Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confedraziun svizra

armasuisse

Langfristiger Forschungsplan 2025 - 2028

Forschungskonzept armasuisse mit Forschungs-schwerpunkten und prioritären Themenfeldern

Langfristiger Forschungsplan (LFP) 2025 - 2028

Forschungskonzept armasuisse mit Forschungsschwerpunkten und prioritären Themenfeldern

Herausgegeben von
Bundesamt für Rüstung armasuisse
Bern, 2024

Impressum

Herausgeber

© Bundesamt für Rüstung armasuisse (ar)
Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS)

Publikation

Oktober 2024

Autoren

Dr. Corina Beerli (ar), Dr. Hansruedi Bircher (ar), Dr. Kilian Wasmer (ar)

Begleit- und Arbeitsgruppen

Arbeitsgruppe LFP 2025-2028:
Dr. Corina Beerli (ar), Dr. Hansruedi Bircher (ar), Nico Grandjean (V, A Stab), Dr. Anita Noli-Kilchenmann (V, A Stab), Dr. Kilian Wasmer (ar), Oberstlt Dominik Winter (V, A Stab), Alexander Zagoda (V, A Stab)

Arbeitsgruppe Politikbereich Friedens- und Sicherheitspolitik 2025-2028:
Dr. Corina Beerli (ar), Dr. Hansruedi Bircher (ar), Dr. Cédric Invernizzi (BABS), Gina Menghini (EDA, AIS), Giorgio Ravioli (BABS), Sylvia Völgyi (EDA, AIS), Christoph Werner (BABS)

Sounding Board:
Daniel Bhend (V, Kdo Ausbildung), Urs Born (V, Kdo Cyber), Dr. Daniel Fuhrer (V, A Stab), Michael Hirschi (V, LBA), Dr. David Humair (V, Kdo Operationen), Michael Nussli (V, LBA), Oberst Daniel Setz (V, Kdo Ausbildung)

Expertengruppe für die wissenschaftliche Begleitung:
Dr. Gérôme Bovet (ar, Data Science), Dr. Peter Erni (ar, Weltraum), Dr. Markus Höpflinger (ar, unbemannte mobile Systeme), Dr. Quentin Ladetto (ar, Technologiefrüherkennung), Dr. Ulrich Langer (ar, Weltraum), Dr. Ronny Lorenzo (ar, Wirkung, Schutz und Sicherheit), Dr. Christof Schüpbach, (ar, Kommunikation), Dr. Matthias Sommer (ar, Simulation), Dr. Bernhard Tellenbach (ar, Cyber Defence), Dr. Peter Wellig (ar, Aufklärung und Überwachung)

Gestaltung

Lucas Ballerstedt (ar)

PDF-Download

www.ressortforschung.admin.ch

Kontakt

armasuisse Wissenschaft + Technologie,
wt@armasuisse.ch

Vorwort

Seit der Erstellung des letzten Forschungsplans haben uns mehrere Ereignisse erschüttert, drei von besonderem Ausmass: die COVID-19-Krise, der Krieg in der Ukraine und die Eskalation im Nahost-Konflikt. Diese Ereignisse haben in der Bevölkerung und auch in den Medien das Interesse an sicherheitspolitischen Aspekten vermehrt in den Fokus gerückt.

Die COVID-19-Krise offenbarte, wie verletzlich unsere Gesellschaft und unsere Wirtschaft sind. So waren soziale Medien grosse Treiber von gesellschaftlicher Radikalisierung und Spaltung. Der Wirtschaft wurde die Kehrseite ihrer internationalen Arbeitsteilung und Versorgungsabhängigkeit vorgeführt. Die COVID-19 -Krise hat auch gezeigt, dass letztlich jedes Land seine eigenen Bedürfnisse und Interessen in den Vordergrund stellt. Auf der anderen Seite ist die COVID-19-Pandemie ein gutes Beispiel dafür, wie in einem innovativen Land wie der Schweiz mittels Forschung die Grundlagen für eine rasche Bewältigung von Krisen bereitgestellt werden können.

Der Ukrainekrieg wiederum zeigte uns, dass moderne Konflikte auf allen Ebenen, militärisch, politisch und wirtschaftlich, ausgetragen werden. Dieser Konflikt zeigt auch die Urbanisierung des Krieges, die gezielte Bekämpfung kritischer Infrastrukturen, die neue Rolle ziviler Akteure im Bereich der Satellitenaufklärung und -kommunikation sowie die zunehmende Bedeutung von weitreichenden Waffen beziehungsweise deren Abwehr zum Schutz der Bevölkerung, der eigenen Kräfte und kritischer Infrastrukturen. Auffallend ist die Kreativität und die hohe Geschwindigkeit, mit der die ukrainische Seite zivile Technologien zeitweise zu ihrem Vorteil zu nutzen vermag, sei dies in der taktischen Aufklärung, in der Zielzuweisung oder in der Lokalisierung von gegnerischen Kontrahenten. Beeindruckend ist auch, wie innovativ sie neue Technologien, wie beispielsweise Drohnen, einsetzen und weiterentwickeln.

Die Komplexität moderner Konflikte stellt für die Weiterentwicklung der Sicherheitskräfte sowie für die Planung, Beschaffung und für den Betrieb von Einsatzmitteln eine grosse Herausforderung dar. Hier spielen wissenschaftliche Kompetenzen, die sowohl auf das zivile als auch auf das militärische Technologieumfeld ausgerichtet sind, eine zentrale Rolle. Die Technologieentwicklung muss beobachtet und daraus resultierende Konsequenzen für die Sicherheit der Schweiz antizipiert und zum Nutzen der Armee umgesetzt werden. Forschung ist somit ein Instrument, um die Expertisefähigkeit von armasuisse im Bereich sicherheitsrelevanter Technologien sicherzustellen. Sie bildet DIE Basis zur Unterstützung der fähigkeitsorientierten Weiterentwicklung der Armee, zur Förderung von technologiegetriebenen Innovationen und zur Unterstützung von Systemevaluationen der Beschaffung von armasuisse. Die Forschung leistet damit einen wesentlichen Beitrag zur nachhaltigen Sicherheit und Unabhängigkeit der Schweiz.

Der vorliegende Langfristige Forschungsplan legt die thematischen Schwerpunkte und die Vorgehensweise zur Erreichung dieser Zielsetzung für die Jahre 2025 bis 2028 fest.

Dr. Urs Loher

Rüstungschef

Inhalt

Zusammenfassung

Die Forschung von armasuisse schafft die Grundlage für ein vertieftes Verständnis derjenigen Technologien, welche für die Sicherheit der Schweiz relevant sind. Durch den Aufbau von technisch-wissenschaftlichen Kompetenzen können die Armee, der Nachrichtendienst des Bundes und das Bundesamt für Cybersicherheit mit fundierten und unabhängigen Expertisen unterstützt werden. Die Erkenntnisse aus der Forschung fliessen sowohl in die langfristige Streitkräfteentwicklung als auch in die Evaluation von Systemen während der Beschaffung durch die armasuisse ein. Ferner bildet ein gutes technisch-wissenschaftliches Expertenwissen auch eine gute Basis für technologiegetriebene Innovationen in der Armee und im VBS.

Im vorliegenden Forschungskonzept, dem Langfristigen Forschungsplan (LFP), werden im Rahmen der Ressortforschung des Bundes die inhaltlichen Forschungsprioritäten für den Zeitraum 2025 - 2028 aufgezeigt. Diese orientieren sich an den festgestellten technologischen Megatrends und am Bedarf der sicherheitspolitischen Akteure des VBS, insbesondere der Armee. Die Forschung von armasuisse verfolgt deshalb einen mittel- bis langfristigen Zeithorizont, ist anwendungsorientiert und konzentriert sich auf einen mittleren Technologiereifegrad bis hin zur Realisierung von Demonstratoren. Dabei werden sowohl Kooperationen im Expertennetzwerk als auch multidisziplinäre Ansätze mit potenziellen Nutzern verfolgt.

Dazu wurden vier aufeinander abgestimmte Forschungsschwerpunkte definiert und sind in Abbildung 1 dargestellt:

- Die Technologiefrüherkennung um disruptive Technologieentwicklungen zu erkennen und deren Konsequenzen im sicherheitspolitischen Kontext abzuschätzen. Die Technologiefrüherkennung dient neben der Reduktion von Planungsrisiken von Sicherheitskräften auch der Identifikation von neuen Forschungsthemen.
- Der Forschungsschwerpunkt «Technologien für operationelle Fähigkeiten» zeigt auf ausgewählten Gebieten den Einfluss der Technologieentwicklung auf die operationellen Fähigkeiten von Sicherheitskräften auf. Dabei werden primär die Auswirkungen der Digitalisierung im Rahmen des Sensor-Nachrichtendienst-Führungs-Wirkungsverbund (SNFW), aber auch Wirk- und Schutzprinzipien untersucht.
- Die Integration von Technologien zu Plattformen ist ein Forschungsschwerpunkt, welcher anhand von Demonstratoren das Technologiepotenzial für Einsätze aufzeigen soll. Damit wird auch die Brücke in technologiegetriebene Innovationen von Plattformen geschlagen.
- Die Querschnittsthemen umfassen Forschungsaspekte, welche für eine gesamtheitliche Betrachtung der anderen Forschungsschwerpunkte relevant sind.

Abbildung 1: Forschungsschwerpunkte und prioritäre Themenfelder des LFP 2025-2028

Résumé

La recherche d'armasuisse crée la base d'une compréhension approfondie des technologies pertinentes pour la sécurité de la Suisse. Le développement de compétences technico-scientifiques permet de soutenir l'armée, le Service de renseignement de la Confédération et l'Office fédéral de la cybersécurité par des expertises fondées et indépendantes. Les connaissances issues de la recherche sont intégrées aussi bien dans le développement à long terme des forces armées que dans l'évaluation des systèmes lors de leur acquisition par armasuisse. Une bonne expertise technico-scientifique constitue également la base importante pour les innovations technologiques au sein de l'armée et du DDPS.

Le présent plan directeur de recherche à long terme (PDRLT) met en évidence les thèmes prioritaires de recherche dans le cadre de l'administration fédérale pour la période 2025 – 2028. Celles-ci s'orientent sur les mégatendances technologiques identifiées et sur les besoins des acteurs de la politique de sécurité du DDPS, en particulier de l'armée. La recherche d'armasuisse s'inscrit donc dans une perspective à moyen et long terme. Elle est aussi orientée vers les cas d'usages et vise un degré de maturité technologique modéré jusqu'à la réalisation de démonstrateurs.

Pour ce faire, quatre axes de recherche coordonnés ont été définis :

- *La prospective technologique permet de reconnaître les développements technologiques aux applications potentiellement disruptives et d'évaluer leurs conséquences dans le contexte de la politique de sécurité. La prospective technologique sert non seulement à réduire les risques de planification des forces de sécurité, mais également à identifier de nouveaux thèmes de recherche.*
- *L'axe de recherche «Technologies pour les capacités opérationnelles» étudie, dans des domaines choisis, l'influence du développement technologique sur les capacités opérationnelles des forces de sécurité. Il s'agit d'étudier en priorité les effets de la numérisation dans le cadre des réseaux de capteurs, de renseignements, de conduite et d'action, mais aussi les principes d'action et de protection.*
- *L'intégration de technologies dans les différentes plates-formes est un axe de recherche qui doit montrer le potentiel technologique d'amélioration ou de substitution à l'aide de démonstrateurs. Cela permettra également de jeter un pont vers les innovations technologiques des plates-formes.*
- *Les thèmes transversaux comprennent des aspects de la recherche qui sont pertinents pour une approche globale des autres axes de recherche.*

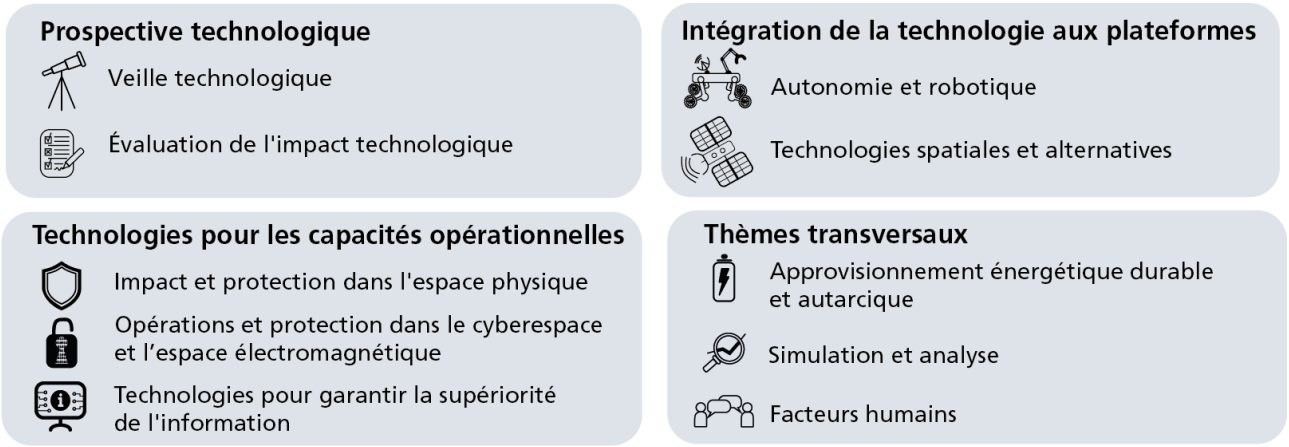


Illustration 1: Axes de recherche et domaines thématiques prioritaires du PDRLT 2025-2028

1 Einleitung

1.1 Forschung in der Bundesverwaltung

Die Bundesverwaltung initiiert und unterstützt wissenschaftliche Forschung, deren Resultate sie zur Erfüllung ihrer Aufgaben benötigt. Diese im öffentlichen Interesse erbrachte Forschung wird als Ressortforschung bezeichnet. Dazu gehören wissenschaftliche Grundlagen für die Politikentwicklung und -ausgestaltung in den verschiedenen Politikbereichen, für Vollzugsarbeiten im Rahmen der gesetzlichen Vorgaben, für legislative Arbeiten oder für die Beantwortung und Umsetzung von parlamentarischen Vorstössen. Die Forschung der Bundesverwaltung kann praktisch alle Ausprägungen von wissenschaftlicher Forschung umfassen, namentlich von der Grundlagenforschung über die anwendungsorientierte Forschung bis hin zur Entwicklung von Pilot- und Demonstrationsanlagen. Die Forschung der Bundesverwaltung richtet sich nach klaren gesetzlichen Grundlagen. Neben der Abstützung auf Art. 64 der Bundesverfassung (SR 101) ist das Forschungs- und Innovationsförderungsgesetz FIFG (SR 420.1) das Rahmengesetz für die Forschung der Bundesverwaltung. Die Hauptverantwortung für die Forschung der Bundesverwaltung liegt bei den einzelnen Departementen und Bundesstellen. Die übergeordnete Koordination der Forschung der Bundesverwaltung wird über einen permanenten interdepartementalen Koordinationsausschuss sichergestellt. Im Hinblick auf die BFI-Periode 2025–2028 wurde ein gemeinsames Dokument der Bundesstellen mit einem Überblick über die Forschung der Bundesverwaltung sowie die grundlegenden künftigen Herausforderungen und zentralen Handlungsfelder erarbeitet. Die Mehrjahresprogramme werden für jeden der elf durch den Bundesrat bestimmten Politikbereiche in Form von ressortübergreifenden Forschungskonzepten ausgearbeitet. Die Forschung der armasuisse fällt dabei unter den Politikbereich der Sicherheits- und Friedenspolitik.

1.2 Überblick Sicherheits- und Friedenspolitik

Grundlagen und Ziele der Schweizer Sicherheits- und Friedenspolitik

Die Schweizerische Eidgenossenschaft schützt gemäss Bundesverfassung die Freiheit und Rechte des Volkes und wahrt die Unabhängigkeit und Sicherheit des Landes. Sie setzt sich zudem für die Wohlfahrt des Landes ein, trägt zur Linderung von Not und Armut in der Welt bei und fördert die Achtung der Menschenrechte und der Demokratie für ein friedliches Zusammenleben der Völker. Der Politikbereich Sicherheits- und Friedenspolitik umfasst im Rahmen der Ressortforschung des Bundes die Unterstützung der politischen Umsetzung von Sicherheits- und Friedensaspekten der Schweiz. Zur Sicherstellung dieser Verfassungsaufträge verfolgt die Schweiz einen integrierten und inklusiven sicherheits- und friedenspolitischen Ansatz.

Im Rahmen der Sicherheitspolitik wird das Ziel verfolgt, die Handlungsfähigkeit, Selbstbestimmung und Integrität der Schweiz und ihrer Bevölkerung zu gewährleisten, ihre Lebensgrundlagen gegen direkte und indirekte Bedrohungen und Gefahren zu schützen sowie einen Beitrag zu Stabilität und Frieden jenseits der nationalen Grenzen zu leisten. Um die sicherheitspolitischen Ziele zu verfolgen, verfügt die Schweiz über verschiedene Politikbereiche und Instrumente, die koordiniert eingesetzt werden. Es sind dies die Politikbereiche Aussen- und Wirtschaftspolitik sowie die Instrumente Armee, Bevölkerungsschutz, Nachrichtendienst, Polizei, Zollverwaltung und Zivildienst.
Das Ziel der Friedenspolitik ist es, Gewaltkonflikte zu verhüten, zu entschärfen oder zu lösen, Menschenrechte zu stärken und demokratische Prozesse zu fördern. Dies geschieht auf politisch-diplomatischem und operationellem Weg durch Vertrauensbildung, Vermittlung und friedensbildende Aktivitäten nach Beendigung von gewaltsamen Auseinandersetzungen. Ausserdem wird das humanitäre Völkerrecht gefördert sowie die politischen, wirtschaftlichen, sozialen und kulturellen Rechte von Personen oder Personengruppen gestärkt.

Sicherheitspolitische Lage und Konsequenzen auf die Sicherheits- und Friedenspolitik

Das sicherheits- und friedenspolitische Umfeld der Schweiz hat sich in den letzten Jahren grundlegend verändert. Es steht im Zeichen einer zunehmenden Konkurrenz der Grossmächte und staatlichem Handeln im Eigeninteresse. Die Infragestellung von internationalen Normen und die zahlreichen Krisen haben mittel- und langfristig einen direkten Einfluss auf die Sicherheit der Schweiz. Die Handlungsfähigkeit internationaler Sicherheitsorganisationen, wie der UNO oder OSZE, nimmt ab. Herausforderungen in den Bereichen Sicherheit, Umwelt oder Gesundheit erfordern eine abgestimmte Reaktion, die über das Handeln ei-

nes einzelnen Landes hinausgeht. Die Schweiz hat daher ein grosses Interesse daran, sich für die Stärkung und Aufrechterhaltung der Regeln des Völkerrechts und der Menschenrechte einzusetzen. Das internationale und humanitäre Engagement der Schweiz wird von der Schweizer Bevölkerung weiterhin stark unterstützt.

Vor diesem Hintergrund ergeben sich Konsequenzen für die Schweizer Bevölkerung, welche aus verschiedenen, gegenseitig abhängigen, teilweise verstärkenden Entwicklungen resultieren. Wie der Krieg in der Ukraine zeigt, kann ein bewaffneter Konflikt mit allen Konsequenzen auf Europa und die Schweiz relativ rasch auf verschiedenen Ebenen wie Versorgung, Wirtschaft, Migration und Diplomatie spürbar werden. Menschenrechte und Rechtsstaatlichkeit werden in solchen Konflikten fortwährend verletzt. Die Schweizer Diplomatie setzt sich für eine friedliche Lösung des Krieges ein, wobei jedoch auch das Schweizerische Verständnis der Neutralität stark unter Druck gerät. Durch die rasche Verbreitung moderner Technologien erhöhen sich die Gefahr des Missbrauchs von Technologien wie Drohnen, künstliche Intelligenz und Cyberwaffen und das Risiko der Weitergabe von Massenvernichtungswaffen. Zudem ist festzustellen, dass vermehrt mit dem Einsatz von Atomwaffen gedroht, Anschuldigungen zu biologischen Waffenprogrammen erhoben und staatliche Operationen mit ABC-Agenzien gegen Oppositionelle verübt werden. Die gesellschaftliche Polarisierung bildet einen Nährboden für gewalttätigen Extremismus und Terrorismus. Zudem gibt es eine Zunahme von klimabedingten Umweltkatastrophen, die oftmals in Krisen oder gar bewaffneten Konflikten münden. Dies ist eine Ursache vermehrt auftretender Migrationsbewegungen, welche die humanitäre Hilfe der Schweiz auch in Zukunft in Anspruch nehmen wird.

1.3 Forschung für die Sicherheits- und Friedenspolitik

Koordination im Rahmen der Ressortforschung

In der Ressortforschung des Bundes werden die Forschungstätigkeiten im Bereich Sicherheits- und Friedenspolitik koordiniert und abgestimmt. Daran beteiligt sind das Bundesamt für Bevölkerungsschutz (BABS) und das Bundesamt für Rüstung (armasuisse) aus dem VBS sowie die Abteilungen Internationale Sicherheit (AIS) sowie Frieden und Menschenrechte (AFM) aus dem Eidgenössisches Departement für auswärtige Angelegenheiten (EDA).

Die vorliegenden Forschungskonzepte der armasuisse und des BABS legen strategische Leitlinien fest und definieren aufeinander abgestimmte Forschungsschwerpunkte und Themenfelder für einen Zeitraum von vier Jahren. Dabei wird die Entwicklung des Umfelds auch innerhalb der Gültigkeitsperiode stets berücksichtigt, um allenfalls die inhaltliche Ausrichtung anpassen zu können. Die Ausrichtung der Aktivitäten im Rahmen der Ressortforschung soll helfen, die Entwicklung in diesem Umfeld zu verstehen und zu antizipieren. So kann sichergestellt werden, dass wissenschaftliche Kompetenzen zeitgerecht als Grundlage für eine adäquate Aufgabenbewältigung im künftigen sicherheits- und friedenspolitischen Umfeld zur Verfügung stehen und damit die interne Beratung von Politik und Verwaltung gewährleistet ist.

Die Zielsetzungen der schweizerischen Sicherheits- und Friedenspolitik können nur durch eine sorgfältige Abstimmung der Instrumente auf aktuelle und absehbare Bedrohungen erreicht werden. Angesichts der Volatilität der sicherheitspolitischen Lage und der Verkettung von Bedrohungen und Gefahren ist die Zusammenarbeit zwischen den sicherheits- und friedenspolitisch relevanten Akteuren sicherzustellen. Dies erfordert die Beherrschung einer hohen Komplexität. Eine wirksame Ausrichtung der verschiedenen Instrumente kann nur dann gelingen, wenn ein flexibler Ansatz gewählt wird. Es ist entscheidend, dass die Aufgabenbereiche der verschiedenen sicherheitspolitischen Akteure klar geregelt und aufeinander abgestimmt sind. Dazu sind fundierte Kenntnisse der Schnittstellen und erzielbaren Wirkungen im Kontext des jeweiligen Umfelds notwendig. Durch die Ressortforschung des Bundes wird im Rahmen der Sicherheits- und Friedenspolitik nicht nur die bundesinterne Koordination der Forschungsaktivitäten sichergestellt, sondern auch die Beauftragung des Zentrums für Security Studies (CSS) der Eidgenössischen Technischen Hochschule in Zürich (ETHZ). Das CSS konzentriert sich primär auf Forschung in sozialwissenschaftlichen Bereichen wie Politikwissenschaft, Geschichte, Management, Führung und Ökonomie. Die inhaltliche Koordination und Zusammenarbeit wird durch den Beirat VBS-CSS, in welchem das Generalsekretariat des VBS, die Militärakademie (MILAK), das BABS, die armasuisse und das CSS beteiligt sind, und durch den Beirat EDA-CSS, in welchem die AIS, AFM, Policy Planning und die Division for Digitalisation vertreten sind, sichergestellt.

Während das EDA seine Forschung auf internationale Friedensförderung, Mediation und Fazilitation

konzentriert, fokussiert das BABS auf Rüstungskontrolle, den Schutz kritischer Infrastrukturen und die Förderung der gesellschaftlichen Resilienz bei atomaren, biologischen und chemischen Ereignissen. Die armasuisse zeigt einerseits die Konsequenzen technologischer Entwicklungen auf die Sicherheitslandschaft der Schweiz auf und unterstützt andererseits dank Forschung den technisch-wissenschaftlichen Kompetenzaufbau der militärischen Gesamtplanung und des Rüstungsablaufs.

Gemeinsame Handlungsfelder in der Sicherheits- und Friedenspolitik

Vor dem Hintergrund der aktuellen sicherheits- und friedenspolitischen Entwicklungen sind in der gemeinsamen Ressortforschung vier Handlungs- und Forschungsfelder relevant (Abbildung 2).

Nachhaltigkeit
Im sicherheitspolitischen Kontext wird der Begriff Nachhaltigkeit sehr breit verstanden. Klimawandel, die weltpolitische Lage und aktuelle Konflikte geben Anlass, bisherige Vorgehensweisen zur Gewährleistung von Sicherheit und Frieden zu überdenken. So bewirkt der Klimawandel extreme Wetterereignisse und fördert dadurch Ressourcenknappheit, Armut, Konflikte und Migration in Schwellen- und Entwicklungsländern. Die Schweiz versucht durch eine ganzheitliche und inklusive Friedenspolitik demokratische und rechtsstaatliche Strukturen vor Ort zu fördern. Auf nationaler Ebene zeigen sich die Auswirkungen des Klimawandels durch ein erhöhtes Risiko von Naturgefahren, Trockenperioden und einer Reduktion der Artenvielfalt. Deshalb sind die Klimaziele des Bundes auch für die Instrumente der Sicherheits- und Friedenspolitik umzusetzen. Zudem ist der nachhaltige Umgang mit Ressourcen sicherzustellen. Für die Schweiz als neutraler Kleinstaat ist es zentral, internationale Organisationen und damit eine regelbasierte Weltordnung als Gegengewicht zur vermehrt feststellbaren Machtpolitik zu fördern. Der Ukraine-Krieg hat gezeigt, dass sich die Schweiz auf die vielfältigen Konsequenzen solcher Konflikte vorbereiten muss und die sicherheitspolitischen Instrumente, insbesondere die Armee, auch für den Verteidigungsfall vorzubereiten sind.

Neue Technologien
Der technologische Fortschritt des letzten Jahrzehnts war enorm und eine Verlangsamung ist nicht absehbar. Traditionelle Geschäftsmodelle wurden verdrängt und neue internationale Grosskonzerne haben eine marktdominierende Rolle eingenommen. Durch ihre Ausrichtung auf möglichst grosse Marktpotenziale sind moderne Technologien breit verfügbar, obwohl feststellbar ist, dass sich sowohl eine amerikanisch als auch eine chinesisch geprägte Wirtschaftssphäre zu etablieren scheinen. Auch ihre Auswirkungen auf die Gesellschaft sind offensichtlich. Im Rahmen der Sicherheits- und Friedenspolitik ist den Auswirkungen des zunehmend komplexen, interdisziplinären technologischen Fortschritts und der Konvergenz der Disziplinen verstärkt Aufmerksamkeit zu schenken. Um der Bedrohung durch Proliferation, Gefahr des Missbrauchs und Nutzung durch gegnerische Akteure fundiert entgegentreten zu können, ist ein grundlegendes Verständnis der technologischen Entwicklung und ihrer Konsequenzen für staatliches Handeln notwendig. Dies betrifft zum Beispiel chemische, biologische und nukleare Waffen, autonome Systeme, künstliche Intelligenz und Fortschritte in der Nutzung des Weltraums.

Resilienz
Zur künftigen Bewältigung internationaler Krisen muss die Schweiz ihre Fähigkeit zur Antizipation und zur Resilienz stärken. Das Ziel ist es, Abhängigkeiten gegenüber Volatilitäten in internationalen Handelsketten zu reduzieren und die Versorgungssicherheit von kritischen, lebenswichtigen und sicherheitsrelevanten Gütern zu stärken. Dazu gehören die Energieversorgung, das Gesundheitswesen sowie sicherheitsrelevante technologische Kompetenzen und industrielle Kapazitäten, welche zur technologischen Souveränität der Schweiz beitragen. Auch der Schutz und die Regenerationsfähigkeit bei Katastrophen und Notlagen sollen verbessert werden. Dazu müssen natur-, technik- und gesellschaftsbedingte Gefahren antizipiert, Ereignissen vorgebeugt, Bevölkerung und Infrastrukturen geschützt und auch Mittel und Strukturen zur Bewältigung bereitgestellt werden. Des Weiteren muss die Schweiz zur Verhinderung von Terrorismus, gewalttätigem Extremismus und organisierter Kriminalität die Etablierung entsprechender Organisationen unterbinden. Dazu sollen der irreguläre Personen- und Warenverkehr an der Grenze und die negativen Begleiterscheinungen der Migration bekämpft werden.

