aktuellen Doktrin der Schweizer Armee findet sich ein Anklang an das Modell von Lykke: «Die Aufgabe der militärstrategischen Führung besteht darin, die drei Faktoren Ziele – Wege – Mittel unter Berücksichtigung des sicherheitsrelevanten Kontextes aufeinander abzustimmen.» Führung und Stabsorganisation der Armee 17 (FSO 17), Reglement 50.040 d, Ziffer 14.

8 Lykke, «Towards an Understanding of Military Strategy» (Fn. 4), S. 1–3.

9 Carl von Clausewitz, *Vom Kriege,* Breslau 1832, Zweites Buch «Über die Theorie des Krieges», I. Einteilung der Kriegskunst.

10 Ebd. (Fn. 9), Erstes Buch «Über die Natur des Krieges», I. Was ist der Krieg? (Kursiv im Original).

11 Vgl. etwa Jeffrey W. Meiser, «Are Our Strategic Models Flawed? Ends + Ways + Means = (Bad) Strategy», *Parameters*, Winter 2016-17, S. 81–91; M. L. Cavanaugh, «It's Time to End the Tyranny of Ends, Ways, and Means», *Modern War Institute At Westpoint,* 24.07.2017, https://mwi.usma.edu/time-end-tyranny-ends-ways-means/ (14.08.2018); Richard E. Berkebile, «Military Strategy Revisited: A Critique of the Lykke Formulation», *Military Review,* May 2018, S. 1–8.

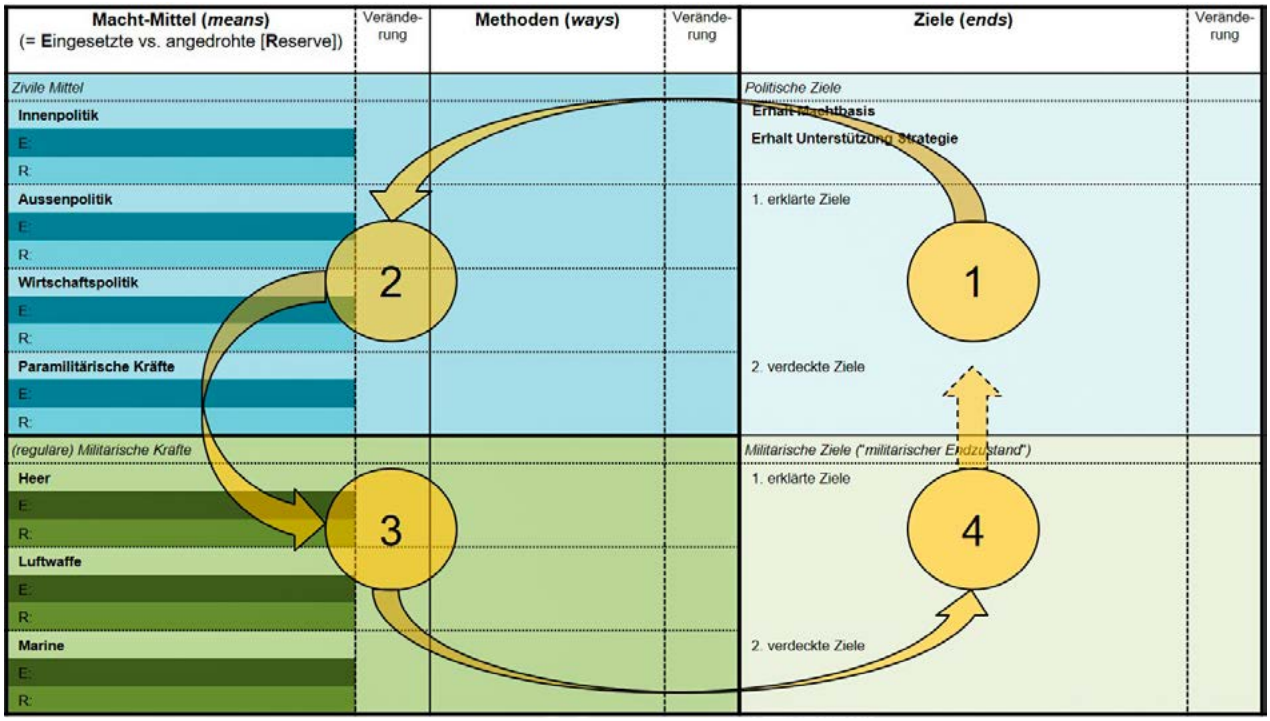


Abbildung 1 Die Analysematrix *in abstractis* mit vier Teilschritten (gelb), die im Gegenuhrzeigersinn zu bearbeiten sind. Dabei entspricht der Startpunkt den erklärten politischen Zielen (1), der Endpunkt den verdeckten politischen Zielen (DSS, MILAK).

teln, welche aussenpolitischer oder wirtschaftlicher Natur sind und/oder irreguläre oder paramilitärische Kräfte umfassen (Schritt 2). Die politischen Ziele werden jedoch auch indirekt angestrebt und zwar durch die Summe der militärischen Ziele, welche in der heutigen amerikanischen Doktrin «military end state» genannt wird (siehe unten). Diese Ziele werden auf eine bestimmte Art und Weise verfolgt, welche in der Spalte Methoden genauer zu beschreiben ist, nach ihrer Form (kombattant/zivil) und ihrem Wirkungsraum. Mit paramilitärischen Kräften können sowohl militärische wie auch politische Ziele verfolgt werden. Zu beachten ist, dass «Aussenpolitik» nicht den Kanal meint, sondern zweierlei Unterstützung der militärischen Bemühungen umfasst: zum einen jene seitens eigener ziviler Behörden, zum anderen solche von Seiten verbündeter Staaten.

In einem dritten Schritt werden die *regulären* militärischen Mittel – im Deutschen gewöhnlich als «Kräfte» bezeichnet – nach Teilstreitkräften aufgelistet. Wie schon bei den zivilen Mitteln soll auch hier mithilfe von Pfeilen angedeutet werden, wie sich die Intensität der Mittelverwendung über den Betrachtungszeitraum veränderte. Diese Veränderung kann, in starker Vereinfachung, durch ansteigende, absteigende, gleichbleibende oder geknickte Pfeile zum Ausdruck gebracht werden (s. unten). Diese haben eine leicht unterschiedliche Bedeutung: Im Falle der Mittel bezeichnen sie den quantifizierbaren Kräfteansatz, im Falle der Methoden die Intensität der Anwendung auf den Gegner und im Falle der Ziele die (relative) Bedeutung derselben im Vergleich zu anderen Zielen. Allgemein gilt, dass die Veränderungen umso grösser sind, je länger ein Krieg dauert.

Aus der Analyse der Verwendungsweise der militärischen Kräfte ergibt sich aber nicht nur eine Liste von (einzelnen) militärischen Zielen und eines militärischen Endzustandes, sondern auch eine Reihe von nicht erklärten politischen Zielen («hidden agenda»).

Mit den militärischen Mitteln werden einzelne politische wie auch militärische Ziele verfolgt, welche in der Regel nicht deklariert werden. Sie sollen aber in ihrer Summe einen «militärischen Endzustand» herbeiführen, welcher dem Erreichen eines «politischen Endzustandes» förderlich ist. Aus der Analyse der Verwendungsweise der militärischen Kräfte ergibt sich aber nicht nur eine Liste von (einzelnen) militärischen Zielen und eines militärischen Endzustandes, sondern auch eine Reihe von nicht erklärten politischen Zielen («hidden agenda»). Damit schliesst sich der «Analysezirkel».

Zu beachten ist, dass die Mittel (bzw. militärischen Kräfte) zwar auf eine bestimmte Art und Weise (Ways) angewendet werden und somit eine horizontale Zuordnung besteht. Mathematisch ausgedrückt, würde diese enge Verknüpfung von Mitteln und Methoden also eher einer Multiplikation als – wie bei Lykke – einer Addition entsprechen. Dies gilt aber nicht für die Ziele, die sich nicht linear aus nur einem einzigen Mittel und seiner Anwendung ergeben. Vielmehr können auch mehrere Mittel ein und demselben Ziel dienen. Dies erklärt, dass es keine (gestrichelten) horizontale Linien zwischen den Spalten Mittel und Methoden einerseits und der Spalte Ziele andererseits gibt.

Ebenfalls gilt es zu beachten, dass sich die Trennung zwischen der zivilen und der militärischen Sphäre in der Farbgebung der entsprechenden Quadranten äussert. Politische Ziele sind hellblau unterlegt, die ihnen entsprechenden Mittel und Methoden blau. Analog dazu die Unterscheidung in grüner Farbe bei den militärischen Zielen resp. Methoden und Mitteln.

Zwingend sind Erklärungen für Veränderungen von Zielen, Methoden und Mitteln, die viel mit dem bisherigen Kriegsverlauf und dem Agieren des Gegners, also der gegnerischen Strategie, zu tun haben.

Die Analysemethodik beschreibt also nur die Strategie *einer* Seite, sie bedarf aber eines vertieften Wissens des gesamten Kriegsgeschehens. Zwingend sind Erklärungen für Veränderungen von Zielen, Methoden und Mitteln, die viel mit dem bisherigen Kriegsverlauf und dem Agieren des Gegners, also der gegnerischen Strategie, zu tun haben. Insofern ist die Methodik äusserst anspruchsvoll. Dieser Problematik steht jedoch eine Reihe von Vorzügen gegenüber, auf welche am Schluss dieses Artikels eingegangen wird.

Das Analysemodell *in concreto:* Die US-Strategie in Vietnam

Das hier vorgestellte Analysemodell soll nachfolgend am Beispiel der amerikanischen Strategie in Vietnam vorgestellt werden, eingeschränkt auf den Zeitraum vom 7. August 1964 («Gulf of Tonkin Resolution» des amerikanischen Kongresses) bis 27. Januar 1973 (Vertrag von Paris). Es ist dies also eine zeitlich limitierte Betrachtung eines länger dauernden Konfliktes auf einem regionalen Kriegsschauplatz. Diese Wahl hat auch wesentlich damit zu tun, dass amerikanischerseits die Quellenlage zum Vietnamkrieg seit den 1970er Jahren günstig und die historische Forschung dementsprechend weit fortgeschritten ist. Dies erlaubt einen nuancierten Blick auf die tatsächlich verfolgte Strategie. Nicht zuletzt ist die Diskrepanz zwischen deklarierten und verdeckten zivilen bzw. militärischen Zielen für die amerikanische Strategie in Vietnam besonders gut fassbar.

Wie jede Strategieanalyse muss auch diejenige der amerikanischen Strategie für Vietnam im zeitgenössischen Kontext verortet werden. Dies gilt insbesondere für die übergeordneten politischen Ziele, denen die entsprechenden Methoden und Macht-Mittel dienen sollten. Der Kriegsschauplatz Südvietnam war geopolitisch und wirtschaftlich unbedeutend. Von Vietnam ging keine Bedrohung für die nationale Sicherheit der USA aus. Stattdessen ging es für die amerikanischen Entscheidungsträger darum, in der Hochphase des Ost-West-Konfliktes ein unmissverständliches Zeichen der eigenen Durchsetzungsfähigkeit, gerade auch in der sogenannten «Dritten Welt», zu setzen. John F. Kennedy brachte dieses Argument gegenüber einem Journalisten der *New York Times* im Jahr 1960 auf den Punkt: «[W]e have a problem in trying to make our power credible, and Vietnam looks like the place.»[12] Die Verantwortung für die Eskalation des Krieges kommt allerdings der Regierung von Lyndon B. Johnson zu. Ihre Entscheidungsfindung für eine «Amerikanisierung» des lodernden Bürgerkrieges in Südvietnam war nicht nur vom Ringen um Glaubwürdigkeit geprägt, sondern auch von der amerikanischen Überzeugung während des Kalten Krieges, das Vordringen des Kommunismus eindämmen zu müssen («Containment»).[13] Dieses Motiv war einerseits eng mit der innenpolitischen Angst einer Wiederkehr des McCarthyismus sowie andererseits mit der sogenannten «Dominotheorie» verbunden. Danach würden, wenn die USA ein Land an den monolithisch wahrgenommenen Kommunismus «verlören», Nachbarländer Gefahr laufen, ebenso von der «roten Strömung des Kommunismus überflutet» zu werden.[14] Johnson wollte demnach nicht Vietnam «verlieren», wie Truman zuvor China «verloren» hatte. Deshalb musste auf lokaler Ebene Südvietnam als eigenständiger, nicht-kommunistischer Staat erhalten werden. Für ein solches Nation Building brauchte es primär innenpolitische Stabilität, die mit einer Pazifizierungskampagne hergestellt werden sollte. Unter dem Commanding General des US Military Assistance Command, Vietnam (MACV), William C. Westmoreland, wurde Pazifizierung als «die Etablierung der inneren Sicherheit, der politischen Stabilität und der wirtschaftlichen Rentabilität» definiert. Pazifizierung war damit nicht nur ein politisches, sondern auch ein militärisches Ziel.[15] Diesbezüglich schrieb der COMUSMACV im August 1966, dass er nicht nur die kommunistischen Insurgenten und Aggressoren aus dem Norden besiegen, sondern auch die Sicherheit in bevölkerten und fruchtbaren Gegenden ausdehnen und alle Aspekte des Nation Buildings unterstützen wolle.[16]

Nicht zuletzt mussten die Regierungen Johnson und Nixon um den Erhalt ihrer Machtbasis und um die Unterstützung der eingeschlagenen Strategie besorgt sein; ein innenpolitisches Ziel also, dass die Voraussetzung einer jeden Strategie, besonders in demokratischen Gesellschaften, darstellt.

Darüber hinaus erhoffte sich die amerikanische Regierung, mit Südvietnam und dessen vornehmlich von den USA finanzierten Streitkräften einen strategischen Verbündeten zu schaffen und so im regionalen Kontext, d. h. im südostasiatischen Raum stabilisierend zu wirken. Die erhoffte Signalwirkung sollte im Kalten Krieg von glo-

12 John F. Kennedy zu James Reston, 1961, zit. nach David Halberstam, *The Best and the Brightest,* New York 1972, S. 76.
13 Vgl. John Lewis Gaddis, *Strategies of Containment: A Critical Appraisal of American National Security Policy During the Cold War,* New York [2]2005.
14 John F. Kennedy, 1956, zit. nach Guenter Lewy, *America in Vietnam,* New York 1978, S. 12–13.
15 James W. Johnson/Charles Anello, *Measurement of Pacification Progress in Vietnam,* September 1968, S. 8, zit. nach Gregory A. Daddis, *Westmoreland's War: Reassessing American Strategy in Vietnam,* New York 2014, S. 12.
16 William Westmoreland an Ulysses S. Grant Sharp und Earl Wheeler, 1966, zit. nach Daddis, *Westmoreland's War* (Fn. 5), S. 84.

Abbildung 2 Nach aussen gab sich William C. Westmoreland immer optimistisch. So auch während einer Pressekonferenz im Weissen Haus an der Seite von Lyndon B. Johnson und Dean Rusk, 07.04.1968 (Wikimedia Commons).

baler Reichweite sein. Das amerikanische Sendungsbewusstsein übersetzte sich in Südvietnam in die Etablierung amerikanischer, kapitalistischer Werte. Aufgrund der wirtschaftlichen Potenz letzterer erhofften sich die amerikanischen Entscheidungsträger, den asiatischen Kommunismus zurückdrängen zu können. Damit gingen handfestere politische Ziele einher. Auf der einen Seite strebten die USA besonders mit dem Fortgang des Krieges danach, vor den Augen der Weltöffentlichkeit einen erniedrigenden Gesichtsverlust gegen einen «viertklassigen Gegner» zu verhindern.[17] Sozialpsychologen verweisen diesbezüglich auf den Trugschluss der sogenannten «versenkten Kosten», wonach Entscheidungsträger nach einer gefühlten hohen Investition von Gütern und Menschenleben auf einer Weiterverfolgung des eingeschlagenen Weges beharren – selbst wenn sie wissen, dass die Erfolgsaussichten von Tag zu Tag geringer werden.[18] Nicht zuletzt mussten die Regierungen Johnson und Nixon um den Erhalt ihrer Machtbasis und um die Unterstützung der eingeschlagenen Strategie besorgt sein; ein innenpolitisches Ziel also, dass die Voraussetzung einer jeden Strategie, besonders in demokratischen Gesellschaften, darstellt.

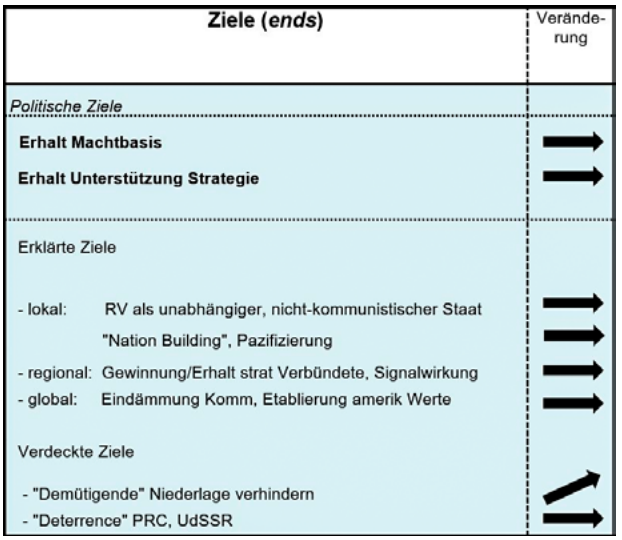


Abbildung 3 Quadrant 1: Die politischen Ziele der USA in Südvietnam im Zeitverlauf (DSS, MILAK).

Diese politischen Ziele sollten mit der Anwendung ziviler Mittel erreicht werden, die in Quadrant 2 schematisch erfasst werden. Da die amerikanische Bevölkerung die Strategie der Regierung unterstützen musste, wurde unter Johnson und Nixon eine Public-Relations-Offensive gestartet. Die offizielle Seite schönte Informationen, damit diese in ein siegreiches Narrativ passten. Wenn nötig wurde sogar gelogen, um der eigenen Bevölkerung die zeitgenössische Metapher des «Lichts am Ende des Tunnels» vorzugaukeln. Kritische Journalisten wie Morley Safer, David Halberstam, Malcolm W. Browne oder Neil Sheehan wiesen jedoch schon früh auf die Diskrepanz zwischen offiziellen Verlautbarungen und interner Lagebeur-

17 Henry A. Kissinger, 1969, zit. nach Seymour M. Hersh, *The Price of Power: Kissinger in the Nixon White House*, New York 1983, S. 126.
18 Siehe Fredrik Logevall, *Embers of War: The Fall of an Empire and the Making of America's Vietnam*, New York 2012 S. xx.

Abbildung 4 Verteidigungsminister Robert S. McNamara erklärt im Pentagon den anwesenden Journalisten die Kriegslage in Vietnam, 07.05.1965 (Wikimedia Commons).

Abbildung 5 Als der Krieg nach Hause kam: Die Ohio National Guard feuert Tränengas ab, um Studenten zu zerstreuen, die sich auf dem Campus der Kent State University in Ohio versammelt haben, um gegen den Krieg in Vietnam zu demonstrieren, 04.05.1970 (Wikimedia Commons).

teilung hin.[19] Dieser Widerspruch wurde wohl am deutlichsten von Robert S. McNamara personifiziert. Als der Verteidigungsminister im Herbst 1966 von einer Fact Finding Mission aus Südvietnam in die USA zurückflog, war er sich bewusst, dass sich die Lage in Vietnam im Vergleich zum Vorjahr überhaupt nicht verbessert hatte. Gegenüber seinen engsten Beratern sagte er an Bord des Flugzeuges sogar, dass die gegenwärtige Situation aufgrund des anhaltenden Widerstands der Gegenseite «eigentlich schlechter geworden» sei. Wenige Minuten nach der Landung aber strahlte McNamara vor versammelter Presse eine ganz andere Haltung aus: «Gentlemen, I've just come back from Vietnam, and I'm glad to be able to tell you that we're showing great progress in every dimension of our effort. I'm very encouraged by everything I've seen and heard over there.»[20] In das gleiche Horn stiessen auch Vertreter des MACV, zum Beispiel als dieses während eines internen Disputs mit der Central Intelligence Agency (CIA) bewusst tiefere Zahlen zur gegnerischen Stärke publizierte.[21] Aber auch der COMUSMACV kann sich dem Vorwurf nicht entziehen, die Öffentlichkeit getäuscht zu haben. Am 21. November 1967 verkündete Westmoreland vor dem National Press Club: «I am absolutely certain that whereas in 1965 the enemy was winning, today he is certainly losing. We are making progress [...] The enemy's hopes are bankrupt [...] We have reached an important point where the end begins to come into view.»[22]

Zehn Wochen nach Westmorelands überoptimistischer Ansprache – und zu Beginn des amerikanischen Präsidentschaftswahljahrs – lancierte die Nordvietnamesische Armee (NVA) und die Nationale Front für die Befreiung Südvietnams (NLF) mit ihren irregulären Kämpfern des «Vietcong» einen landesweiten Grossangriff in den städtischen Zentren Südvietnams. Die «Tet-Offensive» galt aber weniger den militärischen Zielen, als vielmehr dem politischen Rückhalt des Gegners. Bilder von Häuserkämpfen im Stadtzentrum von Saigon hatte in den USA niemand erwartet; die Blamage für die Regierung Johnson war perfekt. So wurde «Tet» nicht nur aussenpolitisch, sondern auch innenpolitisch zu einem Desaster für den Präsidenten. Als Westmoreland weitere 206 000 Truppen verlangte, lehnte Johnson erstmals ab.

Auch wenn die Offensive militärisch rasch zurückgeschlagen werden konnte, führte die Gesamtlage in Südvietnam mit etwas Verzögerung zur Absetzung McNamaras als Verteidigungsminister und Westmorelands als COMUSMACV sowie zum Verzicht Johnsons auf eine zweite Präsidentschaftskandidatur.

19 Siehe etwa David Halberstam, *The Making of a Quagmire: America and Vietnam During the Kennedy Era,* New York 1965; Ders., *The Best and the Brightest,* New York 1972; Malcolm W. Browne, *The New Face of War: A Report on a Communist Guerilla Campaign,* London 1965; Neil Sheehan, *A Bright Shining Lie: John Paul Vann and America in Vietnam,* New York 1988.

20 Robert S. McNamara, 1966, zit. nach Daniel Ellsberg, *Secrets: A Memoir of Vietnam and the Pentagon Papers,* New York 2002, S. 141–142.

21 Siehe Edwin E. Moise, "Order of Battle Dispute", in: Spencer C. Tucker (Hg.), *The Encyclopedia of the Vietnam War: A Political, Social, and Military History,* Santa Barbara [2]2011, S. 864–866; Robert Brewin/Sydney Shaw, *Vietnam on Trial: Westmoreland vs. CBS,* New York 1987.

22 William C. Westmoreland vor dem National Press Club, 1967, zit. n. David F. Schmitz, *The Tet Offensive: Politics, War, and Public Opinion,* Lanham 2005, S. 69.

Abbildung 6 Seite an Seite: Angehörige der 5. U.S. Special Forces Group mit verbündeten südvietnamesischen Soldaten der Spezialkräfte, 1968 (Wikimedia Commons).

Auch wenn die Offensive militärisch rasch zurückgeschlagen werden konnte, führte die Gesamtlage in Südvietnam mit etwas Verzögerung zur Absetzung McNamaras als Verteidigungsminister und Westmorelands als COMUSMACV sowie zum Verzicht Johnsons auf eine zweite Präsidentschaftskandidatur. Die Publikation der «Pentagon Papers» in der *New York Times* und *Washington Post* im Sommer 1971 bewies, dass das politische Establishment von Anfang an alles daran gesetzt hatte, die Öffentlichkeit zu täuschen und den Krieg illegal mit geheimen Operationen auszuweiten. Das Pentagon und die U.S. Army etwa vertuschten Kriegsverbrechen und Massaker amerikanischer und alliierter Truppen, wie das Massaker von «My Lai (4)», bei eine amerikanische Einheit über 500 Zivilisten ermordet hatten.[23] Die Folge dieser unlauteren Informationspolitik war ein politischer Feuersturm und eine Grundsatzdebatte um den ersten Verfassungszusatz, das Recht auf freie Meinungsäusserung.

Längerfristig manifestierte sich eine Glaubwürdigkeitskrise und ein breites Misstrauen der Öffentlichkeit in politische wie auch militärische Institutionen. Denn Nixons Regierung machte dort weiter, wo die Administration Johnson aufgehört hatte. Auch Creighton W. Abrams, der neue COMUSMACV, war nach Sicht der jüngeren Forschung sehr auf Kontinuität mit Westmoreland bedacht. Mehr noch, die Ächtung innen- und aussenpolitischer Feinde erreichte unter «Tricky Dick» eine erneute Klimax; sogar das Abhören und Bespitzeln politischer Gegner erschien Nixon als legitimes Mittel, um grösstmögliche Geheimhaltung und Manipulation für seine Vietnam-Strategie zu erhalten.[24] Die CIA hatte schon seit 1967 Kriegsgegner mit der Operation Chaos im In- und Ausland überwacht.[25] Die Mobilisierung der Nationalgarde zum Kriegsdienst in Südvietnam hätte wahrscheinlich innen- und aussenpolitische Konsequenzen nach sich gezogen, die Johnson nicht eingehen wollte; folglich wurde sie nur im Inneren eingesetzt.

Um den Vorwurf zu entkräften, dass der Vietnamkrieg ein amerikanischer Alleingang sei, erbaten die Vereinigten Staaten und die Republik Vietnam die Unterstützung anderer Nationen der «freien Welt»: Australien, Neuseeland, Südkorea, Taiwan und Thailand entsandten Truppen ins Land an der Mekongmündung, die als Free World Military Assistance Forces (FWMAF) der amerikanischen Militärdoktrin folgten und zumeist unter Kommando des MACV standen (anders als die südvietnamesischen Streitkräfte).[26] Zivile Akteure wie das Aussenministerium der Vereinigten Staaten, die United States Agency for International Development (USAID) und die United States Information Agency (USIA) wurden in die Kriegführung eingespannt, um Hilfe vor Ort zu leisten oder Kontakte zur südvietnamesischen Bürokratie zu pflegen.

