Herausgeber: Chef der Armee

Nr. 1 / 2017
Beilage zur ASMZ 6 / 17 und RMS 3 / 17

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:
Divisionär Urs Gerber
EDA-Kuriersektion
Panmunjom – Korea
3003 Bern
Tel. +82 503 334 83 07
E-Mail: urs.gerber@vtg.admin.ch

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

SIPOL-B 16: Ein Bedrohungsbericht, keine neue Strategiekonzeption 6

Andreas Wenger, Christian Nünlist

Trends in der Logistik machen vor der Logistikbasis der Armee nicht Halt 20

Thomas Kaiser, Emanuel von Wartburg

Resilienz – eine Bestandsaufnahme 24

Hubert Annen

Pour une approche économique de la cybersécurité 36

Marcus M. Keupp, Alain Mermoud, Dimitri Percia David

La quatrième révolution industrielle et son impact sur les forces armées 50

Marc-André Ryter

Buchbesprechungen 63

Titelbild Die technologische Entwicklung beeinflusst auch die Schweizer Armee erheblich. (VBS/DDPS)

Vorwort

Geschätzte Leserinnen und Leser der Military Power Revue

Die Armee ist zwar immer noch das wichtigste Instrument zur Verteidigung unseres Landes. Verteidigt wird aber längst nicht mehr nur mit Kanonen. Vielmehr geht es bei der Verteidigung darum, Gefahren vorzubeugen, Informationen zu beschaffen, dem Terrorismus die Stirn zu bieten und die Integrität unserer Informationssysteme wirksam zu schützen, während es gleichzeitig immer häufiger zu Cyberattacken kommt.

Apropos Cyberattacken: Das Departement, dem vorzustehen ich die Ehre habe, führt mit modernen Mitteln einen harten Kampf gegen dieses Phänomen, das in den Bereichen Wirtschaft und Sicherheit einen Schaden in Milliardenhöhe verursacht. Dabei müssen wir uns bewusst sein, dass wir nur dann etwas erreichen, wenn wir international und bereichsübergreifend zusammenarbeiten. Dafür setzen wir uns aktiv ein.

Verteidigung bedeutet heute auch funktionierende Kooperationen auf allen Stufen, bedeutet, sich jederzeit bereitzuhalten, um zivile Behörden zu unterstützen, sei es bei Naturkatastrophen, im Fall von Migrationsströmen oder bei der Durchführung von internationalen Konferenzen wie dem World Economic Forum WEF.

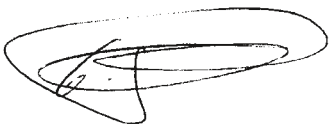
Wie man sieht, hat der Begriff der Verteidigung heute mehrere Bedeutungen. Je nachdem werden andere Kompetenzen verlangt; in den allermeisten Fällen sind Spezialwissen oder besondere Fähigkeiten gefragt, um die Herausforderungen, die weit über den rein militärischen Rahmen hinausgehen, zu meistern. Gleichzeitig werden die Bundesfinanzen einer strengen Abmagerungskur unterzogen.

Kurz: Wir müssen mit weniger Mitteln mehr leisten. Die Verteidigung der Schweiz muss – auch wenn die Anhängerinnen und Anhänger einer konventionellen Armee dies nicht unbedingt gerne hören – sowohl in qualitativer wie auch in quantitativer Hinsicht justiert werden. Und genau das erreichen wir mit der Weiterentwicklung der Armee, der WEA.

Mit der WEA verbessern wir die Ausbildung der Angehörigen der Armee, die Ausrüstung sowie die Bereitschaft. Zudem verstärkt die WEA die Verbundenheit der Armee mit den einzelnen Regionen unseres Landes.

Dass dies gelingt, ist mir persönlich ein grosses Anliegen. Unser Milizsystem hat gezeigt, dass es funktioniert, und die Verteidigung unseres Landes soll ein Gemeinschaftswerk bleiben. Übrigens interessieren sich auch zahlreiche andere Verteidigungsminister für das System des Milizsoldaten, und zwar nicht, weil es so aussergewöhnlich wäre, sondern weil es dazu beiträgt, dass sich die Bürger dieses Landes, unabhängig vom Alter, vom Beruf, von der Herkunft oder der sozialen Stellung einem gemeinsamen Ziel verschreiben. Der Grundsatz der Militärdienstpflicht geht einher mit einem hohen Engagement zugunsten des Vaterlands. Dieses Engagement bildet sozusagen das Rückgrat des Systems. Und nur auf dieser Grundlage ist der Zusammenhalt gewährleistet.

Dies gilt umso mehr zu Beginn einer Reform, die die Armee auf einen Sollbestand von 100 000 Mann reduziert, um die Ausbildung und das Engagement der Truppe zu verbessern. Dank den neuen Rahmenbedingungen wird die Armee nicht nur in ihrer Multifunktionalität gestärkt, sondern sie ist auch rascher einsatzbereit. Sie wird somit in der Lage sein, die eben erwähnten Gefahren in all ihren Facetten wirksam zu bekämpfen.



Chef VBS
Bundesrat Guy Parmelin

Vorwort

Geschätzte Leserinnen und Leser der Military Power Revue

«Le chef, c'est celui qui a besoin des autres» – dieses Zitat des französischen Lyrikers und Philosophen Paul Valéry trifft es für mich auf den Punkt. Erfolg in der Armee basiert immer auf Teamwork. Alleine erreicht niemand etwas. Oder anders gesagt: Es ist mir egal, wer das Tor schiesst. Wichtig ist, dass wir zusammen reüssieren.

Punkto der anstehenden Herausforderungen habe ich vier Schwerpunkte definiert.

Erstens: Alimentierung. Wir brauchen jedes Jahr 18 000 Rekruten, welche die RS bestehen und dann in einen Verband eingeteilt werden. Dafür müssen wir insbesondere die Drop-out-Quote während der ersten Wochen der Rekrutenschulen reduzieren. Fakt ist aber auch, dass wir zu viele Leuten an den Zivildienst verlieren. 2016 waren es über 6000, und es ist davon auszugehen, dass diese Zahl weiter ansteigt. Allfällige Korrekturmassnahmen sind Sache der Politik. Wir müssen aber ehrlich sein: Der Zivildienst ist kein Ersatzdienst für die Sicherheit der Schweiz. Sicherheit wird einzig durch den Dienst in der Armee produziert.

Wir brauchen aber auch 9150 Full Time Equivalents im Departementsbereich Verteidigung, um die anstehenden Arbeiten zu bewältigen. Sind es weniger, kann die Armee die geforderten Leistungen nicht erbringen.

Zweitens: Ressourcierung. Wir brauchen die vom Parlament gesprochenen 5 Milliarden Franken respektive 20 Milliarden Franken in einem Vier-Jahres-Finanzrahmen. Und wir brauchen die damit verbundene Planungssicherheit. Mit weniger Geld sind die nötigen Investitionen nicht machbar. Und es ist zwingend, dass wir investieren können. Eine nur lückenhaft ausgerüstete Armee ist keine ehrliche Lösung. Unsere Soldaten haben das Anrecht auf eine vollständige Ausrüstung.

Zwischen 2025 und 2030 drohen uns strategische Lücken bei unseren Hauptsystemen. Der anstehende Ersatz der Hauptsysteme zwischen 2025 und 2030 ist mit 5 Milliarden pro Jahr nicht zu machen. Das hat im Übrigen auch der Gesamtbundesrat erkannt. Dreh- und Angelpunkt bei allen Beschaffungsvorhaben ist das neue Kampfflugzeug. Schon heute ist aber klar: Falls das Parlament Nein sagt zur Nutzungsverlängerung der F/A-18, dann haben wir ab 2026 keine Luftwaffe mehr.

Drittens: Leistungsprofil. Zum ersten Mal in der Geschichte unserer Milizarmee ist genau definiert, was die Armee können muss. Die Politik hat sozusagen einen operativen Vertrag mit der Armee abgeschlossen. Wir wissen ganz genau, was von uns erwartet wird. Das Leistungsprofil kann man auch als «operationellen Vertrag» bezeichnen. Seit 1848 wird damit zum ersten Mal festgehalten, welche Leistungen die Armee wie rasch und wie lange erbringen muss.

Konkret wollen wir innert drei Tagen 8000 Mann und innert 10 Tagen bis zu 35 000 Mann einsetzen können – das ist eine Leistung, die heute keine einzige Armee in Europa erbringen kann. Auch wir können es aber heute nicht – wir benötigen 3 Monate, um die Leistungskraft von 15 000 AdA auf den Boden zu bringen.

Viertens: Respektierung. Wir alle müssen unseren Angehörigen der Armee den nötigen Respekt entgegen bringen. Die Armee besteht aus unseren Vätern, Brüdern, Söhnen, Ehemännern und Freunden. Und sie besteht aus unseren Müttern, Schwestern, Töchtern, Ehefrauen und Freundinnen. Sie alle setzen sich ein für die Sicherheit von Land und Leuten. Im äussersten Fall tun sie das mit ihrem eigenen Leben.

Dafür haben die Angehörigen der Armee den Respekt von uns allen verdient.

Wir alle zusammen müssen jetzt die Weiterentwicklung der Armee umsetzen. Im Rahmen dieser Umsetzung werden wir auch Dinge korrigieren müssen, verbessern müssen, aber das entspricht zu 100 % den militärischen Führungstätigkeiten. Bei uns heisst das «Revision der Pläne».

Meine Botschaft an Sie ist diesbezüglich ganz einfach: Machen wir es. Faisons-le. Facciamolo. Just do it.

Chef der Armee
KKdt Philippe Rebord

Editorial

**Sehr geehrte Leserinnen und Leser
der Military Power Review**

An dieser Stelle freut es mich besonders, Commandant de Corps Philippe Rebord als neuen Herausgeber der Military Power Revue (MPR) zu begrüssen. Er stellt sich voll und ganz hinter seine Publikation und freut sich auf kompetente und interessante Beiträge, die insbesondere auch die sicherheitspolitische und militärische Diskussion anregen.

Wenn man die derzeitige Lageentwicklung auf praktisch allen relevanten Ebenen analysiert, stellt man fest, dass Unberechenbarkeit und Überraschung nicht nur zu einem ständigen Begleiter in der täglichen Bewältigung sicherheitspolitischer und militärischer Herausforderungen geworden sind, sondern derzeit die Agenda vor allem international und global zu diktieren scheinen. Vielerorts, leider aber vor allem an den globalen Hot Spots wie im Nahen und Mittleren Osten oder rund um die Koreanische Halbinsel, herrscht der Drang vor, den bisher als unlösbar geltenden Gordischen Knoten mit einem (militärischen) Schlag lösen zu wollen. Dabei wird teilweise offen zu Unberechenbarkeit und Überraschung als wesentliches Element dieser Art von Konfliktmanagement zurückgegriffen. Man mag dies bedauern oder gar verurteilen. Angesichts der Tatsache, dass dieser Ansatz auch von globalen Schlüsselakteuren bewusst angewandt oder zumindest angedroht wird, dürfte nur eine möglichst kontinuierliche und trotzdem flexible sowie insbesondere vorausschauende Lagebeurteilung für ein erfolgreiches Krisen- und Konfliktmanagement zielführend sein.

Die vorliegende Ausgabe widmet sich verschiedenen Aspekten künftiger Herausforderungen, die auch die Schweizer Armee bereits mehr oder weniger erfasst haben. Dabei spielt ohne Zweifel der Sicherheitspolitische Bericht 2016 als politisches Rahmeninstrument eine wichtige Rolle. Der Bericht und seine Folgerungen werden einer kritisch-konstruktiven Bewertung unterzogen. Dabei wird festgestellt, dass eine solide und umfassende Lagedarstellung vorliegt, der aber bewusst oder gewollt kein neues Strategiekonzept im Sinne von Folgerungen und Konsequenzen angefügt worden ist. Vor dem Hintergrund der erst anlaufenden Umsetzung der WEA erscheint dies insgesamt zum jetzigen Zeitpunkt nachvollziehbar, darf aber nicht aus den Augen verloren werden.

Auch die Logistik wird mit den sich abzeichnenden künftigen Entwicklungen und Herausforderungen betroffen werden. Sowohl die Prozesse, die entsprechende Infrastruktur wie insbesondere auch die Anforderungen an die Mitarbeitenden sind einem unaufhaltsamen Wandel unterworfen, der sich in Zukunft noch akzentuieren dürfte. Vor diesem Hintergrund ist der Chef LBA konstant in der täglichen und zeitgerechten Leistungserbringung wie gleichzeitig in der Antizipation relevanter Trends der Zukunft gefordert.

Aktuelle und künftige Bedrohungen haben direkt oder indirekt zunehmend Auswirkungen auf die Widerstandsfähigkeit oder Resilienz des Individuums. Die Angehörigen der Armee aller Stufen werden hier ganz besonders gefordert. Was in anderen Kulturen und Streitkräften gerade aufgrund entsprechender Erfahrungen bereits in signifikantem Masse ins Bewusstsein aufgenommen worden ist, befindet sich in der Schweizer Armee noch im Anfangsstadium. Neben körperlicher ist auch geistige Widerstandsfähigkeit ein entscheidendes Attribut zur angemessenen Reaktion und letztlich erfolgreichen Aufgabenerfüllung. Die vorliegende Bestandesaufnahme soll diese Herausforderungen hier einem breiteren Publikum bewusst machen und Ansätze zur Schulung und Krisenbewältigung aufzeigen.

Die zunehmend komplexere und globale Vernetzung schafft zwar enorme Anwendungsmöglichkeiten und kann zur signifikanten Erhöhung von kritischen Fähigkeiten und Lösungsansätzen beitragen. In dieser Cyber-Sphäre eröffnen sich bei jeder neuen Möglichkeit auch gleich neue Verletzlichkeiten und Angriffsflächen, die nach Schutz- und Sicherheitssysteme sowie –mechanismen verlangen. Der vorliegende Beitrag versucht in diesem Spannungsfeld, wirtschaftlich pragmatische und trotzdem tragbare Ansätze aufzuzeigen, welche letztlich auf einem ausreichenden Mass an Vertrauen basieren.

Die vierte industrielle Revolution ist eines der Schlagworte der laufenden Diskussion bezüglich der künftigen Ausrichtungen von Streitkräften. Fachmagazine und Hochglanzbroschüren sind voll von verlockenden Möglichkeiten zur Lösung komplexer Aufgaben, insbesondere auch mit dem Ziel, Überraschungen wie auch Verluste an der wichtigsten Ressource, dem eingesetzten Personal, zu minimieren. Diese schon fast uferlosen Möglichkeiten im Lichte der sich immer rascher entwickelnden Technologien und militärischen Anwendungsfeldern können dazu verleiten, bei der Weiterentwicklung der Streitkräfte den Fokus auf das Wesentliche aus den Augen zu verlieren. Der Beitrag in dieser Nummer versucht, diese Möglichkeiten in einen «helvetisch realistischen» Kontext zu stellen.

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

Mit freundlichen Grüssen
Der Chefredaktor der Military Power Revue

Divisionär Urs Gerber

SIPOL-B 16: Ein Bedrohungsbericht, keine neue Strategiekonzeption

Im August 2016 verabschiedete der Bundesrat einen neuen Bericht über die Sicherheitspolitik der Schweiz. Die fünfte Gesamtschau seit 1973 konzentriert sich auf eine robuste, detailkundige Lageanalyse. Für eine strategische Weiterentwicklung der zentralen sicherheitspolitischen Instrumente bietet der Bericht jedoch nur begrenzt eine Orientierungshilfe. Die entscheidende konzeptionelle Innovation besteht aus einer Erweiterung des Verteidigungsbegriffs. Die Einführung der Begriffstriade «Selbständigkeit – Kooperation – Engagement» trägt hingegen wenig zur Klärung auf die Zukunft gerichteter strategischer Prioritäten der Schweiz bei.

Andreas Wenger, Christian Nünlist

Einleitung

Am 24. August 2016 hat der Bundesrat einen neuen Bericht über die Sicherheitspolitik der Schweiz verabschiedet.[1] Es handelt sich dabei um die erst fünfte Gesamtkonzeption der Schweiz nach den sicherheitspolitischen Berichten von 1973, 1990, 1999 und 2010.[2] Der erste Bericht, der *Bericht 73,* hatte die Sicherheitspolitik der Schweiz 1973 angesichts der einsetzenden Entspannungsperiode im Kalten Krieg neu ausgerichtet und die militärische Landesverteidigung um einen zu stärkenden aussenpolitischen Pfeiler ergänzt. Nach der Epochenwende von 1989/90 plädierte der *Bericht 2000* im Jahre 1999 für einen Ausbau und eine Vertiefung der internationalen Sicherheitszusammenarbeit. Das Leitmotiv «Sicherheit durch Kooperation»[3] empfahl sich dabei als Mittelweg zwischen Autonomie und Integration. Der *Bericht 2010* schliesslich fokussierte die Reorientierung der Armee weg von internationaler Friedensförderung zurück zu Einsätzen im eigenen Land.[4] Er leitete die Neuausrichtung der Schweizer Armee ein, die nun 2016 mit der expliziten Erweiterung des Verteidigungsbegriffs – eine der wenigen konzeptionellen Neuerungen im *Bericht 2016* – eine lange Debatte abgeschlossen hat.

Der *Bericht 2016* hat sich verzögert: Ursprünglich hatte der Bundesrat das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) im Mai 2013 beauftragt, einen neuen sicherheitspolitischen Bericht «bis Ende 2014» auszuarbeiten. Der Bericht sollte das Umfeld der Schweiz analysieren und einen «starken Fokus auf die Analyse der Bedrohungen und Gefahren für die Schweiz legen».[5] Eine parlamentarische Initiative hatte bereits im Juni 2006 gefordert, den traditionellen Publikationsrhythmus von rund zehn Jahren zu beschleunigen.[6] Der Bundesrat erklärte sich 2008 bereit, dem Parlament künftig «Mitte jeder Legislaturperiode» einen solchen Bericht vorzulegen.[7]

Aufgrund von Verzögerungen bei noch laufenden Umsetzungsarbeiten aus dem *Bericht 2010* beschloss der Bundesrat im August 2014, dass ein neuer Bericht erst 2016 erscheinen würde. Es ging ihm darum, in den politischen Diskussionen zur Weiterentwicklung der Armee (WEA) Missverständnisse zu vermeiden. Während es dort um «die kurz- bis mittelfristige Ausrichtung der Armee» ging, so argumentierte der Bundesrat, sollte die Armee vom nächsten sicherheitspolitischen Bericht «Impulse für die Zeit nach 2020» erhalten. Diese beiden Diskussionen sollten getrennt geführt und bei der WEA-Debatte eine strategische Grundsatzdiskussion vermieden werden.[8]

1 Bundesrat, *Bericht,* «Die Sicherheitspolitik der Schweiz» (im Folgenden abgekürzt mit SIPOL-B 16), 24.8.2016.
2 Zudem war am 3.12.1979 aufgrund eines parlamentarischen Vorstosses ein «Zwischenbericht zur Sicherheitspolitik» erschienen. Der Bundesrat nahm darin keine fundamentale Neueinschätzung der Lage vor, wenngleich er wirtschaftliche Abhängigkeiten sowie Spionage, Terrorismus und Subversion stärker gewichtete. Vgl. Kurt R. Spillmann et al., *Schweizer Sicherheitspolitik seit 1945* (Zürich: NZZ, 2001), 135ff.
3 Das dem Bericht 2000 den Titel verleihende griffige Motto «Sicherheit durch Kooperation» wurde bereits im Aussenpolitischen Bericht 1993 im Anhang über die Neutralität erwähnt: «Die traditionelle Formel von ‹Sicherheit durch Neutralität und Unabhängigkeit› wird mehr und mehr ergänzt werden müssen durch diejenige von ‹Sicherheit durch Kooperation›». Bundesrat, *Bericht zur Neutralität: Anhang zum Bericht über die Aussenpolitik der Schweiz in den 90er Jahren,* 29.11.1993, 15.
4 Vgl. Christian Nünlist, «Swiss Security Policy after 2014», in: *European Security & Defence* 3 – 4 (2015), 18 – 21.
5 VBS, *Pressemitteilung,* «Neuer Bericht über die Sicherheitspolitik der Schweiz», 1.5.2013.
6 *Parlamentarische Initiative 06.447* (SVP), «Strategiebericht als Grundlage der Sicherheitspolitik der Schweiz», 23.6.2006.
7 Bundesrat, *Stellungnahme zur parlamentarischen Initiative 06.447,* 2.7.2008.
8 VBS, *Pressemitteilung,* «Bericht über die Sicherheitspolitik erscheint 2016», 27.8.2014.

Gleichzeitig stieg aufgrund des sich rasant wandelnden internationalen Umfelds der Bedarf nach einer neuen Orientierungshilfe. Die nukleare Katastrophe von Fukushima, die arabischen Rebellionen in Nordafrika, der Syrien-Krieg und das Anschwellen der Flüchtlings- und Migrationsbewegungen, der Aufstieg des Islamischen Staates und des dschihadistischen Terrorismus in Europa sowie die russische Annexion der Krim und die Kämpfe in der Ostukraine – die Vielzahl an neuen Krisen und Konflikten im Osten und Süden der Schweiz verlangte nach einer neuen Analyse der sich veränderten Bedrohungs- und Gefahrenlage und der allfälligen Konsequenzen für die Ausrichtung der Schweizer Sicherheitspolitik und ihrer Instrumente.

Im Gegensatz zu den Bruchlinien zwischen dem VBS und dem EDA 2010,[9] welche die mangelnde konzeptuelle und operationelle Verzahnung der Aussen- und Sicherheitspolitik widerspiegelt hatten,[10] funktionierte dieses Mal der Konsultations- und Kooperationsprozess in der interdepartementalen Arbeitsgruppe mit breiter Einbindung der Kantone praktisch reibungslos. Grundsätzlich wurde der Entwurf des Berichts vom Oktober 2015 in der Vernehmlassungsphase im Winter 2015/16 von den Kantonen, Parteien und Organisationen positiv aufgenommen.[11]

Er bietet eine umfassende Aufarbeitung der Entwicklungen im regionalen und globalen Umfeld der Schweiz und verdichtet diese zu drei zentralen Trends.

Inhaltlich konzentriert sich der *Bericht 2016* auf eine robuste Lageanalyse. Er bietet eine umfassende Aufarbeitung der Entwicklungen im regionalen und globalen Umfeld der Schweiz und verdichtet diese zu drei zentralen Trends. Er diskutiert die damit verbundenen für die Schweiz relevanten sicherheitspolitischen Bedrohungen und Gefahren. Der Charakter moderner Bedrohungen wird dabei sehr gut herausgearbeitet. Bezüglich des Zusammenwirkens der sicherheitspolitischen Instrumente bei der Prävention, Abwehr und Bewältigung bietet der Bericht zum ersten Mal eine integrale und gewichtete Darstellung der konkreten Beiträge aller sicherheitspolitischen Instrumente für jedes Bedrohungsbündel.

Er liefert nur begrenzt Orientierung im Sinne der politisch-konzeptionellen Steuerung und damit verbundener Konsequenzen und Anpassungen auf der Ebene der sicherheitspolitischen Instrumente.

Hingegen bietet der *Bericht 2016* nur wenig neue Leitlinien hinsichtlich der Weiterentwicklung der sicherheitspolitischen Strategie und der sicherheitspolitischen Instrumente. Er liefert nur begrenzt Orientierung im Sinne der politisch-konzeptionellen Steuerung und damit verbundener Konsequenzen und Anpassungen auf der Ebene der sicherheitspolitischen Instrumente. Er hat vielmehr den Charakter einer Auslegeordnung bestehender Massnahmen und einer Nachschreibung der Entwicklungen in den jeweiligen Bereichen.

Gesamtbewertung: Konzeptioneller Status quo

Noch nie ist ein sicherheitspolitischer Bericht des Bundesrats in der Schweizer Öffentlichkeit so dünn rezipiert worden wie der *Bericht 2016* zur Sicherheitspolitik der Schweiz.[12] Das Interesse der Medien war womöglich auch deshalb gering, weil es sich primär um einen Bedrohungsbericht handelt, der die wichtigsten Entwicklungen im Umfeld der Schweiz seit 2010 analysiert – nicht aber um eine Strategiekonzeption, welche im Kontext strittiger politischer Richtungsfragen Orientierungslinien für eine Neuausrichtung der Schweizer Sicherheitsstrategie und die Weiterentwicklung ihrer zentralen Instrumente bieten würde.

Während der Erarbeitung und Überarbeitung des neuen Berichts wurde die Sicherheitspolitik der Schweiz im Lichte des Bedrohungswandels diskutiert und auch kritisch hinterfragt – für eine Demokratie ein gesunder Legitimationsprozess einer bürgernahen Sicherheitspolitik.

Damit ging leider auch ein positiver Nebeneffekt der Ausarbeitung des *Berichts 2016* unter: Denn der langwierige Prozess bot über Jahre eine Plattform für einen strukturierten Austausch mit dem Parlament, den politischen Parteien, den Kantonen und weiteren interessierten Organisationen. Während der Erarbeitung und Überarbeitung des neuen Berichts wurde die Sicherheitspolitik der Schweiz im Lichte des Bedrohungswandels diskutiert und auch kritisch hinterfragt – für eine Demokratie ein gesunder Legitimationsprozess einer bürgernahen Sicherheitspolitik.

Im Unterschied zu früheren Berichten enthält der *Bericht 2016* keinen politischen Richtungsentscheid. Er beginnt vielmehr mit der zentralen Feststellung, dass auf der Ebene der wichtigsten sicherheitspolitischen Instrumente – Armee, Aussenpolitik, Bevölkerungsschutz – derzeit noch zahlreiche Reformprojekte am Laufen seien, welche die Phase einer politisch-konzeptionellen Steuerung bereits durchschritten hätten. Deren Umsetzung sollte nicht durch neue strategische Leitlinien verkompliziert oder gefährdet werden.

9 Zu den Querelen zwischen EDA und VBS, vgl. «Calmy-Rey attackiert Maurer», in: *Neue Zürcher Zeitung* (NZZ), 2.8.2009; «Maurer widersetzt sich Vorgaben», in: NZZ, 21.3.2010.

10 Vgl. Andreas Wenger/Christian Nünlist, «Aufwertung der sicherheitspolitischen Beiträge der Schweizer Aussenpolitik», in: *Bulletin zur schweizerischen Sicherheitspolitik* (2016), 19–47.

11 VBS, *Ergebnisbericht*, «Vernehmlassung zum Bericht des Bundesrates über die Sicherheitspolitik der Schweiz», 28.4.2016.

12 Löbliche Ausnahmen sind Stefan Schmid, «Ueli Maurer sieht Flüchtlinge nicht als Sicherheitsrisiko», in: *Nordwestschweiz*, 12.11.2015, ders., «Neutralität als Hindernis?», in: *Nordwestschweiz*, 12.11.2015; Bruno Lezzi, «Wenig griffige Strategie», in: NZZ, 30.12.2015; Jan Flückiger, «Gefahren lauern beim Terrorismus und im Cyberspace», in: NZZ, 24.8.2016.

Abbildung 1 Die Cyber Bedrohung in einer Real Time Aufnahme. (Kapersky Real Time Map)

Abbildung 2 Der Djihadismus ist zur globalen Herausforderung geworden. (a2larm.cz)

Die verhaltene, aber grundsätzlich positive Aufnahme des *Berichts 2016* – ganz im Gegensatz zur überwiegend negativen Reaktion auf den *Bericht 2010* – sollte allerdings nicht dahin gehend interpretiert werden, dass seither eine Überwindung der politischen Blockade hinsichtlich des Spannungsfelds zwischen Neutralität und Öffnung respektive zwischen Selbständigkeit und internationaler Kooperation erzielt worden ist. Die Vernehmlassung zum *Bericht 2016* hat vielmehr deutlich gemacht, dass bei den politischen Parteien hinsichtlich sicherheitspolitischer Rollenbilder nach wie vor kein Konsens besteht. Bei der vorgeschlagenen Strategie-Triade kritisierten BDP, FDP und SP den Kernbegriff der Selbständigkeit, während die SVP zu starke Kooperation und internationales Engagement ablehnte.[13]

Die Hauptleistung des Berichts stellt die Lageanalyse mit einer ausführlichen Umfeldanalyse und einem konzisen Überblick über die für die Schweiz relevanten Bedrohungen und Gefahren dar, die in drei Schritten erarbeitet worden ist. Ausgangspunkt bildeten erstens die Anhörungen, die im Herbst 2013 mit dreizehn Experten aus dem In- und Ausland durchgeführt wurden und deren Gedanken in den Bericht einflossen – auch wenn sowohl die Ukraine-Krise als auch die Ausbreitung des Islamischen Staates damals noch nicht absehbar gewesen waren.[14]

Teilweise wurde der entstehende Bericht aber *zweitens* auch von aktuellen Entwicklungen geprägt. Die Vernehmlassung konzentrierte sich etwa auf die sich 2015 zuspitzende Flüchtlings- und Migrationskrise, deren Zusammenhang mit der Sicherheitspolitik für die Endfassung des Berichts noch einmal überarbeitet wurde. Im Zuge der parlamentarischen Beratungen wiederum verschob sich der Diskussions- und Informationsbedarf im Winter 2016/17 auf die sicherheitspolitischen Folgen des «Brexit» und der Wahl von US-Präsident Donald Trump für Europa und die Schweiz.[15]

Drittens bietet der Bericht eine vertiefte Darstellung der sicherheitspolitischen Zusammenarbeit im regionalen Umfeld der Schweiz. Mit diesem Schwerpunkt nimmt er Bezug auf ein Postulat der sicherheitspolitischen Kommission des Ständerates aus dem Jahre 2011, das vom Bundesrat strategische Überlegungen hinsichtlich einer verstärkten Mitwirkung der Schweiz bei der europäischen Sicherheitsarchitektur eingefordert hatte.[16]

Gerade die Beschreibung der sicherheitspolitischen Kooperation in Europa wirkt jedoch im Bericht wie ein Fremdkörper, da später kein expliziter Bezug mehr dazu genommen wird, der deutlich machen würde, inwieweit und mit welcher Priorität die skizzierten Möglichkeiten zur verstärkten Mitwirkung (etwa in der OSZE, mit der NATO, im Bereich Schengen oder in der militärischen Friedensförderung) in den kommenden Jahren umgesetzt werden sollen.

Inhaltliche Stärken: Bedrohungen und das Zusammenspiel der Instrumente

Bedrohungskonzepte sind zentral für sicherheitspolitischen Debatten und für sicherheitspolitisches Handeln. In der Form aktueller Schlüsselereignissen und informeller Gefahrenlisten prägen sie das sicherheitspolitische Meinungsbild und die Bedrohungsdebatte in der breiteren Öffentlichkeit.[17] In konsolidierter Form, wie im *Bericht 2016* innovativ in eine Typologie von sechs Bedrohungsbündeln verdichtet, sind sie konstitutiv für jede Sicherheitsstrategie. Bedrohungskonzepte signalisieren, «was wie bedroht ist», und Strategien definieren, «wer dies wie schützen» soll. Grundsätzlich definieren nationale Sicherheitsstrategien den Handlungsrahmen für die künftige Umsetzung der Sicherheitspolitik. Die «Ziel-Wege-Mittel»-Steuerungslogik kollidiert und konkurriert in der Praxis allerdings immer mit einer Reihe politischer, bürokratischer, institutioneller und individueller Logiken, die dieser Steuerungslogik entgegenstehen und ihr Grenzen setzen.[18]

Der Bericht 2016 stellt einen Kompromiss zwischen diesen unterschiedlichen Logiken dar. Einerseits orientiert er sich explizit an der beschriebenen Steuerungslogik und skizziert als Ziel die Überprüfung des Zusammenhangs zwischen Bedrohungsanalyse und Anpassungsbedarf bei den sicherheitspolitischen Instrumenten.[19] Auch die Diskussion der Mittel reflektiert den Zusammenhang zwischen dem konzeptuell als relevant angesehenen Bedrohungsspektrum und den Beiträgen, der Ausrichtung und dem Zusammenwirken der sicherheitspolitischen Mittel. Andererseits verweist der Bericht hinsichtlich des Anpassungsbedarfs auf bereits laufende Reformprojekte und in den letzten Jahren erarbeitete Teilstrategien. Damit relativiert der Bundesrat den Anspruch, einen auf die Zukunft gerichteten Handlungsrahmen vorzulegen und neue Akzente zu setzen, von Beginn an bereits deutlich. Zwar stellt er einen markanten Wandel des Umfeldes der Schweiz und der für die Schweiz relevanten Gefahren fest. Hinsichtlich des damit verbundenen Anpassungsbedarfs belässt er es jedoch mehrheitlich beim Hinweis auf bereits eingeleitete Projekte und Massnahmen.

Die «Ziel-Wege-Mittel»-Steuerungslogik kollidiert und konkurriert in der Praxis allerdings immer mit einer Reihe politischer, bürokratischer, institutioneller und individueller Logiken, die dieser Steuerungslogik entgegenstehen und ihr Grenzen setzen.

13 VBS, Ergebnisbericht, op. cit., 4.

14 Bei den 13 Experten handelte es sich um Lars Nicander, Julian Harston, Emmanuel Kwesi Aning, François Heisbourg, David Omand, Alexander Golts, Karl-Heinz Kamp, Andreas Wenger, K.C. Sing, Mohammad-Mahmoud Ould Mohamedou, Mu Changlin, Catherine Kelleher und Alexander Klimburg. Das VBS hat diese Expertenbeiträge 2015 veröffentlicht.

15 SDA, «Debatte im Ständerat», 3.3.2017. Das VBS hatte am 16.12.2016 auf Verlangen der Sicherheitspolitischen Kommission des Ständerats einen fünfseitigen Zusatzbericht nachgereicht, in dem unter anderem auf die Risiken und Chancen des Brexit und einer allfälligen Reduktion des transatlantischen Engagements der USA unter Trump für die Schweizer Sicherheitspolitik eingegangen wurde. Das VBS empfahl darin aufgrund der Werte der Schweiz Distanz zu Russland. Stattdessen solle das sicherheitspolitische Verhältnis zu Westeuropa und zur NATO aufrechterhalten, aber nicht intensiviert werden.

16 *Postulat 11.3469*, «Verstärkte Mitwirkung der Schweiz bei der europäischen Sicherheitsarchitektur», 20.5.2011; SIPOL-B 16, 43 – 65.

17 Siehe dazu die jährlich erscheinenden ETH-Studien *Sicherheit*, http://www.css.ethz.ch/publikationen/studie-sicherheit.html.

18 Vgl. Jonas Hagmann et al., «Schweizer Sicherheitspolitik in der Praxis: Eine empirische Momentaufnahme», in: *Bulletin zur schweizerischen Sicherheitspolitik* (2016), 99 – 134, hier 101 – 105.

19 SIPOL-B 16, 4.

Nachschreibung der Umfeldanalyse: Drei markante Entwicklungen seit 2010

Der *Bericht 2016* beginnt die Lageanalyse mit einer konzisen, aber sehr gehaltvollen Beschreibung und Beurteilung der internationalen Lage. Dabei wird unter anderem auch die zunehmende Nutzung und Abhängigkeit von Technologien im Weltraum angesprochen und mit der bemerkenswerten Forderung verknüpft, die Schweiz, die keine eigenen Satelliten betreibt, solle prüfen, ob sie bei der satellitengestützten Aufklärung, der Navigation und Positionierung oder bei luft- und weltraumgestützten Kommunikationssystemen eigene Kapazitäten aufbauen sollte, um kritische Abhängigkeiten in diesen Bereichen zu verringern.[20]

... macht der Bericht klar: «Die Zunahme der Migration ist an sich keine sicherheitspolitische Bedrohung für die Schweiz», auch wenn sich unter Migranten vereinzelt Personen mit Verbindungen zu Terroristen oder mit terroristischen Absichten befinden könnten oder Migration Spannungen in der Diaspora fördern könnte.

Das politisch emotionale Thema der Migration wird wohltuend nüchtern abgehandelt. Einerseits wird betont, dass überalterte westliche Industriestaaten wie die Schweiz aus demografischen Gründen auf die Zuwanderung ausländischer Arbeitskräfte angewiesen sind, um ihren Wohlstand zu erhalten. Andererseits macht der Bericht klar: «Die Zunahme der Migration ist an sich keine sicherheitspolitische Bedrohung für die Schweiz», auch wenn sich unter Migranten vereinzelt Personen mit Verbindungen zu Terroristen oder mit terroristischen Absichten befinden könnten oder Migration Spannungen in der Diaspora fördern könnte.[21]

Für den Bundesrat zeichnen sich moderne bewaffnete Konflikte zunehmend dadurch aus, dass «militärische, politische, wirtschaftliche und auch kriminelle Mittel und Kräfte unter Einbezug moderner Waffen und Technologien, insbesondere im Kommunikations- und Cyberbereich, orchestriert zusammen eingesetzt werden». Eine solche hybride Kriegsführung, auch unter Einbezug irregulärer Kräfte, sei zwar nicht völlig neu. Neu seien aber einerseits die Informationsmittel und -kanäle für Propaganda, Information und Desinformation sowie der Umstand, dass früher regulären staatlichen Armeen vorbehaltene moderne, leistungskräftige Waffensysteme auch in die Hände irregulärer Kräfte gerieten.[22]

Der Bericht verdichtet die markanten Entwicklungen der letzten Jahre in drei für die Sicherheit der Schweiz wesentliche Trends. *Erstens* hätten sich die Beziehungen zwischen Russland und dem Westen im Zuge der Ukraine-Krise unerwartet, aber nachhaltig verschlechtert. Besorgniserregend sei dabei die russische Bereitschaft, «international anerkannte Grenzen gewaltsam zu verändern und völkerrechtswidrig Gebiete zu annektieren.»[23] Durch das damit verbundene Szenario eines hybriden Krieges sei die Verteidigungsfähigkeit wieder zu einem sicherheitspolitischen Thema in Europa geworden.

Zweitens habe sich die Bedrohung durch den dschihadistischen Terrorismus durch den ebenfalls unerwarteten Aufstieg des Islamischen Staates in Syrien und im Irak weiter verschärft – auch wenn die Schweiz aus gesellschaftlichen, aber auch aussenpolitischen Gründen «weniger Nährboden und Angriffsfläche für dschihadistischen Terrorismus» biete als andere europäische Staaten.[24]

Drittens habe das Ausmass an illegalen Aktivitäten im Cyberraum zugenommen sowie die «Ruchlosigkeit» einzelner Staaten, technische Möglichkeiten für den Missbrauch im Cyberraum zu nutzen. In der Schweiz habe dadurch der Schutz von Informations- und Kommunikationssystemen und -infrastrukturen einen grösseren Stellenwert erhalten.[25]

Charakteristiken der für die Schweiz relevanten Bedrohung und Gefahren

Der Bericht arbeitet die Charakteristiken der aktuell für die Schweiz relevanten Bedrohungen und Gefahren grundsätzlich überzeugend heraus. Eine der innovativen Hauptleistungen des Berichts ist die Bündelung der aktuellen Gefahren zu sechs Bedrohungstypen, welche zurzeit im Zentrum der Schweizer Sicherheitsarbeit stehen:[26] 1) Illegale Beschaffung und Manipulation von Informationen; 2) Terrorismus und Gewaltextremismus; 3) Bewaffneter Angriff; 4) Kriminalität; 5) Versorgungsstörungen; 6) Katastrophen und Notlagen. Die Bedrohung im Cyberraum, der in der Umfeldanalyse eine markant steigende Bedeutung zugemessen wird, wird als Querschnittsbedrohung beschrieben, da sie in ihrer Wirkung bestehende Bedrohungen intensiviere und verknüpfe. Dem ist zuzustimmen, da die Bedrohungen im Cyberraum zusammen mit dem Terrorismus die politisch-strategischen Bedrohungen des Gesamtsystems Schweiz mit den sicherheitspolizeilichen Gefahren im Inneren und den regionalen Konflikten an der europäischen Peripherie vernetzen.

