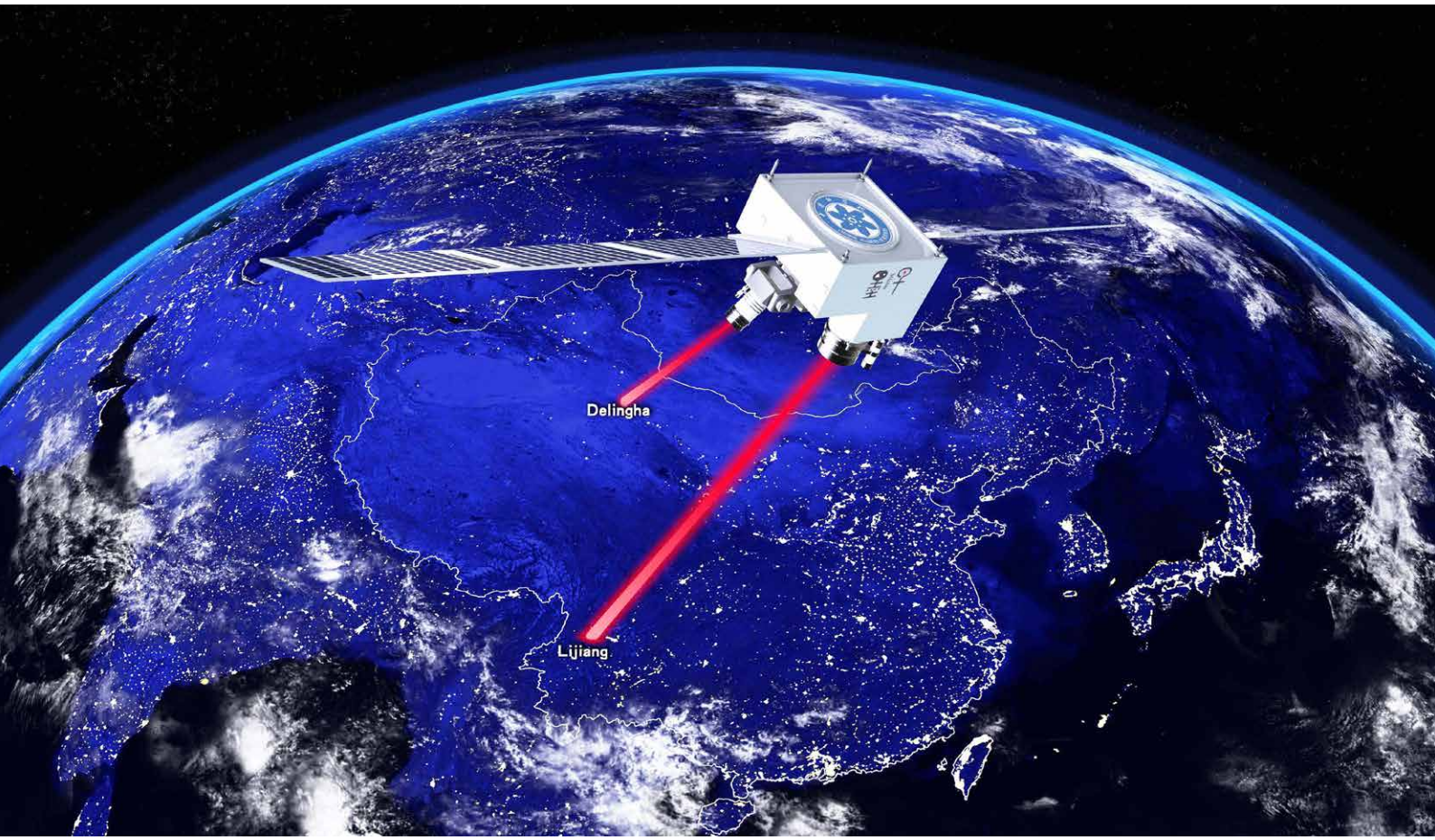
STA info

Schweizerische Gesellschaft
Technik und Armee

Société suisse
Technique et Armée

Società svizzera
Tecnica e Armata

Societad svizra
Tecnica ed Armada



Flash 02/2018

INHALT

03	Editorial
05	Aktuelles aus der Armee
07	Industrieorientierung armasuisse / Herbstveranstaltung STA
09	Neue Studie Industriebeteiligungen
12	Quanten-Computer
15	Blockchain: hält der Hype, was er verspricht?
18	Streitkräfte in Umbruchzeiten
22	Amerikanische Militärmacht im Wandel
24	Technologiefrüherkennung bei armasuisse W+T / 5 JAHRE DEFTECH
28	Ausblick / Information

VORSTAND UND KONTAKTADRESSE

Dr. Fritz Gantert	Präsident
Urs Breitmeier	Vizepräsident und Quästor, Ressort Wirtschaft
Dr. Thomas Rothacher	Ressort Beschaffung und Technologie
KKdt Philippe Rebord	Ressort Armee
Peter Huber	Ressort Wirtschaft
Walter Kägi	Ressort Wirtschaft
Brigitta Pfeuti	Geschäftsführerin, info@sta-network.ch, Tel. +41 31 376 64 52

IMPRESSUM

Herausgeber	Schweizerische Gesellschaft Technik und Armee STA Geschäftsstelle Stauffacherstrasse 65, 3000 Bern 22
Layout	Brigitta Pfeuti
Druck	Engelberger Druck, Stans
Kontakt	info@sta-network.ch
Auflage	600 Exemplare
Titelbild	«Micius» Testsatellit zur Prüfung von Verfahren der Quanten-kommunikation und -kryptographie

EDITORIAL

Leitgedanke der diesjährigen Herbstveranstaltung, die wiederum zusammen mit armasuisse, Swissmem und GRPM durchgeführt wurde, war «Rahmenbedingungen (aktiv) gestalten».

Mit den Referaten des Rüstungschefs und des Chefs der Armee erhielten die rund 240 Teilnehmenden am Morgen eine umfassende Darlegung der heutigen Situation und einen Blick auf die grossen Herausforderungen, die noch vor uns stehen. Als besonderes Highlight am Morgen sei das Referat von Botschafter Erwin Bollinger zum Thema «Rüstungsexporte in einem schwierigen politischen Umfeld» hervorgehoben: mit seinen faktenbasierten Ausführungen gelang es ihm klar aufzuzeigen, was eigentlich die letzten Jahre Sache war und heute ist. Dies war wichtig, hat doch die seitens der Verbände und der Industrie geforderte kleine Erleichterung der Vorschriften zu einem unerwartet hohen (negativen) Echo geführt. Seitens der Absender dieser Forderung wurde die mediale Wirkung ein Jahr vor den kommenden Wahlen im Herbst 2019 total unterschätzt. Die notwendigen Lehren daraus sind zu ziehen.

Der Nachmittag war für den Moderator sicher ein erheblicher Spagat: begann doch die Herbstveranstaltung 2018 mit einem Referat von Prof. Dr. Thomas Friedli von der Universität St. Gallen, gefolgt von den Referaten von Thomas Landolt, Managing Director bei IBM, zum Thema «5 Schlüsseltechnologien der Zukunft» und Frau Dr. Marianne Janik, CEO Microsoft Schweiz, zum Thema «Microsofts Transfomation». Es war spannend, wie in beiden Referaten aus der Industrie die Geschwindigkeit der Veränderung einerseits, andrerseits der Fakt, dass eine erfolgreiche Transformation nur gelingt, wenn man die Mitarbeitenden an Bord hat, hervorgehoben wurde. In seiner «unkomplexen Zusammenfassung» hielt der einmal mehr ausgezeichnet moderierende Jürg Willi fest, dass Offset im Rahmen der Wehrtechnik eine wichtige Quelle für die Technologiebeschaffung sei, diese Technologien dann das Grundgerüst aller Veränderungen bilden werden, die Veränderungen aber nur gelingen würde, wenn alle Mitarbeitenden auf den Zug aufspringen.

Mit sehr grosser Aufmerksamkeit verfolgte die Zuhörerschaft die Ausführungen von Prof. Dr. Friedli. Swiss ASD und GRPM haben ihn im Verlaufe dieses Jahres mit einer Studie zur Wichtigkeit der Industriebeteiligung, also des Offsets im Rahmen von bedeutenden Beschaffungsvorhaben, beauftragt. Anlässlich unserer Herbstveranstaltung wurden die Resultate erstmals einem breiteren Kreis vorgestellt. An dieser Stelle hervorheben möchte ich, dass in dieser Studie doch eine gesamtheitliche Sicht eingenommen wurde. Nicht nur die wirtschaftspolitische Sicht, sondern auch die sicherheitspolitische Bedeutung der Industriebeteiligung wurde klar hervorgehoben. Es liegen nun klar quantifizierte Aussagen zu den Effekten der Industriebeteiligung vor, die in diesem Thema zu einer Versachlichung der Diskussion führen werden. Zumindest wäre das wünschenswert. Ein Artikel in diesem Flash geht detailliert auf die Resultate ein.

Das aktuelle schweizerische sicherheitspolitische Umfeld ist sehr herausfordernd und stark geprägt durch

- ein nach wie vor zu wenig entwickeltes Bewusstsein, welchen Wert die Sicherheit hat,
- eine langsam etwas gesteigerte Bereitschaft, die Kosten dafür zu tragen. Allerdings befürchte ich nach wie vor einen Kampf um Ressourcen im Bundeshaushalt. Es ist nur zu hoffen, dass die bürgerliche Seite konsequent an den gefällten Entscheiden festhält und auch dem verstärkten Druck der diversen Interessensgruppen nicht nachgibt,
- eine permanent ändernde Bedrohungslage,
- die Umsetzung der WEA,
- eine nach wie vor ungewisse Zukunft der schweizerischen Industrie- und Technologiebasis.

Die STA setzt sich weiterhin für den Erhalt von angemessenen wehrtechnischen Kernfähigkeiten und -kapazitäten in der Schweiz ein. Von zentraler Bedeutung dazu sind unsere Thesen 5 und 6, nämlich

These 5: Eigene industrielle Kernfähigkeiten in der Wehrtechnik stärken die strategische Handlungsfähigkeit der Schweiz.

These 6: Das wirtschaftliche Überleben der Schweizer Exportindustrie erfordert Exportpraxis nach europäischem Rechtsstandard sowie internationale Kooperationen beim Rüstungsbeschaffungsprozess.

EDITORIAL

Die Niederschrift dieses Editorials erfolgte am Vorabend der Bundesratswahlen… Ich gebe hiermit meiner Hoffnung Ausdruck, dass in der neuen Zusammensetzung des Bundesrates die sicherheitspolitischen Themen einen höheren Stellenwert in den Diskussionen, in den Entscheiden und in der Zuordnung der finanziellen Ressourcen haben werden. Eine glaubwürdige, auf Langfristigkeit ausgerichtete Sicherheitspolitik und daraus abgeleitete Strategien werden auch in Zukunft eine entscheidende Basis für unseren Wohlstand bilden.

Ich sehe es als Aufgabe der STA an, mit gezielter Informationsvermittlung, aber auch mit attraktiven Podiumsgesprächen weiterhin die Zusammenhänge aufzuzeigen und gleichzeitig auch immer wieder den Bezug zur Sicherheits- und Wehrtechnik und den damit verbundenen industriellen Aktivitäten herzustellen. Das thematische Fundament für die kommenden Jahre, die durch grosse Umbrüche und Veränderungen noch gezeichnet sein werden, ist mit den 7 Thesen zur Sicherheitspolitik gelegt. Ich hoffe aber auch, dass diese Schritte der Veränderung evolutionär und nicht revolutionär ablaufen werden.

Für die kommenden Festtage und das neue Jahr wünsche ich allen Mitgliedern alles Gute, beste Gesundheit und dass das Jahr 2019 jedem von uns das bringen möge, was er für sich erwartet und erhofft.

Ich freue mich, Sie alle an unseren Anlässen auch im 2019 begrüssen zu dürfen.

Der Präsident der STA

Dr. Fritz Gantert

AKTUELLES AUS DER ARMEE

Begriffe wie Cyber War, Cyber Security, Cyber Defence, Cyber Attacken sind seit geraumer Zeit in aller Munde. Etwas weniger bekannt ist, dass es im Bereich Cyber die primäre Aufgabe der Armee ist, die eigenen Netze zu schützen. Dafür werden bis 2023 insgesamt 3,4 Milliarden Franken investiert in Rechenzentren VBS / Bund, ins Führungsnetz Schweiz und in die Telekommunikation der Armee. Mit diesen Massnahmen härten wir unsere Systeme, damit die Führungsfähigkeit der Armee über alle Lagen sichergestellt ist.

Geschätzte Leserinnen und Leser des STA-Flash

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

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

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

Die anlässlich des Cyber-Lehrgangs vermittelte Ausbildung ist ab 2020 auch zivil anerkannt: Nach Abschluss des Lehrgangs kann dank des engen Schulterschlusses mit dem Berufsverband ICT-Berufsbildung Schweiz die Berufsprüfung zum «Cyber Security Specialist» mit eidgenössischem Fachausweis abgelegt werden.

Es ist nicht übertrieben, hier von einer Win-Win-Situation zu sprechen – weil die Armee das Vertrauen der Bildungslandschaft und der Wirtschaft mit einem Beitrag bezüglich Reduktion des Fachkräftemangels zurückzahlen kann.