Digitalisierung
Prozesse von Behörden und Organisationen im sicherheitspolitischen Kontext werden vermehrt digitalisiert, um effizienter, schneller und transparenter erbracht werden zu können. Zudem sollen die digitalen Daten durch künstliche Intelligenz genutzt werden,

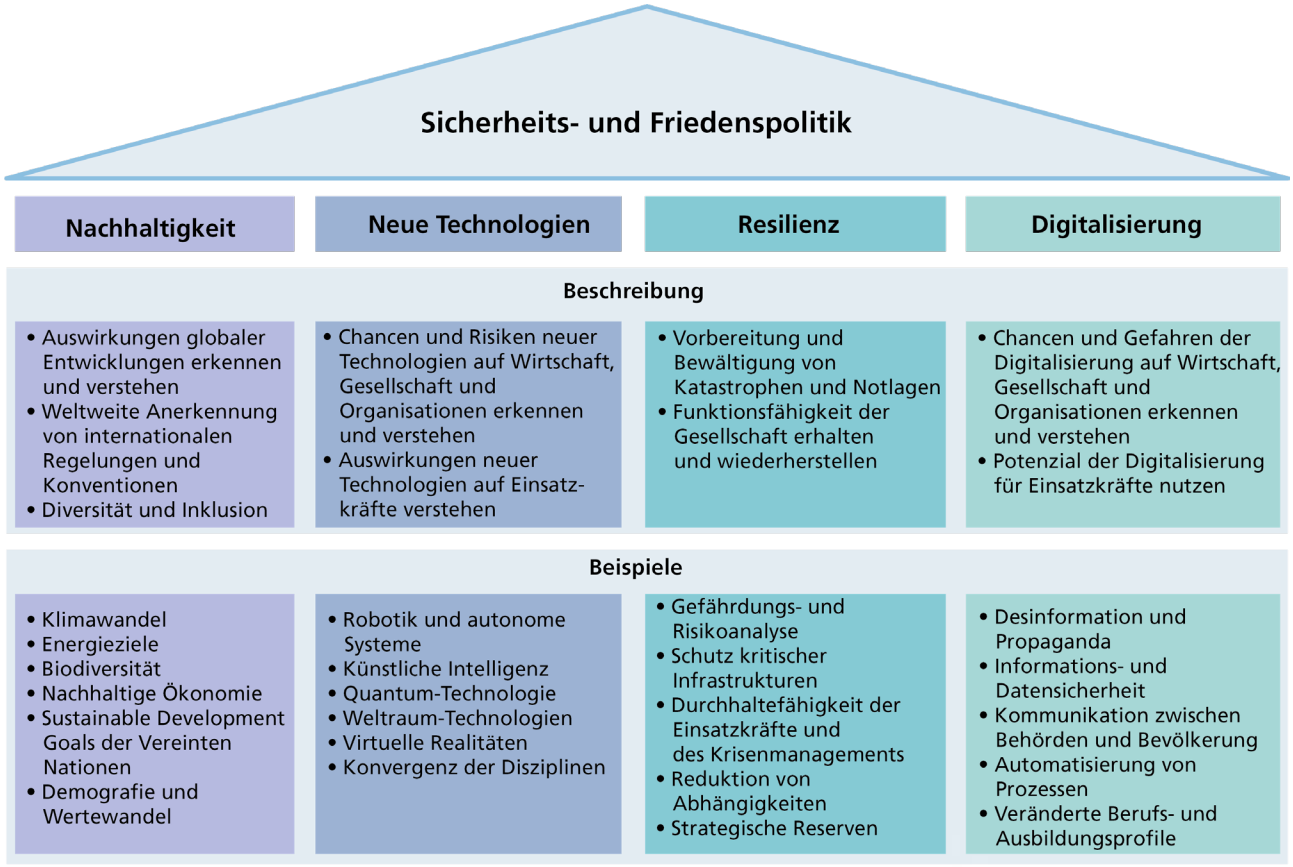


Abbildung 2: Handlungs- und Forschungsfelder der Sicherheits- und Friedenspolitik. Einordnung der gemeinsamen Rahmenbedingungen und deren sicherheits- und friedenspolitischen Auswirkungen auf die schweizerische Bevölkerung, Gesellschaft und Wirtschaft.

um einen höheren Grad an Automatisierung zu erreichen. Digitale Daten und künstliche Intelligenz ermöglichen die Nutzung offener Datenquellen zur Informationsgewinnung und umgekehrt können bundeseigene Daten dem Nutzer zur Verfügung gestellt werden. Um die Chancen der Digitalisierung vollauf zu nutzen, muss die Schweiz den Schutz vor Cyberrisiken weiter erhöhen. Dazu muss sie die sicherheitsrelevanten Entwicklungen im Cyberbereich antizipieren und die nötigen Mittel haben, um Cybervorfälle rasch zu erkennen und durch aktive Gegenmassnahmen einzudämmen. Freie Meinungsbildung und unverfälschte Informationen sind die Grundlage jedes demokratischen Meinungsbildungsprozesses. Der Schutz des Staates und seiner Institutionen, der Wirtschaft und der Bevölkerung vor Cyberbedrohungen, Beeinflussungsaktivitäten, Spionage und Androhung bzw. Ausübung von Gewalt ist sicherzustellen. Dazu muss eine aktive faktenbasierte Kommunikation gewährleistet, aber auch Desinformation und Propaganda identifiziert und notfalls Schutzmassnahmen ergriffen werden.

2 Wissenschaft und Forschung im VBS

Die Umsetzung der sicherheitspolitischen Ziele erfolgt in der Schweiz durch einen integrativen und abgestimmten Ansatz verschiedener Instrumente und operativer Elemente. Das VBS ist zuständig für die Armee, den Bevölkerungsschutz und den Nachrichtendienst. Mit der Neuansiedlung des Bundesamts für Cybersicherheit ist ein weiteres Element dazu gekommen. Während sich das Forschungskonzept des BABS primär am Bedarf des Bevölkerungsschutzes ausrichtet, fokussiert der langfristige Forschungsplan (LFP) von armasuisse Wissenschaft und Technologie (W+T) auf den Bedarf der Schweizer Armee, des Nachrichtendienstes, der Beschaffungsstellen von armasuisse und des Bundesamts für Cybersicherheit. Durch die Forschung von armasuisse werden die wissenschaftlichen Grundlagen zur Beratung und Unterstützung der Bedarfsträger sichergestellt.

2.1 Internationales Umfeld

Generell wird beobachtet, dass die Entwicklung von Technologien, welche für Streitkräfte relevant sind, heute vielfach durch zivile Märkte getrieben wird. Dabei ist die Zeit bis zur Markteinführung von neuen Produkten für viele Unternehmen ein wichtiger Erfolgsfaktor, was die Geschwindigkeit von technologischen Entwicklungen enorm beschleunigt. In Wirtschaft und Gesellschaft ist die Digitalisierung bereits weit fortgeschritten. Die meisten Armeen hinken dieser Entwicklung jedoch hinterher. Die Gründe dafür sind vielfältig. Einerseits mangelte es im militärischen Umfeld lange Zeit an einer Innovationskultur, um den digitalen Wandel voranzutreiben. Andererseits führte die Fokussierung von Technologiefirmen auf zivile Märkte oftmals dazu, dass militärisch notwendige Anforderungen hinsichtlich eines sicheren und robusten Einsatzes aus Kosten- und Zeitgründen nicht implementiert wurden. Somit mussten Technologien für den Einsatz im militärischen Kontext teuren und zeitintensiven Nachentwicklungen unterzogen werden. Die staatliche Beeinflussung der Entwicklung militärischer Technologien erzeugt für militärisch gehärtete Produkte oft Oligopole und Monopole, mit all ihren Nachteilen hinsichtlich der zeitlichen Verfügbarkeit neuster Technologien und deren Preis. Umgekehrt hat der Ukraine-Konflikt gezeigt, dass Low-Cost-Mittel aus der zivilen Welt in Rekordzeit effizient für militärische Zwecke modifiziert und zweckentfremdet werden konnten. Deshalb ist es notwendig die Entwicklung von militärischen und zivilen Technologien zu beobachten, deren Anwendungsmöglichkeiten sowohl für reguläre Streitkräfte als auch für hybrid operierende Einheiten abzuschätzen und so Chancen und Gefahren für die eigenen Streitkräfte rechtzeitig zu erkennen. Eine solide Kompetenz in modernen Technologien aus dem zivilen Umfeld eröffnet ein grosses Innovationspotenzial für Anwendungen im militärischen Kontext.

Für die Schweiz als Nation mit einem vergleichsweise geringen Forschungsbudget im Bereich der sicherheitsrelevanten Technologien ist es unumgänglich, dass Lücken bewusst in Kauf genommen werden müssen. Dies gilt sowohl für die Themenvielfalt als auch für deren Bearbeitungstiefe. Der Vergleich mit den Forschungsthemen anderer westlicher Länder und der Abgleich mit den nachgefragten Kompetenzen im Rahmen der Beauftragung durch Armee und armasuisse zeigt, dass die thematische Ausrichtung der Forschung sowohl weitgehend dem Bedarf als auch den bekannten internationalen Technologietrends entspricht. Die Einbindung von Experten in nationale und internationale Netzwerke sichert sowohl die Qualität des Kompetenzaufbaus als auch den Wissenstransfer aus dem Netzwerk ins VBS.

2.2 Kontext der Forschung im VBS

Die Schweizer Armee verfolgt den für die militärische Gesamtplanung den Ansatz einer fähigkeitsorientierten Streitkräfteentwicklung (FOSKE, Abbildung 3). Der grosse FOSKE-Zyklus, welcher eine Legislatur überspannt, ermöglicht es, (theoretisch) eine neue Armee zu designen, oder auch das bestehende Armeemodell gründlich zu überprüfen. Der grosse Zyklus ist auf einen mittel- bis langfristigen Zeitraum von 8 bis 12 Jahren ausgerichtet. Ausgangspunkt ist dabei die Antizipation, die den militärischen, technologischen, politischen und gesellschaftlichen Kontext, inklusive der Planszenarien betrachtet. Auf dieser Basis werden militärstrategische Überlegungen erarbeitet, darunter die Priorisierung der operationellen Fähigkeiten bzw. der Fähigkeitsbereiche. In einem nächsten Schritt werden Referenzgrundlagen erarbeitet, unter anderem Annahmen zur konkreten Bedrohung. Die Referenzgrundlagen erlauben es, die Militärdoktrin inklusive der operationellen Fähigkeiten (Soll) zu formulieren. Die Doktrin bildet die Basis für die Ausarbeitung von Operationskonzepten, d.h. der konkreten Art und Weise, wie die Armee ihre Aufgaben in den Planszenarien erfüllen soll. Dies bildet die Grundlage, um die

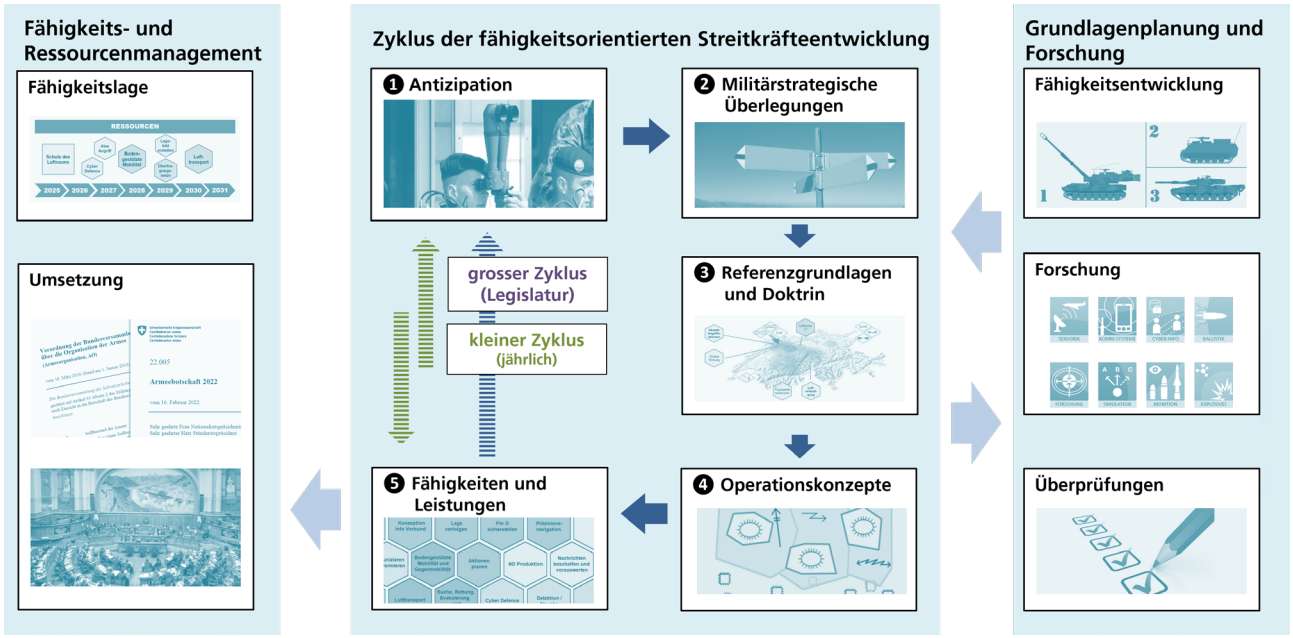


Abbildung 3: Prozess der fähigkeitsorientierten Streitkräfteentwicklung (FOSKE).

benötigten Fähigkeiten und Leistungen sowie das Armeedesign beschreiben zu können. Im kleinen FOSKE-Zyklus werden die im laufenden Zyklus erarbeiteten Produkte – im Sinne eines Updates – jährlich überprüft, insbesondere die Planszenarien sowie die Fähigkeiten und Leistungen.

Das zyklische Vorgehen wird durch laufende Arbeiten unterstützt. Das Fähigkeits- und Ressourcenmanagement beinhaltet einerseits die aktuelle Fähigkeitslage und andererseits die laufende Umsetzung und die Fähigkeitsnutzung. Im Rahmen der Grundlagenplanung und Forschung wird gleichsam eine Landschaft konzeptioneller Überlegungen bewirtschaftet. Diese Überlegungen können einerseits in den Zyklus einfliessen und andererseits als Grundlage für die Umsetzung und für das Fähigkeits- und Ressourcenmanagement dienen. Die Forschung, die Erarbeitung der Grundlagenpapiere und die Überprüfung und Aktualisierung der erstellten Beiträge wird jeweils über mehrere Jahre geplant. Durch die laufende Fähigkeitsplanung wird sichergestellt, dass aktuelle Grundlagen zeitgerecht bereitstehen, bevor fähigkeitsrelevante Grosssysteme ausser Dienst gestellt werden.

In Ergänzung zu diesem Prozess der militärischen Gesamtplanung hat die Armee das Innovationssystem Verteidigung lanciert, bei welchem es um die kurzfristige Umsetzung von innovativen Ideen geht, primär um die digitale Transformation der Streitkräfte und der Militärverwaltung zu fördern. Die Forschung von armasuisse erarbeitet vorausschauend Grundlagen, welche erforderlich sind, um sowohl den FOSKE- als auch die Innovationsprozesse der Armee mit den notwenigen technischwissenschaftlichen Kompetenzen unterstützen zu können.

Diese Aufgabe nimmt die armasuisse gemäss der Organisationsverordnung für das VBS (OV-VBS) wahr. Darin wird dem Kompetenzbereich W+T die Funktion eines Technologiezentrums zugewiesen, welches den Wissenschafts- und Technologiebedarf auch im Rahmen von Netzwerken und Kooperationen mit nationalen und internationalen Partnern abdeckt. Laut der Geschäftsordnung des VBS (GO-VBS) erfolgt die Erschliessung der notwendigen Technologiekompetenzen durch angewandte Forschungstätigkeiten. Auch in den Grundsätzen des Bundesrates für die Rüstungspolitik des VBS wird auf das Instrument der angewandten Forschung, auf internationale Kooperationen und Innovationsförderung verwiesen, dies insbesondere mit dem Ziel einer Stärkung der sicherheitsrelevanten Technologie- und Industriebasis (STIB) in der Schweiz und der Sicherstellung von wesentlichen wissenschaftlich-technischen Kompetenzen gemäss dem Bedarf der Armee. Um die Abhängigkeit vom Ausland zu beschränken, ist beabsichtigt, Kompetenzen in sicherheitsrelevanten Schwerpunkttechnologien wie den Sensor, Informations- und Kommunikationstechnologien nach Möglichkeit mit Schweizer Partnern aufzubauen und zu sichern.

Die Zusammenarbeit zwischen den Departementsbereichen Verteidigung und armasuisse ist mittels einer Zusammenarbeitsvereinbarung (ZUVA) geregelt. Darin ist unter anderem auch die Rolle des Forschungsverantwortlichen definiert, welcher sowohl für die strategische Ausrichtung und Planung, als auch für die operative Umsetzung der Forschung zugunsten von armasuisse und der Armee zuständig ist. Der Wissenstransfer aus der Forschung in die militärische Gesamtplanung und in die Beschaffungsprozesse ist in ZUVA durch die Funktion des Technologieverantwortlichen gewährleistet. Damit soll in einer frühen Planungsphase sichergestellt werden, dass Technologieentwicklungen in Beschaffungsprojekten angemessen berücksichtigt werden. Dabei ist zu berücksichtigen, dass das Kompetenzzentrum für Militär- und Katastrophenmedizin der Armee selber angewandte Forschung betreibt, um den Wissenstransfer in die Aus-, Weiter- und Fortbildung auf einer wissenschaftlich fundierten Grundlage sicherzustellen. Dazu soll ein virtueller Campus aufgebaut werden, der auf der Basis einer digitalen Forschungs- und Wissensplattform die Vernetzung mit der Miliz und dem universitären Umfeld fördert.

Um den künftigen Innovationsbedarf des VBS genügend zu adressieren, wurde armasuisse W+T durch die Departementschefin beauftragt Innovationsräume aufzubauen. Damit sollen für das ganze VBS die organisatorischen, methodischen und fachlichen Voraussetzungen geschaffen werden, um technologiegetriebene Innovationen zu fördern und eine offene Innovationskultur zu schaffen. Die Innovationsräume VBS unterstützen das Innovationssystem der Verteidigung, indem gemäss dem Bedarf der Armee technisch-wissenschaftliche Kompetenzen, das Expertennetzwerk, Methoden und Prozesse zur Erarbeitung von Innovationslösungen bereitgestellt werden. Weitere Umsetzungspartner für die Innovationsvorhaben der Gruppe Verteidigung sind die RUAG Innovation Organisation und die Swiss Innovation Forces.

2.3 Positionierung der Forschung im VBS

Die Forschung der armasuisse verfolgt das Ziel, diejenigen technisch-wissenschaftlichen Kompetenzen bereitzustellen, welche benötigt werden, um die Entscheidungsträger der Armee in Technologiefragen zu beraten, die Expertise- und Erprobungsfähigkeit entlang des Rüstungsablaufs sicherzustellen sowie Technologieentwicklungen und deren Auswirkungen auf die operationellen Fähigkeiten der Armee frühzeitig aufzuzeigen und zu bewerten. Um Chancen und Gefahren in der Anwendung neuer Technologien beurteilen zu können, soll deren Potenzial mit Hilfe von Demonstratoren aufgezeigt und damit die Brücke zum Innovationssystem V und den Innovationsräumen des VBS geschlagen werden. So zielt man darauf ab, den Zeitbedarf von der Forschung bis zum operativen Einsatz einer Technologie zu verkürzen und so die notwendige Flexibilität der militärischen Einsatzkräfte in einem volatilen Umfeld sicherstellen zu können. Aufgrund dieser Zielsetzungen orientiert sich die Forschung von armasuisse an den technologischen Megatrends, der militärischen Gesamtplanung und dem

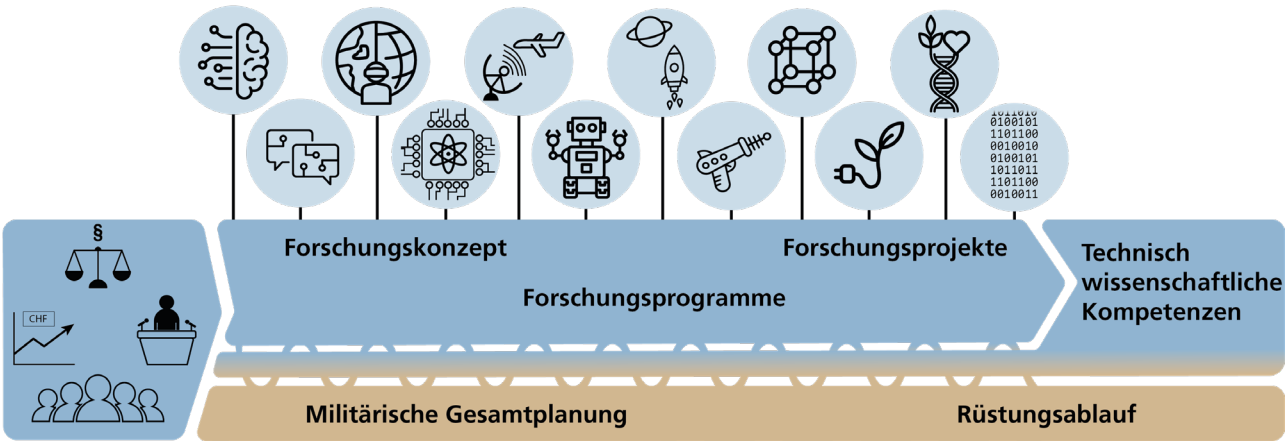


Abbildung 4: Die Forschung der armasuisse wird durch verschiedene Faktoren beeinflusst. Zu den äusseren Faktoren gehören Politik, Wirtschaft, Gesellschaft, Recht und die technologischen Megatrends. Die militärische Gesamtplanung und der Rüstungsablauf beeinflussen einerseits die Ausrichtung der Forschung, andererseits fliessen aber auch Erkenntnisse aus der Forschung in die militärische Gesamtplanung und den Rüstungsablauf. Das Ziel der Forschung ist der Aufbau von technisch-wissenschaftlichen Kompetenzen.

Rüstungsablauf sowie an äusseren Faktoren wie der Politik, Wirtschaft, Gesellschaft und dem rechtlichen Rahmen (Abbildung 4).

Um die wichtigsten technologischen Megatrends (Abbildung 5), welche für die Sicherheitspolitik der Schweiz relevant sind, zu identifizierten, müssen weltweit vorangetriebene Technologieentwicklungen in der Breite beobachtet und kontinuierlich hinsichtlich ihres Anwendungspotenzials bewertet werden. Ein solcher Ansatz ermöglicht neu aufkommende Bedrohungen für eine Gesellschaft rechtzeitig zu erkennen und Massnahmen abzuleiten, um diesen zu begegnen, aber auch Opportunitäten für künftige Einsatzszenare zu nutzen. Dabei ist besonders zu beachten, dass die Kombination technologischer Entwicklungen zu disruptiven Effekten führen kann, die Gesellschaft, Geschäftsmodelle, aber auch Vorgehensweisen von Akteuren im sicherheitspolitischen Umfeld fundamental verändern können. Die Identifikation und Analyse technologischer Megatrends sind somit Instrumente, um technologiegetriebene Veränderungen im sicherheitspolitischen Umfeld frühzeitig zu erkennen und damit den Zyklus der fähigkeitsorientierten Streitkräfteentwicklung zu unterstützen.

Für die Themensetzung der Forschung von armasuisse ist auch der FOSKE-Prozess eine wichtige Grundlage. Ausgehend vom künftigen Fähigkeitsbedarf der Armee und der davon abgeleiteten Umsetzungsplanung werden diejenigen Technologiekompetenzen aufgebaut, welche benötigt werden, um die technisch-wissenschaftliche Expertisefähigkeit zugunsten der Armee sicherzustellen. Diese erstreckt sich von der Mitarbeit in der Grundlagenplanung bis hin zur Wahrnehmung der Rolle des Technologie- oder Erprobungsverantwortlichen in Beschaffungsprojekten. Dabei geht es sowohl um die Wahl geeigneter Technologien für die Sicherstellung von operationellen Fähigkeiten als auch um die Planung der Beendigung und Ablösung von Technologien entsprechend ihren Lebenszyklen. Dazu sind vertiefte Technologiekompetenzen und Anwendungserfahrung notwendig. Beides kann mit Hilfe angewandter Forschung und Innovation aufgebaut werden.

armasuisse W+T nimmt in der Forschungs- und Innovationslandschaft (Abbildung 6) eine Drehscheibenfunktion wahr, welche die Technologiekompetenzen zugunsten der Armee koordiniert und bündelt. Dazu ist ein umfassendes Netzwerk verschiedener Akteure notwendig, welche sich aus dem öffentlichen und privaten Forschungsumfeld und aus der technologieorientierten Start-up- und Unternehmer-Szene zusammensetzt. Die Abstimmung mit den nationalen Forschungs- und Innovationsförderungsinstrumenten hilft thematische Überlappungen zu identifizieren und vorhandene Kompetenzen nach dem Add-on-Prinzip für die Forschung, aber auch für die Innovationsvorhaben des VBS nutzbar zu machen. Schliesslich hilft die Zusammenarbeit mit Forschungs- und Innovationsinstitutionen der North Atlantic Treaty Organisation (NATO) und der Europäischen Verteidigungsagentur (EVA) Technologiekompetenzen und Erfahrungen im Kontext eines militärischen Umfelds zu erarbeiten und auszutauschen.

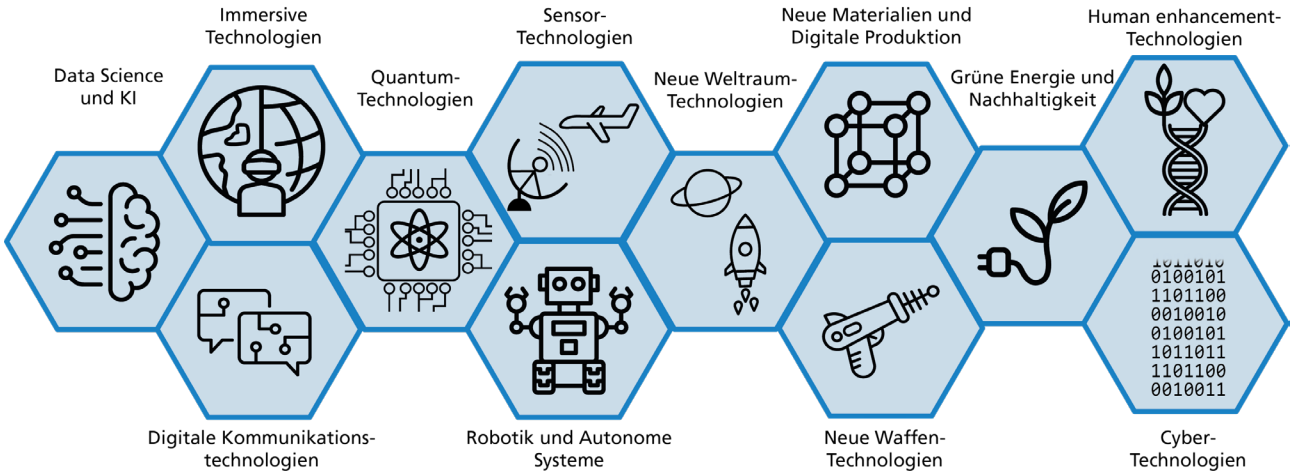


Abbildung 5: Identifizierte technologische Megatrends mit Bedeutung für Sicherheitskräfte.

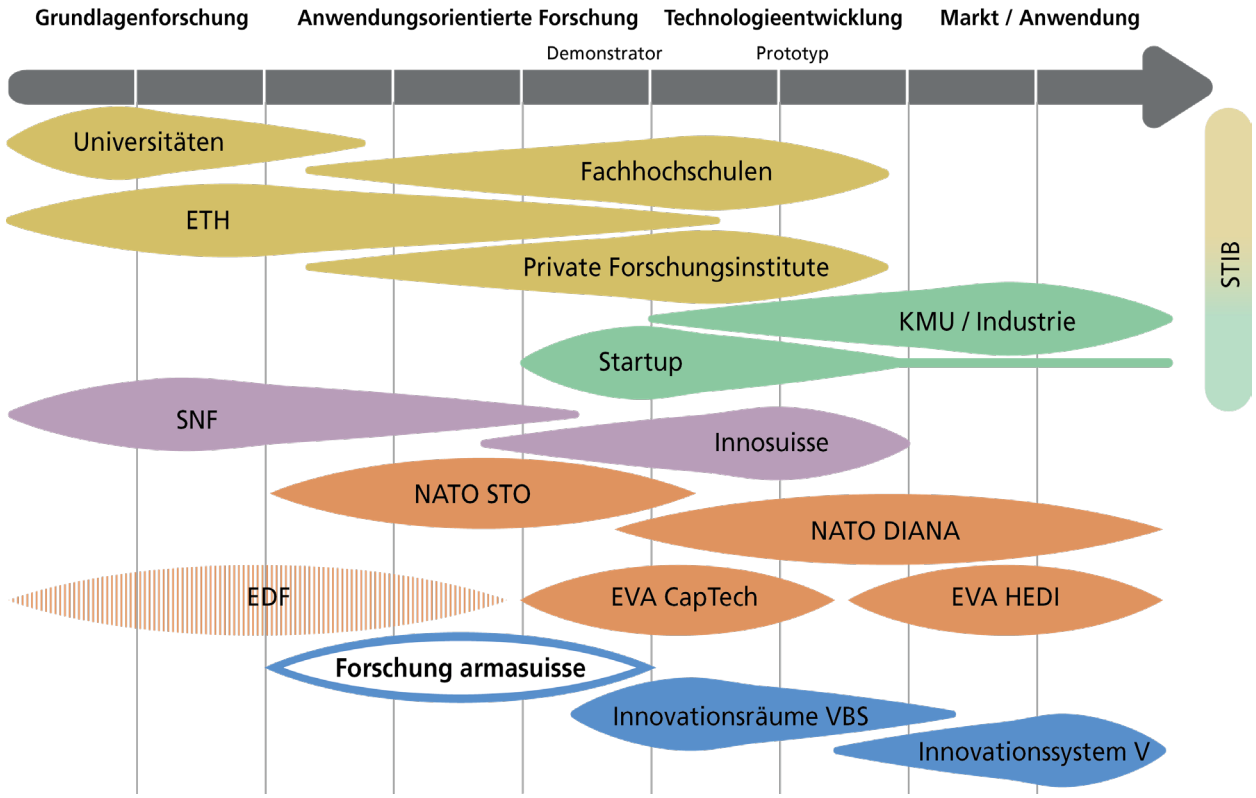


Abbildung 6: Einordnung der anwendungsorientierten Forschung der armasuisse in der Forschungs- und Innovationslandschaft des VBS. Zur sicherheitsrelevanten Technologie- und Industriebasis (STIB) gehören Forschungseinrichtungen und Unternehmen, die in der Schweiz über Kompetenzen, Fähigkeiten und Kapazitäten im sicherheits- und wehrtechnischen Bereich verfügen. Relevante Förderinstrumente sind der Schweizerische Nationalfonds (SNF) im Forschungs- und Innosuisse im Innovationsbereich. International kann sich die Schweiz an Projekten der NATO Science and Technology Organization (STO) und des NATO Defence Innovation Accelerator for the North Atlantic (DIANA) beteiligen. Zudem ist eine Teilnahme in den Capability Technology Groups (CapTechs) der Europäischen Verteidigungsagentur (EVA) und im Hub for EU Defence Innovation (HEDI) möglich. Von Projekten des European Defence Fund (EDF) ist die Schweiz ausgeschlossen. Im VBS werden die Innovationsräume VBS sowie das Innovationssystem der Verteidigung durch die Forschung unterstützt.

2.4 Strategische Umsetzungsgrundsätze

Für die Auswahl der Forschungsprioritäten und die operative Umsetzung der Forschungsaktivitäten im Rahmen des LFP 2025-2028 bilden sechs strategische Umsetzungsgrundsätze die Grundlage.