Schon bevor die ersten Marines im Frühling 1965 in Da Nang an Land gingen, waren sogenannte Strategic Hamlets eingerichtet worden. In diese Wehrdörfer wurden südvietnamesische Bauern umgesiedelt, um diese dem Einfluss der kommunistischen Guerilla zu entziehen. Mit

23 Siehe zum Beispiel Seymour Hersh, *My Lai 4: A Report on the Massacre and Its Aftermath*, New York 1970; ders. *Cover-Up: The Army's Secret Investigation of the Massacre at My Lai 4*, New York 1972.

24 Kenneth Franklin Kurz, *Nixon's Enemies*, Los Angeles 1998, S. 13, 275.

25 Paul G. Pierpaoli, Jr., «Chaos, Operation», in: Tucker, *Encyclopedia of the Vietnam War*, S. 186–187.

26 Stanley Robert Larsen/James Lawton Collins Jr., *Allied Participation in Vietnam*, Washington DC 1975.

der Eskalation des Krieges 1965 wurden diese Massenumsiedlungen allerdings gestoppt. Das ehrgeizige Programm wurde jedoch bald unter dem neuen Namen New Life Hamlets erneut gestartet, ohne die gewünschten Erfolge zu erzielen. Ein Mangel an kulturellem Verständnis führte zum Scheitern der Umsiedlungsmassnahmen und zu grossem Leid unter den etwa fünf Millionen zwangsmigrierten Südvietnamesen – rund einem Drittel der damaligen Gesamtbevölkerung Südvietnams.[27] Für Dörfer ausserhalb der New Life Hamlets wurden Messmethoden wie das Hamlet-Evaluation System oder das Pacification Attitude Analysis System eingeführt, um den Grad der Pazifizierung, meist eine blosse Zahl, zu ermitteln. Hierfür wurden Daten auf monatlicher Basis von 9 000 der 13 000 Dörfer in Südvietnam erhoben und dann in einer Matrix nach rund 18 Indikatoren evaluiert.[28]

In wirtschaftlicher Hinsicht war der Boykott Nordvietnams die logische Folge der Tonkin-Resolution. Der militärische Einmarsch in Nordvietnam war für die USA angesichts des Eskalationsrisikos durch die beiden kommunistischen Atommächte UdSSR und die Volksrepublik China keine gangbare Option. Damit war die militärisch schlagkräftigste Vorgehensweise gegenüber dem Norden der Wirtschafts- und Bombenkrieg. Einerseits wurden die spärlichen wirtschaftlichen Exporte des Agrarstaates boykottiert, andererseits die militärischen und logistischen Zentren Nordvietnams mit einem ausgedehnten Bombenkrieg angegriffen. Innenpolitisch umstrittener war der Einsatz des amerikanischen Auslandgeheimdienstes in Südvietnam. 1947 aus dem Office for Strategic Services (OSS) hervorgegangen, war die CIA in Südvietnam nicht nur für die Sammlung und Analyse von Informationen zuständig, sondern auch für verdeckte Operationen. Auf dem Höhepunkt des Vietnamkrieges verfügte sie über ein umfangreiches Netzwerk von Agenten und Beamten, so dass ihre Vertretung in Südvietnam die grösste ausserhalb der USA war. Im Nachbarland Laos lancierte die CIA gemeinsam mit der lokalen Bevölkerung einen verdeckten Krieg gegen die kommunistische Pathet Lao. In Südvietnam ging es ihr primär darum, die sogenannte Viet Cong Infrastructure (VCI) zu zerstören. Die umstrittenste und brutalste Kampagne der CIA war das Phoenix Program (Phung Hoang), das 1968 lanciert wurde. «Phoenix» sollte in Südvietnam Kader des Vietcong identifizieren und mittels südvietnamesischen Provincial Reconnaissance Units (PRU) durch Verhaftungen, Folter, Fahnenflucht oder Mord neutralisieren.[29] Zudem schuf die US-Botschaft in Saigon im November 1966 das Office of Civil Operations (OCO), das zivile Mitarbeiter von CIA und USAID zusammenfasste, um Pazifizierungskampagnen wie Flüchtlingshilfe oder psychologische Operationen durchzuführen. Da das OCO hinter seinen Pazifizierungszielen zurückblieb, beauftragte Präsident Johnson das MACV 1967 damit, das Office of Civil Operations and Revolutionary Development Support (CORDS) als Nachfolgeorganisation von OCO zu gründen. Unter der Ägide des ehemaligen CIA-Analysten Robert W. Komer fielen nun alle Pazifizierungsoperationen, egal ob zivil oder militärisch, in die Zuständigkeit von CORDS und damit des MACV. Das Personal rekrutierte sich aus den Streitkräften, dem Aussenministerium, der USAID, CIA, United States Information Agency (USIA) und dem Weissen Haus.[30] Das Beispiel CORDS zeigt, dass Methoden im hiesigen Analyseschema nicht immer eindeutig den entsprechenden Mitteln zugeordnet werden können. So könnte OCO/CORDS auch als aussenpolitisches Mittel gesehen werden.

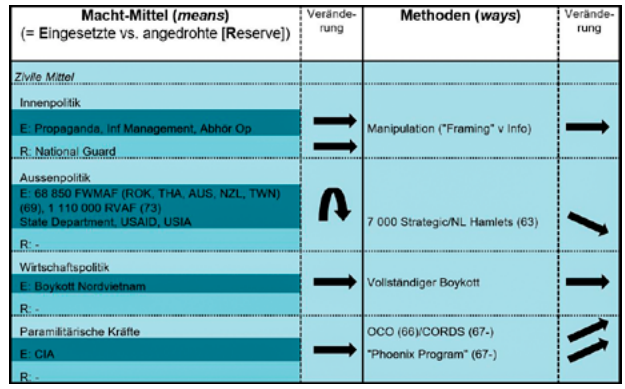


Abbildung 7 Quadrant 2: Die zivilen Macht-Mittel und Methoden der USA in Südvietnam in Zeitverlauf (DSS, MILAK).

Im Wissen darum, dass eine Resolution des Kongresses unter den Vorzeichen eines gegnerischen Angriffs leichter zu Stande kommen würde, hatte Johnson den Zwischenfall im Golf von Tonkin ausgenutzt, um einen Blankoscheck für die Anwendung militärischer Gewalt zu erhalten. Die Tonkin-Resolution erlaubte es dem Präsidenten, ohne formelle Kriegserklärung den Einsatz militärischer Kräfte gegen Nordvietnam zu befehlen. Johnson zeigte sich damit sehr zufrieden und verglich das Dokument mit «Grossmutters Nachthemd, [es] deckte alles.»[31] Dazu gehörte auch die Mobilisierung der Streitkräfte. Als erstes wurde von der Luftwaffe Gebrauch gemacht, die als Vergeltung Operation Pierce Arrow und gemeinsam mit der südvietnamesischen Luftwaffe Operation Flaming Dart flog, welche militärischen Zielen in Nordvietnam galten. Gefolgt wurde «Flaming Dart» von Operation Rolling Thunder, die von 1965 mit Unterbrüchen bis 1968 nordvietnamesische Ziele angriff.[32] Solche strategischen Bombardierungen blieben den ganzen Krieg über erhalten und richteten sich zusehends auch gegen feindliche Ziele in Südvietnam. Der Luftkrieg wurde aber auch auf Kambodscha und Laos ausgeweitet, um dem Vietcong die Infiltration und den Nachschub via Ho-Chi-Minh-Pfad zu verunmöglichen. Schon ab 1962 setzte die Luftwaffe im Rahmen der Operation Ranch Hand das Entlaubungsmittel Agent Orange und andere dioxinhaltige Chemikalien ein, um den Dschungel zu entlauben und dem Gegner die Rückzugs-

27 Christian G. Appy, *American Reckoning: The Vietnam War and Our National Identity,* New York 2015, S. 29.
28 John D. Root, «Hamlet Evaluation System», in: Tucker, *Encyclopedia of the Vietnam War,* S. 449; Gregory A. Daddis, *No Sure Victory: Measuring U.S. Army Effectiveness and Progress in the Vietnam War,* Oxford 2011, S. 118–122; Tran Dinh Tho, *Pacification,* Washington DC 1980, S. 106–108; 206.
29 Michael Share/James I. Matray, «CIA», in: Tucker, *Encyclopedia of the Vietnam War,* S. 183–184; Dale Andradé, *Ashes to Ashes: The Phoenix Program and the Vietnam War,* Lexington 1990; Douglas Valentine, *The Phoenix Program,* New York 1990.
30 Daddis, *Westmoreland's War* (Fn. 15), S. 127–132.
31 Lyndon B. Johnson, undatiert, zit. nach Marc Frey, *Geschichte des Vietnamkriegs: Die Tragödie in Asien und das Ende des amerikanischen Traums,* München ^{9}2010, S. 104.
32 Mark Clodfelter, *The Limits of Air Power: The American Bombing of North Vietnam,* New York 1989; Ronald B. Frankum, Jr., *Like Rolling Thunder: The Air War in Vietnam,* 1964–1975, New York 2005.

räume zu entziehen.[33] Die Brandwaffe Napalm wurde zu einem Symbol des Vietnamkrieges. Napalmbomben und andere Brandwaffen wurden von der US-Luftwaffe über vermuteten Stellungen des Vietcongs abgeworfen und führten bei den Überlebenden zu sehr schlecht verheilenden Verbrennungen. Napalm wurde allerdings auch von Einheiten der Army und der Navy eingesetzt.[34] Zudem wurden konventionelle Bomben über Süd- und Nordvietnam sowie einigen Nachbarstaaten Vietnams abgeworfen. Das wiedervereinte Vietnam wies nach dem Krieg rund 26 Millionen Bombenkrater auf. Alliierte Kampfflugzeuge hatten über Vietnam, Laos und Kambodscha 2 865 808 t Bomben ausgeklinkt – ca. 800 000 t mehr als auf allen Schauplätzen des Zweiten Weltkrieges zusammen.[35]

Abbildung 8 Der nationale Sicherheitsberater Walt Rostow brieft Lyndon B. Johnson im Situation Room zur Kriegslage in und um Khe Sanh, 15.02.1968 (Wikimedia Commons).

Alliierte Kampfflugzeuge hatten über Vietnam, Laos und Kambodscha 2 865 808 t Bomben ausgeklinkt – ca. 800 000 t mehr als auf allen Schauplätzen des Zweiten Weltkrieges zusammen.

Am Boden waren Verbände aus U.S. Army und USMC damit beschäftigt, den Gegner mit einer Abnutzungsstrategie aufzureiben. «Search and Destroy» (S&D) war die Doktrin, die den Vietcong und dessen Nachschub aufzuspüren und zu vernichten suchte. Dabei wurde ausgiebig von Helikoptern Gebrauch gemacht. Die Air Mobility und die Reorganisation der 1st Cavalry Division hatten zum Ziel, Soldaten schnell in die abgelegensten Gebiete Südvietnams verlegen zu können. Von Kriegsbeginn an war klar, dass es in Südvietnam keine napoleonischen Entscheidungsschlachten geben würde. Deshalb konnte der vermeintliche Fortschritt nicht mittels eines konventionellen Erfolgsmassstabes, wie der Eroberung gegnerischen Territoriums, gemessen werden. Stattdessen massen die in Südvietnam zum Einsatz kommenden sieben Army- und zwei USMC-Divisionen ihren Kriegsfortschritt mittels «Body Count» und anderer statistischer Methoden.[36] Diese Präferenz für harte Zahlen führte dazu, dass der Druck auf vermeintlichen Kriegsfortschritt zunehmend auf der Truppenebene durchschlug. Einheiten, die einen hohen «Body Count» vorweisen konnten, erhielten Belohnungen in Form von Urlaubstagen, Extraverpflegung oder Beförderungen. Statistisch erhoben wurde auch die Anzahl der übergelaufenen NVA-Soldaten und Vietcong-Kämpfer. Um solche Fahnenfluchten zu erleichtern, wurde das südvietnamesische «Chieu Hoi Program» geschaffen, das gegnerische Soldaten dazu bewegen sollte, sich der eigenen Seite anzuschliessen.[37]

Abbildung 9 «Feuer fällt vom Himmel»: Die nackte, neun Jahre alte Phan Thi Kim Phuc flüchtet aus ihrem Dorf Trang Bang mit Napalmverbrennungen. Südvietnamesische Soldaten folgen ihr. Das Bild von Huynh Cong «Nick» Ut gewann 1972 den Pulitzer-Preis für das Pressefoto des Jahres (Wikimedia Commons).

Abbildung 10 Search and Destroy und Body Count: Bell UH-1 Iroquois Militärhelikopter laden Truppen im Feld ab, 1965 (Wikimedia Commons).

33 Siehe Michael Gough, *Dioxin, Agent Orange: The Facts,* New York 1986.
34 Siehe Robert M. Neer, *Napalm: An American Biography,* Cambridge 2013.
35 Bernd Greiner, *Krieg ohne Fronten,* Hamburg 2007, S. 41.
36 Daddis, *No Sure Victory* (Fn. 28); Marcel Berni, «Hearts and Minds and Body Count: The Mathematization of War in Vietnam (1965–1972)», in: Tobias Hof (Hg.), *Empire, Ideology, Mass Violence: The Long 20th Century in Comparative Perspective,* München 2016, S. 175–202.
37 Tho, *Pacification* (Fn. 28), S. 134–136.

Einheiten, die einen hohen «Body Count» vorweisen konnten, erhielten Belohnungen in Form von Urlaubstagen, Extraverpflegung oder Beförderungen.

Dass sich der Vietcong gar nicht erst in den ländlichen Dörfern Südvietnams etablieren konnte, war das Ziel des Programms Civilian Irregular Defense Group (CIDG). CIDG bestand aus Spezialkräften der Army, die in den Ortschaften des zentralen Hochlandes verstärkte «Montagnard Villages» einrichteten. An Ort und Stelle wurden dafür rudimentäre Selbstverteidigungsgruppen aus dem Stamm der Montagnards ausgebildet. Im Falle eines kommunistischen Überfalles auf einen Ort sollten diese Montagnards die Speerspitze in der Bekämpfung des Gegners darstellen.[38] Ähnliche lokale Pazifizierungskampagnen wie das Combined Lightning Initial Project der 25th Infantry Division, das Good Neighbor Program der 4th Infantry Division oder die Operation Rolling Stone der 1st Infantry Division wurden von Angehörigen regulärer Infanteriedivisionen durchgeführt.[39] Bei den Marines hiess die entsprechende Operation Combined Action Program (CAP).[40] Auf hoher See und auf den Flussarmen des Mekongdeltas war es Aufgabe der Marine, für die Unterstützung des Boden- und Luftkrieges zu sorgen; ab 1972 wurde sie zudem für die Seeblockade und die Verminung Haiphongs eingesetzt. Der militärische Einmarsch in Nordvietnam und die Besetzung Hanois standen hingegen nie zur Debatte.

Auch der Einsatz von Nuklearwaffen war angesichts des Eskalationsrisikos des Kalten Krieges und Überlegungen zur Proportionalität praktisch ausgeschlossen. Dennoch unterliess es Nixon nicht, mit dem Einsatz von Nuklearwaffen gegen Nordvietnam zu drohen: «I call it the Madman Theory […] I want the North Vietnamese to believe I've reached the point where I might do *anything* to stop the war. We'll just slip the word to them that, ‹for God's sake, you know Nixon is obsessed about Communism. We can't restrain him when he's angry – and he has his hand on the nuclear button› – and Ho Chi Minh himself will be in Paris in two days begging for peace.»[41] Dieser Bluff kann als ein Beispiel für in Reserve gehaltene Macht-Mittel als Teil einer Strategie gesehen werden. Nixons Drohung zeigte jedoch keine Wirkung und der Präsident sah sich gezwungen, an den schon unter Johnson zum Einsatz gelangten Mitteln und Methoden festzuhalten. Allmählich setzte sich in Washington nämlich die Überzeugung durch, dass Alternativen zur Bombardierung des Nordens «leider» nur schwer zu bekommen waren.[42]

Als jedoch in Washington immer klarer wurde, dass der Krieg in Südvietnam nicht zu gewinnen war, wurde versucht, eine möglichst günstige Position für die Friedensverhandlungen zu schaffen.

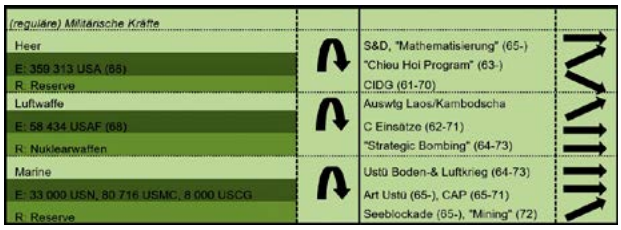


Abbildung 11 Quadrant 3: Die militärischen Macht-Mittel und Methoden der USA in Südvietnam im Zeitverlauf (DSS, MILAK).

Mit diesen militärischen Mitteln und Methoden sollten primär militärische Ziele erreicht werden, welche die Voraussetzung für die Erfüllung der politischen Ziele darstellten. Noch vor der Eskalation des Bodenkrieges hatten amerikanische Berater die südvietnamesischen Streitkräfte auszubilden und materiell sowie finanziell zu unterstützen. Mit der unter Nixon eingeläuteten «Vietnamisierung» sollte der Krieg Schritt für Schritt an die südvietnamesischen Streitkräfte abgetreten werden, welche die Kriegsbemühungen nach dem Frieden von Paris auch tatsächlich übernehmen sollten. Von Beginn an hatten die verbündeten südvietnamesischen, amerikanischen und FWMAF-Truppen das Ziel, den kommunistischen Aufstand im Süden auszuschalten und die Infiltration des Südens aus dem Norden und aus den Nachbarländern Laos und Kambodschas zu unterbinden. Zuletzt sollten die «Hearts and Minds» der lokalen Bevölkerung gewonnen werden; nur so konnte die Pazifizierung erfolgreich sein.[43] Als jedoch in Washington immer klarer wurde, dass der Krieg in Südvietnam nicht zu gewinnen war, wurde versucht, eine möglichst günstige Position für die Friedensverhandlungen in Paris zu schaffen.

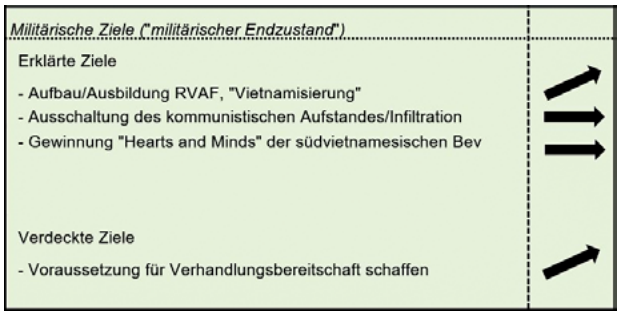


Abbildung 12 Quadrant 4: Die militärischen Ziele der USA in Südvietnam im Zeitverlauf (DSS, MILAK).

Fasst man alle Hauptmerkmale zusammen, so präsentiert sich eine retrospektive Strategieanalyse wie in Abbildung 13 dargestellt.

38 Hieu Dinh Vu/Harve Saal, «Civilian Irregular Defense Group», in: Tucker, *Encyclopedia,* S. 209.
39 Daddis, *Westmoreland's War (Fn. 15),* S. 101–104, 112.
40 Michael E. Peterson, *The Combined Action Platoons: The U.S. Marines' Other War in Vietnam,* New York 1989.
41 Richard Nixon, zit. nach H. R. Haldeman/Joseph DiMona, *The Ends of Power,* London 1978, S. 96 (kursiv im Original).
42 Henry A. Kissinger, zit. n. ders., Bombing Cambodia: A Defense, in: Andrew J. Rotter (Hg.), *Light at the End of the Tunnel:* A Vietnam War Anthology, Lanham ^{3}2010, S. 298–309, hier S. 298.
43 Siehe Richard A Hunt, *Pacification: The American Struggle for Vietnam's Hearts and Minds,* London ^{2}2018.

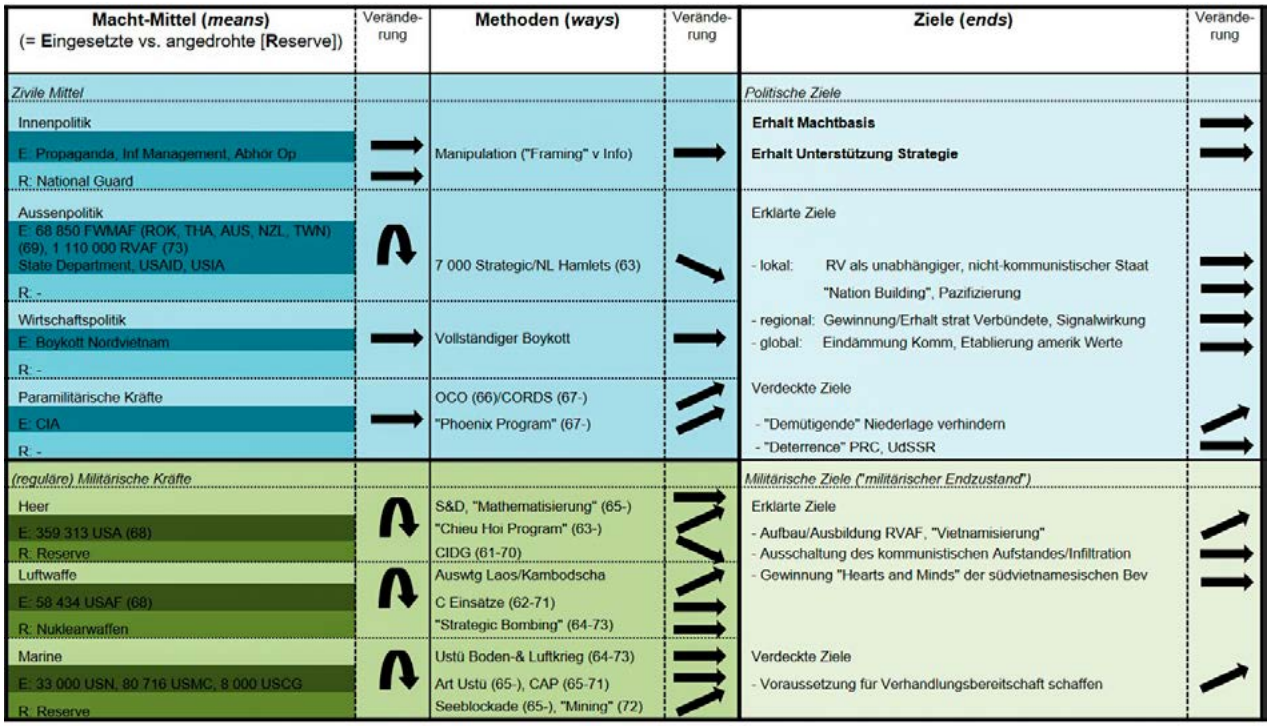


Abbildung 13 Synopse der amerikanischen Strategie in Südvietnam für den Zeitraum August 1964 bis Januar 1973 mit den jeweiligen Höchstzahlen und den spezifischen Jahresangaben in Klammern (DSS, MILAK).

Fazit

Das Analysemodell für operative Strategie der DSS will die Wirkungszusammenhänge zwischen den drei Komponenten von Lykke aufzeigen und darstellen. In keiner Weise wird damit angestrebt, eine Strategie zu bewerten, sei es – wie es Lykke fordert – nach Ausgewogenheit ihrer Komponenten, nach Angemessenheit von Mitteln und Methoden oder nach dem Grad des Erfolges bzw. der Zielerreichung. Die ausgefüllte Matrix ist dabei das Endprodukt einer eingehenden Anwendung der Analysemethodik. Die inhaltliche Erarbeitung ist anspruchsvoll und aufwendig und die Präsentation erfordert fundierte Kenntnisse des Kriegsverlaufs einerseits, der gegnerischen Strategie andererseits, denn viele Anpassungen einer Strategie erfolgen in Reaktion auf entsprechende Aktionen (oder Adaptionen der Strategie) beim Gegner. Nur so können die gezeigten Wirkungszusammenhänge auch begründet werden.

Diese neuartige Analysemethodik weist einen doppelten Vorzug auf:

Es wird damit Strategie operationalisiert, d. h. der Forscher wird gezwungen, die Analyse der Strategie einer Konfliktpartei strukturiert vorzunehmen und offenzulegen. Dies beinhaltet auch, dass er Rechenschaft darüber ablegt, welche der – theoretisch unendlich vielen – Komponenten einer Strategie wirklich wichtig sind und wie sie über einen längeren Zeitraum zusammenspielen und sich verändern.

Das Endprodukt dieser Strategieanalyse wird dem Adressaten in Form einer Synthese präsentiert, also einer *Gesamtdarstellung* der betreffenden Strategie mit ihren wichtigsten Elementen, ihrer Dynamik und ihren Wirkungszusammenhängen über den gewählten Zeitraum, der ebenfalls zwingend offenzulegen und zu begründen ist. Die Synthese wird zur Synopse, in welcher eine Strategie für den Leser oder Zuhörer vollständig manifest wird, was ihm – etwa während des Vortrages – auch erlaubt, «zurückzusteigen» oder vorauszublicken. Er kommt so in den Genuss des «integralen Lagebildes» – anders als beim konventionellen, seriell präsentierten Foliensatz. Kurzum, mit dieser Analysemethodik wird Strategie zu einer *organisierten, disziplinierten intellektuellen Aktivität,* ganz im Sinne von Rear Admiral J. C. Wylie.