Eine der innovativen Hauptleistungen des Berichts ist die Bündelung der aktuellen Gefahren zu sechs Bedrohungstypen, welche zurzeit im Zentrum der Schweizer Sicherheitsarbeit stehen: 1) Illegale Beschaffung und Manipulation von Informationen; 2) Terrorismus und Gewaltextremismus; 3) Bewaffneter Angriff; 4) Kriminalität; 5) Versorgungsstörungen; 6) Katastrophen und Notlagen.

20 Ebd., 11 – 15.
21 Ebd., 19f.
22 Ebd., 21f.
23 Ebd., 41.
24 Ebd., 42.
25 Ebd., 42.
26 Ebd., 25 – 41.

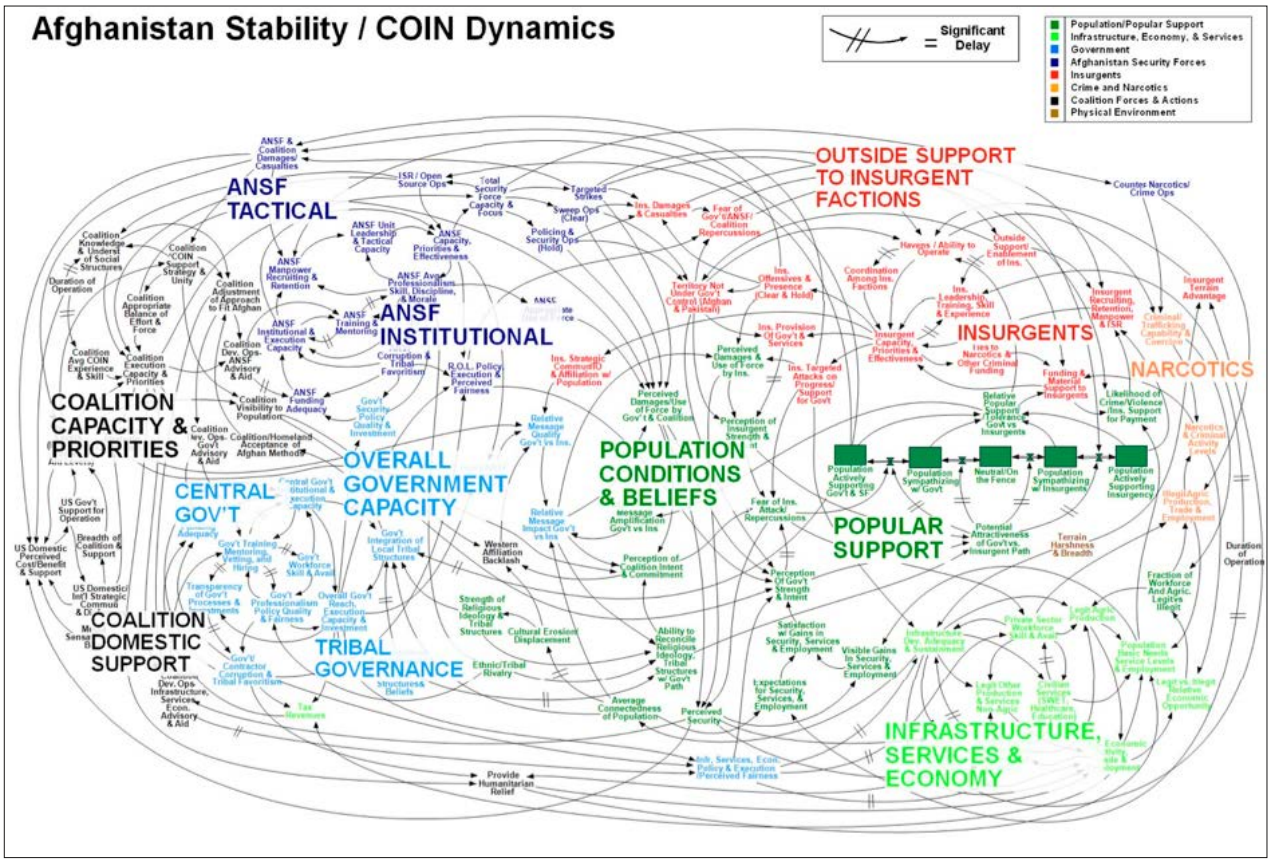


Abbildung 3 Modernes Konfliktmanagement ist eine komplexe Interaktion aller sicherheitspolitischer Instrumente: Hier am Beispiel Afghanistan. (The New York Times)

Gleich zu Beginn betont das entsprechende Kapitel denn auch, dass die Bedrohungen in der Realität nicht einzeln und getrennt auftreten müssten und daher auch nicht einzeln bewältigt werden könnten. Die Kombination oder Verkettung verschiedener Bedrohungen und Gefahren könne die Komplexität der Bewältigung sicherheitspolitischer Herausforderungen markant erhöhen. Die getrennte Abhandlung der jeweiligen Bedrohungstypen sei aber daher notwendig, weil sie nur so in ihren aktuellen Ausprägungen beschrieben werden könnten.[27] Was dabei nicht heraus gearbeitet wird, ist die Feststellung, dass die Bedrohungstypen ein unterschiedliches Verständnis von Sicherheitspolitik reflektieren, an welchem sich die wichtigsten, für die Bewältigung der jeweiligen Bedrohungsbündeln Instrumente und Akteure jeweils orientieren.

Als Hauptmerkmale der aktuellen Bedrohungslage nennt der Bericht die Unberechenbarkeit und Vielseitigkeit, die sich aus der grossen Zahl der potenziell relevanten Akteure und der Vielfalt der eingesetzten Mittel ergeben. Neu ist ebenfalls die Feststellung, dass die Schutzwirkung von Geografie und Distanz zumindest teilweise in Frage gestellt wird. Dies zeigt sich besonders deutlich bei den Aktivitäten im Cyberraum, wo Ländergrenzen bedeutungslos geworden sind. Aufgrund der Verknüpfung zwischen den Bedrohungstypen und kaum vorhersehbaren Rückkoppelungs- und Kaskadeneffekten komme der Widerstands- und Regenerierbarkeit des Gesamtsystems eine steigende Bedeutung zu. In diesem Zusammenhang nennt der Bericht auch den Grundgedanken der Resilienz, ohne ihn allerdings in Bezug zu den im Strategiekapitel diskutierten Konzepten zu setzen.[28]

Aufgrund der Verknüpfung zwischen den Bedrohungstypen und kaum vorhersehbaren Rückkoppelungs- und Kaskadeneffekten komme der Widerstands- und Regenerierbarkeit des Gesamtsystems eine steigende Bedeutung zu.

Vermehrte Anstrengungen zu Stärkung der nationalen Resilienz und eigenständiger Beiträge zur Mitgestaltung globaler Sicherheitsnormen bedingen und ergänzen sich gegenseitig.

27 Ebd., 26.

28 Vgl. dazu Myriam Dunn Cavelty / Tim Prior, «Das Konzept der Resilienz: Gegenwart und Zukunft», in: *CSS-Analysen zur Sicherheitspolitik* Nr. 142 (2013).

Die Erweiterung des Verteidigungsbegriffs ist ein zentrales Anliegen des Berichts. (VBS / DDPS)

Luftpolizeidienst und Luftverteidigung werden die künftige sicherheitspolitische Debatte stark beeinflussen. (VBS / DDPS)

Insgesamt macht der Bericht deutlich, wie stark sich das für die Schweiz relevante Bedrohungsspektrum in den letzten Jahren gewandelt hat. Im Zentrum der Schweizer Sicherheitspolitik steht nicht länger die Abschreckung und Abwehr konkreter nationaler und militärischer Bedrohungen. Konkrete Herausforderungen ergeben sich zunehmend im Zusammenhang mit dem Risikomanagement einer globalisierten Mobilität, die in der Umfeldanalyse sowohl als Bedingung des wirtschaftlichen Fortschritts als auch als potenzielle Quelle von Unsicherheiten beschrieben wird. Dieser neue Schwerpunkt fehlt jedoch hinten bei der Formulierung der Sicherheitsstrategie: Es kann nicht darum gehen, die selbständigen nationalen Anstrengungen gegen das internationale Engagement auszuspielen. Vermehrte Anstrengungen zu Stärkung der nationalen Resilienz und eigenständiger Beiträge zur Mitgestaltung globaler Sicherheitsnormen bedingen und ergänzen sich gegenseitig.[29]

Hybride Kriegführung und die erweiterte Definition von Verteidigung

Der *Bericht 2016* weist zu Recht darauf hin, dass die politischen Gewaltphänomene, die kritische Infrastrukturen der Schweiz in Frage stellen können, nicht mehr ausschliesslich mit den militärischen Potenzialen staatlicher Akteure verbunden seien. Das aktuelle Konfliktbild ist vielmehr von diffusen Netzwerken zwischen staatlichen und politisch wie kriminell motivierten nichtstaatlichen Akteuren geprägt, die Zugang zu Technologien im Luft- und Cyberraum haben. Im Kontext einer als hybrid bezeichneten Kriegführung hat der Bundesrat überprüft, was ein bewaffneter Angriff ist, und sich gefragt, ob das traditionelle Verständnis der Armeeaufgabe «Verteidigung» allenfalls erweitert werden müsse. Er kam zum Schluss, dass das Schadenpotenzial eines bewaffneten Angriffs auch dann erreicht werden könnte, wenn nichtstaatliche Gruppierungen dahinter stehen, die im Inneren des Landes operieren.[30]

Im Rahmen der Vernehmlassung zeigte sich, dass das erweiterte Verständnis von Verteidigung von vielen explizit begrüsst wird.

Die Erweiterung des Verteidigungsbegriffs stellt die entscheidende konzeptionelle Neuerung des *Berichts 2016* dar. Angesichts eines asymmetrischen Bedrohungsspektrums wird die Aufgabe der Verteidigung zunehmend als Schutz sozio-technischer Systeme konzeptualisiert. Dabei machen die im Bericht formulierten Kriterien deutlich, dass «die territoriale Integrität, die gesamte Bevölkerung oder die Ausübung der Staatsgewalt» konkret bedroht sein müssen, um einen derartigen Einsatz der Armee im Innern möglich zu machen. Bundesrat und Parlament müssten im Einzelfall entscheiden, ob «die Armee in einem Fall zur Verteidigung oder subsidiär» eingesetzt werden soll.[31]

Im Rahmen der Vernehmlassung zeigte sich, dass das erweiterte Verständnis von Verteidigung von vielen explizit begrüsst wird.[32] Damit bleibt die Abwehr eines bewaffneten Angriffs die zentrale Aufgabe der Armee. Es ist zu hoffen, dass der teils erbittert geführte Streit um die Ausrichtung der Weiterentwicklung der Armee damit abflaut. Ins Zentrum der Armeedebatte dürfte künftig dafür die Kernfrage rücken, welche militärischen Fähigkeiten für die Abwehr eines bewaffneten Angriffs innerhalb der Schweiz in den nächsten Jahren und Jahrzehnten nötig sind. Die Rüstungsdiskussionen dürften sich dabei neben den Kampfflugzeugen zum Beispiel vermehrt um leichte Panzer drehen.

Das Zusammenspiel der Instrumente bei der Prävention, Abwehr und Bewältigung der Bedrohungen und Gefahren

Der *Bericht 2016* hat für die Behandlung der sicherheitspolitischen Instrumente innovativ eine neue Darstellungsform gewählt. Statt wie in bisherigen Berichten die einzelnen Instrumente zu beschreiben, werden die konkreten Beiträge aller Instrumente zur Prävention, Abwehr und Bewältigung um den jeweiligen Bedrohungstyp gruppiert.

29 Vgl. dazu Wenger / Nünlist, «Aufwertung», 34 – 38.
30 SIPOL-B 16, 24.
31 Ebd., 92f.
32 VBS, Ergebnisbericht, op. cit., 5.

Dies hat den Vorteil, dass die Komplexität und Multidimensionalität der Bedrohungsbündel einfach veranschaulicht werden kann. Zudem kann auch die Koordination und das Zusammenspiel der Mittel bei der Bewältigung der Bedrohungen beschrieben werden. Dabei wird offenkundig, dass die meisten Bedrohungstypen von einem komplexen Geflecht an Schweizer Sicherheitsakteuren bearbeitet werden und dass sich die meisten sicherheitspolitischen Instrumente gleichzeitig mit einer Vielfalt von Bedrohungen auseinandersetzen.[33] Die neu gewählte Darstellung wurde denn in der Vernehmlassung auch überwiegend positiv gewürdigt.

Dabei wird offenkundig, dass die meisten Bedrohungstypen von einem komplexen Geflecht an Schweizer Sicherheitsakteuren bearbeitet werden und dass sich die meisten sicherheitspolitischen Instrumente gleichzeitig mit einer Vielfalt von Bedrohungen auseinandersetzen.

Allerdings hat die gewählte Form auch ihren Preis: So liegt der Fokus nicht auf der Weiterentwicklung der einzelnen Instrumente. Zudem ist es auch schwieriger, aus dem Bericht herauszulesen, welches pro Bedrohungsbündel letztlich die entscheidenden Akteure sind und mit welchen Bedrohungen sich die einzelnen Instrumente hauptsächlich und am Intensivsten beschäftigen.

Konzeptuelle Schwächen: Kaum neue Massnahmen und Konsequenzen

Eine umfassende und vernetzte Sicherheitspolitik stellt hohe Ansprüche an die Politikgestaltung und die Politikumsetzung. Auf der Ebene der Politikgestaltung – der Strategien und Konzepte – geht es darum, die Bereiche der Verteidigung, Aussenpolitik und Inneren Sicherheit besser aufeinander abzustimmen. Auf der Ebene der Politikumsetzung – der Instrumente, Mittel und Ressourcen – geht es um Koordination und Kooperation über sektorielle und departementale Grenzen, über verschiedene Regierungsebenen hinweg sowie zwischen öffentlichen und privaten und zivilgesellschaftlichen Akteuren. In einem auf Machtteilung angelegten föderalen System, an dessen Spitze eine Kollegialregierung steht, sind der politisch-konzeptuellen Steuerung per se Grenzen gesetzt.[34]

... überdeckt der Bericht, dass sich die verschiedenen Akteure in ihrer praktischen Arbeit implizit oder explizit von sehr unterschiedlichen Sicherheitsverständnissen leiten lassen.

Umso wichtiger wäre es allerdings, dass das Politikfeld über möglichst kohärente Konzepte und klare strategische Prioritäten verfügt. Dies vermag der Bericht 2016 nur ansatzweise zu leisten, was teilweise der bereits skizzierten Ausgangslage zuzuschreiben sein mag. Gleichwohl sind auch konzeptuelle Schwächen mitverantwortlich, dass der Bericht nur wenig griffige strategische Handlungsrichtlinien erkennen lässt. Er kann daher auch nur beschränkt als strategischer Orientierungsrahmen dienen, um den Anpassungsbedarf der Sicherheitsinstrumente zu erkennen und zur Diskussion zu stellen. Gleichzeitig überdeckt der Bericht, dass sich die verschiedenen Akteure in ihrer praktischen Arbeit implizit oder explizit von sehr unterschiedlichen Sicherheitsverständnissen leiten lassen.

Weiter und diffuser Begriff der Sicherheitspolitik

Der *Bericht 2016* hält an dem sehr weiten Sicherheitsverständnis des *Berichts 2010* fest. Er definiert Sicherheitspolitik als «die Gesamtheit aller Massnahmen von Bund, Kantonen und Gemeinden zur Vorbeugung, Abwehr und Bewältigung machtpolitisch oder kriminell motivierter Drohungen und Handlungen, die darauf ausgerichtet sind, die Schweiz und ihre Bevölkerung in ihrer Selbstbestimmung einzuschränken oder ihnen Schaden zuzufügen. Dazu kommen die Vorbeugung und Bewältigung natur- und zivilisationsbedingter Katastrophen und Notlagen.»[35]

Mit dem Wegfall der Abgrenzung zwischen Gewalt nicht-strategischen Ausmasses, deren Bekämpfung in der Verantwortung der Kantone lag, und strategischen Gewaltpotenzialen, um die sich der Bund zu kümmern hatte, verwischten sich die Rollen und Verantwortlichkeiten der zwei Staatsebenen zunehmend.

Parallel zur Ausweitung der involvierten Akteure und Staatsebenen liess sich in den letzten Jahren ein Trend hin zu einer diffuseren strategischen Terminologie erkennen. Entscheidend war dabei die Erweiterung des Sicherheitsbegriffs um den Bereich der Alltagsgewalt und die Integration der Sicherheitsbeiträge der Kantone und Gemeinden in den *Bericht 2010*.[36] War damit die vertikale Ausweitung des Sicherheitsbegriffs über die Staatsebenen weit fortgeschritten, so wurde gleichzeitig der strategische Gewaltbegriff fallengelassen, der im *Bericht 2000* zur Abgrenzung des Politikfeldes gedient hatte.[37] Mit dem Wegfall der Abgrenzung zwischen Gewalt nicht-strategischen Ausmasses, deren Bekämpfung in der Verantwortung der Kantone lag, und strategischen Gewaltpotenzialen, um die sich der Bund zu kümmern hatte, verwischten sich die Rollen und Verantwortlichkeiten der zwei Staatsebenen zunehmend.

Man mag einwenden, dieses Verwischen der Aufgaben widerspiegle den Wandel der Bedrohungslage und damit einhergehend die Künstlichkeit der Grenzen zwischen innerer und äusserer Sicherheit. Der grenzüberschreitende Cha-

33 Vgl. dazu auch Hagmann et al., «Schweizer Sicherheitspolitik», 103 – 118.
34 Siehe Karl Haltiner, «Vom schmerzlichen Verlieren alter Feindbilder: Bedrohungs- und Risikoanalysen in der Schweiz», in: Thomas Jäger / Ralph Thiele (eds.), *Transformation der Sicherheitspolitik: Deutschland, Österreich, Schweiz im Vergleich* (Wiesbaden: VS Verlag, 2011), 39 – 58, hier 40f.
35 SIPOL-B 16, 7. Diese Definition wurde wortwörtlich aus dem Bericht 2010 übernommen (dort auf S. 5141).
36 Bundesrat, *Bericht an die Bundesversammlung über die Sicherheitspolitik der Schweiz*, 23.6.2010, 5134.
37 Bundesrat, *Bericht an die Bundesversammlung über die Sicherheitspolitik der Schweiz*, «Sicherheit durch Kooperation», 7.6.1999, 10.

rakter der aktuellen Bedrohungen und Gefahren stellen die Systeme der inneren und äusseren Sicherheit in der Tat vor schwierige Abgrenzungsfragen. Gleichwohl lohnt es sich allein schon aus staatspolitischen und verfassungsrechtlichen Gründen, vertieft über die vertikale und horizontale Abgrenzung des Politikfelds der gesamtstaatlichen Sicherheitspolitik nachzudenken.

Der Preis eines diffusen Sicherheitsbegriffs sind *erstens* unklare Rollenverständnisse und Verantwortlichkeiten zwischen Politikbereichen, operationellen Instrumenten und Staatsebenen; *zweitens* Schwierigkeiten bei der Definition von Schnittstellen zwischen den Führungssystemen auf den verschiedenen Staatsebenen; *drittens* ein unfruchtbares politisches Seilziehen um die Deutungshoheit unscharfer strategischer Konzepte; *viertens* ein strategisch-politischer Steuerungsverlust hinsichtlich einer möglichst bedrohungsgerechten und auf die Zukunft gerichteten Ausrichtung der sicherheitspolitischen Instrumente; *fünftens* eine Änderung im Charakter der sicherheitspolitischen Berichte, die dadurch weniger Wirkung im Sinne einer Prioritätensetzung entfalten, sondern stattdessen stärker deskriptiv Entwicklungen nachschreiben.

Hinsichtlich der horizontalen Ausweitung des Sicherheitsbegriffs – der Abgrenzung der Sicherheitspolitik von anderen Politikfeldern – folgt der *Bericht 2016* seinen Vorgängerberichten im Bemühen um eine limitierte Ausweitung des Sicherheitsbegriffs. Besonders deutlich wird dies hinsichtlich der Schnittstellen zwischen der Sicherheitspolitik und der Wirtschaftspolitik, zwischen der Sicherheitspolitik und der Asyl- und Migrationspolitik sowie zwischen der Sicherheitspolitik und der Klima- und Gesundheitspolitik.[38]

Hilfreich sind gerade auch die Kapitel zu den sicherheitspolitischen Instrumenten, weil hier deutlicher wird, hinsichtlich welcher Sicherheitsaspekte inhaltliche Bezüge zwischen den jeweiligen Politikfeldern bestehen.

Die enge Auslegung der horizontalen Ausweitung der Sicherheitspolitik ist zu begrüssen, weil damit der Fokus des Politikfeldes auf die Abwehr eines strategischen Gewaltpotenzials faktisch erhalten bleibt. Hilfreich sind gerade auch die Kapitel zu den sicherheitspolitischen Instrumenten, weil hier deutlicher wird, hinsichtlich welcher Sicherheitsaspekte inhaltliche Bezüge zwischen den jeweiligen Politikfeldern bestehen. Die konzeptionelle Logik dieser Abgrenzung bleibt allerdings diffus. Wichtig wäre hier die Feststellung gewesen, dass die Schnittstellen zu den anderen Politikfelder an Bedeutung gewinnen, weil sich der Fokus der Sicherheitsstrategie von reaktiven und defensiven Ansätzen vermehrt auf die Bereich der Prävention und Bewältigung verschoben hat.

38 SIPOL-B 17, 9, 20f., 39ff, 53 – 56.

Unterschiedliches Verständnis von Sicherheitspolitik bleibt unklar

Die diffuse übergeordnete Terminologie verdeckt, dass sich die Akteure bei ihrer praktischen Sicherheitsarbeit konzeptionell von sehr unterschiedlichen Sicherheitsverständnissen leiten lassen. Dies reflektiert die historisch getrennte Entwicklung des Sicherheitsbegriffs bei den vier Departementen des Bundes und bei den kantonalen Stellen, die sich mit sicherheitspolitischen Bedrohungen auseinandersetzen.[39] Die Typologie der Bedrohungsbündel ist auch nicht zufällig erfolgt. Vielmehr reflektiert sie den sehr unterschiedlichen Charakter der Bedrohungen sowohl in Bezug auf das konzeptuelle Verständnis von Sicherheitspolitik als auch auf den staatspolitischen und verfassungsrechtlichen Rahmen. Es würde sich lohnen, diese Unterschiede expliziter herauszuarbeiten, um den Nachteilen einer diffusen Terminologie entgegen zu wirken.

Entsprechend an Bedeutung gewonnen hat das Konzept der Resilienz, wobei der fallengelassene strategische Gewaltbegriff indirekt wieder eingeführt wird, um die Verteidigungsaufgabe der Armee von den subsidiären Einsätzen abzugrenzen.

Die drei zuerst genannten Bedrohungsbündel – illegale Beschaffung und Manipulation von Informationen; Terrorismus und Gewaltextremismus; bewaffneter Angriff – fokussieren politische und militärische Gewaltphänomene und repräsentieren den klassischen Bereich gesamtstaatlicher Sicherheitspolitik. Als konzeptueller Angelpunkt dient das Konzept der nationalen Sicherheit; als verantwortliche Akteure stehen das VBS und das EDA im Zentrum der Aufmerksamkeit. Wie im Bericht diskutiert und oben beschrieben, hat sich der Charakter dieser Bedrohungsbündel in den letzten Jahren markant verändert. Neu konzentriert sich das VBS auf strategische Gewaltphänomene, die von staatlichen und nichtstaatlichen Akteuren ausgehen können. Entsprechend an Bedeutung gewonnen hat das Konzept der Resilienz, wobei der fallengelassene strategische Gewaltbegriff indirekt wieder eingeführt wird, um die Verteidigungsaufgabe der Armee von den subsidiären Einsätzen abzugrenzen.[40]

Die Dienststellen des EDA wiederum konzentrieren sich vermehrt auf die mit diesen Bedrohungsbündeln verbundene regionale Instabilität und grenzüberschreitende Phänomene politischer Gewalt. Das Konzept der nationalen Sicherheit wurde daher ergänzt um die Konzepte der menschlichen und globalen Sicherheit.[41]

Das vierte Bedrohungsbündel Kriminalität konzentriert sich auf sicherheitspolizeiliche Bedrohungen und stellt den klassischen Bereich kantonaler Sicherheitspolitik dar. Als konzeptueller Angelpunkt dient das Konzept der öffentlichen Sicherheit und Ordnung; im Zentrum der Aufmerksamkeit stehen die Kantonspolizeien. Auch der Charakter

39 Hagmann et al., «Schweizer Sicherheitspolitik», 103ff.
40 SIPOL-B 16, 92f.
41 Ebd., 86f., 96.

Die vertiefte Kooperation der Führungsorgane aller sicherheitspolitischen Partner ist von besonderer Bedeutung. (VBS / DDPS)

Der Schutz der Bevölkerung vor allen möglichen Risiken und Gefahren stellt auch weiterhin eine erhebliche Herausforderung dar. (VBS / DDPS)

dieses Bedrohungsbündels hat sich in den letzten Jahren markant gewandelt. Vor allem die grenzüberschreitende Natur krimineller Herausforderungen hat stark an Bedeutung gewonnen. Mit Blick auf die grenzüberschreitende Mobilität gewann das Konzept des Risikomanagements an Bedeutung. Damit einhergehend hat das Gewicht von Bundesstellen im EJPD und im EFD zugenommen, die sich an der Schnittstelle zum europäischen Umfeld mit Koordinations- und Kooperationsfragen in den Bereichen Polizei, Grenzschutz, Asyl und Migration auseinandersetzen. Entsprechend steigen die Berührungspunkte zwischen den Kantonen und dem Bund.

Die fünften und sechsten Bedrohungsbündel – Versorgungsstörungen, Katastrophen und Notlagen – folgen einer Logik, die stark von den Konzepten des Risikomanagement, der Resilienz und der Regulation beeinflusst wird. Dies reflektiert die grosse Bedeutung, die in diesem Bereich neben dem Katastrophenmanagement vor allem der Prävention und der Bewältigung zukommt. Neben den natur- und technikbedingten Gefahren erhalten gesellschaftsbedingte Gefahren wie Pandemie neue Bedeutung. Aufgrund der Globalisierung und der immer dichteren Interdependenz der Märkte und Infrastrukturen in den Bereichen Handel, Energie, Information steigen die Verwundbarkeiten und die Bedeutung internationaler Absprachen und Normen. Erforderlich wird in diesem Bereich die Koordination eines dichten Geflechts von öffentlichen Akteuren auf der Stufe des Bundes und der Kantone sowie vielfältigen privaten, zivilen und internationalen Akteuren.

Die unterschiedlichen Sicherheitsverständnisse bleiben einerseits mit Blick auf ihre staats- und verfassungsrechtliche Dimension wichtig. Abgrenzungsfragen an der Schnittstelle der Verantwortungsbereiche von Bund und Kantonen werden sich immer auch am Konzept eines strategischen Gewaltpotenzials orientieren. Dies hat die Diskussion um die Erweiterung der Armeeaufgabe der Verteidigung deutlich gemacht. Liegt die primäre Verantwortung des Bundes bei der Bewältigung strategischer Gewaltpotenziale, konzentrieren sich die Kantone auf die Bekämpfung von Gewalt nicht-strategischem Ausmasses.

Aus Sicht des Bundes – und damit der nationalen Sicherheit – stellte die Zunahme der Migration [...] keine sicherheitspolitische Bedrohung dar.

Die explizite Anerkennung unterschiedlicher Sicherheitsverständnisse kann andererseits auch hilfreich sein, wenn es um die Bewertung und Benennung operationeller Herausforderungen geht. Unterschiedliche Einschätzungen internationaler Entwicklungen können Unterschiede im konzeptionellen Sicherheitsverständnis widerspiegeln und aus institutioneller und bürokratischer Sicht nur schwer in Übereinstimmung zu bringen sein. Dies zeigte sich im Kontext des Erarbeitungsprozesses des *Berichts 2016* insbesondere bei den Einschätzungen der sich zuspitzenden Migrations- und Flüchtlingskrise. Aus Sicht des Bundes – und damit der nationalen Sicherheit – stellte die Zunahme der Migration, wie bereits erwähnt, keine sicherheitspolitische Bedrohung dar. Sie berührt zwar gewisse Aspekte der Sicherheitspolitik – Verbindung zu Kriminalität, ethnischen Spannungen, terroristischen Absichten –, für die aber mit Ausnahme des Nachrichtendienstes primär die sicherheitspolizeilichen Akteure auf der Stufe der Kantone zuständig sind. Auf Bundesebene liegt die primäre Verantwortung für die Migration bei anderen Politikfeldern wie der Asyl-, Migrations- und Integrationspolitik. Aus kantonaler Perspektive sind die Bezüge zur öffentlichen Sicherheit und Ordnung offensichtlich viel direkter. Dies kam in der Vernehmlassung des Berichtsentwurfs deutlich zum Ausdruck, in dem die meisten Kantone eine Überarbeitung der teilweise als relativierend empfundenen Aussagen zur Migration beantragt hatten.[42]

Wenig Strategie: Unklare Konzepte, keine sichtbaren Akzente

Am wenigsten überzeugend im *Bericht 2016* fallen die Ausführungen zur Strategie aus. Dies mag nicht überraschen, weil hier das Dilemma eines Bedrohungsberichts besonders deutlich wird. Der Bundesrat hat zwar markante Veränderungen bei der Lage festgestellt, wollte aber bei der

42 VBS, Ergebnisbericht, op. cit., 3.

Diskussion der Instrumente 2015/16 nicht über damals laufende Reformen hinausgehen. Die Ausführungen zu den nationalen Interessen und den sicherheitspolitischen Zielen hinterlassen einen zwiespältigen Eindruck: Der Begriff der nationalen Interessen bietet generell wenig analytisches Gehalt und es lohnt sich daher auch nicht, ihn zu konkretisieren. Eine sorgfältige und möglichst präzise Formulierung der sicherheitspolitischen Ziele hingegen ist wichtig, da diese Ziele festhalten, was im Rahmen der Sicherheitspolitik geschützt werden soll. Der *Bericht 2016* hält wortwörtlich an der Definition der Ziele vom *Bericht 2010* fest, was insofern auch Sinn macht, als sich sicherheitspolitische Ziele nur langsam ändern. Überlegenswert schiene aber, ob eine explizite Auflistung wie in früheren Berichten (1973, 1990, 1999) die Ziele nicht griffiger machen würde.

Die Definition und Abgrenzung der drei strategischen Kernbegriffe – Kooperation; Selbständigkeit; Engagement – ist nur schwer nachvollziehbar und bietet keine in die Zukunft gerichtete strategische Orientierung. Die Ausführungen scheinen primär rückwärts orientiert und widerspiegeln das politische Seilziehen um den Kooperationsbegriff, das bereits die Debatten um den sicherheitspolitischen Bericht 2010 geprägt hatte.[43]

Die Definition und Abgrenzung der drei strategischen Kernbegriffe – Kooperation; Selbständigkeit; Engagement – ist nur schwer nachvollziehbar und bietet keine in die Zukunft gerichtete strategische Orientierung.

«Kooperation», begrenzt durch die zwei Extreme «Isolation» und «Integration», scheint sich auf die Frage zu konkretisieren, mit wem wie verbindlich zusammen gearbeitet werden soll. «Selbständigkeit» wird als Voraussetzung und nicht als Gegensatz zur Kooperation verstanden und scheint sich auf die Dimension der Unabhängigkeit respektive der Abhängigkeit der eigenen Sicherheitsleistungen von den Leistungen Dritter zu beziehen. Beim «Engagement» geht es laut Bericht darum, «mit gezielten Beiträgen direkt oder indirekt die Sicherheit der Schweiz zu stärken.»[44] Dies ist insofern verwirrend, als die Ausführungen insbesondere zu den internationalen Beiträgen vieles aufnehmen, das zuvor im Bericht unter dem Begriff der internationalen Kooperation diskutiert worden ist.

Nicht nur bleibt der Bezug der drei strategischen Elemente unklar, sie vermögen auch nicht zu überzeugen, was die Priorisierung strategischer Aufgaben und Massnahmen anbelangt. Es bleibt völlig offen, ob der beschriebene Wandel der Bedrohungslage laut Bundesrat insgesamt nach mehr oder weniger Kooperation, Selbständigkeit oder Engagement ruft und inwiefern es auf der Ebene der Mittel diesbezüglich neue Akzente bräuchte.

Erfolgversprechender als strategische Kernbegriffe wären die im Bericht eingeführten Elemente der Prävention, Abwehr und Bewältigung, bei denen allerdings auch nicht klar wird, ob und warum es eine Stärkung des einen oder anderen Elementes braucht. Die Unterscheidung verschiedener Phasen beim Management der aktuellen Risiken reflektiert die skizzierte Entwicklung der Bedrohungslage. Aufgrund der Zunahme an relevanten Akteuren und eingesetzten Mittel, der Unberechenbarkeit, Komplexität und Vernetzung sowie des grenzüberschreitenden Charakters der Bedrohungen sowie einer im Vergleich mit dem Kalten Krieg höheren Eintretenswahrscheinlichkeit vieler Gefahren bei kleinerem Schadenspotenzial erfordert die aktuelle Lage insgesamt vermehrte Anstrengungen in den Bereichen Prävention und Bewältigung.

Status quo bei den Instrumenten: Kein sichtbarer Anpassungsbedarf

Ein Nachteil der gewählten innovativen Darstellungsform im Teil über die sicherheitspolitischen Instrumente ist, dass der Bericht keine systematische Klärung und Priorisierung der strategischen Beiträge der einzelnen Instrumente bietet. Die Darstellung der Instrumente ist letztlich wenig konkret, nicht sehr übersichtlich und in erster Linie deskriptiv. So bleibt beispielsweise unklar, ob und inwieweit die anderswo im Bericht diskutierten Möglichkeiten zur verstärkten Mitwirkung der Schweiz an der europäischen Sicherheitsarchitektur überhaupt in die Überlegungen zu den sicherheitspolitischen Instrumenten miteingeflossen sind.

Diesen Eindruck vermag auch das abschliessende Kapitel zum «Anpassungsbedarf bei den Instrumenten der Sicherheitspolitik» nicht wettzumachen. Dieser Teil konzentriert sich auf die Darstellung der laufenden Reformprojekte und Teilstrategien.[45] Zu Recht wurde in der Vernehmlassung kritisiert, der Bericht biete wenig Konkretes mit Blick auf die Herausarbeitung eines vorausschauenden Handlungs- und Anpassungsbedarfs.[46] Konkrete Konsequenzen des Bedrohungswandels und neue Massnahmen auf der Ebene der Mittel sind in der Tat weitestgehend ausgeklammert worden.

Herausforderungen der strategischen Führung: Kohärenz, Koordination, Kommunikation, Krisenmanagement

Auch die Herausforderungen im Bereich der strategischen Führung stehen in einem direkten Zusammenhang mit dem Wandel der Bedrohungslage. Insgesamt sind die Anforderungen an die strategische Führung in den letzten Jahre deutlich angestiegen, vor allem in drei Bereichen: *Erstens* mit Blick auf die Kohärenz der Politikformulierung über die Bereiche der Verteidigung, der Aussenpolitik und der Inneren Sicherheit weg; *zweitens* mit Blick auf die Koordination der zunehmenden Zusammenarbeit erstens im nationalen Sicherheitsverbund über sektorale und departementale Grenzen sowie über mehrere Ebenen des Regierens hinweg, im Kontext der internationalen Zusammenarbeit im multi-, mini- und bilateralen Rahmen sowie mit Blick auf die Zusammenarbeit des öffentlichen mit den pri-

43 Andreas Wenger et al. «Sicherheitspolitischer Bericht 2010: Viel Politik, wenig Strategie», in: *Bulletin zur schweizerischen Sicherheitspolitik* (2010), 9 – 26.
44 SIPOL-B 16, 75.
45 SIPOL-B 16, 103 – 107.
46 VBS, Ergebnisbericht, op. cit., 5.

vaten und zivilgesellschaftlichen Sektoren; sowie *drittens* mit Blick auf die strategische Kommunikation und das Krisenmanagement. [47]

Die Führungsstrukturen auf der Stufe des Bundes, auf der Stufe der Kantone sowie an den Schnittstellen zwischen Bund und Kantonen haben sich in den letzten Jahren stark gewandelt und weiter entwickelt.[48] Der *Bericht 2016* beschränkt sich auf einen detaillierten Beschrieb eines historisch gewachsenen, hochkomplexen Führungssystems. Zu kurz kommt wiederum der Bezug zu den anderen Kapiteln des Berichts. Insbesondere wird die Frage nur ungenügend aufgenommen, inwieweit sich aufgrund der beschriebenen Bedrohungslage ein Anpassungsbedarf bei den strategischen Führungssystemen ergibt. Eine Ausnahme bildet die Betonung der Wichtigkeit geschützter Anlagen und Kommunikationssysteme als Voraussetzung der Führung.[49] Zu kurz geraten hingegen die Überlegungen zu den Rückwirkungen hybrider Kriegsformen auf die zivil-militärische Zusammenarbeit, zur Zusammenarbeit zwischen Bund und Kantonen sowie zur Angemessenheit der Strukturen für das Krisenmanagement.

Hybride Bedrohung: Eine zivil-militärische Herausforderung

Die Veränderung des aktuellen Konfliktbildes unter dem Stichwort «hybride Kriegsführung» wird im Teil der Lageanalyse auf breitem Raum abgehandelt. Der Einschätzung dieses Trends als bedeutende Veränderung der Bedrohungslage ist ohne Einschränkung zuzustimmen, nicht jedoch der Feststellung, dass diese Veränderung «vor allem die Armee» betreffe.[50] Dies greift aus mehreren Gründen zu kurz: Diese Einschätzung übersieht, dass hybride Kriegsführung als zivil-militärische Herausforderung verstanden werden muss. Auch die Rolle der zivilen Mittel steigt an, und es stellen sich schwierige Fragen hinsichtlich der politischen, wirtschaftlichen und gesellschaftlichen Resilienz des Gesamtsystems.

Der Einschätzung dieses Trends [hybride Kriegführung] als bedeutende Veränderung der Bedrohungslage ist ohne Einschränkung zuzustimmen, nicht jedoch der Feststellung, dass diese Veränderung «vor allem die Armee» betreffe.

In diesem Zusammenhang wird auch auf die zunehmende Bedeutung von staatlicher oder halbstaatlicher Desinformation und Propaganda hingewiesen. Im Analyseteil spricht der Text von der Notwendigkeit, dass die politischen Behörden der Schweiz «die Möglichkeit gegnerischer Informationsoperationen berücksichtigen» und ihr «im Ereignisfall durch wahrheitsgemässe Information und Kommunikation» entgegen treten sollen.[51] In der Darstellung des Führungssystems auf der Stufe Bund bleibt allerdings weitestgehend offen, wie dies genau geschehen soll und ob die bestehenden Führungsmittel und -prozesse den veränderten Rahmenbedingungen zu genügen vermögen.

Die Feststellung, dass die Information und Kommunikation nicht erneut, wie bis und mit dem *Bericht 1999* als sicherheitspolitisches Instrument geführt werden sollen, wird unter Hinweis auf die demokratie-theoretisch problematische Funktion staatlicher Gegenpropaganda begründet.[52] Dem ist zwar grundsätzlich zuzustimmen. Allerdings beantwortet dies nicht die Frage, wie sich die verbreitete Desinformation und Propaganda auf das Gesamtsystem auswirkt und wie der Bundesrat diesem Element im Rahmen seiner strategischen Kommunikation entgegentreten soll.