Lassen Sie mich noch einen Blick in Zukunft werfen. Wie sie wissen, spielt die Umsetzung der Weiterentwicklung der Armee (WEA) in den kommenden Jahren eine entscheidende Rolle. Heute kann ich festhalten: Die für 2018 gesetzten Ziele sind mit Ausnahme der erforderlichen Alimentierung von

KKdt Philippe Rebord, CdA

mindestens 18‘000 ausexerzierten und ersteingeteilten Angehörigen der Armee § pro Jahr weitgehend erreicht.

Die vollständige Erreichung der Ziele der WEA Ende 2022 ist aus heutiger Sicht von der Entwicklung von vier Schlüsselfaktoren abhängig. Es sind dies die Alimentierbarkeit der Armee, die vollständige Ausrüstung, der ausreichende Nachwuchs an militärischem Berufspersonal sowie die Verfügbarkeit der erforderlichen finanziellen Mittel.

Alimentierbarkeit

Der mit der Planung der WEA anvisierte Effektivbestand von 140‘000 Angehörigen der Armee kann Stand heute nicht erreicht werden, obwohl er bis Ende 2022 voraussichtlich auf rund 145‘000 ansteigen wird; Anfang 2023 wird er aber auf 123‘000 absinken. Grund dafür ist der Wegfall der Übergangsbestimmung der Verordnung über die Militärdienstpflicht, wodurch sich der Effektivbestand und der Bestand an Ausbildungsdienstpflichtigen um zusätzliche zwei Jahrgänge reduziert. Der Sollbestand wird der gesetzlichen Vorgabe von 100‘000 AdA entsprechen.

Die Zahlen der Zulassungen zum Zivildienst sind aus Sicht der Armee zu hoch; zur Sicherung des Armeebestandes ist eine Revision des Zivildienstgesetzes zwingend notwendig.

AKTUELLES AUS DER ARMEE

Vollständige Ausrüstung
Auch am Ende der Umsetzung der WEA wird eine vollständige Ausrüstung nicht möglich sein. Dies deshalb, weil Material nicht mehr beschaffbar ist, weil angesichts der Budgets Neubeschaffungen teilweise prioritärer als Nachbeschaffungen sind und weil geplante Neubeschaffungen erst nach 2022 der Truppe zulaufen werden. Die persönliche Ausrüstung der Angehörigen der Armee ist davon wenig betroffen. Alle Angehörigen der Armee sind, abgesehen vom ABC-Schutz, vollständig ausgerüstet.

Nachwuchs militärisches Berufspersonal
Der Nachwuchs an gut qualifiziertem militärischem Berufspersonal ist für die Sicherstellung des Ausbildungsmodells der WEA entscheidend. Aktuell gelingt es nicht, die geforderte Anzahl Kandidaten zu rekrutieren. Durch verstärkte Anstrengungen im Marketingbereich und mit einer Anpassung des Berufsbildes soll dieser Herausforderung mittelfristig begegnet werden.

Finanzielle Mittel
Mit dem von den eidgenössischen Räten verabschiedeten Armeebudget von 5 Milliarden Franken pro Jahr steht ab 2019 pro Jahr rund 1 Milliarde Franken für Investitionen zur Verfügung. Mit anderen Worten: Über einen Zeitraum von 10 Jahren (2023 – 2032) stünden damit 10 Milliarden Franken zur Verfügung.

Maximal 8 Milliarden Franken werden für die Beschaffung neuer Kampfflugzeuge und eines neuen Systems zur bodengestützten Luftverteidigung grösserer Reichweite eingesetzt; im gleichen Zeitraum müssen aber zusätzlich 7 Milliarden Franken für Beschaffungen via Rüstungsprogramme für die anderen Teile der Armee vorgesehen werden.

Aus diesem Grund hat der Bundesrat im November 2017 beschlossen, dass das Armeebudget ab 2021 um real 1,4 Prozent pro Jahr ansteigen soll. Damit stehen für den Zeitraum 2023 – 2032 die benötigten rund 15 Milliarden Franken für die Finanzierung von Rüstungsprogrammen zur Verfügung.

Wenn aufgrund erneuter Sparprogramme zukünftige Armeebotschaften mit kleineren Verpflichtungskreditvolumen aufgelegt werden müssen oder wenn zusätzliche Sparvorgaben zu erfüllen sind, kann das geforderte Leistungsprofil gemäss WEA nicht erfüllt werden.

Die Umsetzung der WEA ist auf Kurs, die Schlüsselfaktoren sind bekannt. Jetzt gilt es, den eingeschlagenen Kurs zu halten. Dabei bin ich auf Sie angewiesen. Bringen Sie sich in die Diskussionen um die Sicherheit unseres Landes mit ein. Dafür möchte ich Ihnen und der STA bereits jetzt danken.

Ihnen allen wünsche ein erfolgreiches und sicheres 2019.

KKdt Philippe Rebord, Chef der Armee

INDUSTRIEORIENTIERUNG ARMASUISSE / HERBSTVERANSTALTUNG STA

Am Nachmittag des vergangenen 8. November hat in der Mannschaftskaserne Bern die traditionelle Herbstveranstaltung der STA stattgefunden. Ebenfalls zur Tradition geworden ist die Industrieorientierung der armauisse, die vormittags am gleichen Ort durchgeführt wurde. Der Kreis der Eingeladenen war weitgehend gleich, so dass die zwischen beiden Anlässen bestehenden Synergien optimal genutzt werden konnten.

Von Kirsten Hammerich, RUAG Corporae Services
Fotos © armasuisse

Die diesjährige Industrieorientierung widmete sich dem Thema «Rahmenbedingungen gestalten». Rüstungschef Martin Sonderegger eröffnete den Anlass mit rund 240 Gästen aus Wirtschaft, Wissenschaft, Armee und Verwaltung mit dem derzeit hochaktuellen Thema Rüstungspolitik. So verabschiedete der Bundesrat am 24. Oktober 2018 die Revision der Rüstungspolitik, die am 1. Januar 2019 in Kraft tritt.

Der Chef der Armee, Korpskommandant Philippe Rebord, äusserte sich zum Masterplan 2018 und zur Investitionsplanung. Er wies darauf hin, dass das künftige Fähigkeitsprofil und das Leistungsvermögen der Armee ab 2032 in Form eines «Zielbildes» aufgezeigt wird und er erlaubte einen Ausblick auf die Herausforderungen, die der Masterplan 2018 mit sich bringt.

Botschafter Erwin Bollinger schloss die Runde mit seinem Referat über Rüstungsexporte in einem schwierigen politischen Umfeld.

Weiterentwicklung, Transformation, Digitalisierung waren die bestimmenden Themen der Herbstveranstaltung der STA nach dem Mittagessen. Nach der Begrüssung des STA-Präsidenten, Dr. Fritz Gantert, sprach Prof. Dr. Thomas Friedli über Offset und stellte bereits im Titel seines Referates die Frage: «Wichtiges Instrument oder lästiges Ärgernis in der Beschaffung?» Die Antwort auf diese Frage belegte Prof. Dr. Friedli mit Untersuchungen: «Die Sicherung der industriellen Fähigkeiten, der Transfer von Technologie und Wissen und der erweiterte Marktzugang überwiegen als positive Aspekte von obligatorischen Kompensationsforderungen bei Rüstungsbeschaffungen, weshalb eine Weiterführung als wichtiges Instrument angestrebt werden sollte. Sie sind die einzige Möglichkeit, auf sicherheitsrelevante Themen Einfluss nehmen zu können», so Friedlis Fazit.

Thomas Landolt, Managing Director bei IBM, führte den Anwesenden fünf Technologien vor Augen, welche uns in den nächsten fünf Jahren helfen sollen, unser Leben zu verän-

Martin Sonderegger, Rüstungschef

KKdt Philippe Rebord

dern: Blockchain-Technologien, Kryptographie, Technische Hilfsmittel mit künstlicher Intelligenz und unvoreingenommene künstliche Intelligenz. Gleichzeitig zeigte er bei jedem dieser Themen auf, wie wichtig sie auch für die Bereiche Verteidigung und Nachrichtendienst sein können – oder müssen.

Den Schlusspunkt setzte Dr. Marianne Janik, CEO von Microsoft Schweiz, mit ihrem Referat über die Transformation von Microsoft. Das Unternehmen hat bereits begonnen, sich von einem innovativen und wachsenden zu einem ganzheitlich orientierten Unternehmen zu wandeln, das wohl weiterhin wächst, dabei aber immer effizienter wird, indem es bei sich selbst beginnt, Veränderungen in der täglichen Zusammenarbeit zuzulassen und zu fördern. Janik betonte, dass ihr die Schweiz ganz besonders am Herzen liege: «Das Land kann uns zeigen, wie Wertschöpfung geht, wie Kooperation geht und dass beides zu Wohlstand und Sicherheit führt», begründete Janik ihr Statement.

Bei der anschliessenden Podiumsdiskussion mit allen Rednerinnen und Rednern wurden die Fragen aus dem Publikum diskutiert und beantwortet.

Beim anschliessenden traditionellen «Chäschüechli-Apéro» hatten die Teilnehmerinnen und Teilnehmer die Gelegenheit, einen spannenden Tag mit hoch interessanten Referaten Revue passieren zu lassen. Im persönlichen Austausch konnten die Anwesenden einerseits behende Kontakte pflegen und andererseits ihr Netzwerk erweitern.

Botschafter Dr. Erwin Bollinger

Prof. Dr. Thomas Friedli

Thomas Landolt

Dr. Marinanne Janik

v.l.n.r. Dr. Fritz Gantert, Thomas Landolt, Dr. Marianne Janik, Prof. Dr. Thomas Friedli, Martin Sonderegger, Divisionär Claude Meier

Download

Die Präsentationen zu den Referaten können aus dem Internet heruntergeladen werden:

www.sta-network.ch / Downloads / Herbstveranstaltungen

NEUE STUDIE INDUSTRIEBETEILIGUNGEN

2008/2009 hat das Center for Security Economics and Technology (CSET) der Universität St.Gallen unter Leitung von Prof. Dr. James Davis eine Studie zum Schweizer Offsetprozess durchgeführt (Friedli et al. 2009). Projektleiter für die Universität St.Gallen war dazumals Prof. Dr. Thomas Friedli vom Institut für Technologiemanagement (ITEM-HSG). In den letzten 10 Jahren haben sich insbesondere im europäischen Ausland die Richtlinien für Industriebeteiligungen stark geändert, weshalb sich eine Erneuerung der Studie aufdrängte. Der Fokus lag dabei vor dem Hintergrund der geplanten Beschaffungen zur Erneuerung der Mittel zum Schutz des Luftraumes (Air2030) auf einem internationalen Vergleich des Schweizer Offset-Ansatzes und der Darstellung des Stimmungsbildes in der nationalen Rüstungsindustrie.

Von Prof. Dr. Thomas Friedli, Philipp Osterrieder, Michael Wiech, Universität St.Gallen

Die Studie zeigt, dass auch 10 Jahre nach der Publikation der ersten Studie Kompensationsgeschäfte bei Rüstungsgeschäften keine Besonderheit sind, sondern den Regelfall auch in (west-)europäischen Ländern darstellen. Zudem besteht in der nationalen Industrie ein weitgehender Konsens über die positiven Auswirkungen von Offset. So äusserten viele befragte Unternehmen, dass vor allem der Zugang zu international tätigen Grosskonzernen mit der Chance auf nachhaltige Geschäftsbeziehungen und langfristige Entwicklungsmöglichkeiten den Hauptnutzen einer industriellen Beteiligungspolitik darstellt. Damit einher geht der Transfer von essenziellen Fähigkeiten zum Erhalt, Auf- und Ausbau der sicherheitsrelevanten Technologie- und Industriebasis (STIB).

Mit Bezug auf die vieldiskutierten Mehrkosten einer Beschaffung mit Offset-Verpflichtungen kommt die Studie zum Schluss, dass diese Mehrkosten stark vom jeweiligen Beschaffungsland abhängen. In Ländern mit einer hochentwickelten industriellen Basis wie der Schweiz sind diese deutlich geringer als in Entwicklungsländern, in denen grundlegende Kompetenzen fehlen. Die Möglichkeit der Anbieter, die Preise massgeblich zu erhöhen, sind ausserdem dadurch eingeschränkt, dass sich diese in einer Wettbewerbssituation befinden und der Preis ein wichtiges Entscheidungskriterium für den Zuschlag ist.

Die Tatsache, dass die Schweiz trotz den geringen Stückzahlen für die Anbieter wegen des transparenten und sachkritierienbasierten Evaluationsprozesses ein wichtiger Referenzmarkt ist, führt zusätzlich dazu, dass zu «vernünftigen» Preisen angeboten wird. Die Studie zeigt ausserdem auf, dass die angenommenen Mehrkosten von 2 bis 5% durch die generierten zusätzlichen Steuereinnahmen weitgehend kompensiert werden. Dies wird im folgenden näher beleuchtet, da dieser Aspekt bis anhin in keiner uns bekannten Studie beschrieben wurde.