Abkürzungsverzeichnis

AUS	Australien
C Einsätze	Einsätze von Chemiewaffen
CIA	Central Intelligence Agency
CIDG	Civilian Irregular Defense Group
COMUSMACV	Commander-in-Chief US Military Assistance Command Vietnam
CORDS	Civil Operations and Revolutionary Development Support
FWMAF	Free World Military Assistance Forces
Inf	Information
Komm	Kommunismus
MACV	Military Assistance Command Vietnam
NL Hamlets	New Life Hamlets
NZL	Neuseeland
OCO	Office of Civil Operations
OSS	Office for Strategic Services
Op	Operation
PRC	Volksrepublik China
PRU	Provincial Reconnaissance Unit
ROK	Republic of Korea

RV	Republic of Vietnam
RVAF	Republic of Vietnam Armed Forces
S&D	Search & Destroy
THA	Thailand
TWN	Taiwan
UdSSR	Union der Sozialistischen Sowjetrepubliken
USA	United States Army
USAF	United States Air Force
USAID	United States Agency for International Development
USCG	United States Coast Guard
USIA	United States Information Agency
USMC	United States Marine Corps
USN	United States Navy
Ustü	Unterstützung
VCI	Vietcong Infrastructure

Mauro Mantovani

Dr. phil., Dozent Strategische Studien MILAK/ETHZ.

E-Mail: mauro.mantovani@vtg.admin.ch

Marcel Berni

M.A., wissenschaftlicher Assistent Dozentur Strategische Studien MILAK/ETHZ, Verfasser einer Dissertation über den Vietnamkrieg, die voraussichtlich 2019 erscheinen wird.

E-Mail: marcel.berni@vtg.admin.ch

Spin Politics – Machtpolitik *anders* lesen

Propaganda war gestern. Heute sind Infrastrukturen, Technologien und die Wirtschaft aber auch PSYOPS sowie CYBEROPS wirkungsvolle Mittel der Konfliktführung. Sie können bewusst diffuse Bedrohungslagen unterhalten um machtpolitische Zielsetzungen zu realisieren. Dies fordert neue Massstäbe der geopolitischen Risikobeurteilung. In diesem Artikel wird argumentiert, dass Operationssphären heute hochgradig vernetzt sind. Dabei wird der Umgang mit der Informationssphäre immer zentraler. Um die Verschränkungen des Informationsraums besser begreifen zu können, werden die Verflechtungen mit dem Begriff *Spin Politics* umschrieben. Die machtpolitischen Ambitionen Chinas illustrieren exemplarisch wie Geopolitik und Militärstrategie betrieben wird.

Remo Reginold

Einleitung

Mit einer multipolaren Weltordnung und der rasanten Vernetzung der Welt ist Machtpolitik[1] heute verschwommener und unberechenbarer denn je. In diesem Artikel wird argumentiert, dass globale Mächteverhältnisse nicht mehr eindeutig auszumachen sind und rein militärische Drohgebärden oft ihre Wirkung verfehlen. In einer solchen Welt werden Informationen, Bilder und Symbole wichtiger. Diese Mittel werden in der strategischen Kommunikation (STRATCOM) zur bewussten Irreführung und Beeinflussung eingesetzt. Nebst ihrer strategischen Bedeutung können Informationen und ihre Träger durchaus unvorhergesehene Aktionen oder Reaktionen auslösen: *Vordergründiges wird plötzlich Beiläufiges und Beiläufiges wird Vordergründiges*. Bestimmende Strukturen, aber auch zufällige Einzelereignisse, stehen heute in einem diffusen Wechselspiel. Diese Unbestimmtheit kann geopolitisch ungeahnte Handlungen, Ereignisse und Fakten produzieren. Mit diesen Effekten wird die strategische Analysearbeit schwieriger. Deswegen werden in der nachrichtendienstlichen Arbeit quellen- und interpretationskritische Anstrengungen zunehmend entscheidender. Nur so können Informationen in einen Gesamtkontext gebracht und strategisch ausgewertet werden.

Box 1: Allgemeine Begriffsbestimmungen
Geopolitik ist die staatliche Praxis, Territorien für sich in Anspruch zu nehmen und zu kontrollieren. In einem weiteren Sinn ist Geopolitik auch die Fähigkeit, die Welt in ihrer Komplexität zu lesen.

Geostrategie bildet die Entscheidungsgrundlage, damit Staaten ihre territorialen Ansprüche zu ihren Gunsten durchsetzen können.

Machtpolitik ist die staatliche Fähigkeit, eigene Ansprüche und Interessen mittels Druckmitteln und Aktionen geltend zu machen.

Dieser Artikel versucht darzulegen, dass unter machtpolitischen Zusammenhängen die Operationssphäre *Informationsraum*[2] (vgl. Abb. 1) kein definierter Raum mehr ist.[3] Als Medium von Informationen ist der Informationsraum

1 Begriffe wie *Machtpolitik*, *Geopolitik* und *Geostrategie* können unterschiedliche Bedeutungen haben und werden in der Forschungsliteratur dementsprechend unterschiedlich bewertet. In Box 1 sind die Ausdrücke definiert, wie sie im Artikel gebraucht werden.

2 Das Informationszeitalter und die Wissensgesellschaft zeichnen sich durch die horizontale Verstrickung von Informationen aus. In diesem Zusammenhang schreibt der Soziologe und Netzwerktheoretiker Manuel Castells: «The shift from traditional mass media to a system of horizontal communication networks organized around the Internet and wireless communication has introduced a multiplicity of communication patterns at the source of a fundamental cultural transformation, as virtuality becomes an essential dimension of our reality» (Castells 2010: xviii). Diese polyzentrischen Verflechtungen kreieren neue Beziehungen zu Raum und Zeit und verschieben die Wahrnehmungen von Geographie, Macht und Akteuren; vgl. Daniel Krauer und Anita Noli-Kilchenmann zur Militärdoktrin 17: «Die hybride Bedrohung und ihre Wesenszüge stellen neuartige Herausforderungen für die Schweiz und deren Sicherheitsarchitektur dar. Um dieser veränderten Gestalt der Bedrohung entgegentreten zu können, ergeben sich grundsätzliche Anforderungen an die Sicherheitsarchitektur der Schweiz und demnach auch an die Schweizer Armee (Fähigkeitskatalog). (...) In hybriden Konflikten gewinnen der Cyber-, der Informations- und der Elektromagnetische Raum an Bedeutung» (Krauer und Noli-Kilchenmann 2016:15).

3 Entgegen der Militärdoktrin ist der Informations- wie auch der Cyberraum weder auf den öffentlichen Raum noch auf die herkömmlichen und neuen Medien zu reduzieren (cf. Krauer und Noli-Kilchenmann 2016: 14).

mehr als alle anderen stark mit den restlichen Operationssphären verschränkt. Diese inhaltliche Verschränkung eröffnet neue geopolitische Interpretationszusammenhänge, die weder einfach einzuordnen noch zu klassifizieren

sind: *Es ist eine Systematik die keine ist* (vgl. Box 2). Die Verbreitung von diffusen Bedrohungslagen und unkonventionellen Beeinflussungsmitteln fordern deshalb neue Massstäbe der Risikobeurteilung, um Geo- und Machtpolitik greifbarer zu machen.

Box 2: Mit Komplexität leben
«Weil die Welt komplex ist, fehlen uns immer Informationen. Weil Informationen fehlen, sind wir immer unsicher. Weil wir unsicher sind, gibt es für uns keine wahre Antwort, sondern nur den Konflikt der Meinungen. Zwietracht, Widerstreit, Dissens. Deshalb müssen wir ohne Grundlagen leben und Abschied vom Prinzipiellen nehmen» (Bolz 2017: 37).

Spin Politics will hinter den Vorhang von klassischer Machtpolitik, Propaganda und STRATCOM schauen, denn hinter machtpolitischen Handlungen können globale, lokale und unsichtbare Akteure ihre Partikularinteressen auf vielfältige Weise verschleiern und instrumentalisieren (Hidden Agenda).

Um die Verschränkung des Informationsraums besser verstehen zu können, wird in diesem Artikel der Begriff *Spin Politics*[4] eingeführt. In Kontrast zu Spin Linguistics, Propaganda und Rhetorik, die vornehmlich auf die Deutung der Welt mittels semantischen[5] und bildlichen Mitteln verweisen (vgl. Box 3), erweitert Spin Politics den Begriff der Information auf die semiotische Deutung[6] der Welt. Damit werden Handlungen und Ereignisse, die nicht nur sprachlicher und symbolischer Natur sind, zentral und bedeutungsvoll. Mit dieser inhaltlichen Erweiterung wird dem Analyseniveau von geopolitischen Zusammenhängen höhere Rechnung getragen und nicht mit Propaganda oder STRATCOM gleichgesetzt. Spin Politics will hinter den Vorhang von klassischer Machtpolitik, Propaganda und STRATCOM schauen, denn hinter machtpolitischen Handlungen können globale, lokale und unsichtbare Akteure ihre Partikularinteressen auf vielfältige Weise verschleiern und instrumentalisieren (vgl. Hidden Agenda). Hinter dem Schleier von Machtpolitik werden Narrative in grössere Kontexte und Ordnungen gesponnen. Diese Praxis ist

4 *Spin* (Englisch: *to spin* = drehen, schleudern, vernetzen, jemanden zu etwas befähigen, aber auch Informationen partikular erscheinen zu lassen). Im Folgenden wird *Spin Politics* als subtiles Instrument der Täuschung jenseits von Sprache und Bildern definiert.

5 Kurzdefinition Semantik: «‹Semantics› is ordinarily understood as a discipline concerned with the meanings of symbols (...). When we know the meaning of a statement, we also know the circumstances under which the statement is true (...)» (Hoyningen-Huene 2004: 191).

6 Kurzdefinition Semiotik: «Semiotics involves the study not only of what we refer to as ‹signs› in everyday speech, but of anything which ‹stands for› something else. In a semiotic sense, signs take the form of words, images, sounds, gestures and objects» (Chandler 2005: 2).

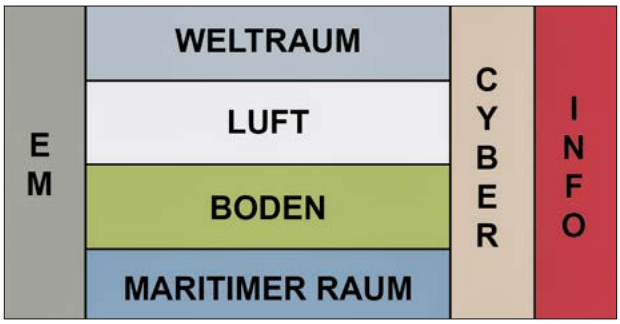


Abbildung 1 Operationssphären (Prinzipdarstellung Autor).

für jeden geostrategischen Akteur von entscheidender Bedeutung, wie die nachfolgenden Ausführungen noch zeigen werden. In diesen Verstrickungen stellt der machtpolitische Wahrheitswert letztlich nur die Spitze des Eisbergs dar. Darum versucht Spin Politics, Handlungen und Ereignisse über die sinnstiftende Ordnungslogik von Sprache, Symbole und Bildern zu stellen.

Box 3: Unternehmenskommunikation
In der Unternehmenswelt wird das Zurechtrücken von Informationen und das Inszenieren eines Unternehmens schon lange als strategisches Mittel eingesetzt (e.g. Corporate Communication, Corporate Identity, Branding, Public Relations, etc.). Auf staatlicher oder politischer Ebene spricht man in diesem Zusammenhang von Propaganda oder STRATCOM. Spin Politics ist anders zu lesen und kann weder ausschliesslich mit Corporate Communication, Propaganda noch mit STRATCOM gleichgesetzt werden. Die Deutungshoheit von Inszenierungen wird mit Spin Politics zu einem machtpolitischen Spielball, deren ungewissen Ausgang Akteure als strategisches Element bewusst in Kauf nehmen.

Der vorliegende Artikel baut (A) auf vier kurzen machtpolitischen Thesen auf, die auf die Mehrdeutigkeit in der geopolitischen Interpretationsarbeit hinweisen und mit der Kausallogik von Ursache-Wirkung brechen. Aufbauend auf diesen Thesen lässt sich festhalten, dass geopolitische Strategien nicht rationalen Mustern folgen. Sie fordern Aufmerksamkeit für Tatsachen und Beziehungen, die nicht kategorisierbar sind. Die Folgen der US-Aussenpolitik sind ein Beispiel für dieses Muster. Die Vereinigten Staaten von Amerika folgten nach dem Ende des Kalten Krieges im Nahen Osten und am Hindukusch einer Interventionslogik, die mittel- bis langfristig nicht Demokratie und wirtschaftliche Stabilität brachte, sondern schlafende Akteure weckte und ungewollte Handlungen und Ereignisse provozierte. Die daraus resultierenden Ereignisse, dieses Interesse geleiteten aber wohlwollenden Souveräns (Zbigniew Brzezinski), hatte man vermutlich so nicht voraussehen können. Das Erstarken des sunnitischen Dschihadismus, der später die Grundlagen für den Islamischen Staat lieferte oder das Bündnisvakuum im Nahen Osten, welches Russland als neuer wirkungsmächtiger Bündnispartner Saudi-Arabiens geschickt auszufüllen wusste, sind solche Beispiele. Aufbauend auf diesen Beziehungsfaktoren, die das vermeintlich Nebensächliche in den Mittelpunkt rü-

cken, wird in einem zweiten Abschnitt (B) mit drei Definitionen zu Spin Politics geantwortet. Mit einer multipolaren Weltordnung wird das Nebensächliche eine interessante machtpolitische Handlungsoption. Kleine geopolitische Akteure wie Nordkorea wissen dies geschickt auszuspielen. In einem dritten Abschnitt (C) werden konzeptionelle Interpretationselemente abgeleitet, um militärstrategische und nachrichtendienstliche Konsequenzen zu formulieren. Erkenntnisse, die Hinweise für eine Militärdoktrin liefern, die nicht mehr auf einem statischen Machtmodell, sondern auf dynamisch-verschobenen Bedingungen basiert. Die Abschnitte (A) bis (C) werden mit Beispielen und Kommentaren zu Chinas aktuellen geopolitischen Machtambitionen ergänzt. Die reale Tragweite dieser Politik ist noch nicht abzuschätzen. Darum ist das Reich der Mitte ein interessantes geopolitisches Fallbeispiel. Der aktuelle Spin Pekings lässt die Lesart zu, dass ihre regionalen Sicherheitsinteressen und ihre globale Strategie engmaschig miteinander verbunden sind. Oft von der Weltöffentlichkeit unbemerkt, eröffnet dies China neue Betätigungsfelder und Handlungsmöglichkeiten. Diplomatische und militärische Entscheidungsträger dürfen sich diesen spinpolitischen Bedingungen nicht verschliessen. Anhand der Handlungsfelder *Geopolitik*, *Diplomatie*, *Ökonomie* und *Technologie* wird in diesem Artikel Chinas Spin getestet. Diese Beispiele sind lediglich Blitzlichter und haben keinen Anspruch auf Vollständigkeit. Sie verweisen auf die enge Verzahnung und die verschwommenen Zusammenhänge, die Spin Effekte produzieren können. Abschnitt (D) bietet ein Fazit, wie Spin Politics heute Einfluss auf die Sicherheitsarchitektur und deren Doktrin hat. Was für Konsequenzen lassen sich für die nachrichtendienstliche Arbeit und auch für die militärstrategische Ausrichtung der Schweizer Armee formulieren?

Vier Thesen zu Spin Politics (A)

Die nachfolgenden Thesen (vgl. Box 4) versuchen Spin Politics als wirkungsmächtige Komplizin von Machtpolitik auszulegen (These 1). Sie verweisen darauf, dass der Kampf um Deutungshoheit das Verschleiern, Interpretieren und Übersetzen verdeckter Absichten ist (These 2). Zugleich ist dieser Kampf einer gewissen Eigendynamik unterworfen, da gewisse Ereignisse und Handlungen weder übersetzbar noch lenkbar sind. Sie entwickeln sich aus Kontexten. Es sind Ereignisse und Handlungen, die aus den Kontexten Fakten schaffen, welche die planenden und ausführenden Akteure möglicherweise so nicht vorausgesehen haben (These 3) – diese Eigendynamik kann zu unkontrollierten Formen der Eskalation führen[7] oder aber Zielbeziehungen bewusst vertuschen (These 4).

Box 4: Vier Thesen zu Spin Politics

These 1: Machtpolitik ist heute *Kampf* um Deutungshoheit.

These 2: Deutungshoheit ist das *Übersetzen* von Handlungen, Ereignissen und Trends mittels der Grammatik von Hidden Agenden.

These 3: Hidden Agenden haben *Eigendynamik* – sie sind Spin-Tools, um Kontexte und Operationssphären zu verwischen.

These 4: Das Verwischen ermöglicht geopolitische *Zielbeziehungen* bewusst zu maskieren.

Sind in einem Cyberraum die Akteure und ihre Absichten noch klar zu identifizieren respektive sind wirtschaftskriminelle Akteure nicht auch Teil staatspolitischer Gefährdung?

Für die militärstrategische Antizipation und das Übersetzen dieser Spin-Tools sind Denken in vernetzten Operationssphären, die Erweiterung von Kontexten sowie die Verflechtung von Handlungen unabdingbar; d. h. Akteure und ihre Ziele, Mittel und Verfahren werden immer schwammiger. Sind in einem Cyberraum die Akteure und ihre Absichten noch klar zu identifizieren, respektive sind wirtschaftskriminelle Akteure nicht auch Teil staatspolitischer Gefährdung? Die Attacke der Schadenssoftware *WannaCry* hat nicht nur eine Cyber-Attacke gegen den *National Health Service* (NHS) von Grossbritannien angetreten, sondern damit auch in Spitälern biochemische Folgekatastrophen in Kauf genommen. In einer Grauzone haben Akteure wie Hacker in ungeahnten Räumen sicherheitspolitische Hebelwirkung.[8] Gerade auch China weiss diese Grauzonen geschickt auszuspielen. Durch vielfach geschichtete Zusammenhänge wissen sie ihre Ambitionen erfolgreich zu vernebeln und setzen gleichzeitig mit einer *Strategie der geopolitischen Bestätigung* klare machtpolitische Zeichen (vgl. *These 3 und 4*): Wer Chinas Vormachtstellung nicht bestätigt, wird eingeschüchtert. Gemäss dem ehemaligen deutschen Aussenminister Sigmar Gabriel[9] versucht Peking mit Zuckerbrot und Peitsche die Einheit der Europäischen Union zu provozieren. Mit Ungarn und Griechenland als europäische Partner der *Belt-and-Road-Initiative* (BRI)[10] versucht China EU-Mitglieder explizit für ihre Strategie zu gewinnen. Gleichzeitig betont China, dass es kein Alternativsystem zu Europa aufbauen wolle.

7 Vgl. Victor Hugos *canon lâché* in *Quatre-Vingt-Treize*: «(…) un canon lâché. Vous ne pouvez pas le tuer, il est mort ; en en même temps, il vit. Il vit d'une vie sinistre qui lui vient de l'infini. Il a sous lui son plancher qui le balance. Il est remué par le navire, qui est remué par la mer, qui est remuée par le vent. Cet exterminateur est un jouet. Le navire, les flots, les souffles, tout cela le tient ; de là sa vie affreuse» (Victor Hugo 2001: 1ère partie., L.2, ch. IV).

8 Die vom Bundesrat verabschiedete *Nationale Strategie zum Schutz vor Cyber-Risiken (NCS) 2018–2022* stellt richtigerweise fest, dass Cyber-Angriffe oft gleichzeitig unterschiedlich motiviert sein können. Damit nimmt der Bericht die Idee von Spin Politics auf: Beispielsweise bedeutet Cyber-Spionage oft auch Cyber-Kriminalität und Cyber-Sabotage wiederum hat oft mit Desinformation zu tun (NCS 2018: 3–4).

9 Vgl. Miller, Nick (2018): *China undermining us «with sticks and carrots»: Outgoing German minister.* In: The Sydney Morning Herald.

10 Die BRI ist ein Infrastrukturprojekt der chinesischen Regierung, welches 2013 startete. Auf dem Landweg erschliesst es Asien und Europa und auf dem Seeweg werden Ost- und Südasien sowie Afrika und Europa erschlossen. Das Projekt wird oft als *Neue Seidenstrasse* bezeichnet. In diesem Artikel wird noch detaillierter auf die BRI eingegangen.

Diese Doppelstrategie kann zu einer Eigendynamik führen, die relevante Kontexte und Handlungsmöglichkeiten verwischen lassen: Für Aussenstehende ist es schwierig zwischen Chinas Kooperationsbemühungen und ihren Machtambitionen zu unterscheiden (vgl. *These* 3). Um diesen Graubereich auszuloten setzt Peking auf Spin, um die eigene Position zu verwischen (vgl. Hidden Agenda).

Auf den vier Thesen und dem Beispiel des Doppelspiels der Chinesen aufbauend können politische, ökonomische, ökologische, kulturelle und militärische Ereignisse zu aktiver Irreführung eingesetzt werden: Geschichtssymbolik, Bilder und Operationen unter falschen Flaggen[11] vermitteln Informationen, die (A) produziert, (B) vertrieben und (C) rezipiert werden (vgl. Abb. 2). Die Verkettung von (A) bis (C) lässt den Fluss des Spin-Effekts erahnen: Informationen sind ein zusammenhängendes Ganzes mit unterschiedlichen Akteuren, die wiederum unterschiedliche Positionen und Absichten haben. Da die Deutung von Kontexten immer partiell-analytisch ist, birgt sie das Potential von *offenen* Lesarten, die wiederum nicht kontrolliert werden können.[12] Diese Eigendynamik führt dazu, dass Schlüsselbegriffe wie Akteure, Raum und Zeit nicht objektiv, sondern kontextuell und relativ auszulegen sind. Das Spektrum muss erweitert werden, da die offensichtlichen Zielbeziehungen sich verschieben. Folglich kann die transportierte Information unterschiedliche Auswirkungen haben und die vermeintlich identifizierten Akteure und Objekte können lediglich als ihr sichtbarster Effekt ausgelegt werden (vgl. *Spin* = Hybridisierung von Informationen, Handlungen und Symbolen). Aus dieser Perspektive sind für eine effektive Kontextanalyse Akteure, Handlungen und Ereignisse (vgl. *politics*) unter unterschiedlichen Zusammenhängen, Bildern und Aktionen zu lesen (vgl. *spin*). Diese Polyvalenz des Kontextes wird von Akteuren bewusst als Grundrauschen unterhalten, um Opportunitäten zu nutzen und so die Deutungshoheit für sich zu beanspruchen. Durch das Verfolgen und Orten von Opportunitäten sind die Rückkoppelungen auf Informationen, Handlungen und Symbole die logischen Konsequenzen von Spin Politics. In diesem Sinne ist Spin Politics opportunistische Machtpolitik mit geostrategischen Zwischentönen.

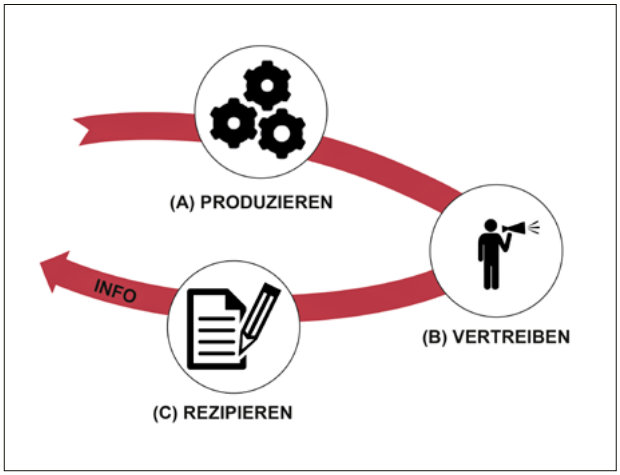


Abbildung 2 Die Entstehung eines Spin Effekts (Prinzipdarstellung Autor).

Kulturell wird Europa von China mit Kunst, Sprache und Geschichte verführt, während auf der anderen Seite mit machtpolitischen Muskeln gespielt wird.

China scheint diese Form von Spin Politics äusserst erfolgreich zu praktizieren. Die Kulturdiplomatie Pekings ist ein Meisterstück dieser opportunistischen Politik samt Rückkoppelungseffekt. Die global rapid zunehmende Ausweitung der Konfuzius Kulturinstitutionen, die Panda-Diplomatie[13] sowie die Internationalisierung des staatlichen Senders *China Central Television* (CCTV) sind zwar klassische Instrumente von *Softpolitics*, lassen sich aber vortrefflich für opportunistische Machtpolitik einsetzen. Sie helfen das Bewusstsein für das kulturelle Erbe Chinas in westlichen Ländern zu stärken und fördern damit einerseits den diplomatischen und zivilgesellschaftlichen Dialog und andererseits bieten sie Rückkoppelungseffekte, die von kultureller Überlegenheit und Standhaftigkeit zeugen. Die Botschaft ist klar: *China bringt nicht Abhängigkeit und Unterdrückung, sondern Kultur – eine über 5 000 Jahre alte zusammenhängende Kultur.* Damit versucht Peking, wie etliche andere Nationen, mit Sprache und Kultur sich zivilisatorisch zu positionieren. Nur sind diese kulturellen und diplomatischen Beziehungen in einen Spin von Beziehungen und Abhängigkeiten verflochten, wo Akteure und Handlungen sich ineinander verkeilen. Dies zeigt China exemplarisch in Bezug auf Europa. Kulturell wird Europa von China mit Kunst, Sprache und Geschichte verführt, während auf der anderen Seite mit machtpolitischen Muskeln gespielt wird. Mit der zunehmenden Fragmentierung Europas kann Peking einen europäischen Loyalitäts- und Stresstest auslösen, der die Sicherheitsarchitektur Europas destabilisiert. Gerade auch auf Grundlage der unklaren Brexit-Verhandlungen können neue Partner und Handlungsräume geschaffen und auch Zielbeziehungen verschoben werden: Wird Grossbritannien neuer Finanzintermediär und strategischer Partner der Chinesen im Westen? Was bedeutet dies für die EU und was für eine Bedeutung hat es, wenn Städte wie Duisburg, Hamburg, Madrid und auch Rotterdam direkt mit der chinesischen Regierung verhandeln? Ob dieser strategische Stresstest letztlich für China aufgehen wird, ist fraglich. Realpolitisch werden sich im günstigsten Fall vermehrt EU-Länder diplomatisch und wirtschaftlich Peking zuwenden und im schlechtesten Fall verliert China einen wichtigen Kooperations- und Regulierungspartner. Die Verbindung zu Europa war geostrategisch insofern wichtig, als China in den letzten Jahren damit ein Gegengewicht und einen wichtigen Rückkoppelungseffekt zu Barack Obamas aussenpoli-

11 Definition *Falsche oder Fremde Flagge*: «Gewinnen einer Person für eine nachrichtendienstliche Tätigkeit durch Täuschung über den wahren Auftraggeber und/oder die tatsächliche Art der Tätigkeit» (Landesamt für Verfassungsschutz Baden-Württemberg: *Glossar* (online: http://la.boa-bw.de/archive/frei/173/0/www.verfassungsschutz-bw.de/spio/spio_glossar_spioabwehr.htm#f)).