Auch hinsichtlich der Cyberdimension aktueller Konflikte stellen sich grundsätzliche Fragen hinsichtlich der Rolle der Armee und des VBS im Rahmen der Bewältigung von Cyberrisiken. Die im Bericht genannte *Nationale Strategie zum Schutz der Schweiz gegen Cyberrisiken* (2012) setzte auf einen föderalen Ansatz und die Führung lag bei der Umsetzung bei den zivilen Stellen; derzeit gibt es Bestrebungen, diese Strategie zu aktualisieren. Aufgrund der Politisierung und der Militarisierung des Cyberraums scheint unbestritten, dass die forensischen Kapazitäten des Nachrichtendienstes und die Cyberdefence-Kapazitäten der Armee ausgebaut werden müssen. Offen ist jedoch, in welchem Verhältnis sie mit den bestehenden Bemühungen auf der zivilen Seite stehen sollen und in welchen Bereichen (Ausbildung, etc.) von Synergien profitiert werden könnte.

Grenzüberschreitende Mobilität: Eine Herausforderung über Staatsebene hinweg

Die aktuelle Bedrohungslage legt nahe, dass das effiziente und effektive Management der grenzüberschreitenden Mobilität zu einer zentralen Herausforderung moderner Sicherheitspolitik geworden ist. Die Bedeutung der geografischen Landesgrenzen mag generell abgenommen haben, weil einige der aktuellen Bedrohungen Grenzen zu überspringen vermögen und sich direkt im Innern der Gesellschaft manifestieren. Insgesamt gewinnt das Management von Grenzen gleichwohl an Bedeutung, wobei Grenzen weiter gedacht werden müssen und Grenzen innerhalb des Landes (beispielsweise an Flughäfen), ausserhalb des Landes (etwa an den europäischen Aussengrenzen) oder Grenzen im Cyber-Raum umfassen können.[53]

Es kann nun aber nicht darum gehen, die Schweizer Grenzen zu schliessen. Dazu ist die Schweiz als exportorientierter Kleinstaat mit einer der weltweit am mobilsten Bevölkerungen viel zu sehr auf eine offene und liberale Ordnung angewiesen. Es gilt vielmehr, die grenzüberschreitende Mobilität im Spannungsfeld von erwünschter Migration und unerwünschter sicherheitsrelevanter Begleiterscheinung bestmöglich zu organisieren. Diese Kernaufgabe moderner Sicherheitspolitik kann nicht nur einer staatlichen Ebene zugesprochen werden, sie transzendiert die hergebrachten Grenzen zwischen der inneren und der äusseren Sicherheit sowie zwischen zivilen und militärischen Mitteln.

47 Wenger / Nünlist, «Aufwertung», 31 – 41.
48 Andreas Wenger, «Sicherheitspolitik», in: Peter Knoepfel et al. (eds.), *Handbuch der Schweizer Politik,* 5. Aufl. (Zürich: NZZ, 2014), 645 – 669.
49 SIPOL-B 16, 117ff.
50 Ebd., 24.
51 Ebd., 25
52 Ebd., 111.
53 Vgl. dazu Matthias Leese / Stef Wittendorp (eds.), *Security / Mobility: Politics of Movement* (Manchester: Manchester University Press, 2017).

Insgesamt gewinnt das Management von Grenzen gleichwohl an Bedeutung, wobei Grenzen weiter gedacht werden müssen und Grenzen innerhalb des Landes (beispielsweise an Flughäfen), ausserhalb des Landes (etwa an den europäischen Aussengrenzen) oder Grenzen im Cyber-Raum umfassen können.

Die zentralen gesamtstaatlich relevanten Sicherheitsfragen weisen innen- wie aussenpolitische Bezüge auf. Zudem haben beide Staatsebenen grenzüberschreitende Verantwortung. Die Kantone leisten wichtige, zunehmend strategisch relevante Beiträge zur Bewältigung politischer relevanter transnationaler Gewaltphänomene. Gleichzeitig übernimmt der Bund zunehmend zentrale koordinative Funktionen im Bereich der sicherheitspolizeilichen Aufgaben an den Schnittstellen zum europäischen Umfeld.

In diesem Kontext stellen sich zunehmend Grundsatzfragen mit Blick auf die hergebrachten Rollen der zwei Staatsebenen im inneren Sicherheitssystem der Schweiz. Zwar betont der *Bericht 2016* die Rolle der Kantone in der Sicherheitspolitik der Schweiz, ohne allerdings auf die Grundsatzfragen vertieft einzugehen. Er vermag damit das innere Sicherheitssystem der Schweiz nicht weiterzuentwickeln, das von einem schleichenden Prozess des Auseinanderlaufens zwischen staatspolitischen und verfassungsrechtlichen Grundsätzen einerseits und pragmatischen Anpassungen der Rollen in der Praxis geprägt ist.

Krisenmanagement: Ad-hoc-Führung und Koordination

Augenfällig in der Darstellung der strategischen Führungssysteme der Schweiz sind schliesslich der Ad-hoc-Charakter der strategischen Führungsprozesse auf der Stufe des Bundes sowie die Beschränkung der Organe des Sicherheitsverbundes Schweiz (SVS) auf Konsultation und Koordination. Je nach Art der Krise soll auf der Stufe des Bundes pragmatisch entschieden werden, wie die Führung auf der Ebene der Bundesräte und der diversen Krisenstäbe geregelt werden soll. Die Organe des SVS sind wiederum nicht für das Krisenmanagement vorgesehen.[54] In der Vernehmlassung zeigte sich denn auch, dass sich verschiedene Kantone eine permanente Anlaufstelle auf der Stufe des Bundes erwünschen.[55] Dass das Führen im Rahmen eines hochkomplexen Sicherheitsverbundes schwierig bleibt, zeigte sich parallel zur Erarbeitung des Berichts in den Diskussionen rund um das Notfallkonzept zwischen Bund und Kantonen für die Bewältigung einer Flüchtlingskrise.

Angesichts einer Bedrohungslage, die durch hybride Bedrohungen, grenzüberschreitenden Terrorismus sowie Angriffe im Cyberraum gekennzeichnet ist, stellen die Fähigkeiten des Gesamtsystems zur integrierten und permanenten Lageanalyse, zur koordinierten Führung eines vielschichten und mehrere staatliche Ebene übergreifenden zivilen und militärischen Instrumentenpools sowie zur zeitverzugslosen und kohärenten strategischen Kommunikation entscheidende Elemente zur Bewältigung komplexer, grenzüberschreitender Krisenlagen dar. In diesem Kontext lässt der *Bericht 2016* eine über die Darstellung des Status quo hinausgehende, vertiefte Auseinandersetzung mit der Frage, ob das historisch gewachsene Führungssystem den Anforderungen der aktuelle Lage gewachsen ist respektive welcher Anpassungsbedarf gegeben ist, vermissen.

Schlussbetrachtung

Mit dem *Sicherheitspolitischen Bericht 2016* hat der Bundesrat einen lesenswerten «Bedrohungsbericht» vorgelegt. Der Bericht zeichnet sich durch eine gehaltvolle Analyse der internationalen Lage aus. Er beschreibt den Charakter der Bedrohungen für die Schweiz sehr gut. Der erste, rundherum gelungene Teil zeigt eindrücklich, wie komplex heutige Sicherheitspolitik geworden ist.

Das Parlament hat wiederholt den Wunsch geäussert, dass der Bundesrat die Kadenz der Berichte erhöhe. Tatsächlich ist das Informations- und Orientierungsbedürfnis angesichts des raschen Wandels der internationalen Beziehungen markant gestiegen, insbesondere was die Nachschreibung der Bedrohungsanalyse anbelangt. Eine kurze und knappe Aktualisierung geostrategischer Trends und der für die Schweiz relevanten Bedrohungsbündel lässt sich in dem bewährten Format eines von sicherheitspolitischen Experten getriebenen Prozesses mit Vernehmlassungsmöglichkeiten für Kantone und zugewandte Milizorte sowie Anhörungen im Parlament auch innerhalb eines Jahres durchführen. Insofern jeweils primär der Bedrohungsteil nachgeführt wird, könnte man diese kürzeren Berichte auch «Zwischenberichte» nennen – so wie 1979 der *Bericht 73* aktualisiert wurde.

Die Erfahrungen mit dem *Bericht 2016* haben einmal mehr bestätigt, dass auf der jeweiligen Konzeption entwickelte Reformprojekte auf der Ebene der sicherheitspolitischen Instrumente zu einem Zeitpunkt in die politischen Detailberatungen kommen, in dem der nächste Überarbeitungsprozess der sicherheitspolitischen Strategie wieder beginnen sollte.

Letztlich wären diese Routineberichte mit einem Fokus auf der internationalen Lage und den davon abgeleiteten Bedrohungen für die Schweiz aber kein Ersatz für strategische Gesamtkonzeptionen, wie sie insbesondere der *Bericht 73* und der *Bericht 2000* darstellten. Für Grundsatzberichte dieser Art sind konzeptionelle Klärungen nötig und der Fokus liegt auf der politischen Steuerung mithilfe zukunftsgerichteter strategischer Prioritäten. Umfassende strategische Konzeptionen als Grundlagen für politische Richtungsentscheide können allerdings nicht in jeder Legislatur erarbeitet werden. Die Erfahrungen mit dem *Bericht 2016* haben einmal mehr bestätigt, dass auf der jeweiligen Konzeption entwickelte Reformprojekte auf der Ebene der sicherheitspolitischen Instrumente zu einem

54 SIPOL-B 16, 108ff.
55 VBS, Ergebnisbericht, op. cit., 5.

Zeitpunkt in die politischen Detailberatungen kommen, in dem der nächste Überarbeitungsprozess der sicherheitspolitischen Strategie wieder beginnen sollte. Nicht zu Unrecht hat der Bundesrat 2014 befürchtet, dass derartige sich überlappende Prozesse sich gegenseitig behindern würden, weil sie in der Kommunikation mit dem Parlament und der Öffentlichkeit nur schwer auseinanderzuhalten wären.

Bevor in den nächsten Legislaturperioden neue Berichte angeschoben werden, sollte daher jeweils noch deutlicher geklärt werden, welche Zielsetzungen damit verfolgt werden sollen. Dabei gilt es zu fragen, ob primär eine Orientierungshilfe hinsichtlich Lage- und Bedrohungsanalyse gefragt ist, im Rahmen deren Erarbeitung sich die Akteure des Sicherheitsverbundes der Schweiz und das Parlament über die Bedeutung aktueller sicherheitspolitischer Entwicklungen austauschen können. Geht es hingegen darum, politische Grundsatzentscheide zur Neuorientierung der sicherheitspolitischen Strategie und Instrumente vorzubereiten, dann wird der Erarbeitungsprozess breiter abgestützt werden müssen und mehr Zeit in Anspruch nehmen. Im *Bericht 73* betonte der Bundesrat explizit, dass der Bericht künftige Entschlüsse zur Gewährleistung der Sicherheit der Schweiz «vorbereiten und erleichtern» solle und «verbindliche Richtpunkte für das Planen und Handeln» der einzelnen Instanzen setzen solle.[56] Der Boden für die damalige Kurskorrektur war allerdings – ähnlich wie mit der Kommission Brunner im Fall des *Berichts 2000* – bereits durch eine Expertenkommission und einen parallelen politischen Prozess vorbereitet worden. Es würde sich lohnen, die Rahmenbedingungen der Erarbeitung von Bedrohungsberichten respektive von strategischen Gesamtkonzeptionen transparenter voneinander abzugrenzen.

Andreas Wenger

Professor für internationale und schweizerische Sicherheitspolitik an der ETH Zürich und Direktor des Center for Security Studies (CSS) an der ETH Zürich (www.css.ethz.ch).
E-Mail: wenger@sipo.gess.ethz.ch

Christian Nünlist

Senior Researcher am Center for Security Studies (CSS) der ETH Zürich und Leiter des Teams «Swiss and Euro-Atlantic Security».
E-Mail: nuenlist@sipo.gess.ethz.ch

56 Bundesrat, *Bericht an die Bundesversammlung über die Sicherheitspolitik der Schweiz (Konzeption der Gesamtverteidigung)*, 27.6.1973, 115.

Trends in der Logistik machen vor der Logistikbasis der Armee nicht Halt

Wer hätte vor 15 Jahren gedacht, dass die Logistikbasis der Armee (LBA) bei einer WEMA (Wiedererstellung der Einsatzbereitschaft des Materials im Ausbildungsdienst) das Material mit Handhelds scannt und damit automatisch zurückbucht? Die Welt hat sich verändert – technologisch und gesellschaftlich - und die LBA mit ihr: vom Zeughaus zu einem modernen Logistikbetrieb. Welche Trends werden die LBA der Zukunft beeinflussen?

Thomas Kaiser, Emanuel von Wartburg

Megatrends und deren Auswirkung auf die LBA

Unsere Gesellschaft ist dauernd in Bewegung. Die heutige Gefahr ist vielleicht morgen schon eine andere. Täglich sind wir einer Flut von Informationen ausgesetzt, die sich manchmal sogar noch widersprechen. Was heute gilt, gilt vielleicht morgen nicht mehr. Sich in dieser Welt zurechtzufinden, bedeutet ständige Marktbeobachtung, Überprüfung und Neuausrichtung.

Globalisierung und Schnelllebigkeit / Diskontinuität

Die Welt wird ein Dorf. Als Beispiel werden die Kartoffeln in Deutschland geerntet, in der Ukraine gewaschen, in Griechenland geschält, in Holland frittiert, in Bulgarien verpackt und in der Schweiz gegessen. Die Distanzen zwischen der Produktion und dem Endkunden werden grösser. Neue Märkte und die Auslagerung der Produktion in Billiglohnländer fördern diesen Prozess und führen zu höheren Anforderungen an die Logistikleistungen. Dies beeinflusst die Beschaffungsquellen, die Produktionsstandorte und den Logistikprozess.

Der Preisdruck sowie die gesetzlichen Vorschriften (WTO) bedeuten für die LBA, dass vermehrt im Ausland beschafft werden muss. Somit ist die LBA abhängig von Transportwegen, die zu längeren Lieferfristen führen. Zudem muss für die Sicherstellung der Verfügbarkeit die Definition des minimalen Lagerbestands für jeden Artikel individuell hinterlegt werden.

«Das Phänomen der Globalisierung geht einher mit einem weiteren Phänomen, das sich als Diskontinuität bezeichnen lässt.»[1]

Diskontinuität kann für abrupte Entwicklungsänderungen stehen, die ohne Vorankündigung eintreten. Dies können zum Beispiel Umweltkatastrophen, Flüchtlingsströme, wirtschaftliche Einflüsse aber auch rasante technologische Entwicklungen sein. Die Weiterentwicklung der Armee, mit der Erhöhung der Bereitschaft, ist die Antwort auf die Diskontinuität. In den Armeelogistikcentern heisst das in Bezug auf die Mobilisierung konkret, dass zusammen mit den Logistikbataillonen über längere Zeit im Schichtbetrieb täglich zwei Bataillone ausgerüstet werden müssen.

Demografischer Wandel

Die zunehmende Überalterung hat dramatische Folgen für die Wirtschaft. Die grösste Herausforderung wird die Finanzierung des Ruhestands aus den Einkommen der nachfolgenden Generationen sein. Wir werden übers heutige Pensionsalter hinaus arbeiten müssen, was gleichzeitig einen Aufwuchs mit «digital natives» verunmöglicht. «Digital natives» ist die Generation, welche nach 1980 geboren worden und damit in der digitalen Welt aufgewachsen ist: Auch in der LBA müssen vermehrt ältere Mitarbeiter mit einer handwerklichen Ausbildung mit neuen Technologien arbeiten. Es entstehen laufend weitere Ausbildungsbedürfnisse und neue Berufsbilder. Das lebenslange Lernen ist eine Voraussetzung auf dem heutigen und künftigen Arbeitsmarkt. Die Herausforderung für die LBA und vergleichbarer Unternehmen wird sein, die Schulungsbedürfnisse eines 20jährigen mit denen eines 60jährigen unter einen Hut zu bringen.

Aufgrund der komplexen Systeme der Armee wird der Spezialisierungsgrad weiter zunehmen. Die Arbeiten in der Supply Chain werden immer mehr aufgeteilt werden müssen. Damit braucht es mehr und komplexeres Spezialwissen und gleichzeitig sind routinierte Generalisten mit einem breiten institutionellen Wissen gefragt.

1 Mühlecourt Thomas, Kontraktlogistik-Management, Grundlagen – Beispiele – Checklisten, 2012, Gabler Verlag / Springer Fachmedien Wiesbaden, Seite 2

Veränderung der Arbeitswelt

Der Geburtenrückgang und die älter werdende Gesellschaft vermindern längerfristig die Anzahl der Arbeitskräfte (insbesondere auch in Europa). Daher ist es zwingend nötig, dass Routineabläufe wie klassische Arbeiten im Lager automatisiert werden. Dies erfordert jedoch Investitionen in Informatik (Digitalisierung) und in entsprechende Infrastruktur. Die Losgrössen werden immer kleiner, der Bestellrhythmus wird erhöht. So haben sich die ehemaligen Zeughäuser zu Schmalganglagern und modernen Werkstätten gewandelt. Im Lager werden «Handhelds» für die Buchungen verwendet. Ein Logistiker findet heute bei der LBA die gleichen Arbeitsinstrumente und Abläufe vor wie in der Privatwirtschaft. Die Herausforderungen an die Mitarbeiter bestehen in der Vielzahl der verschiedenen Artikel mit zunehmend unterschiedlichen Lagervorschriften.

Urbanisierung

Gemäss Bundesamt für Statistik wird die Bevölkerung nicht aufgrund der Geburtstraten steigen, sondern die Migration wird die Anzahl Personen in der Schweiz erhöhen.[2] Dieser gesellschaftliche Wandel wird nicht ohne Folgen bleiben. Die Städte werden wachsen. Zu den grossen Herausforderungen der kommenden Jahrzehnte werden die Bereitstellung und Finanzierung der Infrastruktur gehören. Der ländliche Raum wird immer kleiner werden. Die Wohngebiete werden immer näher an die Armeelogistikcenter rücken. Dies erschwert oder verunmöglicht die nötigen Erweiterungen. Auch die Bodenpreise für Landreserven werden explodieren. Durch die Nähe zu Siedlungsgebieten und Strassen wird der QTNT-Wert[3] für die Lagerung von Munition herabgesetzt werden müssen. Dadurch wird mehr Lagerraum für die gleiche Anzahl Munition benötigt werden. Die Schaffung von neuem Lagerraum ist vor allem für Gefahrgut (Betriebsstoffe, Munition) in der Schweiz nur noch beschränkt möglich.

Neue Technologien

Neue Technologien entwickeln und verbreiten sich schneller als früher. Systeme, insbesondere auch jene der Armee, werden immer komplexer. Neue Technologien werden auch in der LBA überall dort eingesetzt, wo sie die Arbeitsabläufe vereinfachen, sofern sie finanzierbar sind.

Informationsgesellschaft

Digitalisierung

Digitale Medien prägen zunehmend unseren Alltag. Weltweit steigt die Anzahl der digitalen Endgeräte. Die Beschleunigung der Prozesse durch die Digitalisierung führt zu einem Spagat zu den Immobilienprozessen. Die Planung und der Bau von Immobilien dauert seine Zeit und die Gebäude stehen in der Regel 30 – 50 Jahre zur Verfügung. In der digitalen Welt ist was heute angesagt ist, morgen bereits veraltet. Die Verbindungen dieser gegensätzlichen Eigenschaften stellt für die LBA eine Herausforderung dar. Es sind umfangreiche Risikoabklärungen notwendig, damit die Leistungserbringung der LBA bei allfälligem Einsatz solcher Technologien durch eine Gegenseite beispielsweise nicht durch elektromagnetische Störung oder Cyberattacken gestört oder gar verhindert werden kann. Nur schon ein simpler Stromausfall erschwert den Zugriff auf die Daten. Dies erfordert von der LBA die Sicherstellung von Rückfallebenen, um bei einem Ausfall neuer Technologie trotzdem handlungsfähig zu bleiben. Darum wird unter anderem das Material für Miliz mit hoher Bereitschaft separat und nach Einheit eingelagert, um bei einem Informatiksystem-Ausfall trotzdem in der Lage zu sein, der Truppe rasch Material zur Verfügung zu stellen. Weiter sichern aktuelle Lagerspiegel die Übersicht, falls der Zugriff auf die aktiven Systeme nicht mehr oder nur eingeschränkt möglich wäre.

Big Data

Aufgrund der stetig wachsenden Datenflut ist ein gut funktionierendes IT-System einer der Schlüsselfaktoren für den Erfolg eines Unternehmens. Die elektronische Kommunikation zwischen den Systemen ist dabei ein wichtiger Faktor. Die Schnittstellen zwischen Unternehmen werden aufgehoben, die Daten «fliessen» durch die gesamte Supply Chain. Dies trifft jedoch nicht nur auf die «guten» Daten zu. Dies bedeutet, dass erhöhte Sicherheitsanforderungen in der Supply Chain zwingend notwendig sind und werden. Die Integrität der Mitarbeitenden und der Geschäftspartner muss überprüft werden. So muss die LBA sicherstellen, dass bei einer Revision eines Gerätes keine klassifizierten Daten abfliessen, die in falsche Hände gelangen könnten. Die Logistikbasis der Armee muss ständig über aktuelle und zuverlässige logistischen Daten verfügen, um die logistische Lage zu beurteilen und die entsprechenden Massnahmen ableiten zu können. Zur Gewährleistung der Datensicherheit müssen die Daten in sogenannten Rückfallebenen redundant vorhanden sein, falls die aktuellen Datenbanken nicht zugänglich sind oder korrumpiert wurden. Vor diesem Hintergrund finden bei der LBA periodisch Übungen statt, die den Ausfall des Informatiksystems beinhalten.

Mobilität

Der Verkehr wird auch in Zukunft zunehmen, während der zur Verfügung stehende Raum immer kleiner wird. Trotz neuer Technologien und Verkehrskonzepten wird man beim Strassen- wie beim Schienennetz nicht um den Ausbau herumkommen. Die Herausforderung wird neben dem eingeschränkten Raumangebot bei der Finanzierung liegen. Die Gelder der öffentlichen Hand werden knapper. In Zeiten wachsender Produktion und des Transports immer kleinerer Losgrössen (Stichwort E-Commerce) sind die Fertigungs- und Vertriebszeiten von der Leistungskraft und Flexibilität der Transportlogistik abhängig. Die Lastwagenfahrten während der Hauptverkehrszeiten dauern aufgrund der Staus immer länger. Die Überlastung der Verkehrsinfrastruktur auf der Strasse wird noch mehr Bahntransporte zwischen den Armeelogistikcentern erfordern.

Struktur- und Prozessorientierung

Der technologische Wandel, die weltpolitische Lage und die daraus resultierenden veränderten Anforderungen an die Armee und somit an die Logistikbasis der Armee füh-

2 Bundesamt für Statistik, Szenarien zur Bevölkerungsentwicklung der Schweiz, 2015 – 2045, 2015, Herausgeber Bundesamt für Statistik, Neuchâtel, Seite 5

3 Quotient Trinitrotoluol. Das TNT-Äquivalent wird zur Angabe der Sprengkraft von militärischen Waffen, industriellen Sprengstoffen sowie anderen Sprengkörpern verwendet.

Die erhöhten Bereitschaftsvorgaben der WEA sind die Herausforderung für die LBA. Trotz des massiven Einsatzes von Technik braucht es immer noch Menschen zur Leistungserbringung. Die Zusammenarbeit zwischen Mitarbeitern der LBA und der Truppe wird in Zukunft noch wichtiger. (VBS / DDPS)

Schmalganglager, wie sie in der privaten Logistik Standard sind, werden auch in der LBA verwendet. In allen fünf Armeelogistikcentern steht eines im Einsatz / oder noch im Bau. Hier das SGL im ALC Othmarsingen. (VBS / DDPS)

ren dazu, dass sich die Prozesse verändern. Lange Zeit galten die Logistik und insbesondere die Logistik der Armee als eine Branche, die sich nicht automatisieren lässt. Weil sich eben die Armeelogistik in einem wesentlichen Teil von der zivilen Logistik unterscheidet: Sie stellt Ware bereit und nimmt sie schon wenige Wochen später wieder zurück. Dahinter steckt viel Handarbeit, wie zum Beispiel Kontrollen, Instandhaltung, Reinigung. Doch auch bei der LBA werden die Lager immer mehr automatisiert. So ist das Armeeverteilzentrum vollautomatisch, im Textilcenter in Thun wird die Wäsche automatisch gewaschen und künftig werden vollautomatische Containerlager gebaut werden.

Diversifizierung und Privatisierung

Die ehemaligen Bundesbetriebe RUAG, SBB, Schweizer Post, Swisscom wurden in den vergangen Jahren in Aktiengesellschaften umgewandelt. Der Bund ist teilweise 100 % (z. B. RUAG) oder Mehrheits-Aktionär (z. B. Swisscom). Ob und wie die Armee Leistungen auf den Privatsektor auslagern wird, ist letztlich eine politische Frage. Wie bereits erwähnt, werden die Systeme immer komplexer, der Ausbildungsaufwand dafür immer grösser. Fachleute sind im Arbeitsmarkt Mangelware und der Spardruck wird nicht kleiner. So wird die LBA auch in Zukunft gezwungen sein, einzelne Prozessschritte an private Firmen auszulagern. Dabei wird zwischen sicherheitsrelevanten Kernkompetenzen und gängigem Markt unterschieden. Die LBA muss all jene Fertigkeiten eigenständig erhalten, die im Rahmen eines Einsatzes aus dem Stand heraus und in jeder Lage gefordert sind. Eine autonome Logistik ist je nach Ereignis erfolgsrelevant. Werden Leistungen eingekauft, muss die Führung dieser Leistungserbringung immer in der Hand der LBA bleiben. Vertraglich werden alle Eventualitäten verbindlich festgelegt. Die Instandhaltung der LBA hat sich in den letzten Jahren auf die Anforderungen der neuen Systeme der Armee ausgerichtet. Vor dem Hintergrund der eigenständigen Leistungserbringung sind einige Spezialwerkstätten entstanden.

Trends im Gesundheitssektor – der Gesundheitsmarkt als einer der wichtigsten Zukunftsmärkte

Gesundheit ist nicht mehr nur das Gegenteil von Krankheit, sondern wird zunehmend umfassender verstanden. Gesundheit beinhaltet neben dem physischem auch das psychische, das mentale und das soziale Wohlergehen. Die Grenzen zu Fitness-, Wellness und Lifestyle-Angeboten sind bereits heute fliessend. Neben der Erforschung von Krankheit nimmt die Erforschung von Gesundheit immer mehr an Bedeutung zu. Diese Trends und Entwicklungen führen zu vermehrtem Bedarf an Humankapital (Ärzte, Pflegefachpersonen; quantitativer und qualitativer Aspekt) und damit auch zu vermehrten Kosten. Eine kostenoptimierte «Just in time» – Logistik könnte zu Engpässen im Bereich der militärischen und zivilen Gesundheitsversorgung (Engpässe bei Medikamenten, Impfstoffen und weiteren pharmazeutischen Produkten) führen. Dies erfordert gerade auch im sanitätsdienstlichen und logistischen Bereich vorsorgliche Massnahmen (Bevorratung) auf der Basis der Risikobereitschaft der Entscheidungsträger bzw. der verantwortlichen Institutionen auf Stufe Bundesrat und in der Armee. In Notlagen (Medikamentenengpässe, Impfstoffe, Massenanfall bei Epidemien, Katastrophen etc.) muss der Sanitätsdienst der Armee (Formationen, Berufsorganisation und Armeeapotheke) rasch einsatzfähig sein und bildet somit auch in Zukunft das Sicherheitsdepot für die pharmazeutische Versorgung der Schweizer Bevölkerung.

Zusammenfassung und Ausblick

Die beschriebenen Trends stellen eine nicht abschliessende Auswahl dar. Die Trends lassen sich teilweise nicht klar voneinander abgrenzen. Der Zeitraum beeinflusst die Inhalte. Es gelten allenfalls andere Megatrends für die kommenden fünf Jahre als wenn der Zeithorizont auf zehn oder zwanzig Jahre erweitert wird. Sicher ist, dass wir in einer Welt leben, die komplex und weitgehend unvorhersehbar ist. Unsicherheit gehört zu unserem Leben. Deshalb ist es wichtig, auf das Unvorhersehbare

Die immense Datenmenge in der Logistik kann heute nur noch mit Unterstützung durch IT-Systeme bearbeitet werden. Im Bild LBA-Mitarbeiter bei der Evaluation neuer Handhelds. (VBS / DDPS)

Viele logistische Prozesse erforderten bis vor wenigen Jahren viel Handarbeit und damit Personal. Mittlerweile hilft die Automatisierung Stellen einzusparen. Im Bild die teilweise automatisierte Wäscherei des Textilcenters Thun. (VBS / DDPS)

bare vorbereitet zu sein und in Varianten zu denken. Die LBA ist der Meinung, dass die Technologie (Digitalisierung eingeschlossen), das Humankapital (inklusive Aus- und Weiterbildung) und die Finanzen grossen Einfluss auf das zukünftige Geschäftsmodell der LBA haben werden. Die LBA kann und will sich den Trends nicht verschliessen. Sie muss und wird sich ständig weiterentwickeln. Seit einigen Monaten beschäftigen sich unsere Spezialisten mit der Logistikstrategie 2030. Darin wird bewusst auch in scheinbar unmöglichen Modellen gedacht. Für die konkrete Umsetzung ist es jedoch sinnlos, gefährlich und teuer, sofort und als Vorreiter auf jeden Trend aufzuspringen. Die LBA muss ihre Leistung robust und in allen Lagen verlässlich erbringen. Trends sind in der Natur der Sache bei Beginn noch nicht ausgereift. Einen Trend nicht zu verschlafen, die Augen offen zu halten und rechtzeitig einzusteigen, diese Kunst galt in der Vergangenheit und gilt auch in Zukunft.

Thomas Kaiser

Divisionär, Chef Logistikbasis der Armee
Armeeführungsmitglied
www.logistikbasis.ch
LBA.LKZ@vtg.admin.ch

Emanuel von Wartburg

Dr. sc. ETH Zürich, Dipl. Phys. ETH
Chef Unternehmensentwicklung LBA
www.logistikbasis.ch
LBA.LKZ@vtg.admin.ch

Resilienz – eine Bestandsaufnahme

Wenn von der immer komplexer und unsicherer werdenden Welt und den damit verbundenen Herausforderungen an Individuen, Gruppen, Unternehmen oder gar Nationen die Rede ist, kommt man am Begriff der Resilienz nicht mehr vorbei. Auf der individuellen Ebene wird darunter die psychische Widerstandskraft verstanden, die nicht zuletzt auch für Armeeangehörige von zunehmender Bedeutung ist. Das Wissen über Resilienz kann für die Personalselektion sowie für zielgerichtete Trainings genutzt werden, wobei beides nur in einer passenden Kultur die gewünschte Wirkung entfalten wird. Wenn eine Armee die vorhandenen Humanressourcen auftragszentriert und menschenorientiert nutzen will, ist die Auseinandersetzung mit den relevanten Aspekten der Resilienz in Theorie und Praxis unabdingbar.

Logo des Comprehensive Soldier Fitness Programms mit seinen fünf Elementen. (U.S. Army)

Hubert Annen

Resilienz, allgemein verstanden als die *Fähigkeit von Individuen oder Systemen, erfolgreich mit belastenden Situationen umzugehen,* ist in letzter Zeit zu einem schon beinahe inflationär verwendeten Schlagwort geworden. Das ist insofern nicht überraschend, als einerseits die Herausforderungen im täglichen Leben, sei es am Arbeitsplatz oder im Privatleben, zunehmend anspruchsvoller und komplexer werden, und andererseits wird man ununterbrochen mit Medienberichten über Unfälle, Kriminaltaten, Terrorattacken und andere bedrohliche Situationen wie Naturkatastrophen konfrontiert. Vor diesem Hintergrund findet ein psychologisches Konstrukt, dass eine Antwort auf diese unvorhersehbare und oft gefährliche Welt verspricht, natürlich einen guten Nährboden. Aber so willkommen dies auch sein mag, Resilienz ist nicht das Wundermittel, mit dem sich eine Lösung für jede Herausforderung oder Bedrohung herbeizaubern lässt. Allerdings bildet das Wissen über Resilienz in vielen Fällen eine solide Basis für die Lösungsfindung, gibt die Richtung für positive Entwicklungen an und liefert Hilfsmittel für das konkrete Vorgehen. Dementsprechend ist es angezeigt, das Konstrukt umfassend zu verstehen und durch dieses Verständnis eine gute Ausgangslage für die Umsetzung des Wissens zu schaffen. Das heisst für den vorliegenden Beitrag, die theoretischen Grundlagen zu analysieren, die Ergebnisse aus bisheriger und aktueller Forschung zu betrachten sowie Chancen und Gefahren auf dem Weg zur Anwendung zu erörtern. Konkret werden dabei die wesentlichen Aspekte der Resilienz als Persönlichkeitsmerkmal beleuchtet, die Möglichkeiten und Grenzen des Resilienztrainings aufgezeigt und schliesslich die Bedeutung eines resilienzfördernden Umfelds hervorgehoben.

Ein kurzer Blick zurück

In Bezug auf den mentalen Zustand beziehungsweise die psychische Gesundheit von Menschen war ursprünglich eine pathogene Sichtweise dominierend. Man beschäftigte sich vornehmlich damit, wie psychische Krankheiten entstehen, wie sie erkannt und wie sie geheilt werden können. Zentrale Fragen stellten sich folglich zu den Risikofaktoren, zur Anfälligkeit und zu den passenden Therapien. Diese Theorien und Modelle zum Auftreten und zur Behandlung psychischer Erkrankungen trugen indes nicht der Tatsache Rechnung, dass die allermeisten Personen und damit auch solche, die belastende Situationen erleben oder sich in einem ungünstigen Umfeld befinden, gesund sind und bleiben. Erst in den sechziger Jahren des letzten Jahrhunderts wurde dieser einseitigen pathogenen Betrachtungsweise der Begriff Salutogenese – die Entstehung der Gesundheit[1] – gegenübergestellt, und mit den Arbeiten von Emmy Werner in den frühen siebziger Jahren[2] tauchte das Konzept der Resilienz häufiger in der einschlägigen psychologischen Literatur auf.

Antonovskys Betrachtungen und Einsichten basierten zu weiten Teilen auf Berichten zu Überlebenden des Holocausts, die ihre äusserst traumatisierenden Erlebnisse offenbar hatten verarbeiten können und wieder ein normales und gesundes Leben führten. Werners Forschung beschäftigte sich mit Kindern, die unter grosser Armut und in einem schwer belastenden sozialen Umfeld aufwuchsen. Sie fand heraus, dass mindestens ein Drittel dieser Kinder die ungünstigen Bedingungen überwanden und eine normale, erfolgreiche Entwicklung durchliefen. Werner bezeichnete diese Kinder als resilient.

1 Antonovsky, 1979
2 Werner, Bierman, & French, 1971

Die auf diesen Grundlagen aufbauende Forschung trug dazu bei, zuerst mal den Begriff der Resilienz einzugrenzen und mit der Metapher «zurückprallen» («bounce back») zu illustrieren – also die Fähigkeit, sich an herausfordernde, belastende oder gar gefährliche Umstände und Lebensereignisse anzupassen und trotz der damit verbundenen Unsicherheiten oder gar Furcht weiter seinen Weg zu gehen. Überdies konnte gezeigt werden, dass dies mehr die Regel als die Ausnahme darstellt[3] – oder wie es Masten mit seiner Metapher auf den Punkt bringt: «ordinary magic»[4]. Nun stellt sich natürlich die Frage, welches denn die Komponenten dieses «gewöhnlichen Zaubers» sind, um sie auch im Alltag erkennen und nutzen zu können.

Eine genauere Betrachtung

Zuerst gilt es festzuhalten, dass der Begriff Resilienz in Bezug auf verschiedene Ebenen, also vom Individuum über Gruppen bis hin zu Organisationen, Gemeinden oder ganzen Nationen verwendet wird; zudem lässt er sich auf unterschiedliche Bereiche wie beispielsweise die Umwelt oder die Wirtschaftslage anwenden.[5] Im vorliegenden Beitrag wird der Fokus ausschliesslich auf die p*sychologische Resilienz* auf der *individuellen Ebene* gerichtet. Aber selbst wenn man das Feld derart stark eingrenzt, finden sich in der betreffenden Literatur zahlreiche, auf die Resilienz bezogene Faktoren, was es nicht einfach macht, sich ein einheitliches Bild zu verschaffen.

Im Rahmen einer RAND-Studie wurde die wissenschaftliche Literatur zur psychologischen Resilienz systematisch gesichtet.[6] Aus 270 Publikationen wurden deren zwanzig Faktoren identifiziert, die sich der Resilienz zuordnen liessen. Aus diesen wiederum fielen deren sieben unter das Label der individuellen Resilienz: positives Coping (Stressbewältigung), positive Gestimmtheit, positives Denken, Realismus, Verhaltenskontrolle, physische Fitness und Selbstlosigkeit. Eine aktuellere Übersichtsstudie nennt Selbstwirksamkeit, Optimismus, soziale Ressourcen und kognitive (gedankliche) Einschätzung und Bewältigung als psychosoziale Faktoren, welche die Entwicklung von Resilienz begünstigen.[7] Aus einer praxisorientierten Perspektive führt die American Psychological Association vier relevante Faktoren auf: die Fähigkeit, realistische Pläne zu machen und Schritte zu deren Ausführung zu unternehmen; eine positive Sicht auf sich selber und das Vertrauen in die eigenen Stärken; Kommunikations- und Problemlösekompetenzen; sowie die Fähigkeit, mit starken Gefühlen und Impulsen umgehen zu können.[8]

Bevor es endgültig unübersichtlich wird, soll nun aber die Essenz dieser drei Quellen herausgelöst werden:

- Erstens machen sie klar, dass es ein gewisses Mass an Intelligenz bzw. *kognitiven Fähigkeiten* braucht, um den Kern eines Problems zu erkennen und daraus die wesentlichen Schritte in Richtung einer Lösung abzuleiten;
- *Optimismus* ist ein zweites, unabdingbares Element, um diese Schritte überhaupt in Angriff nehmen zu wollen, wozu auch das notwendige Vertrauen in die eigenen Fähigkeiten und Fertigkeiten gehört;
- drittens gehen solche Prozesse normalerweise einher mit intensiven *Emotionen,* die es neu einzuschätzen und zu *regulieren* gilt;
- und schliesslich bedingt die Bewältigung von grossen Herausforderungen ein gewisses Mass an sozialer Unterstützung, also muss die betroffene Person über ein soziales Netzwerk und die *kommunikativen* und *sozialen Kompetenzen* verfügen, dieses zu aktivieren.

Stress entsteht dann, wenn die Person den Stressor als relevant einstuft und ein Ungleichgewicht besteht zwischen den betreffenden Anforderungen und den eigenen Ressourcen, diese Anforderungen zu bewältigen.

Von den Bezügen zu und Überschneidungen mit anderen vergleichbaren Konzepten ist die offensichtlichste Verbindung jene zum *Transaktionalen Stressmodell.*[9] Hier wird davon ausgegangen, dass die Reaktion auf externe Stressfaktoren von Gedanken und Bewertungen einer Person in der jeweiligen Situation abhängt. Stress entsteht dann, wenn die Person den Stressor als relevant einstuft und ein Ungleichgewicht besteht zwischen den betreffenden Anforderungen und den eigenen Ressourcen, diese Anforderungen zu bewältigen. Nun ist es so, dass die Wahrnehmung der Anforderungen und der Ressourcen in der Regel auf subjektiven Einschätzungen beruht, die unter anderem von der aktuellen Befindlichkeit sowie von individuellen Persönlichkeitsmerkmalen abhängen. So wirkt eine kurz bevorstehende Prüfung bedrohlicher, wenn man schlecht vorbereitet ist, zur gleichen Zeit noch weitere Probleme zu bewältigen hat oder sich gerade erst von einer schweren Grippe erholt hat; ebenso eine Rolle spielen positive oder negative Vorerfahrungen mit vergleichbaren Situationen; und schliesslich nehmen von Natur aus ängstliche Personen eine Herausforderung anders wahr als solche, die über eine grundsätzlich zuversichtliche Einstellung verfügen. Beim Transaktionalen Stressmodell geht es also um die Bewertung eines Stressors und wie sich diese auf die Lösungsstrategien auswirkt. Überlappungen mit dem Konzept der Resilienz gibt es somit vor allem in Bezug auf Stressbewältigungstechniken wie kognitive Neubewertung oder Problemlösungsstrategien, die auch in Resilienztrainings geübt werden. Die Resilienz geht aber über den Moment hinaus, sie ist vorwärtsgerichtet und bezieht sich im Allgemeinen mehr auf das Wohlbefinden und die Kompetenzen, um für die zukünftigen Stressoren und deren potenziellen negativen Folgen gerüstet zu sein.