Anwenderorientierung

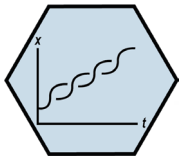
Die Forschung von armasuisse ist auf den Anwender fokussiert, insbesondere für die Auftragserfüllung der Departementsbereiche Verteidigung und armasuisse. Vor diesem Hintergrund sind die Forschungsschwerpunkte auf die operationellen Fähigkeiten und ihre Umsetzung im Rahmen der fähigkeitsorientierten Streitkräfteentwicklung ausgerichtet. Darüber hinaus muss die Forschung auf Effektivität und Effizienz ausgerichtet sein. Die Forschungsergebnisse müssen für die verschiedenen Aufgaben der Armee und ihrer unterstützenden Organisationen wirkungsvoll genutzt werden können. Die Forschung konzentriert sich auf die notwendigen technisch-wissenschaftliche Kompetenzen, um aus technologischer Sicht Optionen zur Weiterentwicklung in den verschiedenen Fähigkeitsbereichen beurteilen zu können. Von gleich grosser Relevanz sind diese Kompetenzen anschliessend, um Umsetzungsmassnahmen, insbesondere die Rüstungsbeschaffung, begleiten zu können. Methodenkompetenzen im Bereich Modellierung und Simulationen unterstützen diese Tätigkeiten und zeigen den Nutzen und die Grenzen neuer Technologien im militärischen Umfeld auf. Somit dienen diese auch als Entscheidungsgrundlage für doktrinelle Überlegungen. Damit technologische Entwicklungen und die Bedürfnisse der Armee bestmöglich aufeinander ab-

gestimmt werden können, muss die Forschung anpassungsfähig sein. So kann sie sich an mögliche Veränderungen anpassen. Eine jährliche Bedarfsermittlung stellt sicher, dass jedes Jahr inhaltliche Anpassungen der Forschung vorgenommen werden können.

Technologiereifegrad

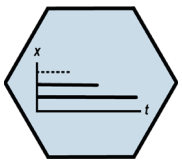
Die Forschung von armasuisse sichert die technisch-wissenschaftliche Kompetenz durch Aktivitäten wie Technologiefrüherkennung, thematische Programme und die Bereitstellung von Demonstratoren. In diesem Zusammenhang konzentriert sich die Forschung von armasuisse auf die Technologiereifegrade 3 (Nachweis der Funktionstüchtigkeit einer Technologie) bis 5 (Versuchsaufbau in Einsatzumgebung) gemäss dem Technology Readiness Level (TRL) Modell der NASA. Die Entwicklung von Prototypen (TRL 6) bis zum qualifizierten System mit Nachweis des erfolgreichen Einsatzes (TRL 9) ist jedoch nicht Gegenstand der Forschung von armasuisse und muss von der Armeeplanung und den Beschaffungsstellen im Rahmen des Rüstungsablaufs, über das Innovationssystem V oder die Innovationsräume VBS durchgeführt bzw. in Auftrag gegeben werden.

Technologie-Lebenszyklus



Der Lebenszyklus von Technologien kann mit dem Lebenszyklus von Produkten verglichen werden und wirkt sich direkt auf die strategischen Optionen aus. Eine Zukunftstechnologie kann sich zu einer Schlüsseltechnologie entwickeln, bevor sie zu einer Basistechnologie wird, die von neuen innovativen Technologien verdrängt werden kann. Im zivilen Bereich hat sich der Lebenszyklus von Technologien in den letzten Jahren stark beschleunigt. Im militärischen Bereich ist der Übergang von einer Technologie zur nächsten oftmals teurer. Weil Systeme oft lange in Betrieb sind, ist die Integration von neuen Technologien durch Subsysteme eine Herausforderung. Die Forschung von armasuisse konzentriert sich vor allem auf die Wachstums- und Reifephasen von Schlüsseltechnologien, da in diesen Phasen wirksame Fortschritte für den Einsatz in Rüstungsgütern zu erwarten sind. Dabei wird auch deren Integration in Legacy-Plattformen betrachtet. Die Kenntnis des Lebenszyklus von Technologien verringert das Risiko, dass Technologien zum falschen Zeitpunkt eingeführt werden und verhindert Fehlinvestitionen.

Mittel- bis langfristiger Zeithorizont

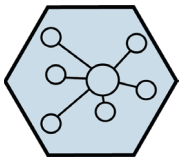


Die Forschung von armasuisse dient dem Aufbau und der Sicherung der technisch-wissenschaftlichen Kompetenzen, die für die Aufrechterhaltung der Expertise- und Beratungsfähigkeit im sicherheitspolitischen Kontext notwendig sind. Der Bedarf an diesen Fähigkeiten wird durch die fähigkeitsorientierte Streitkräfteentwicklung und die spezifischen Aufgaben der Armee bestimmt und kann die Bewertung technologischer Bedrohungen und alternativer Technologien umfassen. Die Interaktion zwischen bestehenden und zukünftigen Systemen der Armee ist ebenfalls wichtig, um Kompatibilität und Leistungsfähigkeit zu gewährleisten. Vor diesem Hintergrund sollen durch die Forschung technologische Trends identifiziert werden, die für die langfristige Sicherheit wichtig sind. Zudem sollen die Fortschritte von Technologien mit disruptivem Potenzial im zivilen und militärischen Bereich beobachtet werden. So werden Technologien, die sich nachhaltig auf die Fähigkeiten der Streitkräfte auswirken könnten, identifiziert und rechtzeitig Massnahmen ergriffen, um die Sicherheit zu gewährleisten.

Kompetenzen durch Kooperationen

Die Bereitstellung technisch-wissenschaftlicher Kompetenzen für die Instrumente der Sicherheitspolitik erfordert aufgrund der komplexer werdenden Aufgabenumsetzung und der wirtschaftlichen Rahmenbedingungen die Zusammenarbeit einer wachsenden Zahl von Akteuren. Hierzu wurden und werden langfristige Netzwerke mit Partnern aus der Wirtschaft, Hochschulen, anderen staatlichen Institutionen und internationalen Organisationen nicht nur aufgebaut, sondern auch weiterentwickelt. Dadurch soll die Nutzung vorhandener Kompetenzen optimiert und deren kontinuierliche Weiterentwicklung zu gewährleistet werden. Strategische Partnerschaften werden gefördert, um die Kontinuität der Kompetenzentwicklung zu gewährleisten und die Qualität der nationalen und internationalen Kooperationsprojekte sicherzustellen. Kooperationen ermöglichen den Zugang zu Schlüsseltechnologien, Einsatzerfahrungen und technischen Bedrohungsanalysen. Durch die bestehenden Kompetenzen der Kooperationspartner kann auf diesen aufgebaut werden, um Kosten zu senken und eine effiziente Nutzung der Ressourcen zu erreichen.

Multidisziplinäre Vernetzung



Die Forschungsergebnisse wirken sich direkt auf die operationellen Fähigkeiten der Armee und die Systemtechnologien aus. Armeesysteme enthalten heute eine grosse Zahl von Technologien, die aus verschiedenen Disziplinen stammen. Deshalb ist es wichtig, dass immer das Gesamtsystem betrachtet wird und die Disziplinen nicht im Silo agieren. Um dies zu erreichen werden übergreifende Forschungsthemen definiert, damit die Qualität und Leistung der Systeme sowie die Effizienz der Betreiber erheblich verbessert und somit die Gesamtkosten gesenkt werden können.

2.5 Gesetzlicher Auftrag und Grundlagen

Der Auftrag für die Forschung von armasuisse ergibt sich hauptsächlich aus dem Bundesgesetz über die Armee und die Militärverwaltung (Art. 109, Revision 2026), der Organisations-Verordnung für das VBS, der Rüstungspolitik des VBS, den Weisungen über die Zusammenarbeit der Departementsbereiche Verteidigung und armasuisse (ZUVA) und der Integrierten Aufgaben und Finanzplanung (IAFP) armasuisse 2024-2026. Die gesetzlichen Grundlagen zur Durchführung der Ressortforschung können aus dem Forschungs- und Innovationsförderungsgesetz (FIFG), sowie aus dessen Verordnung entnommen werden. Eine detaillierte Zusammenstellung relevanter Grundlagen, welche im Rahmen der Forschung von armasuisse beachtet werden müssen, kann aus dem Anhang 2 entnommen werden.

2.6 Rückblick auf Periode 2021-2024

Basierend auf dem Langfristigen Forschungsplan 2021-2024 wurden die Forschungsschwerpunkte «Technologie-Früherkennung», «Technologien für operationelle Fähigkeiten», «Technologieintegration für Demonstratoren» und «Innovation und Querschnittsthemen» systematisch bearbeitet und Erkenntnisse in Form von Expertisen und Beratungsleistungen zur Verfügung gestellt. Dies mit dem Ziel, die entsprechenden Stellen des VBS von der Planung bis zur Entsorgung der materiellen Ausrüstung in Technologiefragen technisch-wissenschaftlich kompetent zu unterstützen. Der Wissenstransfer aus der Forschung in die Planungsprozesse der Armee konnte dabei dank einer guten Zusammenarbeit mit dem Armeestab und weiteren Organisationseinheiten verbessert werden. Durch den etablierten Austausch mit Armeeplanung, Militärdoktrin und Truppe konnten auch die Forschungsprogramme mit den dazugehörigen Kompetenzfeldern laufend auf den Bedarf der Verteidigung ausgerichtet werden.

In der Periode 2021-2024 konnten die Schweizer Armee und weitere Behörden im Umgang mit der Robotik im Sicherheitsumfeld durch das neu etablierte Schweizer Drohnen- und Robotik-Zentrum (SDRZ) unterstützt werden. Für die Zusammenarbeit mit der ETH Zürich wurde eine Vereinbarung für das gemeinsame Programm Sicherheitsrobotik unterzeichnet. Auch der Aufbau des Cyber Defence Campus wurde fortgesetzt, um aufkommende Cyberrisiken zu identifizieren und mit innovativen Lösungen den Bedrohungen im Cyberraum wirksam zu begegnen. Im Weiteren wurde aufgrund der steigenden militärischen Relevanz 2022 ein neues Forschungsprogramm für den Bereich Weltraum lanciert. Dadurch sollen die rasanten Technologie-Entwicklungen im Bereich Weltraum verfolgt und Kompetenzen aufgebaut werden. Für die strategische Beratung hat das VBS einen Technologierat mit der ETH Zürich gegründet. Ausserdem wurden in der Periode 2021-2024 die Innovationsräume VBS geschaffen, um transdisziplinär neuartige Lösungen für die Herausforderungen des Departements zu identifizieren, entwickeln und testen. Dadurch sollen frühzeitig Erkenntnisse für spätere Vorhaben gesammelt und so grössere Fehlinvestitionen vermieden werden.

2.7 Herausforderungen und Handlungsbedarf

National- und Ständerat haben im Frühjahr 2022 beschlossen, die Armeeausgaben ab 2023 schrittweise zu erhöhen, sodass diese bis 2030 mindestens 1 Prozent des Bruttoinlandproduktes betragen sollen. Aufgrund der strukturellen Defizite in den Jahren 2024 bis 2026 beabsichtigt der Bundesrat jedoch eine Abflachung des Wachstumspfads und eine zeitliche Erstreckung bis 2035. Mit der aktuellen Investitionsplanung 2023 bis 2035 möchte die Armee Ausrüstungslücken schliessen und die Durchhaltefähigkeit erhöhen.

Das grundsätzlich wachsende Armeebudget bietet die Chance, Rüstungsbeschaffungen vorzuziehen, bringt aber auch zahlreiche Herausforderungen mit sich. Neben einem erhöhten Aufwand für die Durchführung der Beschaffungsprojekte steigen auch die Anforderungen an die Technologiekenntnisse. Der

technologische Fortschritt bringt kurze Innovationszyklen mit sich, was für die langfristig ausgerichtete Planung und Nutzung von Armeesystemen eine grosse Herausforderung darstellt. Beschaffungsprozesse müssen beschleunigt und vereinfacht werden, um mit der Technologieentwicklung Schritt halten zu können. Aufgrund einer Analyse des Beschaffungsablaufs durch die Beratungsfirma Deloitte wurden mehrere Empfehlungen formuliert. Unter anderem wurde empfohlen, für Vorhaben mit sehr kurzen Innovationszyklen einen vereinfachten Busspur-Prozess einzuführen. Ausserdem wurde darauf hingewiesen, den vergrösserten Handlungsspielraum durch das revidierte Beschaffungsrecht auszunutzen. Um auch in Zukunft auf technologische Entwicklungen und weltpolitische Ereignisse reagieren zu können, wird von allen Beteiligten eine gewisse Flexibilität erforderlich sein.

Eine wichtige Rolle wird weiterhin die Digitalisierung einnehmen. Deshalb ist es auch die Vision der Schweizer Armee, das Potenzial der Digitalisierung auszuschöpfen und in die Kultur zu integrieren. Durch die digitale Transformation können einerseits Prozesse effizienter und einfacher gestaltet werden. Andererseits ermöglicht die Digitalisierung aber auch einen Wissens- und Entscheidungsvorsprung. Für die Umsetzung der Digitalisierung und die Beherrschung der zunehmenden Komplexität ist es wesentlich, die Technologien zu verstehen und beurteilen zu können. Zudem ist es unabdingbar, die gesamte digitale Infrastruktur gegen Cyberangriffe und Ausfälle zu schützen.

Der technische Fortschritt in den vergangenen Jahren war enorm und wird weiter zunehmen. Um technologisch-wissenschaftlich auf dem neusten Stand zu bleiben und die Erkenntnisse für die Armee zu nutzen, bestehen verschiedene Instrumente. Durch die Technologiefrüherkennung können technologische Trends und disruptive Technologien rechtzeitig erkannt und deren Auswirkungen auf die Streitkräfte abgeschätzt werden. Ausgewählte Themen mit militärischer Relevanz können dann in Forschungsprojekten genauer untersucht werden. Der Kompetenzaufbau durch die Forschung ist Voraussetzung dafür, dass Expertisen für die Armee und die Beschaffung erbracht werden können. Der rasche technologische Wandel stellt auch hohe Anforderungen an das Technologiemanagement der Armee. Deshalb muss der Transfer von Wissen und Erkenntnissen aus der Forschung in die Armee sichergestellt werden. So können zur Unterstützung der strategischen Planung Technologie-Roadmaps erstellt werden. Das Potenzial und der disruptive Charakter neuer Technologien können mit Hilfe von Demonstratoren in realitätsnahen Szenarien aufgezeigt werden, welche weitgehend dem Umfeld von Einsätzen der Armee entsprechen. Für die Demonstration moderner Technologien können auch Simulationen und virtuelle Realitäten verwendet werden. Neben den technologischen Aspekten stellen sich oft auch gesellschaftlich-ethische Grundsatzfragen zum Einsatz moderner Technologien, insbesondere künstlicher Intelligenz und autonomer Systeme. Hier muss der interdisziplinäre Diskurs gefördert und unterstützt werden, aber auch in die Umsetzung der Forschungsthemen einfliessen. Es ist zudem darauf zu achten, dass die Erkenntnisse aus diesem Diskurs in die Ausbildung und das Training der Soldaten und Kaderangehörigen einfliessen.

Eine weitere Empfehlung des Deloitte-Berichts war die Einführung des Instruments der Innovationsräume. Im Gegensatz zur Forschung hat die Innovation das Ziel, neue Lösungen für einen konkreten Bedarf zu finden und innerhalb eines überschaubaren Zeitrahmens einsatznahe zu testen. Die Forschung liefert jedoch einen wichtigen Input für die Innovationsprozesse. Häufig geht es in der Innovation darum, bereits vorhandene zivile Lösungen für das militärische Umfeld anzupassen und zu nutzen.

3 Forschungsschwerpunkte und prioritäre Themenfelder 2025-2028

Die Forschung von armasuisse hat zum Ziel, diejenigen technisch-wissenschaftlichen Kompetenzen aufzubauen, welche benötigt werden, um die fähigkeitsorientierte Streitkräfteentwicklung der Gruppe Verteidigung und die Beschaffungsprozesse der armasuisse zu unterstützen. Ferner sollen die Kompetenzgrundlagen geschaffen werden, um Innovationsvorhaben zugunsten des VBS zu beurteilen und umzusetzen. Für die zukünftige Ausrichtung der Forschung wurden vier Forschungsschwerpunkte und jeweils zwei bis drei dazugehörige prioritäre Themenfelder definiert (Abbildung 7).

- Der Forschungsschwerpunkt **«Technologiefrüherkennung»** dient der frühzeitigen Erkennung von Technologieentwicklungen, welche einen potenziellen Einfluss auf die Sicherheit der Schweiz haben. Dabei steht nicht nur die Beobachtung von technologischen Entwicklungen im Vordergrund, sondern auch die Technologiefolgeabschätzung, welche die Konsequenzen auf die Gesellschaft, Wirtschaft und die sicherheitspolitischen Instrumente aufzeigt. Es geht darum, das Disruptionspotenzial technologischer Entwicklungen frühzeitig zu identifizieren und die damit verbundenen Chancen und Bedrohungen im sicherheitspolitischen Kontext zu antizipieren.

- Der Forschungsschwerpunkt **«Technologien für operationelle Fähigkeiten»** setzt sich aus drei prioritären Themenfeldern zusammen, welche primär auf den Kompetenzaufbau zur Unterstützung der fähigkeitsorientierten Streitkräfteentwicklung abzielen. Dazu gehören prioritär die Themenfelder «Wirkung und Schutz im physischen Raum», «Operationen und Schutz im Cyber- und elektromagnetischen Raum» sowie «Technologien zur Generierung von Informationsüberlegenheit».

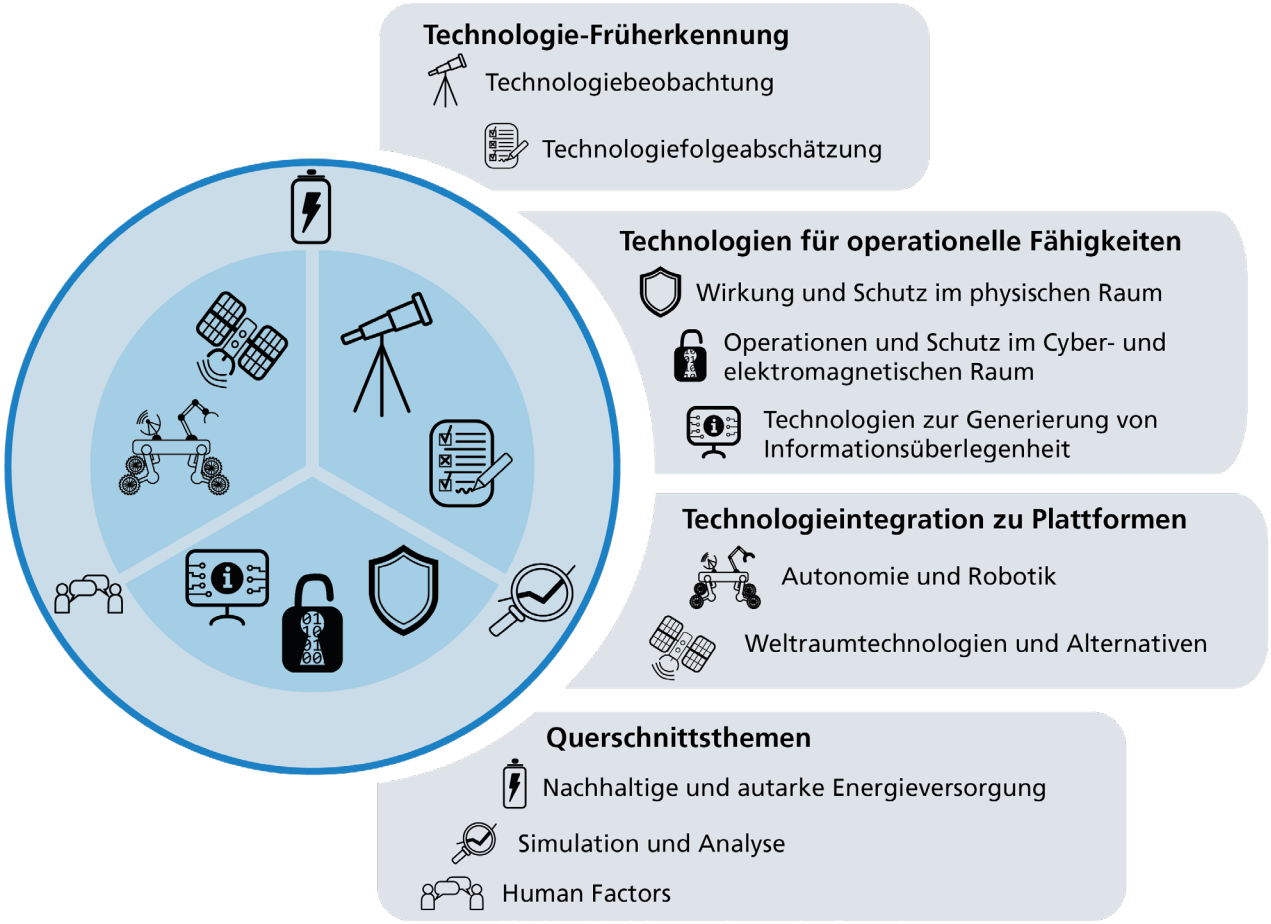


Abbildung 7: Forschungsschwerpunkte und prioritäre Themenfelder des LFP 2025-2028.

Mit dieser Ausrichtung sollen die technologischen Kenntnisse zur Ausgestaltung eines modernen Sensor-Nachrichtendienst-Führungs-Wirkungsverbunds (SNFW) auf dem neusten Stand gehalten und so unter anderem die Vision einer digitalisierten Schweizer Armee verfolgt werden.

- Der Forschungsschwerpunkt **«Technologieintegration zu Plattformen»** verfolgt das Ziel, verschiedenartige Technologien auf einer Plattform zu integrieren, um so Demonstratoren bereitzustellen, welche das Potenzial von Technologien im Labor oder einer einsatznahen Umgebung aufzeigen können. Solche Plattformen haben das Potenzial, mehrere operationelle Fähigkeiten gleichzeitig abzudecken. Ein wichtiges prioritäres Themenfeld in diesem Forschungsschwerpunkt ist «Autonomie und Robotik», in welchem die Einsatzmöglichkeiten von robotischen Systemen an Land, im Wasser und in der Luft aufgezeigt werden. Das zweite prioritäre Themenfeld zielt auf «Weltraumtechnologien und mögliche Alternativen» ab. Es geht darum abzuklären, wie die Operationssphäre Weltraum für einen Kleinstaat wie die Schweiz aus militärischer Sicht gezielt genutzt und wie Ausfälle oder Einschränkungen satellitenbasierter Dienstleistungen durch Alternativen aufgefangen werden können. Der Forschungsschwerpunkt «Technologieintegration zu Plattformen» nimmt eine wichtige Brückenfunktion zur Unterstützung der Innovationsräume des VBS und des Innovationssystems Verteidigung ein.
- Der Forschungsschwerpunkt **«Querschnittsthemen»** fokussiert auf den Kompetenzaufbau in Themenfeldern, welche für die Leistungserbringung von Sicherheitskräften unerlässlich sind. So sind Kenntnisse in «nachhaltiger und autarker Energieversorgung» von grosser Bedeutung, wenn das VBS einen namhaften Beitrag zu den Klimazielen des Bundes leisten will und gleichzeitig seine Aufgaben auch in ausserordentlichen Lagen erfüllen soll. Durch das prioritäre Themenfeld «Simulation und Analyse» werden die Grundlagen für die Streitkräfteentwicklung bereitgestellt und das Konzept für eine holistische Simulationsumgebung der Schweizer Armee weiterentwickelt. Die Armee ist ein soziotechnisches System, bei dem der Mensch und die damit verbundene Komplexität eine wesentliche Rolle spielen. Deshalb adressiert das prioritäre Themenfeld «Human Factors» sowohl die Interaktion zwischen Mensch und Technik als auch die gesellschaftlichen Aspekte, welche bei der Nutzung von Technologien im Kontext der Streitkräfte zu beachten sind.

Der LFP 2025-2028 ist auf den Bedarf der verschiedenen sicherheitspolitischen Instrumente ausgerichtet. Die Abbildung 7 stellt die Forschungsschwerpunkte und die prioritären Themenfelder in einer Übersicht dar. Nachfolgend werden diese im Detail dargestellt und hinsichtlich des Nutzens und der Anwenderorientierung erläutert.

3.1 Technologiefrüherkennung

3.1.1 Technologiebeobachtung

Ausgangslage und Problemstellung

Die heutige Technologie-Entwicklung ist sehr schnell und insbesondere die Digitalisierung hat einen Schub an neuen Produkten und Anwendungen mit sich gebracht. Dabei beobachtet man, dass sich entsprechend den globalen machtpolitischen Einflusssphären zwei Eco-Systeme zu bilden scheinen, in deren Zentrum die USA respektive China stehen. Deshalb erfolgen die technologischen Entwicklungen nicht nur dynamisch und teilweise komplementär, sondern in einigen Gebieten auch parallel zueinander. Auf den Märkten wird die Ablösung von einer Technologie durch eine andere oft in Form eines Leistungsschubs wahrgenommen. Die Zahl solcher Technologiezyklen hat in den letzten Jahrzehnten massiv zugenommen und sie erfolgen in immer kürzeren zeitlichen Abständen. Zudem entwickeln sich verschiedene Technologien nicht isoliert voneinander. Sehr oft führt die Verfügbarkeit einer bestimmten Technologie zu einem Fortschritt bei einer anderen Technologie, was zu einer Kettenreaktion von Entwicklungsschüben in anderen Technologiefeldern führen kann. Dieses Phänomen stellt die Technologiefrüherkennung vor enorm hohe Anforderungen.

Heute wird das Tempo des technologischen Fortschritts in vielen Bereichen durch die erwartete Nachfrage ziviler Märkte bestimmt. Obwohl viele moderne Technologien durchaus über militärisches Anwendungspotenzial verfügen, ist deren Anwendung in Streitkräften bedeutend weniger fortgeschritten. Hauptgrund ist die lange Nutzungsdauer von Hauptsystemen, meist zwischen 20 bis 40 Jahren.

Zwar wird mittels Werterhaltung versucht, auf das aktuelle technologische Niveau nachzurüsten, aber zivile Möglichkeiten der Technologienutzung schreiten immer rascher voran. Zudem stellt das Einsatzumfeld von Streitkräften sehr hohe Anforderungen an die Robustheit, Verfügbarkeit und Sicherheit. Der Markt militärischer Güter ist kleiner als der zivile Markt und oftmals staatlich kontrolliert, so dass die Rüstungsindustrie erst aktiv wird, wenn die Nachfrage der Streitkräfte genügend gross ist und diese auch bereit sind, entsprechende Entwicklungen zu finanzieren. Diese Gründe führen dazu, dass die verwendeten Technologien in Einsatzmitteln von Streitkräften meist nicht dem Stand entsprechen, welcher in zivilen Produkten des täglichen Lebens verfügbar ist.

Die Komplexität und besonderen Anforderungen des militärischen Umfelds erfordern eine systematische Beobachtung von technologischen Entwicklungen. Grundsätzlich sind bei der Technologiefrüherkennung zwei unterschiedliche zeitliche Horizonte zu unterscheiden. Während bei der Technologiebeobachtung ein breiter Zeithorizont gesetzt wird, ist die Technologiefolgeabschätzung eher langfristig ausgelegt. Die Technologiebeobachtung mit ihren beiden Hauptelementen, Technologie- und Marktmonitoring, bilden die Grundlagen für die Bewertungen von Technologien hinsichtlich ihres Reifegrades und ihres Einsatzpotenzials. Auf dieser Basis können Streitkräfte beraten werden, ob sie auf eine neue Technologie setzen sollten und wann der Zeitpunkt dazu ideal ist. Damit kann sichergestellt werden, dass finanzielle Mittel effizient in moderne Technologien investiert werden. Die Erkenntnisse aus der Technologiefolgeabschätzung sind hingegen darauf ausgerichtet, die Prozesse der langfristigen Streitkräfteentwicklung zu unterstützen. In beiden Fällen sind die aktuellen Trends und Entwicklungen laufend zu beobachten.

Das Ziel einer umfassenden Beobachtung von Technologieentwicklungen ist die Konsolidierung der Infor-

mationen aus den laufenden Forschungsaktivitäten und die Identifikation von Technologien, welche sich thematisch ausserhalb der Ausrichtung laufender Forschungsprogramme befinden, aber dennoch relevant für die Aufgabenerfüllung von Sicherheitskräften werden können. Deshalb ist die Technologiebeobachtung sehr umfassend zu verstehen. Sie fasst vorwiegend zivile aber auch militärische Technologien zu einer bewerteten 360°-Technologieübersicht zusammen. Weil Technologien per se ziemlich universell betrachtet werden können, gibt es dazu auf internationaler Ebene einige gute, aktuelle und auch umfassende Studien. Eine wesentliche Aufgabe ist es, die Erkenntnisse aus diesen Studien im Kontext der Schweizer Sicherheitspolitik und ihrer Instrumente zu interpretieren und darzustellen.

Forschungsthemen 2025-2028

Beobachtung technologischer Entwicklungen

- Identifizierung technologischer Treiber mit Relevanz für die Sicherheit der Schweiz
- Verfolgung ziviler Technologie-Entwicklungen mit Potenzial zur militärischen Nutzung
- Entwicklung einer Analyse-Plattform zur automatischen Erkennung von raschen und disruptiven Technologie-Entwicklungen
- Erarbeitung einer intuitiven Darstellung von technologischen Treibern
- Aufbau eines internationalen Netzwerkes zur Verfolgung und Bewertung technologischer Entwicklungen

Bewertung technologischer Entwicklungen

- Abschätzung der Reife von sicherheitsrelevanten Technologien sowie Beurteilung der künftigen Anwendbarkeit bei Einsatzkräften
- Beurteilung des Disruptionspotenzials von Technologien
- Bestimmung des technologischen Lebenszyklus von militärisch relevanten Produkten
- Aufbau von Methoden für die frühe Erkennung und den Umgang mit unerwarteten Ereignissen, welche erhebliche Auswirkungen haben (Black Swans)
- Erarbeitung von Inputs für die Ausrichtung der Forschung im sicherheitsrelevanten Bereich

3.1.2 Technologiefolgeabschätzung

Ausgangslage und Problemstellung

Die Technologiefolgeabschätzung befasst sich mit den Folgen technologischer Entwicklungen auf verschiedenste soziologische Aspekte, welche wiederum den Rahmen für eine künftige Sicherheitspolitik und die Ausgestaltung ihrer Instrumente geben. In diesem Sinne dient die Technologiefolgeabschätzung der Antizipation von möglichen Zukunftsszenarien, wobei sich diese schliesslich auf Themen der nationalen Sicherheit im Allgemeinen und auf die Ausgestaltung von Streitkräften im Speziellen fokussieren.