12 Vgl. Semiose: «Prozess in dem etwas als Zeichen dient» (Morris 1988: 20).

13 Die Panda-Diplomatie bezeichnet Chinas Strategie andere Staaten durch das Verschenken oder Leihen von Pandabären positiv zu beeinflussen.

tischen Strategie *Pivot to Asia*[14] aufbauen konnte. Weil dieses Vakuum zwischen Peking, Brüssel und Washington bestand, setzte China auf Spin Effekte, die Potential für Eigendynamik hatten und nach wie vor haben (vgl. These 3).

Keine noch so mächtige Nation noch ihre Organisationen und Agenturen sind in der Lage, Strukturen zu schaffen, die im Voraus lenken und bestimmen können.

Aus diesen Thesenbildungen ist herauszulesen, dass das Generische an der Information ihre *Nicht-Spezifizität ist*: Hidden Agenden leben von unspezifischen Referenzen, Bildflecken, die plötzlich sehr spezifische Handlungen erfordern.[15] Mit den vier Thesen wird hervorgehoben, dass die Welt vielmehr vom Chaos und dem Moment heraus funktioniert. Keine noch so mächtige Nation noch ihre Organisationen und Agenturen sind in der Lage, Strukturen zu schaffen, die im Voraus lenken und bestimmen können; die kurzfristige Lenkung eines Akteures kann mittel- bis langfristig unintendierte Folgen haben. Ob die BRI den gewünschten Effekt für China liefert, bleibt abzuwarten. Durch die rasante Verbreitung der Informationstechnologie und die Möglichkeiten Informationen in vernetzte Räume zu tragen, wird die zeitliche und strukturelle Analyse immer vielschichtiger. Diese ungleichen Tempi erlauben es China, ihre unterschiedlichen Zielbeziehungen gleichzeitig und auf verschiedenen Ebenen laufen zu lassen. So ist zu fragen: Lassen sich das Raumfahrtprogramm der Chinesen und ihre Fähigkeit Satelliten zu kontrollieren mit den Ambitionen der BRI verknüpfen? Wie würden sich die strategischen Zielbeziehungen verschieben, wenn langfristig China die BRI nicht finanzieren kann? Wo könnte ein neuer Spin gedreht werden und was würde dies für eine multipolare Weltordnung bedeuten? Dieser Vielschichtigkeit Rechnung tragend, lassen sich drei Definitionen zu Spin Politics herauskristallisieren.

Definitionen zu Spin Politics (B)

Definition 1: Handlungen und Ereignisse sind *per se* schon Information. Diese Erkenntnis erweitert den Begriff der Information auf jegliche Form von Handlungen, Zeichen und Symbole. Sie können gezielt zu einer polyvalenten Informationspolitik beitragen und definierte Operationssphären und Ordnungsraster verwischen. Aus diesem Grund kann der Informationsraum nicht als eine eigenständige Sphäre definiert werden. Vielmehr sind Handlungen und Ereignisse persuasiv, wirkungsmächtig aber auch instabil. Sie müssen als eingebetteter Bestandteil jeder Operationssphäre verstanden werden. Mit dieser Erkenntnis ist der analytische Unterschied zwischen den Sphären nicht

Box 5: Eine Lektion in Spin Politics – der Fall Muhammad bin Salman

Die gewollten und ungewollten machtpolitischen Aktionen des saudischen Thronnachfolgers Muhammad bin Salman zeigen exemplarisch wie die Effekte von Spin an einem Tag zusammenkommen und -hängen können.

Szene 1: der sunnitisch-libanesische Premierminister Saad al-Hariri kündigt seinen Rücktritt am 04. November 2017 in Riad an. Er befürchtet von der schiitischen Hisbollah ermordet zu werden. Vermutlich wurde al-Hariri aber vom saudi-arabischen Königshaus dazu gezwungen. So könnte Saudi-Arabien den Stellvertreterkrieg in Syrien in den Libanon verlagern. ***Spin 1:*** Nach dem Sieg in Syrien kehren die Hisbollah-Kämpfer in den Libanon zurück. Mit deren Machtübernahme könnte die Hisbollah die Konfrontation mit Israel suchen. In diesem Szenario würde Israel für bin Salman den Stellvertreterkrieg gegen die Hisbollah im Libanon führen.

Szene 2: Fast gleichzeitig mit al-Hariris Rücktritt am 04. November 2017 wurde eine Rakete aus Jemen auf Riad gefeuert. ***Spin 2:*** Diese Aktion war vermutlich zufällig aber Teil bin Salmans Provokationen/Spin 2015 einen indirekten Krieg im Jemen anzuzetteln. Ausgelegt wird die Aktion durch das saudi-arabische Aussenministerium mit den Worten «Es war eine irakische Rakete, abgefeuert von der Hisbollah».

Szene 3: Am selben Samstagabend festigt bin Salman seine Macht, indem er im Namen der Korruptionsbekämpfung etliche Prinzen und Funktionäre verhaften liess, die ihm möglicherweise in die Quere kommen könnten. ***Spin 3:*** Die gesellschaftliche Liberalisierung Saudi-Arabiens geht einher mit der politischen Erstarkung des Königshauses. Dies lässt eher auf eine neue Form der Autokratie schliessen.

Diese drei Szenen, abgeleitet von Markus Spörndlis Beitrag *Unbekümmert in die nächste Katastrophe*, zeigen, dass Handlungen Spin Effekten ausgesetzt sind und unterschiedlichste Folgen evozieren/provozieren. Die Einschätzung des amerikanischen Präsidenten Donald Trump verweisen auf diese *Nicht-Positionierung*: «Ich habe grosses Vertrauen in König Salman und den Kronprinzen von Saudi-Arabien. (...) sie wissen genau, was sie tun (...)». Spörndli, Markus (2017): *Unbekümmert in die nächste Katastrophe*. In: Wochenzeitung.

14 Die *Pivot to Asia*-Strategie war die Verlagerung der aussenpolitischen Ausrichtung der Obama-Administration von Europa und dem Nahen Osten hin zu Ostasien.

15 Es geht dabei auch um die Frage: *Wie geht man mit Verschwörungstheorien um?* Im Unterschied zu Spin Politics geht man bei Verschwörungstheorien davon aus, dass nichts zufällig geschieht, sondern Akteure im Geheimen einen Plan verfolgen, der zu bestimmten Ereignissen führt (vgl. Butter 2018).

mehr möglich – unter diesen Umständen wird der Politik-Macht-Raum-Nexus sowie die Unterscheidung zwischen *Hard-* und *Softpolitics* obsolet (vgl. Chinas diplomatische Doppelstrategie, die zwischen Kulturdiplomatie und Machtpolitik oszilliert).

Definition 2: Die Verwischung von klaren Ordnungen betont die Eigendynamik. Diese Erkenntnis ist für eine erfolgreiche Kontextanalyse von Spin Politics zentral: Politische, gesellschaftliche, wissenschaftliche/technologische, umweltbezogene und wirtschaftliche Ereignisse sind keine isolierten Phänomene. Sie sind hochgradig performativ und vernetzt. Strategische Deutungsarbeit ist demzufolge anhaltend ein iterativer Prozess zwischen Akteuren (Sender) und Analysten (Empfänger). In dieser Hinsicht erfordert die Verflechtung von Akteuren, Handlungen und Ereignissen eine permanente *veille stratégique.*[16] Mehr noch: Die *veille stratégique* sollte als *processus de signification* verstanden werden, der die multiplen Ereignislinien des Spin-Effektes nicht nur nach-, sondern vor allem vorzeichnen (vgl. Antizipation). Das Verständnis für Spin Politics, ihre Mittel und Effekte ist nur dann möglich, wenn man Handlungen und Ereignisse als einerseits fragiles Unterfangen und andererseits als eigendynamisches *Perpetuum Mobile* versteht (vgl. *canon laché*).

Box 6: 3 Definitionen zu Spin Politics
Definition 1: Spin Politics legt Handlungen und Ereignisse als *Information* aus.

Definition 2: Mit Spin Politics wird Kontextanalyse zu einem *Perpetuum Mobile.*

Definition 3: Spin Politics ist der gezielte Einsatz von Handlungen um *(Des)Information* zu betreiben.

Die *veille stratégique* sollte als *processus de signification* verstanden werden, der die multiplen Ereignislinien des Spin-Effektes nicht nur nach –, sondern vor allem vorzeichnen (Antizipation).

Definition 3: Der globale Kommunikationsraum und die zunehmende Geschwindigkeit, in der Handlungen, Ereignisse aber auch Symbole verbreitet und rezipiert werden, sind schwierig zu orten und nicht schlüssig nachvollziehbar. Aus diesem Grund versucht Spin Politics unterschiedliche Medien, Formate und Mittel zu erproben, um Informationen als persuasives Kampfmittel einzusetzen. Da Informationen hybrid, verflochten und nicht kontrollierbar sind, ist Spin Politics ein starkes Mittel, um gezielt (Des) Informationen zu erwirken und kontrolliert oder unkontrolliert Eskalationen auszulösen. In diesem Sinne spielt das Handlungsmuster von Spin Politics mit der permanenten Möglichkeit der aktiven Schattierung von vorder- und hintergründigen Handlungen, Ereignissen und Symbolen.

Innerhalb der bipolaren Welt folgte das Spiel der Eskalation einer klaren Machtlogik (vgl. atomare Rüstungssymbolik, *tit-for-tat*). Mit multipolaren Voraussetzungen und undurchsichtigen Akteuren hat die rationale Interpretationshoheit ihre Schuldigkeit getan. Anhand der drei Definitionen lässt sich gut ablesen, dass mit Spin Politics bewusst in Kauf genommen wird, dass das Eskalationspotential steigen und die geopolitische Irrationalität zunehmen wird. Die Rationalität einer gezielten Desinformationkampagne ist aber eigentlich gar nicht gezielt; vielmehr ist diese *irrationale* Rationalität für viele Akteure – wie aktuell für Nordkorea – noch die einzige Option sich in einem schneller werdenden politischen und gesellschaftlichen Karussell zu behaupten. Technologische Mittel, soziale Medien aber auch das Erstarken von transnationalen Unternehmen haben die Bedeutung von sicherheitsrelevanten Faktoren wie *Landesgrenze*, *Identität* und *Rechtsprechung* verschoben. Das Verschieben von Bedeutungen und Referenzen öffnet den Blick auf Akteure, deren sicherheitspolitische Relevanz man sich zum Zeitpunkt des Geschehens oft nicht bewusst war. Gerade Forschung und technologische Entwicklungen können mittel- bis langfristig neue Vernetzungen und Realitäten schaffen und sind ein gutes Beispiel für unintendierte Folgen und neue Akteure. Während des Kalten Krieges verfolgte man nicht nur ein militärisches Wettrüsten, sondern auch den Wettbewerb um die besten Technologien und wissenschaftlichen Errungenschaften. Auch heute noch kann Forschung und Entwicklung zur geopolitischen Symbolpolitik beitragen und militärische Überlegenheit demonstrieren. Ein aktuelles Beispiel dafür ist das chinesische Unterwasser-Drohnen Programm. Offiziell wurde das Programm für wissenschaftliche Zwecke und für die Vermessung des maritimen Bodens entwickelt.[17] De facto sind aber Unterwasser-Drohnen effektive Kampfmittel, um neue Formen des Seekrieges zu erproben (vgl. Robotorisierung der Weltmeere, Tiefseedaten für U-Boot Operationen wie auch der Ausbau der Telekommunikationstechnologie). Schätzungsweise arbeiten bis zu fünfzehn Universitäten in China an diesem Unterwasser-Drohnenprogramm.[18] Im Gegensatz zu Luft-Drohnen sind Unterwasser-Drohnen technisch komplex, da Druckschwankungen schlecht für das Material und Radiosignale im Wasser schwierig zu übertragen sind. China testet aktuell im Südchinesischen Meer zwölf Haiyi-Drohnen für hydrographische Echtzeit-Datentransfers. Aufbauend auf diesen Erfolgen will China im westlichen Pazifischen Ozean ein Tiefsee-Kommunikationsnetzwerk aufbauen, welches direkt mit Satelliten kommunizieren kann. Vordergründig soll die neue Technologie Regionen und Menschen zusammenbringen. Damit dieses technologische Powerplay vorangetrieben und gewonnen werden kann, sind Forschung und Entwicklung zentral. Peking treibt dies mit eigenen Forschungsprogrammen und auch mittels Wissenstransfer durch Einkäufe ausländischer Firmen voran. Dies ermöglicht China neue geotechnologische Optionen und erlaubt ihnen globale Monopolbildungen. Im Gegensatz zu Zeiten

16 Armeestab A Stab 2015: 23.

17 Vgl. Chen, Stephen (2017): *Why Beijing is speeding up underwater drone tests in the South China Sea*. In: South China Morning Post.

18 Chase et al. 2015: 3.

des Kalten Krieges wird der technologische Wettbewerb heute vordergründig von privaten Technologiekonzernen und Startups vorangetrieben. Damit sind plötzlich neue Akteure im Spielfeld. Gerade im Bereich der Künstlichen Intelligenz (KI) lassen sich in China interessante Entwicklungen beobachten.[19] Technologieunternehmen, die in einem ersten Schritt wirtschaftliche Interessen verfolgen, sind in einer zweiten Lesart *Enabler* von KI-Algorithmen, die es Peking erlauben, seine Gesellschaft mittels einer elektronisch gesteuerten unsichtbaren Hand zu disziplinieren. Die Kombination von Big Data, Gesichtserkennung sowie Videoüberwachung und KI-Technologien ermöglichen es der chinesischen Regierung, jeden der 1.4 Milliarden Chinesinnen und Chinesen zu kontrollieren und sanktionieren. Indem diese *Totalisierung-durch-Elektronik* Rhetorik öffentlich vorangetrieben wird und mit *Skynet* auch einen von Hollywood inspirierten Namen hat, macht diese mögliche Omnipotenz die Bürgerinnen und Bürger gefügig, auch wenn die technologischen Möglichkeiten noch gar nicht so weit entwickelt sind.[20] In einem zweiten Spin und mit dem konsequenten Vorantreiben neuer Technologien ermöglichen es solche Programme dem Staat, ihre Bürger langfristig zu konditionieren und so das Bild einer grossen, zusammenhängenden und starken Nation nach aussen zu portraitieren. Darum versucht China so gut es geht zu verbergen, dass diese Technologieunternehmen das Bild erwecken, dass sie für staatliche Propaganda benutzt werden. Es scheint offensichtlich, dass die chinesischen Startups *Megvii Inc.* sowie das weltweit höchstbewertete AI-Startup *SenseTime* von chinesischen Staatsgelder gefördert wurden.[21] Zudem haben etablierte Unternehmen wie der Technologiekonzern *Huawei* durchaus spezielle Beziehungen zum chinesischen Militär.[22] *Huawei* wie auch der Plattformbetreiber *Baidu* sind wichtige chinesische Akteure für Infrastrukturen und Datenaustausch, auch in der Schweiz.[23] Nicht nur entwickeln sie computergestützte Kerntechnologien, sondern sie sind als Infrastrukturbetreiber von Unterwasserkabel-Netzwerken und Telekommunikationsinfrastrukturen wichtige Sicherheitsakteure. Im Südchinesischen Meer versucht Peking seit 2016 Satelliten durch leistungsfähigere 4G Unterwasser-Glasfaserkabeln zu ersetzen. Eine klare Kabel-Strategie für einen effizienten interkontinentalen Daten-Highway und eine ausgeklügelte Voice-Kommunikation sind wichtige sicherheitspolitische Stützen, gerade für die Meeresroute der BRI, welche notabene durch die Gewässer des Südchinesischen Meers führt. Die offenen Militärdrohungen im Südchinesischen Meer, aber auch die dort zu künstlichen Inseln aufgeschütteten Riffs mit Militärbasen, sind geschickte Spins, um von ihrer Kabel-Strategie abzulenken und geopolitische Zielbeziehungen zu maskieren.[24] Technologie und Wissenschaft sind wichtige Informationsträger, die Operationsräume, Akteure und Kontexte subtil miteinander verknüpfen und damit geopolitische Tatsachen schaffen. Es ist nicht zu vergessen, dass die Infrastrukturstrategie der BRI mittels global agierenden chinesischen Konzernen flankiert wird; exemplarisch als direkt und oder indirekt Beteiligte sind der Nahrungsmittelkonzern *Cofco*, der Infrastrukturbetreiber *HNA*, der Luxusgüterkonzern *Shandong Ruyi*, die Mischkonzerne *Wanda Group* sowie *Fosun International* zu erwähnen. Es sind alles Unternehmen, die der Agenda Pekings gehörig sind und die Aussenpolitik mittels Beteiligungen oder Aufkauf vornehmlich westlicher Hightech-Firmen vorantreiben. Nichtsdestotrotz ist sich Peking bewusst, dass sie für den Bau und den Betrieb der gigantischen Infrastrukturen nach wie vor von westlichen Firmen wie *Siemens, Schindler, Dupont, Nippon Electric Glass, Kone*, etc. abhängig sind.[25] Dies ist die Eigendynamik und das Spiel mit dem politischen Perpetuum Mobile. Nebensächliche Akteure, respektive kommerzielle Akteure, können plötzlich eine zentrale Rolle in der Expansionsstrategie Chinas spielen.

Box 7: Mit Komplexität arbeiten

Philippe Descola, Wissenschaftsforscher am Collège de France, meint in diesem Kontext, dass «(...) der Vorteil eines realistischeren Erfassens der lokalen Komplexität auf Kosten einer geringeren Verständlichkeit der globalen Komplexität geht, das heisst der vielfältigen Formen des Verhältnisses zu den Existierenden; denn die auf ethnografischer Ebene erreichte Transparenz wird zu einem Faktor der Undurchsichtigkeit, sobald man versucht, die Gründe für die Verschiedenheit der bestehenden Standpunkte zu erklären, für die uns die Ethnografie und die Geschichtswissenschaft Zeugnisse liefern» (Descola 2014: 71).

Technologie und Wissenschaft sind wichtige Informationsträger, die Operationsräume, Akteure und Kontexte subtil miteinander verknüpfen und damit geopolitische Tatsachen schaffen.

Wie das Beispiel China zeigt, ist die heutige Sicherheits- und Interessenpolitik massgeblich von nichtstaatlichen global agierenden Akteuren abhängig. Die klassischen machtpolitischen Stabilitätsfaktoren werden von Spins destabilisiert, die zunehmend von Akteuren ausgehen, die klassisch zu den nicht sicherheitsrelevanten Akteuren zählen (z. B. Infrastrukturunternehmen, Technologiekonzerne aber auch Finanz- und Versicherungsinstitute). Aus sicherheitspolitischer Sicht geht es nicht mehr um die ausschliessliche Täuschung des militärischen Gegners, sondern – man ist gewillt zu sagen – um die Täuschung des undefinierten Gegners. In einem Spin werden die Akteure

19 Vgl. Mozur, Paul (2018): *Inside Chinas's Dystopian Dreams : A.I., Shame and Lots of Cameras*. In: The New York Times.
20 Vgl. Harrison, Jacobs (2018): *China's «Big Brother» surveillance technology isn't nearly as all-seeing as the government wants you to think*. In: Business Insider.
21 Vgl. Harrison, Jacobs und Pat Ralph (2018): *Inside the creepy and impressive startup funded by the Chinese government that is developing AI that can recognize anyone, anywhere*. In: Business Insider sowie Jiang, Sijia und Zhu, Julie (2018): *China's Sense Time valued at $ 4.5 billion after $ 600 million funding led by Alibaba: sources*. In: Business Insider.
22 Vgl. Arthur, Charles (2012): *China's Huawei and ZTE pose national security threat, says US committee*. In: The Guardian.
23 Vgl. Blogeintrag von Steiger, Martin (2012): *Schweizer Netzinfrastruktur mit chinesischen Hintertüren?*, 16. Juli 2012.
24 Weitere Ausführungen zum Südchinesischen Meer in diesem Artikel in Abschnitt *(C) Nachrichtendienstliche Methodik*.
25 Vgl. Peter Nolans Ausführungen in *Is China Buying the World* (Nolan 2012).

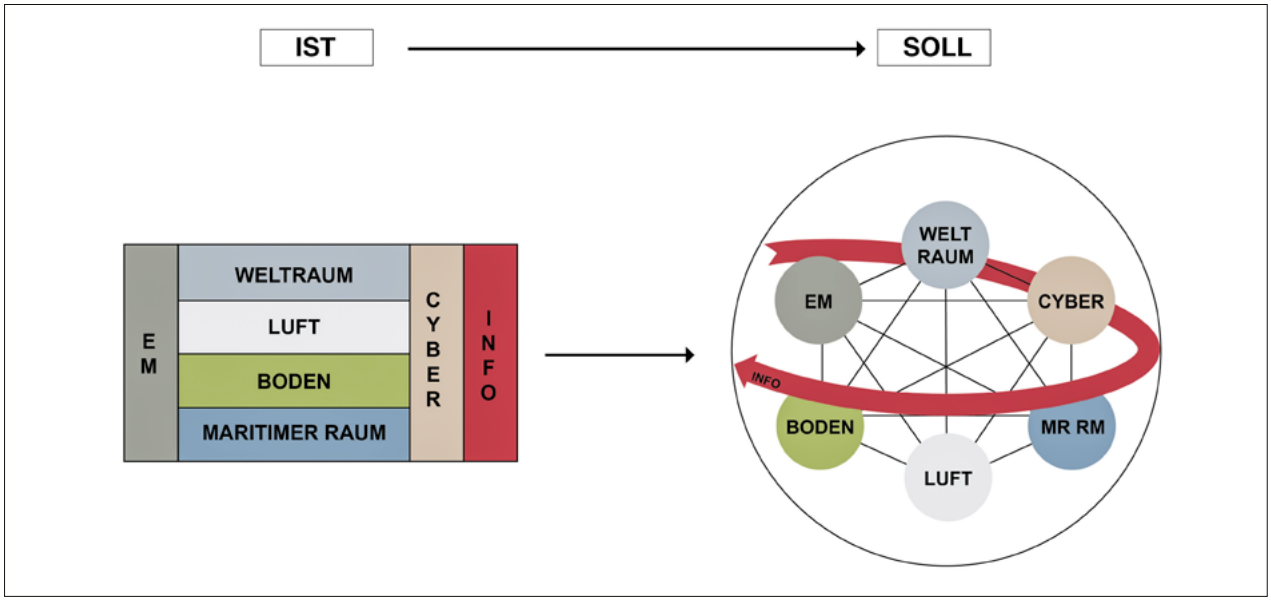


Abbildung 3 Transformation der Operationssphären: Die vernetzten Operationssphären als Spin Circle (Prinzipdarstellung Autor).

stets unterschiedlich virulent und kreieren fortlaufend neue Dispositive für Machtvakua.[26]

Nachrichtendienstliche Methodik (C)

Dass Zusammenhänge und Entwicklungslinien/Trends heute vielschichtig sind, ist keine bahnbrechende Erkenntnis. Dennoch lassen sich aus den Definitionen militärstrategisch relevante Aussagen machen. Mit Spin Politics wird ein Versuch unternommen, die Notwendigkeit eines erweiterten Begriffs von Information und die Virulenz des vernetzten Raumes systematisch herauszuarbeiten. Als integraler Bestandteil militärstrategischer und nachrichtendienstlicher Arbeit muss Spin Politics sich im Sinne einer *veille stratégique* positionieren. Folgende vier Elemente zur Methodik sollen helfen, mit dem Spiel der strategischen Mehrdeutigkeit umzugehen zu lernen und die Idee einer *single theory that explains everything* bei Seite zu legen.

Element 1: Der Spin Circle
Die relevanten militärstrategischen Operationsräume machen in einem durchrationalisierten Weltbild Sinn. Die klare Zuordnung der Räume vereinfacht Analyse, Visualisierung und Deutung, da sie der Logik von Ursache und Wirkung folgen. Spin Politics versucht dagegen, diese Kausallogik subtil zu durchbrechen: Eine Ursache muss nicht direkt zu einer Wirkung führen. Sie lädt zu unterschiedlichen Vernetzungsmöglichkeiten ein, die nicht offensichtlich sind. Damit ist Spin Politics inhärent opportunistisch. Darum sollten für Antizipation und Analyse die Operationssphären aus einem statischen Gefüge in einen Modus der fortlaufenden Vernetzung transformiert werden. Strategische Analysen unter Berücksichtigung von Spin Politics müssen einerseits holistisch sein und zugleich die Feinheiten *zwischen* den Räumen eruieren können. Darum sind die armeerelevanten Operationssphären permanent und in einem endogenen Spin zu lesen; die Operationssphären werden zu *Enabler* von Spin Politics. (Abb. 3).

Wenn man also Geopolitik unter diesen Prämissen liest, muss man aus militärstrategischer Warte die Operationssphären in einen hochgradig vernetzen Spin Circle bringen.

Element 2: Kontextanalyse – Akteur-Netzwerk-Theorie (ANT)
Die Schwierigkeit in der Modellierung von potentiellen Entwicklungslinien liegt darin, aus deren Konsequenzen unterschiedliche Muster herauszulesen (vgl. Deutung). Die asymmetrischen Realitäten der Akteure und deren Machtverhältnisse erschwert die Modellierung. Mit dem Bewusstsein der offenen Interpretation hat sich die Akteur-Netzwerk-Theorie (ANT)[27] zu einem interessanten Interpretations-Tool entwickelt. Sie liefert bemerkenswerte Perspektiven für Spin Politics. Auf der Prämisse aufbauend, dass Grenzen und Differenzen nicht klar sind und Dinge sowie nicht-menschliche Entitäten ebenfalls Ak-

26 Der Medienwissenschaftler Norbert Bolz macht im Zusammenhang zu Gesellschaftsformations-Theorien (hier in Bezug auf die Systemtheorie Niklas Luhmanns) eine interessante Beobachtung zum Problem der undefinierten Antizipation und dem daraus entstehenden Vakuum: «Dass wir Zukunft haben, aber kein Wissen von der Zukunft, ist Vorder- und Rückseite derselben Freiheit. Wir bewegen uns auf ein Ziel zu, das sich selbst bewegt. So gilt, dass man die Zukunft nicht prognostizieren, sondern nur provozieren kann» (Bolz 2017: 37).