Ebenfalls verwandt mit dem Konzept der Resilienz ist der so genannte *Kohärenzsinn* (sense of coherence, SOC). Hier geht es darum, ob die Welt als verständlich, überschaubar und sinnvoll wahrgenommen wird.[10] Konfrontiert mit einem Stressor wird eine Person mit ausgeprägtem Kohä-

3 Meichenbaum, 2013
4 Masten, 2001
5 Vgl. dazu Lucini, 2014; Masten & Obradovic, 2008; Soucek, Ziegler, Schlett, & Pauls, 2016
6 Meredith et al., 2011
7 Vanhove, Herian, Perez, Harms, & Lester, 2015
8 American Psychological Association, online
9 Vgl. Lazarus & Folkman, 1984
10 Antonovsky, 1996

renzsinn grundsätzlich motiviert sein, diesen bewältigen zu wollen, weil sie daran glaubt, dass die betreffende Herausforderung einen Sinn hat, und sie der Überzeugung ist, über genügend persönliche Stärken zur Überwindung der stressreichen Situation zu verfügen. Man kann auch sagen, dass der Kohärenzsinn gewissermassen die Operationalisierung des salutogenetischen Ansatzes darstellt.

Und letztlich kann Resilienz auch als Ausdruck der – mehr oder weniger – bewussten Anwendung der Positiven Psychologie im Umgang mit ungünstigen oder bedrohlichen Situationen betrachtet werden. So werden in Resilienztrainings das Erkennen und Nutzen individueller Stärken betont, das kognitive Umstrukturieren stressauslösender Situationen und damit verbundener Überzeugungen erlernt sowie die Anwendung konstruktiver und positiver Kommunikationsstile geübt[11] – alles Elemente notabene, die eng mit den theoretischen Grundlagen der Positiven Psychologie verknüpft sind.

Es existiert eine umfangreiche, um nicht zu sagen unüberschaubare Literatur über Resilienz und deren Elemente. Ausserdem gibt es inhaltliche Überschneidungen mit diversen anderen etablierten Konzepten. Als Zwischenfazit und Orientierung kann an dieser Stelle festgehalten werden, dass der salutogenetische Ansatz als ideologische Orientierung, in der sich der Wandel von «fix what's wrong» zu «build what's strong» widerspiegelt, dient; Resilienzprogramme dementsprechend vor allem auf die Prävention ausgerichtet sind; und die Positive Psychologe das theoretische Fundament für die Resilienztrainings liefert.

Wenn nun im folgenden Abschnitt noch detaillierter auf die Resilienz als Persönlichkeitsmerkmal und die psychometrischen Instrumente zu deren Einschätzung eingegangen wird, ergeben sich gleichzeitig vertieftere Kenntnisse zu den massgebenden Faktoren von Resilienz und wie man sie erkennen und einschätzen kann.

Resilienz als Veranlagung

Obschon Resilienz die Anpassung an Herausforderungen und damit einen dynamischen Prozess betont, wird sie häufig auch als stabile Persönlichkeitseigenschaft thematisiert.[12] Die Betrachtung der Resilienz als spezifische Persönlichkeitsdisposition geht auf die oben erwähnten Arbeiten von *Werner* und *Antonovsky* zurück.[13] Der Vorteil dieser Herangehensweise besteht darin, dass man dadurch Resilienz wie andere etablierte Persönlichkeitseigenschaften klassifizieren und mit bewährten Methoden der Persönlichkeitspsychologie operationalisieren kann.[14] Folglich gibt es diverse Studien, die eine genetische Veranlagung zu Resilienz postulieren und obwohl das Auftreten resilienten Handelns damit nicht vollständig erklärt wird, kann zumindest davon ausgegangen werden, dass Personen diesbezüglich ein unterschiedliches Potenzial aufweisen.

Angesichts dieser Annahme ergibt es insbesondere in Organisationen mit hohen Anforderungen an Sicherheit und Zuverlässigkeit (z. B. Spitäler, Polizei, Feuerwehr, Flugüberwachung, Atomkraftwerke, Militär) Sinn, im Rahmen der Personalselektion auch die Resilienz zu messen. Es ist dementsprechend nicht überraschend, dass beträchtliche Anstrengungen unternommen werden, um Attribute, die zum Wohlbefinden und zu hoher Arbeitsleistung selbst unter schwierigsten Bedingungen beitragen, zu erfassen und einzuschätzen. Die betreffenden Faktoren werden normalerweise als unabhängige Variablen oder Prädiktoren einer abhängigen Variable, die für eine erfolgreiche Anpassung steht, betrachtet.[15]

Angesichts dieser Annahme ergibt es insbesondere in Organisationen mit hohen Anforderungen an Sicherheit und Zuverlässigkeit (z. B. Spitäler, Polizei, Feuerwehr, Flugüberwachung, Atomkraftwerke, Militär) Sinn, im Rahmen der Personalselektion auch die Resilienz zu messen.

Mit dem Ziel, brauchbare Masse und Skalen für Resilienz zu identifizieren, deren psychometrische Qualität einzuschätzen und daraus Folgerungen für die Theorie und Praxis abzuleiten, wurde kürzlich eine umfassende Sichtung der vorhandenen Instrumente durchgeführt.[16] Die Analyse zahlreicher wissenschaftlicher Publikationen führte fünfzehn Fragebogen zu Tage, die in der Praxis oder zu Forschungszwecken angewendet werden. Keines dieser Messinstrumente vermochte jedoch hinsichtlich relevanter Qualitätskriterien vollumfänglich zu überzeugen. Es fällt somit schwer, generelle Empfehlungen abzugeben, welche Resilienzskalen verwenden werden können resp. sollen. Für potenzielle Anwender bedeutet das, dass man sich klar darüber sein muss, in welchem Kontext und wofür man das Instrument einsetzen will, um dann jenes auszuwählen, welches den eigenen Inhalten und Zielsetzungen am nächsten kommt.

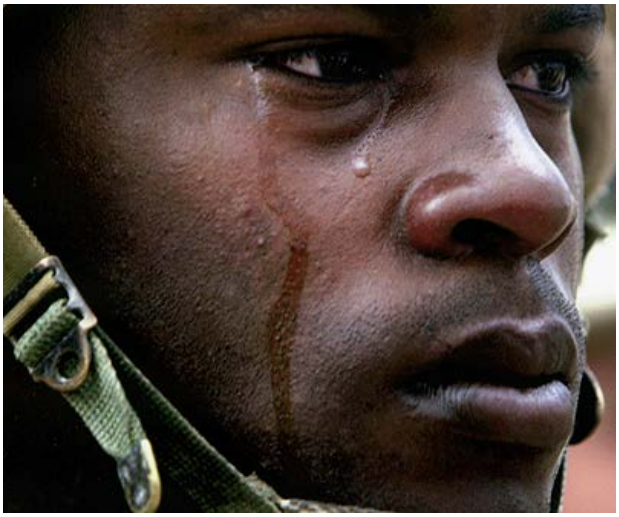
... werden mit 25 Fragen (Items) die fünf Persönlichkeitsmerkmale Gelassenheit, Durchhaltevermögen, Sinngebung, Selbständigkeit und Einsamkeit erfasst.

Im Rahmen diverser, auch in der Schweizer Armee durchgeführten Untersuchungen hat sich die so genannte Resilience Scale (RS)[17] schon mehrfach bewährt. In ihrer ursprünglichen Version werden mit 25 Fragen (Items) die fünf Persönlichkeitsmerkmale Gelassenheit, Durchhaltevermögen, Sinngebung, Selbständigkeit und Einsamkeit erfasst. Weiterführende Analysen zeigten jedoch eine zweidimensionale Struktur, bestehend aus persönlichen Kompetenzen und dem Akzeptieren von sich selbst und seinem Leben. Die deutsche Version des RS besteht sogar

11 Vgl. Reivich & Shatté, 2003
12 Pangallo, Zibarras, Lewis & Flaxman, 2015
13 Vgl. Werner, 1971, und Antonovsky, 1979
14 Schumacher, Leppert, Gunzelmann, Strauss, & Brähler, 2004
15 King & King, 2013
16 Windle, Bennett, & Noyes, 2011
17 Wagnild & Young, 1993

nur aus einem Faktor[18], was schliesslich in eine aus 11 Items bestehende Kurzversion mündete (RS-11). Die RS-11-Skala bewährte sich als zuverlässiges, valides und vor allem ökonomisches Instrument, um psychologische Resilienz als Persönlichkeitsmerkmal zu messen. Als solches ist es im deutschsprachigen Raum weit verbreitet. In der Schweizer Armee wurde es im Rahmen einer umfassenden Studie zu den Belastungen in der militärischen Grundausbildung[19] eingesetzt und zeigte sich unter anderem als bedeutendster psychologischer Prädiktor von wesentlichen Leistungsmerkmalen in der Rekrutenschule.[20]

... resiliente Personen weisen grundsätzlich überdurchschnittlich hohe Werte im Fünf-Faktoren Modell (FFM) der Persönlichkeit, bestehend aus Emotionaler Stabilität, Verträglichkeit, Gewissenhaftigkeit, Extraversion und Offenheit für Erfahrungen, auf.



Der resiliente Soldat ist nicht unberührbar, aber kann Schicksalsschläge verarbeiten. (Psychology Today)

Alle Resilienzskalen haben gemeinsam, dass sie eine Reihe mehrheitlich allgemeiner Persönlichkeitsmerkmale und sozialer Kompetenzen, die für Resilienz stehen und resilientes Handeln begünstigen, zu erfassen versuchen. Aus wissenschaftlicher Perspektive stellt sich demzufolge die Frage, ob man überhaupt Resilienz misst oder nicht ein anderes, gewissermassen verstecktes Konstrukt erfasst. So wurde beispielsweise in einer Studie gezeigt, dass resiliente Personen grundsätzlich überdurchschnittlich hohe Werte im Fünf-Faktoren Modell (FFM)[21] der Persönlichkeit, bestehend aus Emotionaler Stabilität, Verträglichkeit, Gewissenhaftigkeit, Extraversion und Offenheit für Erfahrungen, aufwiesen.[22] In einer anderen Untersuchung offenbarte sich, dass das Fünf-Faktoren Modell einen höheren Erklärungswert hinsichtlich des adaptiven Verhaltens von Adoleszenten hat als bestimmte Resilienzskalen.[23] Folglich bleibt offen, inwiefern Resilienz nicht schon mit bewährten Faktoren aus eher generell orientierten Persönlichkeitsfragebogen eingeschätzt werden kann oder ob es eigens dafür konstruierte Instrumente wie eine Resilienzskala braucht.

Selbst wenn obige Ausführungen etwas gar fachspezifisch ausgefallen sind, sollte deutlich geworden sein, dass die Betrachtung der Resilienz als Persönlichkeitsdisposition durchaus Sinn ergibt sowie Praxisrelevanz besitzt. Dennoch ist es insgesamt weder ein einfach zu fassendes noch statisches Konstrukt. So kann die gleiche Person in einem Lebensbereich (z. B. Arbeit) resilient und in einem anderen (z. B. Familie) verletzlich sein, auch dürfte das Ausmass der Resilienz in bestimmten Lebensphasen (z. B. Adoleszenz verglichen mit mittlerem Alter) unterschiedlich ausgeprägt sein, oder die Reaktion kann auf eine bestimmte traumatisierende Situation anders ausfallen als auf eine andere.[24] Deshalb muss der Anwendungsbereich von entsprechenden Messinstrumenten klar definiert werden, ausserdem gilt es den individuellen Verlauf in Bezug auf bestimmte Merkmale in Betracht zu ziehen. Es lohnt sich also auch, die Resilienz im Rahmen der individuellen Entwicklung eines Menschen zu beobachten und zu quantifizieren.[25]

... Erfahrungsberichte zeigen indes, dass sich Personen während oder nach herausfordernden, stressreichen oder gar traumatischen Erfahrungen sogar positiv entwickeln, gewissermassen daran wachsen können.

Insgesamt lässt sich angesichts des Forschungsstands festhalten, dass Resilienz auf einer gewissen individuellen Disposition beruht. Zahlreiche Studien sowie Erfahrungsberichte[26] zeigen indes, dass sich Personen während oder nach herausfordernden, stressreichen oder gar traumatischen Erfahrungen sogar positiv entwickeln, gewissermassen daran wachsen können. Es ist klar, dass Individuen unterschiedliche Startpositionen haben, wenn sie mit bestimmten Herausforderungen oder Bedrohungen zurecht kommen müssen, aber diese Ausgangslage ist nicht in Stein gemeisselt, die betreffenden Fähigkeiten können entwickelt werden und dieser Entwicklungsprozess lässt sich mit spezifischen Trainingsmethoden beschleunigen und verstärken.

18 Schumacher et al., 2004
19 PROGRESS; Wyss & Annen, 2011
20 Niederhauser, Huber & Annen, 2016
21 Costa & McCrae, 1992
22 Robins, John, Caspi, Moffitt & Stouthamber-Loeber, 2011
23 Waaktar & Torgersen, 2010
24 Masten, 2001
25 King & King, 2013
26 Vgl. Reivich & Shatté, 2003

Ready and Resilient Kampagne der U.S. Army. (U.S. Army)

Resilienz kann trainiert werden

In den letzten Jahren haben Unternehmungen zunehmend Resilienztrainings zur Prävention von Absentismus, kontraproduktivem Verhalten, Burnout und anderen stressbedingten Folgen eingeführt. Aktuell macht es jedoch den Anschein, als würden Aufwand und Ertrag in einem Missverhältnis stehen, denn auf der Basis der vorhandenen wissenschaftlichen Literatur zur Evaluation solcher Programme scheint der allgemeine Effekt relativ gering zu sein.[27] Angewandt auf eine grosse Anzahl Personen können aber selbst kleine Effekte zu einem bedeutsamen ökonomischen und sozialen Nutzen führen. Dementsprechend dient das Comprehensive Soldier and Familiy Fitness-Programm (CSF2) der U.S. Army[28], das gemäss unserem Wissen das grösste Projekt dieser Art ist, als gutes Beispiel für die kennzeichnenden Aspekte eines Resilienztrainings.

Vor allem sollen sie zentrale Kompetenzen der Resilienz wie Selbstbewusstsein und -reflexion, Selbstregulation, Optimismus, mentale Beweglichkeit, Charakterstärken und Kommunikation thematisieren und verbessern helfen.

CSF2 besteht aus drei Elementen. Das erste ist das so genannte Global Assessment Tool (GAT), ein eigens entwickeltes psychologisches Messinstrument, das online bearbeitet werden kann und auf effiziente Weise vier Dimensionen der psychologischen Fitness (Emotionen, Soziales, Familie, Spiritualität) erfasst.[29] Armeeangehörige erhalten nach Ausfüllen des Online-Tests ein individualisiertes Feedback mit Verbesserungshinweisen. Hier setzt das zweite Element des Programms an: Basierend auf den zuvor mit dem GAT identifizierten persönlichen Stärken wird den Soldaten eine gezielte Auswahl konkreter Vorschläge, in welche Richtung und mit welchen Methoden sie sich weiterentwickeln können, präsentiert. Die dritte Säule von CSF2 ist die Ausbildung und der Einsatz der Master Resilience Trainer (Master Resilience Training, MRT). Das sind in der Regel Unteroffiziere, die in einem zehntägigen, intensiven Kurs darauf vorbereitet werden, Wissen und Übungsmöglichkeiten zur Resilienz in ihren Einheiten zu verbreiten. Vor allem sollen sie zentrale Kompetenzen der Resilienz wie Selbstbewusstsein und –reflexion, Selbstregulation, Optimismus, mentale Beweglichkeit, Charakterstärken und Kommunikation thematisieren und verbessern helfen.[30]

Es versteht sich von selbst, dass ein derart aufwändiges Programm fortlaufend evaluiert wird. Bis anhin sind vier ausführliche Berichte publiziert worden. Die ersten zwei Berichte erbrachten den Nachweis, dass Resilienz und psychische Gesundheit einen bedeutsamen Zusammenhang mit wichtigen Erfolgsmassen wie beispielsweise geringerer Suchtmittelkonsum, gute soziale Einbettung oder Karriere im Beruf aufweisen. Im dritten Bericht konnte gezeigt werden, dass Soldaten mit Resilienztraining ihre GAT-Werte deutlich stärker verbesserten als solche ohne Resilienztraining. Des Weiteren schien das Training für Soldaten im Alter zwischen 18 und 24 Jahren effektiver zu sein als für ältere Soldaten. Letztlich war die Wirkung des Trainings deutlich besser, wenn die Kommandanten darauf achteten, dass das Training sinnvoll im Arbeitsplan integriert war und wenn sie motivierte und vertrauenswürdige junge Führungskräfte als Resilienztrainer einsetzten.[31] Im vierten Bericht wurde untersucht, inwiefern das Training auch einen Einfluss auf das längerfristige Gesundheitsverhalten hat, was die folgenden zwei zentralen Ergebnisse hervorbrachte: Erstens wiesen Einheiten, die ein Master Resilience Training auf Kompaniestufe erhielten, 60 % weniger Fälle von Drogen- und Alkoholmissbrauch auf also solche ohne MRT; zweitens hat-

27 Vanhove, Herian, Perez, Harms, & Lester, 2015
28 Cornum, Matthews & Seligman, 2011
29 Vgl. dazu ausführlich Peterson, Park & Castro, 2011
30 Vgl. dazu ausführlich Reivich, Seligman, & McBride, 2011
31 Lester, Harms, Herian, Krasikova & Beal, 2011

Resilienz heisst auch, Emotionen kontrollieren zu können. (VBS / DDPS)

ten Einheiten mit MRT verglichen mit solchen ohne MRT insgesamt 13 % weniger Diagnosen von Angststörungen, Depressionen und Posttraumatischen Belastungsstörungen (PTBS).[32]

… wiesen Einheiten, die ein Master Resilience Training auf Kompaniestufe erhielten, 60 % weniger Fälle von Drogen- und Alkoholmissbrauch auf also solche ohne MRT.

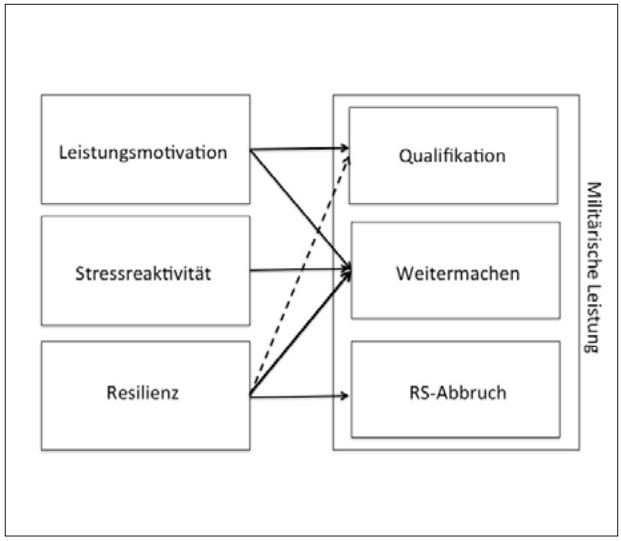
Eine weitere Studie stützte sich auf eine Online-Befragung unter Angehörigen der National Guard sowie Zivilisten zu ihren Erfahrungen mit dem Resilienztraining.[33] 92 % der Befragten gaben an, dass sie das Training als hilfreich empfanden und dass sie ihre Fähigkeiten im Umgang mit stressreichen Situationen verbessern konnten; gar 97 % hielten fest, dass sie die im Training erlernten und geübten Kompetenzen in der Folge in ihren militärischen oder zivilen Jobs umsetzten. Darüber hinaus zeigte eine detailliertere Messung der Resilienz, dass die Teilnehmenden bei sich eine gesteigerte Selbstwahrnehmung, eine optimistischere Haltung, eine erhöhte mentale Flexibilität sowie einen besseren Kontakt zu anderen feststellten. Und schliesslich führte die von den Teilnehmenden berichtete Steigerung der Resilienzkompetenzen zu weniger psychischen Problemen, vor allem bei jenen, die in der Phase der Befragung ein ausgeprägteres Stressempfinden hatten (Puffereffekt).

Zu erwähnen ist schliesslich noch eine Studie, die als erste ihrer Art die Anwendung des Resilienztrainings im Kontext eines Einsatzes zum Gegenstand hatte.[34] In einer militärischen Einrichtung in Afghanistan füllten Soldaten vor und nach einem Resilienztraining entsprechende Fragebogen aus. Die Resultate führten zu Tage, dass trotz des Trainings resilientes Denken im Verlauf des Einsatzes abnahm. Anzufügen ist jedoch, dass eine Vergleichsgruppe ohne Resilienztraining fehlte und die betreffenden Ergebnisse somit nur als Evaluation des Trainingsprogramms betrachtet werden können. Ihr hauptsächlicher Wert besteht somit darin, die Erwartungen der militärischen Kommandostellen ins MRT und in ähnliche Programme auf ein realistisches Niveau zu bringen.

Trotz der Bemühungen um die fortlaufende wissenschaftliche Evaluation des CSF2-Programms liegen momentan noch nicht allzu viele wissenschaftlich fundierte Resultate vor. Demzufolge bietet sich die genauere Betrachtung einer Übersichtsstudie (Metaanalyse) zum Thema an.[35] Im Rahmen einer umfassenden Sichtung der einschlägigen Literatur wurden 42 unabhängige Stichproben, d.h. Resilienztrainings-Programme, identifiziert. Die systematische Analyse machte deutlich, dass Teilnehmende von Resilienztrainings erhöhte Werte bei der Leistungsfähigkeit und dem Wohlbefinden und verringerte Werte im Bereich psychosozialer Defizite aufwiesen. Insgesamt zeigen aber auch diese Resultate, dass sich die Effekte des Trainings über die Zeit deutlich abschwächten. Was den Anwendungsbereich betrifft, konnte sowohl im militärischen als auch im nicht-militärischen Kontext eine zumindest kurzfristige positive Wirkung des Trainings nachgewiesen werden. In Bezug auf die Frage, ob mit gezielten, z. B. auf eine bestimmte Herausforderung wie einen militärischen Einsatz ausgerichteten Trainings bedeutsamere Effekte erreicht werden als mit eher allgemeinen Programmen, waren die Ergebnisse weniger klar. Das Gleiche gilt für die Ergebnisse der Untersuchung über die Art und Weise, wie die Inhalte vermittelt wurden (computerbasiert / Gruppenarbeit / Theoriesaal / individueller Unterricht / Train-the-Trainer). Immerhin gibt es erstens Hinweise darauf, dass mit gezielten Trainings auf lange Sicht mehr Wirkung erzielt wird. Zweitens macht es den Anschein, dass die individuelle, also eins-zu-eins Vermittlung am erfolgversprechendsten ist. Allerdings werden die relevanten Inhalte in den allermeisten Fällen im Theoriesaal und in Gruppensettings vermittelt, weshalb ein Vergleich mit den ganz wenigen Programmen mit einem alternativen didaktisch-methodischen Ansatz mit Vorsicht zu geniessen ist.

Als Fazit lässt sich sagen, dass eine starke Zunahme diverser Trainingsprogramme zur Stärkung der Resilienz beobachtet werden kann, wobei mitunter bemerkenswerte finanzielle, materielle und personelle Ressourcen investiert werden. Hingegen gibt es immer noch ein Ungleichgewicht zwischen den Bestrebungen für die professionelle Durchführung der Trainingsprogramme und wissenschaftlich fundierten Studien zu den Effekten solcher Anstrengungen. Insbesondere in einem derart praxisorientierten Umfeld wie jenem des Militärs gilt es indes Fakten und Zahlen zu liefern, um die Unterstützung und das längerfristige Commitment der Vorgesetzten zu gewinnen. Ansonsten könnte der in einer der Studien[36] geschilderte Fall eintreffen, als die Teilnahme am Programm für die Angehörigen einer Einheit als freiwillig erklärt wurde und in der Folge niemand mehr zum Kurs erschien. Das

32 Harms, Herian, Krasikova, Vanhove & Lester, 2013
33 Griffith & West, 2013
34 Carr et al., 2013
35 Vanhove, Herian, Perez, Harms & Lester, 2012
36 Carr et al., 2013



Mit der Resilienzskala RS-11 werden wichtige Leistungsmasse vorhergesagt. (Niederhauser, Huber & Annen)

Intensive Auseinandersetzung mit wichtigen Themen im Master Resilience Training. (U.S. Army)

bedeutet, dass in Ergänzung zu den fortlaufenden Bestrebungen, das Training und dessen Effekte wissenschaftlich zu evaluieren, Einfluss auf die Erwartungen, Haltungen oder gar Vorurteile aller beteiligter Personen genommen werden muss.

Schaffen einer resilienzfördernden Kultur

Alle Bemühungen, die Resilienz von Individuen oder Gruppen zu verstärken, müssen mit Massnahmen einher gehen, die eine resilienzfördernde Kultur auf allen Stufen des Unternehmens begünstigen, schaffen und erhalten. Wiederum dient hier das CSF2-Programm als passendes Beispiel. Hier war es ursprünglich so, dass der Stabschef der Armee das Projekt initiierte und seinen Support öffentlich kundtat[37]. Wie andere Studien zu psychosozialen Interventionen in Grossunternehmen gezeigt haben, ist eine Top-Down-Unterstützung unabdingbar.[38] Überdies bedurfte es einer gezielten strategischen Kommunikation, um das Commitment der Führungspersonen auf allen hierarchischen Ebenen zu gewinnen, und zwar bevor sie aus anderen Quellen von diesem Programm erfuhren. Angesprochen wurden jedoch auch weitere Beteiligte im Militär, die Politik und die Medien. In der Tat zeigte sich, dass es vor allem bei den Familienangehörigen von Soldaten sehr gut ankam, als sie anhand diverser Berichte aus unterschiedlichen Quellen sahen, dass CSF2 nicht nur auf soldatische Fertigkeiten ausgerichtet ist, sondern die Teilnehmenden auch zu besseren Menschen machen möchte.[39] Es muss aber gleichzeitig darauf geachtet werden, mit solchen Informationen nicht unrealistische Erwartungen zu wecken, vielmehr soll das Bewirken einer positiven Einstellung gegenüber psychologischer Aspekte und Interventionen im Vordergrund stehen.

In diesem Bereich besteht nach wie vor Handlungsbedarf. Trotz gross angelegten Projekten wie CSF2 hat die Inanspruchnahme psychologischer Unterstützung besonders in militärischen Organisationen immer noch einen negativen Beigeschmack.[40] Programme zur Stärkung der individuellen Resilienz müssen diesem Sachverhalt Rechnung tragen und in Betracht ziehen, wie die damit verbundenen Hürden abgebaut werden können. Das bedeutet einerseits ganz pragmatisch, die organisatorischen Schwellen so niedrig wie möglich zu halten. So sollten Resilienztrainings in den normalen Tagesablauf eingebaut werden und im Hinblick auf allfällige Beratungssequenzen sollten die administrativen Abläufe (Urlaub, Kinderbetreuung, Transport, etc.) Teil von Standardprozessen sein. Andererseits stellen bestimmte Haltungen und Vorurteile oft die grösseren Hindernisse dar, wenn es darum geht, ein resilienzförderndes Umfeld aufzubauen. Nebst dem bereits erwähnten Stigma, dass das Annehmen psychologischer Hilfe ein Zeichen der Schwäche ist, gibt es noch weitere weniger offenkundige Merkmale der militärischen Kultur, die erschwerend wirken.

So tendieren militärische und vergleichbare Organisationen dazu, Prozesse und damit verbundene Regeln zu stark zu gewichten. Planung und Nullfehlertoleranz wird gross

37 Casey, 2011
38 Annen, 2013
39 Cornum, 2012

40 Bryan & Morrow, 2011

Kritische Selbstreflexion im Master Resilience Training. (U.S. Army)

geschrieben und folglich steckt man viel Zeit und Energie in Aktivitäten, um sich für das Unvermeidliche vorzubereiten, alles Kontrollierbare zu kontrollieren und das Unerwünschte zu verhindern. Das ist durchaus nachvollziehbar, aber Routine ist bei neuartigen Ereignissen wenig hilfreich und menschliche Fehlbarkeit ist ein Naturgesetz und folglich nicht hundertprozentig zu eliminieren.[41] Systeme und Organisationen reagieren auf Störungen und Fehler meist mit neuen Regeln und Verboten, um zu vermeiden, dass sich derselbe Zwischenfall in Zukunft wiederholt. Weitere zusätzliche Vorschriften belasten jedoch das System, d.h diese Art von Reaktion geht meist auf Kosten der Flexibilität, auf darauffolgende unvorhergesehene Veränderungen angemessen zu reagieren. Ein resilientes System, sei es eine Organisation oder ein Individuum, zeichnet sich nicht durch möglichst zahlreiche und ausführliche Vermeidungsstrategien, sondern durch Offenheit, Gelassenheit sowie das Bereithalten und Einüben verschiedener Lösungsoptionen aus.[42] Oder anders ausgedrückt bedingt es ein Bekenntnis zu jener Art von Resilienz, in der man akzeptiert, dass man überrascht werden oder Rückschläge erleiden kann, und somit die Energie darauf konzentriert, sich an Veränderungen anpassen zu können. Dabei ist wichtig zu betonen, dass in diesem Verständnis von Resilienz Voraussicht und Vorbereitung nach wie vor einen bedeutenden Platz einnehmen. Gerade Führungskräfte müssen sich aber deren Grenzen bewusst sein und sich nicht der Illusion hingeben, dass sich mit umfassender Planung alle Eventualitäten ausräumen lassen.[43]

Ein weiteres heikles Element im Kontext der militärischen Kultur sind Emotionen. Da sie für die Optimierung der Fähigkeiten zur Selbstregulation unverzichtbar sind, stehen sie im Zentrum eines jeden Resilienztrainings. Dem steht gegenüber, dass militärisches Personal immer noch zu oft aufgefordert wird, den Emotionen generell ein nicht zu grosses Gewicht beizumessen und im Einsatz nach Möglichkeit ganz beiseite zu lassen.[44] Das ist eine weitere Hürde, die es auf dem Weg zu einer resilienzfördernden Kultur zu überwinden gilt, beinhalten doch Resilienztrainings zahlreiche Methoden und Übungen, um Emotionen zu erkennen und akzeptieren, zu kontrollieren und sie zu Gunsten des sozialen Umfelds oder der militärischen Mission zielgerichtet einzusetzen.

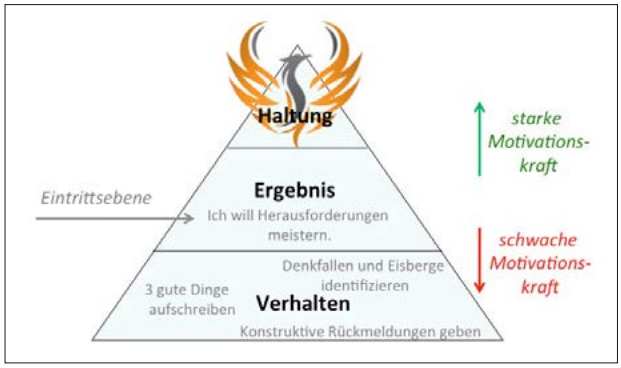
Die bisherigen Ausführungen machen deutlich, dass wir über ausreichend Wissen und Werkzeuge verfügen, um hinsichtlich der Stärkung von Resilienz massgeschneiderte Trainings für Organisationen, Gruppen oder Individuen zu entwickeln und durchzuführen. Resilienztrainings zu implementieren, ist der erste Schritt in diese Richtung. Geschieht dies jedoch als reine Anordnung, wird in erster Linie die extrinsische Motivation der Teilnehmenden angesprochen. Damit besteht die Gefahr, dass sie ein solches Training als reine Pflichtübung wahrnehmen und sich bei erstbester Gelegenheit davon abwenden werden. Die Einführung von Resilienztrainings muss deshalb stets mit entsprechender Sinnvermittlung einher gehen, die Einstellung der Beteiligten ansprechen und deren intrinsische Motivation berücksichtigen.

41 Reason, 1997
42 Sutcliffe & Vogus, 2003
43 Weick & Sutcliffe, 2011

44 Griffith & West, 2013

Die Teilnehmende im Master Resilience Training müssen die gelernten Inhalte schliesslich selber vermitteln können. (U.S. Army)

Psychologische Hilfe anzunehmen, kostet viele Soldaten Überwindung. (Israel Defense Forces)



Bei den Zielsetzungen gilt es alle Ebenen zu berücksichtigen. (Annen)

Resiliente Führungskräfte wirken glaubwürdiger. (VBS / DDPS)

Dabei lohnt es sich, einen Blick auf die unterschiedlichen Arten von Zielsetzungen zu werfen. So neigen Personen dazu, ausgehend von einem angestrebten Ergebnis wie z. B. «Ich will Herausforderungen meistern» unmittelbar klar definierte Verhaltensziele abzuleiten. Ein eben absolviertes Resilienztraining liefert hierfür genügend Material und folglich wird man sich vornehmen, eigene Denkfallen zu erkennen, Emotionen zu regulieren und mit anderen konstruktiv zu kommunizieren – und das Ganze wird dann noch schulbuchmässig in der Art von S.M.A.R.T-Zielen[45] formuliert. Nun verhält es sich aber damit wie mit Neujahrsvorsätzen: Die positiven Effekte werden sich nicht umgehend einstellen und fürs gelegentliche Abweichen von den Vorsätzen wird man nicht unmittelbar bestraft – und in der Folge dürften das Vorhaben bald einmal aus dem Blickfeld verschwunden sein. Die motivationale Kraft eines Ziels hängt eben nicht in erster Linie von dessen konkreter, verhaltensnaher Formulierung, sondern von der damit verbundenen persönlichen Grundhaltung ab. Es ist somit in erster Linie von Relevanz, dass sich die Person voll und ganz mit dem Ziel identifiziert und die Einstellung entwickelt, es auch wirklich erreichen zu wollen.[46] Im Idealfall entwickelt sich diese Einstellung mit der Zeit zu einer Art «Bauchgefühl» und wird so die Person in ihrem alltäglichen Denken und Handeln begleiten und auch kleine, vielleicht unbedeutend erscheinende Entscheidungen auf dem Weg zum übergeordneten Ziel beeinflussen. Um diese umfassende positive Grundhaltung zu unterstützen, haben sich so genannte Motto-Ziele[47] bewährt – beispielsweise in Form eines einprägsamen Spruchs, eines Porträts einer besonders resilienten Person oder eines passendes Bildes. Diese helfen, das Bewusste mit dem Unbewussten sowie die extrinsische mit der intrinsischen Motivation zu verknüpfen. Wenn immer also auf der Basis von Resilienztests oder -trainings Massnahmen zur Stärkung der Resilienz abgeleitet werden, ist es nicht ausreichend, verhaltensorientierte S.M.A.R.T- Ziele und «Was wenn…»-Pläne zu formulieren, vielmehr gilt es zuerst Motto-Ziele zu kreieren, die eine umfassende positive Einstellung hinsichtlich der Resilienz und der damit verbundenen Anstrengungen bewirken.

Lange Rede, kurzer Sinn: Resilienz ist nicht nur zusammengesetzt aus einer bestimmten Disposition und der Ansammlung antrainierter Verhaltensweisen, sie ist vielmehr eine Grundhaltung, die am Ursprung alltäglicher Entscheidungen und Handlungen steht.

… in eine resiliente Zukunft

Wissenschaft liefert nie klare Ergebnisse und schon gar keine Rezepte. Das Fehlen einer einheitlichen Messung von Resilienz wie auch eines klaren Beweises der Effektivität von Resilienztrainings soll jedoch nicht als Begründung genommen werden, nichts in diese Richtung zu unternehmen. Dank der Orientierung an den persönlichen Stärken des Einzelnen führt uns die Auseinandersetzung mit Resilienz ganz generell in die richtige Richtung, wenn es darum geht, die Leistungsfähigkeit von Armeeangehörigen zu optimieren. Auch konnte weiter oben gezeigt werden, dass es durchaus valide psychometrische Messinstrumente gibt, die als Teil von Selektionsprozessen wertvolle Hinweise liefern, die zur systematischen Selbstreflexion im

45 Locke & Latham, 1990
46 Storch, 2009
47 Storch & Faude-Koivisto, 2014

Rahmen von Kursen und Trainings beitragen, oder die als Werkzeug zur Einschätzung der mentalen Bereitschaft von Individuen oder Gruppen vor, während und nach herausfordernden Situationen wie einem militärischen Einsatz dienen. Es braucht weitere Forschung, um das Konstrukt der Resilienz noch klarer abzugrenzen, den Mehrwert von Resilienzskalen hervorzuheben oder präziser zu zeigen, welcher Aspekt von Resilienz in welcher Situation gemessen werden soll.

Das Master Resilience Training der U.S Army steht als eindrückliches Beispiel für die Vielzahl von theoretisch gut fundierten Trainingsmethoden. Der viel zitierte Vergleich mit dem physischen Training dient nicht nur dazu, dem Resilienztraining das Stigma zu nehmen, das noch zu oft psychologischen Interventionen anhaftet, sondern auch um es in einen realistischen Kontext zu stellen: Die Methoden des physischen Trainings basieren auf einer langen Tradition sportwissenschaftlicher Forschung sowie Erkenntnissen aus unzähligen Wettkämpfen. Nichtsdestotrotz ist der Trainingserfolg alles andere als garantiert, hängt er doch wesentlich vom Talent, der persönlichen Disposition, der Motivation, dem aktuellen gesundheitlichen und mentalen Befinden des Einzelnen sowie den jeweiligen Rahmenbedingungen ab. So darf es nicht erstaunen, dass in wissenschaftlichen Untersuchungen zu Resilienztrainings auch nur von mässigen Effekten die Rede ist. Angewendet auf eine grosse Gruppe und als Teil eines Präventionsprogramms dürfte die ökonomische Bilanz im Vergleich mit dem Diagnose-Behandlungs-Ansatz trotzdem recht günstig ausfallen. Dennoch sind weiterführenden Anstrengungen zur wissenschaftlichen Evaluation von Resilienztrainings nötig, wobei alternative Methoden und Messgrössen ins Auge zu fassen sind. In Zukunft sollte das wissenschaftliche Interesse eher auf die Reaktionen in bestimmten Stresssituationen gerichtet werden. Beispielsweise könnten die Teilnehmenden vor dem Resilienztraining unter kontrollierten Bedingungen einem standardisierten Stresstest ausgesetzt werden, wobei subjektive (z. B. wahrgenommener Stress, emotionale Befindlichkeit) als auch objektive (z. B. Herzratenvariabilität, Speichelcortisol) Stressparameter gemessen würden. Nach dem Resilienztraining würde das ganze Prozedere nochmals durchgeführt und verglichen mit einer Kontrollgruppe ohne Resilienztraining könnte erfasst werden, inwiefern das Resilienztraining das Auftreten einer angemessen Stressreaktion begünstigt.[48]

Die besten Messinstrumente und die besten Trainingsmethoden bringen jedoch nicht die gewünschten Effekte hervor, wenn die Organisation und ihre Mitglieder die Möglichkeiten, die sich durch die Auseinandersetzung mit der Resilienz ergeben, nicht wertschätzen oder allenfalls gar nicht erkennen wollen. Jegliche Intervention, die Resilienz zu fördern, muss von Aktionen begleitet werden, welche die Einstellung des Einzelnen sowie die Kultur der ganzen Organisation in die gewünschte Richtung beeinflussen. Dies reicht von Informationen zu Handen der obersten Führungsebene, mit dem Ziel, ihr Wohlwollen und ihre Unterstützung sicherzustellen, bis hin zur Bildung einer positiven Haltung unter allen beteiligten Personen. Erreicht wird diese einerseits durch die Vermittlung von Vorteilen, die sich für den Einzelnen ergeben, und längerfristig vor allem dadurch, dass der Einzelne bei sich und seinen Kameraden sicht- und spürbare Fortschritte feststellt.