Ein Schwerpunkt im Rahmen der Technologiefolgeabschätzung liegt darin, Technologien mit einem hohen Disruptionspotenzial zu erkennen und mögliche Auswirkungen sowohl im militärischen als auch im zivilen Kontext zu antizipieren. Beides ist notwendig, weil sich die beiden Bereiche gegenseitig beeinflussen. Im zivilen Umfeld haben wir solche Disruptionen beispielsweise schon im Rahmen der fortschreitenden Digitalisierung erlebt. Digitale Plattformen, welche sich als Intermediäre zwischen Kunden und Leistungserbringern positionierten, haben die Geschäftsmodelle ganzer Branchen auf den Kopf gestellt. Etablierte Firmen, welche den Schritt in die Digitalisierung verpasst haben, sind verschwunden. Durch die Digitalisierung sind aber auch gesellschaftliche Veränderungen sichtbar, welche sich beispielsweise in neuen digitalen Formen der Interaktion von Individuen oder Gruppen zeigen. Im Vergleich zum zivilen Umfeld ist bei den Streitkräften die Digitalisierung noch nicht so weit fortgeschritten. Es ist aber zu erwarten, dass die fortschreitende Digitalisierung der Streitkräfte zu Disruptionen ähnlicher Tragweite führen wird, wie wir dies aus dem zivilen Alltag kennen. Die rechtzeitige Erkennung disruptiver Entwicklungen ist zentral, damit für die fähigkeitsorientierte Streitkräfteentwicklung die richtigen Konsequenzen abgeleitet und Risiken reduziert werden können.

Die Technologiefolgeabschätzung im sicherheitspolitischen Umfeld muss einen holistischen Ansatz verfolgen, um möglichen Handlungsbedarf in verschiedenen Zukunftsszenarien abzuleiten. Dabei geht es nicht darum Zukunftsszenarien hinsichtlich ihrer Eintretens-

wahrscheinlichkeiten zu bewerten, sondern diese zu durchdenken, um damit die Basis für künftige Handlungsoptionen zu legen. Besonders herausfordernd ist dabei der Umgang mit möglichen Disruptionen, welche aufgrund technologischer Entwicklungen eintreten können. Dafür ist offenes, transdisziplinäres Denken notwendig, welches die Interaktion von Technologie, Ökonomie, Gesellschaft, Recht, Ethik, Ökologie und Politik berücksichtigt.

Damit kann die Technologiefolgeabschätzung einen Beitrag zur Antizipation möglicher Zukunftsszenarien und damit auch von möglichen Krisen leisten, so wie dies im Sicherheitspolitischen Bericht gefordert wird. Die Ergebnisse könnten aber auch interdepartemental und mit weiteren Akteuren geteilt werden, welche daran interessiert sind, sich über zukünftig mögliche Entwicklungen ihrer Interessensgebiete auszutauschen. Für die Folgeabschätzung von neuen Technologien müssen sowohl die möglichen Chancen als auch die Bedrohungen betrachtet werden. Chancen ergeben sich dann, wenn Aufgaben der Armee effizienter erbracht oder wenn aus dem Einsatz von neuen Technologien ein operationeller Vorteil und dadurch eine operative Überlegenheit resultieren. Das Spektrum möglicher Bedrohungen kann sehr vielfältig sein. Im Rahmen der Technologiefolgeabschätzung geht es darum, diejenigen Bedrohungen zu erkennen, welche in ihrer Konsequenz der Gesellschaft grossen Schaden zufügen, die souveräne Handlungsfähigkeit des Staates einschränken oder die Armee in ihrer Auftragserfüllung limitieren können.

Vor diesem Hintergrund soll durch die Technologiefolgeabschätzung eine antizipative Grundlage für die fähigkeitsorientierte Weiterentwicklung der Streitkräfte gelegt werden, mit dem Ziel, langfristige Planungsrisiken zu reduzieren. Es geht darum, das Potenzial von aufkommenden und disruptiven Technologien in Zukunftsszenarien mit Hilfe von Simulation und Wargaming abzuklären und die Konsequenzen durch ihren Einsatz aufzuzeigen.

Forschungsthemen 2025-2028

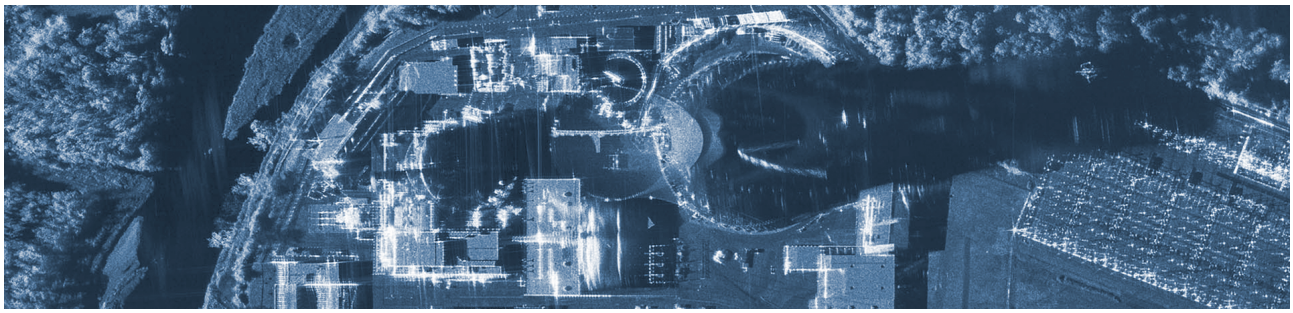
Szenarien Entwicklung

- Aufbau von Methoden und Kreativitäts-Techniken zur Szenarien-Entwicklung und Analyse von Technologiefolgeabschätzungen, sowie Überführung in strategische Handlungsempfehlungen
- Entwicklung von Narrativen zur Veranschaulichung technologiegetriebener Disruption in sicherheitsrelevanten Szenarien
- Verwendung von visionären und spekulativen Ansätzen zur Identifikation und Verbreitung zukünftiger technologischer Entwicklungen und ihrem Anwendungspotenzial
- Entwicklung von zukünftigen Kompetenzprofilen für die verschiedenen Funktionen in der Armee
- Bildung eines Expertennetzwerkes unter internationaler Beteiligung
- Betrachtung der Konsequenzen von technologischen Entwicklungen auf politische, wirtschaftliche, soziokulturelle, ökologisch-geografische und rechtliche Aspekte (PESTEL)

Simulation und Wargaming

- Entwicklung von Wargaming-Methoden mit Fokus auf Zukunftstechnologien mit Disruptionspotenzial
- Umsetzung von Szenarien durch digitale Simulationen unter Berücksichtigung von Zukunftstechnologien
- Aufbau eines Schweizerischen Expertennetzwerkes zur Antizipation technologischer Entwicklungen

3.2 Technologien für operationelle Fähigkeiten



3.2.1 Wirkung und Schutz im physischen Raum

Ausgangslage und Problemstellung

Die Armee kann ihren Auftrag nur erfüllen, wenn sie in der Lage ist, koordiniert und synchronisiert in allen Operationssphären so zu agieren, wie es für die aktuelle Lage angemessen ist. Man spricht von sogenannten Multi-Domain-Operationen. Diese beinhalten einerseits die Fähigkeit mit taktischen Aktionen operative Ziele zu erreichen. Andererseits soll dies der Gegenseite verunmöglicht werden. Kampfhandlungen finden schon heute und mit grosser Wahrscheinlichkeit auch künftig vor allem im überbauten und nur teilweise evakuierten Gebiet statt. Daraus leiten sich naturgemäss sehr hohe Anforderungen an die Präzision und Skalierbarkeit der eigenen Wirkmittel ab. Einerseits soll die maximale Wirkung in diesem anspruchsvollen Gelände erreicht werden, andererseits sollen damit lediglich minimale Kollateralschäden verursacht werden, insbesondere wenn auch eigene Infrastrukturen und Lebensraum davon betroffen sind. Damit ein Ziel in der beabsichtigten Art und Weise getroffen werden kann, ist ein rascher SNFW die Voraussetzung. Dies ist das Resultat eines erfolgreichen Zusammenspiels von aktuellem Lagebild, schneller Zielzuweisung, präziser Feuerleitung sowie technischer Zielgenauigkeit und Störfestigkeit des Wirkmittels. Um die Handlungsfreiheit und die Durchhaltefähigkeit zu maximieren, ist ausserdem dem Schutz von Personal, Material und Infrastruktur der Armee eine zentrale Bedeutung beizumessen. Dies nicht zuletzt deshalb, weil mögliche Standorte der Armee lange vor Ausbruch konkreter Kampfhandlungen weitgehend aufgeklärt sein dürften.

Wirkung im physischen Raum

Damit mit begrenzten Mitteln eine maximale Wirkung erzielt werden kann, braucht es eine optimierte Zusammensetzung der Verbände. Durch Betrachtung von klassischen Erfolgsfaktoren wie Mobilität, Wirksamkeit und Verwundbarkeit von Systemen, Präzision mittels autonomer Navigation und Reichweite von Wirkmitteln können Aussagen zur Kampfkraft von Verbänden abgeleitet werden. Indem aktuelle Trends der Streitkräfteentwicklung und der Forschung im Bereich der Waffensysteme auf Schweizer Verhältnisse angepasst und für verschiedene Einsatzszenarien durchgerechnet werden, können weiterführende Abklärungen und eigene Forschungstätigkeiten auf die vielversprechendsten Varianten fokussiert werden.

Durch Fortschritte in Technologien des SNFW kann die Effektivität und Effizienz von Einsätzen massgeblich gesteigert werden. Gleichzeitig steigen dadurch aber auch die Anforderungen an Mobilität und Autonomie der Systeme immer mehr. Im Bereich des Bogenfeuers bedeutet dies zum Beispiel, dass Geschütze vermehrt autonom operieren und über grössere Distanzen einsatzspezifisch zu Feuereinheiten zusammengeschlossen werden. Dadurch wird zwar die Verwundbarkeit des einzelnen Geschützes reduziert, gleichzeitig steigen aber die Anforderungen an Vernetzung und Feuerleitung deutlich. Der dezentrale Einsatz von Effektoren kann zusätzlich mit dem Einsatz von verschiedenen Systemen mit abgestufter Reichweite und Präzisionsmunition weiter optimiert werden. Loitering Munition treibt das Einsatzprinzip der dezentralen Effektoren auf die Spitze, indem der Effektor über einen längeren Zeitraum über dem Zielgebiet verharrt und entweder ein erkanntes Ziel autonom bekämpft oder auf eine Zielzuweisung wartet. Intelligente Munition, z.B. Angriffsdrohnen oder eben Loitering Munition, könnte auch für den gezielten autonomen oder teilautonomen Einsatz gegen sehr spezifische Ziele wie

Radar- oder Kommunikationssysteme eingesetzt werden.

Die Bekämpfung dieser intelligenten autonomen Wirkmittel und Präzisionsmunition ist ein weiterer Schwerpunkt aktueller Entwicklungen. Während traditionell Mittel der bodengestützten Luftverteidigung zum Einsatz kommen, mangelt es diesen Systemen jedoch je nach Bedrohung an Präzision oder sie sind zu träge. Durch die zivil getriebenen technologischen Entwicklungen bei Laserquellen und angepasster Optik rücken Laser als Waffen in den Bereich eines möglichen Anwendungsspektrums. Die Vorteile von Laserwaffen sind vielfältig: z.B. sind diese sehr präzise, rasch einsetzbar, unendlich oft wiederverwendbar, skalierbar in der Wirkung, signaturarm und ohne Munition betreibbar. Dagegen ist die Bereitstellung von genügend Energie und der Umgang mit den meteorologischen Verhältnissen eine grosse Herausforderung. Die Lasertechnologie eignet sich auch zur Blendung von Sensoren. Dabei ist insbesondere an die Bekämpfung von intelligenter Munition sowie weltraumgestützter Aufklärungsmittel zu denken.

Mikrowellen eignen sich ebenfalls zur Erzeugung einer gezielten Wirkung. Auch diese wirken unsichtbar und geräuschlos. Dank Mikrowellen ist es möglich, auf kurze Distanzen elektronische Bauteile und auch Drohnen temporär zu stören oder auch nachhaltig zu schädigen. Im militärischen Kontext sind Mikrowellenwaffen, sogenannte High Power Microwave (HPM) Systeme auf dem Markt. Sie gehören zur Kategorie der Directed Energy Weapons, die mit gebündelter Energie Ziele ausser Funktion setzen, schädigen oder vernichten können.

Schutz im physischen Raum

Für moderne Streitkräfte ist die Kernfähigkeiten des Eigenschutzes zur Gewährleistung der Überlebensfähigkeit unerlässlich, damit die Aufgabenerfüllung sichergestellt werden kann. Die Einsatzbedingungen, die allgemeinen technologischen Entwicklungen, z.B. neue Werkstoffe, und die Charakteristik der gegnerischen letalen bzw. nichtletalen Wirkmittel bestimmen Umfang und Ausmass des benötigten Schutzes. Während bei Körperschutzsystemen dank moderner Kunststoffe und Keramiken weiterhin merkliche Gewichtsreduktionen bei gleichbleibender Schutzleistung realisiert werden, scheint das Potenzial bei mobilen Plattformen weitgehend ausgeschöpft zu sein. Entsprechend ist in diesem Bereich eine Verschiebung der Entwicklungs- und Forschungstätigkeit hin zu reaktiven und verstärkt auch aktiven Schutzlösungen festzustellen. Speziell aktive Schutzlösungen versprechen eine deutliche Verbesserung der Schutzleistung bei maximal gleichbleibendem Gewicht. Beide Varianten haben jedoch den Nachteil, dass sie je nach Funktionsprinzip und Referenzbedrohung erhebliche Kollateralschäden verursachen können und bisherige Einsatzverfahren angepasst werden müssen.

Die Bedrohung durch ballistische Raketen ist nicht neu. Deren Abwehr ist für die Schweiz nur im Rahmen internationaler Zusammenarbeit möglich. Eine neue Kategorie von weitreichenden Waffen stellen die hypersonischen Flug- und Raketensysteme dar, welche aufgrund ihrer erdnahen Flugbahn für terrestrische- und luftgestützte Aufklärungsmittel erst wenige Minuten vor Erreichen des Ziels detektiert werden können. Die hohe Geschwindigkeit und der grosse damit verbundene Zielraum stellen zusammen mit den engen Zeitverhältnissen die Abwehr von hypersonischen Waffen vor grosse Herausforderungen, selbst für High-Tech-Nationen mit umfangreichen Rüstungskompetenzen. Zudem haben westliche Staaten ihre eigenen Programme zur Entwicklung hypersonischer Waffen reaktiviert oder intensiviert. Auch wenn erwartet wird, dass solche Waffen aufgrund der hohen Kosten nur gegen Ziele mit hoher strategischer oder symbolischer Bedeutung eingesetzt werden, muss deren Entwicklung hinsichtlich möglicher Schutzkonzepte beobachtet werden. Stationäre Einrichtungen wie militärische Infrastruktur im In- und Ausland, kritische Infrastrukturen und Einrichtungen der Grundversorgung sind sowohl in kriegerischen Auseinandersetzungen als auch in hybriden Konflikten vulnerabel.

Das nach wie vor erhöhte Risiko terroristischer Anschläge hat die Sensibilität für die Gefahren des Einsatzes biologischer, chemischer und radiologischer Waffen gefestigt. Aufgrund ihres Schadenspotenzials muss der Schutz gegen biologische Kampfstoffe und Biotoxine, die eigentlich international geächtet sind, evaluiert werden. Da diese Kampfstoffe sehr schnell auf Umwelteinflüsse reagieren, dient die Forschung der Identifizierung und dem Nachweis biologischer und chemischer Stoffe durch Sensoren sowie der Entwicklung geeigneter Schutz- und Abwehrmassnahmen. Fortschritte in der Biotechnologie und der Gentechnik sowie ihre Zugänglichkeit sind in dieser Hinsicht von besonderer Bedeutung. Die Möglichkeit, Eigenschaften von Organismen zu verändern, bietet Chancen für den verbesserten Schutz, stellt aber auch ein Risiko von neuen Kampstoffen dar. Bei radiologi-

schen Waffen werden radioaktive Stoffe durch konventionelle Sprengstoffe freigesetzt. Die Schutzmassnahmen sind dieselben, welche bei der Freisetzung von Radioaktivität aus Unfällen von Kernkraftwerken vorzunehmen sind.

Trotz Fortschritten bei der Detektion und Neutralisierung von improvisierten Ladungen, sogenannten Improvised Explosive Devices (IED), stellen improvisierte Sprengladungen für Einsatzkräfte und die Bevölkerung in Konfliktsituationen eine latente Bedrohung dar. Daher ist es wichtig, dass die Detektion von IEDs und mögliche Neutralisierungstechniken weiter verbessert werden. Wie Erfahrungen aus Einsatzgebieten zeigen, kann die Verhinderung von Anschlägen sehr effektiv sein, wenn versucht wird, Anomalien in der Handels- und Logistikkette spezifischer Bauteile und Substanzen, welche für den Bau von IEDs verwendet werden, aufzuspüren. Damit lassen sich Hersteller von IEDs identifizieren und vor dem Auslösen einer Gewaltaktion neutralisieren.

Die Verwendung von (teil-)autonomen Drohnen als Transportmittel für IEDs, mit oder ohne Anreicherung mit biologischen, chemischen oder radiologischen Stoffen, stellt eine neuere Bedrohung und eine erhebliche Herausforderung dar. Dank ihrer geringen Grösse ist es nicht nur schwierig sie rechtzeitig zu detektieren, sondern auch eine Bekämpfung in sicherer Distanz zu ihrem Angriffsziel ist gegenwärtig eine ungelöste Frage.

Auch Aktionen im Cyber- und elektromagnetischen Raum leisten einen wesentlichen Beitrag zum Schutz im physischen Raum. Der Schutz gegen elektromagnetische Störung (EMP), Mikrowellenwaffen (HPM) und Cyberattacken ist von Bedeutung, um kritische Infrastrukturen zu schützen. Diese zeigen oftmals eine hohe gegenseitige Abhängigkeit auf und dies kann bei Angriffen auf ein oder mehrere Infrastrukturelemente zu Kettenreaktionen führen. Diese Abhängigkeiten und ihre Risiken müssen genau untersucht und beschrieben werden, damit effektive Massnahmen zur Eindämmung und Handhabung von Schadensereignissen getroffen werden können. Auch elektromagnetische Felder können gegen Menschen eingesetzt werden, um deren Leistungsfähigkeit negativ zu beeinflussen. Deshalb müssen nicht nur Infrastrukturen und Ausrüstung, sondern auch Personen vor starken elektromagnetischen Strahlen geschützt werden.

Der effektivste Schutz wird jedoch durch die Verschleierung der eigenen Mittel vor der gegnerischen Aufklärung erreicht. Multispektrale Tarnung und Täuschung sind dazu effektive Ansätze. Heute ist davon auszugehen, dass die meisten ortsfesten Installationen aufgeklärt und deren Koordinaten bekannt sind. Mobile Objekte können hingegen getarnt werden, indem man ihre elektromagnetische Signatur der Umgebung anpasst und Emissionen, wie Lärm oder Rauch, unterdrückt. Damit wird deren Ortung, Identifikation und Verfolgung durch einen Gegner erschwert. Insbesondere in der Luftfahrttechnik, aber auch vermehrt bei see- und landgestützten Plattformen bedient man sich zur Reduktion der Radarsignaturen der Tarnkappentechnologie, wobei der Tarnkappeneffekt durch den Einsatz bestimmter Verbundwerkstoffe, durch die Verwendung radarabsorbierender Materialien und Beschichtungen oder durch spezifische Plattformkonstruktionen erzielt wird. Dem gleichen Ziel dient das Morphing zur Veränderung von Oberflächeneigenschaften wie der Anpassung der Farbe, oder zur Veränderung der Oberflächenstrukturen wie z.B. die Veränderung eines Flugzeugflügels im Flug.

Forschungsthemen 2025-2028

Schutz von Fahrzeugen, Flugzeugen und Personen

- Untersuchung neuer Materialien zur Verbesserung des ballistischen Schutzes von Personen
- Verfolgung der Entwicklungen bei aktivem und reaktivem Schutz von Fahrzeugen und Aufbau der zugehörigen Beurteilungsfähigkeit
- Erforschung neuartiger Ansätze im Bereich Tarnung und Täuschung sowie Aufbau der Beurteilungsfähigkeit für zukünftige Systeme
- Weiterentwicklung der Verwundbarkeitsmodelle von Plattformen zur Verbesserung des Eigenschutzes und der Einsatzverfahren
- Erforschung möglicher Technologien zum proaktiven Schutz vor unbemannten Plattformen (UAV/UGV)
- Untersuchung und Modellierung der Wirkung sowie des Schadenspotenzials improvisierter Ladungen zur Förderung des Risikobewusstseins, Verbesserung von Einsatzverfahren und zur Unterstützung der Schutzkonzeption von Plattformen und Infrastruktur

Schutz und Sicherheit von Gebäuden und Infrastruktur

- Erforschung und Modellierung der Wirkmechanismen elektromagnetischer Pulse und Entwicklung

von Vorgaben zur Konzeption von entsprechenden Schutzlösungen
- Untersuchung und Modellierung der Schadenspotenziale von grossen Sprengladungen zur Unterstützung der Planung neuer und zur Verbesserung der Notfallpläne bestehender Infrastruktur
- Unterstützung bei der Entwicklung von Lösungen zur nachträglichen Härtung von Gebäuden gegen Ladungen und Projektile und zur Erhöhung des Schutzgrades bestehender Bauten
- Verfolgen der Entwicklung im Bereich der Abwehr von unbemannten Plattformen (UAV/UGV) und Aufbau der Beurteilungsfähigkeit
- Analyse der Entwicklung im Bereich der Detektion und Abwehr von Boden-Boden-Wirkmitteln zum Aufbau des Wissens für Expertisen

Wirkung

- Monitoring der Entwicklungen im Bereich der hypersonischen Waffen mit speziellem Fokus auf Manövrierbarkeit und Wirkung im Ziel sowie Analyse zu möglichen Gegenmassnahmen.
- Verfolgen der Entwicklungen bei autonomen Waffensystemen mit Schwerpunkt auf Einsatzprinzipien, Steuerung und Koordination sowie Wirkfähigkeit
- Simulation von Boden-Luft und Luft-Luft Systemen, inkl. der Modellierung der Gefechtsköpfe zur Optimierung ihres Einsatzes
- Erforschung der Grundlagen gerichteter elektromagnetischer Strahlung mit hoher Energiedichte zur Ermittlung ihres Wirkungspotenzials
- Ausweitung der ballistischen Kompetenz auf moderne Systeme unter spezieller Berücksichtigung von Endphasenlenkung und Raketenantrieb
- Untersuchung der Möglichkeiten zur Verbesserung der Feuerleitung und Zielzuweisung von Bogenfeuer und Raketenartillerie mit dem Ziel einer schnelleren und präziseren Informationsübermittlung zwischen Sensor und Wirkmittel
- Entwicklung der ballistischen Kompetenzen für Luft-Boden Einsätze zur Unterstützung eines entsprechenden Fähigkeitsaufbaus

Sicherheit von Explosivstoffen und Munition

- Untersuchung der Initiierungs- und Umsetzungscharakteristik von Explosivstoffen zur Förderung der Sicherheit im Umgang mit Explosivstoffen
- Erforschen der Alterung von modernen Explosivstoffen und Treibladungspulvern zur Optimierung der Lagerungsbedingungen sowie der Lebensdauerberechnung von Munition und Explosivstoffen
- Erforschung des Alterungsprozesses von Materialen für den ballistischen und detonischen Schutz zur Vorhersage der Schutzwirkung über die gesamte Lebensdauer
- Ermitteln der Umweltauswirkungen von Munition und Munitionsrückständen mit dem Ziel die Sanierung von Altlasten zu optimieren und die Schädigung der Natur durch die Nutzung von Munition und Explosivstoffen zu minimieren

3.2.2 Operationen und Schutz im Cyber- und elektromagnetischen Raum

Ausgangslage und Problemstellung

Aktuelle Konflikte werden mit starkem Einbezug des Cyber- und elektromagnetischen Raums (CER) geführt. Bereits im Alltag sehen sich die Schweizer Armee und die Gesellschaft regelmässig mit Cyberangriffen konfrontiert, wobei die zunehmende Digitalisierung die Verwundbarkeit durch derartige Angriffe erhöht. Die Notwendigkeit, diese Herausforderungen sowohl bei der Weiterentwicklung der Armee als auch bei der fortschreitenden Digitalisierung der Schweiz zu berücksichtigen, ist unbestritten. Wie dies geschehen soll, skizzieren die Gesamtkonzeption Cyber des VBS und die nationale Strategie zum Schutz vor Cyberrisiken (NCS). Die Gesamtkonzeption Cyber fokussiert dabei auf die Weiterentwicklung der Armee im Bereich Cyber bis in die 2030er Jahre.

Im Zentrum stehen dabei die Erreichung und Beibehaltung des eigenen Informationsvorsprungs für eine überlegene Entscheidungsfindung im CER. Erreicht wird dies einerseits durch einen starken Eigenschutz, um dem Gegner einen Vorsprung zu verwehren, und andererseits durch gezielte Aktionen respektive Operationen. Ziel ist es, den Gegner mit Informations- und damit Entscheidungsverzögerungen zu konfrontieren. Beide Bereiche sollen gegenüber dem heutigen Stand längerfristig deutlich ausgebaut werden: Zuerst zentral und mit Blick auf die Kerninfrastrukturen, danach auch lokal und autonom bei Einheiten im Feld.

Diesem qualitativen und quantitativen Ausbau stehen vielfältige Herausforderungen gegenüber, wobei die meisten in der wachsenden Vernetzung und Digitali-

sierung, im stetigen Wandel des Cyberraums, in der Kurzlebigkeit der Informations- und Kommunikationstechnologie (IKT) und in der grossen Zahl an neuen Technologien und Innovationen begründet sind. So ist beispielsweise ein Kampfpanzer nach wie vor ein hoch geschütztes Waffensystem zur direkten Bekämpfung von Bodenzielen. Er ist aber durch seine IKT auch mit dem CER verbunden und somit ein Angriffsziel in diesem Raum. Im Falle einer erfolgreichen Beeinträchtigung seiner IKT wird der Panzer sogar zum Ausgangspunkt von Angriffen.

Um mit diesen Herausforderungen umzugehen und angemessene staatliche Fähigkeiten und die Eigenständigkeit im Cyberraum zu stärken, müssen die Kräfte durch nationale Kooperationen und partnerschaftliche Zusammenarbeit in Bildung, Forschung und Wirtschaft gebündelt werden. Nur so können relevante technologische Entwicklungen antizipiert und Fachkräfte für aktuelle und zukünftige Herausforderungen ausgebildet und gewonnen werden. Der Forschung kommt sowohl bei der Integration von inkrementellen als auch disruptiven Technologieentwicklungen eine zentrale Rolle zu. Durch eine frühzeitige Auseinandersetzung mit solchen Entwicklungen lassen sich deren Chancen und Risiken im Hinblick auf den Informationsvorsprung und eine überlegene Entscheidungsfindung abschätzen und im Rahmen von Beschaffungen und Wissenstransfer rasch in operationelle Fähigkeiten überführen.

CER Eigenschutz

Armee, öffentliche Verwaltung, kritische Infrastruktur, Wirtschaft und Gesellschaft sind in hohem Grad digital vernetzt und viele Prozesse und Fähigkeiten sind digitalisiert. Das Internet der Dinge (IoT) ist mit teilautonomen Fahrzeugen und Fluggeräten, vernetzten Sensoren zur Steuerung von Gebäuden, Stromnetzen oder auch ganzen Smart-Cities zur Realität geworden. Dies birgt Chancen und Risiken. Der zunehmende Einsatz von Informations- und Kommunikationsmitteln erfordert Schutzmassnahmen, insbesondere was die Verfügbarkeit, Integrität und Vertraulichkeit der Informations- und Kommunikationssysteme betrifft. Dabei stellt die Verwendung ziviler Software und die Produktionskette wichtiger Hardwarekomponenten mit eingebetteten Softwarefunktionen ein schwierig abzuschätzendes Verwundbarkeitspotenzial der Informations- und Kommunikationsinfrastruktur dar.

Die Vernetzung und Digitalisierung werden auch in den kommenden Jahren fortschreiten und damit die Fragilität des Cyberraums weiter erhöhen. Dabei werden jene Prozesse, Fähigkeiten und Technologien besonders anfällig sein, bei denen der Eigenschutz im Cyberraum aus verschiedenen Gründen bisher keine oder kaum eine Rolle gespielt hat. Dies z.B. weil diese zuvor gar nicht digital oder vernetzt waren wie im Falle von Kaffeemaschinen, Alarmanlagen oder Fahrzeugen, oder weil Angreifende vor hohen technischen und finanziellen Hürden standen. Eine ähnliche Anfälligkeit weisen potenziell auch gänzlich neuartige Prozesse, Fähigkeiten und Technologien auf. Dazu gehören zum Beispiel neue kryptographische Verfahren und Protokolle, die Angriffen durch leistungsfähige Quantencomputer widerstehen können. Sollten genügend leistungsfähige Quantencomputer entwickelt werden können, müssen somit nicht alle Systeme, die Kryptographie nutzen, ersetzt oder angepasst werden. Quantencomputer werden besonders asymmetrische Verfahren, die keinen vorgängigen Austausch eines Schlüssels benötigen, unbrauchbar machen. Da diese jedoch den Alltag durchdringen, sie sind zum Beispiel die Basis für die Absicherung der Kommunikation mit Diensten im Internet, hat der Quantencomputer hier klar disruptives Potenzial. Weitere Technologien mit disruptivem Potenzial sind beispielsweise die künstliche Intelligenz (KI) oder 5G+ Netzwerke.

Die Auswirkungen von Bedrohungen aus dem Cyberraum gestalten sich sehr mannigfaltig und reichen von kurzfristigen Operationen zur Störung kritischer Infrastruktur, wie beispielsweise Distributed-Denial-of-Service (DDoS) Angriffe, bis hin zur unerkannten, langfristig ausgerichteten Einbettung von Cyberwaffen in IKT-Systeme, welche im Bedarfsfall ausgelöst werden können. Während ein ausschliesslich im Cyberraum geführter Konflikt heute als unrealistisch erachtet wird, sind solche Angriffe zur Vorbereitung auf einen militärischen Konflikt oder als Bestandteil von militärischen Einsätzen während eines Konflikts bereits Realität.

Längst nicht jeder Cyberangriff ist jedoch militärisch motiviert. Cyberkriminalität wird gemäss NCS durch zivile Behörden bekämpft. Dem gegenüber gibt es im Fall der Cyberspionage sowohl wirtschaftliche als auch militärische Aspekte. Cyberspionage findet laufend, verdeckt und unabhängig von Konflikten statt. Dabei sind Regierungsnetzwerke mit klassifizierten Informationen genauso betroffen, wie Unternehmen und Forschungsinstitutionen. Beispielsweise betrifft die Infiltration von Software- und Hardware-Lieferketten breite Teile der Wirtschaft. Solche Aktionen sind komplex und benötigen seitens der Angreifer viel Vorlauf-

zeit. Deshalb ist der Eigenschutz auch ausserhalb von Krisenzeiten eine permanente und wichtige Aufgabe.