Die folgenden Ausführungen dienen einer groben Abschätzung der im direkten Zusammenhang mit Kompensationsgeschäften stehenden Steuerrückflüsse. Die sich aus langfristigen Geschäftsbeziehung ergebenden zusätzlichen Steuereinnahmen werden nicht berücksichtigt.

Relevantes Kriterium für ein Kompensationsgeschäft ist gemäss der Offset-Rahmenbedingungen die «Zusätzlichkeit»: Aufträge, welche als direkte Folge der Offset-Verpflichtung entstanden sind und ohne das Rüstungsgeschäft nicht zu Stande gekommen wären (armasuisse, 2016, S. 7). Diese «Zusätzlichkeit» generiert zusätzliche Gewinnsteuern. Des Weiteren werden durch eben diese zusätzlichen Aufträge Mitarbeitende in den beteiligten Unternehmen beschäftigt, die wiederum ihre Löhne versteuern und somit Einkommenssteuereinnahmen erzeugen. Diese beiden Arten der Steuereinnahmen werden im folgenden Modell als direkte Steuerrückflüsse bezeichnet (siehe Abbildung 1).

Zusätzlich generieren Offset-Aufträge Steuereinnahmen zweiter Ordnung, die in den Zulieferbetrieben entstehen. Gleichfalls kann hier zwischen Unternehmens- und Einkommenssteuern unterschieden werden. Die Steuereinnahmen zweiter Ordnung werden im Folgenden als indirekte Steuerrückflüsse bezeichnet (siehe Abbildung 1).

Neben den direkten und indirekten Steuerrückflüssen gibt es relevante nachgelagerte Effekte, die wiederum besteuert und als induzierte Steuerrückflüsse bezeichnet werden. Diese werden hier allerdings nicht näher betrachtet. Zur Abschätzung der tatsächlichen Steuerrückflüsse wird im Folgenden zunächst das steuerrelevante Kompensationsvolumen bestimmt, welches den Offset-Nehmern tatsächlich zufliesst (siehe Abbildung 1). Wie in Abbildung 1 dargestellt, dient hierfür das um den durchschnittlichen Offset-Multiplikator bereinigte «Gesamt Kompensationsvolumen» als Basis.

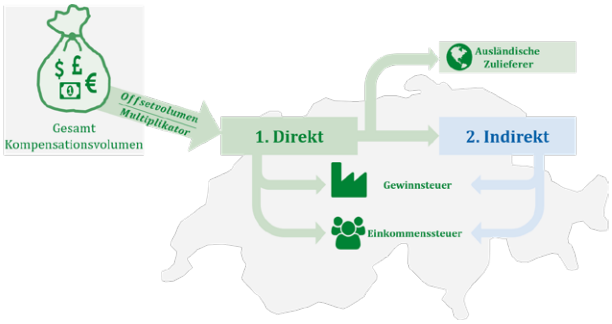


Abbildung 1: Abschätzung der direkten und indirekten Steuerrückflüsse

Die Abschätzung eines solchen durchschnittlichen Multiplikators erweist sich als schwierig, weshalb Abbildung 2 die Abhängigkeit der Rückflüsse vom Multiplikator darstellt.

Direkte Steuerrückflüsse

Die Abschätzung des Gewinns beruht auf dem arithmetischen Mittel der relevanten Industriegruppen. Durchschnittlich erwirtschafteten Unternehmen dieser Branchen in den letzten Jahren einen Return on Sales [ROS] von 7.44% (Orbis Datenbank, 2018). Für eine grobe Abschätzung des Unternehmensgewinnsteueraufkommens stellen ROS in Kombination mit durchschnittlicher Gewinnsteuer von 20.71% (Chatagny, Koethenbuerger & Stimmelmayr, 2017, S. 946) die massgeblichen Grössen dar.

Zur Berechnung der direkten Steuerrückflüsse durch Einkommenssteuern von Privatpersonen wird das adjustierte Offset-Volumen als Umsatzbasis der Unternehmen betrachtet und auf den Anteil der Arbeitskosten reduziert. Dieser Arbeitskostenanteil beträgt in den oben aufgeführten Branchen 20.68% des Umsatzaufkommens (Bundesamt für Statistik [BFS], 2014). Die Berechnung des zu versteuernden Bruttoeinkommens basiert auf einer Bereinigung des Arbeitskostenanteils von den Lohnnebenkosten (z.B. AHV- und IV-Beiträge). Abzüglich Lohnnebenkosten in Höhe von 18.85% verbleibt ein Anteil von 81.15% des Bruttolohnes, welcher von den Mitarbeitenden mit einem durchschnittlichen Steuersatz von 14.48% zu versteuern ist (OECD, 2018).

Indirekte Steuerrückflüsse

Neben den oben aufgeführten direkten Steuerrückflüssen sind in der Lieferkette nachgelagerte Effekte zu beachten. Die Offset-Nehmer beziehen Vorleistungen von Schweizer Zulieferbetrieben, deren Gewinne und Personalausgaben weiteres Steueraufkommen generieren. Differenzierender Faktor bei diesen indirekten Steuerrückflüssen ist die Wertschöpfungstiefe bei den Offset-Nehmern. Zusätzlich ist der Anteil an erbrachter Wertschöpfung von Lieferanten aus der Schweiz relevant (siehe Abbildung 1).

Gemäss der oben beschriebenen Annahme und Daten ergeben sich für Kompensationsgeschäfte in der Schweiz Steuerrückflüsse in Höhe von 4.5-5% am «Gesamt Kompensationsvolumen».

Abbildung 2 verdeutlicht den Zusammenhang zwischen Offset-Multiplikator und den Steuerrückflüssen. Eine Erhöhung des Multiplikators schmälert den Zufluss von Umsatzvolumen und verringert entsprechend die möglichen Steuereinnahmen.
Letztlich zeigt die grobe Abschätzung der Steuerrückflüsse, dass die Diskussion um Mehrkosten durch Kompensationsvereinbarungen diesen Aspekt einbeziehen sollte. Die Steuerrückflüsse decken, je nach Annahme bezüglich der Höhe dieser Mehrkosten, diese entweder teilweise oder sogar gänzlich. Des Weiteren ignoriert die oben vorgenommene Abschätzung die zusätzlichen Steuereinnahmen durch induzierte Effekte und blendet Rückflüsse aus langfristigen Geschäftsbeziehungen, initiiert durch Kompensationsobligationen, aus.

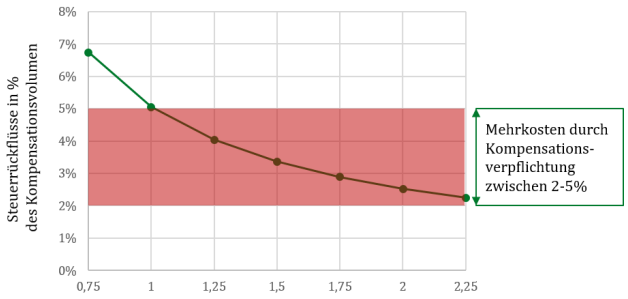


Abbildung 2: Steuerrückflüsse in Abhängigkeit vom Multiplikator

Die wirkliche Bedeutung von Offset liegt aber nicht in den volkswirtschaftlichen Effekten, sondern darin, dass Offset eine der wenigen Möglichkeiten ist, um die sicherheitsrelevante Technologie- und Industriebasis zu sichern. Der Schweizer Offset-Prozess ist in der heutigen Form vernünftig und effizient. Die Weiterführung der industriellen Beteiligungspolitik wird von Seiten der nationalen Industrie mit wenigen Ausnahmen begrüsst und auch aus den Vergleichen im internationalen Umfeld gestützt. Nichtsdestotrotz besteht weiterhin Potenzial zur steten Verbesserung der ope-

rativen Umsetzung von Offset. So wäre die Vereinigung der Steuerungs- und Controlling-Verantwortung von direktem und indirektem Offset anzustreben. Es ist auch im Sinne des Gesamten, wenn man sicherstellen könnte, dass die auf unterschriebenen Offset Declaration Forms (ODF) aufgeführten Geschäfte insbesondere auch das Kriterium der Zusätzlichkeit erfüllen. Kommunikativ sollte die Begründung der «Sicherheitsrelevanz» stärker in den Vordergrund gerückt werden, da dies auch die legale Grundlage zur Abweichung vom üblichen Wettbewerbsrecht ist.

Referenzen

armasuisse. (Juni 2016). Offset-Policy (Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS, Hrsg.). Bern.

Bundesamt für Statistik [BFS]. (2014). Strukturelle Arbeitskostenstatistik.

Chatagny, F., Koethenbuerger, M. & Stimmelmayr, M. (2017). Introducing an IP license box in Switzerland. Quantifying the effects. International Tax and Public Finance, 24 (6), 927–961. https://doi.org/10.1007/s10797-017-9441-8

Friedli, T., Neumueller, K., & Platzgummer, P. (2009). Nachhaltige Offset-Ansätze für die Schweiz: Aufzeigen von Optimierungspotenzialen und strategischen Stossrichtungen: C SET-IPW-HSG

Orbis Datenbank. (2018). Datensatz „Vorsteuerertrag und Umsatz aller aktiven Schweizer Unternehmen der NACE Rev. 2 Klassen 22-33 (exkl. 31)

Quanten-Computer bringen neue Security Herausforderungen - eröffnen aber auch viele Chancen!

In letzter Zeit wurden Quanten-Computer immer mehr als die grösste Bedrohung für die heute bekannten Sicherheitsprinzipien, welche dem Internet und unserer IT-Sicherheit zugrunde liegen, angesehen. Obwohl dies teilweise zutrifft, muss angemerkt werden, dass die grossen Hürden keine technischen sind. Verschlüsselung und den Verschlüsselungsprozess zu verstehen und sauber zu managen, ist eine grosse Herausforderung für Organisationen. Unsere heutigen PKIs auf die Quantensicherheit vorzubereiten wird aufgrund der vielen Akteure, die diese Infrastrukturen bilden, viel Arbeit erfordern. In diesem Artikel wird erklärt, was Quanten-Computer so anders macht, welche Art von Anwendungen es gibt und wie Sie sie einsetzen können, was Sie als Organisation tun müssen, um bereit zu sein, und welche Sicherheitsmöglichkeiten sich aus Quantentechnologien ergeben.

Von Frederik Kerling MSc., Senior Quantum Expert, Atos Scientific Community und Patrick Nyfeler, Client Partner Atos AG

Quantum-Computer

Quanten-Computer arbeiten anders als herkömmliche «klassische» Computer. Anstatt mit binären Bits, die entweder 0 oder 1 sind, zu arbeiten, arbeiten Quanten-Computer mit Qubits, die eine beliebige Überlagerung zwischen 1 und 0 haben können. Ein Qubit könnte beispielsweise eine Kombination aus 1 und 0, 40% 1 und 60% 0 sein. Das bedeutet, dass 2 Qubits in einer beliebigen Überlagerung der 4 möglichen Kombinationen stehen können, 3 Qubits haben 8 Kombinationen und so weiter und so fort. Das bedeutet, dass ein Satz von 300 Qubits 2 300 Kombinationen hat, obwohl diese Anzahl grösser ist als die Anzahl der Atome im Universum. Wenn wir uns diese 300 Qubits ansehen, finden wir nur eine der möglichen Kombinationen von 1 und 0. Obwohl Qubits in einer Überlagerung vieler Kombinationen existieren, führt eine Messung der Qubits immer zu einer einzelnen binären deterministischen Antwort. Die Quantenalgorithmen stellen sicher, dass das Endergebnis tatsächlich das richtige Ergebnis ist.

Die meisten Quanten-Computer arbeiten bei sehr niedrigen Temperaturen nahe dem absoluten Nullpunkt und benötigen daher grosse Kühlsysteme, um zu funktionieren. Die kommerzielle Entwicklung findet hauptsächlich in den USA statt, wobei Unternehmen wie Google, IBM, Intel, Microsoft und Rigetti im Vordergrund stehen. Die Entwicklung in China wird grösstenteils von der Regierung unterstützt, die europäische Entwicklung findet hauptsächlich in kleineren Forschungsinstituten statt. Auch die australische UNSW (University of New South Wales) hat ein vielversprechendes Programm. Rigetti hat für 2019 einen Quanten-Computer mit 128 Qubits angekündigt, der voraussichtlich der erste mit kommerziellen Anwendungen sein wird.

Abbildung 1: Google's 72-qubit Bristlecone, the first quantum computer to be able to claim "Quantum Supremacy". (The ability to outperform a classical computer to simulate its quantum effects).

Applikationen und Leistung

Da Quanten-Computer unterschiedlich zu herkömmlichen Computern arbeiten, benötigen sie auch völlig neu konzipierte Anwendungen, um Probleme zu lösen. Problemlösungen mit vielen möglichen Lösungen sind für Quanten-Computer prädestiniert wie zum Beispiel die Simulation in der Physik und Bio-Chemie. Quantum Applikationen sind für einfache Operationen nicht optimal eingesetzt. Sie sind jedoch bei bestimmten Aufgaben um ein Vielfaches schneller und effi-

Figure 2: The Atos Quantum Learning Machine (Atos QLM) is a complete on-premise environment designed for quantum software developers. It is dedicated to the development of quantum software, training and experimentation. It embeds a programming platform and a high-performance quantum simulator. Its capabilities and performances are unmatched on the market

zienter als klassische High-Performance-Computer. Beispiel dafür sind Risikoanalysen im Finanzbereich, maschinelles Lernen, Simulation der Physik und das Lösen von komplexen Verschlüsselungs-Algorithmen. Letzteres klingt bedrohlich, es wird jedoch einige Zeit dauern, bis kommerzielle Quanten-Computer die Grösse erreichen, um heute bekannte Verschlüsselungen zu durchbrechen (frühestens ~ 2025). Für Simulationsrechnungen in der Physik und Chemie ist dies anders – hier kann es bereits in weniger als zwei Jahren rentable Lösungen geben wie z.B. die Atos Quantum Learning Machine (QLM) geben.