Psychologische Resilienz in der Schweizer Armee

Zum Schluss stellt sich nun noch die Frage, welchen Nutzen die Schweizer Armee aus den Kenntnissen zur psychologischen Resilienz ziehen kann. Wie bereits oben erwähnt, konnte verschiedentlich nachgewiesen werden, dass mit einer einfachen und kurzen Resilienzskala eine gute Vorhersage relevanter Erfolgskriterien in der militärischen Grundausbildung, wie z. B. den Verbleib in der RS, die Qualifikation und das Weitermachen, liefern. Es wäre also zu überlegen, ob die Tests in der Rekrutierung mit einer solchen Skala ergänzt werden könnten.

Was das Training betrifft, so ist an der Militärakademie bereits ein Forschungsprojekt am Laufen, in dem die Methoden des MRT auf die Gegebenheiten einer Offiziersschule (OS) der Schweizer Armee angepasst wurden. Die betreffenden Trainingsmodule à 4 × 90 Minuten sind bereits einmal mit Offiziersaspiranten durchgeführt worden, ebenfalls haben jene ganz zu Beginn der OS, unmittelbar vor und nach dem Training sowie während des Praktischen Dienstes bestimmte Fragebogen ausgefüllt. Geplant sind zudem Interviews nach Abschluss des Praktischen Dienstes, mit denen die längerfristige Wirkung auch in Bezug aufs Zivilleben erfragt wird. Im weiteren Verlauf des Projektes werden dieselben Messungen mit Offiziersaspiranten durchgeführt, die kein Resilienztraining absolvieren, womit ein Vergleich zwischen Interventions- und Kontrollgruppe angestellt werden kann. Im Rahmen des darauffolgenden Zyklus' werden die Selbstbeschreibungen der Aspiranten mit objektiven Daten wie Herzratenvariabilität und Speichelcortisol ergänzt und die oben erwähnten standardisierten Stresstests werden ebenfalls wichtiger Bestandteil des Forschungsvorhabens sein. Mit diesem umfassenden Projekt werden drei hauptsächliche Ziele verfolgt: Erstens orientieren sich die Inhalte an den spezifischen Herausforderungen, denen sich Milizkader der Schweizer Armee zu stellen haben. Bewähren sich die betreffenden Trainingsmodule, könnten sie inskünftig zu einem gewinnbringenden Element der Führungsausbildung werden. Zweitens leistet man mit der umfassenden, subjektiven und objektiven Erfassung relevanter Masse, die mit Resilienz zusammenhängen, einen bedeutenden Beitrag zur Forschung auf diesem Gebiet. Drittens stellt die Resilienz von Führungskräften aus theoretischer Sicht noch weitgehend ein unbeackertes Feld dar. Auf Grund der praktischen Erfahrungen in diesem Projekt kann dieses spezifische Konstrukt inhaltlich besser ein- und abgegrenzt und mit den empirischen Ergebnissen abgestützt werden.

Die Ressourcen der Schweizer Armee sind nicht nur in finanzieller Hinsicht begrenzt. Aus diversen Gründen sind auch die Humanressourcen eher ein knappes Gut. Es ist also angezeigt, diese sowohl auftragszentriert als auch menschenorientiert möglichst optimal zu nutzen. Die generelle Verbesserung der mentalen Fitness ist ein wichtiger Teil dieses Vorhabens, der für die Armeeangehörigen auch in ihrem zivilen Leben äusserst hilfreich sein kann.

48 vgl. Annen & Boesch, 2014; La Marca et al., 2012

Literatur

American Psychological Association (online). *The Road to Resilience.* www.apa.org/helpcenter/road-resilience.aspx

Annen, H. (2013). Stell' Dir vor, es ist Coaching, und keiner geht hin … In R. Wegener, A. Fitze & M. Loebbert (Hrsg.), *Coaching-Praxisfelder. Forschung und Praxis im Dialog* (S. 376–385). Wiesbaden: Springer VS.

Annen, H. & Boesch, M. (2014). *Resilience as a predictor for military training outcomes.* Presentation at the 56th Annual Conference of the International Military Testing Association, Hamburg/Germany.

Antonovsky, A. (1979). *Health, Stress and Coping.* San Francisco: Jossey-Bass.

Antonovsky, A. (1996). The salutogenic model as a theory to guide health promotion. *Health Promotion International,* Vol.11, No. 1, 11–18.

Bryan, C.J. & Morrow, C.E. (2011). Circumventing Mental Health Stigma by Embracing the Warrior Culture: Lessons Learned From the Defender's Edge Program. *Professional Psychology: Research and Practice,* 42,1, 16–23.

Carr, W., Bradley, D., Ogle, A.D., Eonta, S.E., Pyle, B.L., & Santiago, P. (2013). Resilience Training in a Population of Deployed Personnel. *Military Psychology,* 25, 2, 148–155.

Casey Jr., G.W. (2011). Comprehensive Soldier Fitness: A Vision for Psychological Resilience in the U.S. Army. *American Psychologist,* 66, 1, 1–3.

Connor, K.M. & Davidson, J.R.T. (2003). Development of a new resilience scale: The Connor-Davidson resilience scale (CD-RISC). *Depress Anxiety,* 18 (2), 76–82.

Cornum, R. (2012). «Does it really help …?» – Resilience Training in the US Army. In: H. Annen (Ed.), *Psychische Widerstandskraft – Wesentliche Faktoren und Konsequenzen für die militärische Ausbildung und Führung. MILAK Schrift Nr. 14.* (pp. 81–89). Birmensdorf: Militärakademie an der ETH Zürich.

Cornum, R., Matthews, M.D., & Seligman, M.E. (2011). Comprehensive soldier fitness: building resilience in a challenging institutional context. *American Psychologist,* 66(1), 4–9.

Costa, P.T. & McCrae, R.R. (1992). Normal personality assessment in clinical practice. The NEO Personality Inventory. *Psychological Assessment,* 4, 5–13.

Harms, P.D., Herian, M.N., Krasikova, D.V., Vanhove, A., & Lester, P.B. (2013). *The Comprehensive Soldier Fitness Programm Evaluation. Report #4: Evaluation of Resilience Training and Mental and Behavioral Health Outcomes.* Monterey, CA: Research Facilitation Team (RFT).

Griffith, J. & West, C. (2013). Master Resilience Training and Its Relationship to Individual Well-Being and Stress Buffering Among Army National Guard Soldiers. *Journal of Behavior Health Services & Research,* 40/2, 140–155.

King L.A. & King, D.W. (2013). Measuring Resilience and Growth. In B.A. Moore & J.E. Barnett (Eds.), *Military Psychologists' Desk Reference* (pp. 301–305). New York: Oxford University Press.

La Marca, R., Bösch, M., Sefidan, S., Annen, H., Wyss, Th., Mäder, U., Roos, L., & Ehlert, U. (2012). A decrease in perceived social support during military service is associated with a concominant increase in baseline and decrease in stress reactivity levels of salivary alpha-amylase. *Eur J Psychotraumatology* (Suppl 1), 109.

Lazarus, R.S., & Folkman, S. (1984). *Stress appraisal and coping.* New York, NY: Springer.

Lester, P.B., Harms, P.D., Herian, M.N., Krasikova, D.V., & Beal, S.J. (2011). *The Comprehensive Soldier Fitness Programm Evaluation. Report #3: Longitudinal Analysis of the Impact of Master Resilience Training on Self-Reported Resilience and Psychological Health Data.* Washington, DC: Department of the Army.

Locke, E. & Latham, G. (1990). *A theory of goal setting and task performance.* Englewood Cliffs, NJ: Prentice Hall.

Lucini, B. (2014). *Disaster Resilience from a Sociological Perspective.* Heidelberg: Springer.

Masten, A.S. (2001). Ordinary magic: Resilience-processes in development. *American Psychologist,* 56, 227–238.

Masten, A.S. & Obradovic, J. (2008). Disaster Preparation and Recovery: Lessons from Research on Resilience in Human Development. *Ecology and Society,* 13 (1), 9.

Meichenbaum, D. (2013). Ways to Bolster Resilience Across the Deployment Cycle. In B.A. Moore & J.E. Barnett (Eds.), *Military Psychologists' Desk Reference* (pp. 325–328). New York: Oxford University Press.

Meredith, L.S., Sherbourne, C.D., Gaillot, S., Hansell, L., Ritschard, H.V., Parker, A.M., & Wrenn, G. (2011). *Promoting Psychological Resilience in the U.S. Military.* Santa Monica, CA: RAND Corporation.

Niederhauser, M., Huber, C., & Annen, H. (2016). Der Einfluss von Resilienz auf die militärische Leistung. *Allgemeine Schweizerische Militärzeitschrift,* 3/2016, 48–49.

Pangallo, A., Zibarras, L., Lewis, R., and Flaxman, P. (2015). Resilience through the lens of interactionism: A systematic review. *Psychological Assessment,* 27, 1–20.

Peterson, C., Park, N., & Castro, C.A. (2011). Assessment for the US Army Comprehensive Soldier Fitness Program: the Global Assessment Tool. *American Psychologist,* 66 (1), 10–18.

Reason, J.T. (1997). *Managing the Risks of Organizational Accidents*. Brookfield, Vt.: Ashgate.

Reivich, K.J., Seligman, M.E., & McBride, S. (2011). Master Resilience Training in the U.S. Army. *American Psychologist,* 66 (1), 25–34.

Reivich, K. & Shatté, A. (2003). *The Resilience Factor.* New York: Broadway Books.

Robins, R.W., John, O.P., Caspi, A., Moffitt, T.E., & Stouthamber-Loeber, M. (1996). Resilient, overcontrolled, and undercontrolled boys: Three replicable personality types. *Journal of Personality & Social Psychology,* 70, 157–171.

Schumacher, J., Leppert, K., Gunzelmann, T., Strauss, B., and Brähler, E. (2004). *Die Resilienzskala – Ein Fragebogen zur Erfassung der psychischen Widerstandsfähigkeit als Personmerkmal.* Online: http://www.mentalhealthpromotion.net/resources/resilienzskala2.pdf (07.09.2016).

Soucek, R., Ziegler, M., Schlett, Ch., & Pauls, N. (2016). Resilienz im Arbeitsleben – Eine inhaltliche Differenzierung von Resilienz auf den Ebenen von Individuen, Teams und Organisationen. *Gruppe. Interaktion. Organisation,* 2016, 47, 131–137.

Storch, M. (2009). Motto-Ziele, S.M.A.R.T.-Ziele und Motivation. In: B. Birgmeier (Ed.), *Coachingwissen: Denn sie wissen nicht, was sie tun?* (pp. 183–205). Wiesbaden: Verlag für Sozialwissenschaften.

Storch, M. & Faude-Koivisto,, T. (2014). Ressourcen aktivieren mit Mottozielen. In: Ryba, Rauw, Gnati, & Rietmann (Eds.), *Professionell coachen* (pp. 334–347). Weinheim: Beltz.

Sutcliffe, K.M., & Vogus, T.J. (2003). Organizing for Resilience. In: K.S. Cameron, J.E. Dutten, & R.E. Quinn (Eds.), *Positive Organizational Scholarship* (pp 94–110). San Francisco: Berrett-Koehler.

Vanhove, A.J., Herian, M.N., Perez, A.L.U., Harms, P.D., & Lester, P.B. (2015). Can resilience be developed at work? A meta-analytic review of resilience-building programme effectiveness. *Journal of Occupational and Organizational Psychology,* 2015, 1–27.

Waaktaar, T. & Torgersen, S. (2010). How resilient are resilience scales? The Big Five scales outperform resilience in predicting adjustment in adolescents. *Scandinavian Journal of Psychology,* 51, 157–163.

Wagnild, G.M. & Young, H.M. (1993). Development and psychometric evaluation of the Resilience Scale. *Journal of Nursing Measurement,* 1, 165–177.

Weick, K.E., & Sutcliffe, K.M. (2011). *Managing the Unexpected. Resilient Performance in an Age of Uncertainty (2nd Edition).* San Francisco, CA: Jossey-Bass.

Werner, E.E., Bierman, J.M., & French, F.E. (1971). *The children of Kauai: a longitudinal study from the prenatal period to age ten.* Honolulu: University of Hawaii Press.

Windle, G., Bennett, K.M., & Noyes, J. (2011). A methodological review of resilience measurement scales. *Health and Quality of Life Outcomes,* 2011, 9:8.

Wyss, Th. & Annen, H. (2011). *PROGRESS - Einfluss von progressiv aufgebauter körperlicher Belastung, Sport und Führungsstil auf Fitness, Verletzungen, Austritte, militärische Leistungsfähigkeit, Stress und Motivation bei Schweizer Rekruten.* Magglingen / Birmensdorf: Interne Studie BASPO / MILAK.

Hubert Annen

Dr. phil., Dozent für Militärpsychologie und Militärpädagogik
an der Militärakademie an der ETH Zürich
E-Mail: hubert.annen@milak.ethz.ch

Pour une approche économique de la cybersécurité

La cybersécurité ne se limite pas aux sciences informatiques. Une approche holistique et multidisciplinaire est nécessaire pour renforcer notre souveraineté numérique. Deux recherches scientifiques adoptant une approche économique de la cybersécurité sont présentées. La première se concentre sur les incitations au partage de l'information sur les cybermenaces. La deuxième porte sur l'efficience des technologies de rupture pour la cyberdéfense. Ces deux études visent à augmenter la résilience des forces armées et des infrastructures critiques.

Marcus M. Keupp, Alain Mermoud[1], Dimitri Percia David

Renforcer notre souveraineté numérique

La souveraineté nationale – condition *sine qua non* pour maîtriser notre destin politique, économique et social – est désormais étroitement liée à la souveraineté numérique.[2] Certains auteurs, comme Pierre Belanger, estiment que : « sans souveraineté numérique, la mission de défense ne sera à terme plus exécutable. La souveraineté numérique est la condition de la sécurité nationale et de la défense ».[3] La Confédération doit donc agir pour assurer notre souveraineté dans le cyberespace. Elle doit prolonger l'existence et la défense de la Suisse dans cette quatrième dimension, comme elle le fait pour la terre, l'air et ses intérêts maritimes. La sûreté des données des citoyens, la sécurité des infrastructures critiques, ainsi que l'autonomie de l'infrastructure numérique, sont devenues des enjeux incontournables pour la confiance générale dans notre société de l'information encore émergente. La notion de souveraineté démocratique, comprise comme le droit exclusif du peuple d'exercer le pouvoir, transcende désormais les clivages politiques classiques.[4] Le champ du cyberespace n'échappe pas aux tendances souverainistes, favorisées par l'émergence d'une ère post-vérité[5] et d'un monde de plus en plus volatile, incertain, complexe et ambigu (VICA).[6]

La souveraineté numérique est la condition de la sécurité nationale et de la défense.

La couche physique du cyberespace[7] est avant tout une ossature matérielle composée d'infrastructures interconnectées: câbles sous-marins, antennes, satellites, etc. Ces infrastructures sont réparties sur les territoires de différents États qui ont leurs propres intérêts stratégiques et géopolitiques.[8] La majorité des câbles sous-marins de fibres optiques (au nombre de 366) appartiennent à des opérateurs privés. Ils sont exploités en collaboration avec les États et assurent 99 % du trafic mondial des données. Ils sont posés directement sur le fond marin et évitent la lenteur et le coût plus élevé des transmissions par satellites. La maîtrise de ces câbles intercontinentaux représente aujourd'hui un enjeu stratégique majeur.

La carte des câbles sous-marins (Fig. 1) indique que le Royaume-Uni est une plaque tournante des télécommunications mondiales.[9] Le service de renseignements électroniques du Royaume-Uni (*Government Communications Headquarters:* GCHQ) profite de cet avantage grâce à son programme Tempora. En effet, ce programme lui permet d'intercepter massivement les données transitant entre l'Europe et les États-Unis. Le GCHQ et son homologue américain, la *National Security Agency* (NSA), peuvent ainsi surveiller les échanges transatlantiques et partager les informations récoltées avec leurs partenaires des «*Five Eyes*».[10] La surveillance des câbles est devenue un élément central de la stratégie de surveillance

1 Auteur correspondant : alain.mermoud@vtg.admin.ch
2 La souveraineté numérique désigne l'application des principes de la souveraineté aux technologies de l'information et de la communication (TIC). Elle est un enjeu majeur pour la gouvernance d'Internet, c'est-à-dire l'élaboration et l'application conjointes par le secteur privé, la société civile et les États, de normes visant à réguler les usages dans le cyberespace.
3 Bellanger, P. 2014. *La souveraineté numérique.* Stock.
4 Citons par exemple l'initiative pour la souveraineté alimentaire déposée par le syndicat paysan *Uniterre*. Le Conseil national soutient actuellement un contre-projet visant à inscrire la sécurité alimentaire dans la Constitution.
5 Le néologisme *post-truth politics* a été consacré mot de l'année 2016 par le dictionnaire d'Oxford. Celui-ci en donne la définition suivante : « la post-vérité fait référence à des circonstances dans lesquelles les faits objectifs ont moins d'influence pour modeler l'opinion publique que les appels à l'émotion et aux opinions personnelles ».
6 Valla, P. 2004. *Sommes-nous aptes à gérer un monde volatile, incertain, complexe et ambigu (VICA)?* Military Power Revue.
7 Le cyberespace est à la fois physique (serveurs, routeurs, câbles), logiciel (protocoles, programmes), et cognitif (le sens de l'information portée par les réseaux).
8 Huyghe, F-B., et al. 2016. *Gagner les cyberconflits : au-delà de la technique.* Economica.
9 Cette supériorité remonte au XIXe siècle, lorsque les britanniques dominaient déjà le marché du câble sous-marin télégraphique dans l'océan Atlantique.
10 Le terme *Five Eyes* (Cinq Yeux) désigne l'alliance entre les services de renseignement de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis. Ces pays sont liés par le traité *UKUSA,* un accord qui règle la coopération pour la collecte de renseignements électromagnétiques. Ce traité signé en 1946 est resté secret jusqu'aux révélations liées au réseau Echelon (système mondial d'interception SIGINT) à la fin des années 1990.

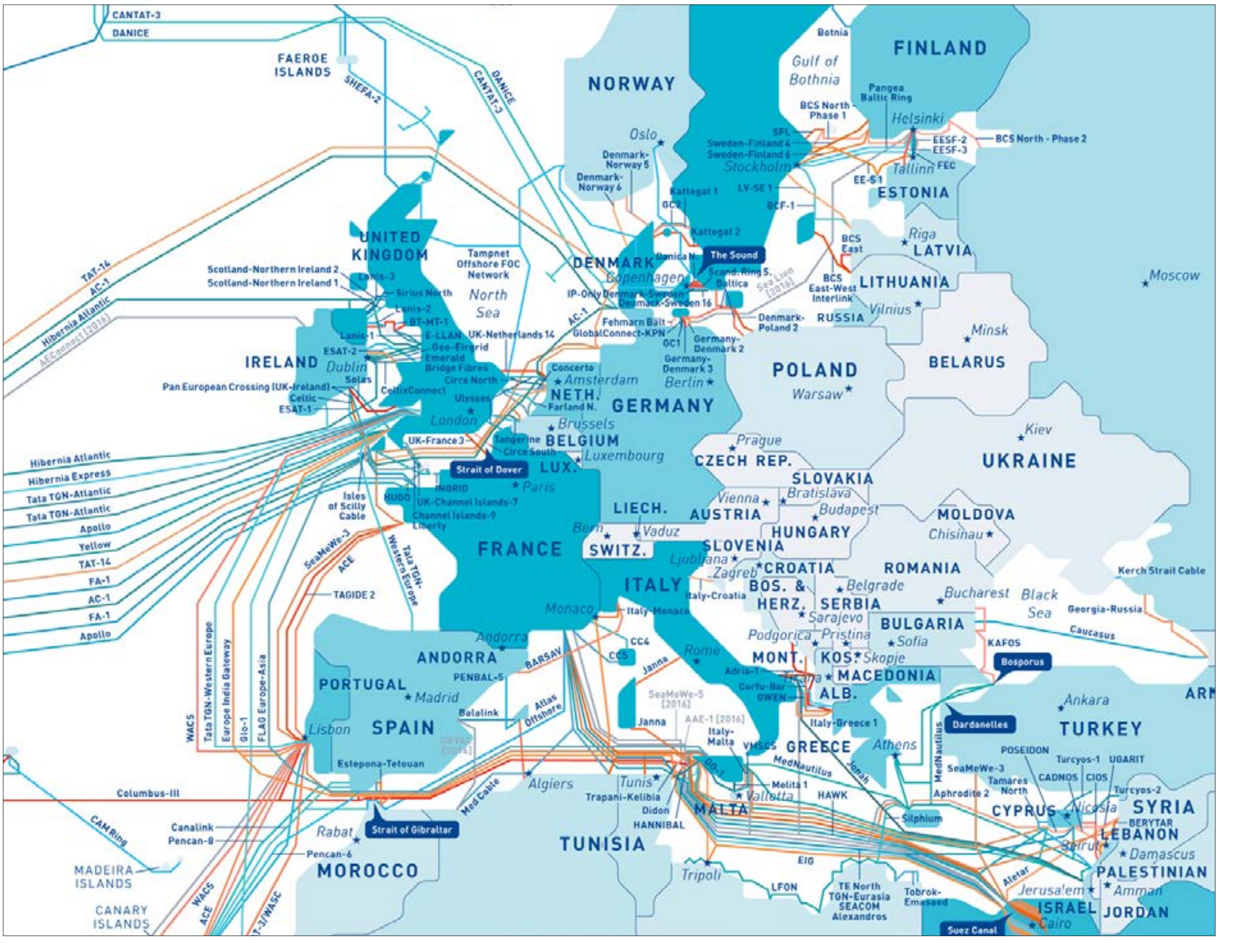


Figure 1 Le Royaume-Uni concentre un grand nombre de câbles sous-marins, ce qui lui permet de surveiller à large échelle le trafic Internet passant sur son territoire. (telegeography.com)

de la NSA, car elle sert à la sécurité nationale, mais aussi au renseignement économique et à l'espionnage industriel.[11] Pour maintenir et accroitre sa souveraineté, un État doit maîtriser la surveillance qui s'exerce sur et depuis son territoire.

Figure 2 Le sous-marin nucléaire d'attaque *USS Jimmy Carter* (SSN-23) a la capacité de mettre sur écoute la fibre optique sous-marine. (Wikipedia)

Pour maintenir et accroitre sa souveraineté, un État doit maîtriser la surveillance qui s'exerce sur et depuis son territoire.

Le réseau Internet est devenu le symbole de la globalisation et des échanges internationaux. Cependant, ce réseau a une origine militaire – le réseau *ARPANET* – et constitue ainsi un lien direct avec la défense de la souveraineté.[12] Les *révélations Snowden* n'ont fait que confirmer l'importance de l'information pour la sécurité nationale, comme précédemment défendu par Thomas Hobbes au XVIIe siècle dans son Léviathan: *«L'information c'est le pouvoir!»*.

Dès les années 1990, les États-Unis ont compris que dans une économie de la connaissance, l'importance de l'information pourrait être comparée à celle du pétrole dans la société industrielle: le principal carburant et le relais de la croissance. Les données sont donc la principale matière

11 Cette surveillance n'est toutefois pas un phénomène nouveau. Au XIXe siècle la communauté du renseignement s'intéressait déjà à la collecte de données issues des câbles sous-marins. Lors de la première guerre mondiale, les Britanniques et les Allemands cherchaient à interrompre systématiquement les communications en sectionnant ces câbles. Durant la Guerre froide, l'opération *Ivy Bells* (menée conjointement par la *NSA* et l'*US Navy*) permettait de placer les câbles sous-marins soviétiques sur écoute.

12 Suite à la crise des missiles de Cuba, la *Defense Advanced Research Projects Agency* (DARPA) développa en 1969 le premier réseau de téléinformatique à transfert de paquets, baptisé *ARPANET*. La *DARPA* est une agence du département de la Défense des États-Unis et elle est chargée de la recherche et du développement destinés aux usages militaires.

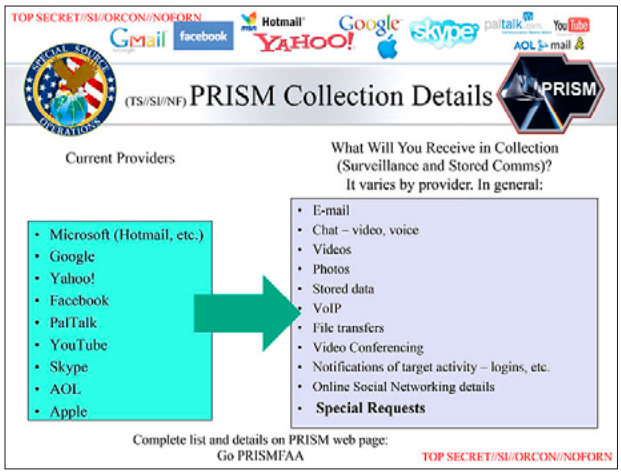


Figure 3 Le programme de surveillance électronique PRISM révélé par Edward Snowden en 2013. Ce programme a pour but de collecter des données sur le réseau Internet, en collaboration avec les grandes sociétés high-tech américaines. Certaines entreprises stratégiques américaines utilisent les informations collectées pour se créer un avantage compétitif. (NSA)

Figure 4 L'ancien secrétaire américain à la défense, Leon Panetta, a mis en garde son pays contre la possibilité d'un « Cyber Pearl Harbor ». (istockphoto.com)

première de la quatrième révolution industrielle.[13] Comme le pétrole, elles doivent d'abord être extraites, puis raffinées pour devenir utilisables. Elles sont réparties d'une manière inégale et représentent donc un intérêt géoéconomique pour les États. La technologie n'est pas neutre. Elle s'inscrit dans un contexte géopolitique et dans les idéologies. Les GAFA (Google-Apple-Facebook-Amazon) forment aujourd'hui les premières capitalisations boursières mondiales et dépassent le produit intérieur brut (PIB) de certains États. Cette suprématie numérique américaine s'est construite sur plusieurs décennies autour d'un partenariat public-privé efficace.[14] La stratégie consiste à allier les intérêts économiques, les investissements, les écosystèmes entrepreneuriaux de la *Silicon Valley*, les besoins des services de renseignement, et les intérêts militaro-stratégiques. Cette alliance forme aujourd'hui un véritable complexe militaro-numérique qui permet d'assurer l'hégémonie américaine dans le cyberespace et de consacrer l'extraterritorialité du droit américain.[15]

La technologie n'est pas neutre. Elle s'inscrit dans un contexte géopolitique et dans les idéologies.

Notre dépendance aux technologies de l'information et de la communication (TIC) se développe de manière exponentielle. Par conséquent, les États, les entreprises et les individus sont la cible de cyberattaques de plus en plus fréquentes et sophistiquées. Le développement rapide de l'informatique dématérialisée en nuage et de l'Internet des objets (dont la sécurité de base est très limitée) amplifie encore cette perte d'autonomie. Les forces armées et les infrastructures critiques[16] n'échappent pas à la datafication et dépendent de plus en plus du réseau Internet pour accomplir leurs mandats respectifs. L'interruption (même partielle et éphémère) de certaines infrastructures critiques pourrait entraîner des effets en cascade. Si l'interconnexion des réseaux engendre de nombreuses opportunités, elle implique également l'interconnexion des risques. Ceux-ci sont encore trop souvent mesurés et gérés de façon isolée. Par analogie à la crise des *subprimes*[17] en 2008, cette cyber-interconnexion des risques est appelé cyber-apocalypse ou cyber-subprime par certains experts. *L'Autorité bancaire européenne* (ABE) prévoit d'ailleurs d'élargir ses stress tests au domaine de la cybersécurité des banques *too big to fail* (trop grandes pour faire faillite). La fragilité de notre monde interconnecté représente donc un nouveau risque systémique dont les conséquences restent trop peu étudiées.

13 La quatrième révolution industrielle désigne les nombreuses innovations de ruptures bouleversant actuellement les économies développées. Ces innovations s'appuient sur les technologies numériques et transforment radicalement les moyens de production, de distribution et d'accès aux biens et services. Le réseau Internet est au cœur de cette révolution et permet l'interconnexion de ces technologies (robotique, impression 3D, biotechnologie, etc.) avec la société et le corps humain (on parle alors de transhumanisme).

14 L'entreprise *Palantir Technologies* symbolise parfaitement cette alliance. Cette société spécialisée dans la science des données développait à ses débuts des logiciels d'analyses pour la communauté américaine du renseignement. Elle s'est ensuite diversifiée dans les secteurs de l'assurance, de la finance, de la santé et s'exporte désormais à l'international. Cette entreprise a été financée dès sa fondation par *In-Q-Tel*, un fonds de capital-investissement géré par la *Central Intelligence Agency* (CIA).

15 L'accord transatlantique *Privacy Shield* qui règle la protection des données personnelles est remise en cause par le nouveau gouvernement américain. Officialisé en juillet 2016, cet accord était censé garantir aux citoyens la protection des données stockées dans le cloud et collectées par les GAFA, et qu'elles ne feraient pas l'objet d'une surveillance massive.

16 Dans cet article, nous définissons une infrastructure critique comme un actif vital et essentiel pour le bon fonctionnement de l'État, de la société et de l'économie.

17 La crise des *subprimes* désigne la crise financière qui a touché le secteur des prêts hypothécaires à risque en 2007. Cette crise est partie des États-Unis et a débouché sur une crise bancaire mondiale, entraînant la plupart des pays industrialisés dans la Grande Récession, soit la pire crise économique depuis la Grande Dépression de 1929.

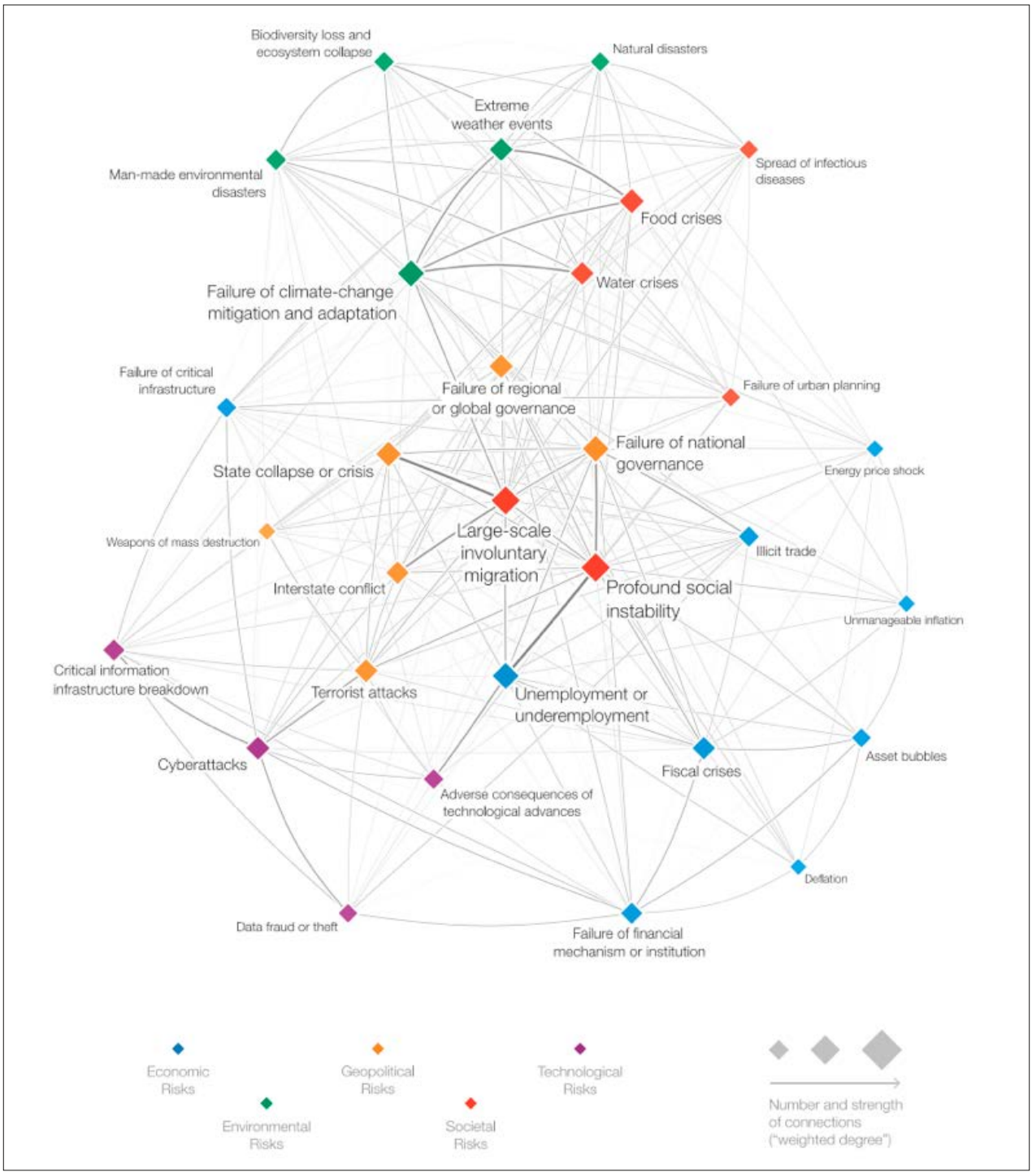


Figure 5 Chaque année le *World Economic Forum* (WEF) établi son *Global Risks Report*. La carte ci-dessus montre les interconnexions des risques globaux en 2017. Le risque technologique (en violet) est surtout corrélé avec le risque économique et le risque géopolitique. (WEF)

Si l'interconnexion des réseaux engendre de nombreuses opportunités, elle implique également l'interconnexion des risques.

Colonne vertébrale de notre économie, les TIC sont devenues la structure sur laquelle tous les biens et les services s'appuient, mais aussi un relais de croissance pour les économies développées. Cette concentration de richesses et de savoirs dans le cyberespace rend celui-ci économiquement attractif pour mener des opérations de guerre économique,[18] de guerre de l'information ou des actions cybercriminelles. Le quasi-anonymat et la difficulté d'attribuer une cyberattaque renforcent encore cette attractivité.

18 La chaire *Economie de Défense* de l'ACAMIL a organisé une grande conférence sur la guerre économique – défis et stratégies – en septembre 2016. La doctrine Gerasimov est analysée dans les actes de la conférence disponibles sur le site www.milak.ch (consulté le 31.03.17).

Le cyberespace transcende désormais tous les aspects de notre société, y compris la souveraineté étatique. Celle-ci se trouve compromise par notre manque d'emprise sur le réseau Internet, ses données et ses services.[19] Si les infrastructures critiques venaient à être sévèrement touchées par une cyberattaque, les citoyens seraient dépossédés de leurs données et l'État ne serait plus capable d'accomplir ses missions régaliennes. Deux des trois conditions de la formation de l'État moderne (citoyens, pouvoir, territoire) ne seraient alors plus réunies. Depuis deux décennies, des plans gouvernementaux de défense des infrastructures critiques se développent. Paradoxalement et parallèlement, les infrastructures critiques connaissent une dérégulation, une privatisation et une libéralisation. L'interaction entre ces deux développements antagonistes posent des questions doctrinales non résolues pour les forces armées. De plus, certaines données nécessaires à l'accomplissement de leurs mandats sont aujourd'hui détenues par des sociétés ou des opérateurs privés.

L'ère de post-vérité et les réseaux sociaux offrent une caisse de résonnance sans précédent à la désinformation et aux opérations de déceptions.[20] Les bulles de filtres et les chambres d'échos[21] viennent encore amplifier la portée des « faits alternatifs », souvent diffusés par des « usines à trolls ».[22] Ce type de propagande inspirée de *l'astroturfing*[23] est le cœur de la stratégie d'ingérence de la Russie dans les dernières élections américaines.[24] Dans son concept de guerre de quatrième génération, William Lind[25] avait déjà théorisé l'apparition de ces phénomènes. Ils permettent de gagner du pouvoir coercitif (P2C) sans utiliser de moyens conventionnels et brouillent les frontières traditionnelles entre guerre et paix, national et étranger, civil et militaire. Dans ce contexte, une victoire sans combat devient possible, réalisant ainsi le vieux rêve du général et stratège chinois *Sun Tzu*.

L'érosion de la souveraineté numérique créé des conditions favorables à la guerre hybride, aux violences infra-guerrières, aux attaques indirectes et non linéaires, théorisées par le Général Gerasimov en 2013 et mises en pratique lors de la crise de la Crimée en 2014.[26] Selon la doctrine Gerasimov, les cyberattaques ne sont qu'un épiphénomène à replacer dans le contexte plus général de la guerre de l'information et de la guerre économique.[27] L'absence de souveraineté numérique crée des conditions favorables aux attaques sur la couche sémantique du cyberespace. Dès lors, la guerre de l'information tend à devenir le centre de gravité des conflits contemporains.[28] La maîtrise du réseau Internet, de ses données et de ses applications devient donc la mère des batailles.

L'absence de souveraineté numérique crée des conditions favorables aux attaques sur la couche sémantique du cyberespace.

L'économie de la cybersécurité, de quoi s'agit-il ?

L'économie de la cybersécurité est un champ de recherche multidisciplinaire qui existe depuis une quinzaine d'années. Cette discipline est issue des sciences informatiques et a ensuite évolué dans de multiples champs de recherche comme la stratégie, la science militaire, les sciences de la complexité, la psychologie sociale, ou encore l'économie comportementale. La majorité des chercheurs sont anglo-saxons et proviennent de prestigieuses universités. Cette communauté de recherche se réunit chaque année au sein du *Workshop on the Economics of Information Security* (WEIS).[29]

L'idée de base de cette discipline est de transférer des modèles et concepts économiques dans les sciences informatiques.

L'idée de base de cette discipline est de transférer des modèles et concepts économiques dans les sciences informatiques. D'autres disciplines ont également participé au décloisonnement de la cybersécurité, comme par exemple : la psychologie avec son concept de résilience[30], la géopolitique qui permet de mieux comprendre les motivations et les conflits qui précèdent les cyberattaques, et la stratégie et la polémologie qui permettent de replacer les cyber-conflits au cœur de la dialectique des volontés. Le droit et les relations internationales sont également des disciplines importantes pour réguler le cyberespace. Le renseignement peut, quant à lui, permettre d'anticiper une cyberattaque ou d'aider à son attribution. Cette approche holistique et multidisciplinaire de la cybersécurité est un changement de paradigme indispensable pour la sécurité numérique.