Im Bereich Eigenschutz im Cyberraum stehen Technologien zur frühzeitigen Erkennung von Cyberrisiken, zur Verbesserung der Verteidigungsmassnahmen und zur Suche und Validierung von Schwachstellen bzw. von Sicherheitsproblemen im Zentrum. Manuelle Analysen von potenziell schadhaften Programmen können allerdings nicht mehr mit dem Tempo der Entwicklung und der Anzahl potenzieller Schwachstellen schritthalten. Bei der Automatisierung von Sicherheitsanalysen ist deshalb mit grossen Fortschritten zu rechnen. Dies betrifft diverse Aspekte wie die Suche fehlerhafter Muster im Quellcode und die Verhaltensanalyse von Programmen während deren Ausführung. Software wird meist aus verschiedenen Standardkomponenten zusammengesetzt. Deshalb ist es wichtig, verdächtige Komponenten mit bekannten Sicherheitslücken zu identifizieren. Wurden Schwachstellen gefunden, braucht es zudem automatisierte Methoden zur Überprüfung der Ausnutzbarkeit für Angriffe, um die effektive Bedrohung abschätzen zu können.

Bei der frühzeitigen Erkennung von Cyberrisiken und deren Beurteilung steht die Sicherheit von einzelnen Systemen, aber auch die Sicherheit der ganzen Lieferkette im Zentrum. Um diese Fähigkeitslücke im Hinblick auf ein einzelnes System zu schliessen, müssen die Komponenten über alle zugänglichen Schnittstellen kontrolliert werden können. Als Schnittstelle gelten jegliche vom System für den Austausch von Daten oder Steuersignalen vorgesehenen Anschlüsse und Protokolle. Dies gilt sowohl für Software als auch für Hardware. Ein herausforderndes Thema dabei sind Möglichkeiten zum Austausch von Daten oder Steuersignale über andere Wege als die vorgesehenen Schnittstellen. Solche zusätzlichen Möglichkeiten werden unter dem Begriff der Seitenkanäle zusammengefasst. So kann beispielsweise ein vom Internet isoliertes System, welches via Supply-Chain kompromittiert wurde, durch gezielt verursachte Blinkmuster der Festplattenaktivitätslampe Daten an ein benachbartes System mit Kamera übermitteln. Neben vielen bereits bekannten und bezüglich Gefahrenpotenzial gut studierten Seitenkanälen gibt es insbesondere bei den heute aus mehreren Rechen- und Speichereinheiten bestehenden heterogenen Computersystemen auch neue Ansätze, um Seitenkanäle für Angriffe zu nutzen. Diese beruhen auf der gegenseitigen Beeinflussungsmöglichkeit der verschiedenen Bausteine. Bei funkbasierten Seitenkanälen können beispielsweise Systeme wie Gebäudeautomation oder Ladesysteme für Elektrofahrzeuge, welche über das Stromnetz miteinander kommunizieren, beeinflusst und angegriffen werden.

Die Angriffsmuster im Cyberraum werden immer ausgefeilter. Es ist daher notwendig, dass die Verteidigungsmassnahmen mit der fortscheitenden Entwicklung der Angriffsmuster Schritt halten. Im Zentrum stehen dabei weitere Verbesserungen von meist auf künstlicher Intelligenz basierenden Methoden zur Erkennung von Angriffen und der automatischen Reaktion auf diese. Eine besondere Herausforderung stellen hier die immer schneller werdenden Netzwerktechnologien, die Virtualisierung von Infrastruktur und deren Verschiebung in die Cloud dar. Traditionelle Verteidigungsansätze funktionieren in solchen Fällen nur noch bedingt, weil die grossen und rasch zu verarbeitenden Datenmengen diese nicht mehr zulassen oder die Kosten zu stark in die Höhe treiben würden. Ein weiteres Gebiet, welches im Bereich der Verteidigungsmassnahmen vermehrt in den Fokus der Forschung gerückt ist, befasst sich mit Tarn- und Täuschungstechnologien, wie beispielsweise die In-Network Moving Target Defense für 5G+. Dabei werden kontinuierlich Systemparameter und -topologien variiert, um Angreifer aus dem Tritt zu bringen. Dieses Gebiet ist aus militärischer Sicht interessant, da es sowohl für den Eigenschutz als auch für Aktionen im CER von Relevanz ist. Mittels Adversarial Artificial Intelligence und Zugriff auf ein vom Verteidiger eingesetztes, KI-basiertes Angriffserkennungssystem, kann ein Angreifer zum Beispiel Wege finden, einer Entdeckung zu entgehen. Oder alternativ kann das System dazu gebracht werden, bestimmte vom Angreifer verwendete Angriffsmuster nicht zu erkennen, sofern der Angreifer die Trainingsdaten für das vom Verteidiger eingesetzten System mindestens teilweise beeinflussen kann.

Cyber Lagebilder

Ein vollständiges Cyber-Lagebild ist entscheidend, um Risiken und konkrete Bedrohungen rechtzeitig zu erkennen, zu analysieren und angemessen darauf zu reagieren. Zu den zentralen Bausteinen bei der Erstellung von Cyber Lagebildern gehören Technologien und Methoden um Cyberrisiken in IKT Infrastrukturen zu erfassen, Daten mit verschiedenen Stellen und Partnern möglichst automatisiert, maschinenlesbar und ohne zu viel über sich selbst zu exponieren auszutauschen, im Cyberraum Open-Source-Intelligence

(OSINT) zu sammeln und die Informationen nutzbringend zu fusionieren.

Die genaue Kenntnis der eigenen IKT Infrastruktur ist eine unabdingbare Voraussetzung, um Cyberrisiken identifizieren zu können. Dabei müssen sämtliche Aspekte von der einsatzkritischen Anwendung bis hin zum einzelnen Gerät berücksichtigt werden. Wegen modernen Technologien wie Software Defined Networking, 5G+, IoT und Cloud werden IKT Infrastrukturen immer dynamischer und diverser. Durch die Verbesserung von Methoden und Technologien könnten die Bestandteile von IKT Infrastrukturen in Zukunft vollautomatisiert zu erfassen.

Im Bereich der Beschaffung von Daten für das Cyber Lagebild wird der Austausch und die Kooperation mit verschiedenen Stellen und Partnern immer wichtiger. Herausforderungen dabei sind insbesondere die wachsende Menge an Informationen und der Wunsch Informationen so zu teilen, dass ein möglichst grosser Nutzen entsteht, ohne jedoch gleichzeitig zu viel über sich selbst preiszugeben. Für den Umgang mit grossen Datenmengen stehen Technologien und Methoden im Zentrum, die helfen, beliebige Informationen zusammenzufassen und zur einfacheren Verarbeitung in strukturierte, maschinenlesbare Formate zu übersetzten. Die Fortschritte im Bereich der grossen Sprachmodelle lassen hier neuartige Lösungen erwarten. Beim Austausch von Informationen liegt der Fokus auf Lösungen, die sicherstellen, dass bei den geteilten Daten keine Daten enthalten sind, deren Austausch eine Datenschutzverletzung darstellt oder die anderwärtig problematisch sind. Verschiedene Technologien wie Homomorphe Verschlüsselung, Multi-Party Computation oder Confidential Computing haben hier das Potenzial weitere Hürden bezüglich Praxistauglichkeit zu nehmen und breiter einsetzbare Lösungen hervorzubringen.

Wenn es um die Einschätzung der Cyber-Bedrohungslage geht, sind neben Informationen von Partner insbesondere auch im Cyberraum gesammelte, öffentlich zugreifbare OSINT-Informationen hochrelevant. Während viele interessante Datenquellen und zugehörige Methoden zur Ableitung nützlicher Informationen bereits bekannt sind, gibt es ein grosses Potenzial für weitere Quellen und Methoden. Die Menge der Daten und die Anzahl der Dienste und Nutzungsarten des Cyberraums wachsen weiterhin stark. Aufgrund der hohen Dynamik der Entwicklungen im Cyberraum braucht es robuste Ansätze, um die Qualität und den Nutzwert der OSINT Daten zu beurteilen und längerfristig überwachen zu können. Um alle Informationen gewinnbringend zusammenzubringen, braucht es schliesslich geeignete Methoden und Technologien zur Fusion von Daten (vergleiche dazu Kapitel 3.3.3 Data Science und Lagebild).

Robuste und sichere Datenverarbeitung

Die Fähigkeit zur robusten und sicheren Datenverarbeitung und -verteilung ist für die Handlungsfähigkeit der Armee und der zu grossen Teilen digitalisierten Wirtschaft und Gesellschaft essenziell. Um dies zu erreichen ist es erforderlich, dass die Bestandteile und Technologien der IKT Infrastrukturen für sich selbst genommen robust und sicher sind und nicht auf zusätzliche Massnahmen und Technologien zur Erkennung und Bekämpfung von Sicherheitsproblemen angewiesen sind. Dies kann durch den Einsatz von Technologien erreicht werden, bei denen Sicherheit und Robustheit bereits beim Design berücksichtigt wurden oder die spezifisch für den Betrieb in feindlicher Umgebung gebaut wurden. Hier sind verschiedene relevante Entwicklungen zu beobachten wie Technologien für Kommunikationsnetze, die gegen Angriffe wie die Umleitung des Verkehrs über problematische Netzwerkpfade oder bestimmte Arten von Denial-of-Service Attacken robust und sicher sind.

Weitere Beispiele für relevante Entwicklungen finden sich im Bereich der Kryptografie und der Technologien zur Reduzierung der sogenannten Trusted Computing Base. Die Trusted Computing Base bezeichnet die Gesamtheit an Software und Hardware, der man vertrauen muss, um sicher zu sein, dass ein System oder eine Anwendung die erwarteten Sicherheitseigenschaften aufweist. Je kleiner die Trusted Computing Base, desto kleiner ist die Angriffsfläche von aussen und somit das Risiko, kompromittiert zu werden.

Im Bereich der sicheren Datenverarbeitung sind insbesondere Forschungsgebiete zu erwähnen, die sich aus der Entwicklung von Quantencomputern ergeben: die Quantum- und Post-Quantum-Kryptographie. Letztere erforscht Verschlüsselungs- und Signaturmethoden, die auch gegen Angreifer mit Quantencomputern sicher sind. Das disruptive Potenzial von Quantencomputern für das gesamte Internet macht ein genaues Verfolgen und Erforschen der Entwicklungen in diesem Bereich zwingend. Insbesondere müssen konkrete Risiken frühzeitig antizipiert werden, weil ein Nachrüsten mit Post-Quantum-Kryptographie in bestehenden (zivilen und militärischen) Systemen nicht

trivial ist und mehrere Jahre dafür eingeplant werden müssen. Erfolgen in dieser Zeit sprunghafte Entwicklungen, so öffnet sich für Angreifer ein nutzbares Zeitfenster.

In der Kryptographie sind zudem Fortschritte beim Thema Confidential Computing zu erwarten. Damit sind Technologien zusammengefasst, die es erlauben, auf nicht vertrauenswürdiger Hard- und Software, wie z.B. in der Public-Cloud, Daten zu speichern und zu verarbeiten. Basistechnologien wie Trusted Execution Environments, also sichere abgetrennte Umgebungen für die Ausführung von Programmen, oder neue Sicherheitsfunktionen in modernen Prozessoren tragen genauso dazu bei wie viele darauf aufsetzende Technologien. Mittels spezieller Methoden können sogar Berechnungen auf sensitiven Daten über mehrere Parteien hinweg durchgeführt werden, ohne dass die Daten für Drittparteien sichtbar werden. Dies ermöglicht Anwendungen, die bisher aufgrund von Datenschutzanforderungen unmöglich waren.

Neben diesen Bereichen sind aber auch in diversen weiteren Bereichen relevante Entwicklungen zu erwarten, beispielsweise bei hochsicheren Betriebssystemen, Technologien zur Verifikation von Sicherheitseigenschaften von Soft- und Hardware oder auch in Bezug auf neue, hochsichere Kommunikationsprotokolle.

Aktionen im Cyberraum

Der Krieg in der Ukraine zeigt, dass der Einsatz von Angriffsmitteln im Cyberraum für machtpolitische Zwecke bereits heute Standard ist. Die Störung der zivilen Telekommunikation und Energieversorgung erfolgt heute durch Aktionen, welche zwar vorwiegend im elektromagnetischen Raum, aber zunehmend auch im Cyberraum durchgeführt werden. Dabei gehören klassische Cyberangriffe ebenso zum Repertoire wie Attacken und Spionageaktionen mit Malware. Die Armee muss jederzeit in der Lage sein, solche Angriffe zu erkennen und ihre eigenen Systeme und Infrastrukturen zu schützen. Zur Abwehr von Cyberattacken können auch aktive Massnahmen eingesetzt werden. Die entsprechenden Mittel der Armee werden prioritär für den Eigenschutz eingesetzt. Die gesetzlichen Grundlagen zum Ausbau und Ergreifen aktiver Massnahmen und Gegenmassnahmen im Rahmen der Cyber-Defence ist im Nachrichtendienstgesetz und dem revidierten Militärgesetz geregelt.

Aufgrund der sich ständig und schnell weiterentwickelnden Technologiewelt, in der typische IKT Systeme alle fünf bis sechs Jahre erneuert werden, ist die Entwicklung und Nutzung der nötigen Fähigkeiten und Werkzeuge für Aktionen im Cyberraum eine grosse Herausforderung. Erschwerend kommt hinzu, dass ein Angriffswerkzeug von einem Moment auf den anderen seine Wirkung verlieren kann, beispielsweise wenn eine Schadsoftware von der Gegenseite entdeckt wird. Weiter kann die genutzte Sicherheitslücke auch durch reguläre Systempflege wie Updates bewusst oder durch Zufall aufgrund einer Änderung am System im betroffenen Bereich behoben werden.

Bei den Angriffswerkzeugen sind verschiedene Trends zu beobachten. Die Verwendung von Quantencomputern für Angriffe auf kryptographische Verfahren und radikale Fortschritte in der Nutzung künstlicher Intelligenz könnten auch in diesem Bereich zu disruptiven Veränderungen führen. Damit eine Schwachstelle für einen Angriff genutzt werden kann, muss ein sogenannter Exploit entwickelt werden. Dieser besteht meist aus einer spezifischen Abfolge von Befehlen und Datenstücken oder aus Programmcode. Die Entwicklung von Exploits ist oft mit sehr grossem personellem Aufwand verbunden. Die Situation wird durch die meist kurze Einsetzbarkeit eines solchen Exploits verschärft. Deshalb wird intensiv an der Automatisierung zur Entwicklung von Exploits gearbeitet.

Die Identifizierung von Schwachstellen bildet eine wesentliche Grundlage für Aktionen im Cyberraum. Die Methoden und Technologien, welche für den Cyberschutz erarbeitet werden, können folglich auch hier eingesetzt werden und umgekehrt. Im CER verhält es sich gleich wie in allen anderen Operationssphären: Wer den Schutz und die Gegenmassnahmen eines Gegners nicht kennt, kann die Wirkung seiner operativen Mittel nicht abschätzen. Wer die Wirkungsfähigkeit seines Opponenten nicht abschätzen kann, weiss nicht, wie er den Schutz seiner eigenen Mittel bewerten soll.

Forschungsthemen 2025-2028

CER Eigenschutz

- Weiterentwicklung der technisch-wissenschaftlichen Kompetenzen für den Eigenschutz im CER mit Hilfe von Sicherheitstechnologien zur Prävention, Detektion und Korrektur von schädlichen Cyberaktivitäten

- Erforschung, Weiterentwicklung und Evaluation von Methoden und Technologien zur Automatisierung des Einsatzes von eigenen Cyberkräften
- Erforschung und Evaluation von Methoden zum automatisierten Finden von Schwachstellen in eigenen und fremden Systemen
- Monitoring und Beurteilung von Lösungen für den Schutz von Systemen im Cyberraum auf der Basis von Künstlicher Intelligenz mit Schwerpunkt auf deren Robustheit im Anwendungsbereich
- Erforschung von Schwachstellen in Machine Learning Modellen und Methoden, um ihre Robustheit gegenüber Angriffen zu verbessern

Cyber Lagebilder

- Monitoring von neuartigen Angriffsvektoren und anderen Entwicklungen, die ausserordentliche Chancen und Gefahren für die Sicherheit im Cyberraum darstellen
- Entwicklung und Verbesserung von öffentlich verfügbaren Indikatoren (OSINT) sowie Aufbau des Wissens zur Beurteilung ihrer Qualität und des Nutzwerts
- Untersuchung und Weiterentwicklung von Technologien zum sicheren und datenschutzkonformen Austausch von Informationen zu Cyberangriffen sowie die Beurteilung der Sicherheit dieser Technologien

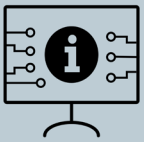
Robuste und sichere Datenverarbeitung

- Identifikation und Kompetenzaufbau zu neuen Sicherheits- und Privacy-Technologien wie beispielsweise Post-Quantum Kryptographie, Confidential Computing oder Quantum-basierte Technologien
- Erforschung und Potenzialbeurteilung von Hardware- und Softwarebasierter Isolationstechnologien, z.B. zur Nutzung mobiler Endgeräte oder Cloud-Infrastrukturen für Arbeiten mit unterschiedlichem Schutzbedarf
- Untersuchung und Beurteilung von Next-Generation-Netzwerktechnologien und Protokollen bezüglich Chancen, Risiken und Rahmenbedingungen für deren Einsatz

Aktionen im Cyberraum

- Erarbeitung von Methoden zur automatisierten Ausnutzung von Schwachstellen
- Erforschung neuartiger Angriffsvektoren und deren Wirkung, z.B. neuartige Denial-of-Service Vektoren
- Beobachten von internationalen Benchmarks und Standards zur Beurteilung der Effektivität von Angriffsvektoren
- Monitoring von neuen Methoden und Technologien zur Tarnung und Täuschung im Cyberraum
- Weiterentwicklung von Methoden und Technologien zur Automatisierung des Vorgehens von gegnerischen Cyberakteuren für Trainingssituationen von Blue Teams
- Untersuchung neuer Ansätze und Technologien zur Verteidigung von Cybersystemen durch eigene offensive Aktionen

3.2.3 Technologien zur Generierung von Informationsüberlegenheit



Ausgangslage und Problemstellung

In vielen Armeen spielen moderne Technologien eine zentrale Rolle bei der Implementierung eines durchgängigen und intelligenten SNFW. Das zeigen sowohl konventionelle Konflikte wie auch asymmetrische Szenarien der jüngsten Vergangenheit. Primär geht es darum, Sensordaten und nachrichtendienstlichen Informationen möglichst in Echtzeit zu einem stufengerechten und übersichtlichen Lagebild zu fusionieren, damit Operationen in einem Umfeld der Informationsüberlegenheit geführt und adäquate Wirkungen abgestimmt und zeitgerecht erzielt werden können. Neben der Beschleunigung der Befehlszyklen, von der Erfassung der Lage bis zur Analyse der erzielten Wirkung, ermöglichen moderne Technologien auch eine Verbesserung des Lageverständnisses, weil mehr Daten und Informationsquellen parallel und in höherer Qualität verarbeitet werden können. Die Verknüpfung von digitalen Lagebildern mit der Möglichkeit zur Simulation zugunsten der Operationsplanung und Befehlsgebung in einem Einsatzraum trägt zu einem optimalen Einsatz der zur Verfügung stehenden Mittel bei. Auf der anderen Seite müssen aber neue Herausforderungen in der Generierung der Informationsüberlegenheit im Rahmen des SNFW adressiert werden, etwa aufgrund von neuen intelligenten Möglichkeiten in der Tarnung, Täuschung und Störung, wie auch aufgrund von modernen Gegenmassnahmen im Cyber- und elektromagnetischen Raum.

Die Informationstechnologien haben einen starken Einfluss auf die Gesellschaft, die kontinuierlich neuen Informations- und Kommunikationstechnologien ausgesetzt ist. Insbesondere die Generation Z ist mit digitalen Technologien wie Internet, Smartphones und Tablets aufgewachsen. Die Gesellschaft insgesamt hat sich an die Technologieentwicklungen angepasst und verwendet die neuen Technologien im Alltag. Für die militärische Operationsführung ist es jedoch schwierig, einen hohen Vernetzungsgrad auch in aussergewöhnlichen Situationen mit den derzeitigen Standardmitteln effektiv zu erreichen

Der aktuelle Wandel führt zu einer neuen Art der Kommunikation und Information, bei der Fotos, Videos und Informationen sofort einem grossen globalen Publikum zugänglich gemacht werden. Dies beschleunigt den Informationsaustausch und weckt eine steigende Nachfrage nach Online-Daten, die für alle zugänglich sind. Nachrichtendienste nutzen seit jeher offene Quellen und vermehrt auch soziale Medien, um an Informationen zu gelangen (OSINT und SOCMINT). Die Nutzung dieser Quellen kann jedoch auch für missbräuchliche Zwecke verwendet werden, weshalb es so wichtig ist, Falschinformationen zu erkennen. Leider werden Fake News und manipulierte Videos immer raffinierter.

Digitalisierung, künstliche Intelligenz und Big Data haben sich deutlich weiterentwickelt und sind mittlerweile in der Zivilgesellschaft angekommen. Smartphones nutzen schon lange intelligente Algorithmen, um Fotos zu sortieren, Gesichter, Stimmen und Orte zu erkennen und Texte vorherzusagen. Dennoch ist die KI noch nicht in allen Anwendungsbereichen, insbesondere in militärischen Systemen, vollends erfolgreich. Das liegt an der grossen Anzahl benötigter klassifizierter Referenzdaten, den komplexen Anwendungen und der Verwundbarkeit von KI gegenüber feindlicher Angriffe, sogenannter Adversarial Attacks.

Solange viele KI-Anwendungen zu Resultaten führen, welche bestenfalls plausibilisiert, aber oft nicht im Detail erklärbar und auch nicht nachvollziehbar sind, gibt es im militärischen Bereich eine gewisse Zurückhaltung solche einzusetzen. Dies ist durchaus verständlich, zumal sich die Tragweite der Entscheidungen wesentlich von zivilen Anwendungen unterscheiden kann. Es sei aber ebenso bemerkt, dass intuitiv gefällte Entscheide durchaus auch unter dem Mangel zur Nachvollziehbarkeit leiden können. Die Grenzen der KI müssen in Zukunft kritisch beleuchtet werden. Dennoch sind die Automatisierung in militärischen Systemen auf der Grundlage des OODA-Zyklus (Observe, Orient, Decide, Act) und die Beschleunigung der Informationsgewinnung unumkehrbare Trends. In den kommenden Jahren sind erhebliche Verbesserungen zu erwarten.

Neben den Trends zu KI und Big Data ist in der Gesellschaft auch der Trend zu lokalen intelligenten Lösungen zu beobachten. Tragbare Sensoren, sogenannte Wearables, messen Körperfunktionen und führen lokale Auswertungen durch. IoT-Geräte und IoT-Netzwerke gewinnen zunehmend an Bedeutung. Diese Geräte erfassen nicht nur ihre Umgebung, sondern verarbeiten die Messwerte lokal und senden die Ergebnisse stark komprimiert über mobile Kommunikation weiter. Da oft viele Geräte in einem Netzwerk verbunden sind, wird auch von Maschine-zu-Maschine-Kommunikation gesprochen. Die lokale Intelligenz, auch Edge Intelligence genannt, ist ein unübersehbarer Trend. Im militärischen Bereich wecken Edge Intelligence und IoT-Netzwerke ebenfalls Interesse. Es müssen jedoch spezielle Anforderungen hinsichtlich Robustheit, Sicherheit, Störresistenz und Resilienz im militärischen Umfeld erfüllt werden, da zivile IoT-Netzwerke diese Anforderungen nicht vollständig erfüllen.

Aufklärung und Überwachung

Um eine Informationsüberlegenheit zu erreichen, ist eine zielgerichtete und zeitnahe Informationsgewinnung entscheidend. Aufklärung und Überwachung sind eine wichtige Quelle, um den Informationsfluss zwischen Sensoren, Entscheidungsträgern und Effektoren anzustossen. Verschiedene Informationsquellen wie Menschen (HUMINT), Bild- (IMINT), Signal- (SIGINT), Radar- (RADINT), raumbezogene- (GEOINT), mess- und signatur-technische (MASINT) sowie elektrooptische (VISINT) Aufklärung werden dazu genutzt. Multisensorsysteme, intelligente Auswerteverfahren und Sensordatenfusion spielen bei der Verarbeitung der Informationen eine zentrale Rolle. Dank der Digitalisierung von Sensordaten und der steigenden Prozessorleistung sind Echtzeitanwendungen und intelligente Vorauswertungen in hoher Qualität möglich. Diese Entwicklung ermöglicht die automatisierte Verarbeitung von Sensordaten zu Aufklärungs- und Überwachungsinformationen direkt auf der Einsatzplattform. Damit können Plattformen sowohl für Aufklärungs- als auch für Überwachungsaufgaben ausgelegt werden. Was zur Kosten- und Personaleinsparung beitragen kann. Die zeitnahe Gewinnung und Aufbereitung von Informationen sowie die Erstellung aktueller Lagebilder werden dadurch erleichtert.

Um die Informationsüberlegenheit im Rahmen einer vernetzten Operationsführung zu gewährleisten, werden auf internationaler Ebene enorme finanzielle Mittel in die Erforschung und Entwicklung moderner Detektions- und Aufklärungstechnologien investiert. In diesem Zusammenhang ist auch zu beobachten, dass weiterhin grosse Anstrengungen im Bereich des elektronischen Kampfes (Electronic Warfare) unternommen werden. So sind zunehmend intelligente Täuschungs- und Störungsmassnahmen sowie Gegenmassnahmen im elektromagnetischen Raum zu beobachten.

Die Menge und Qualität digitaler Sensordaten hat sowohl im militärischen als auch im zivilen Bereich erheblich zugenommen. Im zivilen Bereich liegt der Schwerpunkt in erster Linie auf der Entwicklung preiswerter Sensoren für kurze und mittlere Reichweiten, wie z. B. Radargeräte für Autos oder Sensoren für Smartphones. Der heute wohl am weitesten verbreitete Sensortyp ist das Kamerasystem. Die Verbesserung der Auflösung erhöht die Detailgenauigkeit und den Informationsgehalt der Fotos, aber auch die Datenmenge und den Speicherbedarf. Die fortschreitende Miniaturisierung der Sensoren und ihr reduzierter Energieverbrauch tragen dazu bei, dass Daten von jedermann, zu jeder Zeit, an jedem Ort und auf jedem Medium wie Minidrohnen aufgezeichnet werden können und dass sie miteinander kommunizieren (IoT). Daher ist die Erkennung von Bedrohungen durch Mini- und Mikrodrohnen heute sowohl für zivile als auch für militärische Sicherheitskräfte von Bedeutung. Der Markt bietet eher preiswerte Systeme zur Drohnenerkennung für private Sicherheitsfirmen sowie umfangreiche und hochentwickelte Systeme für militärische Anwender.

Die Miniaturisierung der Satelliten ermöglicht es Unternehmen, neue Satellitenprodukte mit doppeltem Verwendungszweck, hohem Informationsgehalt und guter zeitlicher Auflösung anzubieten. Es ist heute möglich, spezielle Satellitenbilder, insbesondere hochauflösende visuelle und Radarbilder von Konfliktgebieten, kommerziell zu erwerben. Früher waren diese Bilder den Geheimdiensten vorbehalten, doch nun sind sie der Öffentlichkeit zugänglich. Westliche Medien und Institute für öffentliche Sicherheit haben diese Bilder genutzt, um die jüngsten Konflikte zu analysieren und zu dokumentieren. Obwohl die Qualität der Bilder von Kleinsatelliten nicht mit derjenigen von Spionagesatelliten vergleichbar ist, enthalten sie dennoch wichtige Informationen. Diese Entwicklung spielt daher eine entscheidende Rolle für alle Akteure, die an der Informationsgewinnung aus Satellitenbildern beteiligt sind.

Informationsgewinnung, Aufklärung und Überwachung lassen sich nicht auf einfache technische Fragen reduzieren. Neben der Verfügbarkeit und Vernetzung technischer Systeme spielen Faktoren wie organisatorische und kulturelle Merkmale sowie doktrinäre Richtlinien eine entscheidende Rolle bei der Verarbeitung von Informationen, insbesondere bei multinationalen Operationen. In einem militärischen Kontext sind Aufklärung und Überwachung entscheidend für die Beschaffung von Informationen und die Erlangung von Informationsüberlegenheit gegenüber gegnerischen Kräften.

Kommunikation

Kommunikationssysteme vernetzen die Daten- und Informationsquellen mit den Entscheidungsträgern und Effektoren und müssen jederzeit zur Verfügung stehen. Sie bilden somit das Rückgrat des Gesamtsystems der Armee und ermöglichen den Einsatz von Führungs- und Informationssystemen, sowohl im militärischen als auch im zivilen Bereich. Eine sichere, robuste, echtzeitfähige und mobile Übertragung von Daten wie Sprache, Bildern und Text ohne ungewollte Medienbrüche sind wesentliche Voraussetzungen für die Durchführung erfolgreicher Einsätze. Heterogene Kommunikationsnetze sind bei vernetzten Einsätzen von grösster Bedeutung, da keine Technologie allein alle Anforderungen erfüllen kann. Die Interoperabilität zwischen den eigenen Kommunikationssystemen und denen der Partner ist von entscheidender Bedeutung. Die Entwicklungstrends im Bereich der Informations- und Kommunikationstechnologien (IKT) werden vor allem durch die Nachfrage nach der Übertragung grosser Datenmengen auf den zivilen Märkten bestimmt. Dies führt zu einem steigenden Bedarf an Bandbreite, so dass die Mobilfunkbetreiber ihre Netze ständig erweitern und mit den neuesten Technologien ausstatten müssen. Derzeit investieren die zivilen Telekommunikationsanbieter in den Aufbau des 5G-Mobilfunknetzes, um die Voraussetzungen für intelligente Anwendungen in der Wirtschaft, im Privatsektor und in der öffentlichen Verwaltung zu schaffen. Auch die Diskussionen über die Möglichkeiten von 6G haben bereits begonnen.