Die Atos QLM (Quantum Learning Machine) hat diese Simulationsanwendungen entweder vorprogrammiert oder sie kann zur Entwicklung dieser Anwendungen verwendet werden. Die QLM umfasst im Wesentlichen die Entwicklungsplattform, die Compiling Engine sowie das dazugehörige Betriebssystem, integriert in einer Highend-Server-Plattform. Die Atos QLM oder ein ähnliches System wird auch in Zukunft zur Steuerung der Quantenhardware als Basis für Quanten-Hybrid-Anwendungen dienen.

Quantumsicher werden!

Es ist jedoch eine riesige Herausforderung, unsere Computer- und Kommunikationssysteme quantumsicher zu machen. Dies ist nicht nur eine technische Herausforderung, sondern auch eine Managementaufgabe. Die Verschlüsselung wird in den meisten Umgebungen oft schlecht oder gar nicht verwaltet. Ausserdem ist die Verschlüsselung in Hardware und Software eingebettet und manchmal schwer zu ersetzen.

2025 ist nicht mehr weit weg. Organisationen müssen jetzt mit einer Quantenrisikobewertung beginnen, um zu identifizieren, wo die Schwachstellen liegen. Sie müssen in der Lage sein, sich auf die langwierigen Änderungsmanagementprozesse vorzubereiten, um auf quantengesicherte IT umzustellen. Von heute an sollten die verwendeten Verschlüsselungstypen immer unter der Verantwortung des CISO (Chef Information Security Officer) verwaltet werden. Je grösser die Organisation, desto eher sollte sie damit beginnen. Ist eine Organisation besonders anfällig für Angriffe feindlicher staatlicher Akteure, hätte sie eigentlich schon beginnen sollen. In verschiedenen Ländern ist eine Zunahme der Aktivitäten zu beobachten, Regierungen und Verteidigungsministerien quantensicher zu machen. Auch der Finanzsektor muss ständig modernisieren, da Quanten-Computer die fundamentale Basis von Blockchain[1]-Angriffen sein könnten – d.h. auch Blockchain Technologie muss laufend modernisiert werden, um quantumsicher zu bleiben.

Quantum Kryptographie

Quantum Kryptographie ist der Anwendungsfall, bei dem der Austausch von Quanteninformationen für kryptographische Aufgaben verwendet wird. Dies kann Punkt-zu-Punkt sein, wie in der Quantum Key Distribution (QKD) oder es kann End-to-End sein, was die Verfügbarkeit eines Quantum Internets (QI) erfordert.

[1] *Quantum safe blockchains do exist, e.g. the Quantum Resistant Ledger*

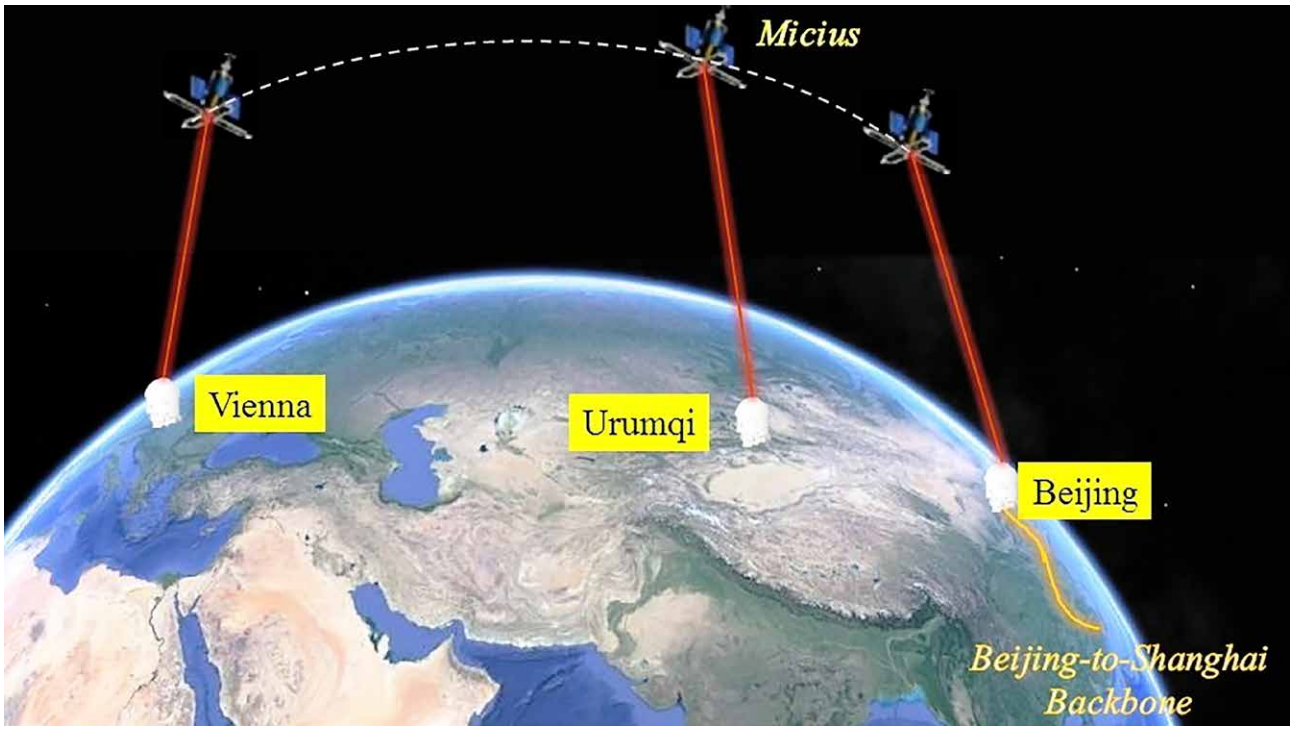


Figure 3: The Chinese Micius sattelite allows the Chinese government to be presently the only one capable of establishing unbreakable QKD encryptions anywhere in the world. Multiple cyberpowers (US, UK, China and Japan) have established QKD networks, with a call underway in the EU.

Für QKD existieren bereits seit über 10 Jahren Lösungen auf der Grundlage relativ einfacher Protokolle. Grundvoraussetzung dafür ist ein guter und schneller Glasfaser-Zugang. Auf Basis von Standard «Off-the-shelf» QKD-Hardware kann bereits eine sehr sichere Punkt-zu-Punkt-Kommunikation aufgebaut werden. Neuere Technologien auf Basis komplexerer Protokolle sind noch in der Entwicklung. QKD hat den klaren Nachteil einer Punkt-zu-Punkt Verschlüsselung – heutige Anwendungsfälle fordern aber ganz klar End-to-End-Sicherheit der Verschlüsselung.

Der erste QI-Pilotversuch wird voraussichtlich bis 2022 in den Niederlanden durchgeführt. Im Gegensatz zu einem reinen Quantum-Computer hat ein QI, also die Kombination von mehreren Quanten-Computern, das Potential zu einer höchst effizienten und sicheren End-to-End-Verschlüsselung. Die Verwendung von Satelliten wird es eines Tages ermöglichen, mit einer nachweislich sicheren Methode sogar für eingesetzte Armeen Codes auf die ganze Welt zu bringen. Der QI hat andere Möglichkeiten, mehrere Technologien zu kombinieren, um einen neuen Sicherheitsstandard zu schaffen, welcher einer raschen Entwicklung der Technologie in der Zukunft standhalten kann.

Darüber hinaus bietet ein QI ein interessantes Potential für Quantum Clouds. Dieses sogenannte «Blind Computing» würde absoluten Schutz der Nutzung von Quanten-Codes auf einem Remote-Quanten-Computerserver ermöglichen. Ein staatlicher Akteur könnte unbemerkt und einfach einen sensiblen asymmetrischen Schlüssel in einem öffentlichen Quanten-Computer-Cluster leicht entschlüsseln.

Auf jeden Fall denken wir, dass IT Sicherheit mit Quantentechnologien in Zukunft deutlich verbessert wird. Wie sehr die Sicherheit sich verbessert, hängt davon ab, wie schnell wir uns auf den Technologiewechsel vorbereiten und diesen implementieren.

BLOCKCHAIN: HÄLT DER HYPE WAS ER VERSPRICHT?

Neue Technologien erreichen uns häufig mit ausgedehnten Versprechen und weitreichenden Hypothesen. Der *Gartner Hype Cycle*[1] ist eine verlässliche Darstellung, wenn es darum geht, die Frage zu beantworten, wie reif eine Technologie an sich ist und wie sich deren Entwicklung gestalten könnte.

Von Martin Deutschmann, Digital Innovations Architekt und Mitglied der Blockchain Experten Gruppe Atos

Im Hinblick auf die Blockchain Technologie ist in Abbildung 1 erkennbar, dass der erste Hype-Zyklus tatsächlich vorüber sein könnte und wir uns nun in einer Phase leichter Desillusionierung befinden (so auch gespiegelt am Kurs-Rutsch einer der prominentesten Blockchain Projekte – Bitcoin. -75% zum vorjährlichem Kurs-Hoch).

Nachdem die Blockchain-Hype-Maschinerie die vergangenen Jahre auf Hochtouren lief, erscheint dieses Abklingen beinahe schon wohltuend für das persönliche Empfinden - vor allem aber notwendig für den technologischen Fortschritt der Materie. Zumindest widmet man sich nun wieder vorerst der Technik und weniger den – durch externe Einflüsse beeinträchtigten – Kurswerten der betreffenden Unternehmen. Darüber hinaus zeichnet sich die momentane Phase auch dadurch aus, dass sich jene Anwendungsfälle der Technologie offenbaren, die reales Potenzial aufweisen und nachhaltig angewandt werden können. Wie kann man aber nun die Blockchain Technologie in wenigen Worten zusammenfassen und warum wird das Thema in so vielen Bereichen thematisiert?

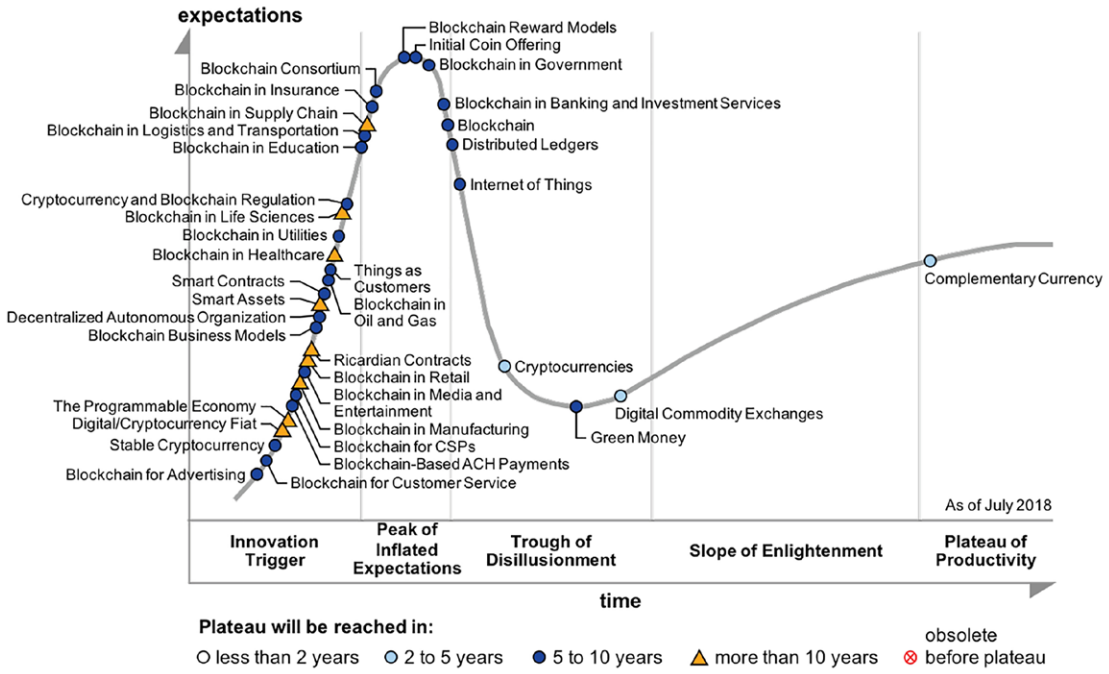


Abbildung 1: Gartner Hype Cycle 2018

[1] *https://www.gartner.com/en/research/methodologies/gartner-hype-cycle*

Blockchain Technologie

Die Blockchain ist eine kontinuierlich erweiterbare Liste von Datensätzen, den «Blöcken» der Kette. Die Blöcke beinhalten Bündel von digitalen Transaktionen und sind mittels kryptographischer Verfahren miteinander verbunden. Dies hat zur Folge, dass Änderungen in einem Block auch zu Veränderungen in allen Folgeblöcken führen. Damit ist es für Angreifer sehr schwer, Inhalte zu manipulieren. Man bedient sich hierfür etablierter mathematischer Protokolle sowie digitaler Signaturen und Hash Funktionen. Die Inhalte der Blockchain werden mit allen Teilnehmern des Netzwerks – unter Zuhilfenahme eines sogenannten Konsensus-Algorithmus[2] Mechanismus – synchronisiert. Dieser Prozess kann im Falle von öffentlichen Blockchain Netzwerken (wie z.B. Bitcoin) sehr aufwändig sein und eine grosse Menge an Ressourcen verschlingen - einer der Gründe, warum Blockchains oft in der Kritik stehen. Die gesamten Prozesse, wie das Schreiben von Transaktionen oder Hinzufügen neuer Blöcke an die Kette, erfolgt ohne die Notwendigkeit einer zentralen Verwaltungsstelle. Alle Knoten (oder Teilnehmer) dieser Netzwerke sind gleichberechtigt. Das Vertrauen wird quasi verteilt. Wie in Abbildung 2 skizziert, können Transaktionen unterschiedlichste Formen annehmen und Inhalte wie Verträge, Zertifikate oder auch Gutachten repräsentieren. Es wäre also zu schmal gegriffen, Blockchains nur auf die Finanzwelt zu reduzieren.