27 Kurzerklärung zur ANT-Theorie: «Die Attraktivität des Netzwerk-Begriffs scheint insbesondere darin zu bestehen, dass er es ermöglicht, die Grenzen etablierter Unterscheidungen zu überschreiten. So wird der Netzwerk-Begriff verwendet, um auf Formen interorganisationaler Kooperation zu verweisen, die weder durch Markt noch durch Hierarchie strukturiert werden oder umgekehrt durch beides zugleich. Als Netzwerke werden Zusammenhänge beschrieben, die sich jenseits der Grenzen operational geschlossener Systeme ausbilden. Und der Netzwerk-Begriff wird reklamiert, um handlungs- und strukturorientierte Beobachtungen aufeinander zu beziehen. Der Netzwerk-Begriff eignet sich für derartige Bestrebungen, weil er selbst wenige inhaltliche Vorgaben erfordert: Von Netzwerken zu sprechen, setzt zunächst nur voraus, dass man es mit wie auch immer gearteten Einheiten zu tun hat, die in wie auch immer gearteten Beziehungen zueinander stehen» (Schulz-Schaeffer 2000: 187).

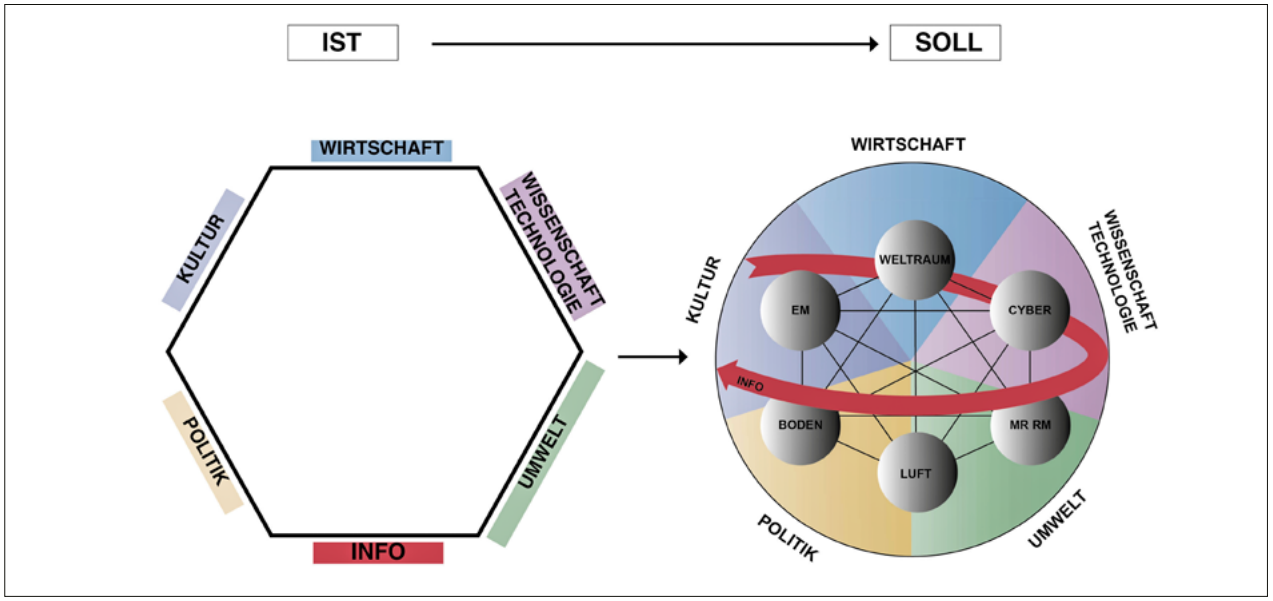


Abbildung 4 Erweiterung der Kontextanalyse (Prinzipdarstellung Autor).

teure sind, verweist ANT auf die Potentialität von Handlungen und deren Simulationen hin. In dem das *Was* nicht klar ist, kommt es stark auf das *Wie* an. Statt den Standpunkt des neutralen Betrachters einzunehmen und damit Objektivität auf die unterschiedlichen Räume und Akteure zu projizieren, dürfen Operationssphären nicht als Black Box vorausgesetzt werden (*als etwas Gegebenes, Vorgefundenes*, etc.). Analysten müssen sich auf die Sachen selbst, ihre Handlungen, Verknüpfungen und Verbindungen einlassen. Wer beispielweise ein Akteur ist, kann auch plötzlich ein Netzwerk sein. Der Spin kreiert diese *hermeneutische Zirkelbewegung:* In der Auslegung ist man selber immer schon mitgefangen und vergisst zu rasch, dass man in der Deutung selbst schon Architekt von Interpretationen ist. Dies führt dazu, dass man an gewisse Narrative glaubt und für die Politik des eigenen Standpunktes blind ist. So wird in diesem Artikel China spinpolitische Motivationen nachgesagt, obgleich der Verfasser vermutlich diesem Narrativ selber verfallen ist und/oder seinen eigenen Spin hat. Mit ANT soll hingewiesen werden, dass der Analyst immer schon Teil der Analyse ist und das Spin Politics gerne mit dieser Tatsache spielt. Demzufolge sind politische Institutionen und deren Mächte in einer permanenten Abhängigkeit von anderen Akteuren, deren Handlungen und Infrastrukturen (vgl. Kontext ist in der Analyse *King*, Abb. 4). Mit dem Zufügen eines jeden weiteren Akteurs oder Ereignisses spinnt das Rad von Spin Politics weiter. Nicht nur sind sie voneinander abhängig, sondern die Gewichtung von Akteuren und Parametern (z. B. Wohlstand, politische Stabilität, sozialer Ausgleich, kulturelle Praktiken, militärisches Rüstungspotential, urbane Infrastrukturen, meteorologische Veränderungen, etc.) sind auf einer Linie zu lesen: Dualismen wie Soft- vs. Hardpower, stark und schwach, verbündet vs. unverbündet, etc. müssen via Infrastrukturen der Weltpolitik kontextualisiert werden. Das Hexagon der militärstrategischen Stabsarbeit (Abb. 4) nimmt die Grundidee der ANT auf, sollte aber mit dem Spin-Mechanismus erweitert werden[28]: Kontexte und Entwicklungslinien erklären nicht, sondern kartographieren[29] und beschreiben (vgl. materiell-semiotisch). Diese Erweiterung ermöglicht es, nationale Sicherheitsstrategien zu formulieren, die die geopolitische Komplexität nicht auf Schwarzweiss-Bilder reduziert.

Element 3: Konfliktverlauf

Um Konfliktintensitäten und Konfliktverläufe zu verstehen, muss der geopolitische Kontext nicht mehr statisch, sondern dynamisch und vernetzt weiterentwickelt werden. Die aktuellen Ereignisse im Südchinesischen Meer sind ein gutes Beispiel für die fortlaufende Kontextanalyse (vgl. Abb. 5 und 6). Mit einer bewusst angestrebten Vormachtstellung im Südchinesischen Meer, nimmt Peking die offene militärische Konfrontation mit seinen Nachbarstaaten und der im Pazifischen Ozean stationierten Siebten Flotte der US Navy in Kauf. Damit macht China klare geopolitische Ansprüche geltend. Die historische und juristische Deutung der so genannten *Nine-Dash Line* und die dazugehörenden Inselgruppen[30] beleuchten die geopolitische Interpretationshoheit, die Peking für sich in Anspruch nimmt. Damit projektiert es, dass seine nationale Sicherheitsstrategie nicht machtpolitisch getrieben ist, sondern sich auf den Spin der Geschichte und des interna-

28 Armeestab A Stab 2015: 8.

29 Durch Mapping-Techniken lässt sich die Verbindung von Ereignissen und Aktionen nachvollziehen. Das Navigieren durch visualisierte Maps hilft Kontexte besser zu antizipieren, deckt neue Verbindungslinien auf und schützt vor fixierten Erklärungen (vgl. Die ANT-Forscherin Albena Yaneva schreibt dazu: «Exploring [conflicts] offers access to the complexity that all of the possible lines of explanation could trace and prevent us from embracing any of them individually. Mapping [conflicts] will help us to understand the uncertainties surrounding [contexts] in greater depth (…)» (Yaneva 2012: 89)). Gerade bei unvorhergesehenen Ereignissen lässt Mapping das Hintergründige vordergründig erscheinen – Verbindungslinien werden auch ohne offensichtlicher Evidenz gezogen. Yaneva: «Thus, maps are not just representational tools; map-making and mappings perform. Exploring the ways in which maps and mapping function in contemporary societies, cultural geographers followed how they produce subjects, shape bodies and constitute identities. This way of thinking about maps emphasizes the unremitting materiality of a world where there are no pre-existing objects and fixed identities» (Yaneva 2012: 89).

30 China hält die Definition der Nine-Dash Line bewusst ambivalent. Vage formuliert, beansprucht China alle terrestrischen und maritimen Gebiete innerhalb dieser Linie. Präzise Koordinaten und Grundlinien fehlen aber. Um diese juristische Ungenauigkeit zu umgehen, rechtfertigt Peking die Nine-Dash Line historisch.

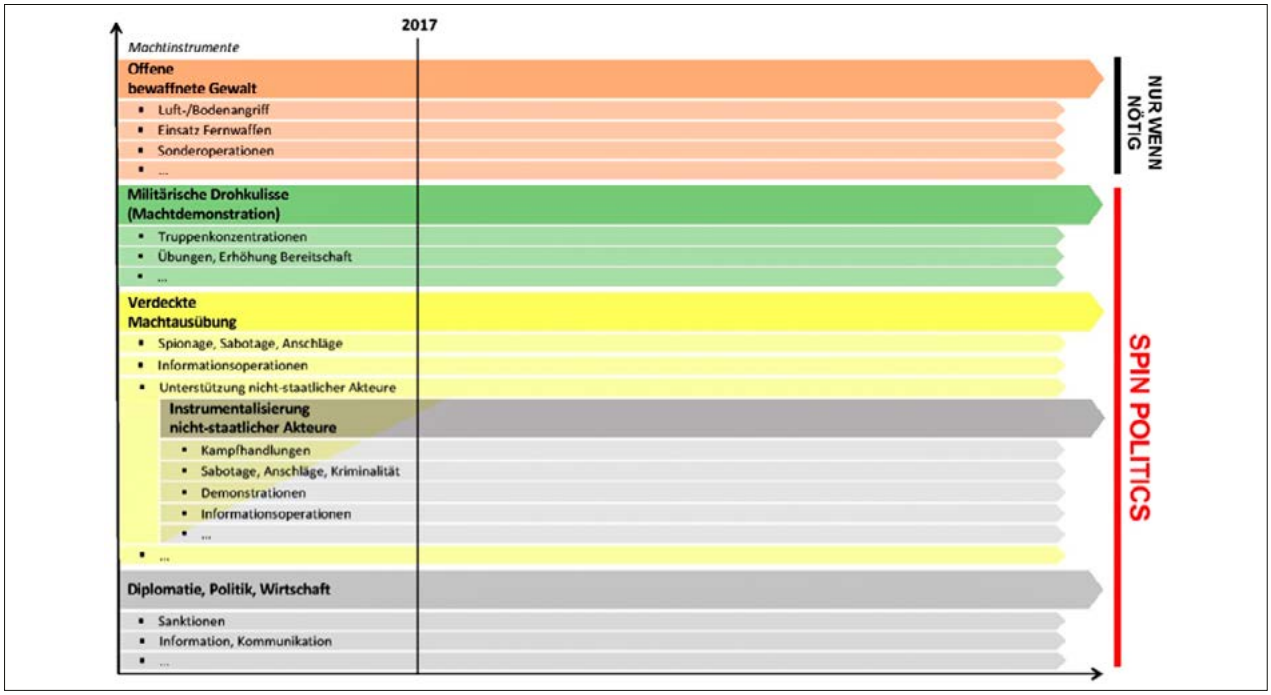


Abbildung 5 Verschachtelung des geopolitischen Kontextes: Dimensionen der Konfliktführung in einem hybriden Umfeld (Prinzipdarstellung Autor).

tionalen Seerechts stützt. Diesen Spin verstärkt Peking mit einem innenpolitischen Spin. So sind in den neuen chinesischen Pässen auf Seite acht die Nine-Dash Line sinnigerweise als Wasserzeichen abgebildet.[31] Der regionale Affront wird innenpolitisch als Fakt normalisiert. Zudem wird mit der Angleichung der Uniformen der chinesischen Marine an diejenige der US Navy eine weitere Normalisierung vorgenommen: *Die chinesische Marine operiert auf Augenhöhe mit Supermächten und kann darum die im Pass verbrieften Nine-Dash Line legitimiert verteidigen.* Dieses Beispiel zeigt, dass China seine geopolitischen Ziele durch historische, juristische und militärische Symbolpolitik geschickt vernebelt und damit einen Spin kreiert, der in der Deutung bewusst ein geopolitisches Vakuum zulässt. Damit können Hebelwirkungen erfolgen, deren Konsequenzen analytisch schwer abzuschätzen sind.

Die historische und juristische Deutung der so genannten *Nine-Dash Line* und die dazugehörenden Inselgruppen beleuchten die geopolitische Interpretationshoheit, die Peking für sich in Anspruch nimmt.

Zielgerichteter sind Chinas militärdiplomatischen Bemühungen. Chinas Teilnahme an multilateralen Übungen hat im Jahr 2016 massiv zugenommen.[32] Im Gegensatz zu bilateralen Kooperationen ermöglichen multilaterale Engagements effektive Opportunitäten auszumachen. Dank Kooperationen und internationaler Partizipation kann China so seine geostrategischen Ambitionen vordergründig entdramatisieren und hintergründig neue Realitäten schaffen. Wesentlich zu dieser Neutralisierung hat Pekings Spitzendiplomatin Fu Ying beigetragen; sie trägt den Titel des *Vice Minister of Foreign Affairs*. In ihrer unorthodoxen Art betont sie, dass China kein Wettbewerb der Systeme provoziert, sondern zum globalen Frieden beitragen will. Fu Ying benutzt nicht nur zugängliche und konziliante Formulierungen, sondern sie sucht aktiv den Dialog mit westlichen Medien und Institutionen. Damit unterscheidet sie sich von ihren Kollegen, die vornehmlich über chinesische Kanäle kommunizieren und trocken die Parteidoktrin wiedergeben. Fu Ying spricht lieber vom Grossen Land und nicht von der Supermacht China. Zudem verweist sie darauf, dass das Grosse Land im Inland noch etliche Herausforderungen im Bereich Wirtschaft, Umweltschutz, soziale Spannungen und Korruption zu meistern habe. Damit lenkt sie den Spin von Aussen- auf Innenpolitik und kehrt damit die geopolitische Deutungshoheit um. Dieser Spin wird Fu Ying abgenommen, da sie selber durch ihre feminine Erscheinung aber auch durch ihre Biographie dem prototypischen chinesischen Parteidiplomaten widerspricht: Fu Ying ist eine Frau, spricht fliessend Englisch, gehört der mongolischen Minorität an und ihre Jugend, während der Zeit Maos, war durch Entbehrung und poli-

31 Vgl. Fisher, Max (2012): *Here's the Chinese passport map that's infuriating much of Asia.* In: The Washington Post.

32 Zwischen 2003 und 2014 waren es total 130 und im 2016 alleine 124 Übungen. Vgl. Wuthnow 2017: 18.

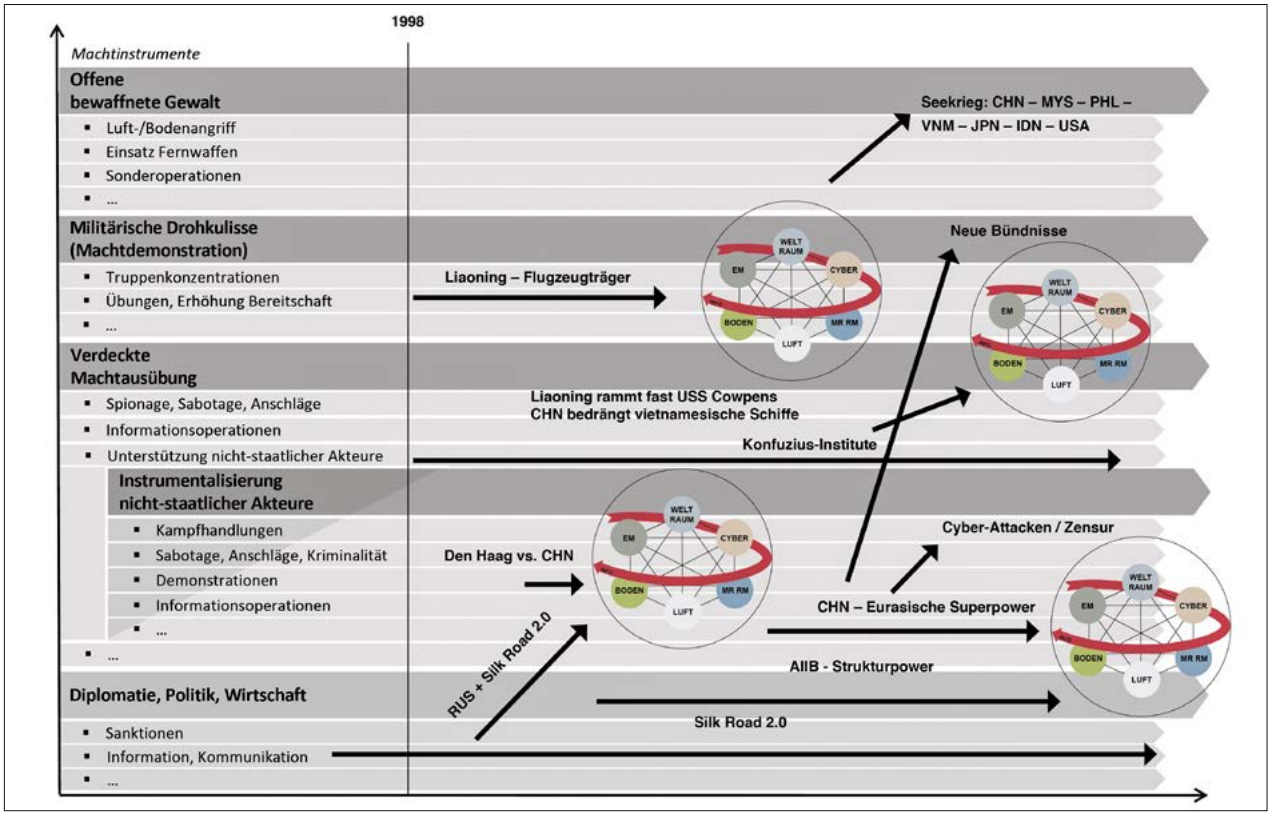


Abbildung 6 Verschachtelung des geopolitischen Kontextes – Beispiel Spin Politics im Südchinesischen Meer (Prinzipdarstellung Autor).

tische Demütigung geprägt gewesen. Mit dieser biographischen Symbolkraft und ihrem diplomatischen Geschick hat Fu Ying alle spinpolitischen Mittel in der Hand, um Chinas Deutungshoheit und ihre Agenda in eine entsprechende Deutung subtil aber stetig zu lenken. Chinas diplomatischer Spin wiederspiegelt die Eigendynamik von Hidden Agenden, da ihre Bemühungen in der Verbindung mit anderen Zielbeziehungen auch hier plötzlich ungeahnte Hebelwirkungen auslösen können. Dies kann vor allem dann der Fall sein, wenn Softpolitics nicht mehr mit offenen militärischen Machtambitionen im Einklang stehen.

In der Tat sind die in Abbildung 5 und 6 aufgeführten Kategorien *Diplomatie, Politik, Wirtschaft, Verdeckte Machtausübung, Militärische Drohkulisse* sowie *Offene bewaffnete Gewalt* nicht klar zu unterscheiden. Die Zusammenfassung dieser spezifischen Themen auf breiter abgestützte Schlüsselbegriffe wie *Geopolitik, Diplomatie, Technologie* und *Ökonomie* können die geostrategische Virulenz noch besser einfangen (vgl. Abb. 7).

Das heisst im Konkreten, dass der Spin, der zu einer militärischen Drohkulisse geführt hat, vermutlich in einem anderen Kontext viel virulenter Einfluss nehmen wird. Darum ist Deutung kontextgebunden, iterativ und permanent relativ.[33]

Die schon mehrmals erwähnte BRI ist aktuell das vermutlich prominenteste geoökonomische Projekt Chinas. Ein fast schon unüberschaubares Unternehmen, das zukünftig durchaus Realitäten kreiert, welche die Führung Chinas heute so nicht intendiert. Gerne auch mit dem Marshallplan verglichen, ist es ein gigantisches Infrastrukturprojekt zu Land und zu Meer, welches über 65 unterschiedlichste Nationen und über 62 Prozent der Weltbevölkerung zwischen Zentralasien, dem Nahen Osten, Afrika und Europa näherbringen und wirtschaftlich vernetzen soll. Eine Strecke der Freundschaft, die unter anderem aber auch Befriedigungspolitik mit der uigurischen Minderheit im Westen Chinas erwirken und Länder einbinden sollte, die historisch Russland zugewandt waren. Mit der *Asian Infrastructure Investment Bank* (AIIB) hat China ein Vehikel geschaffen, um die internationale Gemeinschaft für ihre Zwecke einzuspannen und damit regionale Bedingungen und lokale Infrastrukturen mit chinesischen Baukonzernen global neu zu kartographieren. Etliche europäische Länder haben sich der AIIB angeschlossen, was auf Strahlkraft und strategischen Opportunitäten hindeutet. Mit der BRI werden Chinas Machtambitionen sichtbar und können als merkantil getarnter Spin gelesen werden. Diese Initiative ist durch ihre schiere Dimension ein geopolitisches Perpetuum Mobile. Da das Projekt zeitlich und räumlich nicht abzustecken ist, kann Chinas Führung sein Jahrhundertprojekt an der losen Leine halten und sich fortlaufend auf neue Bedingungen einlassen.[34] Die BRI ist Spin Politics in Reinkultur: Eine spezifische Agenda wird verfolgt und

33 Bewertungskriterien werden verwoben und die Ursache-Wirkung Logik verfehlt ihre Wirkung.

34 «The narrative of the Belt and Road Initiative (BRI) as spanning over 65 countries and gathering 62 percent of the world population, 31 percent of its GDP, and 40 percent of global land area should once and for all disappear now that China has announced the extension of the BRI to Latin America» (Brînza, Andreea (2018): *Redefining the Belt and Road Initiative. The BRI is not about physical routes in Eurasia. It is about global strategy.* In: The Diplomat).

zugleich lässt der Spin fortlaufend Handlungsvakua zu, die dann von China situativ und opportunistisch militärisch, diplomatisch, ökonomisch und/oder technologisch besetzt und ausgespielt werden können. Oder mit anderen Worten, je mehr China in die BRI-Infrastruktur investiert, umso mehr hat es auf unterschiedlichsten Ebenen national und international Interessenswertes zu schützen. Falls militärische Spannungen zwischen gewissen BRI-Partnern und China unerwartet auftreten, können die aufmüpfigen Länder via die von China zur Verfügung gestellten Infrastrukturen (vgl. Häfen, Eisenbahnlinien, Telekommunikation, etc.) oder den Verpflichtungen gegenüber der AIIB gemassregelt werden. Zudem wird sich der Renminbi durch die Bedeutung der BRI wahrscheinlich als internationale Währung durchsetzen können. Damit wird ein weiteres internationales Druckmittel kreiert.

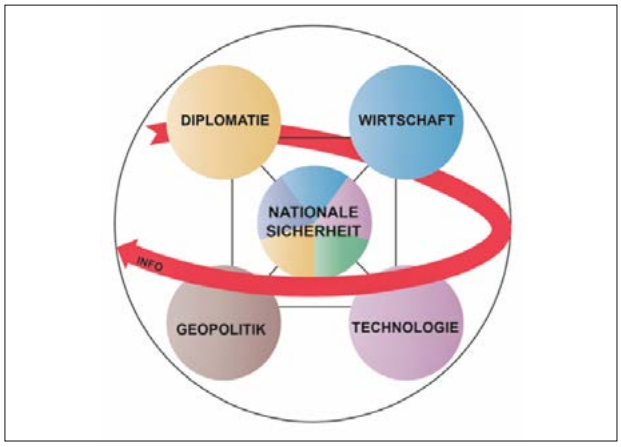


Abbildung 7 Geopolitischer Konfliktverlauf dynamisch (Prinzipdarstellung Autor).

Die BRI ist Spin Politics in Reinkultur: Eine spezifische Agenda wird verfolgt und zugleich lässt der Spin fortlaufend Handlungsvakua zu, die dann von China situativ und opportunistisch militärisch, diplomatisch, ökonomisch und/oder technologisch besetzt und ausgespielt werden können.

Element 4: Mapping Spin Politics – Wie kartographiert man Wissen?