Die Sicherheitskräfte haben spezifische Anforderungen an die Ausfallsicherheit des Netzes und die Vermeidung von Störungen. Dabei steht im militärischen Umfeld die Robustheit der eigenen Kommunikations-

mittel gegen Störaktionen im elektromagnetischen Raum im Zentrum, weil dadurch der SNFW sowohl zeitlich als auch qualitativ eingeschränkt würde. Diese Härtung der Systeme, aber auch den Schutz vor unberechtigtem Zugriff auf Informationen wird oftmals von zivilen Anbietern nicht ausreichend berücksichtigt. Daher müssen die Sicherheitskräfte ihre eigenen spezifischen Lösungen entwickeln, was höhere Kosten und eine längere Entwicklungszeit mit sich bringt. Es ist aber wichtig, mit den Trends Schritt zu halten und die Konnektivität zwischen militärischen und zivilen Kommunikationsanwendungen zu gewährleisten.

Der Trend, immer grössere Daten- und Informationsmengen zu übertragen und damit immer grössere Bandbreiten zu beanspruchen, wird den Druck erhöhen, Frequenzbänder, welche heute für Anwendungen im Sicherheitsbereich reserviert sind, für die zivile Nutzung zugänglich zu machen. Es gilt also die vorhandenen Frequenzressourcen möglichst effizient zu nutzen. Mit modernen Funktechnologien wie Software Defined Radio (SDR) und Cognitive Radio ist es möglich, die Wellenform und damit die räumliche Ausbreitung, die Frequenz sowie die benötigte Bandbreite der Belegung des elektromagnetischen Raums anzupassen und auf den Bedarf der Informationsübermittlung zu optimieren. So können Netzwerke für Sicherheitskräfte nicht nur flexibler und zugleich robuster aufgebaut, sondern auch leistungsfähiger betrieben werden. Zudem ist es dank künstlicher Intelligenz möglich, das Routing von Daten und somit den Datenfluss zu optimieren. Die Übertragung grosser Datenmengen werden auch im militärischen Bereich den Betrieb zellulärer Netzwerke erfordern. Dabei ermöglicht vor allem die Technologie aus dem zivilen Mobilfunk die Nutzung verteilter Rechenleistung innerhalb von lokalen Netzwerken, welche über semi-mobile Knoten an Hochleistungsinfrastruktur angebunden werden können. Damit werden rückwärtig generierte Dienste wie beispielsweise Bilderkennung, Übersetzungsleistungen oder die Identifikation von gegnerischen Systemen vor Ort verfügbar.

Durch die zunehmende Leistungsfähigkeit und Miniaturisierung werden Funkgeräte immer vielseitiger einsetzbar. Funksignale werden digitalisiert und können dadurch auf beliebige Art und Weise verarbeitet werden. Dies eröffnet die Möglichkeit, neben den klassischen Kommunikationsdiensten auch andere Fähigkeiten wie Aufklärung im elektromagnetischen Raum auf der gleichen Plattform zu integrieren. Dies wird in Zukunft nicht nur die Integration unterschiedlicher Anwendungen vereinfachen, sondern auch einen massiven Fähigkeitszuwachs generieren.

Data Science und Lagebild

Die Allgegenwärtigkeit von Daten in unserer Gesellschaft in Kombination mit den aktuellen technologischen Fortschritten hat dazu geführt, dass digitale Daten in grossem Umfang generiert und ausgetauscht werden. Diese Daten gelten als Goldgruben, da sie es Marketing- und Internetunternehmen ermöglichen, durch die Optimierung von Prozessen neue Umsatzmodelle zu schaffen und Kunden effektiver anzusprechen. Algorithmen des maschinellen Lernens werden eingesetzt, um diese Daten zu analysieren und zu nutzen, indem sie ähnliche Profile gruppieren, Daten klassifizieren oder zeitliche Trends vorhersagen.

Diese Art der Datenauswertung ist nicht nur der zivilen Welt vorbehalten. Auch die Armee und andere staatliche Institutionen, insbesondere der Nachrichtendienst des Bundes (NDB), die Nationale Alarmzentrale (NAZ) und das Bundesamt für Polizei (fedpol), können Daten nutzen, die sie selbst produzieren oder über verschiedene Kanäle erhalten haben. Es kann auch ein Trend zur Zusammenführung von Daten aus verschiedenen Quellen beobachtet werden, sowohl aus internen als auch aus freien Quellen. Durch den Einsatz intelligenter Algorithmen können je nach betrieblicher Aufgabe unterschiedliche Produkte erstellt werden.

Ein Lagebild ist ein Instrument, das ausgewertete Nachrichten zu Informationen zusammenfasst, mit dem Ziel, den Entscheidungsträgern ein übersichtliches Bild der aktuellen Lage in einem bestimmten Interessensraum zu vermitteln. Dabei können sowohl militärische als auch öffentliche Nachrichtenquellen genutzt werden. Ein kombiniertes Lagebild ermöglicht ein gemeinsames Verständnis der Situation und ein koordiniertes Handeln zwischen den verschiedenen Stellen. Durch den Einsatz von künstlicher Intelligenz ist es möglich, solche Lagebilder für die verschiedenen Operationssphären automatisch zu erzeugen und zu konsolidieren. Ein aktuelles, vollständiges, stufengerechtes und übersichtliches Lagebild ist die Basis für fundierte Führungsentscheide und spielt daher als Führungsinstrument eine Schlüsselrolle.

Auf taktischer Ebene ist es wichtig, schnell auf Bedrohungen zu reagieren. Bilder und Informationen aus beliebigen Quellen wie Aufklärungssystemen, Drohnen und Satelliten müssen automatisch und in Echtzeit analysiert werden. Dabei sind KI-Algorithmen von ent-

scheidender Bedeutung, um Objekte, Personen, Fahrzeuge oder Bedrohungen zu identifizieren. Darüber hinaus können diese Algorithmen eine entscheidende Hilfe bei der Identifizierung und Einordnung von Bildern aus dem Internet oder sozialen Netzwerken sein, die wichtige Informationen über Gegner enthalten. Künstliche Intelligenz findet aber auch in vielen anderen Anwendungsmöglichkeiten ihren Nutzen. Dazu ist die KI auf vielen Ebenen präsent, sei es zentral, aber auch auf Sensoren, insbesondere zur Automatisierung von sich wiederholenden oder langwierigen Aufgaben.

Die Informationen, die entweder vor Ort oder aus anderen Quellen gesammelt werden, sind oft in fremden Sprachen oder sogar Dialekten verfasst. Herkömmliche Übersetzungssysteme können nicht als sicher angesehen werden und sind nicht in der Lage, Dialekte zu übersetzen. Um die Analysten zu unterstützen, müssen ihnen Übersetzungssysteme zur Verfügung gestellt werden, die den Kontext berücksichtigen. Auch hier werden die Entwicklungen bei maschinellen Übersetzungssystemen neue Möglichkeiten bieten, Texte zu integrieren, die bislang von Spezialisten übersetzt werden mussten.

In der Zukunft ist es absehbar, dass viele taktische oder operative Systeme auf künstlicher Intelligenz beruhen werden. Obwohl dies viele Vorteile bieten kann, ist ihr Einsatz auch mit Risiken verbunden. Weil Deep-Learning-Modelle immer komplexer werden, ist es nicht mehr möglich, deren Entscheidungen zu interpretieren oder zu begründen, sprich die Nachvollziehbarkeit ist meistens nicht mehr gegeben. Dies kann ein ethisches Problem darstellen, insbesondere bei Anwendungen zur Steuerung von Effektoren. Deep-Learning-Algorithmen können durchaus beeinflusst und damit angegriffen werden, indem man beispielsweise bei der Optimierung eines neuronalen Netzwerkes unvollständige Trainings-Datensätze verwendet und dadurch das Erkennen bestimmter Muster verhindert oder indem man die Zielfunktion manipuliert. In Zukunft wird es notwendig sein, die Sicherheitsaspekte bei der Nutzung künstlicher Intelligenz zu berücksichtigen und sicherzustellen, dass sie, wie jedes andere Computersystem auch, robust gegen Angriffe geschützt ist.

Forschungsthemen 2025-2028

Luftraumüberwachung der Zukunft

- Entwicklung neuer Ansätze und Methoden für kognitive, multifunktionale und multistatische Radarsysteme
- Untersuchung des Einflusses von komplexen Umgebungen wie Windkraftanlagen, Solarparks oder urbane Umgebungen auf die Radarzielerkennung sowie Bestimmung von Gegenmassnahmen bei Störungen
- Beurteilung von Herausforderungen und Chancen bei der Kombination von Radar- und Kommunikationsanwendungen
- Untersuchung der Technologien zur Erkennung, Verfolgung und Identifikation von Drohnen und Drohnenschwärmern in komplexer Umgebung auf der Basis von Multi-Sensorik und Multi-Plattformen
- Untersuchen von Verfahren für die Nutzung von Kommunikationssendern als Beleuchter für Passivradaranwendungen

Bildaufklärung

- Potenzialabschätzung und Untersuchung von hyperspektraler Sensorik sowohl für grossräumige Bildaufklärung als auch für die Aufklärung eines kleinen Perimeters
- Beurteilung und Untersuchung von neuen Optionen und Trends für die wetterunabhängige Bildaufklärung durch Synthetic Aperture Radare (SAR) auf Drohnen, bemannten Flugzeugen und Satelliten
- Entwicklung und Beurteilung von neuen Methoden für die adaptive Tarnung
- Beurteilung von Methoden mit künstlicher Intelligenz zur Aufklärung von Tarnmassnahmen im visuellen und infraroten Spektrum
- Untersuchung neuer Ansätze für die Generierung von 3D-Szenen auf der Basis von Radar- und elektrooptischen Sensoren
- Prüfung des Einflusses von Wetter und Saison auf Objekterkennungsmodelle

Künftige Aufklärungssensorik

- Technologiemonitoring im Bereich Quantum-Sensorik, insbesondere zu Quantenbildgebung auf der Basis von Lasern und speziellen Photon-Detektoren
- Monitoring von Sensortechnologien, um Objekte auch bei nicht direkter Sichtverbindung zu erkennen

- Weiterentwicklung und Beurteilung von Methoden und Sensoren zur Erkennung von bewegten Zielen
- Erforschung von Entwicklungen im Bereich IoT, im Speziellen deren Potenzial für verteilte und energieeffiziente Sensorik mit lokaler Intelligenz
- Weiterentwicklung von Sensoren und Methoden zur Detektion von biologischen, chemischen und nuklearen resp. radiologischen Gefahren

Integrierte Kommunikations-Netzwerke

- Entwicklung und Implementierung von Modellen für die Simulation von Kommunikationsnetzwerken für die Beurteilung von Leistungsgrenzen
- Untersuchen von Software Defined Radio Verfahren für moderne, komplexe Wellenformen und kognitive Kommunikationsansätze
- Technologiemonitoring von IoT Netzwerktechnologien und Erarbeiten von Anwendungsfällen und Demonstratoren für die Armee
- Verbesserung der spektralen und räumlichen Effizienz von Funksystemen durch intelligente Antennensysteme
- Evaluation von Technologiefortschritten in der photonischen Signalbearbeitung und Erzeugung sowie Entwicklung von Demonstratoren für Kommunikations- und Radaranwendungen
- Entwicklung und Evaluation von Methoden der Zeitsynchronisation in Sensornetzwerken, um die Abhängigkeit von Satellitennavigationssystemen zu verringern
- Verbesserung und Weiterentwicklung von Electronic Warfare Verfahren für die Aufklärung und Wirkung im elektromagnetischen Raum

Sensor-Effektor-Loop

- Verbesserung der Automatisierung von Aufklärung und Lagebeurteilung im OODA Loop, um Entscheidungsgrundlagen schneller zur Verfügung zu haben
- Entwickeln von Konzepten für die Integration von Simulation für die Entscheidungsunterstützung unter der Berücksichtigung von menschlichen Faktoren
- Abklärung der ethischen Fragestellungen bei der Verwendung von automatisierten Sensor-Effektor-Loops
- Integration von Command and Control (C2) Systemen mit Wargaming Ansätzen für das Trainieren und Testen in Truppen

Data Science und Künstliche Intelligenz zur Darstellung von Lagebildern

- Erforschung und Optimierung von Algorithmen, um multimodale Daten für die Erstellung von Lagebildern zu fusionieren
- Entwicklung von Algorithmen für Texterkennungs- und Übersetzungsaufgaben
- Identifikation und Verifizierung von Open Source und Dark Web Datenquellen und Entwicklung von Algorithmen zur Fusion von Daten, um ein Lagebild zu erstellen
- Beurteilung und Entwicklung von Big Data Architekturen für verschiedene Datentypen und Anwendungen
- Erforschung und Beurteilung von Hybrid-Cloud Lösungen, um Speicher dynamisch aufzuteilen
- Erforschung von Privacy-Mechanismen, um Daten und Algorithmen anhand ihrer Klassifizierung entweder lokal oder in der Cloud Infrastruktur automatisch zu verteilen

Informationsüberlegenheit und Künstliche Intelligenz

- Aufbau der Kompetenz, um die Robustheit von Machine Learning Modellen automatisch zu überprüfen
- Entwicklung von Kriterien für die Beurteilung der Grenzen und Sicherheit von KI-basierten Systemen
- Erforschung von Methoden zur Erklärbarkeit von verschiedenen Machine Learning Modellen
- Identifikation der ethischen Herausforderungen bei der Anwendung von künstlicher Intelligenz
- Identifikation und Verfolgung der zukünftigen Entwicklungen und potenziellen Anwendungen von generativen, Zero-Shot Learning und Large Language Modellen (GPT)

3.3 Technologieintegration zu Plattformen

3.3.1 Autonomie und Robotik

Ausgangslage und Problemstellung

Auf internationaler Ebene ist die Forschung im Bereich der Robotik resp. unbemannten Systemen zu einer Priorität geworden, im zivilen wie auch im militärischen Sektor. Die Hauptziele des Einsatzes von Robotik sind vielfältig. Sie umfassen in erster Linie die Steigerung der Effektivität und Effizienz bei der Ausführung bestimmter Aufgaben, die Entlastung von Menschen von repetitiven, langweiligen und ermüdenden Aufgaben und das Fernhalten von Menschen aus gefährlichen und bedrohlichen Umgebungen. Somit können Roboter dazu dienen, sowohl die Produktivität und die Arbeitsqualität zu erhöhen als auch Leben zu schützen. Das entsprechende Einsatzspektrum ist sehr breit und umfasst fast alle Operationssphären. Unbemannte Luftfahrzeuge können beispielsweise für die Aufklärung, Überwachung oder Kommunikationsunterstützung eingesetzt werden, Bodenfahrzeuge für Bergung, Evakuation oder Logistik. Aber auch im Bereich von Ausbildung, Wartung und Instandhaltung lassen sich sinnvolle Aufgaben für zukünftige Roboter finden.

Generell beruht im Bereich der unbemannten Systeme die Geschwindigkeit leistungsfähiger Entwicklungen auf Systemkompetenzen, die eine geschickte Integration von kommerziellen Komponenten von der Stange (COTS) und militärischen Komponenten von der Stange (MOTS) ermöglichen. Die Bereitstellung leistungsfähiger autonomer Systeme hängt wesentlich von Fortschritten bei den sogenannten Enabler-Technologien ab, wie Sensoren-, Rechner- oder Kommunikationstechnologien oder Fortschritten im Bereich von Antrieb, Navigation, Energiespeicherung oder Mensch-Maschine- und Maschine-Maschine-Schnittstellen. Vor allem die Fortschritte der künstlichen Intelligenz der letzten Jahre zeigen, dass Roboter für immer schwierigere Aufgaben und Umgebungen zunehmend unabhängig vom Menschen eingesetzt werden können.

Dennoch hängt der Einsatz unbemannter Systeme nicht nur von technischen Aspekten ab, sondern auch von einer Vielzahl sozialer, legislativer und ethischer Faktoren wie dem Vertrauen und der Akzeptanz der Nutzer und der Gesellschaft in diese Systeme, der Entwicklung der nationalen und internationalen Rechtslage oder von ethisch-moralischen Debatten.

Bei zivilen und militärischen Behörden und Organisationen mit Sicherheitsaufgaben nimmt der Stellenwert der Robotik zu. In bewaffneten Konflikten besetzen Drohnen und Roboter eine immer wichtigere Rolle, sowohl bei staatlichen als auch bei nichtstaatlichen Akteuren. Die begrenzten Bestände an teuren ausgebildeten Soldaten und Spezialisten sowie der Druck durch die Werte unserer Gesellschaft erfordern militärische Operationen, deren Risiken weitgehend minimiert werden. Der Einsatz von unbemannten Systemen ist daher eine Selbstverständlichkeit. Bisher wurden unbemannte Plattformen meist aus der Ferne, aus einer hinteren Position und mit hohem Personalaufwand eingesetzt. Die Fortschritte bei eingebetteten Systemen mit Algorithmen der KI ermöglichen jedoch eine zunehmende Autonomie unbemannter Plattformen. Darüber hinaus ermöglichen die neuen Fähigkeiten zur Durchführung von Langzeitmissionen eine deutliche Erweiterung der möglichen Missionstypen für diese autonomen Systeme. Es ist daher absehbar, dass unbemannte Systeme als Plattformen in einem sehr breiten Spektrum operationeller Fähigkeiten eingesetzt werden, insbesondere überall dort, wo Soldaten oder Zivilisten sehr grossen Gefahren

ausgesetzt werden müssten oder wo die Ermüdung der Besatzung aufgrund der Dauer eines Einsatzes zu einem Problem werden würde. Dennoch sind für eine optimale Einsatzleistung mehrere Voraussetzungen erforderlich. Erstens bedarf es intuitiver Benutzeroberflächen, welche die Bedienung durch den Anwender erleichtern. Zweitens muss sowohl eine weitgehende technische Interoperabilität mit der bestehenden Systemumgebung als auch eine nahtlose Integration in die Prozesse der Sicherheitskräfte gewährleistet sein. Um neue taktische Aspekte in operativen Einsatzkonzepten zu nutzen, ist es zwingend notwendig, die Zusammenarbeit von Mensch und Maschine doktrinell abzustützen.

Die technologischen Fortschritte bei unbemannten Systemen sind bei Aufklärungs- und Überwachungsoperationen von Vorteil, erweisen sich aber aus Sicht der Bedrohungslage als Nachteil. Ein typisches Beispiel, das oft unterschätzt wurde, sind Low-Tech-Mikro- und Minidrohnen. Die hohe Verfügbarkeit, die relativ niedrigen Kosten, die minimalen logistischen Hürden und der Betrieb ohne teure Infrastruktur machen ihren Einsatz selbst in asymmetrischen Szenarien oder auf Eskalationsstufen unterhalb der Kriegsschwelle wahrscheinlich. In diesem Zusammenhang erfordert ihr Einsatz durch gegnerische Kräfte die Einführung von Schutzmassnahmen und Gegenmassnahmen, um Soldaten, teure Systeme und kritische Infrastrukturen zu schützen. Es muss daher vertieft darüber nachgedacht werden, wie mit bewaffneten oder unbewaffneten gegnerischen Systemen umgegangen werden kann. Unbemannte Systeme stellen aufgrund ihres Potenzials verschiedene Bedrohungen dar, deren Auswirkungen heute noch nicht abschliessend beurteilt werden können. Dies stellt Sicherheitskräfte künftig vor grosse Herausforderungen, welche teilweise ein Umdenken erfordern werden.

In den letzten Jahren haben vor allem die zivilen Märkte die Entwicklung von Drohnen und Robotern bestimmt. Sie sehen in diesen Systemen eine Möglichkeit, neuartige Dienstleistungen zu erbringen oder bestehende Dienstleistungen zu optimieren. So werden die ersten autonomen Stadttaxis für Personen angeboten, Pakete und Waren von autonomen Drohnen transportiert oder Industrieanlagen inspiziert und überwacht. Selbst in höheren Lufträumen werden sich fliegende Plattformen aufgrund der günstigen Bedingungen und reduzierten Vorschriften bewegen und als kostengünstiger Ersatz für Satelliten in der Stratosphäre eingesetzt werden können. Durch die Vernetzung mehrerer solcher Höhenplattformen (HAP) könnten beispielsweise auch in infrastrukturschwachen und schwer zugänglichen Regionen schnell Kommunikationsnetze aufgebaut und über einen längeren Zeitraum betrieben werden.

Die Nutzung unbemannter militärischer Flugsysteme der HALE- und MALE-Klasse in dafür ausgeschiedenen Lufträumen ist nicht neu. Neu ist jedoch, diese mit einer ausgebauten Autonomie in zivil genutzte Lufträume zu integrieren, so wie dies künftig auch in der kommerziellen Aviatik der Fall sein wird. Die Militarisierung von Mikro- und Minidrohnen hat in der Tat ebenfalls bereits begonnen und zukünftige Entwicklungen sind nur eine Frage der Zeit. Forschungsresultate im Bereich der Kampfdrohnen sind ein perfektes Beispiel dafür, wie technologische Entwicklungen aus dem zivilen Bereich genutzt werden, um die Leistungsfähigkeit militärischer Systeme zu verbessern. Die fortschreitende Miniaturisierung elektronischer Komponenten und Steigerung der Leistungsfähigkeit von Antrieben führen zu höherer Agilität, längeren Einsatzzeiten und mehr Autonomie. Es ist absehbar, dass es zu gemischten Einsätzen von Menschen und Maschinen kommen wird, bei der in einer einfachen Version der Kopilot eines Hubschraubers eine Drohne steuert. Auch der Einzug von hochautomatischen Einwegdrohnen, sogenannter Loitering Munition, für präzise Wirkung auf mittlere oder grössere Distanz hat markant zugenommen.

Wie bei den unbemannten Flugsystemen sind auch bei der autonomen Mobilität am Boden die zivilen Forschungseinrichtungen und Märkte die treibende Kraft. Schon heute sind Fahrerassistenzsysteme die Vorboten zukünftiger autonomer Systeme auf der Strasse. Obwohl einige autonome Strassenfahrzeuge bereits testweise zugelassen sind, ist mit einer flächendeckenden Einführung nicht zu rechnen, bevor die rechtlichen Aspekte geklärt sind. Selbstfahrende Strassenfahrzeuge können für die Streitkräfte nützlich sein, die militärischen Anforderungen stellen jedoch zusätzliche Herausforderungen dar. So können Strassen mit Hindernissen blockiert oder zerstört sein und die Verwendung von Sensoren kann von elektronischen Gegenmassnahmen des Gegners erkannt oder gestört werden. Die militärische Härtung von autonomen Landsystemen führt zu erheblichen Mehrkosten und Verzögerungen bei der Einführung.

Im militärischen Bereich bieten unbemannte Bodenfahrzeuge die Möglichkeit, die Gefahrenexposition

der Sicherheitskräfte zu verringern, z. B. bei der Neutralisierung von Bomben und Munition, beim Aufspüren und Räumen von Minen, bei der Aufklärung in städtischen Gebieten und in nicht direkt einsehbaren Räumen, beim Transport von Verletzten und Versorgungsgütern in gefährlichen Gebieten und bei der Aufklärung in mit ABC-Agenzien kontaminierten Gebieten. Letztendlich steht fest, dass die Mobilität am Boden noch sehr grosse Fortschritte machen wird, vor allem in zwei Hauptbereichen. Der erste betrifft die Art der Fortbewegung. So werden die klassischen Konzepte des Rad- und Raupenantriebs weiterentwickelt und durch Hybrid- oder Elektroantriebe und neue Regelalgorithmen ergänzt werden. Diese neuen Technologien führen zu taktischen Vorteilen, beispielsweise durch eine Reduktion der akustischen Signatur oder durch eine Erhöhung der Geländegängigkeit. Der zweite Bereich bezieht sich auf neuartige Antriebskonzepte, beispielsweise inspiriert durch die Natur. Tatsächlich hat sich die Fortbewegung mit Beinen in den letzten Jahren enorm weiterentwickelt und verdrängt die traditionellen Konzepte der kleineren Fahrzeuge unter 50 kg mit Rädern oder Raupen, insbesondere in unwegsamen, über- oder unterirdischen, natürlichen oder künstlichen Umgebungen.

Forschungsthemen 2025-2028

Unbemannte Vehikel

- Untersuchung der technischen Möglichkeiten zum Einsatz von unbemannten Vehikeln in den verschiedenen Operationssphären, prioritär den Sphären Luft und Boden
- Aufzeigen der Potenziale von neuartigen Konzepten zur Fortbewegung in der Luft, am Boden und im Wasser
- Aufbau der Kompetenz zur Beurteilung des Einflusses eines modernen Gefechtsfeldes auf den Einsatz der unbemannten Vehikel, beispielsweise zur Beurteilung der Methoden zur Lokalisierung in GNSS-degradierter Umgebung
- Erforschung von missionsrelevanten Nutzlasten und deren Integration in unbemannte Plattformen
- Abschätzung der Auswirkungen von Entwicklungen in Schlüsseltechnologien hinsichtlich der Erweiterung der Fähigkeiten von unbemannten Systemen

Mensch-Maschine & Autonomie

- Identifizieren der Möglichkeiten zur optimalen Interaktion und dem Teaming zwischen Menschen und unbemannten Vehikeln
- Untersuchung von neuartigen Benutzerschnittstellen, z.B. durch Augmented Reality, und Aufzeigen von deren Vor- und Nachteilen
- Erforschung von verschiedenen Aspekten in Mehrroboter-Systemen, von Kooperation und Kollaboration bis hin zu Swarming und Interoperabilität
- Untersuchung der Nutzung von künstlicher Intelligenz zur Optimierung der Autonomie und Fähigkeiten

Integration in die militärische Anwendung

- Aufzeigen der Möglichkeiten sowie der Chancen und Gefahren des zukünftigen militärischen Einsatzes von unbemannten Vehikeln
- Untersuchung der Herausforderungen des Einsatzes von unbemannten Vehikeln, von der normalen Lage bis zum hochintensiven modernen Konflikt
- Aufzeigen der Möglichkeiten zum Umgang mit neuen Bedrohungsformen durch unbemannte Vehikel
- Untersuchung von Gegen-Gegenmassnahmen, z.B. zum Umgang in elektromagnetisch-gestörter Umgebung
- Analysieren der Technologie- und Marktentwicklung im Bereich Robotik sowie Implikationen für die Streitkräfte
- Beobachtung und Beurteilung der Entwicklung von letalen, autonomen Waffensystemen
- Adressieren von ethischen und rechtlichen Fragestellungen zu autonomen Waffensystemen
- Berücksichtigung des nicht-technischen Umfeldes zur Identifikation von Chancen und Risiken für die Schweiz auf politischer, militär-strategischer und operationeller Stufe

3.3.2 Weltraumtechnologien und Alternativen

Ausgangslage und Problemstellung

Weltraumgestützte Anwendungen gehören zum Alltag einer leistungsfähigen Industrienation wie der Schweiz. Auf Daten von Satelliten im Weltraum basieren verschiedene Anwendungen wie Wettervorhersagen, globale Kommunikation und digitale Vernetzung, Steuerung von Verkehrs- und Energienetzen, Klima- und Umweltüberwachung oder Orientierung mit dem Smartphone an einem fremden Ort. Satelliten bieten die einzigartige Möglichkeit, den gesamten Erdball regelmässig und in hoher Auflösung zu beobachten und dadurch neue Erkenntnisse zu gewinnen. Satellitendaten dienen als Entscheidungsgrundlagen in diversen Bereichen wie Verkehr, Landwirtschaft, Umwelt, Sicherheit und Verteidigung.

Zu Beginn des Weltraumzeitalters war es nur Grossmächten möglich im Weltraum aktiv zu sein. Heute können sich dank günstigeren Produktions- und Startkosten immer mehr Staaten im Weltraum engagieren und eigene Satelliten entwickeln und betreiben. Neben Staaten gibt es aber auch zahlreiche private Unternehmen, die zur weiteren Erschliessung des Weltraums beitragen. Die Kommerzialisierung wird in verschiedenen Sektoren vorangetrieben, wobei die Telekommunikation sowie die Bild- und elektronische Aufklärung bisher am weitesten fortgeschritten sind. Diese Entwicklung führt zu immer mehr Starts und einer höheren Anzahl Satelliten. Immer kleinere und günstiger produzierte Satelliten eröffnen neue und bisher ungeahnte Möglichkeiten, wie zum Beispiel den Aufbau von Mega-Konstellationen bestehend aus hunderten oder gar tausenden Plattformen für die globale Kommunikationsabdeckung oder auch für die hochaufgelöste Erdbeobachtung quasi in Echtzeit. Einige Beispiele für diese Konstellationen bzw. Mega-Konstellationen sind Iridium, Starlink, Oneweb, Planet, Blacksky, Capella, Iceye, Umbra, Hawkeye, Spire oder Kleos.

Diese Entwicklung hat die Schweiz veranlasst, eine neue Weltraumpolitik zu formulieren und nun auch eine Weltraumgesetzgebung auszuarbeiten, welche an internationale Vereinbarungen anknüpft. Damit soll sichergestellt werden, dass Schweizer Unternehmen und Institutionen künftig die Grundlagen erhalten, Weltraumvorhaben zu lancieren oder sich an solchen zu beteiligen. Der vereinfachte Zugang zum Weltraum ist sicherheitspolitisch sowohl hinsichtlich Opportunitäten als auch hinsichtlich potenzieller Risiken relevant. Die Raumfahrt war stets auch getrieben und geprägt von militärischen Interessen, aber in den vergangenen Jahren konnte nun eine zunehmende Militarisierung des Weltraums beobachtet werden. Der Weltraum ist für moderne Streitkräfte eine zunehmend entscheidende Operationssphäre. Einige Nationen etablieren deshalb eigene Weltraumkommandos. Die Nutzung weltraumbasierter Plattformen dient dabei dazu, andere Wirkmittel in den Einsatz zu bringen oder deren Einsatz erst zu ermöglichen und zu unterstützen. Durch die Militarisierung des Weltraums entsteht die Möglichkeit, im Orbit militärische Aktionen durchzuführen. So könnte der Weltraum vom Raum mit rein funktionaler Bedeutung als Enabler selbst zum Raum der Konfliktaustragung werden. Mehrere Staaten haben spezifische Teilstreitkräfte und dazugehörende Kommandostrukturen geschaffen. Auch die NATO erklärte den Weltraum zur Operationssphäre. Die aufgebauten militärischen Fähigkeiten ermöglichen potenziell feindliche Handlungen auf Ziele im All oder auf der Erde, beispielsweise den Abschuss von Satelliten oder Cyberangriffe. In den kommenden Jahren dürfte der Weltraum ein Schauplatz verstärkter Militarisierung und konfrontativen Verhaltens bleiben.

Infolge der Digitalisierung und der zunehmenden Vernetzung werden Streitkräfte in Zukunft noch stärker von weltraumbasierten Fähigkeiten abhängig sein. Durch die vielfältige und alltägliche Nutzung von Daten und Diensten aus dem Weltraum wächst die Abhängigkeit von Weltrauminfrastrukturen. Damit steigt die Verletzlichkeit gegenüber Ausfällen oder Beeinträchtigungen solcher Infrastrukturen. Satelliten sind bereits heute für viele zivile und militärische Anwendungen unabdingbar und stellen selbst kritische Infrastrukturen dar. Daher müssen die Satelliten nicht nur gegen Cyberangriffe, sondern zukünftig verstärkt auch gegen kinetische und elektromagnetische Einwirkung, insbesondere auch gegen Sonnenstürme geschützt werden können.