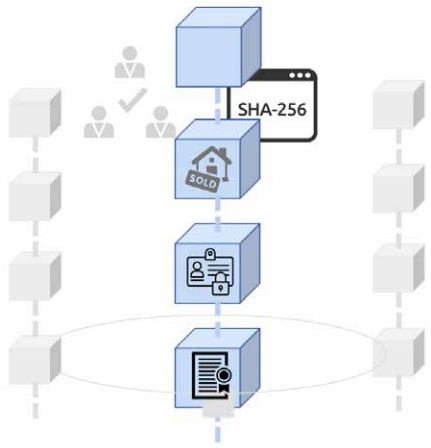


Abbildung 2: Prinzip der Blockchain Technologie

Anwendungsfälle der Blockchain

Blockchains wurden vor allem durch die bereits angesprochenen Krypto-Währungen wie Bitcoin bekannt. Es ist wichtig zu betonen, dass die möglichen Anwendungsfälle aber weit über dies hinaus gehen. Insbesondere muss nicht jede Blockchain öffentlich sein. Ein gutes Beispiel sind Lieferketten, wo eine beschränkte Anzahl von Akteuren, z.B. Rohstoffproduzenten, Logistiker, Verarbeiter, Vertrieb, sich zusammentun und eine sogenannte Konsortium-Blockchain aufbauen, an der nur berechtigte Teilnehmer mitmachen dürfen. Atos konnte gemeinsam mit dem Bureau Veritas in Taiwan einen produktiven Piloten lancieren, mit dem Ziel, die Herkunft von Thunfisch in der Blockchain abzubilden.

Wir haben es geschafft die gesamte Lieferkette in der Blockchain abzubilden, so dass auch der Endkonsument genau und fälschungssicher nachvollziehen kann, wo der Fisch gefangen wurde, wie er verarbeitet und transportiert wurde und wann er es in die Regale des Supermarktes geschafft hat.

Im öffentlichen Sektor bedient man sich seit jeher in breitem Umfang und langer Tradition technologischer Fortschritte. Ein weiterer Anwendungsfall betrifft daher den Bereich öffentliche Sicherheit und Verteidigung. Sicherheitsüberprüfungen, z.B. bei der Rekrutierung von Mitarbeitenden im Sicherheitsdienst, umfassen viele unterschiedliche Akteure. Der gesamte Prozess muss nachvollziehbar, demonstrierbar und die Daten unveränderbar sein. Aktuelle Prozesse benötigen die Einbindung von mehreren Sicherheitsstellen und kosten daher viel Zeit und sind komplex. Atos entwickelte gemeinsam mit einem Verteidigungsministerium einen Blockchain-basierten Prozess zum Abwickeln von Personensicherheitsüberprüfungen. Die Zeit für eine Zertifizierung konnte von Monaten auf Wochen reduziert werden und die Kosten wurden entsprechend deutlich gesenkt.

Weitere Anwendungsfälle im Bereich der öffentlichen Sicherheit betreffen die Verwaltung von sensiblen Daten, wie Luftaufnahmen resp. Lagebildern. Wir setzen gerade ein Pilot-Projekt um, in dem Drohnen Lagebilder aufnehmen, diese verschlüsselt in einer sicheren Cloud-Plattform ablegen und sämtliche Aktivitäten in einer Blockchain geloggt werden. Es ist für alle Akteure der Blockchain transparent nachvollziehbar, wann ein Bild aufgenommen wurde, wer die Aufnahme gemacht hat und ob der Pilot die entsprechende Berechtigung hatte. Ausserdem werden die digitalen «Fingerabdrücke» der Bilder in der Blockchain mitgeloggt und damit eine 1:1 Verbindung der Daten in der verschlüsselten Cloud und der entsprechenden Transaktion in der Blockchain ermöglicht.

[2] *Ein Konsensmechanismus bezeichnet einen Algorithmus, der eine Einigung über den Status eines Netzwerkes zwischen seinen Teilnehmern erzielt um sicherzustellen, dass alle Teilnehmer eine identische Kopie der verteilten Datenbank besitzen.*

Im Gesundheitswesen kann die Blockchain eingesetzt werden, um die Behandlungshistorie eines Patienten fälschungssicher transparent abzubilden und das unter der Wahrung der Privatsphäre der Person. Berechtigte Ärzte können auf einen Blick nachvollziehen, welche Behandlung erfolgte und ob die richtigen Medikamente ausgestellt und auch erworben wurden.

Die Finanzwelt verschliesst sich der neuen Technologie auch nicht und es gibt eine Reihe von Projekten, wo Datenaustausch zwischen Banken mit Hilfe der Blockchain geloggt wird. Ausserdem werden Identitätssysteme auf Basis von Blockchain entwickelt. Diese verfolgen auf der einen Seite das Ziel, der einzelnen Person mehr Souveränität über die eigene Identität zu erlauben. Auf der anderen Seite wird die Abwicklung von Bankgeschäften oder Behördengängen erleichtert.

Blockchain: «Die Vorteile auf einen Blick»

- Datenintegrität: Durch den Einsatz von kryptographischen Verfahren sind Blockchain-Inhalte praktisch unveränderbar.
- Dezentralisierung des Netzwerkes schafft Transparenz und macht Hackerangriffe fast unmöglich.
- Flexibilität: Je nach Anwendungsfall ist es möglich, die Inhalte der Blockchain für die Öffentlichkeit oder nur für einen bestimmten Nutzerkreis sichtbar zu machen.
- Mehr als Krypto-Währung: Alles was digital abgebildet werden kann, lässt sich in der Blockchain verwalten.

Zusammenfassung und Ausblick

Viele Unternehmen stellen sich heute oft die Frage: Brauche ich eine Blockchain? Die Frage sollte aber vielmehr lauten: Habe ich einen Blockchain-Anwendungsfall? Weiter sei erwähnt, dass es technologische Herausforderungen gibt, die lösbar sind - es ist aber vor allem wichtig, organisatorische Rahmenbedingung zu schaffen. Und: Blockchain ist ein Team-Sport, bei dem alle Spieler von Beginn an eingebunden werden müssen und der Nutzen der Technologie stets ins Zentrum gestellt werden sollte. Gerade im Sicherheitsbereich gibt es viele interessante Anwendungsfälle, wo ein Einsatz der Blockchain sehr naheliegend und vielversprechend erscheint.

Nun gilt es, sich den Herausforderungen stellen, um das Potenzial der Technologie bestmöglich auszuschöpfen. Es ist eben nicht nur ein Hype, sondern eine vielversprechende Technologie und das Potenzial ist noch lange nicht ausgeschöpft.

Worte zum Autor:
Martin Deutschmann ist Teil des Digital Innovation Teams von Atos und begleitet Kunden auf dem Weg der Digitalen Transformation. Durch sein Studium der technischen Mathematik, mit Fokus auf Datensicherheit und Kryptographie ist Martin fasziniert von disruptiven Technologien, wie Blockchain, Quantum Computing oder Künstlicher Intelligenz.

STREITKRÄFTE IN UMBRUCHZEITEN

Seit der weltpolitischen Wende zu Beginn der neunziger Jahre versuchen die Streitkräfte, sich laufend auf neue Kriegsformen einzustellen. Dabei gerät strategisches Denken zunehmend in den Hintergrund – auch in der Schweiz. Welche Folgen hat das?

Von Bruno Lezzi

Schon 1973 hat der bekannte britische Historiker und Strategiewissenschafter Sir Michael Howard in einem Vortrag mit dem Titel «Military Science in an Age of Peace» lapidar festgehalten, dass jede in Friedenszeiten erarbeitete Militärdoktrin falsch sei. Das spiele allerdings keine Rolle, sagte er, denn es komme eher darauf an, im richtigen Moment den richtigen Weg einzuschlagen, und zwar möglichst rasch. Deshalb sei es entscheidend, den Hauptakzent auf geistige und organisatorische Anpassungsfähigkeit zu setzen. Im übrigen habe man, so Howard abschliessend, die Bedeutung technischer Neuerungen für die Kriegsführung meist überschätzt.

In der Tat: neue und sich erst noch in rascher Folge ablösende und überlagernde Kriegsformen machen militärische Planung aktuell zu einem noch schwierigeren Unterfangen, als dies im Kalten Krieg unter weitgehend bekannten Parametern der Fall war. Die Suche nach einer Doktrin, das heisst: die Formulierung von grundlegenden Prinzipien für die Kampfführung aufgrund von mittel- und langfristigen Bedrohungsprognosen, ist je länger, desto mehr von grosser Unsicherheit geprägt.

Der moderne Krieg, wie er seit der strategischen Wende zu Beginn der neunziger Jahre des 20. Jahrhunderts beobachtet werden kann, ist zu vielschichtig und facettenreich, als dass er mit den wohlbekannten Adjektiven «asymmetrisch» und «hybrid» schlüssig eingeordnet werden könnte[1].

Die ignorierten Anzeichen einer neuen Kriegsform

Einen Markstein in dieser Hinsicht bildete der Irakkrieg von 1991. Die USA und ihre Koalitionspartner wendeten hier die sogenannte AirLand-Battle-Doktrin, die auf die Verteidigung gegen einen mit gepanzerten Grossverbänden und massiven Lufteinsätzen geführten Grossangriff des Warschauer Paktes zugeschnitten war, fast lehrbuchartig an. Dieser Krieg ist insofern ein Schlüsselereignis, als er einer umfassenden und, wie in den USA üblich, vorwiegend technologisch bestimmten Transformation der amerikanischen Streitkräfte unter dem Stichwort «Revolution in Military Affairs» zusätzliche Dynamik verlieh – das entsprechende operative Einsatzmodell hiess «Network Centric Warfare». Ein auf allen operativ-taktisch relevanten Führungsstufen praktisch in Echtzeit verfügbares elektronisches Lagebild, vernetzte Aufklärungs-, Kommunikations-, Führungs- und Waffensysteme und Präzisionsmunition beschleunigten die Entscheidungsprozesse und erhöhten damit das Tempo und die zielgenaue Wirkung militärischer Operationen.

Dabei wurden allerdings Entwicklungen nicht genügend zur Kenntnis genommen, die zurzeit die Konfliktbewältigung stark erschweren. Die blutigen Auseinandersetzungen auf dem Balkan und der Krieg in Tschetschenien in den neunziger Jahren zeigten, womit man in Zukunft konfrontiert sein könnte. Nationalistische und partikularistische Bewegungen, die Tito und die sowjetischen Machthaber unter Kontrolle gehalten hatten, breiteten sich – nicht selten in Verbindung mit der organisierten Kriminalität – weiträumig aus. So war es nicht erstaunlich, dass die Blauhelme der UNProfor, die mit einem wenig klar definierten, ja eigentlich artfremden Auftrag zur Beruhigung der Lage in Kroatien und in Bosnien-Herzegowina eingesetzt worden war, keine Erfolge erzielen konnten. Da die anschliessend mit starken Kräften geführten Stabilisierungsoperationen der Nato in Bosnien und später im Kosovo ermutigende Resultate lieferten, bestand kein Anlass zu einer grundsätzlichen Neuausrichtung. Die Kommandostrukturen der Allianz wurden zwar an die Erfordernisse von Auslandeinsätzen angepasst und beispielsweise rasch verlegbare Hauptquartiere zur Führung von aus den Teilstreitkräften Heer, Luftwaffe und Flotte gebildeten Einsatzverbänden ausserhalb des eigentlichen Bündnisgebietes geschaffen; Arbeiten zur Formulierung neuer Einsatzverfahren wurden aber noch nicht an die Hand genommen[2].