La cybersécurité a trop longtemps été associée uniquement à la sécurité informatique, se limitant ainsi exclusivement à des mesures techniques de sécurité. Les antivirus, la cryptographie et autres pare-feu – pour ne citer que

19 La présence massive de portes dérobées dans les *firmwares* de nos smartphones, téléviseurs et véhicules intelligentes renforcent encore cette perte d'autonomie.
20 Volkoff, V. 1999. *Petite histoire de la désinformation.* Editions du Rocher.
21 Les *filter bubbles* désignent la personnalisation de contenu informationnel, par des algorithmes, à l'insu de l'internaute. Celui-ci se retrouve alors isolé dans une echo chamber médiatique où ses idées et croyances sont constamment amplifiées et répétées.
22 La notion *d'usine à trolls* qualifie une stratégie de propagande visant à contrôler de nombreux comptes en ligne dans le but de simuler des mouvements de masse, principalement sur les sites et forums des médias de référence.
23 L'*astroturfing* est une technique de propagande utilisée dans les campagnes de relations publiques, publicitaires ou politiques. Elle consiste à simuler un mouvement citoyen, venu de la société civile, dans le but de donner l'impression d'un comportement spontané ou d'une opinion publique dominante.
24 Cette stratégie vise à avantager des candidats favorables à la Russie. Dès lors, il est probable que cette même stratégie soit utilisée lors de l'élection présidentielle française ce printemps et lors des élections générales en Allemagne cet automne.
25 Lind, W., et al. 1989. *The changing face of war: into the fourth generation.* Marine Corps Gazette.
26 En février 2017, le ministre russe de la Défense a confirmé la création, il y a quatre ans, d'une entité consacrée à la guerre de l'information. Ce département, inspiré par la doctrine Gerasimov, est spécialisé dans la contre-propagande, le piratage informatique et la diffusion de fausses nouvelles.
27 Mermoud, A. 2013. *La place financière suisse au cœur de la guerre économique.* Infoguerre.fr
28 Vernez, G. 2009. *L'information, zone de conflit et risque stratégique majeur.* Military Power Revue.
29 Les résultats de nos recherches seront également présentés dans cette conférence scientifique http://weis2017.econinfosec.org/ (consulté le 31.03.2017).
30 En sciences informatiques, la résilience désigne la capacité d'un système à s'adapter et à continuer à fonctionner en mode dégradé pendant une attaque, puis à revenir rapidement à son état initial.

les plus connus – ont longtemps été considérés comme les moyens les plus pertinents pour protéger le cyberespace. Pourtant, des chercheurs de renom ont empiriquement démontré que de nombreux défis liés à la cybersécurité pouvaient être rendus intelligibles, expliqués et résolus en utilisant une approche économique. Des experts affirment même que certains défis en cybersécurité ne peuvent être résolus sans une approche économique. A titre d'exemple, les faiblesses d'un système informatique sont souvent causées par des motivations divergentes des acteurs, formulées par la théorie de l'agence[31], dont la compréhensibilité dépasse les sciences informatiques.

En employant le cadre analytique de cette même théorie à la sécurité du cyberespace, Anderon et Moore[32] ont démontré que les organisations fournissant de la cybersécurité ne supportent pas elles-mêmes les coûts et les pertes d'une cyberdéfaillance. Dès lors, les systèmes de sécurité alloués ne peuvent produire un service à la hauteur des attentes. L'économiste Adam Smith utilise le concept d'aléa moral pour désigner cet effet.[33] Dans le domaine de la cybersécurité, l'aléa moral est accentué par le phénomène croissant de l'externalisation informatique et de l'informatique en nuage.[34]

Les externalités négatives d'une cyberattaque contre une infrastructure critique peuvent être extrêmement élevées.

Les externalités[35] négatives d'une cyberattaque contre une infrastructure critique peuvent être extrêmement élevées,[36] en raison de l'interconnexion des risques et des effets en cascade subséquents. En revanche, les investissements sont forcément limités et ne peuvent compenser que partiellement les externalités. Selon une étude de 2015 de la compagnie d'assurance *Zurich*[37], les risques liés au réseau Internet pourraient supplanter les bénéfices dès 2020, ce qui pourrait engendrer le retour du low-tech volontaire dans certains secteurs stratégiques et un ralentissement du développement de la quatrième révolution industrielle.

Pour une organisation, une cyber-assurance permet de transférer le risque financier d'une cyberattaque. Toutefois, il est peu probable que le marché de la cyber-assurance se développe pour les infrastructures critiques dont le coût des externalités est par définition difficilement quantifiable. Par conséquent, le prix de la prime pour assurer un cyber-risque systémique serait trop élevé, même pour une réassurance. Il convient alors de gérer le risque en appliquant les concepts connus du plan de continuité des activités (PCA)[38] et les méthodes de gestion de crises bien connues des militaires. C'est dans cet esprit que *l'Office fédéral de la population* (OFPP) a rédigé son guide[39] pour la protection des infrastructures critiques en 2015. Ce guide classe les infrastructures critiques par secteurs et sous-secteurs, en évaluant à chaque fois le niveau de criticité selon : « *l'importance relative du sous-secteur par rapport à la dépendance, à la population et à l'économie* ».

Le guide de l'OFPP applique la théorie des coûts marginaux[40] pour identifier les mesures de protection optimales sur le plan économique, selon la méthode suivante : « *l'approche basée sur les coûts marginaux vise un rapport optimal entre les dommages résultant des défaillances ou des dérangements des infrastructures critiques et les coûts des mesures à mettre en œuvre. La quantité de mesures optimales est celle qui donne le total des coûts le plus bas selon le schéma ci-dessous* ».

Secteurs	Sous-secteurs
Autorités	Représentations diplomatiques, organisations internationales
	Recherche et enseignement
	Biens culturels
	Parlement, gouvernement, justice, administration
Energie	Approvisionnement en gaz naturel
	Approvisionnement en pétrole
	Approvisionnement en électricité
Elimination	Déchets
	Eaux usées
Finances	Banques
	Assurances
Santé	Soins médicaux et hôpitaux
	Laboratoires
Industrie	Industrie chimique et pharmaceutique
	Industrie mécanique, électrique et métallurgique
Information et communication	Technologies de l'information
	Médias
	Trafic postal
	Télécommunications
Alimentation	Approvisionnement en denrées alimentaires
	Approvisionnement en eau
Sécurité publique	Armée
	Services d'urgence (police, sapeurs-pompiers, sauvetage)
	Protection civile
Transports	Trafic aérien
	Trafic ferroviaire
	Trafic fluvial
	Trafic routier

Criticité très importante*
Criticité importante*
Criticité normale*

* – On entend par «criticité» l'importance relative du sous-secteur par rapport à la dépendance, à la population et à l'économie (≠ importance absolue). Selon la situation, on tiendra également compte de la menace et de la vulnérabilité des infrastructures critiques.
– L'évaluation se réfère à une situation de risque normale.
– L'évaluation ne donne aucune information sur la criticité des éléments considérés individuellement.

Figure 6 Extrait du guide pour la protection des infrastructures critiques. En rouge les huit sous-secteurs dont la criticité est très importante en Suisse. (OFPP)

31 La théorie de l'agence est une branche de l'économie qui étudie les conséquences du problème *principal-agent*. Ce problème apparaît lorsque l'action d'un acteur économique (*le principal*) dépend de l'action ou de la nature d'un autre acteur (l'agent) sur lequel le principal est imparfaitement informé.

32 Anderon, R., Moore, T. 2006. *The Economics of Information Security*. Science.

33 Un aléa moral (*moral hazard*) peut apparaître dans certaines situations à risque lorsqu'un agent se comporte différemment selon son degré d'exposition au risque. L'aléa moral est, par exemple, observable dans le domaine des assurances, lorsqu'un assuré augmente sa prise de risque, par rapport à la situation où il supporterait seul les coûts d'un sinistre.

34 Le *cloud computing* consiste à exploiter la puissance de calcul et du stockage de serveurs distants via le réseau Internet.

35 Une *externalité* se caractérise par le fait qu'un agent économique crée, de par son activité, un effet externe négatif ou positif en procurant à autrui, et sans contrepartie monétaire, un avantage ou un dommage.

36 Gordon, L., Loeb, M., Lucyshyn, W., Zhou, L. 2015. *Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model*. Journal of Information Security.

37 Zurich Insurance Group, Atlantic Council. 2015. *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures*. http://publications.atlanticcouncil.org/cyberrisks/ (consulté le 31.03.2017).

38 Un *PCA* a pour but de garantir la survie d'une organisation après un sinistre important. Ce plan stratégique permet à l'organisation de continuer à fonctionner en mode dégradé, puis de redémarrer l'activité le plus rapidement possible.

39 Le guide complet est disponible sur le site http://www.babs.admin.ch/fr/aufgabenbabs/ski.html (consulté le 31.03.2017).

40 Le coût marginal de production est le coût supplémentaire induit par la dernière unité produite. Le coût marginal joue un rôle fondamental dans l'analyse des décisions de production.

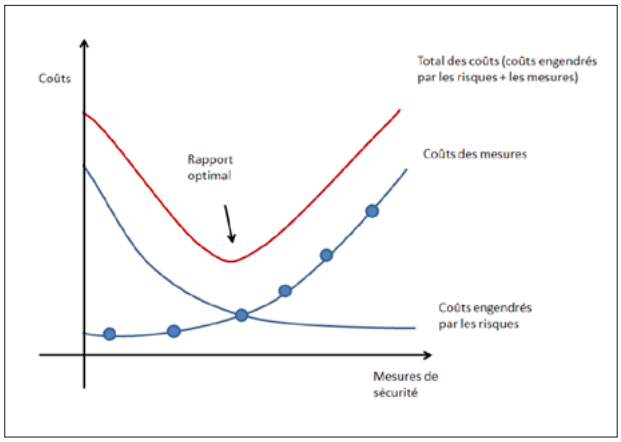


Figure 7 Principe des coûts marginaux. Les points bleus représentent les différentes mesures. Chaque mesure implémentée réduit le coût des dommages résultant d'une défaillance ou d'une perturbation d'une IC. La combinaison est optimale lorsque les coûts totaux (c.-à-d. la somme des coûts des mesures et des dommages résultant de défaillances ou de dérangements des IC) sont au point le plus bas. (OFPP)

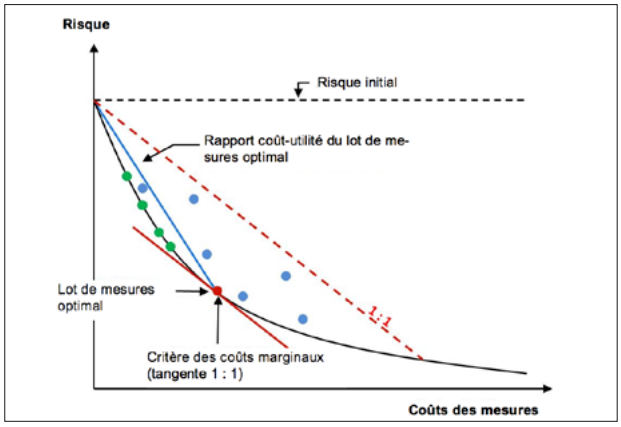


Figure 8 Procédure pour déterminer la combinaison optimale de mesures sur le plan économique. La courbe noire représente la limite inférieure de l'ensemble des mesures. Sur cette courbe, les mesures atteignent une utilité maximale (réduction des risques) avec des coûts minimaux. Toutes les mesures situées au-dessous de la ligne rouge en pointillé (points bleus) ont bien un rapport coût-utilité supérieur à 1 mais elles ne sont efficaces ou optimales que si elles se trouvent sur la ligne noire avant le point de tangente (point rouge) = coûts marginaux des mesures (points verts). (OFPP)

L'économie de la cybersécurité aborde également des problèmes importants à propos des investissements en cyberdéfense. Ceux-ci ne sont pas forcément corrélés avec les bénéfices produits. Il convient donc de trouver le montant optimal d'investissement en cyberdéfense et de mesurer la productivité des mesures choisies. La méthode des coûts marginaux décrite ci-dessus est nécessaire, mais insuffisante. De nombreuses contributions empiriques sont encore attendues par la communauté de recherche en économie de la cybersécurité. Il existe par exemple un besoin important de tester les modèles théoriques développés à ce jour. Afin de contribuer à ce champ de recherche, la chaire *Économie de Défense à l'académie militaire* (ACAMIL) à l'*EPF de Zurich* (EPFZ) mène actuellement deux études scientifiques qui seront présentées dans les sections suivantes. La première se concentre sur les incitations au partage volontaire des informations concernant les cybermenaces. La deuxième porte sur les gains d'efficience engendrés par les technologies de rupture pour la cyberdéfense. Ces deux recherches scientifiques contribuent à renforcer notre souveraineté numérique et la résilience des infrastructures critiques avec des coûts réalistes. Elles répondent aux besoins stratégiques de la défense, de l'industrie et de la recherche académique.

L'humain, ce maillon faible

Cette étude scientifique, menée par Alain Mermoud dans le cadre de sa thèse de doctorat, se focalise sur les incitations au partage volontaire des informations concernant les cybermenaces.[41] Un cadre théorique issu de l'économie comportementale est appliqué dans le contexte de la protection des infrastructures critiques. Un nouveau modèle détaille le mécanisme incitatif qui permet d'orienter les comportements humains vers l'échange volontaire d'informations et qui permet ainsi d'optimiser l'efficience de la cybersécurité. Ce modèle, peu coûteux et relativement simple à mettre en place, permet d'abaisser le coût optimal d'investissement dans la cyberdéfense et contribue à renforcer notre souveraineté numérique. Il permet également de lutter contre les phénomènes de rétention d'information entre les différents acteurs de la chaîne sécuritaire.

L'opération *Olympic Games*[42] restera probablement dans l'histoire comme la première grande campagne de cyberguerre. Le ver informatique utilisé, baptisé *Stuxnet*, a exploité des vulnérabilités *Zero day*.[43] Son inhabituelle complexité en a fait une cyber-arme redoutable pour perturber et dégrader les centrifugeuses iraniennes. Il est intéressant de relever que le virus a été inoculé par ingénierie sociale, c'est-à-dire que les failles humaines des ingénieurs iraniens ont été utilisées pour les inciter à connecter des clés USB infectées sur le réseau interne des centrifugeuses. Cet exemple démontre que la manipulation psychologique humaine joue un rôle important même dans le cas d'attaques techniquement complexes. Les comportements humains inadéquats sont souvent le maillon faible de la chaîne sécuritaire.

Les comportements humains inadéquats sont souvent le maillon faible de la chaîne sécuritaire.

Par conséquent, les techniques d'ingénierie sociale ont fortement progressé ces dernières années. Une tendance a émergé dans la littérature scientifique selon laquelle les

41 L'échange d'information sur les cybermenaces consiste à partager des informations pertinentes pour la cybersécurité entre agents économiques. Ces informations peuvent porter sur une faille, une vulnérabilité, un maliciel, des techniques de hameçonnages (*phishing*), une fuite de données, etc. Un agent peut également partager des informations à propos des bonnes pratiques (résolution d'un incident), une compétence particulière, des avis et conseils d'experts, ou encore des renseignements pertinents pour la cybersécurité.

42 L'opération *Olympic Games* est une série de cyberattaques secrètes, menées en 2010 par les États-Unis et Israël, contre le programme nucléaire iranien.

43 *Zero day* (jour zéro) désigne une vulnérabilité informatique inconnue du public et qui ne dispose pas d'un correctif connu. La partie adverse peut exploiter cette asymétrie de l'information à son avantage.

problèmes de cybersécurité sont souvent liés à de mauvais comportements humains.[44] Ceux-ci sont généralement engendrés par un mauvais design des systèmes d'information et de mauvaises incitations. L'exemple typique est celui du mot de passe inscrit sur un post-it à côté de l'ordinateur. L'utilisateur sait qu'il s'agit d'un mauvais comportement qui peut mettre en danger sa propre sécurité. Cependant, la mémorisation d'une quantité exponentielle de mots de passe complexes n'est pas gérable pour un utilisateur lambda, ce qui l'incite à de mauvais cybercomportements. Cet exemple démontre l'importance d'une approche multidisciplinaire de la cybersécurité et qu'il est donc essentiel de mener la recherche académique au-delà du domaine traditionnel de la sécurité informatique.

La politique de sécurité du WEF a réuni de nombreux experts scientifiques en cybersécurité lors de sa dernière édition. Les experts présents, en collaboration avec *Interpol* et *Europol*, ont démontré que l'échange d'informations entre le secteur public et le secteur privé permettait d'aboutir à des systèmes de protection efficaces. Toutefois, cet échange nécessite une importante confiance entre les régulateurs, l'industrie et le secteur public. Cette confiance doit se construire sur le long terme. Elle est particulièrement difficile pour les multinationales qui opèrent dans des juridictions différentes et complexes. Il est donc essentiel de clairement définir les responsabilités des différents acteurs. Si les experts s'accordent sur la nécessité de partager des compétences et des informations, ils divergent cependant sur le type de modèle à déployer pour favoriser la confiance réciproque.

Les experts s'accordent sur la nécessité de partager des compétences et des informations.

Du point de vue du renseignement, le partage d'informations sur les cybermenaces permet de produire du *Cyber Threat Intelligence* (CTI). Le CTI est une discipline basée sur le cycle du renseignement (analyse des besoins, collecte, analyse et diffusion des informations) qui est bien connue des militaires. Elle a pour finalité la production du renseignement lié aux cybermenaces, par exemple dans le but d'alimenter les systèmes de détections précoces ou les CERTs.[45] Ce renseignement sur et depuis le cyberespace est la première ligne de défense contre les cyberattaques. Il permet d'anticiper les attaques, de s'adapter et de contribuer à l'attribution d'une cyberattaque en identifiant son origine ou son auteur, ou en détectant des tendances sur les méthodes utilisées et les secteurs touchés. Il existe donc un lien indissociable entre le renseignement et la cybersécurité.

Ce renseignement sur et depuis le cyberespace est la première ligne de défense contre les cyberattaques.

Plusieurs économistes et actuaires ont proposé des modèles quantitatifs pour pallier au manque d'investissement chronique dans le domaine de la cybersécurité. Ces modèles d'investissements ont théoriquement démontré le potentiel de l'échange d'informations entre infrastructures critiques. Pour une organisation, le partage d'informations permet de réduire le niveau optimal d'investissement en cybersécurité. D'un point de vue économique, l'échange d'informations permet – entre autres – de réduire l'asymétrie d'information,[46] les externalités négatives et surtout d'anticiper les menaces afin d'augmenter la résilience des systèmes d'information. Cependant, les problèmes de rétention d'information et du passager clandestin[47] sont persistants, ce qui ne permet pas d'exploiter tout le potentiel de l'échange d'informations pour prévenir les cybermenaces.

Ainsi, certains régulateurs proposent de contraindre les infrastructures critiques au partage d'informations.[48] Cette contrainte serait similaire à l'obligation d'annonce pour les médecins et les hôpitaux pour certaines maladies transmissibles à déclaration obligatoire.[49] Les premiers résultats montrent toutefois que la régulation ne peut pas fonctionner sans incitations. La Suisse semble plutôt suivre une tendance régulatrice basée sur l'adhésion volontaire. Depuis 2004, la *Centrale d'enregistrement et d'analyse pour la sûreté de l'information* (MELANI) facilite le partage d'informations entre les infrastructures critiques.[50]

Il est important d'identifier les incitations économiques et sociales qui peuvent permettre aux infrastructures critiques de partager des informations spontanément et volontairement.

Plusieurs études ont démontré que l'échange délibéré d'informations concernant les cybermenaces, au sein d'un partenariat public-privé, était plus performant que la contrainte. Dès lors, il est important d'identifier les incitations économiques et sociales qui peuvent permettre aux infrastructures critiques de partager des informations spontanément et volontairement. Un nouveau modèle est donc nécessaire pour comprendre le mécanisme incitatif permettant d'orienter les comportements vers l'échange volontaire d'informations. La confiance demeure une condition primordiale, mais pas suffisante, à

44 Ghernaouti, S. 2013. *Cyber Power : Crime, Conflict and Security in Cyberspace.* EPFL Press.

45 Les CERT *(Computer Emergency Response Team)* sont des centres d'alertes dotés de personnels prêts à réagir aux cyberattaques.

46 En sciences économiques, l'*asymétrie d'information* désigne un échange dans lequel certains des participants disposent d'informations pertinentes que d'autres n'ont pas. La présence d'asymétrie d'information conduit au problème du risque moral.

47 Le problème du passager clandestin *(free-rider)* désigne le comportement d'un agent qui profite d'un avantage sans y avoir investi autant d'efforts (en argent ou en temps) que les autres agents d'un groupe.

48 En 2015, les États-Unis ont adopté le *Cybersecurity Information Sharing Act* (CISA) et l'Union Européenne (UE) le *Network and Information Security Directive* (NIS).

49 Art.12 *de la loi fédérale sur la lutte contre les maladies transmissibles de l'homme.* Selon cette loi, l'*Office fédéral de la santé publique* (OFSP) est contraint d'exploiter, en collaboration avec d'autres services fédéraux et avec les services cantonaux compétents, les systèmes de détection précoce et de surveillance des maladies transmissibles.

50 L'échange d'informations entre MELANI et les exploitants d'infrastructures critiques sera régi par la *Loi fédérale sur la sécurité de l'information* (LSI).

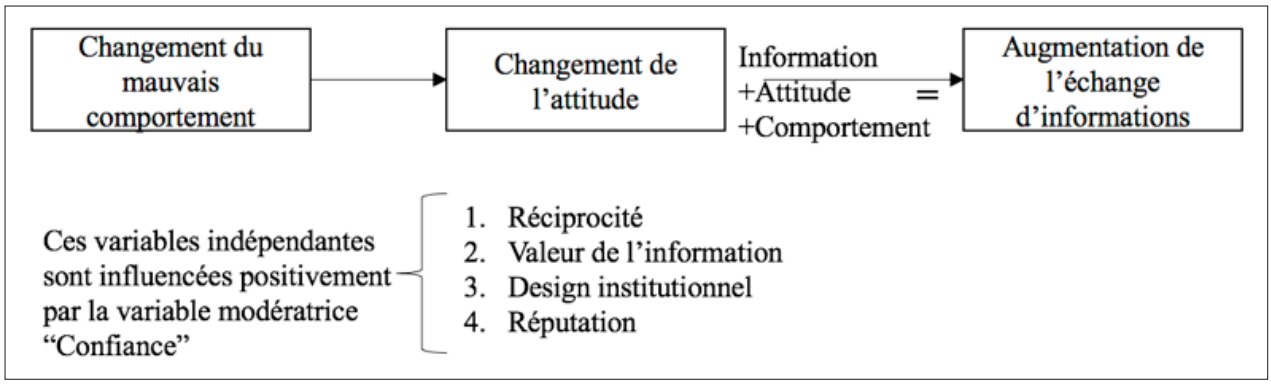


Figure 9 Notre mécanisme théorique permet d'inciter les acteurs de la cybersécurité à échanger des informations. Ce modèle est inspiré de l'économie comportementale et de la théorie des perspectives. (Kahneman & Tversky)

l'échange d'informations. Par conséquent, nous avons défini la confiance comme une variable modératrice dans notre modèle théorique présenté ci-dessous. Ce modèle a été validé par un comité scientifique international et présenté lors d'une conférence scientifique.[51]

Notre recherche a pour but de confirmer ou d'infirmer les impacts de facteurs clés dans le partage de l'information cybernétiquement pertinente. Les quatre variables indépendantes étudiées sont les suivantes : la réciprocité dans l'échange d'informations, la valeur de l'information, la réputation et le design institutionnel des plateformes d'échanges. Lors d'études précédentes, ces quatre « effets » ont été identifiés comme des éléments précurseurs au partage de l'information.[52] Nos résultats devraient permettre d'investiguer les facteurs pertinents à développer afin d'atténuer les problèmes de rétention d'information et du passager clandestin.

Nos résultats devraient permettre d'investiguer les facteurs pertinents à développer afin d'atténuer les problèmes de rétention d'information et du passager clandestin.

Notre modèle incitatif est compatible avec une vision libérale et décentralisée de la cyberdéfense. Cette vision se base sur l'idée que, pour bien fonctionner, un système doit reposer sur la responsabilité individuelle et la motivation intrinsèque de ses membres, plutôt que sur la contrainte juridique. Cette vision, similaire à celle du système de milice, repose donc fondamentalement sur la confiance et une collaboration forte entre le secteur public et le secteur privé. Ce modèle a été développé dans le cadre de la protection des infrastructures critiques, mais il peut aussi être utilisé dans d'autres domaines (par exemple : le partage d'informations entre agences de renseignement). La Suisse offre un cadre idéal au déploiement de ce modèle grâce à sa stabilité politique et son haut degré de confiance envers les institutions.

Technologies de rupture et cybersécurité

Cette étude scientifique, menée par Dimitri Percia David dans le cadre de sa thèse de doctorat, vise à déterminer les effets des technologies de rupture[53] sur la dynamique des investissements en cybersécurité et des gains d'efficience subséquents. L'avènement de technologies de rupture comme les systèmes d'analyses et de traitement des mégadonnées (*Big Data Analytics;* BDA)[54] ou la chaîne de blocs[55] – pour ne citer que celles-ci – implique un retour sur investissement disruptif vis-à-vis des mesures de cybersécurité conventionnelles. Le succès de ces mesures restant limité, le marché de la sécurité informatique commence à s'adapter. Cette étude scientifique se déroule dans le contexte de la protection des infrastructures critiques et vise à délivrer des recommandations politiques afin d'optimiser les investissements dans le domaine de la cyberdéfense. La partie théorique de cette thèse a été validée par un comité scientifique international et présentée lors d'une conférence scientifique.[56]

Le modèle présenté précédemment vise à réduire le problème de la rétention d'information et des mauvais comportements humains. D'un point de vue théorique, une autre solution serait de supprimer ou diminuer les interactions humaines (par exemple en automatisant le processus du partage d'informations). D'un point de vue pratique, cette solution n'a encore jamais été appliquée. Cependant, la chaîne de blocs pourrait remettre en question les modèles développés à partir de l'économie comportementale. En effet, cette technologie permet de supprimer les intermédiaires et de

51 Mermoud, A., Keupp M.M., Ghernaouti, S., Percia David, D., 2016. *Using incentives to foster security information sharing and cooperation: a general theory and application to critical infrastructure protection.* The 11th International Conference on Critical Information Infrastructures Security, Paris. http://www.critis2016.org/ (consulté le 31.03.2017).

52 ENISA. 2010. *Incentives and challenges for information sharing in the context of network and information security.* https://www.enisa.europa.eu (consulté le 31.03.2017)

53 Une technologie de rupture *(disruptive technology)* est une innovation radicale qui remplace à terme une technologie existante. Par opposition, les technologies de continuité améliorent par incréments successifs une technologie existante.

54 Le terme mégadonnées *(Big Data)* se réfère aux données dont la complexité rend leur traitement (extraction, gestion, sollicitation et analyse) irréalisable par les technologies quantitatives classiques. La complexité des mégadonnées est définie par trois aspects: 1) le volume (téraoctets, pétaoctets, ou même exaoctets (1000^6 octets) ; 2) la vitesse (à laquelle les données sont générées) et 3) la variété (liée aux mélanges de données structurées et non structurées).

55 La chaîne de blocs *(blockchain)* est une base de données distribuée qui fonctionne d'une manière décentralisée. Les monnaies cryptographiques, comme le *bitcoin* (système de paiement pair à pair), utilisent cette technologie. Toutes les transactions sont transparentes, vérifiées par les nœuds du réseau et enregistrées dans un registre public théoriquement infalsifiable.

56 Percia David, D. Keupp, M. M., Ghernaouti, S., Mermoud, A., 2016. *Cyber Security Investment in the Age of Big Data: Reassessment of Gordon-Loeb Model and Application to Critical Infrastructure Protection.* The 11th International Conference on Critical Information Infrastructures Security, Paris.

générer automatiquement de la confiance entre les utilisateurs. De plus, son mode de fonctionnement décentralisé est parfaitement compatible avec le fédéralisme helvétique et elle pourrait permettre d'automatiser le partage d'informations. Réputée inviolable, cette technologie balbutiante est promise à un bel avenir et les débouchés pour la cybersécurité sont nombreux.

Les systèmes d'analyse des mégadonnées sont susceptibles de devenir la prochaine génération de technologies de l'information. Certains experts pensent que le futur des *Information Sharing and Analysis Centers* (ISACs)[57] réside dans l'émergence des Fusion Centers. Ces centres ont été créés aux États-Unis après les attentats du 11 septembre 2001, pour favoriser le partage d'informations entre les différentes agences de renseignement, le *Département de la Sécurité intérieure* et le *Département de la Justice*. Ils permettent de collecter, d'agréger et de fusionner des informations provenant de différentes sources hétérogènes. Contrairement à la chaîne de blocs, cette solution centralisatrice et bureaucratique semble moins bonne dans le contexte helvétique.

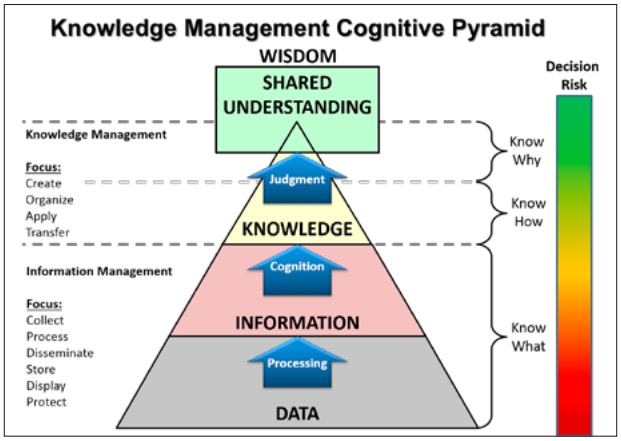


Figure 10 La pyramide de DIKW (Data, Information, Knowledge, Wisdom) adaptée par l'*US Army*. Le but du BDA est en fait de générer du Small Data. Cette pyramide montre le processus nécessaire pour transformer et contextualiser des données non structurées (matière première) en sagesse, voire en Smart Data. (Wikipedia CC BY-SA 4.0)

Ces technologies de rupture sont essentielles pour renforcer notre souveraineté numérique et investir d'une manière optimale dans la cyberdéfense.

Dans tous les cas, ces technologies de rupture sont essentielles pour renforcer notre souveraineté numérique et investir d'une manière optimale dans la cyberdéfense. En développant un modèle actuariel basé sur les coûts liés à la cybersécurité, *Gordon et Loeb*[58] ont proposé d'investiguer le niveau optimal d'investissement en cybersécurité, *ceteris paribus*. En partant du principe que la préoccupation principale de chaque organisation est de maximiser son bénéfice net provenant de ses dépenses en cybersécurité, les deux chercheurs déterminent une fonction permettant d'établir un niveau optimal d'investissement en cybersécurité. Ce dernier correspond à la minimisation du coût total, c'est-à-dire à la somme de la valeur de la perte générée par des failles cybersécuritaires et de la valeur du montant investi afin d'acquérir des technologies ayant pour but de se prévenir de telles failles.

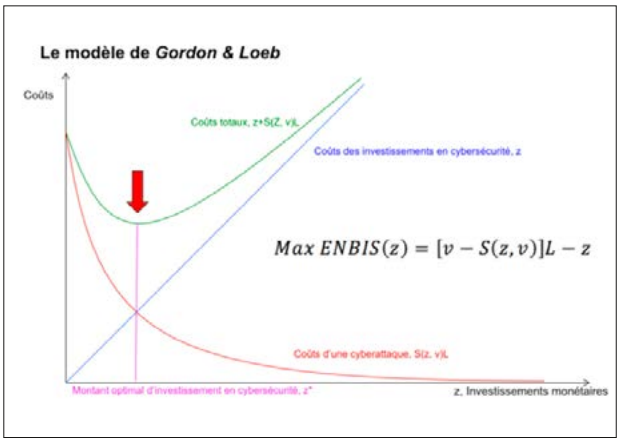


Figure 11 Ce modèle permet de calculer le montant optimal d'investissement en cybersécurité (flèche rouge) en fonction de la vulnérabilité des systèmes et de la perte potentielle dûe à une cyberdéfaillance. (Gordon & Loeb, 2002)

Ce modèle permet par exemple de calculer une prime pour une cyber-assurance. Il permet ainsi de conclure que le montant investi par une organisation pour sa cybersécurité ne devrait pas dépasser 37 % des pertes potentielles engendrées par une cyberattaque. Les pertes liées aux risques cybersécuritaires, ainsi que le montant investi dans les technologies de protection informatique, sont intrinsèquement liés à l'efficacité des produits et services du marché de la sécurité numérique. Depuis une trentaine d'années, ce dernier propose de nombreux moyens techniques conventionnels basés sur l'analyse des signatures, pour accroître la sécurité informatique. Les mécanismes de contrôle d'accès, les systèmes de détection d'intrusion, les techniques de cryptage, pare-feu et logiciels anti-virus ont ainsi vu le jour. Or, le succès de ces mesures est toutefois limité.

Les technologies actuelles basent leur stratégie essentiellement sur la détection des menaces qui ont déjà été observées dans le passé.

Les technologies actuelles basent leur stratégie essentiellement sur la détection des menaces qui ont déjà été observées dans le passé. Une telle approche devient de moins en moins appropriée face à une cybercriminalité grandis-

57 Les *ISACs* sont des plateformes, qui s'appuient généralement sur un partenariat public-privé et à but non lucratif, dont l'objectif est de favoriser l'échange d'informations entre les infrastructures critiques privées et publiques.
58 Gordon, L.A., Loeb, M.P. 2002. *The economics of information security investment*. ACM Transactions on Information and System Security (TISSEC).

sante. La complexité et la rapidité d'exécution deviennent des défis colossaux. Un écart grandissant se fait ressentir entre les moyens de la cybercriminalité et le retard de détection des signatures inappropriées. De plus, les vulnérabilités dites *Zero day* ne peuvent pas être prises en considération par une telle approche. Par conséquent, les techniques conventionnelles peuvent être facilement rendues inefficaces par les cybercriminels. Ce constat d'échec devient davantage alarmant à l'ère des mégadonnées. En effet, des exaoctets d'informations sont transférés tous les jours, ce qui donne de nombreuses possibilités aux cybercriminels pour accéder à des réseaux en dissimulant leur présence et en infligeant des dégâts difficilement détectables.

Afin de répondre à une cybersécurité défaillante, le marché de l'informatique commence à s'adapter en donnant moins d'importance à l'approche conventionnelle et en développant une approche novatrice de détection d'actions inappropriées. La récente discipline académique que les Anglo-Saxons nomment *Security Analytics* permet d'opérer ce changement de vision. En employant les technologies dérivées du BDA, des procédés de détection précoce (basés sur la prospection active de menaces en temps réel) permettent la création de renseignements ciblés afin de prévenir les cybercrimes. Ces méthodes sont susceptibles de devenir la prochaine génération de technologies de l'information et permettront un retour sur investissement disruptif par rapport aux mesures conventionnelles. Cette rupture fondamentale permettrait ainsi de passer du principe clé de résilience des infrastructures (élément réactif) au principe d'anticipation (élément actif) des infrastructures. L'avènement d'une telle technologie et ses conséquences disruptives sur le niveau optimal d'investissement en cybersécurité, ainsi que l'étude des nouvelles dynamiques d'investissements, sont des éléments qui méritent d'être investigués. Quels que soient les résultats d'une telle recherche académique, les apprentissages délivreront de multiples indices sur la façon d'optimiser les investissements en cybersécurité et permettront ainsi d'augmenter l'efficience des mesures envisagées.

Passer du principe clé de résilience des infrastructures (élément réactif) au principe d'anticipation (élément actif) des infrastructures.

Nous proposons d'étendre le modèle de *Gordon et Loeb* à plusieurs périodes et de relaxer l'hypothèse de continuité de la fonction de probabilité de défaillance sécuritaire. Ces adaptations permettent de capturer les aspects dynamiques des investissements tels que l'avènement d'une technologie radicalement innovante (le BDA ou la chaîne de blocs). Nous proposons ainsi d'étudier théoriquement et empiriquement les conséquences d'une telle technologie sur les investissements.

En basant la conceptualisation d'une expérience sur la théorie des jeux et sur les systèmes de sécurité interdépendants, les données récoltées seront utilisées par un modèle économétrique afin de corroborer ou infirmer nos hypothèses d'efficience et leurs conséquences pour la cybersécurité. Nous illustrerons notre approche dans le contexte de la protection d'une infrastructure critique représentée par les forces armées. Bien que les technologies du BDA soient considérées comme prometteuses pour la protection des infrastructures critiques, leurs effets concrets n'ont à notre connaissance jamais été investigués dans le milieu académique. Cette étude devrait permettre de répondre à ce besoin.

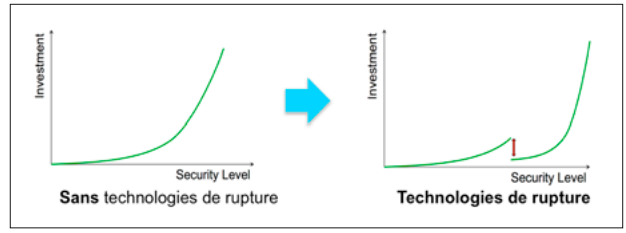


Figure 12 Le but de cette recherche est d'analyser l'impact des technologies de rupture sur le modèle de Gordon et Loeb. (ACAMIL)

État stratège et Intelligence Economique

En conclusion, la cybersécurité ne se limite pas aux aspects techniques des sciences informatiques. Les études présentées dans cet article contribuent au développement d'un nouveau champ de recherche : l'économie de la cybersécurité. Elles fournissent des pistes pour renforcer notre souveraineté numérique et augmenter l'efficience de la cyberdéfense. Les deux recherches présentées sont complémentaires, puisque la deuxième bénéficie directement des résultats de la première. Les résultats scientifiques détaillés des deux thèses de doctorat seront publiés dans des périodiques scientifiques spécialisés.

Depuis 2010, les cyberattaques n'ont cessé de se multiplier contre les intérêts nationaux.

Nos recherches présentent des conséquences politiques pour la Suisse, sa souveraineté numérique, sa sécurité économique et ses forces armées. Depuis 2010, les cyberattaques n'ont cessé de se multiplier contre les intérêts nationaux. Le cas américain démontre qu'une stratégie de maintien et d'accroissement de puissance passe aujourd'hui obligatoirement par la maîtrise des systèmes d'information, de leurs services et usages incontournables. Toute proportion gardée, la Suisse doit donc se doter d'une stratégie numérique pragmatique et d'un partenariat public-privé efficace. Seule une approche holistique de la souveraineté numérique – respectant le fédéralisme et le contexte helvétique – permettra de combler notre vide stratégique numérique.[59]

A ce titre, la stratégie « *Suisse numérique* » adoptée en 2016 fixe des idées cohérentes. Cette stratégie est une première base indispensable permettant de produire de la valeur liée aux données, nouveau pétrole de l'ère numérique. La Suisse doit créer et maintenir des conditions favorables

59 Baumard, P. 2012. *Le vide stratégique.* CNRS Editions.

pour bénéficier de la quatrième révolution industrielle, renforçant ainsi ses atouts : stabilité et neutralité politique, système d'éducation performant et capital humain de haute qualité, culture de la confidentialité, et surtout le développement d'un cadre juridique garantissant la protection des données. Cette prise de conscience se matérialise déjà par la récente création de *VIGISWISS*[60], une association qui regroupe les sociétés actives dans le stockage et la protection des données en Suisse.[61] A titre d'exemple, avec la fin du secret bancaire, la Suisse pourrait ainsi proposer la sécurité des données comme nouveau modèle d'affaire.[62]

Avec la fin du secret bancaire, la Suisse pourrait ainsi proposer la sécurité des données comme nouveau modèle d'affaire.

La première *Stratégie nationale de protection contre les cyber-risques* (SNPC)[63] 2012 – 2017 a permis d'implémenter 15 des 16 mesures prévues. Le Conseil fédéral a néanmoins décidé de mettre en place une deuxième stratégie pour les années 2018 – 2023. Ces nouvelles mesures pourraient intégrer une réflexion stratégique sur la souveraineté numérique. Si une autarcie numérique helvétique semble impossible sur la couche physique du cyberespace[64], il convient toutefois de tendre vers une souveraineté numérique sur les couches logiques et sémantiques. La création d'un *cloud souverain*, basé sur des logiciels libres permettant de rapatrier des données stratégiques sur notre territoire, serait par exemple une mesure intéressante concernant la couche logique.[65] A titre d'exemple, Swisscom propose désormais un cloud suisse dans son offre de base. La souveraineté numérique tend donc à devenir un argument commercial.

La Suisse pourra ainsi augmenter sa capacité à produire son propre renseignement, afin de réduire sa dépendance aux services étrangers.