Die Bedeutung des Weltraums ist insbesondere auch für Schweizer Akteure relevant, welche mit der Umsetzung sicherheitspolitischer Aufgaben betraut sind.

Dabei setzt man auf die Dienstleistungen von Drittstaaten, Organisationen oder kommerziellen Anbietern. Im sicherheitspolitischen Kontext betreibt die Schweiz als Staat bis heute jedoch keine eigenen Satelliten. Die Schweiz engagiert sich seit Beginn der Raumfahrt in Europa als Mitglied der European Space Agency (ESA) an deren Satellitenprogrammen und ist über Beteiligungen auch in anderen staatlichen Raumfahrtprogrammen involviert. Darüber hinaus betreiben einige Schweizer Anbieter Kleinsatelliten im Rahmen von kommerziellen und wissenschaftlichen Dienstleistungen.

Zur Wahrnehmung ihrer Aufgaben ist auch die Schweizer Armee auf Leistungen aus dem Weltraum angewiesen, dies insbesondere in Form von Beiträgen zur Nachrichtenbeschaffung, zur Führungsunterstützung, zur Präzisionsnavigation und zur Synchronisation ihrer Systeme. Aktuell werden vornehmlich für die Aufklärung und Kommunikation Angebote von Drittstaaten, Organisationen oder kommerziellen Anbietern genutzt. Der Zugriff auf solche Informationen könnte jedoch im Krisen- sowie Konfliktfall beschränkt werden oder ganz verwehrt bleiben. Diese Abhängigkeiten stellen ein sicherheitspolitisches Risiko dar. Um militärische Operationen genügend vor Aufklärung aus dem All zu schützen, ist vermehrt ein «Lagebild Weltraum» erforderlich, in welchem Überflugbahnen und Aufklärungsleistung von Satelliten berücksichtigt werden. Schliesslich muss durch die Erfassung der Weltraumlage ein Mittel zur Verfügung stehen, welches abzuschätzen erlaubt, inwieweit Leistungen von Satellitensystemen verfügbar bleiben, wenn diese mit Schrottteilchen kollidieren, gezielt durch Gegner gestört oder sogar zerstört werden oder erhöhten Sonnenwindaktivitäten ausgesetzt sind.

Heute wird sowohl von staatlicher als auch von privater Seite an der Entwicklung wiederverwendbarer Raumtransportsysteme gearbeitet, um die Kosten zu senken. Die Zukunft wird zeigen, ob die Zuverlässigkeit solcher Systeme so weit gesteigert werden kann, dass das Vertrauen der Kunden gewonnen werden kann. Aufgrund der Miniaturisierung von Komponenten ist es heute schon möglich, bedeutend kleinere Satelliten zu bauen. Dies erlaubt einerseits die Kosten der Satelliten deutlich zu reduzieren und andererseits eine viel grössere Anzahl von Satelliten im Rideshare Konzept gleichzeitig zu starten, was wiederum die Zugangskosten zum Weltraum reduziert.

Die Reduktion der Kosten und die bessere Verfügbarkeit von Raumtransportsystemen haben in den letzten Jahren den Aufbau grosser Konstellationen ermöglicht. Diese werden vor allem für die Satellitenkommunikation, für die elektronische Aufklärung sowie für die Erdbeobachtung eingesetzt. Insbesondere für die Aufklärung und Überwachung steigt mit der Grösse der Konstellation die Überflugsrate über einem bestimmten Zielgebiet. Damit steigt sowohl das gesammelte bzw. übertragbare Datenvolumen als auch die Robustheit des Systems beim Ausfall eines einzelnen Satelliten. Dank breitbandiger Inter-Satelliten-Kommunikation und einem Netz von Bodenstationen ist es möglich, sämtliche Daten zeitnah an eine einzelne Bodenstation zu übermitteln. Zu diesem Zweck wird immer öfter auch die optische Kommunikation mittels Laserlink eingesetzt. Diese erlaubt neben der verschlüsselten Übertragung von Daten auch die Verteilung von quantenbasierten Schlüsseln. Bereits heute überziehen erste grosse Konstellationen die Erde mit einem flächendeckenden satellitengestützten Kommunikationsnetz. Auf diese Weise können breitbandige Verbindungen an allen Orten der Erde und auch über den Ozeanen angeboten werden. Um Konstellationen zu kommissionieren und später stabil zu halten, müssen die einzelnen Satelliten manövrierbar sein. Dabei werden vermehrt elektrische Antriebe eingesetzt, die vor allem kleinen Satelliten erlauben, aktive Manöver durchzuführen und so ihre Einsatzdauer zu erhöhen. Die Manövrierbarkeit erlaubt zudem, dass ein Satellit am Ende eines operativen Einsatzes gezielt in die Erdatmosphäre oder in eine Friedhofsumlaufbahn gelenkt wird oder dass Ausweichmanöver eine mögliche Kollision mit Weltraumschrott verhindern. Für solch autonome Manöver werden verschiedene Sensoren an Bord des Satelliten eingesetzt und mittels künstlicher Intelligenz eigenständige Entscheidungen in der Lagekontrolle des Satelliten getroffen. Es ist zu erwarten, dass einzelne Satelliten oder Konstellationen in Zukunft multifunktional oder umkonfigurierbar ausgelegt sein werden, also mehrere verschiedene Sensoren und auch Kommunikationselemente als Nutzlast mitführen, die je nach Bedürfnissen eingesetzt werden können.

Diese Trends führen zu riesigen Datenmengen, die durch Analysten nicht mehr ohne weiteres und nicht mit der notwendigen Geschwindigkeit bewältigt werden können. Eine sensornahe Auswertung an Bord des Satelliten, das Erkennen von Signaturen oder Objekten mit Hilfe künstlicher Intelligenz und die automatisierte Erkennung von detektierten Veränderungen

aufgrund einer umfassenden Datenbasis bilden die Grundlage für aktuelle satellitengestützte Informationen und Dienstleistungsprodukte für Firmen und Behörden. Die Nutzung von Kleinstsatelliten und künstlicher Intelligenz erlaubt in Zukunft auch die Anwendung von Formations- und Schwarmkonzepten, bei denen eine Vielzahl von Satelliten in unterschiedlichen Konfigurationen und im autonomen Betrieb zum Einsatz kommen. In solchen Konzepten können auch Methoden des Advanced Space Manufacturing (3D-Druck im All) helfen, Teile oder Komponenten von Kleinstsatelliten direkt im Weltraum zu produzieren. Die letzten Jahre haben gezeigt, dass die Anzahl der gestarteten Satelliten sprunghaft auf über 2000 pro Jahr angestiegen ist, und der Trend geht in Richtung noch höherer Startkadenzen. Dies wird das Problem des Weltraumschrotts zusätzlich verschärfen, wenn nicht dafür gesorgt wird, dass Satelliten am Ende ihrer Lebensdauer durch einen gezielten Wiedereintritt in die Erdatmosphäre verglühen.

Aufgrund der technischen und kommerziellen Entwicklungen im Weltraum kann beobachtet werden, dass auch kleinere Staaten mit einem vernünftigen Aufwand in der Lage sind, Aufklärungssatelliten mit guter räumlicher Auflösung oder gar kleine Konstellationen zu betreiben. Dies kann für die Schweiz eine Chance darstellen, aber auch eine Gefahr. Auch für gegnerische Organisationen oder Staaten wird es mit einem moderaten Budget möglich sein, andere Satelliten zu bekämpfen und so GNSS-Navigation zu stören oder Kommunikationsverbindungen zu unterbrechen. Es ist damit zu rechnen, dass die Schweiz einer Quasi-Permanentüberwachung aus dem All ausgesetzt sein wird, wobei gegenüber optischen Aufklärungssatelliten eine Wolkenabdeckung von rund 60 % und der Tag-Nacht-Zyklus auch in Zukunft einen gewissen Schutz bieten. Anders ist die Situation bei bildgebenden SAR-Radarsensoren, vor welchen ein Schutz durch elektronische Gegenmassnahmen aufgebaut werden müsste. Auf alle Fälle könnten Truppenbewegungen, Aktivitäten auf Flugplätzen oder Verschiebungen von Waffensystemen quasi in Echtzeit verfolgt werden. Ist Satellitenaufklärung heute primär als strategisches Aufklärungsmittel von Bedeutung, wird sie in Zukunft vermehrt auch taktisch-operativ eingesetzt werden. Für die beschleunigte Reaktionsfähigkeit geht die Entwicklung auch in die Richtung einer reaktionsschnellen Verbringung von Satelliten, um bei Bedarf schnellstmöglich Fähigkeiten im Weltraum zu etablieren oder bei Ausfall zu ersetzen. Die sinkenden Kosten für den Bau, Betrieb und Start von Satelliten und der deutlich erleichterte Zugang zum Weltraum haben auch die Schweiz bewogen abzuklären, ob Leistungen aus dem Weltraum zumindest teilweise durch ein nationales Programm abgedeckt werden können. Dies würde in Krisen und bei Konflikten eine gewisse Unabhängigkeit von Dritten garantieren. Diese Überlegungen wurden im Grundlagenkonzept der Operationssphäre Weltraum und im Grundlagenpapier Weltraum detailliert beschrieben.

Forschungsthemen 2025-2028

Lagebild Weltraum

- Entwicklung von Methoden zur Synthese und Analyse von öffentlichen und eigenen Sensordaten zur Darstellung eines autonomen Lagebildes
- Erarbeitung von Technologien zum terrestrischen Tracking von Satelliten und Aufbau von Demonstratoren
- Verbesserung von Verfahren zur Überwachung von Abschussrampen
- Berücksichtigung der Weltraumwetters hinsichtlich der Verfügbarkeit von satellitenbasierten Leistungen

Weltraum-Anwendungen und Alternativen

- Systematisches Technologie- und Markt-Monitoring für Anwendungen im Weltraum
- Monitoring der Fähigkeiten und verwendeten Technologien fremder Weltraumkommandos
- Untersuchung der Einsatzmöglichkeiten und Grenzen sowie Bewertung der Verfügbarkeit, Zuverlässigkeit und Sicherheit von Satelliten-Konstellationen zur Kommunikation
- Durchführung von Machbarkeitsstudien, um die Möglichkeiten und Grenzen von Satelliten-Konstellationen für die Bild- und Signalaufklärung zu beurteilen
- Aufzeigen möglicher Alternativen für die satellitenbasierte Navigation und Synchronisation
- Entwicklung von Methoden für die autonome und intelligente Datenverarbeitung an Bord eines Satelliten zur Beschleunigung der Informationsbeschaffung

Satelliten- und Missionskompetenzen

- Durchführung von Technologie-Studien für die Entwicklung und den Einsatz von Kleinsatelliten
- Erarbeitung von Grundlagen zur Errichtung von Bodenstationen und dem Betrieb eines Mission-Kontrollzentrums

- Bewertung von Konzepten für den reaktionsschnellen Einsatz von Satelliten (Responsive Space)
- Schaffung von Technologiegrundlagen für den Einsatz von flexiblen Satellitenplattformen und Nutzlasten
- Förderung des Ökosystems Space Schweiz und Aufbau von strategischen Partnerschaften

Schutz und Gegenmassnahmen im Weltraum

- Erarbeitung und Überprüfung von Konzepten für die End-to-end Verschlüsselung von Satelliten-Missionen
- Weiterentwicklung von Methoden zum aktiven und passiven Schutz vor gegnerischer Aufklärung aus dem Weltraum
- Durchführung von Risiko-Analysen bei der Verwendung von Dienstleistungen aus dem Weltraum.
- Erarbeitung von Kooperationsmodellen auf militärischer, ziviler und internationaler Ebene

3.4 Querschnittsthemen

3.4.1 Nachhaltige und autarke Energieversorgung

Ausgangslage und Problemstellung

Die Themen Klimawandel und nachhaltige Energieversorgung erhalten seit einigen Jahren grosse Aufmerksamkeit in der Politik und Gesellschaft. Die Energiewende, also der Übergang von der nicht-nachhaltigen Nutzung von fossilen Energieträgern und Kernenergie zu einer nachhaltigen Energieversorgung mittels erneuerbarer Energien, stellt die zivile und militärische Energieversorgung vor grosse Herausforderungen. Die Schweiz hat 2015 das Pariser Klimaabkommen unterzeichnet, mit dem Ziel, die globale Erwärmung im Vergleich zur vorindustriellen Zeit auf unter 2 Grad Celsius, wenn möglich maximal 1.5 Grad Celsius, zu begrenzen und bis 2030 die CO2-Emissionen im Vergleich zu 1990 um 50 % zu reduzieren. Ausserdem wurde durch das 2023 vom Stimmvolk angenommene Klima- und Innovationsgesetz das Ziel gesetzt, dass die Schweiz bis 2050 die Klimaneutralität erreicht. Da CO2-Emissionen nicht vollständig vermieden werden können, werden für das Netto-Null Ziel auch Lösungen benötigt, um das CO2 aus der Atmosphäre zu entfernen und dauerhaft zu speichern.

Das VBS als grösstes Departement ist ein Energie-Grossverbraucher und muss bis 2030 seine CO2-Emissionen im Vergleich zu 2001 um mindestens 40 % senken. 2021 emittierte das VBS pro Jahr knapp 200'000 Tonnen CO2. Davon stammten rund 47 % aus der Luftfahrt, 24 % aus dem Strassenverkehr, 20 % aus den Immobilien, 7 % aus dem Verkehr der Armeeangehörigen und 2 % aus der Stromnutzung. Die Gruppe Verteidigung ist für etwa 98 % der CO2-Emissionen des VBS verantwortlich. Die restlichen 2 % werden von den anderen Bundesämtern des Departements verursacht. Gemäss Aktionsplan Energie und Klima hat das VBS eine klare Vision: «Spätestens im Jahr 2050 ist die CO2-Bilanz des VBS ausgeglichen (Netto Null). Das Departement deckt seinen Energiebedarf vornehmlich aus erneuerbaren Quellen und produziert seine benötigte Energie so weit wie möglich selbst». Dazu wurden vier Stossrichtungen festgelegt:

- Fossile Energie reduzieren und substituieren
- Erneuerbare Energien und Eigenproduktion ausbauen
- Speicherkapazität erhöhen
- Innovative Projekte fördern

Aus Sicht der Schweizer Armee ist, neben der CO2-Reduktion, auch das Ziel einer autarken Energieversorgung ein wichtiger Treiber in der Diskussion um einen nachhaltigen Umgang mit Energie. Durch die zunehmende Vernetzung und Digitalisierung steigt der Energiebedarf und insbesondere IKT Systeme sind sehr abhängig von einer zuverlässigen Energieversorgung. Die Energiesicherheit ist deshalb eine Achillesferse, die nicht vernachlässigt werden darf und in allen Lagen sichergestellt sein muss. Technologien zur nachhaltigen Produktion und Speicherung von Energie haben das Potenzial einer weitgehend lokalen und autarken Anwendung. Damit eröffnet sich die Möglichkeit kritische Armeestandorte unabhängig von zivilen Energieversorgern zu betreiben und dadurch in Krisensituationen einen wesentlichen Beitrag zur Durchhaltefähigkeit zu leisten.

Die öffentlichen Ausgaben für die Energieforschung in der Schweiz haben in den vergangenen Jahren stark zugenommen und bewegen sich aktuell im Bereich von CHF 400 Millionen pro Jahr. Diese Forschung deckt das ganze Spektrum der Energiethematik ab, ist jedoch stark auf erneuerbare Energien und die effiziente Energienutzung ausgerichtet. Erkenntnisse aus

der zivilen Forschung können natürlich auch für die Anwendungen im militärischen Umfeld genutzt werden. Für die Energieerzeugung beispielsweise sind die Technologien grundsätzlich dieselben. Trotzdem gibt es auch Aspekte, die in der zivilen Forschung nicht untersucht werden. Für militärische Systeme bestehen oft erhöhte Anforderungen an die Zuverlässigkeit und Einsatzfähigkeit. Die Herausforderung ist es, die Erkenntnisse der zivilen Forschung auf den militärischen Kontext zu übertragen und weiterzuentwickeln.

Der Treibstoff-Verbrauch von Luftwaffe und Heer ist für den grössten Teil der CO2-Emissionen des VBS verantwortlich. Dienstfahrzeuge und teilweise auch Logistikfahrzeuge können durch Fahrzeuge mit alternativen Antriebsarten wie Brennstoffzellen, Wasserstoffverbrennungsmotor oder batterie-elektrischem Antrieb ersetzt werden. Bei taktischen und schweren Militärfahrzeugen sowie Flugzeugen und Helikoptern sind die Möglichkeiten jedoch sehr eingeschränkt. Bei leichten Militärfahrzeugen besteht die Option, den Verbrennungsmotor durch Alternativen zu ersetzen. Dies ist jedoch nicht ohne Kompromisse bei der Durchhaltefähigkeit und Nutzlast möglich. Der Einsatz von Fahrzeug-Demonstratoren mit alternativen Antrieben muss deshalb ausführlich im Feld getestet werden. Neben den technischen Eigenschaften darf auch nicht ausser Acht gelassen werden, dass die Infrastruktur zur Betankung oder Aufladung neu konzipiert und aufgebaut werden muss. Der Einsatz von Fahrzeugen mit alternativem Antrieb soll nicht nur in der normalen Lage funktionieren, sondern muss insbesondere auch in der ausserordentlichen Lage gewährleistet sein.

Bei schweren Militärfahrzeugen und bei der Luftwaffe werden Flüssigtreibstoffe noch lange eine grosse Rolle spielen. Kohlenwasserstoffe haben bei weitem die höchste Leistungsdichte und können deshalb nicht ohne grosse Nachteile beim Gewichts- und Platzbedarf ersetzt werden. Zudem ist die Logistik für den Transport von Flüssigtreibstoffe bekannt, effizient und bewährt. Besonders getrieben durch die zivile Aviatik sind nachhaltige Treibstoffe, sogenannte Sustainable Aviation Fuels (SAF), jedoch bereits heute in kleinen Mengen vorhanden. Es gibt ein begrenztes Angebot an nachhaltigen biogenen Treibstoffen und auch die Produktion von synthetischen Treibstoffen, die durch sogenannte Power-to-X (PtX) Technologien produziert werden, wird in den kommenden Jahren sehr stark hochgefahren. Zusätzlich ist Wasserstoff ein wichtiger Energieträger, der in der Regel durch Elektrolyse-Verfahren hergestellt wird. Das Anliegen der Armee ist es, einen Teil der nachhaltigen Treibstoffe für den Eigenbedarf in der Schweiz zu produzieren.

Die Immobilien des VBS sollen in Zukunft mit Strom und Wärme versorgt werden, die vollständig aus erneuerbaren Quellen stammen, wenn möglich aus Eigenproduktion. Dies dient nicht nur zur CO2-Reduktion, sondern unterstützt auch das Ziel der Energie-Autarkie. Dazu muss die eigene Stromproduktion stark hochgefahren werden. Neben dem aktuellen Fokus auf Solarenergie stehen auch noch andere Energiequellen zur Verfügung. Da die nachhaltige Energieerzeugung sehr tages- und saisonabhängig ist, muss auch das Problem der begrenzten Energiespeicherung angegangen werden. Dies ist essenziell, damit die Verteidigung ihre eigene Energieversorgung zu jedem Zeitpunkt gewährleisten kann. Eine bedeutende Rolle wird dabei die Sektorkopplung spielen, also die Verbindung der Energiesektoren Strom, Wärme und Verkehr über ein Energiemanagementsystem.

Energie muss nicht nur an stationären Standorten zur Verfügung stehen, sondern auch für die Truppen im Einsatz. Heute wird die Stromversorgung im Feld standardmässig mittels Dieselgeneratoren gesichert. Um diese zu ersetzen, müssen entweder Generatoren mit nachhaltigen Energieträgern wie Wasserstoff eingesetzt werden oder die nachhaltige Energiebereitstellung geschieht über Speicherlösungen wie Akkumulatoren. Der korrekte Umgang mit diesen ist wichtig, um sowohl die Lebensdauer zu verlängern als auch die Sicherheit zu gewährleisten.

Forschungsthemen 2025-2028

Mobilitätskonzepte und Einsatz in der Armee

- Technologie- und Marktabklärungen zu alternativen Antriebskonzepten wie Wasserstoff-Brennstoffzellen, batterieelektrischer Antrieb, Hybridantrieb oder nachhaltig betriebene Verbrennungsmotoren für militärische Fahrzeuge
- Entwicklung von militärischen Fahrzeug-Demonstratoren mit Elektroantrieb, Brennstoffzellenantrieb oder nachhaltig betriebenem Verbrennungsmotor
- Ausführliche Tests der militärischen Fahrzeug-Demonstratoren im Feld und im Einsatz
- Untersuchung der Möglichkeit zur Hybridisierung von aktuellen Armeefahrzeugen und Systemen
- Abklärungen zur Sicherheit von Batterien und Wasserstofftanks im Einsatz, zum Beispiel bei Beschuss

- Erstellung eines Infrastrukturmodells für die Betankung bzw. Aufladung von Militärfahrzeugen
- Technologie- und Marktabklärungen für Kleinflugzeuge mit Elektro- oder Brennstoffzellenantrieb und Abschätzung des Potenzials für den Einsatz als Schulungsflugzeuge

Nachhaltige Treibstoffe

- Beurteilung und Vergleich der Herstellungsverfahren für biogene oder synthetische Treibstoffe
- Machbarkeitsabklärungen und Demonstration von kostensenkenden Massnahmen für die Treibstoffsynthese
- Potenzialabschätzung und Machbarkeitsstudie zur Herstellung von synthetischen Treibstoffen in der Schweiz
- Untersuchung der Qualität und Eigenschaften von nachhaltigen Treibstoffen, die durch verschiedene Verfahren wie Fischer-Tropsch, oder HEFA hergestellt wurden
- Untersuchung der Auswirkungen von nachhaltigen Treibstoffen auf die Funktionsfähigkeit und Lebensdauer von Motoren militärischer Fahrzeuge
- Erprobung von verschiedenen Wasserstoff-Anwendungen im militärischen Kontext

Nachhaltige Energiebereitstellung für Infrastruktur

- Monitoring der Technologien für nachhaltige Stromerzeugung in den Bereichen der Solarenergie, Wasserkraft, Windkraft, Geothermie, Biomasse sowie deren kombinierte Nutzung
- Machbarkeitsabklärungen und Evaluation von geeigneten Methoden für die lokale Energieerzeugung an ausgewählten Standorten der Armee
- Beobachtung der Entwicklungen zur Speicherung von grossen Energiemengen durch Technologien wie Batterien, Druckluftspeicher oder die Umwandlung von Strom zu Energieträgern wie Wasserstoff oder Methan
- Demonstration von Energieerzeugungs- und Speichertechnologien im Umfeld der Armee
- Erstellung eines Konzeptes für den Inselbetrieb von ausgewählten Armee-Standorten und Auswahl von geeigneten Technologien
- Aufzeigen der Möglichkeiten für die Anwendung der Sektorkopplung an Armeestandorten
- Untersuchung und Demonstration von nachhaltigen Notstrom-Konzepten

Energieversorgung für mobile Truppen

- Erfassung der typischen Strombedürfnisse der Truppen und in Feldlagern
- Evaluation von alternativen Methoden zur lokalen Stromerzeugung im Feld
- Monitoring und Beurteilung der aktuellen und zukünftig verfügbaren Technologien für tragbare Energieversorgungslösungen für den Soldaten
- Untersuchung des Einsatzes von Stromerzeugungsprinzipien, die mit erneuerbarer Primärenergie oder nachhaltigen Sekundärenergien wie z.B. Wasserstoff und Methanol funktionieren
- Aufzeigen der Einsatzmöglichkeiten von Wasserstoff im mobilen Umfeld
- Untersuchung der Sicherheit von Batterien, Wasserstoffsystemen und weiteren Energie-speichersystemen

3.4.2 Simulation und Analyse

Ausgangslage und Problemstellung

Die Möglichkeiten von Simulationen und Analysen haben in den letzten Jahren erhebliche Fortschritte gemacht, was einerseits auf die Verbesserung der Rechenleistung und der Softwarekapazitäten und andererseits auf Weiterentwicklungen bei den Algorithmen zurückzuführen ist. Die bemerkenswertesten Entwicklungen wurden durch zivile Akteure in verschiedenen Bereichen wie Hochleistungsrechnen, künstliche Intelligenz (KI), digitale Zwillinge, Multiphysik- und Multidomänensimulationen sowie Echtzeitsimulationen vorangetrieben.

Alle diese technologischen Verbesserungen eröffnen ausgezeichnete Möglichkeiten für den militärischen Bereich, insbesondere dann, wenn die Armee mit Aufgaben von hoher Komplexität, besonderen Risiken sowie grossem Personal- und Materialaufwand konfrontiert ist. In einem solchen Umfeld ist es oft schwierig, fundiert über Aspekte wie Einsatzmodalitäten, Streitkräfteentwicklung oder Prozessoptimierungen zu entscheiden. Auch die Ausbildung von Soldaten an Systemen zur Bewältigung ihrer Aufgaben stellt eine wesentliche Herausforderung dar. Zwar können Experimente in reeller Umgebung und Training mit realen Systemen in einigen Fällen bis zu einem gewissen Punkt weiterhelfen. Leider sind sie aber oft

zu teuer, zu langsam oder zu risikoreich, um extensive Anwendung zu finden. In diesem Zusammenhang können Computersimulationen als Abbild der Realität eine interessante Alternative bieten. Zudem können sie eine Reduktion des Ressourcenverbrauchs und der CO2-Emissionen mit sich bringen. Es gibt jedoch drei grosse Herausforderungen. Die erste besteht darin, schrittweise universelle Simulationsplattformen zu schaffen, die synergetisch und kompatibel sind und je nach Bedarf in bereits bestehende Systeme integriert werden und mit diesen interagieren können. Zweitens muss mit den technologischen Entwicklungen, die in diesem Bereich sehr schnell sind, Schritt gehalten werden. Drittens müssen die Simulationsplattformen flexibel genug sein, um einen möglichen Transfer auf eine neue, leistungsfähigere Technologie zu ermöglichen.

Um den Zusammenhang zur ursprünglichen Fragestellung herzustellen, müssen Instrumente zur Analyse von Daten aus Simulationen bereitstehen. Die möglichen Anwendungen lassen sich in folgende Kategorien einteilen:

- Streitkräfteentwicklung
- Einsatzunterstützung
- Ausbildung

Im Bereich Streitkräfteentwicklung werden Konzepte entwickelt, mit denen die Armee den veränderten Rahmenbedingungen Rechnung tragen kann. Dabei wird unter anderem ein Prozess, bekannt als Concept Development and Experimentation (CD&E), befolgt. Neben der eigentlichen Konzepterzeugungsarbeit werden hier also auch Experimente zur Generierung von neuen Strategien, zur Hypothesenüberprüfung sowie zur Verifizierung durchgeführt. Dabei können Simulationen einen wertvollen Beitrag leisten.

Bei der Einsatzunterstützung stehen kurzfristige Entscheidungsfindungen im Vordergrund. Die Vorhersagezeiträume reichen von Wochen über Stunden bis zu Real-Time-Anwendungen. Damit Modellierung, Simulation und Analyse für diese zeitkritischen Anwendungen fristgerecht zur Verfügung stehen, werden diese oft in dezidierten Applikationen gebündelt.

Beim Anwendungskomplex Ausbildung wiederum wird Simulation eingesetzt, um virtuelle taktische Szenarien zu erzeugen, in denen Auszubildende trainiert werden können. Dabei ist das Ziel solcher Simulatoren nicht immer eine grösstmögliche Realitätsnähe. Stattdessen liegt hier der Fokus auf der effizienten Verwendung von Systemen im Verbund sowie der Kommunikation innerhalb und zwischen den Einheiten. Dazu ist eine Simulationsarchitektur notwendig, die zentrales Datenmanagement in einer dezentralen holistischen Nutzerumgebung zulässt. In der Live-Simulation werden Zieldarstellungen, welche auf augmentierter Realität beruhen und virtuelles Feuer die klassischen Laserschusssimulatoren ablösen.

In allen Anwendungskategorien werden unterschiedliche Anforderungen an Modellierung, Simulation und Analyse gestellt. In jedem Fall wird aber ein dezidiertes Modell benötigt. Out-of-the-box-Modelle sind aufgrund der starken Spezialisierung nur in Ausnahmefällen verfügbar. Auch ist es aufgrund der Komplexität der Gesamtsysteme nötig, diese Modelle auf der Basis des aktuellsten Standes der Forschung zu entwickeln.

Forschungsthemen 2025-2028

Simulation für die Streitkräfteentwicklung

- Erforschung von Algorithmen und Modellen für die Unterstützung im CD&E-Prozess für die Weiterentwicklung der Armee
- Entwicklung von KI-Algorithmen für die Optimierung auf taktischer und operativer Stufe

Simulation für die Einsatzunterstützung

- Untersuchung von KI-Ansätzen zur Analyse und Optimierung der Einsatzplanung
- Entwicklung von Werkzeugen für die datenbasierte Entscheidungsunterstützung

Simulation für die Ausbildung & Training

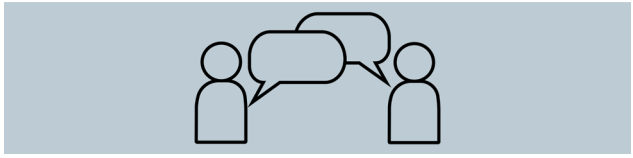
- Erforschung der Möglichkeiten für personalisiertes taktisches Training von Soldaten und Entscheidungsträgern mittels künstlicher Intelligenz
- Verfolgen und experimentelle Verifikation der Technologien sowohl zur Zieldarstellung mittels augmentierter Realität (AR) im scharfen Schuss als auch zu dessen Substitution mittels digitalem Feuer

Übergreifende Simulationsthemen & Analyse

- Erforschung von Machine Learning Verfahren zur automatisierten Auswertung und Interpretation von Simulationsdaten
- Entwicklung von Digital Twin Modellen, um die Systemlandschaft der Armee abzubilden
- Untersuchung der Machbarkeit einer holistischen Simulationsumgebung mit zentralem Datenma-

nagement und Analysemöglichkeiten unter Nutzung von Data-Science Fähigkeiten sowie dezentraler Simulationsnutzung

3.4.3 Human Factors



Ausgangslage und Problemstellung

Menschliche Faktoren (Human Factors) spielen eine entscheidende Rolle für die Leistungsfähigkeit von Organisationen wie der Armee, die in jeder Situation zuverlässig funktionieren müssen. Da Human Factors bei fast jeder militärischen Aktivität für deren Erfolg von Bedeutung sind, müssen sie innerhalb der Schweizer Armee als Querschnittsgebiet betrachtet werden. Human Factors können einerseits im individuellen Kontext betrachtet werden, spielen jedoch auch im operationellen und organisationalen Kontext eine Rolle.