1 *Als «wahres Chamäleon» bezeichnete schon der preussische Kriegstheoretiker Carl von Clausewitz in seinem Werk «Vom Kriege» den Krieg, weil dieser seine Natur – heute spricht man gewöhnlich von Charakter – je nach Situation ändere.*

2 *Der Satz: «Die Sicherheit der Bundesrepublik Deutschland wird heute auch am Hindukusch verteidigt», den der damalige deutsche Verteidigungsminister Peter Struck 2002 spontan fallenliess, war wohl eingängig, aber als Leitlinie für eine tragfähige Verteidigungspolitik zu allgemein gehalten.*

Kurz nach der Jahrtausendwende wurde nun rasch klar, dass der Irak ein zu komplexes staatliches und gesellschaftliches System war, als dass man ihn mit systemtheoretisch konzipierten Schlägen gegen Gravitationszentren hätte aushebeln können. Schon der damalige General und heutige Verteidigungsminister James Mattis sowie der seines Amtes enthobene Sicherheitsberater Präsident Trumps, der frühere Generalleutnant Herbert McMaster, waren damals überzeugt: Man gäbe sich einer Täuschung hin, glaubte man, Gefechtsfelder dank modernster Technologien jederzeit dominieren (full spectrum dominance) und Friktionen unverzüglich eliminieren zu können[3]. In Anlehnung an Erfahrungen der französischen Streitkräfte im Algerienkrieg in den fünfziger und frühen sechziger Jahren wurden neue Einsatzverfahren für den Kampf im Irak und in Afghanistan entwickelt und mit dem Reglement FM 3-24 («Counterinsurgency») als verbindlich erklärt.

Der «hybride Krieg»

Wie richtig solche Beurteilungen waren, liessen und lassen die neuen unter der Bezeichnung «hybride Kriegsführung» zu beobachtenden Einsatzformen im Nahen und Mittleren Osten, auf der Krim und in der Ukraine erkennen. Die entsprechenden gedanklichen Grundlagen haben James Mattis und Frank Hoffman in einem 2005 publizierten Beitrag mit dem Titel «The Rise of Hybrid Wars» gelegt[4]. Darunter sind Kampfformen zu verstehen, im Rahmen derer konventionelle Waffen und Strukturen, terroristische Aktionen, Guerillataktik und kriminelle Praktiken und nicht zuletzt modernste Kommunikationstechnologie unter Einschluss sozialer Medien zum Einsatz gelangen.

Obschon der «Islamische Staat», der sich als Meister hybrider Einsatzverfahren erwies, als militärischer Machtfaktor praktisch ausgeschaltet werden konnte, wird er weiterhin in der Lage sein, Terroroperationen durchzuführen. Diese Bedrohung zwingt gerade die europäischen Armeen dazu, in enger Zusammenarbeit mit Nachrichtendiensten und Polizeikräften entsprechende Abwehrvorkehrungen zu treffen. Im übrigen hat die erstaunlich rasche Ausbreitung des «Islamischen Staates» im Irak und in Syrien gezeigt, dass von einer Entterritorialisierung des Krieges und seiner Verlagerung in den Cyberraum nicht gesprochen werden kann. Cyberangriffe sind meist Teil einer Gesamtstrategie mit weitgesteckten politischen Zielen und demzufolge nur ein Element im strategischen Instrumentarium.

Eine eigentliche Weichenstellung für eine Kurskorrektur bedeuteten die Annexion der Krim 2014 und die Ukrainekrise, wo der russische Generalstabschef Waleri Gerassimow die hybride Kriegsführung durchexerzieren liess. Interessanterweise bezieht auch er sich, wie er in einem Artikel schreibt, auf konzeptionelle Überlegungen der USA[5]. Aufgrund ernüchternder Erfahrungen im Georgienkrieg von 2008 sind inzwischen organisatorische Massnahmen getroffen worden, die schnelle Operationen im Verbund der Teilstreitkräfte ermöglichen: Anfänglich lag ein Hauptakzent auf der konsequenten Bildung von Brigaden; inzwischen treten auch Divisionshauptquartiere im Organigramm des Heeres wieder in Erscheinung
.

Wachsender Stellenwert der Landstreitkräfte

Die russischen Streitkräfte haben also in den letzten etwas mehr als zwanzig Jahren einen beachtlichen Weg zurückgelegt. Die deplorable, demoralisierte Truppe, die ich im ersten Tschetschenienkrieg 1995 im apokalyptisch zerstörten Grosny zu Gesicht bekam, entwickelte sich zu einer modern ausgerüsteten und entsprechend strukturierten Streitmacht, deren Logistik allerdings noch nicht raumgreifende Operationen erlauben soll.

Diese überraschend zielstrebigen russischen Reorganisationsschritte riefen die Nato auf den Plan. Aufgrund der an den Gipfeltreffen von Wales 2014 und Warschau 2016 getroffenen Beschlüsse wurden Massnahmen zur Optimierung der Krisenbereitschaft wie die Bildung einer Very High Readiness Joint Task Force zur Verstärkung der Nato Response Force (NRF) getroffen. Die Bündnisverteidigung rückte wieder ins Zentrum des Blickfeldes. Vom «integrierten Ansatz» (Comprehensive Approach), vom Verbund diplomatischer, wirtschaftlicher, polizeilicher und militärischer Mittel zur Krisenbewältigung, spricht zurzeit fast niemand mehr.

Bereits im Herbst 2014 übte der Stab des Allied Joint Force Command Brunssum unter Leitung General Hans-Lothar Domröses die Verteidigung des Baltikums gegen einen Angreifer, der – trotz fiktiver Bezeichnung – nur Russland sein konnte. Inzwischen sind regelmässige Übungen im Baltikum und in Polen an der Tagesordnung. Die Stationierung von multinationalen Bataillonen – die sogenannte Enhanced Forward Presence – soll, abgestützt auf das Nuklearpotenzial der Allianz, Russland vor militärischen Abenteuern abschrecken.

3 *Herbert R. McMaster: Continuity and Change. The Army Operating Concept and Clear Thinking about Future War. In: Military Review, März/April 2015. / Herbert R. McMaster: The Human Element: When Gadgetry Becomes Strategy. In: World Affairs Journal, Winter 2009.*

4 *James Mattis und Frank Hoffman: Future Warfare: The Rise of Hybrid Wars. In: Proceedings Magazine, November 2005.*

5 *Valery Gerasimov: The Value of Science Is in the Foresight. New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. In: Military Review, Januar/Februar 2016.*

Der Verbesserung der gemeinsamen Ausbildung und der Interoperabilität dienen der «Readiness Action Plan» und die «Connected Forces Initiative». Und die Verlegung von amerikanischen Truppenverbänden im Rotationsverfahren nach Osteuropa vollzieht sich im Rahmen der «European Reassurance Initiative» und der Operation «Atlantic Resolve».

Unter diesen Vorzeichen geniessen vor allem die Landstreitkräfte einen hohen Stellenwert. Ganz einfach ist deren Ausrichtung auf die neue Lage, das heisst: auf die Bewährung in Kriegen hoher Intensität, indessen auch nicht, wie der frühere französische Generalstabschef Pierre de Villiers in seinem kürzlich veröffentlichten Buch «Servir» schreibt. Schwer gepanzerte Formationen sind zugunsten von Operationen ausserhalb des Bündnisraumes substanziell abgebaut worden. Während der ehemalige deutsche Generalinspekteur Wolfgang Schneiderhan aufgrund der verteidigungspolitischen Richtlinien von 2011 noch 2013 die Zeit gekommen sah, sich vom Denken in den Kategorien des Kalten Krieges zu verabschieden, sind die jetzigen Planungen der Bundeswehr wieder ganz auf die Territorialverteidigung im Bündnisrahmen zugeschnitten. So hat sich Deutschland dazu verpflichtet, der Nato bis 2032 drei voll ausgestattete, einsatzbereite Divisionen zur Verfügung zu stellen.

«Trotz vollmundigen Absichtserklärungen von EU-Politikern wird die Verteidigung Europas Sache der Nato bleiben, die strategisch denkt und handelt.»

Bruno Lezzi

Der Kampfpanzer behält also seine Bedeutung, auch wenn er vermehrt eine Rolle als Unterstützungswaffe spielen soll, die mit präzisem Feuer Einsätze in begrenztem Rahmen begleitet. Die US Army, deren Brigade Combat Teams zwar rasch verlegbar, aber bezüglich Schutz und Feuerkraft der Entwicklung nachhinken, meldet nun Erneuerungsbedarf bei den schweren Gefechtsfahrzeugen an.

Konzeptionell befindet sich das amerikanische Heer also in den vordersten Rängen: Unter dem Stichwort «Multi-Domain Battle» richtet es sich auf ein breites Konfliktspektrum aus. In Analogie zur AirLand-Battle-Doktrin des Kalten Krieges soll die Army den Kampf der verbundenen Waffen im Zusammenwirken mit der Navy und der Air Force auch gegen Seeziele in Küstengewässern und im Cyberraum führen können. Modernste Kommunikationssysteme und unbemannte Systeme, die die Kriegsführung in weniger als zwei Jahrzehnten revolutionieren könnten, sind zwingende Voraussetzungen für die Realisierung eines solchen Konzepts. Zu den Modernisierungsbestrebungen gehört im übrigen auch das kürzlich lancierte Projekt eines Space Command, das in wenigen Jahren als weitere Teilstreitkraft etabliert werden soll.

Nato und EU: Kooperation unter vielen Vorzeichen

Die Vereinigten Staaten sind sich trotz ihres grossen Potenzials bewusst, dass Konflikte nur in Kooperation mit Partnern zu bewältigen sind. Genau deshalb fordert Präsident Trump, dass sich die Nato-Mitgliedstaaten endlich dazu aufraffen, bald 2 Prozent ihres Bruttoinlandsprodukts für die Verteidigung auszugeben. Der damit ausgelöste Streit ist deshalb fruchtlos, weil praktisch keine Antworten auf die Frage gegeben werden, was mit den beträchtlichen zusätzlichen Finanzen geschehen soll. Bei gegebenem Personalumfang ist das Fassungsvermögen der gegenwärtigen Strukturen begrenzt. Mit dem Ziel, Synergien zu gewinnen und Kosten zu sparen, setzt nun die Europäische Union einen starken Akzent auf die sicherheitspolitische und militärische Kooperation: Die Ständige Strukturierte Zusammenarbeit (Permanent Structured Cooperation), wie sie im Vertrag von Lissabon 2007 vorgesehen ist, soll den Weg zu einer eigentlichen europäischen Verteidigungsunion ebnen. Die EU ist sich allerdings im Klaren, dass eine Verstärkung ihrer Verteidigungsvorbereitungen nur in enger Absprache und Zusammenarbeit mit der Nato erfolgen kann, wie dies in den gemeinsamen Erklärungen vom 8. Juli 2016 und vom 10. Juli 2018 zum Ausdruck kommt. Die Allianz selber verfolgt mit der Bearbeitung von Fähigkeitsclustern und dem Rahmennationskonzept, das heisst: der Verankerung von Streitkräften mit breitem Einsatzspektrum mit solchen, die über geringere Kapazitäten verfügen, fast die gleichen Ziele wie die EU.

Der aufwändige, zahlreiche Stäbe beanspruchende Koordinationsaufwand scheint zwar insofern unumgänglich zu sein, als die Mitgliedschaften in Nato und EU nicht völlig deckungsgleich sind. Mit organisatorischer Feinmechanik und Kommandostäben wird aber noch keine Kampfkraft geschaffen. Letztlich widerspricht ein solches Vorgehen dem in der taktischen Führung bewährten Grundsatz einer Konzentration der Kräfte: Es ist nicht zu übersehen, dass trotz einer Vielzahl von neuen Organisationsformen immer dieselben Truppen beansprucht werden, was unweigerlich zu einer Überlastung führen wird. So gesehen sind die bis jetzt noch nie in ihrer Grundstruktur eingesetzten EU-Battlegroups überflüssig.

Trotz vollmundigen Absichtserklärungen von EU-Politikern wird die Verteidigung Europas gemäss Artikel 5 des Nord-

atlantikvertrages bei der Nato bleiben, die strategisch denkt und handelt, etwa mit der Bildung eines Logistikkommandos in Ulm und eines dritten Joint Force Command, welches das frühere Atlantikkommando (Saclant) in neuer Form wiederaufleben lassen will. Die Allianz unterstreicht damit die ungebrochene Bedeutung der Verbindung mit den USA.

Mittendrin: die Schweiz

Von diesen Entwicklungen ist natürlich auch die Schweiz betroffen. In den sicherheitspolitischen Berichten, die seit 1990 verfasst worden sind, wird den jeweils eingetretenen Lageveränderungen zwar Rechnung getragen; das Motto «Sicherheit durch Kooperation», das den Sicherheitsbericht 2000 und damit die Strategie der Schweiz prägen sollte, ist aber nicht verinnerlicht worden. Die in der Bevölkerung tief verwurzelte Neutralität und das Milizsystem erschweren eine pragmatische Anpassung an neue Erfordernisse, auch wenn im neuesten Sicherheitspolitischen Bericht 2016 die internationale Kooperation als nach wie vor bedeutsam beurteilt wird – allerdings mit weniger einprägsamen Formeln, als dies kurz nach der Jahrtausendwende der Fall gewesen war. Und so ist es nicht erstaunlich, dass sich in den letzten Jahren alle Vorhaben für einen Armeeumbau an diesen «Auflagen» orientierten und deshalb ihren Kompromisscharakter kaum verleugnen können.