Um diese Virulenz auslegen zu können, sind Mapping Techniken ein interessantes Analysewerkzeug. Impulse für die folgenden vier Analysewerkzeuge (vgl. Box 8) und deren Visualisierung (Mapping) kommen von Albana Yaneva's Monographie *Mapping Controversies in Architecture*. Zu ***Werkzeug A:*** Das Sammeln von ***kontextuellem Wissen*** hilft vor der Reduktionismus-Falle. Gerade Open Source-Informationen (OSINT) zielen auf die Exklusivität, Sensation und damit auf die reduktionistische Lesart von Ereignissen ab. Argumente und Positionen in Kontexten können dem entgegenwirken. Sie können diffuse und unterschwellige Verbindungslinien jenseits von geopolitischen und sozialen Erklärungen aufzeigen. Zu ***Werkzeug B: Akteure, Argumente und Positionen*** werden mit Big Data Analytics[35] gesammelt und ***geordnet.*** Akteure und Ereignisse werden nicht klassifiziert, sondern ausgelegt (vgl. mapping – parametric analysis[36]). Zu ***Werkzeug C:*** Die ***Visualisierung*** durch Mapping hilft dank neuen digitalen Möglichkeiten Kontexte nicht nur zu repräsentieren, sondern vielmehr als Navigationselement auszulegen.[37] Zu ***Werkzeug D:*** Durch ***Mapping-Techniken*** lässt sich die Verbindung von Handlungen und Ereignissen besser nachvollziehen. Das Navigieren durch visualisierte Maps hilft Kontexte zu antizipieren, deckt neue Verbindungslinien auf und schützt vor fixierten Erklärungen.[38] Gerade bei unvorhergesehenen Ereignissen lässt ***Mapping*** das Hintergründige vordergründig erscheinen – Verbindungslinien werden auch ohne offensichtliche Evidenz gezogen. Ein gutes Beispiel für das Kartographieren von diffusen Zusammenhängen ist das Unglück der Columbia Shuttle STS-107 von 2003 (vgl. Box 9).

Box 8: Vier Analyse-Werkzeuge im Dienste von Spin Politics

Werkzeug A: *Kontextuelles Wissen* über unterschiedliche Quellen sammeln.

Werkzeug B: *Akteure, Argumente und Positionen ordnen.* Inhaltliche Veränderungen zeitlich und räumlich festhalten.

Werkzeug C: Analyse und *Visualisierung* durch Mapping.

Werkzeug D: *Mapping* hilft Spin-Politics zu lesen.

35 Vgl. Die Forschungsarbeiten am *Medialab Science Po Paris* sowie ihre Daten-Tools (vgl. *Seealsology*): http://www.medialab.sciences-po.fr/projets/teaching-controversy-mapping/ und http://tools.medialab.sciences-po.fr/seealsology/

36 Vgl. Yaneva: «Responding to the challenges posed to network maps, an animation of the controversy was developed using parametric modelling. We use parametric modelling to visualize how an assembly of heterogeneous actors, their locations in time and space, and conflicting concerns work in tandem to shape the controversy. This animation showcases how the controversy unfolds as it is driven by a number of concerns: cost, legacy, community and design. It also provides a worldview of all the actors in relation to media attention, depicting when they entered and exited the debate. This simulation allows us to track the actors' involvement in the controversy in a dynamic way and to identify the nature of their involvement. One can witness the flexible grouping and regrouping of heterogeneous actors gravitating around the concerns, their attraction or shrinking as time unfolds and the different speeds of swarm formation according to the changed magnitude of the concerns in the media debate» (Yaneva 2012: 97f.).

37 Vgl. Yaneva: «Thus, maps are not just representational tools; map-making and mappings perform. Exploring the ways in which maps and mapping function in contemporary societies, cultural geographers followed how they produce subjects, shape bodies and constitute identities. This way of thinking about maps emphasizes the unremitting materiality of a world where there are no pre-existing objects and fixed identities» (Yaneva 2012: 89).

38 Vgl. Yaneva: «Exploring [conflicts] offers access to the complexity that all of the possible lines of explanation could trace and prevent us from embracing any of them individually. Mapping [conflicts] will help us to understand the uncertainties surrounding [contexts] in greater depth (...)» (Yaneva 2012: 89).

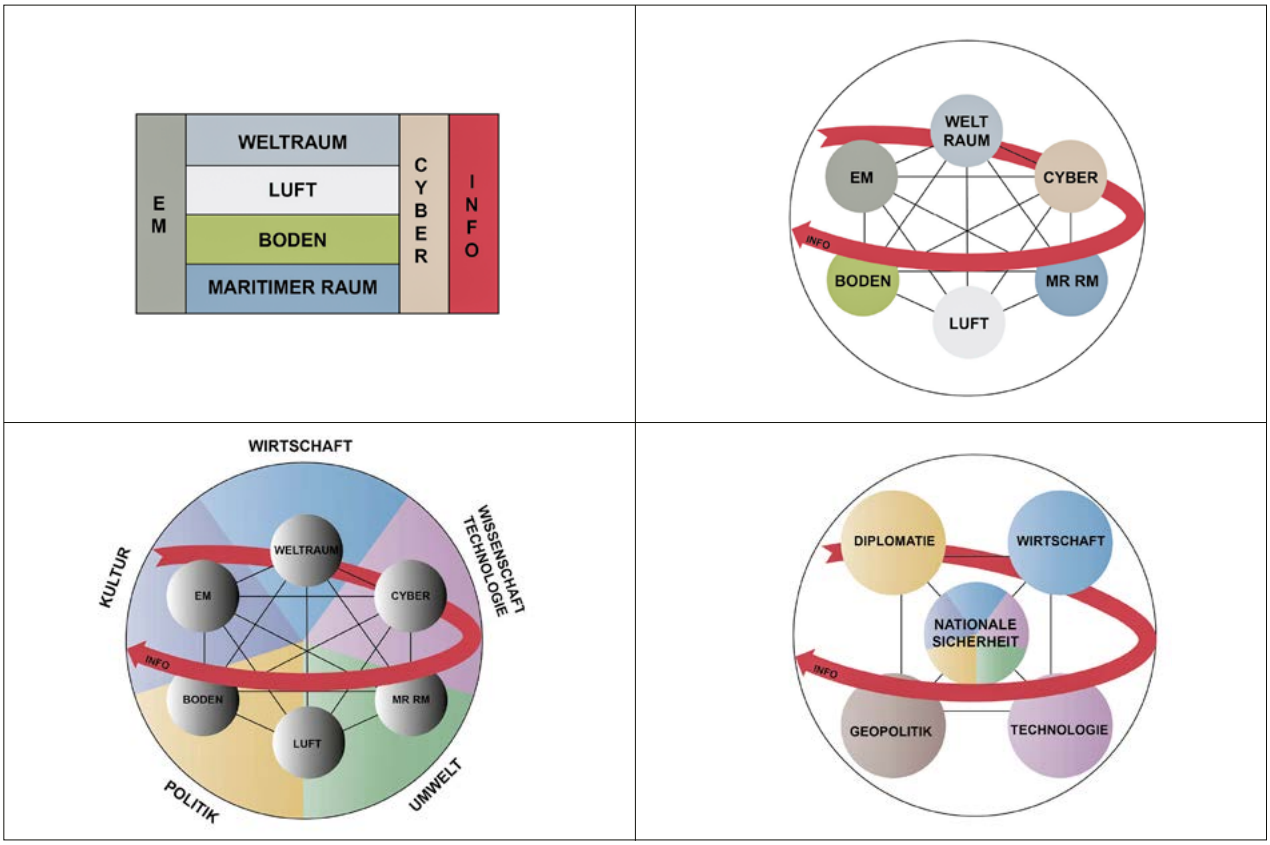


Abbildung 8 Erweiterte strategische Deutungsfelder (im Uhrzeigersinn von links oben):
(1) Doktrin, (2) Militärstrategie, (3) nationale Sicherheitsstrategien sowie (4) geopolitische Interpretation (Prinzipdarstellung Autor).

Box 9: Ursachenlogik – Columbia-Shuttle STS-107
Das Beispiel des Columbia-Shuttle STS-107 Unglücks ist ein exemplarisches Beispiel für die vernetzte Betrachtung und Analyse unterschiedlichster Faktoren, Akteure und Zusammenhänge. Die Columbia STS-107 war in der Luft nicht nur ein fliegendes Objekt, sondern ein komplexes Ereignis innerhalb eines Beziehungsgefüges der NASA, der Öffentlichkeit, der Wissenschaft, etc. Die Ursache des Columbia-Shuttle-Unglücks 2003 war nicht alleine aeronautisch-materieller Ursache wegen Überhitzung des Tragflächeninneren, sondern resultierte aus einem Schwarm von Zusammenhängen: bürokratische Abläufe innerhalb der NASA, Raketentechnologie, meteorologische Einflüsse, Pilotenausbildung, politische Akteure, öffentliche Erwartung, Faktor Zeit, Atmosphärenverhalten, Erfolgsdrang, etc.

Mit dem Einsatz von ANT können die Spin Elemente besser herausgelesen werden, die die NASA, die Medien und die Politik produzierten, vgl. Latour, Bruno (2010).

Militärstrategisch optimierter Nachrichtendienst (D)

Mit einem Nachrichtendienst, der militärstrategische Zusammenhänge beleuchtet, wird das Bewusstsein für Spin Politics, die hermeneutische Kritikfähigkeit sowie deren Quellenanalyse gestärkt; d. h. ein militärstrategischer Nachrichtendienst hat als *moteur de recherche* die Fähigkeit, die vagen Akteure, Ziele, Mittel und Verfahren in einem übergeordneten Moment und in unterschiedlichen Kontexten zu kartographieren und zu analysieren. Ein solcher Dienst setzt sich mit Doktrin, Analyse-Methoden und Techniken nachrichtendienstlicher Arbeit auseinander und liefert die Grundlagen für unterschiedliche sicherheitspolitische Zwecke: (1) ***Doktrin,*** (2) ***Militärstrategie,*** (3) ***nationale Sicherheitsstrategien*** sowie (4) ***geopolitische Interpretationen*** (Abb. 8). Aus dieser Warte können gezielt der Militärdoktrin übergeordnete Faktoren und Sphären beobachtet und flexible geopolitische Systeme analysiert werden wie (a) Veränderungen von Arbeits- und Führungsstrukturen (Sozioökonomie), (b) Entwicklungen im Bereich *digital democracy* (Soziopolitik), (c) Auswirkung von *virtual* und *augmented reality* (Soziotechnologie) und (d) Umfeld-Veränderungen bezüglich Religion, Formen des Zusammenlebens sowie Generationsfragen (Soziokultur).

... ein militärstrategischer Nachrichtendienst hat als *moteur de recherche* die Fähigkeit, die vagen Akteure, Ziele, Mittel und Verfahren in einem übergeordneten Moment und in unterschiedlichen Kontexten zu kartographieren und zu analysieren.

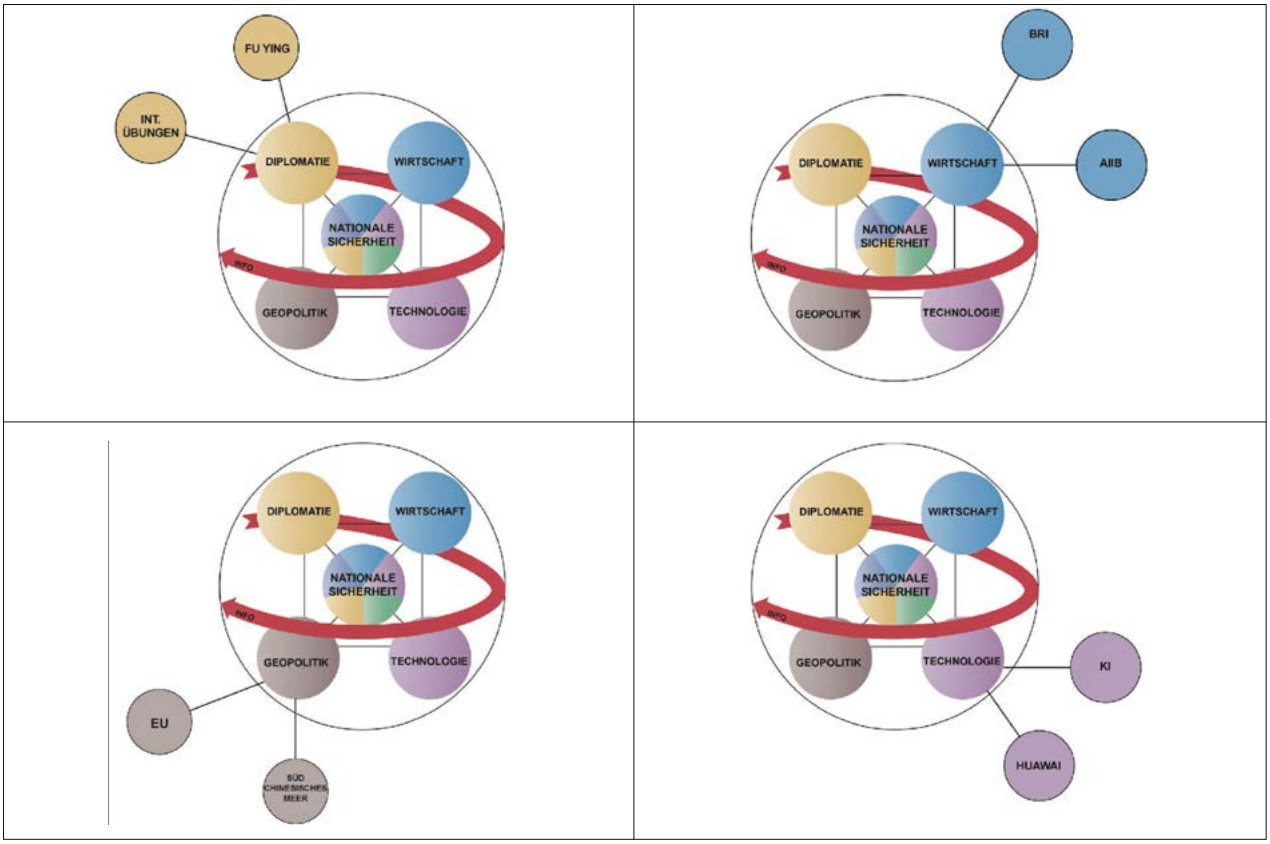


Abbildung 9 Chinas Prinzipbeispiele: diplomatische, ökonomische, geostrategische und technologische Agenden (Prinzipdarstellung Autor).

In letzter Konsequenz reduzieren sich heute geopolitische Fakten auf die 280 Buchstaben eines Tweets.

Mit der Verflechtung des globalen Kommunikationsraums, der Produktion von alternativen Wahrheiten und postfaktischem Wissen wird die Aufwertung der unterschiedlichen Intelligence-Kanäle für die Auswertung von Rohdaten und gelenkten Informationen immer wichtiger.[39] Die fortschreitenden Entwicklungen in der Big-Data Sammlung und der künstlich intelligenten Auswertung helfen Rohdaten zu ordnen und unterschiedlichste Zielbeziehungen zu visualisieren.[40] Da sich die Konzentration der Medienkanäle auf ein paar wenige global agierende Unternehmen fokussiert, sind Informationen und Deutungen zunehmend gebündelter und einseitiger (vgl. OSINT): Handlungen, Ereignisse und Fakten sind allzu oft ein Produkt von Medien. Mit dem Abbau umfassender Korrespondentennetze und Journalismus à la Newsroom können Medientitel stärker für spinpolitische Zwecke eingesetzt oder missbraucht werden.[41] Beispiele dafür sind die durch Russland oder China geförderten Kanäle *RT Kanal*, *CCTV* oder durch das als *Rockefeller Foundation* getarnte Kulturprogramm der *CIA* im Kalten Krieg. Auch der Abbau des Korrespondentennetzes der *Neuen Zürcher Zeitung* (NZZ) verweist auf Abhängigkeiten in der Informationsbeschaffung und Interpretation. Dank digitaler Verbreitung werden heute Kommentare und Meinungen schneller in Umlauf gebracht als faktengestützte Berichte. Diese Medienlogik folgt der Ökonomisierung der Informationskanäle: Nur was Klicks fördert, sind für Medienhäuser und soziale Medien *gute* Informationen. Zudem werden Nachrichten vermehrt von Roboter-Programmen generiert. In letzter Konsequenz reduzieren sich heute geopolitische Fakten auf die 280 Buchstaben eines Tweets.

Die spinpolitischen Effekte von Geopolitik, Diplomatie, Ökonomie und Technologie zeigen anhand des Beispiels China exemplarisch auf, wie engmaschig Zusammenhänge gesponnen werden können. China hat verstanden, dass Handlungen Informationen sind, dass deren Kontexte perpetuum mobile-ähnliche Eigendynamiken auslösen und damit auch gezielt zur (Des)Information beitragen. Spin Politics ist in diesem Sinne kein Konzept, sondern ein flexibles System ohne wirklichen geopolitischen Kanon. Die Kraft der Ordnung des chinesischen Spins oszilliert zwischen einer Strategie der Zustimmung, der Einschüchterung und der Unwissenheit und ist damit um einiges anspruchsvoller als China mit Begriffen wie Han-Nationalismus, Gleichschaltungspolitik oder globaler Supermacht zu kategorisieren. In diesem bewusst offenen Spannungsfeld,

39 Deutschland fördert seit 2017 interdisziplinäre Forschungsprojekte im Bereich *Social Media Intelligence*. Die Erkenntnisse und Methoden sollen zu präventiven Zwecken in der nachrichtendienstlichen Netzwerkanalyse eingesetzt werden. Erwähnenswert sind dabei die Projekte *X-Sonar*, *RadigZ* und *Integer*.

40 Die Möglichkeiten und Auswirkungen von KI auf die geopolitische Analyse- und Interpretationsarbeit werden vielfältiger und vernetzter. Leider würden weiterführende Bemerkungen zu *KI Mapping* und *Big Data Intelligence* den Rahmen dieses Artikels sprengen.

41 Vgl. Die Massnahmen zur Bedrohung von Cyber-Risiken (NCS 2018: 14).

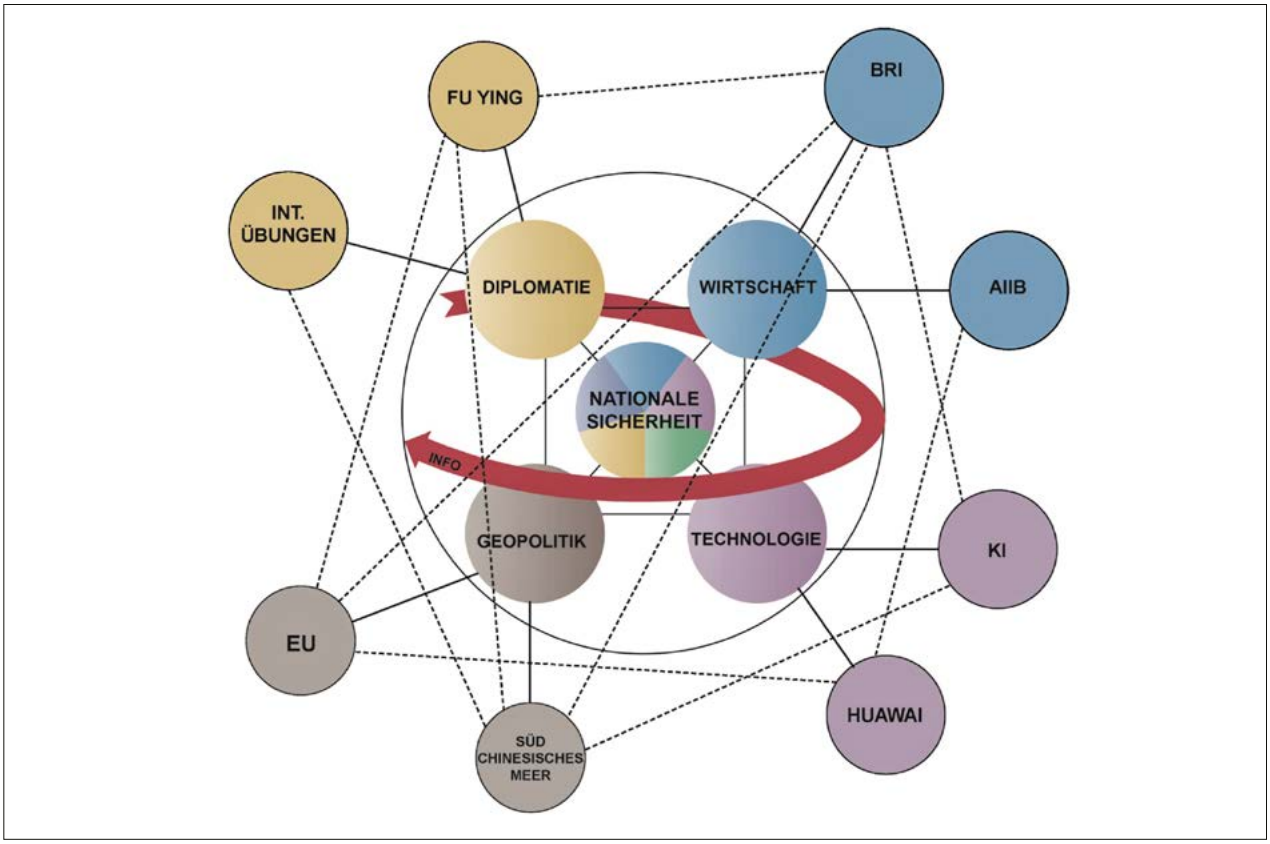


Abbildung 10 Chinas spinpolitische Agenda (Prinzipdarstellung Autor).

ohne Kanon und flexibler Sicherheitsarchitektur, müssen geopolitische und spinpolitische Zusammenhänge vermessen und gelesen werden. Chinas Flexibilität und deren Spin lässt sich an seiner militärischen Strategie ablesen: Bestätigt durch die Kommunistische Partei, deren Zentralkomitee und der zentralen Militärkommission im Jahr 2003, setzt die chinesische Volksbefreiungsarmee[42] in ihrer Verteidigungsdoktrin konsequent auf die dreidimensionale Kriegsführung (*Three Warfares*: rechtliche, psychologische und mediatische Dimension[43]). Eingelöst wird diese mehrdimensionale Strategie exemplarisch durch die Infrastrukturpolitik der BRI. Das Spiel zwischen Symbolpolitik, offener Machtpolitik und auch ökonomischer Befriedigungspolitik ist nicht simple Strategie hinter der Strategie.[44] Sie muss in der Eigendynamik des endogenen Spins gelesen werden. Diese Spins helfen China ihre Dilemmas[45], internen Machtinteressen und Opportunitätsüberlegungen zu entdramatisieren.

Gute militärstrategische und nachrichtendienstliche Arbeit muss über die Fähigkeit verfügen, Ereignisse und Handlungen in ihren unterschiedlichsten Zielbeziehungen zu analysieren und zu verstehen.

Wie das Fallbeispiel China zeigt, müssen für eine effektive militärstrategische Führung, die agiert und nicht reagieren muss, Kontext und Informationen erweitert, vernetzt und kartographiert werden. Nur so kann man mit Faktoren wie Mehrdeutigkeit und Zufall analytisch arbeiten.[46] Es geht nicht mehr darum, Geopolitik zu verstehen, sondern vielmehr mit der Hebelwirkung von Graubereichen zu operieren, wo Kooperation, Machtdemonstration und Unwissenheit eng miteinander verzahnt sind.

Gute militärstrategische und nachrichtendienstliche Arbeit muss über die Fähigkeit verfügen, Ereignisse und Handlungen in ihren unterschiedlichsten Zielbeziehun-

42 Im Gegensatz zu einer nationalen Armee, die ihren Staat und ihre Bevölkerung schützt, ist die Volksbefreiungsarmee durchaus da, um die politische Stärke der Staatspartei zu garantieren und zu festigen (vgl. European Parliament, Think Tank (2015) sowie Lew, Christopher (2016): *Complexities of Controlling the Gun: the PLA Role in CCP Politics.* In: Asia Dialogue).

43 Vgl. Sangkuk 2014: 198–221.

44 Im Gegensatz zu Henrique Schneiders Ausführungen zur BRI (Schneider 2017: 8–9).

45 Das *Malakka Dilemma* ist ein gutes Fallbeispiel, um Chinas endogenen Spin herauszuarbeiten. Die Wasserstrasse von Malakka, zwischen Malaysia und Indonesien, ist Teil der BRI und strategisch eine wichtige Handelspassage (ca. 30 Prozent des weltweiten Handels geht durch diese Passage). Um wachsen zu können, ist China auf diese Verbindungslinie angewiesen. Das Dilemma besteht darin, dass die Staaten entlang der Malakka-Strasse Amerika wohlgesinnt sind. Darum versucht Peking diese Abhängigkeit zu umgehen und setzt dabei auf versteckte und offene Macht- und Symbolpolitik.

46 Stefan Halber in einem Expertenbericht für das amerikanische Verteidigungsministerium: «Our war colleges and military research traditions emphasize kinetic exchange, the positioning and destruction of assets and metrics that measure success by kill ratios and infrastructure destruction. US Strategic analysis addresses the central challenge of battle space dominance and the optimum applications of C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance). By adopting the Three Warfares as an offensive weapon, the Chinese have sidestepped the coda of American military science. Our institutional apparatus and intellectual traditions are focused on a different phenomenon when we speak of, or think of, war. They have introduced a military technology which has not previously been considered as such in the West» (Halper 2013: 19).

gen zu analysieren und zu verstehen. Darum ist es von entscheidender Bedeutung, Informationen auch jenseits von Propaganda und STRATCOM in grösseren Zusammenhängen lesen zu können. Ereignisse und Handlungen wie auch Fakten sind ein Produkt von Deutungen. Darum verlangen sie, dass wir unsere Perspektiven und Sichtweisen ständig kalibrieren; der Zugriff auf Tatsachen ist vermittelt und durch unterschiedliche Filter gelenkt. Geopolitische Strategien sind nicht einfach übersetzbar, sondern sie schälen sich aus Kontexten heraus. Eine konsequent angewandte strategische Analyse unterstützt effektiv die sicherheitspolitische sowie die militärisch-operative Lagebeurteilung. Um dies zu stärken, bestünde eine Option im Ausbau der militärstrategischen Antizipationsfähigkeit und im Aufbau einer Task Force, bestehend aus Miliz- und Berufskomponenten. Sie könnten die methodischen Grundlagen und Instrumente für den Analystenalltag erarbeiten und die strategischen Zusammenhänge von *Information-Handlung-Kontext* exemplifizieren. Die NATO verfügt mit dem *NATO Strategic Communications Centre of Excellence* (NATO StratCom COE) in Riga über eine Einheit, die der Informationspolitik und deren militärischen Relevanz zentrale Bedeutung beimisst. Die EU wiederum hat seit 2015 mit der *East StratCom Task Force* einen strategischen Informationskanal, der der Informationspolitik Russlands entgegenzuwirken versucht und zugleich die eigenen EU-Positionen stärkt. Der Einsatz dieser STRATCOM-Einheiten zeigt, dass Spin Politics in einer multipolaren Welt ein immer wichtigeres machtpolitisches Instrument wird. Darum wird die strategische Deutung von Informationen und Handlungen sowie die Art, die Welt zu lesen, für den operativen militärischen Alltag immer entscheidender. Die Kompetenz der Milizangehörigen der Schweizer Armee ist für die Antizipation und Kontextanalyse von entscheidender Bedeutung; die fachlichen Kenntnisse von HistorikerInnen, EthnologInnen, AnthropologInnen, LinguistInnen, ÖkonomInnen, TheologInnen, PolitikwissenschaftlerInnen, HumangeographInnen etc. können zu einem holistischen und kontextuellen Verständnis beitragen und Impulse für die Militärdoktrin und strategischen Stabsarbeit liefern.