Concernant la couche sémantique, la nouvelle loi sur le renseignement *(LRens)* entrera en vigueur en septembre 2017. Elle apportera des nouvelles ressources au *Service de renseignement de la confédération* (SRC). La Suisse pourra ainsi augmenter sa capacité à produire son propre renseignement, afin de réduire sa dépendance aux services étrangers. La *LRens* permettra au SRC et à la Confédération de disposer d'une monnaie d'échange informationnelle, renforçant ainsi leur crédibilité sur le marché international du renseignement.[66]

Ces différentes mesures sont un premier pas en direction d'une souveraineté numérique, mais cela est insuffisant par rapport aux enjeux civilisationnels liés à la quatrième révolution industrielle. Selon de nombreux experts cette révolution est d'ordre structurel : « la blockchain n'est pas la révolution tant annoncée, elle n'est que l'outil d'un monde lui-même entré en révolution ».[67] La chaîne de blocs ressemble au modèle suisse : décentralisation, sécurité, confiance. Les monnaies cryptographiques (systèmes de paiement pair à pair) remettent par exemple en question le monopole de l'État sur la création monétaire. Les forces armées n'échapperont évidemment pas à cette révolution. Par conséquent, il est nécessaire de revoir la traditionnelle appréciation de la situation pour y ajouter un sixième facteur « information » (liée à la guerre de l'information) et relativiser l'importance du facteur milieu (géographique).

Inspirée du renseignement, l'Intelligence Economique offre une grille d'analyse permettant de décrypter le dessous des cartes.

Un agenda numérique soutenu par une politique publique d'Intelligence Economique (IE)[68] pourrait permettre l'émergence d'un « soft power ». Cette puissance d'influence est aujourd'hui indispensable pour former un « smart power suisse », soutenu par le « hard power ». L'IE peut permettre l'émergence d'un État stratège capable de mieux anticiper, pour moins se laisser surprendre. Un tel État doit se doter d'un outil de pilotage stratégique capable de détecter de manière proactive les risques et les opportunités. Inspirée du renseignement, l'IE offre une grille d'analyse permettant de décrypter le dessous des cartes et d'armer intellectuellement l'Etat pour comprendre les forces à l'œuvre, décrypter les alliances et les stratégies d'actions. L'IE permet également d'optimiser le transfert de connaissances et de méthodologies entre la sphère militaire et la sphère économique.[69] L'IE est également une méthode permettant de créer de la sécurité économique pour nos entreprises. Par ailleurs, une telle politique permettrait d'augmenter notre emprise sur nos réseaux informatiques, colonne vertébrale de notre économie. Car « si l'on fait la guerre comme on produit des richesses »[70] les conflits futurs se cristalliseront autour de l'information, de ses systèmes et de ses réseaux. Il est toutefois nécessaire de rappeler que les nouvelles cybermenaces viennent s'ajouter aux menaces conventionnelles (sans les remplacer) et que la majorité des conflits finissent par devenir territoriaux.

60 https://www.vigiswiss.ch/fr/ (consulté le 26.02.17).
61 La nouvelle loi sur la protection des données est toutefois jugée insuffisante par les organisations de protection des consommateurs car elle n'attribue pas le contrôle des données aux citoyens. Ceux-ci sont privés de deux éléments essentiels de la législation européenne : le droit à la portabilité et le droit à l'oubli.
62 La société *Swiss Data Safe SA* rachète et rénove des anciens bunkers de l'Armée suisse. Cette société utilise la sécurité associée à la Suisse pour vendre un coffre-fort de données privées.
63 https://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs.html (consulté le 28.02.2017).
64 Le développement du dernier *Smaky* autonome a complètement cessé en 1995. Ce micro-ordinateur helvétique avait été développé à l'EPFL par le Prof. Nicoud et vendu par la société *EPSITEC SA*.
65 En 2014, la France s'est dotée d'un *Institut à la souveraineté numérique* (ISN) dont le but est de faire connaître les enjeux de la souveraineté numérique au grand public et aux élus.
66 Mermoud, A., Percia David, D. 2016. *La LRens : réduire le vide stratégique numérique suisse.* Revue Militaire Suisse.
67 Leloup, L. 2016. *Blockchain, la révolution de la confiance.* Eyrolles.
68 L'Intelligence Economique (IE) peut se résumer en une formule : la bonne information, à la bonne personne, au bon moment, et d'une manière sûre. L'IE repose sur trois piliers fondamentaux : la veille stratégique, la protection de l'information, l'influence. L'IE fait partie du renseignement de défense et du renseignement d'intérêt militaire avec, pour ne citer qu'un exemple, le renseignement scientifique.
69 Mermoud, A., Percia David, D. 2016. *L'Intelligence Economique : du renseignement militaire au renseignement privé.* Revue Militaire Suisse.
70 Wicht, B. 2013. *Europe Mad Max demain ? Retour à la défense citoyenne.* Favre.

Figure 13 Une équipe suisse de milice a gagné l'édition 2015 du Cyber Challenge. (Atlantic Council, GCSP)

La majorité des conflits finissent par devenir territoriaux.

A ce titre, la République et canton de Genève fait figure de pionnier avec sa stratégie économique 2030 qui fait explicitement référence à l'IE. Avec l'entrée en vigueur de sa nouvelle *Loi sur la police* (LPol), le canton s'est doté d'un conseil consultatif de sécurité qui a rédigé une stratégie sécuritaire 2030.[71] Ce document stratégique réitère l'importance de développer une capacité de veille stratégique et d'IE. Fin 2017, le canton prendra également part à un exercice de conduite stratégique. Ces exercices sont essentiels et permettent de développer une réflexion stratégique, ainsi que de tester la coordination entre les différents acteurs de la chaîne sécuritaire. Dès lors, il est essentiel que le prochain exercice du Réseau national de sécurité (ERNS 19) adopte une approche holistique et multidisciplinaire de la cybersécurité.

Sur le plan international, les exercices de conduite politico-stratégique adoptent de plus en plus une approche publique-privée, dans le but d'intégrer l'ensemble des parties prenantes. Les risques ne peuvent plus être gérés en silo et l'interopérabilité est une condition nécessaire à la réussite. Organisée pour la première fois en Europe, l'édition 2015 de la compétition internationale *Cyber 9/12 Student Challenge*[72] est à ce titre un bon exemple. Les participants à ce concours de référence avaient pour but de présenter des mesures de gestion de crise à des décideurs politiques, économiques et militaires, afin de trouver une réponse appropriée à une cybercrise internationale. Soudés par leur solide formation militaire, les participants suisses ont rapidement appliqué les méthodes d'activités de conduite. La Suisse a brillé non seulement comme pays hôte grâce à l'organisation du *Geneva Center for Security Policy* (GCSP), mais également grâce à son équipe qui a décroché la médaille d'or.[73]

Les équipes professionnelles spécialisées dans la cyberdéfense n'ont pas mieux performé que l'équipe de milice.

Cette première place confirme la force de notre modèle de milice qui a permis de réunir une équipe de quatre étudiants aux profils éclectiques (ingénieur, juriste, militaire, économiste), parlant différentes langues et provenant de

71 http://www.ge.ch/dse/doc/news/170315_DSE-Brochure_strat_securitaire.pdf (consulté le 31.03.2017).

72 http://www.atlanticcouncil.org/programs/brent-scowcroft-center/cyber-statecraft/cyber-9-12 (consulté le 31.03.2017)

73 Mermoud, A. 2015. *La Suisse championne du monde de cybersécurité.* Le Temps.

diverses institutions : *ACAMIL, Center for Security Studies* (CSS) et *HEC Lausanne*. Contrairement à ce qu'on l'on pourrait penser, les équipes professionnelles spécialisées dans la cyberdéfense n'ont pas mieux performé que l'équipe de milice. L'équipe de milice a naturellement adopté une approche multidisciplinaire face à un scénario dont l'intensité a rapidement dépassé celui d'une cybercrise de basse intensité. Cet exemple démontre que notre système de milice est adapté à la cyberguerre. Nos deux écoles polytechniques fédérales *(EPF)* forment parmi les meilleurs spécialistes en sécurité informatique du globe. Il convient maintenant d'optimiser le transfert de connaissances, via le système de milice, entre la sphère académique et la sphère militaire. Dans cette optique, l'idée récemment évoquée d'une « cyber école de recrues » nous semble pertinente. Le détachement de cryptologues mis en place au sein de la *Brigade d'aide au commandement 41* est également une initiative intéressante pour favoriser le transfert de connaissances.[74]

La Suisse est idéalement positionnée pour favoriser et accompagner l'émergence d'un Traité International du Cyberespace.

Le *GCSP* est une fondation internationale regroupant 45 États membres. Il est précurseur dans le domaine de la cyberdiplomatie et profite de la Genève internationale pour développer une gouvernance technique du réseau Internet en Suisse.[75] Autres atouts : notre neutralité pourrait permettre d'accompagner la résolution de cyber-conflits en étendant les bons offices au cyberespace[76] Avec ses nombreuses institutions internationales, la Suisse est idéalement positionnée pour favoriser et accompagner l'émergence d'un Traité International du Cyberespace.[77] Celui-ci pourrait offrir une base juridique pour réguler le cyberespace et pour poursuivre les auteurs d'infractions opérant dans différentes juridictions, ce qui n'est pas possible actuellement. *Microsoft* a appelé en février 2017 les États à signer une « convention digitale de Genève » (basée sur la *Convention de Genève* de 1949 relative à la protection des civils en temps de guerre) pour protéger l'usage civil du réseau Internet. En l'absence de souveraineté numérique, des multinationales risquent de se poser en gendarme du cyberespace et de dicter des régulations aux politiques. Rappelons que le droit à l'autodétermination est un principe reconnu par le droit international. Ce principe doit aujourd'hui également s'appliquer au cyberespace. Chaque peuple doit pouvoir disposer librement de son destin, y compris de son destin numérique. La maîtrise des données sur le plan individuel est une première étape vers une souveraineté collective. La souveraineté numérique doit donc être considérée comme un droit fondamental, car elle symbolise la maîtrise de notre destin sur les réseaux informatiques et *in fine* de nos libertés politiques, économiques et sociales.

74 Schmidlin, M. 2016. *Mit angewandter Mathematik zu mehr Sicherheit.* ASMZ.
75 Le cyberespace est un espace non régulé. En 2013, un groupe d'experts mandatés par l'*OTAN* a publié le *Manuel de Tallinn*. Ce manuel propose une transposition du droit international aux cyber-conflits et formule des recommandations non contraignantes. Il est disponible à cette adresse: https://ccdcoe.org/tallinn-manual.html (consulté 31.03.17).
76 La *Stratégie de politique étrangère 2016 – 2019* considère la cybersécurité comme un instrument de paix et de stabilité internationale.
77 Ghernaouti, S. 2017. *Pourquoi il faut une Déclaration de Genève du cyberespace.* Le Temps.

Marcus M. Keupp

Dr. oec., Dipl.-Kfm., Privat-docent Economie militaire
Titulaire de la chaire Economie de Défense à l'Académie militaire à l'EPF de Zurich (EPFZ)
E-mail: marcus.keupp@vtg.admin.ch

Alain Mermoud

Doctorant en systèmes d'information à HEC Lausanne et collaborateur scientifique à la chaire Economie de Défense à l'Académie militaire à l'EPF de Zurich (EPFZ)
Capitaine, officier de renseignement
E-mail: alain.mermoud@vtg.admin.ch

Dimitri Percia David

Doctorant en systèmes d'information à HEC Lausanne et collaborateur scientifique à la chaire Economie de Défense à l'Académie militaire à l'EPF de Zurich (EPFZ)
Capitaine, commandant de compagnie
E-mail: dimitri.perciadavid@vtg.admin.ch

La quatrième révolution industrielle et son impact sur les forces armées

Les évolutions technologiques en cours constituent globalement une révolution dans la mesure où elles ouvrent des perspectives entièrement nouvelles. Elles vont avoir des répercussions sur le comportement des individus, des collectivités publiques, des organisations les plus diverses et des entreprises et ainsi avoir un impact croissant sur la sécurité des sociétés et des individus.

Marc-André Ryter

De quoi s'agit-il?

Les pays et les sociétés civiles vont se développer en intégrant voire en subissant les évolutions technologiques. Celles-ci créent des opportunités dans tous les domaines de la société, et pourront être utilisées pour augmenter l'efficacité et la rapidité des processus. Pourtant, les nouvelles technologies vont aussi créer de nouveaux défis et de nouvelles vulnérabilités. Les pays vont être menacés différemment et il faudra qu'ils s'adaptent au nouvel environnement. Les nouvelles technologies auront de ce fait une influence directe et indirecte sur les défis posés aux forces armées et donc sur leur évolution. Elles vont remplacer des systèmes qui sont actuellement chers et compliqués. Si l'on combine les opportunités naissantes avec les nouvelles vulnérabilités qu'elles vont créer, on peut prévoir que les évolutions technologiques en cours vont influencer les relations entre les États dans le domaine de la sécurité dans un sens positif et négatif. La discussion actuelle sur l'introduction de ces nouvelles technologies se concentre surtout sur deux aspects radicalement opposés: d'une part les économies substantielles qui semblent possibles sur le long terme et d'autre part les coûts importants qui pourraient au départ constituer un facteur limitant. D'autant plus qu'il faudra instaurer un nouveau système de gouvernance et de contrôles qui aura lui aussi un coût. Les aspects liés à la sécurité de cette évolution sont par contre trop souvent absents du débat.

Le but de cet article est de sensibiliser aux conséquences de cette évolution et de mettre en évidence l'impact sur la sécurité et pour les forces armées, en particulier pour l'armée suisse, et de montrer à quel point les nouvelles technologies sont pertinentes pour son développement. Dans un futur prévisible, la plupart des innovations technologiques en cours seront intégrées dans le domaine de la défense, ceci indépendamment de la menace. Il est certain que des investissements importants seront nécessaires et donc qu'il y aura des conséquences non-négligeables sur les budgets militaires.

Cet article ne traitera pas des aspects éthiques de cette évolution, et en particulier de la dimension de l'éthique liée à l'autonomie des systèmes d'armes. Cette question est traitée dans un projet spécifique du domaine Doctrine militaire de l'état-major de l'armée et fera l'objet d'une prochaine publication[1].

La quatrième révolution industrielle, qui est ici en discussion, est constituée à la fois par la mise en réseau complète de la production et des processus et par le développement de nouvelles technologies qui l'appuient. En fait, elle consiste à intégrer les technologies digitales à toutes les fonctions constitutives de la vie et à intensifier le travail entre les humains et les machines. Les relations entre les humains et les machines ainsi qu'entre les machines entre elles vont évoluer par la délégation croissante aux machines de certaines qualités sensorielles, de mobilité et d'intelligence, ainsi que de certaines compétences décisionnelles.

Partout, l'évolution technologique amène des progrès: l'efficacité et l'efficience des systèmes sont améliorées, la coordination entre les systèmes et la gestion des actions par les systèmes sont optimisées. L'analyse intégrée d'un plus grand nombre de données doit permettre d'opérer de manière plus flexible et surtout innovatrice. L'information et les idées se répandent instantanément et à l'échelle planétaire, sans que les personnes n'aient besoin de se déplacer. Mais ce ne sont là que quelques exemples d'applications concrètes générées par les évolutions technologiques.

1 Martin Krummenacher: «Letale autonome Waffensysteme – Fluch oder Segen? Ethische Betrachtungen und sozialtechnische Vergleiche» (Arbeitstitel).

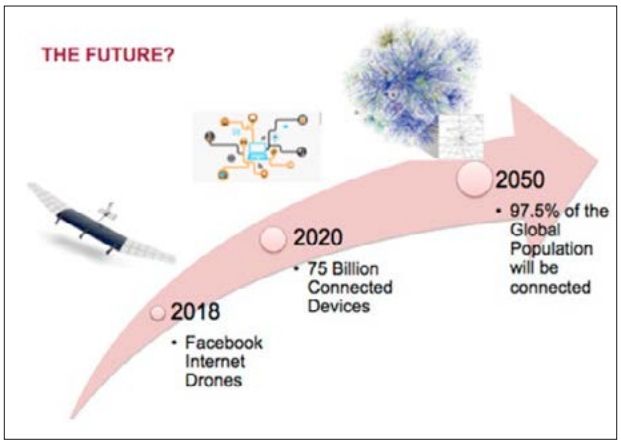


Illustration 1 L'évolution de la connectivité. (www.isaca.org)

Si l'on se base sur le fait qu'en 2015, il y avait encore 85 % des machines qui n'étaient pas connectées et près de 80 % des données qui n'étaient pas classées et donc pas utilisables pour générer du savoir, on réalise le saut qualitatif qui est encore à venir.

Celles-ci se baseront sur une multiplication des objets connectés et une augmentation exponentielle du volume des données disponibles et à traiter. Ceci aura de telles répercussions que l'on peut parler d'un changement de paradigme, d'où la notion de quatrième révolution industrielle.[2] L'évolution la plus significative concerne le volume des données qui vont être générées et échangées et la prise de contrôle par les algorithmes. Entre 2015 et 2020, il y aura 15 fois plus de données générées par des machines. Durant la même période, il y aura aussi 50 fois plus de données stockées. Si l'on se base sur le fait qu'en 2015, il y avait encore 85 % des machines qui n'étaient pas connectées et près de 80 % des données qui n'étaient pas classées et donc pas utilisables pour générer du savoir, on réalise le saut qualitatif qui est encore à venir.[3] L'intelligence artificielle sera de plus en plus nécessaire ne serait-ce que pour trier la masse de données qui va être générée. Il est préoccupant de constater que la question de la sécurité est insuffisamment intégrée dans cette évolution, ce qui va obligatoirement impliquer des coûts importants, plus élevés que l'acquisition, lorsqu'il s'agira de mettre à jour la sécurité des systèmes.

L'attrait de la quatrième révolution industrielle provient de l'immense potentiel d'amélioration présumé dans de très nombreux domaines de notre vie. Il sera donc très difficile de freiner, voire de contrôler les développements dans ce domaine, malgré des risques qui ne sont pas encore complètement évalués, comme la possibilité pour des ma-

Illustration 2 Drone américain Instant Eye. (www.usni.org)

Illustration 3 Robot LS3 (Legged Squad Support Systems) de Boston Dynamics. (www.bostondynamics.com)

Illustration 4 Multi-Utility Tactical Transport (MUTT) de General Dynamics Land Systems. (www.defensetech.org/2014/09/25)

Illustration 5 Exemples de «Lethal Autonomous Robotics» (LARS) et de robots armés autonomes. (https://artselectronic.wordpress.com/2013/05/25/lars-lethal-autonomous-robotics/ et http://www.article36.org/statements/ban-autonomous-armed-robots)

Illustration 6 Armes dans l'espace. (https://sofrep.com/60485/60485/)

Illustration 7 Meegaperf, casque EEG (pour électroencéphalographie) de la société Physip qui mesure l'activité cérébrale de son porteur et en déduit son état de stress et de fatigue. (http://hightech.bfmtv.com/produit/l-equipement-high-tech-au-service-du-soldat-du-futur-984618.html)

Illustration 8 GBU-44/E Viper Strike smart munition. (http://www.deagel.com/library/GBU-44E-Viper-Strike-smart-munition_m02012041700001.aspx)

2 Voir: Bloem, Jaap, van Doorn, Menno, Duivestein, David, Maas, René et van Ommeren, Erik: «The Fourth Industrial Revolution: Things to Tighten the Link Between IT and OT», VINT Research Report 3, Groningen, 2014, p.4.

3 Tous ces chiffres dans Wind River Systems: The Internet of Things for Defense, White Paper, 10/2015, p. 3., disponible sous http://events.windriver.com/wrcd01/wrcm/2016/08/WP-IoT-internet-of-things-for-defense.pdf (consulté le 21.03.2016).

chines dans le futur d'échapper au contrôle des humains. Il est d'ores et déjà possible de dire que l'usage qui est fait du Big Data n'est plus sous contrôle, respectivement que ceux qui contrôlent une partie de ce Big Data, en particulier le Cloud, possèdent un pouvoir considérable.

Mais il y a aussi d'autres risques, beaucoup plus terre-à-terre, qui provoqueront des tensions. La production des systèmes liés aux nouvelles technologies requiert une grande quantité de matériaux rares. Il y aura donc une compétition croissante pour ces ressources. De plus le fonctionnement de ces systèmes nécessite beaucoup d'énergie, ce qui a des conséquences importantes et coûteuses sur le développement de l'infrastructure énergétique.

Il se pourrait même qu'à un certain moment, l'intelligence artificielle prenne le dessus sur l'intelligence humaine, surtout en raison de sa vitesse d'évolution.

A plus long terme, le développement de l'intelligence artificielle pourrait avoir des conséquences qui ne sont à l'heure actuelle pas prévisibles. Il se pourrait même qu'à un certain moment, l'intelligence artificielle prenne le dessus sur l'intelligence humaine, surtout en raison de sa vitesse d'évolution. Ce sujet, étudié sous le label de la *singularité technologique*, n'est cependant pas abordé dans cet article.

De quelles évolutions technologiques parle-t-on?
Il s'agit de différencier les technologies de leurs applications. Les technologies suivantes, associées à la quatrième révolution industrielle, sont le plus souvent citées. Elles sont avant tout civiles, mais ont un impact sur la sécurité du fait qu'elles peuvent être appliquées aux forces armées et à la conduite de la guerre et de manière plus générale être utilisées pour nuire:

- Intelligence artificielle;
- Internet des objets;
- Robots de nouvelle génération;
- Big Data;
- Biologie synthétique;
- Substances nootropiques;
- Impression 3 ou 4D;
- Calculateur quantique;
- Technologies neuromorphiques;
- Energie renouvelable, produite sur place;
- Nanotechnologies.

Certaines de ces technologies ont déjà des applications pour les forces armées, et pour d'autres, ces applications sont encore à développer. La combinaison de ces technologies peut ouvrir de nouveaux horizons et générer des applications qui sont pour le moment encore inconnues. Klaus Schwab cite par exemple les possibilités d'agir directement sur le système nerveux des combattants.[4]

Pour le moment, la discussion sur les nouveaux équipements qui peuvent être utilisées sur le champ de bataille porte sur les applications suivantes:

- Drones;
- Robots de combat;
- Véhicules autonomes;
- Armes autonomes;
- Armes dans l'espace;
- Exosquelettes et autres équipements servant à améliorer les performances des combattants;
- Munitions intelligentes;
- Substances permettant d'améliorer l'efficacité des combattants;
- Armes cybernétiques[5];
- Armes biologiques et biochimiques.[6]

Il est donc important de suivre l'évolution de ces technologies et de leurs applications potentielles afin d'en déduire lesquelles sont susceptibles d'être utilisées par un adversaire et partant lesquelles devraient être introduites dans l'armée suisse ou au minimum doivent être prises en compte. Il faudra surtout s'occuper de développer les réponses à ces technologies afin de protéger nos soldats et notre population en fonction de deux aspects principaux. D'abord, il faudra être capable de contenir et de garder sous contrôle la diffusion et les capacités de nuire de ces nouvelles technologies, en particulier de celles à double-usage (dual-use). Ensuite, il va s'agir de s'assurer que nos processus de décision et d'introduction de nouveaux matériels puissent le cas échéant être assez rapides et flexibles pour nous permettre de développer et de mettre en œuvre les options retenues à temps.

Selon l'agence européenne de la défense, il y a actuellement quatre facteurs qui évoluent très vite et qu'il faut intégrer dans les réflexions sur le développement technologique des forces armées:

- La compétition globale pour la supériorité technologique;
- L'émergence de nouveaux domaines de connaissances et des technologies convergentes;
- Les cycles d'innovations toujours plus rapides;
- L'importance croissante des investissements privés pour l'innovation.[7]

La combinaison de ces quatre facteurs est déjà une réalité et constitue le véritable caractère révolutionnaire de l'évolution technologique.

4 Voir: Schwab, Klaus, «The Fourth Industrial Revolution», WEF, 2016, p. 88.

5 Les possibilités de ces armes sont expliquées notamment dans l'article de Freedberg, Sydney J. Jr, «Wireless Hacking In Flight: Air Force Demos Cyber E-130», disponible sous http://breakingdefense.com/2015/09/wireless-hacking-in-flight-air-force-demos-cyber-ec-130/, consulté le 21.03.2017.

6 Pour une vue d'ensemble et une analyse détaillée de toutes les nouvelles technologies relevantes dans le domaine de la sécurité, se référer à l'ouvrage de Ladetto, Quentin: «Technologiefrüherkennung: Trends und Potenziale 2015 – 2025», armasuisse Wissenschaft + Technologie, Thun, 2015.

7 Voir: «The next industrial (r)evolution: What implications for the security and defence sector?», in *European defence Matters*, European Defence Agency, Nr. 10/2016, p. 13.

La quatrième révolution industrielle et son impact sur la sécurité

La quatrième révolution industrielle est comme une pièce avec ses deux faces. D'un côté, les progrès technologiques possibles ouvrent des perspectives positives qui laissent envisager une meilleure sécurité, une plus grande interopérabilité entre les systèmes, une réduction des coûts, une meilleure efficacité et rapidité. Ces nouvelles capacités vont bénéficier à la fois aux secteurs civil et militaire, et permettre une meilleure préparation aux situations extraordinaires, avec ou sans l'engagement de forces armées. Par contre, ces progrès technologiques impliquent aussi une gamme très large de vulnérabilités et donc de perturbations et manipulations possibles. A ceci s'ajoute le fait que le risque d'erreurs humaines en raison de la complexité toujours croissante est plus élevé. En effet, la gestion de ces nouveaux risques nécessite des ressources et des compétences souvent nouvelles qui impliquent une élévation massive des interdépendances. Pour les forces armées, cela implique une interdépendance croissante entre les composantes, mais aussi et surtout envers l'extérieur. De plus, la gestion des nouveaux risques génère une lourde charge sur les utilisateurs, car il s'agit de prévenir des incidents qui auraient des conséquences graves pour les sociétés.

L'hyperconnectivité profite ainsi aux acteurs non-étatiques et élargit leurs possibilités d'actions ainsi que leur emploi en tant que proxy.

Schwab parle d'une évolution qui va vers ce qu'il appelle l'hyperconnectivité.[8] Selon lui, cette hyperconnectivité va encore accroître les inégalités dans le monde, et donc le fractionner encore plus. Comme cela a déjà été démontré, ces phénomènes créent les conditions favorables aux extrémismes de tous bords et contribuent au renforcement de la menace contre les États et les sociétés. L'hyperconnectivité profite ainsi aux acteurs non-étatiques et élargit leurs possibilités d'actions ainsi que leur emploi en tant que proxy. Elle donne plus d'options pour des actions criminelles, des actes de terrorisme ou de chantage, y compris à des acteurs possédant de faibles ressources. Il s'agit ici plus d'une évolution déjà en cours, qui peut cependant aboutir à des conséquences bien plus menaçantes que ce que nous connaissons pour l'instant. L'usage à très large échelle des médias sociaux afin de décrédibiliser des institutions de manière ciblée au moyen de propagande peut provoquer et attiser des troubles sociaux importants. Il s'agit toutefois d'une arme à double tranchant qui peut être utilisée de la même manière par les gouvernements.

De nombreux risques faisant partie intégrante de l'évolution technologique peuvent remettre en cause le fonctionnement des sociétés et constituent donc des menaces existentielles. Leur potentiel destructeur est très élevé et génère un sentiment de vulnérabilité par rapport à cette évolution. Les risques sont le plus souvent liés au stockage de données et aux contrôles nécessaires qui en découlent. Les doutes les plus évidents concernent le contrôle de ce qui se passe avec les données accumulées et les possibilités d'usages détournés ou malhonnêtes que va ouvrir la mise en réseau de plus en plus d'informations.

De plus, on ne sait pas toujours quelles bases légales s'appliquent, surtout lorsque l'on ne sait même pas précisément où se trouvent les données stockées (cloud), à qui elles appartiennent, qui peut les consulter, les utiliser ou les modifier et surtout lorsque les connections entre elles sont peu claires. Il faut prévoir une possibilité de faire corriger ou éliminer de fausses informations et prévenir dans toute la mesure du possible une utilisation frauduleuse. Autant de questions essentielles qui ne sont pour le moment pas réglées. Et lorsque l'on sait que la gestion des banques de données et le développement des programmes pour ce faire sont déjà automatisés et s'appuient sur l'intelligence artificielle[9], on prend conscience des enjeux derrière le Big Data.

De plus, on ne sait pas toujours quelles bases légales s'appliquent, surtout lorsque l'on ne sait même pas précisément où se trouvent les données stockées (cloud), à qui elles appartiennent, qui peut les consulter, les utiliser ou les modifier et surtout lorsque les connections entre elles sont peu claires.

Trois groupes de risques principaux sont en ce moment étudiés par les scientifiques.[10] En premier lieu, tous les risques liés à une programmation incomplète des machines et qui pousseraient les robots dotés d'une intelligence artificielle à ne pas effectuer correctement la mission initialement prévue. On aurait affaire dans ce cas à des effets secondaires négatifs. Deuxièmement, les robots pourraient exécuter leur mission jusqu'à un point extrême qui n'est pas recherché. Ces effets de saturation entraînent des comportements qui peuvent se révéler dangereux. Enfin, l'intelligence artificielle implique une certaine autonomie des machines, qui pourraient aller au-delà de ce qui était pensé, avec là encore des effets négatifs. Ces dérives de l'autonomie constituent sans doute le plus grand danger pour des machines qui ont une capacité d'apprentissage autonome.

Le défi suivant consiste dans le triage et la vérification des informations. Déjà aujourd'hui, de fausses informations peuvent être créées intentionnellement et distribuées à large échelle très rapidement, poussant à des comportements irrationnels. Il devient de plus en plus facile de manipuler les foules et de créer des groupes de protestataires persuadés de leur bonne foi.

Ces *dérives de l'autonomie* constituent sans doute le plus grand danger pour des machines qui ont une capacité d'apprentissage autonome.

8 Voir: Schwab, Klaus, «The Fourth Industrial Revolution», WEF, 2016, p. 80.

9 Voir: Tuck, Jay: «Evolution ohne uns», Kulmbach, Plassen Verlag, 2016, p. 32.

10 Cités par Demeure, Yohan: «Les risques liés à l'intelligence artificielle enfin pris au sérieux», Science et Vie, 05.07.2017, p. 2.

Illustration 9 Système MS-177 multi-spectral imaging (MSI) avec senseurs de renseignements à longue distance, surveillance et reconnaissance (ISR), monté sur un Northrop Grumman RQ-4B Global Hawk Unmanned Aircraft System. (http://www.unmannedsystemstechnology.com/2016/07/utc-aerospace-systems-to-integrate-isr-sensor-onto-global-hawk-uas/)

Le risque est de plus en plus élevé que la sécurité de l'individu soit remise en question par le déni d'accès à des services essentiels pour ce qui est encore trop souvent considéré comme faisant partie du bien-être, mais qui en fin de compte concerne la survie. La manipulation de la distribution d'eau, d'électricité ou d'hydrocarbures peut rapidement créer des situations de détresse. La perturbation des communications, de l'approvisionnement en denrées alimentaires, du réseau de santé ou du trafic aérien, routier ou ferroviaire peut rapidement mettre en danger le fonctionnement des sociétés.

L'évolution technologique comprend encore d'autres risques qui peuvent être exploités pour nuire et sont de ce fait significatifs d'un point de vue militaire. La rapidité de l'évolution des composants et des programmes crée de facto des vulnérabilités liées au fait que ces éléments sont rapidement dépassés s'ils ne sont continuellement mis à jour, créant par là une dépendance des consommateurs par rapport aux fournisseurs. Une autre vulnérabilité provient de la complexité croissante des réseaux et de l'impossibilité de les protéger complètement, en particulier face aux piratages informatiques. Cette quasi-impossibilité pousse de plus en plus d'organisations, étatiques ou non, à fonctionner sur des réseaux fermés.[11]

En résumé, les sociétés devront intégrer les risques issus des évolutions technologiques afin de garantir leur sécurité et en particulier la paix sociale. Il est difficile de prévoir les conséquences d'une automatisation à outrance et de la suppression des postes de travail pour les humains qui peut en découler.

Implications sur la défense et les forces armées

L'utilisation croissante par les forces armées de technologies de pointe n'est pas en soi une chose nouvelle. La notion de guerre en réseau (network centric warfare / network enabled operations) a déjà été intégrée dans les forces armées de la majorité des pays à des degrés divers depuis de nombreuses années. Au départ, il s'agissait de relier entre elles les différentes composantes des forces et de mettre à disposition des militaires des liaisons rapides et multiples avec différents types de senseurs (drones, satellites, etc.).

Comme le secteur de la défense n'est plus le déclencheur principal des évolutions technologiques, il devra s'adapter aux innovations venues de l'industrie civile.

Les évolutions en cours nécessiteront une adaptation des forces armées, afin que celles-ci soient prêtes à faire face aux surprises stratégiques possibles. Comme le secteur de la défense n'est plus le déclencheur principal des évolutions technologiques, il devra s'adapter aux innovations venues de l'industrie civile. Cette adaptation touchera le noyau de la capacité de défense, et ne constituera pas simplement un suivi de l'évolution des technologies utilisées actuellement. Elle va permettre d'aller au-delà du C4ISTAR actuel, principalement en raison du développement de la dimension informationnelle et d'une automatisation plus poussée. L'importance de la maîtrise de l'information va devenir toujours plus essentielle afin d'établir et de garder une supériorité opérationnelle relative.[12]

La capacité à choisir et décider mieux et plus vite que l'adversaire, en restant protégés de fausses informations et de manipulations de systèmes, est donc centrale.

11 Même si le cas STUXNET a démontré qu'une coupure complète des réseaux avec l'extérieur (air gap) ne constitue plus une protection absolue.

12 Voir: Goetz, Pierre et Cahuzac-Soave, Olivia: «Impact de la numérisation sur l'exercice du commandement», Compagnie Européenne d'Intelligence Stratégique (CEIS), Les notes stratégiques, décembre 2015, pp. 11 – 12.

Illustration 10 Quelques possibilités d'améliorer les capacités des soldats. (http://www.defenseone.com/technology/2015/10/talking-helmets-robot-built-bases-army-peers-future-3d-printing/122551/)

Illustration 11 De plus en plus d'informations vont pouvoir être intégrées dans l'image du champ de bataille. (http://armypress.dodlive.mil/2016/09/26/big-data-war-games-necessary-for-winning-future-wars/(consulté le 01.03.2017))

La supériorité dans le domaine de l'information doit permettre d'assurer certains avantages sur le terrain, comme la capacité à surprendre l'adversaire, la disponibilité et l'adéquation des moyens, la rapidité de l'action ou la flexibilité de la réaction. La capacité à effectuer le bon choix entre les différentes options, et de concentrer les moyens au moment et à l'emplacement corrects demeureront des facteurs opérationnels décisifs. La capacité à choisir et décider mieux et plus vite que l'adversaire, en restant protégés de fausses informations et de manipulations de systèmes, est donc centrale. De nouveaux systèmes, capables de connecter les capteurs, les systèmes de prise de décision du commandement, les systèmes de contrôle et les systèmes d'armes automatisés ou autonomes sont en cours de développement et seront introduits à terme dans les forces armées. En plus, des systèmes permettant l'évaluation permanente de la situation seront aussi connectés afin d'améliorer la conduite. Cependant, même si les réactions sont plus rapides et plus précises, l'automatisation de la décision dans le domaine militaire et le fait que des machines puissent être programmées pour combattre de manière autonome restent des sujets sensibles, principalement en raison des dimensions éthiques.

De plus en plus, les innovations issues de la recherche civile se répercutent sur le militaire avec leurs risques et leurs nouvelles vulnérabilités. Il y a donc un inversement complet en raison des coûts de la recherche, du développement, de la production et d'exploitation. Toutefois, les technologies reprises dans le domaine militaire font en principe l'objet d'adaptations afin que leur sécurité, en plus de leur fiabilité et résistance, soit accrue.

D'un point de vue militaire, plusieurs aspects doivent être pris en compte de manière prioritaire. L'évolution des technologies va permettre l'utilisation accrue, tant quantitativement que qualitativement, de nouvelles dimensions, en particulier l'espace et les profondeurs maritimes. Ensuite, l'analyse de plus d'informations dans des délais plus rapides va créer un avantage en permettant d'ajuster en permanence les actions tactiques et la conduite interforces. Il y aura ainsi une amélioration sensible de la compréhension du champ de bataille (battlespace awareness) qui s'appuiera sur une meilleure transparence, malgré les contre-mesures qui seront immanquablement développées. Les systèmes pourront plus facilement reconnaître les positions, dispositifs et déplacements de troupes. Finalement, le soutien et la coordination interarmes seront améliorés, les munitions deviendront plus intelligentes, avec moins de dommages collatéraux. Ceci sera particulièrement avantageux en milieu urbain et lors de l'utilisation d'une stratégie hybride, où les civils seront toujours mélangés aux combattants et où ces derniers sont parfois difficiles à identifier.

Mais il y aura aussi des conséquences négatives. Un adversaire aura plus de possibilités pour influencer et perturber la conduite militaire de l'adversaire à tous les échelons. Il peut agir sur ses senseurs, qui sont de plus en plus nombreux, sur ses réseaux de communication en tous genres ainsi que directement sur ses systèmes de conduite ou sur les fournisseurs extérieurs dont dépendent de plus en plus les forces armées. L'adversaire pourra avoir la possibilité d'accéder aux informations-clés et de les modifier afin de créer une fausse image de la situation. Une protection suffisante des systèmes constituera donc une absolue nécessité, tout en sachant qu'une seule erreur de manipulation peut ouvrir une brèche pour l'adversaire. Cette protection sera renforcée par des technologies de vérification (cross-check) basées sur l'intelligence artificielle qui deviendront incontournables. En raison de la complexité de leurs systèmes, qui relieront de nombreux équipements et impliqueront de nombreux programmes, avec des connections et des points d'entrée multiples, les applications militaires seront particulièrement vulnérables aux disfonctionnements les plus divers et aux perturbations.

L'introduction de nouvelles technologies devient nécessaire voire incontournable car la quantité d'informations disponibles pour prendre une décision juste a augmenté de manière exponentielle. L'utilisation de stratégies hybrides crée aussi un besoin d'informations plus grand, car il devient plus difficile de savoir ce qui ce passe. Une image plus précise du champ de bataille est à son tour nécessaire pour identifier en continu les nouveaux besoins en informations. La question qui se pose est de savoir si toutes les informations disponibles pourront être analysées avec la pertinence et dans les délais nécessaires, et si les informations relevantes pourront être identifiées au sein d'un nuage formé par un nombre quasi infini de données. Le risque est très élevé de se perdre dans les détails, de ne plus pouvoir différencier les informations et de recourir à une automatisation du triage qui serait en soit défaillante.

L'introduction de nouvelles technologies devient nécessaire voire incontournable car la quantité d'informations disponibles pour prendre une décision juste a augmenté de manière exponentielle.

La numérisation aura un impact majeur sur toutes les phases du cycle OODA (observer, orienter, décider, agir), car les nouvelles technologies appuient l'ensemble des activités développées à chaque étape du cycle.[13] En particulier, l'observation sera faite en intégrant plus de données, l'orientation pourra s'appuyer sur la simulation, la décision sur de nombreux outils d'aide à la décision et l'action sur une donnée d'ordres numérisée. En plus, l'amélioration de la communication, de l'échange et du traitement d'informations aura des conséquences jusque dans les lignes d'approvisionnement.

La « biosphère », soit ce qui se passe à l'intérieur des corps des combattants, va de plus en plus devenir un espace à considérer dans le contexte militaire.

Les nouvelles technologies ne s'appliqueront pas seulement aux machines, mais aussi aux combattants. Ceux-ci pourraient voir leurs capacités au combat améliorées par des mesures techniques et chimiques. Les progrès biologiques permettront une meilleure résistance à la douleur, à la peur et au stress. La « biosphère », soit ce qui se passe à l'intérieur des corps des combattants, va de plus en plus devenir un espace à considérer dans le contexte militaire.