Die mit der jüngsten Reform «Weiterentwicklung der Armee» anvisierten Verbesserungen von Bereitschaft, Ausrüstung und Ausbildung sind richtig. Hingegen sind strukturelle Eigenheiten erkennbar, die nicht zu überzeugen vermögen: Die Trennung von Kampftruppen zur Gefechtsführung und Schutztruppen zur subsidiären Unterstützung der zivilen Behörden entspricht nicht dem modernen Kriegsbild. Brigaden, die Aufträge in einem weiten Spektrum selbständig erfüllen können, wären die zweckmässigere Lösung gewesen.

Trotz langjährigen Engagements auf dem Balkan fehlen der Schweiz Kriegserfahrungen. In dieser Hinsicht hat Schweden, das im Kalten Krieg – wie die Schweiz – zur Gruppe der neutralen und nichtgebundenen Länder gehörte, einen anderen Weg eingeschlagen: Das Land beteiligte sich nicht nur an der International Security Assistance Force in Afghanistan, sondern auch an der Operation gegen Libyen 2011; und auch bei der NRF ist Schweden engagiert.

Gerade mit Blick auf die geplante grundlegende Erneuerung der Luftverteidigung durch die Beschaffung neuer Kampfflugzeuge und eines bodengestützten Luftabwehrsystems im Rahmen des Projekts «Air 2030» wird die Frage der internationalen Kooperation wieder Aktualität erhalten. Auch bei bester Ausrüstung ist die Schweiz im Bereich der Luftverteidigung darauf angewiesen.

Ausblick: der Wert strategischen Denkens

In einer Welt mit grossem Konfliktpotenzial, in der kaum mehr zwischen Krieg und Frieden unterschieden wird, Kriegserklärungen und Friedensschlüsse der Vergangenheit anzugehören scheinen, ist die Versuchung gross, unverzüglich mit militärischen Mitteln in Konflikte einzugreifen. Berufsstreitkräfte erleichtern solche Entscheide. Gefährlich ist eine solche Entwicklung aber insofern, als strategisches Denken und Handeln in einem Gedankengebäude, das durch politische Ziele, Mittel und Massnahmen bestimmt wird, durch rein militärische Überlegungen und technologisches Kalkül verdrängt werden. Waffensysteme mit künstlicher Intelligenz, die die Entscheidungsprozesse unter höchsten zeitlichen Druck setzen werden, dürften diese Situation noch verschärfen. So hat der von den USA, Grossbritannien und Frankreich geführte jüngste Luftschlag gegen das Chemiewaffenarsenal Assads keine politische Lösung gebracht.

Überschattet wird die an und für sich schon düstere weltpolitische Kulisse noch durch die Gefahr, dass die Nuklearschwelle, wie Studien sie jetzt schon prognostizieren, drastisch gesenkt werden könnte, um das Fehlen von konventionellen Reserven wettzumachen[6]. Da sich zurzeit keine Initiativen zur Rüstungskontrolle im nuklearen und konventionellen Bereich abzeichnen, werden Streitkräfte weiterhin und wohl vermehrt zur Durchsetzung von nationalen Interessen bleiben. Da Systeme kollektiver und kooperativer Sicherheit wie die UNO und die OSZE erhebliche Einbussen an Stosskraft erlitten haben, fehlen wesentliche Bremsfaktoren zur Verhinderung oder Begrenzung blutiger Auseinandersetzungen, die unsägliches Leid und Zerstörungen mitbringen.

---

*6 Matthew Kroenig: The Renewed Russian Nuclear Threat and NATO Nuclear Deterrence Posture. Issue Brief February 2016. Washington D.C.: Atlantic*Council. Web: www.atlanticcouncil.org/images/publications/Russian_Nuclear_*Threat_0203_web.pdf /Wesley Clark, Jüri Luik u.a.: Closing NATO's Baltic Gap. Tallinn: International Center for Defence and Security. Web: icds.ee*

Zum Autor: Bruno Lezzi ist Militärhistoriker und Lehrbeauftragter am Institut für Politikwissenschaft der Universität Zürich. Von 1983–2009 war er NZZ-Redaktor für Sicherheits- und Verteidigungspolitik. Als Generalstabsoberst war er in letzter Funktion in der Sachgruppe Strategie des Armeechefs eingeteilt.

Dieser Artikel ist in der Septemberausgabe des «schweizer monat» *erschienen und wurde uns mit freundlicher Genehmigung des Chefredaktors zur Publikation freigegeben.*
www.schweizermonat.ch

AMERIKANISCHE MILITÄRMACHT IM WANDEL

Der 11. September 2001 oder 9/11, wie man den Anschlag auf das World Trade Center in New York und auf das Pentagon in Washington in den USA allgemein nennt, war eine Zäsur: Das erste Mal kam der Krieg aufs Festland der USA. Dieser als Kriegserklärung aufgefasste Terroranschlag prägte nicht nur das kollektive Bewusstsein, sondern resultierte auch im vielzitierten Ausdruck «War on Terror». Und genau dieser Krieg dem Terror war während den letzten 15 Jahren der Kerngedanke, der die amerikanischen Rüstungsanstrengungen, die Struktur und Einsatzdoktrin der Truppen und die Investitionen in neue miltärische Fähigkeiten bewegte.

Von Peter Huber, Mitglied Vorstand STA

Der seit dem kalten Krieg ausgedünnte Aufklärungsdienst wurde personell und materiell wieder auf- und ausgebaut. Neben der elektronischen Aufklärung wurden wieder vermehrt Spione eingesetzt und der Kampf im Cyber-Space wird heute von über 6000 Armeeangehörigen dauernd geführt und ist weiterhin im Aufbau begriffen. Die amerikanischen Truppen haben in der Zwischenzeit 15 Jahre Erfahrung in der asymmetrischen Kriegführung gewonnen. Schmerzliche Verluste führten zu Anpassungen in der Ausrüstung und im Einsatz. Gezielte Tötungen von Terroristen in verschiedenen Weltregionen, oft mit Drohnen, waren lange an der Tagesordnung, oft auch von Kollateralschäden begleitet, politisch von allen Seiten instrumentalisiert und in der Presse breit kommentiert.

Man kann unterschiedlicher Ansicht über dieses Vorgehen und die damit verbundenen lokalen politischen Verwerfungen sein, aber man muss heute feststellen, dass die Terroranschläge auf dem Gebiet der westlichen Demokratien sich in einem sehr bescheidenen Mass bewegen. Aus amerikanischer Sicht ist dieser Krieg weitgehend gewonnen. Man ist sich heute sicher, dass man diese Gefahr in den Griff gekriegt hat und ist auch bereit, weiterhin erbarmungslos und unter Inkaufnahme von Kollateralschäden gegen radikalisierte Gruppen vorzugehen.

Als Schweizer sollten wir uns die Frage stellen, ob wir bis jetzt vom Terror vor allem wegen unserer guten Aussenpolitik oder wegen dem Einsatz der Amerikaner vorschont wurden. Niemand kann mit Bestimmtheit eine Antwort geben, denn wir wissen nicht, wie die alternative Entwicklung verlaufen wäre. Es ist jedoch davon auszugehen, dass in den doch etwas kriegsmüden USA die weiterhin immensen Kosten für die Terrorbekämpfung nicht ohne guten Grund getragen werden.

Nun aber scheint der nächste Wendepunkt für die amerikanische Militärdoktrin gekommen zu sein. Terroristische Gruppen als Bedrohung für die westliche Welt sind auf Rang 4 bis 5 abgerutscht. An ihre Stelle sind getreten: China, Russland, Iran und Nordkorea. Während viele Leute in Europa darüber rätseln, ob wir auf einen neuen kalten Krieg zusteuern, sind wir in den Augen der amerikanischen Experten schon mittendrin. Diese von Diktatoren gesteuerten Staaten sind alle daran, sowohl atomar aufzurüsten als auch ihre konventionellen Streitkräfte massiv auszubauen. Die amerikanische Sicht der Dinge ist klar: Wer daran glaubt, dass diese Bemühungen auf Verteidigung ausgerichtet sind, hat entweder nichts im Geschichtsunterricht verstanden und verfügt über keine Kentnisse der Waffensysteme dieser Länder oder ist einfach unheilbar naiv. Was heisst das nun für die USA?

Die Antwort ist so erschreckend wie einfach. Die konventionellen Streitkräfte für «Large Scale Operations», das heisst für eine Kriegführung gegen einen anderen Staat, werden ausgebaut. Es ist kein Zufall, dass die USA im November dieses Jahres Artilleriegeschütze mit 70 km Reichweite getestet haben. Der Fokus auf die asymmetrische Kriegführung der letzten 15 Jahre hat dazu geführt, dass der technologische Vorsprung der USA im Bereich der konventionellen Grosssysteme (Panzer, Artillerie, Kriegsschiffe etc...) gegenüber den genannten Staaten geschrumpft oder ganz erodiert ist. Diese Systeme sind zwar nicht so hoffnungslos veraltet, wie die in weiten Teilen Europas im Einsatz stehenden Museumsstücke, aber sie sind auch nicht mehr auf dem neusten Stand der Technik.

Die Absicht der USA ist nun aber, diesen technologischen Vorsprung, den sie im Bereich der Luftkriegführung (vor allem mit dem F-35 und dem F-22) noch immer haben, auch wieder mit den grossen Systemen der Land- und Seestreitkräfte zu erreichen. Dabei wollen sie den Entwicklungszyklus von der Definition bis zur Inbetriebsetzung solcher Systeme von 12 bis 15 Jahren auf 4 bis 7 Jahre schrumpfen. Die entsprechenden Prozesse und Regulierungen werden zur Zeit in intensiver Zusammenarbeit zwischen der Regierung und der Rüstungsindustrie angepasst und schlanker gestaltet. Techni-

sche Innovation ist wieder eine primäre Komponente geworden. Nun ist es eine politische Entscheidung, wie viel Geld dafür von der amerikanischen Regierung in den nächsten Jahren freigegeben wird. Aber die Stossrichtung ist gegeben und zwar unabhängig davon, wer im Weissen Haus sitzt. Vor diesem Hintergrund ist auch klar, weshalb die USA, die 70 bis 80 % der gesamten NATO-Kosten tragen und damit auch die Verteidung Europas finanzieren, eine sinkende Begeisterung dafür aufbringen, amerikanische Steuergelder für ihre Freunde in Europa auszugeben. Sie werden dieses Geld für die eigenen neuen Bedürfnisse brauchen, denn auch ihre Ressourcen sind nicht unbeschränkt.

Man kann den Stil des amerikanischen Präsidenten kritisieren, aber wenn 350 Mio. Personen 80 % zahlen und 450 Mio. Personen 20 %, dann ist der Ausdruck «unfair» wohl nicht unpassend. 2 % vom BIP für Verteidigung ist nicht eine Zahl, die irgend ein Irrer aus dem Hut gezaubert hat, sondern ist das Resultat von profunden Analysen und strategischen Überlegungen. Die USA geben etwas über 3 % vom BIP für Verteidigung aus. Der Druck auf die NATO-Partner, mindestens 2 % zu erreichen, wird nicht nachgeben und birgt in sich das Risiko von grossen Zerwürfnissen. Den Amerikanern ist nach 15 Jahren Diskussion nun einfach die Geduld ausgegangen. Es wird an den eurpäischen NATO-Partnern liegen, ob sie weiterhin an einer militärischen Verteidigung ihrer Länder festhalten wollen oder nicht. Die Zeit, in der die Amerikaner dafür bezahlten, ist jedenfalls mit einer kurzen Zündschnur am Ablaufen.

Die Schweiz als Kleinstaat kann sich den Veränderungen der global wirkenden Machtverschiebungen nicht entziehen, kann sie aber weder steuern noch wesentlich beeinflussen. Sie kann diese nur in ihre eigenen Überlegungen einbeziehen. Heute steht der dringende Ersatz aller grossen Waffensysteme der Schweizer Armee über die nächsten 15 Jahre an, begonnen bei der Luftwaffe und der Fliegerabwehr. Die zu erwartenden öffentlichen Diskussionen werden sicher politisch, emotional, zum Teil dogmatisch und ideologisch geführt werden.

Die STA steht hinter einer starken und gut ausgerüsteten Schweizer Armee und wird sich für eine faktenbasierte Debatte einsetzen.

DEFTECH-Workshop «Swarming & Machine Teaming»

In der Navigation ist das richtige Timing entscheidend und Navigation ist wiederum ein Schlüsselelement im Thema «Physical Swarming». Das fünf Jahre Jubiläum von DEFTECH war somit die perfekte Gelegenheit, um den letzten Workshop im 2018 dem Thema «Swarming and Machine Teaming» zu widmen. Die internationale Konferenz fand am 21. November in Thun statt. Rund 120 Experten mit unterschiedlichen Perspektiven auf die Thematik nutzten diese Chance, um angeregt über die für die Verteidigung potenziell disruptiven Technologieentwicklungen zu diskutieren.