Bibliographie

- Armeestab A Stab, Schweizer Armee, Eidgenössisches Department für Verteidigung, Bevölkerungsschutz und Sport VBS (2015): *Militärstrategische Stabsarbeit.*
- Arthur, Charles (2012): *China's Huawei and ZTE pose national security threat, says US committee.* In: The Guardian, https://www.theguardian.com/technology/2012/oct/08/china-huawei-zte-security-threat (8.10.2018).
- Bolz, Norbert (2017): *Das Genie der Gesellschaftstheorie. Vor neunzig Jahren kam der deutsche Kultautor Niklas Luhmann zur Welt. Was bleibt?* In: Neue Zürcher Zeitung, 06. 12. 2017, S. 37.
- Brînza, Andreea (2018): *Redefining the Belt and Road Initiative. The BRI is not about physical routes in Eurasia. It is about global strategy.* In: The Diplomat, https://thediplomat.com/2018/03/redefining-the-belt-and-road-initiative/ (20. 03. 2018).
- Butter, Michael (2018): *Nichts ist, wie es scheint. Über Verschwörungstheorien.* Berlin: Suhrkamp.
- Castells, Manuel (2010): *The Rise of the Network Society.* Oxford: Wiley-Blackwell.
- Chandler, Daniel (2005): *Semiotics: The Basics*. London: Routledge.
- Chase, Michael S. et al. (2015): *Emerging Trends in China's Development of Unmanned Systems.* A RAND Report.
- Chen, Stephen (2017) : *Why Beijing is speeding up underwater drone tests in the South China Sea*. In: South China Morning Post, https://www.scmp.com/news/china/policies-politics/article/2103941/why-beijing-speeding-underwater-drone-tests-south-china (26.07.2018).
- Descola, Philippe (2014): *Die Ökologie der Anderen. Die Anthropologie und die Frage der Natur.* Berlin: Matthes&Seitz.
- European Parliament, Think Tank (2015): *The role of the army in China's politics,* http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2015)564375 (29.06.2015).
- Fisher, Max (2012): *Here's the Chinese passport map that's infuriating much of Asia.* In: The Washington Post, https://www.washingtonpost.com/news/worldviews/wp/2012/11/26/heres-the-chinese-passport-map-thats-infuriating-much-of-asia/?noredirect=on&utm_term=.4773eeb53b50 (26.11.2012).
- Halper, Stefan (2013): *CHINA: The Three Warfares. Study prepared for Andy Marshall, Office of the Secretary of Defense*. Washington D. C.
- Harrison, Jacobs (2018): *China's «Big Brother» surveillance technology isn't nearly as all-seeing as the government wants you to think.* In: Business Insider, http://uk.businessinsider.com/china-facial-recognition-limitations-2018-7?r=US&IR=T (15.07.2018).
- Harrison, Jacobs und Pat Ralph (2018) *Inside the creepy and impressive startup funded by the Chinese government that is developing AI that can recognize anyone, anywhere*. In: Business Insider, http://uk.businessinsider.com/china-facial-recognition-tech-company-megvii-faceplusplus-2018-5?r=US&IR=T/#the-buzziest-and-formany-most-terrifying-use-of-face-has-been-by-chinese-police-china-already-has-170-million-security-cameras-in-use-for-its-so-called-skynet-system-with-400-million-more-on-the-way-face-is-already-being-used-as-part-of-that-system-one-of-megviis-biggest-investors-is-chinas-state-venture-capital-fund-8 (8. Juli 2018).
- Hoyningen-Huene, Paul (2004): *Formal Logic. A Philosophical Approach.* Pittsburgh: University of Pittsburgh Press.
- Hugo, Victor (2001): *Quatre-vingt-treize*. Paris: Edition de Bernard Leuilliot.
- Jiang, Sijia und Julie Zhu (2018): *China's Sense Time valued at $ 4.5 billion after $ 600 million funding led by Alibaba: sources*. In: Business Insider, http://uk.businessinsider.com/r-chinas-sensetime-valued-at-45-billion-after-600-million-funding-led-by-alibaba-sources-2018-4?r=US&IR=T (9.04.2018).
- Krauer, Daniel und Noli-Kilchenmann, Anita (2016): *Die Militärdoktrin (MD 17)*. In: Military Power Revue der Schweizerischen Armee, Nr. 2/2016, S. 5–23.
- Landesamt für Verfassungsschutz Baden-Württemberg (?): *Falsche oder Fremde Flagge.* In: *Glossar* Online, http://la.boa-bw.de/archive/frei/173/0/www.verfassungsschutz-bw.de/spio/spio_glossar_spioabwehr.htm#f (30. 09. 2017).

- Latour, Bruno (2010): *Networks, Societies, Spheres: Reflections of an Actor-network Theorist.* Keynote speech for the International Seminar on Network Theory: Network Multidimensionality in the digital age, Annenberg School for Communication and Journalism, Los Angeles (19.02.2010).
- Lew, Christopher (2016): *Complexities of Controlling the Gun: the PLA Role in CCP Politics.* In: Asia Dialogue, http://theasiadialogue.com/2016/12/06/complexities-of-controlling-the-gun-the-pla-role-in-ccp-politics/ (06.12. 2016).
- Miller, Nick (2018): *China undermining us «with sticks and carrots»: Outgoing German minister.* In: The Sydney Morning Herald, https://www.smh.com.au/world/europe/china-undermining-us-with-sticks-and-carrots-outgoing-german-minister-20180219-p4z0s6.html (19.02.2018).
- Morris, Charles William (1988): *Grundlagen der Zeichentheorie. Ästhetik der Zeichentheorie.* Frankfurt am Main: Fischer Taschenbuch.
- Mozur, Paul (2018): *Inside Chinas's Dystopian Dreams : A.I., Shame and Lots of Cameras*. In : The New York Times, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html (8.08.2018).
- NCS, Der Bundesrat (2018): *Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022.*
- Nolan, Peter (2012): *Is China Buying The World?* Cambridge: Polity Press.
- Sangkuk, Lee (2014): *China's «Three Warfares»: Origins, Applications, and Organizations.* In: Journal of Strategic Studies. Vol 37:2. S. 198–221.
- Schneider, Henrique: *Geopolitische Implikationen der «one belt, one road»-Strategie Chinas*. In: Allgemeine Schweizerische Militärzeitschrift (ASMZ), 183 Jahrgang, 10/2017, S. 8–9.
- Schulz-Schaeffer, Ingo (2000): *Akteur-Netzwerk-Theorie: zur Koevolution von Gesellschaft, Natur und Technik.* In: Weyer, Johannes (Ed.): Soziale Netzwerke: Konzepte und Methoden der sozialwissenschaftlichen Netzwerkforschung. München: Oldenbourg, S. 187–210. – Spörndli, Markus (2017): *Unbekümmert in die nächste Katastrophe*. In: Wochenzeitung, http://static.woz.ch/1745/saudische-machtdemonstration/unbekuemmert-in-die-naechste-katastrophe (09. 11. 2017).
- Steiger, Martin (2012): *Schweizer Netzinfrastruktur mit chinesischen Hintertüren?* In: Steiger Legal, https://steigerlegal.ch/2012/07/16/sunrise-netzinfrastruktur-mit-chinesischen-hintertueren/ (16.07.2012).
- Wuthnow, Joel (2017): *Chinese Perspectives on the Belt and Road Initiative: Strategic Rationales, Risks, and Implications.* INSS: China Strategic Perspectives 12. Washington, D. C: National Defense University Press.
- Yaneva, Albena (2012): *Mapping Controversies in Architecture.* Surrey: Ashgate.

Remo Reginold

FachOf (Hptm), Dr. phil., Politikwissenschaftlicher Berater und Lehrbeauftragter Universität Basel. Stab Militärischer Nachrichtendienst (MND).

E-Mail: remo.reginold@gmx.ch

Ethics in Military Public Affairs: a practical framework

In general, military doctrine states mission and duties of military public affairs. It often fails, however, in establishing the specific ethical standards for military public affairs. In addition, most military doctrines do not provide any guidance on how to trade off public affairs-related courses of action with ethical implications. This is an important gap, because the ethical content of military public affairs affects the military organization's social capital – for example, its credibility and trust. This, in turn, influences the overall ability of the military organization to complete its mission. This article addresses this gap in ethical guidance for military public affairs a) by discussing how public affairs and ethics interact creating social capital for the military organization and b) by developing a practical framework for ethical decision-making in military public affairs.

Henrique Schneider

Introduction: Public Affairs and Ethics

The ethical quality of public affairs in general[1] and of military public affairs in particular[2] is often doubted. At least in the eyes of some observers, (military) public affairs have a propagandistic streak. While propaganda is per se neither unethical nor irrational, it might affect the long-term credibility of an organization if perceived as wrong or void of ethical content. On the other hand, it is possible to combine ethical desiderata with (military) public affairs to increase the long-term credibility of an organization, for example, by creating trust. With a grain of salt, faulty propaganda diminishes the social capital of an organization while public affairs guided by ethics is likely to increase it.[3] This mutually beneficial combination is to be examined. From a practical point of view, this essay offers a framework for aligning ethics and military public affairs, hence is increasing the social capital of a military organization.[4] Practical means that the framework can be used in day-to day-situations.

Based on the North Atlantic Treaty Organization (NATO) as a proxy for military organizations, the ethical dimensions of military public affairs will be explored. Naturally, NATO doctrine does not automatically apply to all alliance members nor do its guidelines constitute a global standard. However, the references to NATO are sufficiently abstract to serve as a general description of military public affairs. The alliance is representative of its member states and cooperation partners, all of which have public affairs

Figure 1 Ethics entail trade-off between alternatives (Source: https://cdn.quotesgram.com/img/58/59/2064112258-ethics-and-compliance.jpg).

units. In addition, the alliance has a well-established doctrine, which is a sufficiently abstract point of departure.[5] While NATO is serving here as a proxy for military organizations, the practical framework developed in this article is likely to fit to any specific military environment.

Military Public Affairs Officers/Offices (PAO) are formal organizational units in a military context. They are tasked with dealing with or managing the flow of information, communication, the media and, often, with community issues. For more specific and limited purposes, the term also denotes media relations offices within the military. Apart from developing and managing their own communica-

1 Bowen, 2016
2 Floridi, Taddeo, 2014
3 Ostrom, 1994; Fukuyama, 1995
4 In this paper, the term "military organization" stands for any military organization, e.g., a unit, a task force, a mission, an army, or joint forces.
5 NATO, 2011

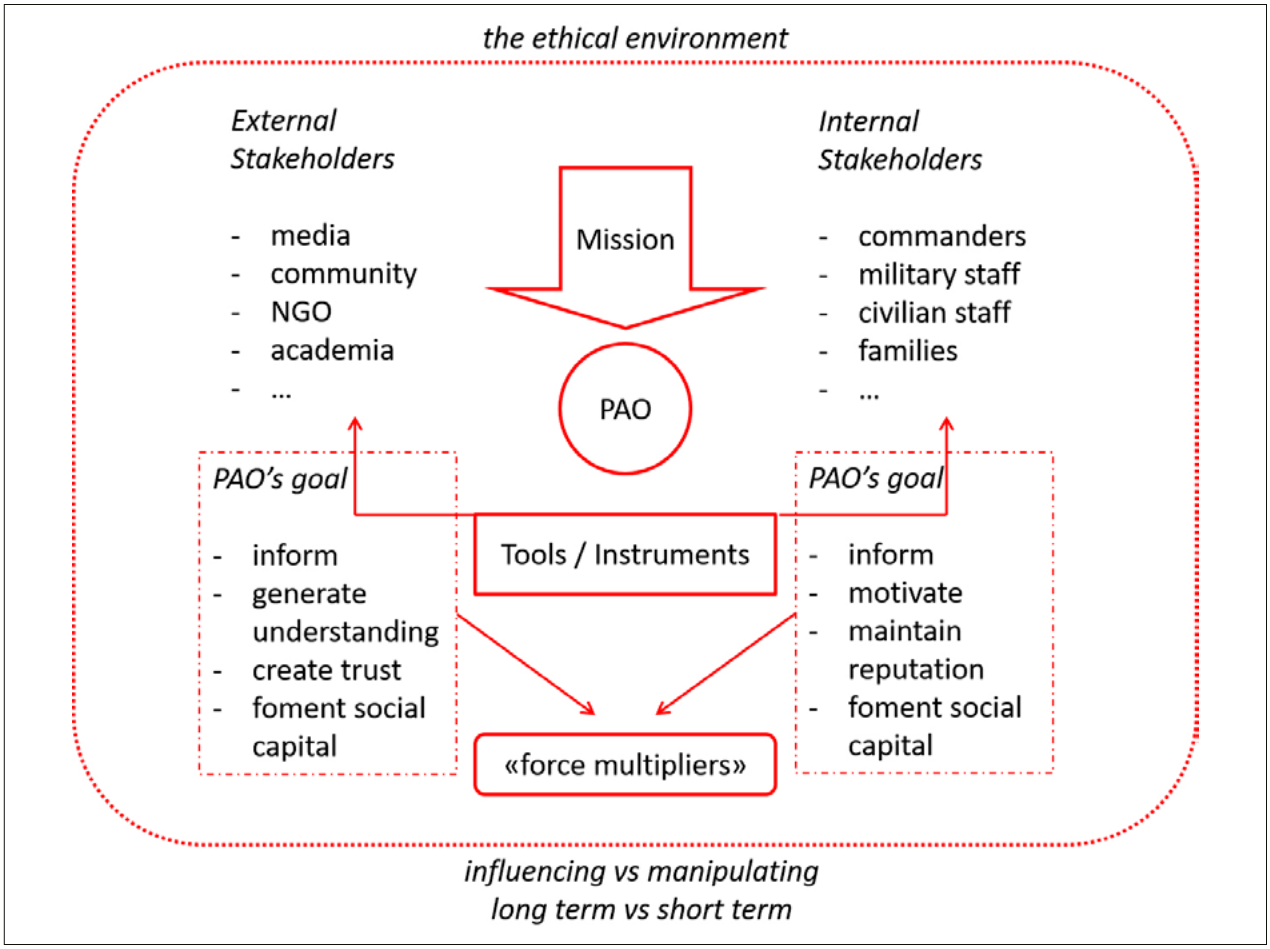


Figure 2 PAO's mission, stakeholders, and tools, embedded in ethics (Author's visualization).

tion programs, PAOs provide public affairs advice, counsel, and support, usually targeting commanders and senior staff members.[6]

NATO formulates the mission of PAOs as such: "The mission of NATO military PA is to support commanders by communicating accurate information in a timely manner to audiences to improve public awareness and understanding of the military aspects of the Alliance's role, aims, operations, missions, activities and issues, thereby enhancing organisational credibility. Audiences can be allied, international, regional, local or internal, depending on the issue or activity."[7]

The mission is not only stated in terms of input, or of tasks to fulfill, but also in terms of output, or of intended effects.

This passage illustrates that while PAOs should coordinate the flow of information-at-large, its mission also has a consequential component. The mission is not only stated in terms of input, or of tasks to fulfill, but also in terms of output, or of intended effects. These effects are to improve the public's awareness and to foment understanding of military activities. This should lead to more credibility and trust in the military organization. In short, the activities of PAOs have an effect – or should have an effect – on the organization's social capital in terms of credibility and the amount of trust that (internal and external) stakeholders posit on it.

While this comes as no surprise, because of it, the specific goals of PAOs as well as the desired impact of PAO activities have ethical implications. These implications arise first, because the intended effects such as "credibility" and "trust" are conceptionally tied to ethics; and second, because the tasks themselves presuppose some sort of ethical commitment. NATO's statement of a PAO mission resorts to concepts with ethical denotations, connotations, or implications such as "audience", "accurate", "timely", "understanding", or "credibility". This shows that ethics play a role for PAOs regarding input as well as output. While using these concepts, NATO, however, does not clarify these ethical implications. This is the first gap to be addressed here.

6 Henry, 2015
7 NATO, 2011, Pt. 6

NATO's statement of a PAO mission resorts to concepts with ethical denotations, connotations, or implications such as "audience", "accurate", "timely", "understanding", or "credibility".

The ethical dimensions in management of communication and information are well researched areas.[8] In addition, public affairs, since its beginning as a management practice, have been the object of critical reflection.[9] However, there is considerably less research specifically on military public affairs.[10] Consequentially, there is only little research dedicated to the ethical dimension of military public affairs and a PAO's mission or duties. Conversely, there is little transfer from the theoretical research to the practical realm. This is the second gap to be addressed.

For assessing both identified gaps, the first part briefly provides an overview over the many tasks that PAOs typically perform. The second part lays out the area of potential tension between the democratic process, human rights, and military ethics as well as between a PAO's mission, stakeholders' rights, and values. Basing on Parsons' "Ethics in Public Relations: A Guide to Best Practice"[11], the third part develops a practical framework for ethical decision-making. The framework serves as a guideline for harmonizing the areas of tension identified in part two and, mainly, for handling the ethical implications of military public affairs while envisaging the increase of the organization's social capital.

PAO: Position and Constraints[12]

PAO duties can be understood along these terms: PAOs are involved in planning and managing public relations programs to promote a broad understanding of a military organization's or a military mission's objectives, functions, and accomplishments using several channels of communication.[13] NATO's wording is: "NATO military PA is the function responsible to promote NATO's military aims and objectives to audiences in order to enhance awareness and understanding of military aspects of the Alliance. This includes planning and conducting external and internal communications, and community relations. Military PA at each level of command directly supports the commander and may therefore not be further delegated or subordinated to other staff functions."[14]

PAOs identify stakeholders and target publics, define strategic messages, devise communication strategies, manage flows of information and communication influencing their content, select media and methods of presentation, set program objectives and policies, as well as advise higher commanders on the public relations aspects of decisions and actions. Often, PAOs serve as a liaison and even as a coach in matters concerning information and communication.

Figure 3 Elements of ethics displayed at a NATO / SHAPE Public Affairs Conference in Kosovo 2016 (NATO/SHAPE).

Identifying these stakeholders, their expectations, as well as addressing their information and communication-related needs while respecting their rights is pivotal for the successful build-up of social capital by PAOs.

In fulfilling these duties, next to the organization's own expectations, PAOs deal with many stakeholders, whether they are internal or external to the military organization. Identifying these stakeholders, their expectations, as well as addressing their information and communication-related needs while respecting their rights is pivotal for the successful build-up of social capital by PAOs.

From the operative point of view, stakeholders are the target publics of specific activities or campaigns. However, from the point of view of strategy, it is the other way around. Stakeholders are the agents that influence the military organization. Or, as the concept's first definition goes, stakeholders are "groups without whose support the organization would cease to exist".[15] In order to gain their long-term support – and influence them in the short-term view –the respective military organization and their PAOs need to take stakeholders' rights, needs, and opinions into account. These rights, needs, and opinions are diverse and even contradictory, since there are several different stakeholder groups. Nonetheless, it is an important part of a PAO mission and tasks.

The goal of external communications is to achieve a "force multiplier" effect.

8 For example: Johannesen, Valde, Whedbee, 2008; Turilli, Floridi, 2009; Eberwein, Porlezza, 2016; Meisenbach, 2017
9 For example: Frederick, 1988; Pearson, 1989; Bowen, 2008, 2016; Parsons, 2016
10 Notable exceptions are: Burk, 2002; Robinson, De Lee, Carrick, 2008; Plowman, 2017; Karadag, 2017
11 Parsons, 2016
12 The contents of this section are visualized in figure 2.
13 Darley, 2005
14 NATO, 2011, Pt. 7
15 Freeman, Reed, 1983

NATO, for example, identifies the following stakeholder groups (or target publics): "In external communications, PAO should entertain good relations with the media and should prepare other military personnel to interact with it. Reaching out to non-media institutions, for example, academia, think tanks, or non-governmental organizations, is equally important." The goal of external communications is to achieve a "force multiplier" effect. And: "In internal communications, facilitating communication with and among NATO military and civilian personnel and their families should create an awareness of the organization's goals and activities, improve work quality, and make command personnel more effective representatives of the organization." The aim is, again, to turn the military force into "force multipliers" – but possibly force multipliers of another kind.[16]

In order to make the ethical trade-offs of these activities clearer: PAOs are to influence stakeholders in their understanding and being sympathetic to the respective military organization. The aim of PAO activities is to create "force multipliers", i. e. to increase the military organization's social capital. However, PAOs should refrain from manipulating stakeholders for ethical and/or operational reasons. First, manipulation is unethical. But then how can the line be drawn between influencing and manipulating?[17] Second, wrongly addressing stakeholder groups leads to a loss of social capital. But then how can a balance be found between the short-term goal of a public affairs activity or campaign and the long-term build-up of social capital?[18]

Tacitly acknowledging these trade-offs, NATO commits PAOs to the following principles: "Tell and show the NATO story; provide accurate information in a timely manner; ensure that information provided is consistent, complementary, and coordinated; practise appropriate operational security; conduct work mindful of multinational sensitivities, and respectful of the local and regional cultural environment."[19]

Deciding between different courses of action, or trading-off goals and means, is per se an ethical activity.

While these principles might provide guidance on how PAOs should perform duties combining the mission with (implicit) ethical standards, one of the most important aspects of practical ethics is still lacking, which is decision-making. In particular, these principles do not offer support in appreciating and trading-off different, contradictory, and influencing factors such as stakeholders' needs, rights and opinions, and courses of action.

Deciding between different courses of action, or trading-off goals and means, is per se an ethical activity.[20] It presupposes formulating preferences and criteria in order to be able to compare and rank alternative courses of action. Formulating preferences and criteria as well as assigning weight to them is a normative action. Normative actions entail judgement. Judgement entails the conception of ethics. Even if decision-making does not occur as a standardized procedure after mainly following intuition or "gut feeling", making a choice and later being responsible for it still entails at least some notion of discerning "right" and "wrong". This, again, belongs to the realm of ethics. The principles quoted above do not cover this aspect of PAO duties.[21]

The principles also do not address the unique position of a PAO. The office is not just a rotary wheel of information. As discussed earlier, PAOs influence the content, form, speed and rhythm of flows of information. Furthermore, PAOs are part of a military organization, stand in a line of command, and act instrumentally according to the organization's objectives. This triple function as the information hub, the unit in a command structure, as well as the organization's instrument puts PAOs in a position of power. In an organization, any position has some power marker. The salient point regarding PAOs is that, on the one hand, internal and external stakeholders expect certain neutrality of PAOs and, on the other hand, PAOs, by virtue of the position, cannot be neutral.[22] Therefore, a framework for ethical decision-making in PAOs should address the activities as well as the position of a PAO.

Ethics: Areas of (Potential) Tension[23]

The ethical challenges of PAOs can occur on the level of activities as well as on the level of their position within the organization's structure. After having identified where challenges can arise, this section lays out which and how challenges arise.

Information or communication ethics is a descriptive theory that explores the activities and structures of power influencing attitudes and cooperative practices; it is also a normative theory to optimize those values committed to the general reason of the "good".[24] Applying this definition to PAO duties, information or communication ethics explores and evaluates the management of normative values within the flow of information and communication, the creation of new structures of power, hidden contradictions and agendas in information and communication practices, as well as the development of ethical conflicts in this field.

In order to analyze these interdependences, this section constructs two isomorphic areas of tension, one at a macro level and one at the micro level. The macro level is an area of tension between human rights, democracy, and military ethics. The procedure for forming political will – usually, the polity's parliament – is in the center of this area of

16 NATO, 2011, Pt. 8
17 Sunstein, 2016
18 Webster, 2014
19 NATO 2011, Pt. 9
20 Shapiro, Stefkovich, 2016
21 Ferrell, Fraedrich, 2015
22 Ferrell, 2016
23 The contents of this section are visualized in figure 4.
24 Parsons, 2016

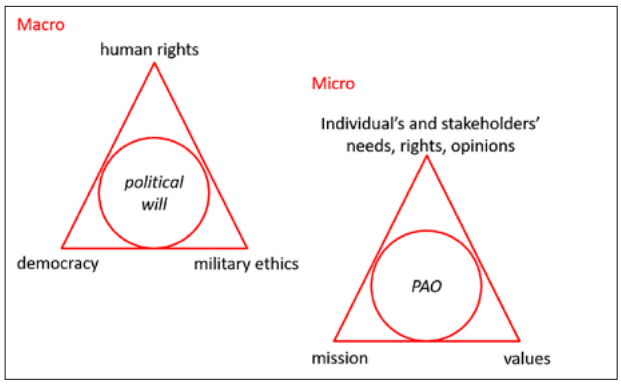


Figure 4 Isomorphic structures for ethical analysis (Author's visualization).