L'engagement de robots dans les forces armées, tout comme dans les domaines non-militaires, doit avant tout libérer les soldats des tâches dangereuses, sales et répétitives[14], et dans des domaines où le besoin de conduite est limité voire absent. Certes, les robots ont l'avantage de ne pas être sensibles à la fatigue, garantissent une meilleure précision et ont plus de force que les humains, mais ils ont aussi besoin de techniciens pour leur entretien et ont des limites lorsqu'il s'agit de réagir face aux changements, ce qui est particulièrement limitatif en phase de combat. C'est pourquoi, les robots offrent de très bonnes perspectives avant tout dans les domaines de la logistique (en particulier pour la maintenance) et des transports. Cependant, d'autres applications sont également envisageables pour des mini-drones ou des robots de petites tailles, comme par exemple des missions de sabotage. L'avantage est qu'il sera possible de déclencher l'opération en donnant la mission aux robots ou drones et qu'ensuite, ces machines pourront accomplir leur mission de manière autonome et sans nécessiter de conduite. Bien sûr, ce genre d'actions est susceptible d'échouer en raison de la fragilité des machines et en particulier de leurs senseurs, caméras, microphones, GPS, etc. voir même de leurs moteurs.

Les innovations technologiques permettent d'améliorer à la fois les processus de conduite, les performances des soldats et des armements.

Ces réflexions montrent qu'il y a très clairement deux domaines bien différents qui sont concernés par l'introduction de nouvelles technologies dans les forces armées. En premier lieu, certaines technologies permettent d'améliorer les prestations de bases et l'établissement de la disponibilité de base, principalement en automatisant de nombreuses fonctions. Les senseurs permettront de n'effectuer des maintenances sur le matériel que lorsque celles-ci sont réellement nécessaires. Ensuite il y a le niveau de la conduite des opérations, jusqu'à l'échelon du soldat. Les innovations technologiques permettent d'améliorer à la fois les processus de conduite, les performances des soldats et des armements. Des capteurs portés par les soldats permettront en temps réel d'identifier les mesures à prendre pour garantir une efficacité maximale au combat et donneront des indications qui constitueront un facteur nouveau et important pour la prise de décision. Les nouvelles technologies s'avèrent ainsi adaptées à la fois lorsqu'il s'agit de gérer de nombreux sites et de nombreux outils ou machines et lorsqu'il s'agit de coordonner des processus à différents échelons.

En raison de son potentiel prometteur d'amélioration, l'intelligence artificielle va certainement être utilisée de manière croissante dans les forces armées. Ce développement se fera en fonction de cinq facteurs qui joueront tous un rôle clé :

- la rapidité du travail des machines dans tous les domaines, comme l'analyse des données, l'alerte, la défense dans le cyberespace, la conduite de la guerre électronique par exemple ;
- la complémentarité croissante entre l'homme et la machine, en particulier dans le processus de prise de décision ;

13 Voir: Goetz, Pierre et Cahuzac-Soave, op. cit., pp. 14 – 15.
14 Voir: Bloem, op. cit, p.13. Il parle de la capacité des robots à s'occuper de tout ce qui est couvert par les 3 D: «dirty, dangerous and dull work».

– l'amélioration des capacités des soldats à analyser leur environnement et à réagir de manière adéquate ;
– l'engagement combiné d'hommes et de machines afin d'améliorer l'efficience ;
– l'engagement de systèmes d'armes autonomes, qui seront résistants aux attaques cyber et électroniques.[15]

Ceci montre une fois de plus que la plupart des nouvelles technologies joueront un rôle central aussi bien dans les forces armées que dans le domaine civil. La problématique du double emploi, liée à celle de la prolifération, aura des implications importantes dans le domaine de la sécurité. Une densité de plus en plus élevée de capteurs et senseurs va créer des systèmes de systèmes qui seront chargés de fusionner la multitude de données, ce qui va générer des besoins de protection considérables à tous les niveaux. La facilité d'utilisation restera elle aussi un enjeu majeur.

Impact sur la doctrine et le champ de bataille

Il apparaît donc évident que l'évolution technologique va avoir un impact sur la nature des conflits et engendrer une métamorphose plus ou moins rapide du champ de bataille. Il est cependant encore difficile de prédire exactement comment et jusqu'à quel point les nouvelles technologies vont changer la manière avec laquelle les pays vont conduire leurs opérations et quel sera leur impact sur les guerres. En particulier, il va être toujours plus difficile de clairement faire une distinction entre l'état de paix et l'état de guerre. De même, la distinction entre combattants et non-combattants sera un défi majeur des conflits futurs.[16] Ces derniers seront toujours plus caractérisés par une combinaison d'actions à l'échelon local et à l'échelon global et ceci dans les différentes dimensions du conflit, en d'autres termes dans les différentes sphères d'opérations. Ils constitueront un mélange d'actions militaires et / ou terroristes à une très petite échelle avec des campagnes de grandes envergure, le tout soutenu par de la propagande locale et globale. Les conflits seront caractérisés par une combinaison de toutes sortes d'actions allant de la conduite de la guerre classique à des actions couvertes qui ne sont en principe pas associées à des forces militaires étatiques classiques. Les médias sociaux joueront un rôle de plus en plus grand, que ce soit dans le domaine de la propagande et de la désinformation ou du recrutement. Le potentiel exact des nouvelles technologies ne prête pas à beaucoup d'optimisme car de nouvelles armes au sens large seront plus faciles à acquérir et elles pourront plus facilement causer des dommages à large échelle.

… la distinction entre combattants et non-combattants sera un défi majeur des conflits futurs.

L'évolution des technologies vise à diminuer les incertitudes du champ de bataille. Cependant, et malgré le développement exponentiel de la masse d'informations disponible à tous les niveaux, il est peu probable que la surprise disparaisse du champ de bataille. Il y aura des limites aux capacités à anticiper les décisions de l'adversaire, malgré des moyens de soutien toujours plus performants. Les évolutions technologiques vont également augmenter les possibilités de surprendre l'adversaire[17], principalement grâce aux possibilités de l'induire en erreur. Ainsi, dans le domaine de l'information, les nouvelles technologies impliqueront à la fois des chances et des risques. Elles fourniront de nouvelles possibilités d'entretenir le doute et de donner une fausse image des intentions d'action par la diffusion augmentée de fausses informations. Les nouvelles technologies augmenteront à la fois la capacité à éviter la surprise et l'aptitude à surprendre.

Une autre conséquence de l'évolution technologique sera la mise à disposition immédiate de plus d'informations jusqu'à l'échelon du soldat. Ainsi, il sera possible d'engager des drones qui transmettront leurs images directement au soldat afin de lui donner une image précise de son environnement immédiat. De même, des senseurs sur les hommes et les machines permettront d'avoir une image de l'état physique des combattants et des besoins de maintenance des systèmes. En particulier pour ces derniers, ces indications permettront de prévoir les besoins de maintenance et d'améliorer de manière substantielle leur disponibilité. Cela pourrait s'avérer essentiel dans des domaines aussi sensibles que la disponibilité des avions de combat.[18]

Les nouvelles technologies augmenteront à la fois la capacité à éviter la surprise et l'aptitude à surprendre.

Des questions fondamentales se posent dans ce contexte à propos du futur rôle du soldat. Celui-ci va évoluer et le soldat pourrait perdre de son autonomie, respectivement de sa liberté à décider comment combattre dans une situation donnée. A l'échelon des formations, l'évolution dans le domaine de la conduite pourrait remettre en cause la *Auftragstaktik* et favoriser une conduite plus rigide dans le sens de la *Befehlstaktik*. Mais d'un autre côté, si l'on considère la masse d'information et les possibilités de diffuser des fausses informations qui proviennent des nouvelles technologies, il apparaît évident que le soldat devra garder une faculté d'analyse et de décision propre. Il se peut même que se pose la question de la confiance que pourront placer les chefs militaires et les soldats dans les systèmes sensés les aider. Ainsi, il sera nécessaire d'engager les nouvelles technologies pour appuyer les militaires plutôt que pour les remplacer.[19] Les systèmes doivent donc être considérés comme un appui aux capacités analytiques du soldat, qui restera l'élément central qui interagit avec le milieu où il se trouve et les acteurs présents dans cet

15 Voir: Hwang, Jennie S.: «The Fourth Industrial revolution (Industry 4.0): Intelligent Manufacturing», SMT Magazine, July 2016, p.14.
16 Voir: Schwab, Klaus, «The Fourth Industrial revolution», in Foreign Affairs, December 2015.
17 Voir: Hémez, Rémy: «L'avenir de la surprise tactique à l'heure de la numérisation», études de l'Ifri, N0 69, Juillet 2016, pp. 25 – 27.
18 Voir: Mariani, Joe, Williams, Brian and Loubert, Brett: «Continuing the march: The past, present, and future of the IoT in the military», Deloitte University Press, 2015, pp. 11 – 13.
19 Voir: Wood, Colin, D.: «The Human Domain and the Future of Army Warfare: Present as Prelude for 2050», in Small Wars Journal, August 2016, p. 3.

environnement. Les qualités d'analyse des individus resteront essentielles dans l'optique de garantir la résilience d'un système qui sera ainsi capable de mieux s'adapter à l'évolution du combat.

A l'échelon des formations, l'évolution dans le domaine de la conduite pourrait remettre en cause la Auftragstaktik et favoriser une conduite plus rigide dans le sens de la Befehlstaktik.

La nature même de la conduite du combat va être affectée par les évolutions technologiques. La question se posera de savoir jusqu'à quel point l'on pourra laisser des robots ou d'autres armes à intelligence artificielle mener le combat de manière autonome, c'est-à-dire sans que les actions ne soient dirigées par l'être humain. Jusqu'où peut-on automatiser le combat, peut-on déléguer la décision d'ouvrir le feu ? Ces aspects éthiques concernent en premier lieu la décision de tirer sans intervention humaine, mais d'autres actions sont à considérer, comme par exemple les mesures que pourraient prendre les machines pour assurer leur survie.

La prédominance du secteur civil dans le développement des nouvelles technologies a également des conséquences pour la doctrine. Le marché civil, qui est orienté uniquement sur le gain, progresse rapidement. De nouvelles possibilités apparaissent à un rythme élevé. Les doctrines des forces armées ne peuvent évoluer aussi vite, respectivement ne peuvent constamment s'adapter en raison d'une nouvelle percée technologique. Il faudra donc redéfinir ce que doit contenir une doctrine, comment elle peut évoluer et surtout identifier les évolutions significatives. La conséquence sera un décalage croissant entre les possibilités technologiques existantes et les systèmes en usage dans les forces armées.

Les qualités d'analyse des individus resteront essentielles dans l'optique de garantir la résilience d'un système qui sera ainsi capable de mieux s'adapter à l'évolution du combat.

Globalement, les nouvelles technologies vont générer de nouveaux risques pour les forces armées, risques qui peuvent être classés en six groupes distincts :

(1) En premier lieu, les efforts en vue de constamment raccourcir la durée du cycle de décision et d'accroître le volume d'informations analysées provoque une augmentation du nombre d'interactions tout au long de la chaîne de commandement et augmente donc le nombre de possibilités d'erreurs. (2) Ensuite, l'avantage de pouvoir réagir rapidement lorsque la situation évolue très vite implique aussi le risque de voir les échelons supérieurs s'impliquer directement dans les décisions et dans la conduite de l'échelon tactique. (3) Les capacités des systèmes vont susciter des attentes toujours plus élevées de la part des décideurs, ce qui peut entraîner des paralysies systémiques pour plusieurs raisons. D'abord, dans le cas où aucune décision n'est prise car on attend toujours des informations complémentaires, ensuite, si personne ne décide en raison de l'attente d'instructions. Enfin, dans les cas où les systèmes donnent des indications jugées insuffisantes. (4) Les systèmes de transmissions des données deviennent fragiles en raison des volumes importants à transmettre, ce qui génère des perturbations et un ralentissement généralisé des cycles de décision. (5) Les bonnes informations ne peuvent plus être identifiées dans la masse de données à disposition. (6) L'augmentation du volume de données et d'informations disponibles, ajoutées à la multiplication des interventions de parties prenantes toujours plus nombreuses, peut facilement générer le chaos.

La possibilité de voir des pays ou acteurs s'affronter sur un champ de batailles uniquement par l'intermédiaire de robots est parfois évoquée par certains auteurs.[20] Elle est cependant à considérer avec précaution pour plusieurs raisons. En premier lieu, il est difficile, dans la plupart des pays et en particulier en Europe, d'imaginer de larges zones non habitées et dans lesquelles des guerres entre robots pourraient se dérouler. Ensuite, même lors de batailles dans des zones inhabitées, des combats entre robots ou autres machines auront certainement des conséquences pour les populations en cas de destructions ou de dommages faits aux infrastructures critiques.

Le cyberespace comme champ de bataille particulier

Traiter le cyberespace en particulier se justifie par le fait qu'une guerre dans cet espace est souvent considérée comme la menace principale liée aux développements technologiques en cours. La cyberguerre et les cybervulnérabilités sont souvent évoquées lorsqu'on évoque les nouvelles technologiques et leur impact sur la sécurité, même si leur potentiel demeure souvent négligé. Des secteurs entiers de la société peuvent être paralysés ou mis hors service via des actions dans le domaine cyber. Cela provient en partie du fait que les conséquences d'attaques cyber sont difficiles à évaluer, et peuvent même se retourner contre l'agresseur.

La relevance de ce thème a été démontrée à de nombreuses reprises lors de la dernière décennie. Des gouvernements et des ministères ont été directement ciblés, de même que des compagnies privées revêtant une importance vitale et stratégique pour leur pays. De plus en plus, on constate des affrontements, même entre États, dans le cyberespace. Les rapports de force génèrent la création de frontières érigées comme mesures de protection. La dimension humaine et politique reste pourtant essentielle dans le cyberespace car au-delà des aspects techniques, il y a un affrontement bien réel entre des stratégies et des intérêts qui visent des buts concrets qui ne sont donc plus ni virtuels ni immatériels. Plusieurs États, comme la Chine et la Russie, cherchent à imposer leur contrôle aussi dans le cyberespace et ne se gênent pas pour l'utiliser à leur profit. Ce dernier est devenu un champ de bataille comme le sol,

20 Par exemple par Schwab, Klaus, «The Fourth Industrial Revolution», WEF, 2016, p. 85.

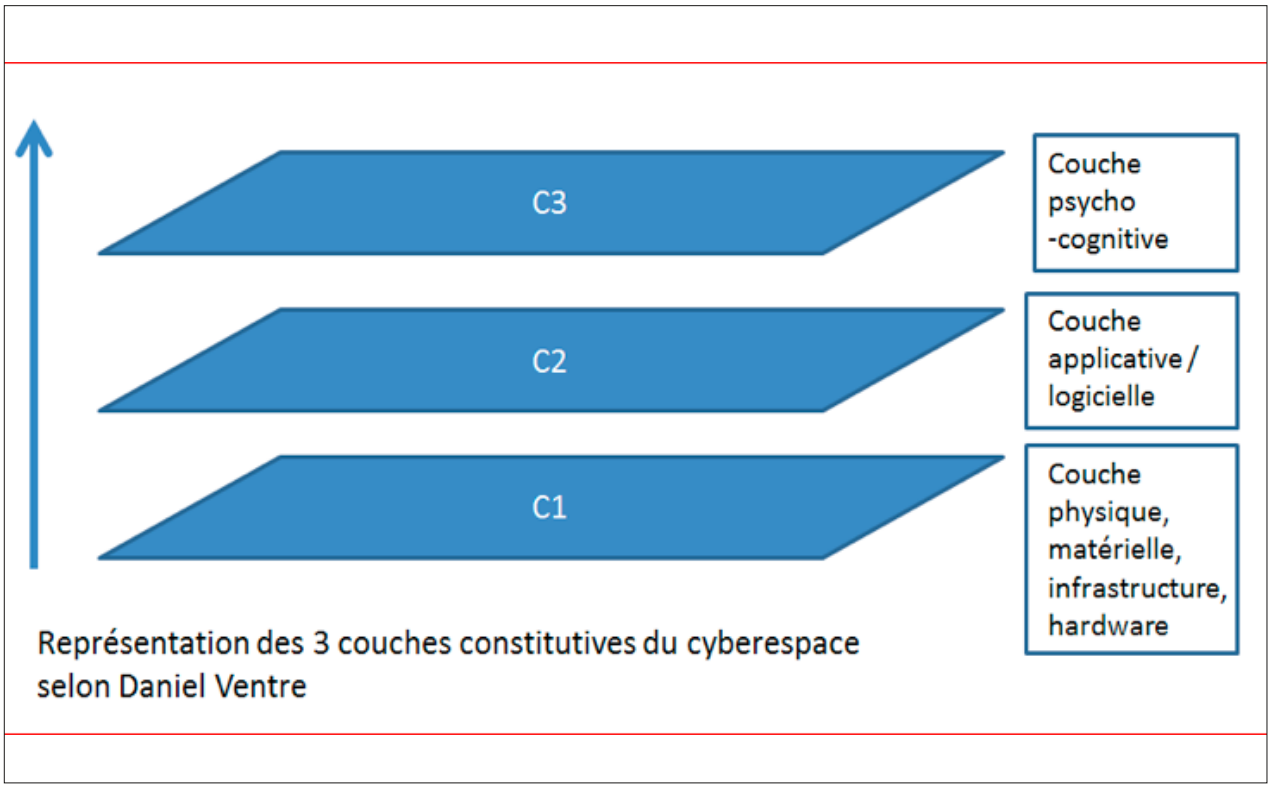


Illustration 12 Les 3 couches du cyberespace. (Daniel Ventre)

l'air, la mer ou l'espace[21], avec un potentiel qui devient de plus en plus évident.

En se référant à la définition du cyberespace comme un espace constitué de 3 couches distinctes[22], on peut mettre en évidence les différents types d'actions hostiles possibles dans chaque couche.

(1) Dans la couche physique, des attaques contre des infrastructures, équipements, armements ou réseaux sont envisageables. Il est intéressant de noter que dans cette couche, le lien entre le cyberespace et les autres espaces est évident. Un raid aérien peut par exemple détruire des bâtiments qui accueillent des serveurs et ainsi bloquer des capacités ou fonctions dans le cyberespace. L'isolation du cyberespace comme un champ de bataille particulier est donc toute relative. (2) Dans la couche logicielle, les attaques surviennent le plus souvent par l'introduction de logiciels malveillants qui permettent de détruire les systèmes et logiciels adverses, de les rendre inopérants ou d'en prendre le contrôle. Enfin, (3) dans la couche cognitive, un adversaire visera le vol d'informations ou la modification de données stockées ou transmises afin de pousser l'adversaire à prendre de fausses décisions. On voit ici la diversité des actions possibles contre des forces armées dans le cyberespace et les nombreuses vulnérabilités qu'il s'agit de contrôler. Il est très difficile de fixer des priorités tant les conséquences dans les trois couches peuvent s'avérer fatales pour le système global. Quasiment toutes les actions possibles sont relevantes pour la sécurité militaire.

Le cyberespace doit être considéré comme un théâtre d'opérations à part entière, même s'il est souvent utilisé en parallèle avec des théâtres d'opérations dans d'autres sphères. Il faut être conscient que le cyberespace, en raison des possibilités qu'il offre et des dégâts qu'il peut générer, peut tout-à-fait être utilisé de manière exclusive, même si les bénéfices des actions se situent dans d'autres domaines, comme l'économie. Il n'est donc pas étonnant que des questions se posent par rapport à la nature des conflits et au seuil à partir duquel un pays peut se sentir attaqué et en position légitime de se défendre s'il est victime d'attaques cyber. La mise en danger de l'économie d'un pays peut en effet de plus en plus être considérée comme une attaque en raison de conséquences parfois ou potentiellement très similaires à celles d'un conflit classique. L'accroissement de la connectivité qui met de plus en plus d'objets en réseau ne fait que renforcer ce risque. La domination des États-Unis dans cet espace, avec la surveillance qu'ils peuvent exercer, poussent de plus en plus d'États à vouloir disposer de leur propre infrastructure afin de pouvoir les contrôler, les filtrer et le cas échéant les bloquer.

Le cyberespace doit être considéré comme un théâtre d'opérations à part entière, même s'il est souvent utilisé en parallèle avec des théâtres d'opérations dans d'autres sphères.

21 Voir: Cattaruzza, Amaël et Sintès, Pierre: «Géopolitique des conflits», Editions du Bréal, Mesnil-sur-l'Estrée, 2016, p. 148.
22 Voir: Ventre, Daniel: «Le Cyberespace: définitions, représentations», Revue de Défense Nationale, juin 2012, No 751, p. 36.

Mais il peut aussi y voir des attaques plus clairement identifiables. Il en est ainsi lorsque des domaines civils importants sont gravement perturbés, au point de menacer le bon fonctionnement de la société. Les réseaux toujours plus importants dans les sociétés modernes deviennent à la fois cibles et vecteurs des attaques. *In fine,* c'est, comme dans le cas d'une attaque conventionnelle, la sécurité de la population qui est mise en danger. Une guerre dans le cyberespace peut ainsi amener la victoire en attaquant les infrastructures civiles critiques dans les domaines de l'approvisionnement énergétique (eau, gaz, électricité), de la santé, du trafic routier, ferroviaire et aérien, et de l'approvisionnement en général. Il est donc prévisible que certains pays réagiront à des attaques cyber, dans la mesure où l'agresseur peut être identifié, par des actions militaires conventionnelles. Lors de conflits ouverts, les armes cyber sont utiles, dans la mesure où elles permettent de perturber ou d'influencer les senseurs, les communications et donc la prise de décision.

… rappelons encore que le cyberespace est un espace de prédilection pour l'utilisation de l'intelligence artificielle, car elle seule peut gérer à son profit la masse d'informations qui s'y trouve et utiliser l'immense réseau que constitue internet.

Dans tous les cas de figure, l'avantage principal pour un agresseur d'utiliser le cyberespace vient de la difficulté pour son adversaire de reconnaître qu'il est attaqué et d'identifier l'auteur de l'attaque. Un agresseur peut ainsi non seulement être un État ou un groupe armé, mais aussi un pirate isolé, un groupe terroriste avec des moyens très limités, comme une microcellule d'activistes en tous genres, ou encore des groupes criminels motivés uniquement par le gain. Il peut agir de n'importe où et instantanément. En fait le cyberespace permet à chaque individu qui pour une raison ou une autre est en désaccord avec un État de le combattre et de causer des dégâts importants. La flexibilité du cyberespace permet à chaque acteur ou à chaque usager de construire « son espace en fonction de son utilisation, de ses représentations, de ses intérêts ».[23] Il est très difficile de reconnaître un acte de guerre visant à nuire à un pays et à sa population et à le distinguer d'un acte criminel.

En conclusion, rappelons encore que le cyberespace est un espace de prédilection pour l'utilisation de l'intelligence artificielle, car elle seule peut gérer à son profit la masse d'informations qui s'y trouve et utiliser l'immense réseau que constitue internet.

Conclusions et conséquences

L'introduction des nouvelles technologies, qui globalement constitue la quatrième révolution industrielle, implique donc à la fois des risques et des opportunités, tant pour les domaines civil que militaire. Le rôle et l'équipement des forces armées, respectivement la palette d'outils au sens le plus large, vont devoir évoluer. Le volume des données échangées et à analyser (« infobésité »[24]) afin d'en déduire un savoir utilisable pourrait constituer une limite au développement et à l'introduction de nouvelles technologies en général, et au sein des forces armées en particulier. La maintenance pourrait créer des limites, même si elle pourrait elle aussi être au moins en partie automatisée.

Des pays autres que les superpuissances ou qui ne sont pas membres d'alliances militaires, comme la Suisse, n'auront pas les ressources pour suivre continuellement le tempo des évolutions technologiques et introduire des systèmes complexes dans leurs forces armées.

Les coûts constituent sans doute la limite la plus importante. Peu de pays seront à même de financer des forces armées disposant de tous ces nouveaux systèmes.[25] Des pays autres que les superpuissances ou qui ne sont pas membres d'alliances militaires, comme la Suisse, n'auront pas les ressources pour suivre continuellement le tempo des évolutions technologiques et introduire des systèmes complexes dans leurs forces armées. Leur dépendance envers la recherche et l'appui du secteur privé va s'accroître plutôt que diminuer. Ces limitations subsisteront même si l'internet des objets réduira au moins en partie les coûts dans de nombreux domaines, et améliorera l'efficacité des moyens engagés, tant dans des missions d'appui que de combat. La protection des systèmes et le besoin en spécialistes vont générer des coûts importants, ce qui pourrait bien mener à un jeu à somme nulle, ou les gains d'efficacité et la réduction du nombre de systèmes pourraient être compensés par l'augmentation des coûts des matériels et du personnel.

L'importance du rôle de l'humain, et donc la nécessité de garder une part à l'intervention humaine, est un sujet central et déterminant.

L'impact de la mise en réseau croissante des machines, surtout si ces dernières disposent d'une certaine autonomie, reste pour le moment difficile à évaluer. L'importance du rôle de l'humain, et donc la nécessité de garder une part à l'intervention humaine, est un sujet central et déterminant. Plusieurs auteurs s'accordent sur le fait que l'intervention et le travail humains vont garder toute leur importance, y compris dans le domaine de la collecte des données et de leur introduction dans les systèmes.[26] Tout ne pourra être automatisé. Il va s'agir de définir des espaces spécifiques dans lesquels les machines peuvent agir de manière autonome, et d'autres ou l'intervention de l'être humain demeure indispensable. La question se posera sans doute de savoir s'il

23 Voir: Cattaruzza, Amaël et Sintès, Pierre, op. cit., p. 152.

24 Voir: Hémez, Rémy, op. cit., p. 27

25 Bloem estime qu'entre 2013 et 2016, près de 95'000 robots de nouvelles générations, pour un coûts total de 14 milliards de dollars (soit près de 150'000 dollars pièce) ont été mis en service dans l'industrie. In Bloem, op. cit., p. 14.

26 Par exemple Zheng, Denise E. et Carter, William A.: «Leveraging the Internet of Things for a More Efficient and Effective Military», Center for Strategic and International Studies (CSIS, Report of the CSIS Strategic Technologies Program, September 2015, p. 19.

est opportun de donner aux machines le pouvoir de corriger certaines décisions des êtres humains lorsqu'elles jugent qu'il s'agit d'une erreur. Dans ce cas, la machine prendrait en quelque sorte le contrôle total de l'action.[27]

Pourtant, la capacité de la défense à intégrer et contrôler le développement des nouvelles technologies sera la clé de la sécurité dans le futur. Ce développement, comme avec les anciens systèmes d'armes moins sophistiqué se développera aussi sur deux axes opposés : d'un côté, les nouvelles technologies seront utilisées pour améliorer l'efficacité et de l'autre, pour améliorer la protection. La capacité à détruire et la capacité à survivre conserveront leur importance respective et les progrès dans ces deux dimensions tendront aussi à l'avenir à se neutraliser. Les nouvelles technologies vont profiter des efforts militaires, qui vont les rendre plus fiables et plus résistantes.

La dimension humaine demeurera donc un enjeu essentiel, aussi pour la Suisse. Il faudra de plus en plus de spécialistes pour engager et entretenir les machines, même si celles-ci auront un grand degré d'autonomie. Il faudra aussi plus de personnes capables d'interpréter les données. Dans le cas d'une armée de milice comme l'armée suisse, la question se pose de savoir si l'on pourra trouver le nombre nécessaire de spécialistes civils astreints au service militaire, si l'on aura la capacité à les former selon les besoins ou s'il faudra procéder à une professionnalisation dans ces domaines. Au final, la question de l'importance de l'intuition dans le processus de décision se posera. Celle-ci ne pourra pas être remplacée par des processus techniques, même si l'intelligence artificielle aura la capacité d'intégrer les expériences passées.

Dans le cas d'une armée de milice comme l'armée suisse, la question se pose de savoir si l'on pourra trouver le nombre nécessaire de spécialistes civils astreints au service militaire, si l'on aura la capacité à les former selon les besoins ou s'il faudra procéder à une professionnalisation dans ces domaines.

Il faudra encore intégrer dans la doctrine la possibilité d'attaques cyber et la manière d'y répondre, de manière proportionnée, lorsque l'attaque est avérée. La conséquence logique est qu'il faut disposer d'une capacité offensive dans ce secteur. Le débat sur la possibilité de répondre à une attaque cyber par des actions dans le domaine conventionnel montre les interactions entre les espaces dès que les conséquences d'activités dans le cyberespace débordent dans d'autres espaces.

Il ne faut pas oublier que les évolutions technologiques profiteront aussi aux acteurs non-étatiques, principalement en raison de la miniaturisation et de la baisse des coûts qui sont prévisibles. Cela ouvrira de nouvelles perspectives pour ces acteurs, et donc nécessitera une réponse des États dans le sens de réactions contre de nouvelles vulnérabilités. La coopération entre les industries civile et militaire, et entre les nations, deviendra une caractéristique centrale du développement des forces armées, aussi bien pour des raisons budgétaires que technologiques.

L'évolution vers plus de digitalisation, en particulier dans les forces armées, va être favorisée par quatre facteurs principaux. Il y aura en premier lieu (1) la baisse des prix des senseurs et des capteurs en tous genres, de même que la réduction de leur taille. Ensuite, (2) l'accroissement de la connectivité avec des réseaux de plus en plus denses et de plus en plus compétitifs fournira la base nécessaire à ce développement. Il y aura aussi une (3) miniaturisation des appareils de stockages et de traitement des données. Finalement, il faut s'attendre à (4) de nouveaux programmes qui vont permettre de traiter les données en vue d'identifier les actions adéquates et de les déclencher.

Mais d'un autre côté, il y aura également cinq facteurs majeurs qui vont sans doutes limiter l'expansion des nouvelles technologies sur le champ de bataille: (1) les conditions météorologiques, (2) la distinction entre combattants et non-combattants, (3) le piratage / sabotage informatique, (4) la vitesse de développement des systèmes qui va provoquer des problèmes entre les générations de produits et (5) les autres risques impliqués.

Ces limitations viennent du fait que l'hyperconnectivité peut générer des erreurs, et il faudra donc élaborer des mécanismes de contrôle afin de prévenir les erreurs.

L'utilisation par les forces armées des nouvelles technologies implique que celles-ci seront exposées aux mêmes risques que la société civile. Le contrôle de l'intelligence artificielle représentera un défi central, car les machines pourront agir en pensant bien faire et échapper au contrôle des militaires, ce qui peut représenter un danger significatif. En particulier, la distinction entre amis et ennemis représentera un défi qu'il sera difficile de déléguer à des machines.

En résumé, pour l'armée suisse, il doit y avoir trois étapes fondamentales qui dirigeront l'intégration de nouvelles technologies:

- La définition des besoins en vue d'obtenir une véritable plus-value;
- L'identification des solutions possibles par rapport aux technologies existantes ou en développement;
- L'adaptation des technologies choisies aux contraintes de l'utilisation militaire, en particulier dans le domaine de la sécurisation.[28]

Durant tout ce processus, il faudra encore intégrer la problématique de la compatibilité entre machines et programmes de générations différentes et qui pour-

27 Voir: Haski, Pierre: «Faut-il avoir peur de l'intelligence artificielle», Nouvel Observateur, 26.08.2016, p. 7.

28 Adapté de Goetz, Pierre et Cahuzac-Soave, op. cit., p. 34.

raient entrer en conflit. Il est probable que l'armée suisse ne pourra, pour des raisons financières principalement, suivre chaque étape technologique et adapter constamment l'ensemble de ses moyens. Il y aura donc une adaptation et intégration progressive de nouvelles technologies éprouvées, comme ce qui se fait déjà avec les FA-18, qui peuvent être au moins en partie considérés comme des ordinateurs volants. D'autres applications sont envisageables dans l'automatisation de certains systèmes d'armes, selon un modèle similaire.

Marc-André Ryter

Colonel, 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

Die unsichtbaren Veteranen. Kriegsheimkehrer in der deutschen Gesellschaft

Marcel Bohnert / Björn Schreiber (Hrsg.)

324 Seiten, Miles-Verlag Berlin 2016
ISBN: 978-3-945861-27-1

Militärische Auslandsmissionen, die insgesamt die Tendenz haben, länger anzuhalten als ursprünglich geplant, konfrontieren eine Vielzahl von Soldaten aller Dienstgrade mit Herausforderungen in einer für sie oft völlig fremden Umgebung, welche sie nach Rückkehr in die Heimat zu verarbeiten haben. Militärtechnisch wird dies meist etwas euphemistisch als Einsatzerfahrung gepriesen, was zu einem gewissen Teil sicher zutrifft und auch durchaus positiv genutzt werden kann. Wenn dann Missionen wie in Afghanistan über die Zeit von einem relativ ruhigen Friedensförderungseinsatz in einen eigentlichen Kriegseinsatz mutieren, dann werden die eingesetzten Soldatinnen und Soldaten sehr oft mit Situationen konfrontiert, die der nachhaltigen Verarbeitung bedürfen. Wenn dann die Stimmung zum entsprechenden Konflikt in der Heimat negativ oder als unbeteiligt konnotiert ist, wird diese individuelle Verarbeitung in der Familie und der Gesellschaft zur noch grösseren Herausforderung.

Vor dem Hintergrund, dass unterdessen weit über 350'000 Angehörige der Bundeswehr in Auslandmissionen gedient und entsprechende positive oder negative Erfahrungen bei ihrer Rückkehr gemacht haben, versucht der vorliegende Buchband, das Bewusstsein für diese Menschen, für ihre Erfahrungen, Schicksale und Anliegen einer breiteren Öffentlichkeit zugänglich zu machen. Neben den eindrücklichen, ungeschönten und prägnanten Darstellungen von Betroffenen ist bereits die Ausgangsdefinition des Titels sehr interessant und war bei der Entstehung umstritten. So haben sich offenbar etliche Autorinnen und Autoren mit dem im Titel verwendeten Begriff der «Kriegsheimkehrer» nicht identifizieren können und wollen. Dies reflektiert sehr wohl die Komplexität gerade im deutschen Umfeld, wo zum einen der Begriff «Krieg» wie auch «Kriegsheimkehrer» politisch, rechtlich wie auch historisch negativ belegte Konnotationen auslösen. Es erscheint aber insgesamt sehr verdienstvoll, diesen Menschen, welche sich immerhin für ihr Land in einer sehr anforderungsreichen und letztlich gefährlichen Umgebung oft unter Lebensgefahr eingesetzt haben, eine derartige Plattform zu bieten.

Die zahlreichen persönlichen Erlebnisbereiche sind in drei Kapitel gegliedert, wobei das erste unter dem Titel «Aus den Auslandeinsätzen der Bundeswehr", das zweite das Thema «Veteranen und Gesellschaft» sowie das dritte Kapital das komplexe Thema «psychische Einsatzfolgen» abdecken. Bei der Lektüre der einzelnen Beiträge fällt die enorme Breite der angesprochenen Erfahrungen und Erkenntnisse auf. Zudem ist es bereichernd und deshalb auch positiv zu vermerken, dass die Autorinnen und Autoren bezüglich des Inhalts offensichtlich nicht oder kaum angeleitet worden sind. Die Publikation lässt die persönliche Betroffenheit besonders wirken und vermag auch ein realistisches und aus der persönlichen Perspektive zutreffendes Bild vermitteln. Aus dem breiten Spektrum der Beiträge sticht dabei derjenige von Rainer Buske heraus. Oberst Buske war zuerst 1999 im Kosovo und dann 2008 als Leiter des deutschen PRT in Kunduz eingesetzt. Seine Ausführungen zu den «Anforderungen an den militärischen Führer im Einsatz» sind unbedingt lesenswert und sollten eigentlich von allen militärischen Führern im Einsatz tel quel umgesetzt werden.

Insgesamt kann der vorliegende Band einer interessierten Leserschaft aus dem militärischen wie auch gesellschaftspolitischen Umfeld empfohlen werden. Einzelne Beiträge daraus gehörten eigentlich zur Standardlektüre für militärische Führungskräfte vor oder während ihres Auslandeinsatzes.

GEU

Der (Alb)traum vom Kalifat. Ursachen und Wirkung von Radikalisierung im politischen Islam

Jasmina Rupp (Hrsg.)

374 Seiten, Internationale Sicherheit und Konfliktmanagement Schriftreihe des Center für Strategische Analysen, herausgegeben von Walter Feichtinger, Band 9, Böhlau Verlag Wien, Köln, Weimar 2016
ISBN: 978-3-205-20330-8

Spätestens seit der Ausrufung des Kalifats durch den sogenannten Islamischen Staat (IS) im Sommer 2014 ist diese meist nur noch den spezialisierten Historikern und Politologen geläufige Form von Staatlichkeit wieder in den Fokus der öffentlichen Meinung getreten. Zuerst bestand die Wahrnehmung vornehmlich aus einem Phänomen der letztlich doch weitentfernten Kriegsschauplätze des Iraks und Syriens. Unterdessen hat sich diese Wahrnehmung erheblich verändert und ist viel stärker in die Alltagsrealität unserer europäischen Gesellschaften eingedrungen, als man sich das realistischerweise hat vorstellen können und wollen. Die Tatsache, dass junge Menschen sich aus der Mitte der europäischen Gesellschaften für diese Idee und den dahinterstehenden menschenverachtenden Ansichten und Praktiken in immer grösserer Zahl radikalisieren lassen und dafür sogar bereit sind, in den «heiligen Krieg» zu ziehen, ist zu einem Fokuspunkt auch in den aussen- und innenpolitischen Debatten geworden. Die eigentliche Verlagerung des «Gefechtsfelds» des IS auch in urbane Zentren Europas unter Nutzung des radikalisierten Potenzials ist zu einer der wesentlichen Bedrohungen Europas und ihrer Staatengemeinschaft herangewachsen.

Vor diesem Hintergrund versucht der vorliegende Band aus der Reihe «Internationale Sicherheit und Konfliktmanagement» in verdankenswerter Weise, Antworten und auch Lösungsansätze zu dieser komplexen Thematik zu erarbeiten. Unter der Schriftleitung der Arabistin und Politikwissenschafterin Jasmina Rupp versuchen namhafte Autoren und Experten, dieser herausfordernden Aufgabe gerecht zu werden. Dabei wird in einem ersten Block das Schwergewicht auf die Darstellung eines möglichst breiten Kontexts mit Definitions- und Abgrenzungsversuchen gelegt. In einem zweiten Teil geht es darum, mit Fallstudien die Entwicklungen und Herausforderungen in ausgewählten islamischen Staaten aufzuzeigen. Es ist für den interessierten Leser erfreulich, dass dabei sowohl geographisch wie auch inhaltlich ein möglichst grosser Bogen gespannt wird, der von Marokko über das Phänomen von Boko Haram bis nach Indonesien reicht, durchaus aber ein Schwergewicht im Nahen und Mittleren Osten hat. Diese Darstellungen vermögen auch gut die enorm divergierenden Perzeptionen und Perspektiven dessen aufzuzeigen, was gemeinhin zur «islamischen Welt» reduziert wird.

Der dritte Teil stellt sich der eigentlich grössten Herausforderung, nämlich den «Wegen aus der Radikalität». Die Darstellungen zu den Massnahmen und Entwicklungen in ausgewählten muslimischen Staaten, in der Europäischen Union und spezifisch in Österreich sind bezüglich der jüngsten Vergangenheit und der Gegenwart aussagekräftig, bleiben letztlich aber deskriptiv. Der Umstand, dass Entwicklungsmöglichkeiten und kreativer Ausblick eher zu kurz kommen, dürfte doch auch auf eine gewisse Ratlosigkeit in Bezug auf dieses komplexe Phänomen hinweisen.

Insgesamt liegt hier eine lesenswerte und stimulierende Schrift vor, dies eine wesentliche sicherheitspolitische und gesellschaftliche Thematik zeitgerecht aufgenommen hat. Leider sind die Illustrationen etwas spärlich ausgefallen, wo mit Karten oder Übersichten zusätzliche Verständlichkeit hätte geschaffen werden können. Der speziell interessierte Leser dürfte aber die insgesamt sorgfältigen Glossar, Akronym- und Abkürzungsverzeichnis und das umfangreiche sowie weiterführende Literaturverzeichnis schätzen.

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. 1 / 2017 80.024d 05.2017 18 700