Von Patricia Zwygart, armasuisse

Presentation of Manned unmanned teaming and Swarming opportunities and challenges by Martin Hagström from the Swedish Defence Research Agency (FOI)

Relevanz für Verteidigung

Wieso messen wir diesem Thema in Bezug auf die Verteidigung eine solch hohe Bedeutung bei? Weil es sowohl bei «Swarming» als auch bei «Multi-Roboter-Kooperation» darum geht,

1. dass Roboter gefährliche Aufgaben übernehmen und so das Risiko für den Menschen senken.

2. dass die immer frappanter steigenden Kosten des Betriebes und der Instandhaltung von militärischen Plattformen wie Panzer und Kampfflugzeuge reduziert werden.

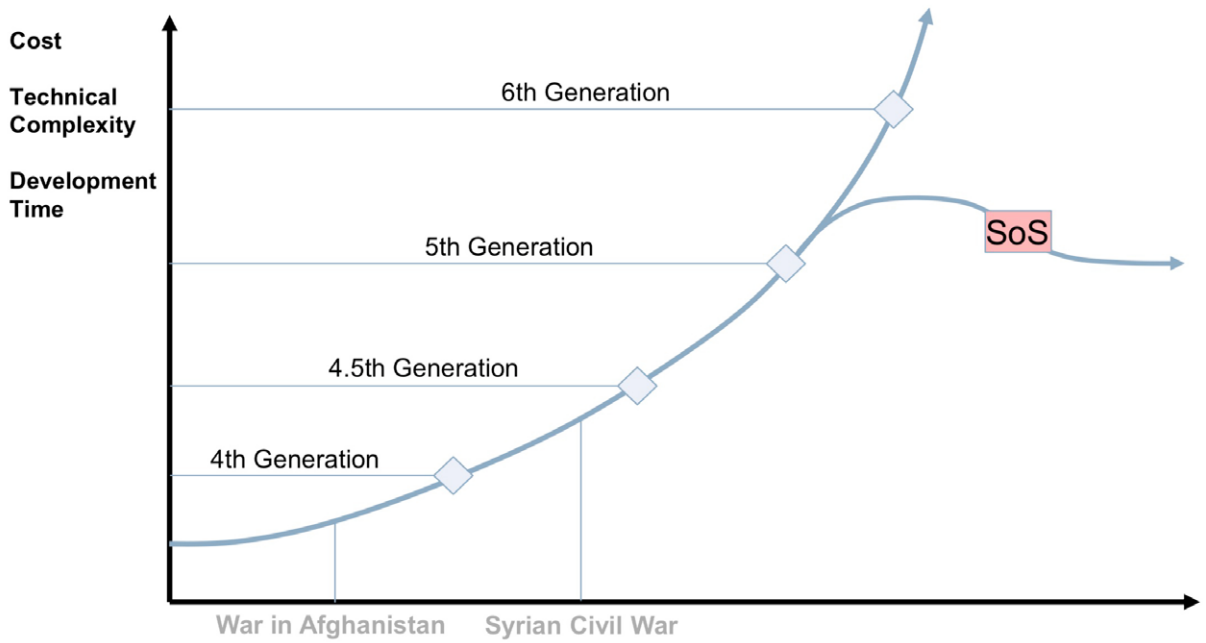
Konkret geht es bei der Reduktion der Kosten um die Frage, wie kostspielige Einzelsysteme durch eine Vielzahl von kostengünstigen Komponenten ersetzt werden können. Bereits liegen erste Lösungsansätze von Forschenden vor. Allerdings ist es nicht ratsam, Lösungsansätze aus Laborexperimenten 1:1 in die «reale Welt» zu übertragen. Zu viele unberechenbare Faktoren wie das Wetter oder sich immerfort wandelndes städtisches Terrain spielen im echten Einsatz eine bedeutsame Rolle.

Herausforderungen

Vertrauen – Das Kreieren von Vertrauen zwischen Mensch und Maschine ist keineswegs eine einfache Aufgabe. Damit Vertrauen entstehen kann, muss der Mensch die Maschine verstehen, ihre nächste Handlung abschätzen können. Fakt ist - ohne Vertrauen werden diese heterogenen Teams nie erfolgreich zusammenarbeiten können.

Technologien – Kommunikationsschnittstellen und unterschiedliche Geschwindigkeiten der Systeme sowie der Energieverbrauch insgesamt sind Hürden, welche der aktuelle Stand der technologischen Entwicklung noch nicht befriedigend überwinden kann.

Armee – Die Integration solcher Elemente in die Truppen wird eine massgebliche Anpassung der Doktrin, der operationellen Vorgehensweisen und nicht zuletzt der logistischen Prozesse bedeuten.



The use of swarming with low-cost systems as a possibility to reduce the cost and the development time of the new air platforms. Source: Dr. Prazeres da Costa, Georg Dietz, IABG 2018.

.

Fazit

Diese Herausforderungen müssen vor einer erfolgreichen Einführung der neuen Technologien erst einmal gemeistert werden. Das braucht Zeit. Experten schätzen die benötigte Zeit bis zur vollen Integration auf rund 20 Jahre. Es lohnt sich jedoch bereits jetzt, dran zu bleiben, denn sowohl die Akademien als auch die Industrien weltweit arbeiten fieberhaft an unterschiedlichsten, befähigenden Technologien wie künstliche Intelligenz oder «Machine Learning».

TECHNOLOGIEFRÜHERKENNUNG BEI ARMASUISSE W+T
5 JAHRE DEFTECH

Forschungsprogramm «Technologiefrüherkennung»

Pünktlich zum Jubiläum hat auch das Forschungsprogramm neue Horizonte eröffnet. Eine Kombination aus «Science-Fiction» und «Serious Game» hilft den Teilnehmenden in scheinbar reale Situationen einzutauchen, während die Umgebung unter vollständiger Kontrolle bleibt.

Die Science-Fiction-Erzählungen haben sich in den 50er- und 60er-Jahren mit den Technologiebereichen und Trends auseinandergesetzt, die heute Wirklichkeit werden. In welchem Zusammenhang wurden diese Technologien betrachtet und was waren die entsprechenden Befürchtungen oder Hoffnungen? In dieser Publikation wird die Fiktion den sehr reellen Entwicklungen, die sie möglich machen sollen, gegenübergestellt

Science-Fiction

Die starken Bilder einer erfundenen Zukunft geben den Teilnehmenden eine Übersicht über die Situation. Die fiktive Welt hilft ihnen dabei, nicht darüber nachzudenken, ob eine Technologie (oder ein neues Produkt) existieren kann. Sie befinden sich ausserhalb jedes sozio-wirtschaftlichen, ethischen, rechtlichen usw. Kontexts.

Der Einsatz von Science-Fiction erlaubt uns, in Workshops extreme Hypothesen und Szenarien zu testen, die - wenn sie zu sehr mit der Gegenwart verbunden sind - grosse Vorbehalte oder markante Verzerrungen zur Folge haben können.

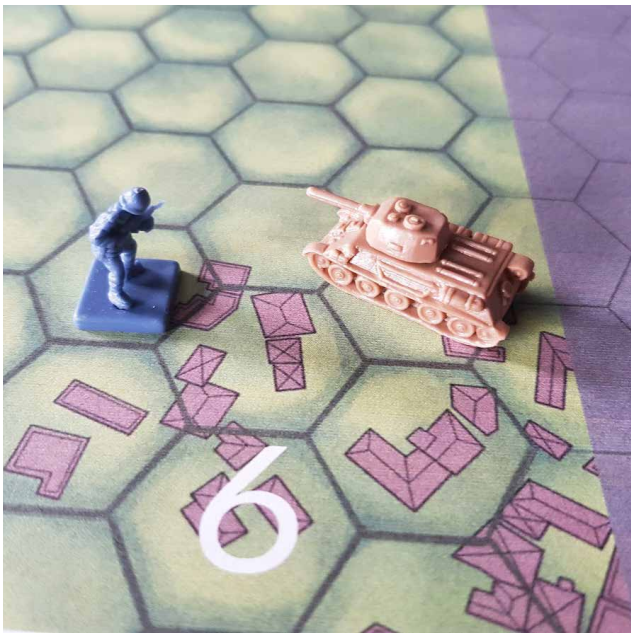
Serious Game

Das sogenannte «ernsthafte Spiel» bietet den Teilnehmenden die Gelegenheit, den Beitrag einer neuen Technologie zu messen. Es ermöglicht ihnen, sich die Zukunft mit einem geringeren Risiko und - was nicht unbedeutend ist - zu geringeren Kosten, anzueignen.

Das Spiel beginnt, indem zunächst eine taktische Situation (blau gegen rot) mit aktuellen Einsatzsystemen und -verfahren gespielt wird. Anschliessend wird die gleiche Situation erneut gespielt, wobei diesmal eine der kriegführenden Parteien mit einer neuen Ausrüstung ausgestattet ist. Dies gibt den Spielenden die Möglichkeit, ein Bewusstsein für Vor- und Nachteile der Veränderung zu erhalten.

Fazit

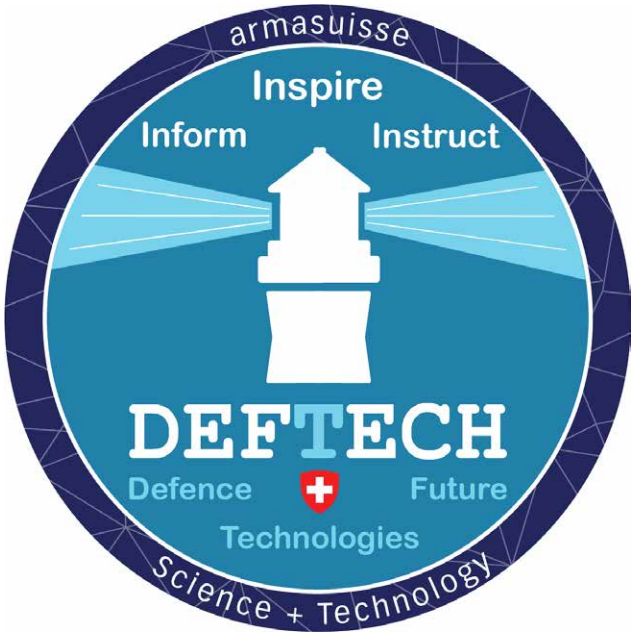
Zukunftszenarien spielerisch zu testen und darin Technologien auszuprobieren, welche erst in ferner Zukunft verfügbar sein werden – das ist die Aufgabe, welcher sich die DEFTECH-Workshops stellen. Sie befähigen die Teilnehmenden mit ih-



Mit dem Serious Game (ernsthaften Spiel) kann veranschaulicht werden, wie noch nicht existierende Technologien und Systeme bei Einsätzen verwendet werden könnten. Die Spieler können sich in dieser Etappe die Zukunft aneignen und sich rasch und einfach des möglichen Mehrwerts dieser neuen Elemente bewusst werden, wobei sie gleichzeitig ihre möglichen Situationen und ihre Integration in neue militärische Kapazitäten berücksichtigen können.

rem experimentellen Ansatz, die Auswirkung und Wichtigkeit einer Technologie besser zu assimilieren.

Durch diese Interaktion mit den verschiedenen Stabsstellen der Schweizer Armee, die für deren zukünftige Entwicklung verantwortlich sind, kann die Verwendung dieser disruptiven Technologien aus verschiedenen Blickwinkeln analysiert werden. Damit wird ermöglicht, Befürchtungen und Hoffnungen besser zu erfassen und so Aufschlüsse über Chancen und Risiken zu erhalten.



Die visuelle Identität von DEFTECH wird mit einem Scheinwerfer symbolisiert, der der Reihe nach die 360° des technologischen Horizonts beleuchtet und als Bezugspunkt (oder Eingang) für die verschiedenen Fragen in Bezug auf die technologischen Trends und ihre militärischen Folgen dient.

Links

Alle Informationsprodukte sind auf der folgenden Seite zugänglich:

https://deftech.ch

Forschungsprogramm «Technologiefrüherkennung»:
http://wt.deftech.ch/

Forschungsprogramme von armasuisse Wissenschaft und Technologie:
http://sicherheitsforschung.ch

armasuisse Wissenschaft und Technologie:
http://www.armasuisse.ch/wt

Kooperative Technologieplattform: https://envisioning.io

AUSBLICK STA 2019

Präsentation Armeeboschaft 2019
Dienstag, 2. April 2019, Thun

Generalversammlung STA
Mittwoch, 22. Mai 2019, Emmen

Industrieorientierung armasuisse / Herbstveranstaltung STA
Donnerstag, 7. November 2019, Mannschaftskaserne, Bern

STA - VORSTAND

Titel	Name Vorname	Ressort	Funktion / Institution	E-Mail
Dr.	Fritz Gantert	Wirtschaft	Unabhängiger Verwaltungsrat / Unternehmer	fbg@bluewin.ch
	Urs Breitmeier	Wirtschaft	CEO / RUAG Holding AG	urs.breitmeier@ruag.com
	Peter Huber	Wirtschaft	Selbstständiger Verwaltungsrat	peter.huber@sublevo.ch
	Walter Kägi	Wirtschaft		kaegi3@bluewin.ch
Dr.	Thomas Rothacher	Beschaffung & Technologie	Leiter KB Wissenschaft + Technologie / armasuisse	thomas.rothacher@armasuisse.ch
KKdt	Philippe Rebord	Armee	Chef der Armee / Departamentsbereich Verteidigung	philippe.rebord@vtg.admin.ch