Figure 5 Embedding the military in the community, 4-Tage-Marsch (http://www.communicators.ch/aktuell/article/2018/01/19/grossartige-tribuene-fuer-die-schweizer-armee/).

tension, trading-off between these dimensions. The micro level is a derivation of the first, applied to the situation of a PAO. It is an area of tension between individual and stakeholders' needs, rights, and opinions, the military mission, as well as the values with the PAO as its trading-off centre. These structures work as follows:

For the macro level: Many national constitutions – to which military organizations are bound – contain provisions with values influencing information and communication ethics. The Universal Declaration of Human Rights – as an abstract proxy to the different constitutions – states such values, for example, in the right to freedom of opinion and expression (Art. 20) or the right to freedom of thought, conscience, and religion (Art. 19) or the respect for the dignity of human beings (Art. 1).[25]

However, human rights or constitutions – taken as proxy lists of ethical desiderata – are not ethics per se. They are normative bases. At the same time, they interact with other normative subsystems, for example, with the political system of a country – in the case of most NATO members: democracy – or the outcomes of political decision-making and, in the military case, with the specific military ethics. These three elements are not always aligned, or they are not aligned on their own. The procedures for establishing the political will of a specific polity balance this area of potential tension on the macro level.[26]

However, human rights or constitutions – taken as proxy lists of ethical desiderata – are not ethics per se.

For the micro level: The triangle formed by the democratic process, human rights, and military ethics is relevant at a macro level. On the micro level of the military and the PAO, the triangle is replicated by another one formed by the mission, the needs, rights, opinions, and values of stakeholders. This triangle is also marked by a set of trade-offs. Unlike the macro triangle, which is managed by society as a whole or its political bodies, the micro triangle is balanced by PAOs.[27] For managing this triangle, PAOs need to resort to ethics in activities and campaigns. This triangle, however, puts PAOs, again, in a position of trust, power, and responsibility – all of these with ethical implications of their own.

25 This paper does not claim that human rights are a normative basis for military public affairs. Rather, human rights are a proxy for the ethical values shared by countries subscribing to the Declaration, or at least they summarize many ethical expectations that state and non-state agents have. Furthermore, human rights are often a normative basis for military interventions.

26 There is much research on different aspects of the interaction between the democratic process, human rights as a proxy for what countries consider ethical desiderata, and military ethics. The triangle formed by them is especially marked by many trade-offs. While these trade-offs are important, their analysis falls outside the scope of this article, which is the micro level, or the role of a PAO. For further analysis, each focusing on different aspects of the relationships of democracy, human rights, and military ethics, refer to: Donnelly, 2013; Toner, 2015; Headley, 2016

27 This approach to ethical analysis is not exclusively applicable to PAOs. It can also be applied to commanding officers et al., by considering them the trading-off center of the area of tension. This article chooses to focus on power.

Figure 6 PAO turning military commanders in public figures (US Army Southwest Command).

However, commanding officers, the chain of command generally, and especially PAOs are in the position and have the mission's mandate to interfere with the "free" flow of information if they deem it necessary to fulfil their mission.

Handling the micro triangle is not only a matter of how to balance ethical desiderata in making decisions. It is especially about unifying the theoretical and practical aspects of military and ethical decision-making. Some examples illustrate this aspect: Soldiers have the freedom to access information and the right to communicate – even if they lack the formal right, they often have the means to do so, for example, via the web or social media. Stakeholders have the right to know how a military activity affects them specifically and what it means for the political body they care about – again, even if they lack the formal right, they have means for exchanging and expressing their knowledge and apprehensions or, worse, speculations. However, commanding officers, the chain of command generally, and especially PAOs are in the position and have the mission's mandate to interfere with the "free" flow of information if they deem it necessary to fulfil their mission. This situation requires careful scrutiny whether a PAO is to trade off interests while building up the social capital of the military organization.

In addition to these remarks, the ethical dimensions of a PAO's position, trust, power, and responsibility warrant some comments. It is a dilemma to assign a person or group to a position of trust, since trust is a function of human capital. Therefore, trust is something that grows or is accumulated.[28] On a personal level, it is impossible to ask for trust. However, the position of the PAO demands institutional trust. The person or group holding the position trusts the organization and the organization entrusts the PAO with managing different flows of information and communication. From this institutional position on, the person/people advance to gain the trust of the various stakeholders in order to fulfill the assigned duties. It is a double-sided idea: Trust is entrusted institutionally to the PAO, but, at the same time, the PAO should gain and accumulate the trust of the stakeholders. With institutional trust and amounting trust from all stakeholders, PAOs gain power or influence over the organization and over people as well as groups.[29] It is a matter of responsibility of both amassing trust and using the resulting influence for the "good" of the organization.

Ethics for a PAO: a Practical Framework[30]

PAOs manage activities with ethical implications. PAOs operate in a position of power, which in itself has ethical implications. Balancing the area of potential tension, PAOs aim to create "force multipliers" or to increase the social capital of the military organization. How to accomplish this?

28 Ostrom 1994; Fukuyama, 1995
29 Luhmann, 1979
30 The contents of this section are visualized in figure 7.

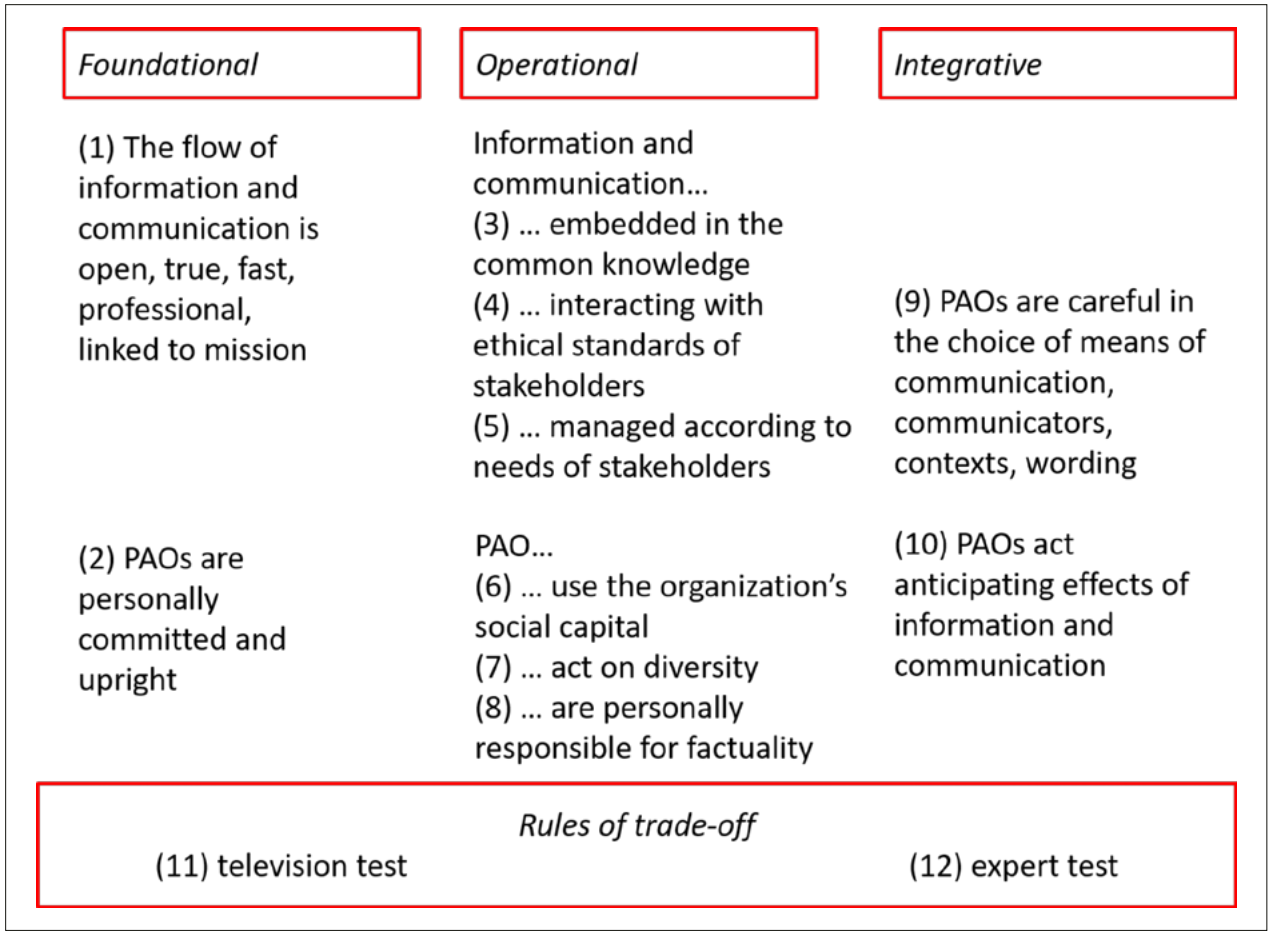


Figure 7 PAO's ethical framework (Author's visualization).

Balancing the area of potential tension, PAOs aim to create "force multipliers" or to increase the social capital of the military organization.

The framework developed in this section provides systematic support for the management of this micro triangle, from the ethical point of view. It is a practical roster for PAOs to consist of 12 guidelines. The first two are of foundational nature. Guidelines 3–10 operationalize these fundamentals in its different aspects of this foundation and are tying them together. The last two are guidelines on how to decide ethically, i. e. on how to trade off.

Foundational guidelines are:

- (1) The flow of information and communication in general should be open, true, fast, professional, and linked to the organization's mission.
- (2) PAOs need personal commitment to the role; personal commitment demands integrity.

There is an intended parallelism between both guidelines: (1), and subsequently (3)–(5), address the level of PAO activities in view of PAO ethics of a while performing an activity. (2), and subsequently (6)–(8), focus on the position and personality of a PAO. These mirrored structures address the gap identified in the previous sections and acknowledge the interdependence of task and personality, which is especially prevalent in ethics.

Following this logic, the first guideline states how the flow of information and communication is managed and the second imposes a personal commitment on a PAO for doing so. This personal commitment is necessary for creating trust in the position as well as the military organization. In other words, while managing the flows of information and communication, PAOs become keepers of social capital. In order for this to happen, PAOs have to demonstrate a particular personal commitment to their role and function. The personal commitment cannot only be to the mission but has to involve the other aspects of the area of potential tensions.

Integrity and honesty are expanding this commitment that entails keeping to one's word, keeping information factual, neither embellishing nor distorting information and communication, carefully selecting the context and wording of information and communication, and managing the flow of knowledge to envisage the greater "good" of the organization.[31]

31 Toner, 2015

Communication can only be a reliable source for leadership if the given information is always true and based on facts or, in the case of interpretations or hypotheses, clearly marked as such.

Note that a managed flow of information does not conflict with these guidelines.[32] Communication can only be a reliable source for leadership if the given information is always true and based on facts or, in the case of interpretations or hypotheses, clearly marked as such. Truth is not relative to the stakeholder but is an objective commitment. This is not just because of the ethical value truth might have inherently, but it also because it is difficult to keep an untrue story undiscovered. Thus, it also has a consequential aspect. By being committed to informational truthfulness and factuality, PAOs also ensure the mid and long-term ability of an organization to accumulate trust and its ability to serve as a partner to stakeholders.[33]

Once the truthfulness and factuality of pieces of information is checked and the degree of information to be circulated is determined, PAOs still should select the means of information, the tone, the wording, the context of dissemination, inter alia. The next question is who is giving information to whom. PAOs will have to motivate different people – superiors and subordinates, sometimes people outside their own organization – to inform as well as to accept information. In this sense, turning different people – superiors, subordinates, and external parties – into communicators is committing them to an exchange with each other according to the multiple sides' needs and situations. Therefore, PAOs should provide channels for top-down, bottom-up, top-top, and bottom-bottom information and communication internally as well as externally. By providing channels and putting the right people in the right knots of the information flow, a PAO shows that information and communication is not necessarily linked to a PAO's position but to a function of the organization. At the same time, the personal involvement of a unit's personnel with communication and information strengthens the personal commitment of the organization's members themselves, which is a valuable resource in leadership and enforces different aspects of the second postulate mentioned above. It becomes self-establishing.

This reasoning leads to guidelines (3)–(5) providing guidance on how to operationalize guideline (1):

- (3) Information and communication occur embedded in the previous experience and common stock of knowledge of an organization.
- (4) Information and communication interact with the ethical standards of each stakeholder group, i. e. information and communication are a dialogue between PAOs and stakeholders.
- (5) PAOs manage different flows of information and communication according to the needs of the involved stakeholders – for example, chain of command, bottom-up, bottom-bottom, internal and external.

Guidelines (6)–(8) operationalize foundational guideline (2):

- (6) The upright PAO knows mission, needs, rights, and opinions of stakeholders, as well as the values of the military organization. The upright PAO uses this stock of knowledge for the long-term good of the organization.
- (7) Act on diversity in internal and external stakeholders.
- (8) PAOs are personally responsible for the truth and factuality of the content as well as the flows of information and communication they manage.

Guidelines (9) and (10) align both aspects, the quality of the flow of information and communication with the individual qualities of the management of that flow:

- (9) PAOs are careful in the choice of means of communication, communicators, contexts in which communication takes place, and the wording of communication.
- (10) PAOs check all effects that the information and communication flow might have on the organization and external audiences.

These guidelines are necessary but not sufficient for dealing with ethical decision-making. Even when following them, ethical dilemmas arise. Or, especially while following them, ethical dilemmas will become more apparent to PAOs. The guidelines cannot, by themselves, minimize or mitigate situations in which ethical judgement calls are needed. The last two guidelines provide approaches on how to make those judgement calls or how to trade off.

Naturally, these guidelines do not substitute the rational ethical judgement, but they provide two useful ways of thinking about ethical dilemmas as a thought experiment in the form of two tests.

- (11) Television test: Can the PAO explain the decision about the course of action taken on national television? Can the PAO explain the decision and convince a broad public?

If a PAO is able to explain the decision taken in such a way that it passes the ethical scrutiny of the broad public intuition, in matter as well as in presentation, then the decision can count as ethical in a sense of prevailing within the general ethical dialogue.

This first test assesses the broad understanding of a decision and the broad acceptance of its sense. It assesses technical criteria such as wordings, body language, and the choice of the communication instrument. The assumption behind this test is that the public – or the specific stakeholders – has good ethical intuitions. If a PAO is able to ex-

32 Reichman, 2001
33 Brandts, Cooper, Weber, 2014

plain the decision taken in such a way that it passes the ethical scrutiny of the broad public intuition, in matter as well as in presentation, then the decision can count as ethical in a sense of prevailing within the general ethical dialogue. Note that this test is not about tricking the public into accepting a narrative or rationalization but about asking whether the reasoning of a PAO is attuned to the ethical intuitions of the stakeholders. Most day-to-day decisions can be made using this test.[34]

Furthermore, fundamental decisions might require more scrutiny. It comes in the form of the expert test.

– (12) Expert test: Can a PAO explain the decision to ethics experts? Is a PAO able to explain the decision to ethics experts and convince them that the decision is optimal under due constraints?

This second test presupposes the first. However, it deems necessary to deepen the logical coherence of the used arguments as well as their rationality. This test requires PAOs to examine the decision-making much more in-depth, to list and review arguments, to reflect critically about their consistence and coherence, as well as to second-guess ethical intuition. This test is to be applied when intuition alone does not guarantee a good outcome or when intuition might lead to a dubious result. This might be the case when intuition itself is biased or its suggested results are clearly contradictory to its aims.[35]

Final Remarks

The 12 guidelines form a practical framework for PAOs to perform their mission and duties while being aware of the ethical implications of military information and communication management as well as addressing the different stakeholders' stances. The guidelines cannot lead unilaterally to ethical behaviour, but they provide guidance on how PAOs could reflect ethics in decision-making, aiming especially at making military public affairs more effective.

However, these guidelines still warrant further research. On a practical level, they still have to be tested. Also, several other areas remain for further research, for example: If the management of the flow of information and communication, in short, the flow of knowledge, is understood as a multi-sided ethical dialogue, the differentiation in internal and external communications becomes obsolete. In today's context, all information diffused to the outside of a military organization can easily be turned into inside information and vice versa. Even if the aforementioned differentiation of stakeholder groups is conducted, it has to be acknowledged that information given to a specific group can be easily appropriated by a different group. This does not mean that the differentiation of stakeholder groups becomes unimportant; it means that it becomes more important to think about how disseminated information is reaching people.

If the management of the flow of information and communication, in short, the flow of knowledge, is understood as a multi-sided ethical dialogue, the differentiation in internal and external communications becomes obsolete.

In any case, military public affairs work in a triangle formed by their mission, the stakeholders' stances, and values. Navigating this triangle is a constant exercise in trading-off ethical desiderata. Furthermore, public affairs are a means for leadership and, as such, is subjected to ethical scrutiny. At the same time, by being committed to ethics, military public affairs have the potential to increase the credibility of an organization as a whole. Finally, exploring the ethical implications of PAO duties can advance resources that remain otherwise untapped. The practical framework to apply ethical thinking to their duties, especially guides PAOs in the trading off of ethical implications in decision-making.

References

– Bowen, S. A. (2008). A state of neglect: Public relations as "corporate conscience" or ethics counsel. *Journal of Public Relations Research, 20*(3), 271–296.
– Bowen, S. A. (2016). Values, Ethics, and Professionalism in Public Affairs. *The SAGE Handbook of International Corporate and Public Affairs,* 316–331.
– Brandts, J., Cooper, D. J., & Weber, R. A. (2014). Legitimacy, communication, and leadership in the turnaround game. *Management Science, 61*(11), 2627–2645.
– Burk, J. (2002). Theories of democratic civil-military relations. *Armed Forces & Society, 29*(1), 7–29.
– Darley, W. M. (2005). Why public affairs is not information operations. *Army Magazine,* 55(1), 9–10.
– Donnelly, J. (2013). *Universal human rights in theory and practice.* Ithaca: Cornell University Press.
– Eberwein, T., & Porlezza, C. (2016). Both Sides of the Story: Communication Ethics in Mediatized Worlds. *Journal of Communication, 66*(2), 328–342.
– Ferrell, O. C., & Fraedrich, J. (2015). *Business ethics: Ethical decision making & cases.* Toronto: Nelson Education.
– Ferrell, O. C. (2016). A framework for understanding organizational ethics. In *Business ethics: New challenges for business schools and corporate leaders* (pp. 15–29). New York: Routledge.
– Floridi, L., & Taddeo, M. (eds.). (2014). *The ethics of information warfare.* Cham: Springer Science & Business Media.
– Frederick, W. C. (1988). *Business and society: Corporate strategy, public policy, ethics.* New York: McGraw-Hill Companies.
– Freeman, R. E. & Reed, D. L. (1983). Stockholders and Stakeholders: A new perspective on Corporate Governance. *California Management Review,* 15(3), 88–106.
– Fukuyama, F. (1995). *Trust: The social virtues and the creation of prosperity.* Hoboken: Free Press Paperbacks.

34 Ferrell, Fraedrich, 2015
35 Ferrell, Fraedrich, 2015

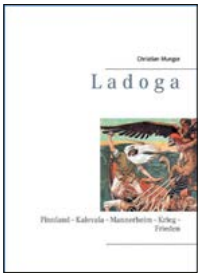
- Headley, J. M. (2016). *The Europeanization of the world: On the origins of human rights and democracy.* Princeton: Princeton University Press.
- Henry, N. (2015). *Public administration and public affairs.* New York: Routledge.
- Johannesen, R. L., Valde, K. S., & Whedbee, K. E. (2008). *Ethics in human communication.* Boston: Waveland Press.
- Karadag, H. (2017). Forcing the Common Good: The Significance of Public Diplomacy in Military Affairs. *Armed Forces & Society, 43*(1), 72–91.
- Luhmann, N. (1979). *Trust and power.* Chichester: Wiley.
- Meisenbach, R. J. (2017). Integrating Ethics and Responsibility Into Organizational Communication Research: Issues and New Directions. *Management Communication Quarterly, 31*(1), 146–152.
- NATO (2011). *Nato Military Public Affairs Policy.* MC 0457/2, February 2011.
- Ostrom, E. (1994). Constituting Social Capital and Collective Action. *Journal of Theoretical politics, 6*(4), 527–562.
- Parsons, P. J. (2016). *Ethics in public relations: A guide to best practice.* New York: Kogan Page Publishers.
- Pearson, R. (1989). Business ethics as communication ethics: Public relations practice and the idea of dialogue. *Public relations theory, 12*(2), 111–131.
- Plowman, K. D. (2017). Big strategy to little strategy: a multiple case analysis of public affairs planning. *Journal of Public Affairs, 17*(3), 1627–1636.
- Reichman, H. (2001). *Censorship and selection: Issues and answers for schools.* Philadelphia: American Library Association.
- Robinson, P., De Lee, N., & Carrick, D. (Eds.). (2008). *Ethics education in the military.* New Haven: Ashgate Publishing.
- Shapiro, J. P., & Stefkovich, J. A. (2016). *Ethical leadership and decision making in education: Applying theoretical perspectives to complex dilemmas.* New York: Routledge.
- Sunstein, C. R. (2016). *The ethics of influence: Government in the age of behavioral science.* Cambridge: Cambridge University Press.
- Toner, J. H. (2015). *Morals under the gun: The cardinal virtues, military ethics, and American society.* Lexington: University Press of Kentucky.
- Turilli, M., & Floridi, L. (2009). The ethics of information transparency. *Ethics and Information Technology, 11*(2), 105–112.
- Webster, F. (2014). *Theories of the information society.* New York: Routledge.

Henrique Schneider

Chief economist, Swiss Federation of Small and Medium-sized Enterprises. He also teaches economics at the Nordakademie (Germany) and the City University of Seattle (USA).

E-Mail: h.schneider@sgv-usam.ch

Ladoga.
Finnland – Kalevala – Mannerheim – Krieg – Frieden



Christian Munger

223 Seiten, BoD-Books on Demand, Norderstedt 2017, ISBN: 978-3-7431-8851-8

2017 hat Finnland mit einigem Aufwand, aber auch zurecht mit Stolz, seinen 100. Geburtstag als unabhängige Nation gefeiert. Christian Munger, der längere Zeit auch in Finnland gearbeitet hat, hat dies zum Anlass genommen, verschiedene interessante und auch erwähnenswerte Ereignisse und Episoden aus diesem für Finnland sehr prägenden Centenarium in lockerer Form aufzuzeigen. Dies unter anderem auch vor dem Hintergrund, dass gerade auch im Zusammenhang mit den einschneidenden Ereignissen in der jüngeren finnischen Geschichte und ihren tragenden Persönlichkeiten eine bis heute anhaltende schweizerische Affinität und auch Freundschaft zu Finnland besteht. Feldmarschall Carl Gustav von Mannerheim und sein aus dem bernischen Oberlangenegg stammende General Karl Lennart Oesch als Schlüsselfiguren Finnlands zumindest der ersten Hälfte des 20. Jahrhunderts stehen im Vordergrund der primär militärischen Freundschaftsaktivitäten zwischen den beiden Nationen. Dies wird auch unter dem «Mannerheim-Stipendium» laufende Austauschprogramm für schweizerische und finnische Stabsoffiziere bis heute gepflegt.

Mit der Zustimmung Lenins erklärte Finnland nach der erfolgreichen Oktoberrevolution in Russland am 6. Dezember 1917 seine Unabhängigkeit vom russischen Reich. Seit der Abtretung durch Schweden 1805 war Finnland ein Grossfürstentum im zaristischen Russland. Damit begann eine sehr wechselvolle Geschichte eines unabhängigen Staates mit einer langen gemeinsamen Grenze zur neu geschaffenen und sich über die Zeit in blutigen Auseinandersetzung konsolidierenden Sowjetunion. Dieser Übergang erfolgte aber alles andere als friktionslos, zumal sich in den Garnisonen auf finnischem Territorium noch zahlreiche russische Einheiten befanden, die sich teilweise der neuen Führung der Bolschewiken anschlossen. Damit begann die erste Phase des finnischen Befreiungskampf 1917–1919. Die Schlüsselfigur auf finnischer Seite war hierbei der bis zur finnischen Unabhängigkeitserklärung in zaristischen Diensten stehende General Carl Gustav von Mannerheim.

Sowohl in dieser ersten Phase wie insbesondere dann auch im Kampf gegen die Rote Armee während des Winterkriegs 1939–1940 und seiner Fortsetzung 1941–1944 gelang es den finnischen Streitkräften unter der Führung Mannerheims unter enormen Anstrengungen und unter sehr harten Bedingungen, das Gros des finnischen Territoriums zu verteidigen. Im vorliegenden Werk werden gerade auch zu einzelnen bisher wenig bekannte Teilaspekte der Kampfführung aufgezeigt, die die Herausforderungen an die beteiligten Soldaten und Offiziere erahnen lässt.

In der nur summarisch dargestellten letzten grossen Offensive der Roten Armee nach der Sprengung der Umklammerung von Leningrad im Sommer 1944 kommt dann auch insbesondere der für die finnischen Operationen verantwortliche Generalleutnant Karl Lennart Oesch zum Tragen. Unter seiner Führung gelang es, die überlegenen Sowjetkräfte an der sogenannten «Mannerheimlinie» zu stoppen und damit die von Stalin geforderte Einnahme Helsinkis zu verhindern. In Finnland wurde dieser harterkämpfte Erfolg für sehr lange Zeit primär Mannerheim zugeordnet, zumal Oesch auf sowjetischen Druck vor ein Kriegsverbrechertribunal gestellt und verurteilt worden war. Seine Rehabilitierung erfolgte erst viel später.

Christian Munter kommt das Verdienst zu, eigene Erfahrungen und Erkenntnisse zur bewegten Geschichte, zur besonderen Kultur und zu weiteren Besonderheiten Finnlands in gut lesbarer Form nachzuzeichnen. Er möchte damit insbesondere Generationen erreichen, welche keinen direkten Bezug zur ersten Hälfte des unabhängigen finnischen Centenariums haben. Die anekdotische Form erleichtert wohl die Lesbarkeit, lässt aber gleichzeitig auch den Fluss der Eindrücke und Informationen unterbrechen, zumal die inhaltlichen Sprünge von einem zum anderen Thema manchmal etwas gar abrupt erfolgen. Zudem weist die Sprache einige Unebenheiten aus, was vermutlich auch der engagierten persönlichen Auseinandersetzung des Autors mit einer ihm am Herzen liegenden Materie geschuldet ist. Dennoch kann dieses handliche Werk dem interessierten Leser für Schlüsselereignisse und -entwicklungen der finnischen Geschichte in der ersten Hälfte des 20. Jahrhunderts und besonders des immer wieder beeindruckenden Freiheitskampfs des finnischen Volkes dieser Zeit empfohlen werden.

GEU

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. 2/2018 80.024d 11.2018 18700