Im individuellen Kontext geht es darum, dass menschliche Fehler reduziert und die Leistungsfähigkeit von Armeeangehörigen gesteigert wird. Technologische Systeme werden immer komplexer und stellen erhöhte Anforderungen an den Anwender. Auch die Zusammenarbeit zwischen Menschen und Maschinen muss funktionieren, um die technologischen Möglichkeiten uneingeschränkt nutzen zu können. Wenn Systeme nicht intuitiv zu bedienen sind und Spezialistenwissen erfordern, führt dies schnell zu einer Überforderung der Anwender. Technologische Systeme und Instrumente müssen so angewendet werden können, dass sie den Entscheidungsfindungsprozess vereinfachen und nicht komplizierter machen.

Zur Steigerung der menschlichen Leistungsfähigkeit müssen sowohl psychologische als auch körperliche Aspekte betrachtet werden. In sogenannten Human Enhancement Technologien wie beispielsweise in der personalisierten Medizin oder in der Biosensorik gibt es aktuell rasche Entwicklungen, die auch bald im militärischen Umfeld angewendet werden könnten. Ein spezielles Augenmerk sollte dabei auf Mess- und Auswertemethoden von Vitalfunktionen unter physischen und psychischen Stressbedingungen gerichtet werden. Damit können sowohl die Selektionskriterien von hochspezialisierten Militärpersonen mit anspruchsvollen Aufgaben verbessert werden, als auch personalisierte Trainingspläne zusammengestellt werden.

Häufig werden die menschlichen Anforderungen erst erkennbar, wenn konkrete Missionen oder Projekte anstehen. Dann geht es darum, die Human Factors Effekte zu quantifizieren und zu kontrollieren und damit eine Grundlage für datenbasierte Interventionen zu liefern. Hierfür stehen grundsätzlich eine Vielzahl von Methoden und Verfahren aus dem Fachbereich Human Factors zur Verfügung, welche für die Anwendung im militärischen Kontext ausgewählt, adaptiert und aufeinander abgestimmt werden können.

Human Factors beeinflussen die Leistungsfähigkeit von ganzen Organisationen. Deshalb ist es wichtig, sowohl die Resilienz von einzelnen Armeeangehörigen zu stärken, als auch jene von ganzen Streitkräften. Eine resiliente Organisation muss sowohl über die Fähigkeit verfügen eine gewisse Robustheit gegen Unwägbarkeiten zu entwickeln, als auch auf grundlegende Veränderungen flexibel zu reagieren und sich anzupassen. In einer Welt mit zunehmender Komplexität und Vieldeutigkeit wird die Widerstandsfähigkeit gegenüber kognitiver Kriegsführung an Bedeutung gewinnen. Diese unkonventionelle und subversive Art der Konfliktaustragung kommt immer häufiger zum Einsatz und zielt darauf ab, die menschliche Wahrnehmung, Meinungsbildung und schlussendlich das Verhalten von Individuen und Gruppen zu beeinflussen. Das Internet und soziale Medien lassen eine schnelle Verbreitung von Informationen und eine rasche Interaktion von Teilnehmenden zu, egal ob dies Menschen sind oder künstliche Chatbots. So kann im Rahmen der kognitiven Kriegsführung die Bildung von Blasen gesteuert und die Wahrnehmung von Menschen durch tendenziöse oder falsche Informationen gezielt manipuliert werden. Dies kann langfristig ein ganzes Wertesystem beeinflussen, Organisationen destabilisieren oder ganze Gesellschaften spalten.

Forschungsthemen 2025-2028

Human Enhancement

- Verfolgung der Technologie-Trends zur menschlichen Leistungssteigerung in Bereichen wie personalisierte Medizin, Biosensorik, Biotechnologie und Mensch-Maschinen-Interaktion
- Entwicklung von Methoden, um die Leistungsfähigkeit von Soldaten und Piloten zu verbessern

- Erarbeitung von Grundlagen für die Beurteilung der ethischen und rechtlichen Aspekte von Human Enhancement Technologien
- Verständnis der Funktionsweise von Kognitiver Kriegsführung und Abschätzung der Auswirkung auf Individuen, Truppen und die Bevölkerung
- Entwicklung von Instrumenten zur Unterstützung des Menschen in Entscheidungsprozessen

Quantifizierung von Human Factors

- Weiterentwicklung von Methoden zur Beurteilung des menschlichen Einflusses auf die Effektivität von Systemen und Prozessen
- Beurteilung der Akzeptanz von Künstlicher Intelligenz und Abschätzung des Einflusses auf menschliche Entscheidungen
- Untersuchung der Interaktionen zwischen Menschen und Maschinen und Aufzeigen von Weiterentwicklungspotenzial
- Erarbeitung von Methoden für die Zusammenstellung von effizienten Teams

Resilienz

- Erforschen von Möglichkeiten zur Stärkung der individuellen Resilienz von Angehörigen der Armee
- Beurteilung der Fähigkeit der Verteidigung, auf Veränderungen zu reagieren und sich daran anzupassen, zukünftige Bedrohungen und Chancen zu antizipieren und eigene Schwachstellen zu erkennen
- Entwicklung eines Modells für die Streitkräfte-Resilienz aufgrund der Bedürfnisse der Schweizer Armee

4 Finanzierung

4.1 Finanzierung 2021-2024

Die öffentliche Finanzierung der sicherheitspolitischen Forschung mit Relevanz für die Verteidigung erfolgt in der Schweiz ausschliesslich durch das VBS. Andere Instrumente des Bundes wie der Schweizerische Nationalfonds oder Innosuisse schliessen die rein wehrtechnische Forschung aus. Vielfach können Dual Use Technologien jedoch sowohl für zivile als auch für militärische Zwecke verwendet werden. Die scharfe Trennung zwischen ziviler und wehrtechnischer Forschung ist deshalb nicht möglich. Neben der öffentlich finanzierten Forschung investiert auch die in der Schweiz ansässige Rüstungsindustrie in die wehrtechnische Forschung. Die genauen Investitionen der Privatindustrie sind nicht nach Forschung und Entwicklung aufgeschlüsselt und ergeben daher kein kohärentes Bild im Vergleich zu den Aufwendungen in der Ressortforschung.

Der Forschungsaufwand der armasuisse setzt sich aus Eigenleistungen (intramuros) und der Finanzierung von Aufträgen an externe Forschungspartner (extramuros) zusammen (Abbildung 8). Die Eigenleistungen umfassen das Forschungsmanagement, die Führung von Forschungsprogrammen und die interne Durchführung von Projekten in Form einer Vollkostenrechnung. Die Vergabe von Forschungsverträgen an Partner aus Hochschulen und Industrie erfolgt auftragsbezogen und projektbasiert. Seit 2019 hat der Forschungsaufwand stark zugenommen. Dies hängt vor allem mit dem Aufbau des Cyber Defence Campus und der damit verbundenen Erhöhung des Personalbestands und des Forschungsbudgets zusammen.

4.2 Finanzierung 2025-2028

Die Verknüpfung der strategischen Forschungsausrichtung der armasuisse mit dem entsprechenden finanziellen Engagement gilt als schützenswert, da die Aufgabenerfüllung von Teilen der Bundesverwaltung oder von Teilen der Armee bei Bekanntwerden beeinträchtigt werden kann. Deshalb sind diese Informationen gemäss Artikel 6, Lit. e der Verordnung über den Schutz von Informationen des Bundes (ISchV, SR 510.411) und dem von der Konferenz der Generalsekretäre festgelegten Klassifizierungskatalog als VERTRAULICH zu klassifizieren. Die finanziellen Kennzahlen werden in einer klassifizierten Beilage zum Langfristigen Forschungsplan bereitgestellt. Das vorliegende Dokument ohne Beilage unterliegt keiner Klassifizierung.

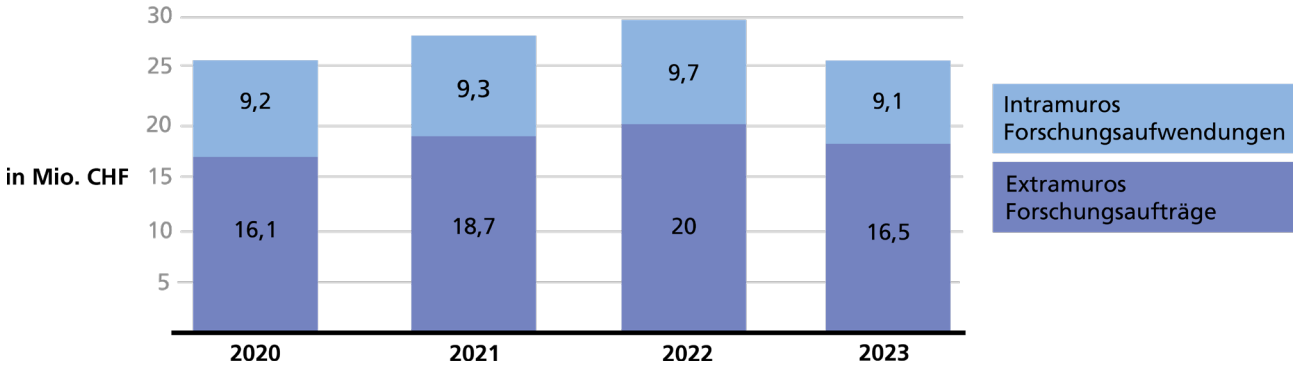


Abbildung 8: Forschungsaufwand der armasuisse für die Periode 2020 – 2023.

5 Akteure und Schnittstellen

5.1 Beschreibung der wichtigsten Akteure

Die Forschung von armasuisse verfolgt das Ziel, diejenigen Kompetenzen sicherzustellen, welche es erlauben für die Sicherheitskräfte der Schweiz, insbesondere für die Armee, den Nachrichtendienst und das Bundesamt für Cybersicherheit, unabhängige Expertisen auf dem neusten Stand von Wissenschaft und Technik zu erstellen. Ferner sind die Kompetenzen aus der Forschung eine wichtige Grundlage, um technologie-getriebene Innovationen zu fördern und umzusetzen. In Absprache mit den Stakeholdern aus dem Umfeld der sicherheitspolitischen Instrumente steuert armasuisse die Forschung von der strategischen Ebene bis zur Umsetzung in Projekten. armasuisse richtet das Kompetenznetzwerk bedarfsgerecht aus und sorgt für den Wissenstransfer aus den Forschungsprojekten in die Strategie-, Planungs-, Innovations- und Beschaffungsprozesse des VBS.

Ein solches Netzwerk muss strategisch und nachhaltig aufgebaut werden. Die Partnerschaften werden mittel- bis langfristig ausgelegt und basieren neben den ursprünglich vorhandenen Kompetenzen der Forschungsinstitution auf gemeinsamen inhaltlichen Interessen, insbesondere für Technologien, welche bei Sicherheitskräften Anwendungspotenzial haben. Das nationale Kompetenznetzwerk kann in vier verschiedene Partnerkategorien eingeteilt werden (Abbildung 9).

- **Hochschulen** und nicht-Profit-orientierte wissenschaftlich tätige Institute: Neben den beiden Eidgenössischen Technischen Hochschulen in Zürich und Lausanne sind die Universitäten Zürich und Bern sowie verschiedene Fachhochschulen wichtige Forschungspartner. Um die Zusammenarbeit zu verstärken, hat armasuisse W+T strategische Partnerschaftsabkommen mit der ETH Zürich im Bereich der Robotik und mit der Universität Zürich auf dem Gebiet der Radaraufklärung abgeschlossen. Ferner wurde auf Stufe des Departements ein Technologierat geschaffen, der mit hochrangigen Vertretern aus dem VBS und der ETH Zürich besetzt ist. Mit der EPFL bestehen strategische Partnerschaften im Rahmen des Cyber Defence Campus und des Space Campus. Die Hochschulen und Institute bilden das wissenschaftliche Rückgrat der technisch-orientierten Forschung im VBS.
- **Start-up Firmen** sind als Forschungspartner interessant, weil diese sehr oft versuchen, neue Produkte auf den Markt zu bringen, die auf technologischen Spitzenentwicklungen der Hochschulen basieren. Die Start-up-Szene besticht in vielen Fällen durch ihre Unbefangenheit Neues zu versuchen und trägt deshalb viel zur dynamischen Entwicklung von ökonomischen Systemen bei. Je nach Entwicklungsphase eines Start-ups leisten sie wichtige Beiträge in angewandter Forschung, indem sie Demonstratoren realisieren, oder sie sind wichtige Partner bei der Realisierung von technologie-getriebenen Innovationsvorhaben. Die Zusammenarbeit mit Start-ups ist meistens zeitlich begrenzt, weil ein grosser Teil entweder durch etablierte Firmen aufgekauft wird oder weil sich der erhoffte Durchbruch der Geschäftsidee nicht einstellt. armasuisse beobachtet die Start-up-Szene der Schweiz genau, weil sie ein wichtiger Indikator für technologische Entwicklungen darstellen.
- In der Schweiz zeichnen sich Kleine und mittlere Unternehmen (**KMU**) nicht selten durch eine hohe Spezialisierung und Spitzenprodukte im Hightech-Bereich aus. Diese können ihre Stellung nur dann halten, wenn sie sich stetig weiterentwickeln. Für armasuisse sind solche Firmen besonders dann interessant, wenn deren Produktepipeline ein grosses Dual-Use-Potenzial haben. Dabei soll geklärt werden, welchen Effekt solche Technologien für Anwendungen von Sicherheitskräften haben und welche Anpassungen vorgenommen werden müssten, um den Anforderungen in ihrem Umfeld zu genügen.
- Interessant ist auch die Zusammenarbeit mit klassischen **Rüstungsfirmen**, insbesondere mit jenen, die in der Schweiz über eigene Forschungs- und Entwicklungsabteilungen verfügen. Diese sind zwar auf ihre Produktepalette ausgerichtet und decken daher bei weitem nicht alle relevanten Technologien ab. Trotzdem sind sie wichtige Partner, die mit ihrem fundierten Wissen zu Demonstrationszwecken wertvolle Integrationsleistungen von modernen Technologien auf bestehenden Plattformen erbringen können. Zudem können sie im Rahmen von Innovationsprojekten wichtige Engineering- und Unterstützungs-Leistungen erbringen.

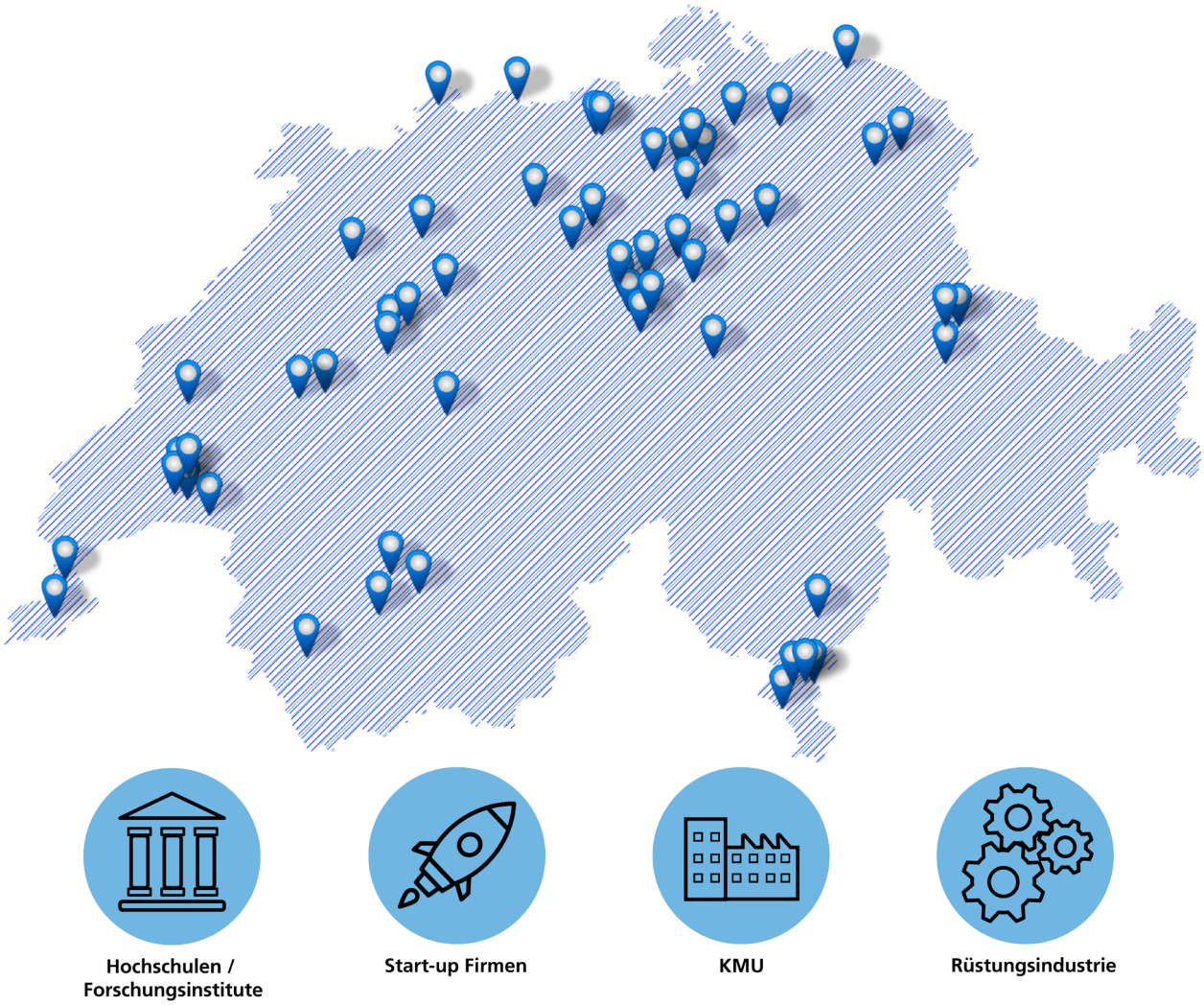


Abbildung 9: Partnerkategorien des Kompetenznetzwerks von armasuisse.

Das umfangreiche Kompetenznetzwerk muss laufend gemäss dem Bedarf und dem technologischen Fortschritt in Schlüsseltechnologien für Schweizer Sicherheitskräfte weiterentwickelt werden. Der Aufbau von Wissen mit Hilfe von Netzwerken erfolgt im Rahmen von Projekten und als Auftrag zur Klärung konkreter Forschungsaspekte (Auftragsforschung). Dabei wird der Forschungspartner im Voraus nach dem Add-On-Prinzip evaluiert. Dies bedeutet, dass sich die Auftragsvergabe primär an den bereits vorhandenen Kompetenzen des Forschungspartners orientiert und nach Möglichkeit nur diejenigen Aspekte als Forschungsgegenstand definiert werden, welche für Sicherheitskräfte spezifisch sind. Durch die Fokussierung auf einen Technologiereifegrad zwischen 3 und 5 vermeidet man zudem die Investition in Grundlagenforschung, welche grundsätzlich durch andere Quellen wie den SNF gespiesen werden.

Es gibt aber auch Technologien für Sicherheitskräfte, bei denen es in der Schweiz nur in ausgewählten Bereichen geeignete Forschungspartner gibt. Teilweise können solche Lücken durch Kooperationen mit ausländischen Forschungspartnern gefüllt werden. Zum Teil werden in diesem Fall die Forschungsprojekte aber auch direkt innerhalb von armasuisse durchgeführt.

5.2 Schnittstellen zu anderen Bundesämtern

Die Koordination der Schnittstellen zu anderen Bundesämtern und bundesnahen Organisationen im Forschungsbereich wird durch den interdepartementalen Koordinationsausschuss für Ressortforschung des Bundes sichergestellt. In Arbeitsgruppen und Workshops werden gemeinsame Interessen der verschiedenen Bundesämter identifiziert, um so Synergien bei der Erstellung der verschiedenen Forschungskonzepte zu

nutzen und Doppelspurigkeiten zu vermeiden. Ferner bietet diese Plattform auch die Möglichkeit zum Austausch mit dem SNF und Innosuisse, den beiden wichtigsten nationalen Förderorganisationen für Forschung und Innovation. So hat armasuisse auch die Möglichkeit auf Fachstufe sowohl zu den Vorschlägen des SNF im Rahmen der Nationalen Forschungsprogramme (NFP) und Forschungsschwerpunkte (NFS) Stellung zu nehmen, als auch die Flagship-Programme von Innosuisse zu kommentieren. Damit kann die Ressortforschung von armasuisse nahtlos an die nationalen Forschungs- und Innovationsförderungsinstrumente anknüpfen.

Durch die Koordination mit anderen Bundesämtern konnten folgende thematische Kooperationsfelder identifiziert werden:

- Bundesamt für Bevölkerungsschutz (BABS): Forschung in den Bereichen Biotoxine und Nachweis von biologischen Kampfstoffen, Messung und Kartierung von Radioaktivität mit Hilfe von Drohnen, Trendanalysen und Schutz kritischer Infrastrukturen
- Bundesamt für Energie (BFE) und Bundesamt für Zivilluftfahrt (BAZL): Beteiligung am Förderprogramm «Swiss Energy research for the Energy Transition» (SWEET) zur Herstellung von synthetischem Kerosin im Rahmen des Aktionsplans «Energie und Klima VBS»
- Bundesamt für Cybersicherheit: Technische Unterstützung durch Trendanalysen und Forschungsaktivitäten im Rahmen der Umsetzung der nationalen Cyberstrategie (NCS)
- Abteilung Internationale Sicherheit (AIS) im Staatsekretariat des Eidgenössischen Departements für auswärtige Angelegenheiten (EDA): Technische Beratung in den Bereichen der künstlichen Intelligenz und der Robotik im Rahmen multilateraler Verhandlungen

Ferner existiert im Rahmen der Ressortforschung für den Politikbereich «Sicherheits- und Friedenspolitik» eine Arbeitsgruppe, die aus Vertretern des BABS, der AIS und des Bundesamts für Rüstung (armasuisse) besteht. In dieser Arbeitsgruppe werden aufgrund der sicherheits- und friedenspolitischen Vorgaben die Leitlinien für die Forschungskonzepte erarbeitet und deren operative Umsetzung in prioritären Themenfeldern und Projekten abgestimmt.

5.3 Internationale Zusammenarbeit

Der Zusatzbericht zum Sicherheitspolitischen Bericht 2021 hält unter anderem fest, dass die internationale Kooperation der Schweiz im Bereich der Sicherheitspolitik und ihrer Umsetzung verstärkt werden soll. Auch wenn die NATO das bisherige Zusammenarbeitsformat «Partnerschaft für den Frieden» (PfP) weiterführt, ist sie doch dazu übergegangen eine massgeschneiderte Zusammenarbeit mit Partnerstaaten anzustreben, was der Schweiz entgegenkommt. So haben die NATO und die Schweiz in einem Individually Tailored Partnership Programm (ITPP) die strategischen Ziele ihrer Zusammenarbeit festgelegt, wobei unter anderem auch vorgesehen ist, die technisch-wissenschaftliche Kooperation durch die Etablierung eines strategischen Dialogs und die praktische Umsetzung in Form gemeinsamer Forschungs-, Innovations- und Entwicklungsvorhaben zu vertiefen. Hinsichtlich Forschung bedeutet dies ein Ausbau des Engagements in der «Science and Technology Organisation» (STO) der NATO. Dies soll durch die Vertretung der Schweiz in zusätzlichen Steuergruppen (Panels) erreicht werden. In Bezug auf Innovation bietet sich der Defence Innovation Accelerator für the North Atlantic (DIANA) als Zusammenarbeitsplattform an. Das Angebot der STO erstreckt sich von Ausbildungskursen in bestimmten technisch-wissenschaftlichen Gebieten, über Expertentreffen zu ausgewählten Themen bis hin zur Durchführung von gemeinsamen Studien und Forschungsprojekten. Der Austausch mit internationalen Experten und die gemeinsamen Forschungsaktivitäten erbringen eine sehr hohe Wertschöpfung und Erkenntnisse, welche sonst kaum mit vernünftigem Aufwand erschlossen werden können. Die Erfahrungen bezüglich der Teilnahme an NATO/PfP STO Aktivitäten sind durchwegs positiv.

Die Unterzeichnung einer administrativen Vereinbarung mit der Europäischen Verteidigungsagentur (EVA) im Jahr 2012 ermöglicht der Schweiz an Forschungsaktivitäten der EVA teilzunehmen. Diese sind in fähigkeitsbasierten Technologiebereichen, sogenannten CapTechs organisiert. Ziel dieser CapTechs ist die Koordination und Förderung der europäischen Forschungszusammenarbeit, insbesondere auch der Industrie, im Bereich der Verteidigungstechnologien. Die Schweiz ist heute in fünf CapTechs vertreten. Im Gegensatz zu den Forschungsrahmenprogrammen der europäischen Kommission erfolgt die Finanzierung von CapTech-Projekten durch Aufteilung der Kosten unter den beteiligten Ländern, was zu einem

erheblichen Koordinationsaufwand und auch zu einer gewissen Ineffizienz führt. Das Engagement des Hub for EU Defence Innovation (HEDI) erschliesst für die Schweiz neue Möglichkeiten in der Umsetzung ihrer Innovationsvorhaben und ist somit eine logische Fortsetzung aus den Tätigkeiten im Rahmen der CapTechs.

Schliesslich findet internationale Zusammenarbeit auch im Rahmen von Staatsverträgen, bi- oder trilateralen Kooperationsvereinbarungen und davon abgeleiteten technischen Vereinbarungen statt. Dabei wird die Kooperation mit staatlichen oder staatlich finanzierten Instituten im Ausland gesucht, welche sehr oft spezifische Kompetenzen in Technologien für Sicherheitskräfte ausweisen können, welche in der Schweiz nicht verfügbar sind. Neben der bilateralen Zusammenarbeit mit dem nahen Ausland ist erwähnenswert, dass im Rahmen eines trilateralen Abkommens zwischen Deutschland, Österreich und der Schweiz (DACH) 2023 ein Absprachedokument unterzeichnet wurde, welches die Kooperation in der militärischen Forschung und Entwicklung zwischen den drei Ländern vereinfachen soll. Ferner existiert seit 2019 auch eine Research, Development, Test and Evaluation (RDT&E) Vereinbarung, welche Kooperationen mit Forschungslaboratorien der amerikanischen Streitkräfte erlaubt.

6 Organisation und Qualitätssicherung

6.1 Interne Organisation

In armasuisse ist der Kompetenzbereich Wissenschaft und Technologie für die Leitung und Durchführung der Forschung verantwortlich. Dies erfolgt im Rahmen der zugewiesenen NFB-Leistungsgruppe «Technologiemanagement und Expertisen». Das Technologiemanagement ist eine bereichsübergreifende Tätigkeit, die von der Früherkennung und Bewertung von Technologien bis zur Erstellung von Technologie-Roadmaps für mögliche Beschaffungen reicht, jedoch mit einem Schwerpunkt auf der Schnittstelle zwischen Forschungsprogrammen und den verschiedenen Innovationsgefässen innerhalb des VBS. Die Ziele sind nicht nur die Verringerung technologischer und finanzieller Risiken, sondern auch die Mitwirkung an der militärischen Gesamtplanung. Um diesen Auftrag zu erfüllen, führt armasuisse W+T gezielte angewandte Forschungsaktivitäten durch, um technologische Kompetenzen aufzubauen, die für die mittelfristige Erfüllung der Aufgaben des VBS unabdingbar sind. Die Grundlagen für die Abstimmung der Forschungstätigkeiten mit dem Bedarf der militärischen Gesamtplanung bilden die ZUVA sowie die Vereinbarung über die Zusammenarbeit zwischen dem Departementsbereich Verteidigung und armasuisse Wissenschaft und Technologie vom 16. November 2017.

Für die Erarbeitung des Langfristigen Forschungsplans und der jährlichen Umsetzungsplanung ist der Fachbereich «Forschungsmanagement und Operations Research» verantwortlich. Der LFP wird nach erfolgter Vernehmlassung innerhalb des Departements durch den Rüstungschef freigegeben. Der Kompetenzbereichsleiter W+T bewilligt die jährliche Umsetzungsplanung. Die geplanten Forschungsschwerpunkte mit den prioritären Themenfeldern des vorliegenden LFP werden durch Forschungsprogramme bearbeitet, welche auf die erforderlichen und zukünftigen Fähigkeiten der Schweizer Armee ausgerichtet sind. Die designierten Programmverantwortlichen legen durch systematische Bedarfsanalysen bei den relevanten Anspruchsgruppen die inhaltliche Priorität der Forschungsprogramme fest und stellen deren Umsetzung sicher. Für die strategisch korrekte Ausrichtung des Programmportfolios und deren Finanzierung sorgt die Forschungsaufsicht, welche aus Vertretern des Armeestabs und armasuisse W+T zusammengesetzt ist. Sie richtet ihren Fokus auf die Zweckmässigkeit, die Wirksamkeit und die Wirtschaftlichkeit der Forschung von armasuisse.

Forschungsprogramme umfassen in der Regel mehrere mittel- bis langfristig zu bearbeitende Kompetenzfelder, in welchen verschiedene Projekte bearbeitet werden. Um den Wissenstransfer von der Forschung zugunsten der Expertisentätigkeit für Armee und Sicherheitskräfte bereitzustellen, erfolgt die Projektleitung innerhalb der Fachbereiche von armasuisse W+T. Die Umsetzung der Forschung erfolgt in Form einer Matrixstruktur, wodurch die Kompetenzen der internen Experten auf den aktuellen Stand von Technik und Wissenschaft gebracht werden können. Forschungsprojekte werden teilweise intern, in vielen Fällen aber mit Partnern aus Hochschulen und Wirtschaft im Rahmen sogenannter Auftragsforschung bearbeitet. Die Vergabe von Forschungsaufträgen basiert auf dem Bundesgesetz über das öffentliche Beschaffungswesen (BöB, SR 172.056.1). Forschungsverträge werden weitgehend auf der Basis der Allgemeinen Vertragsbedingungen des Bundes für Forschungsverträge vergeben, welche durch das Eidgenössische Finanzdepartement (EFD) und die Beschaffungskonferenz des Bundes (BKB) erarbeitet wurden. Abweichungen zu diesen Regelungen werden im Forschungsvertrag schriftlich festgehalten. Dies betrifft insbesondere die Publikationsrechte und die Verwertung des geistigen Eigentums, welches im Rahmen des Forschungsauftrags entsteht. Das Projektmanagement folgt den internationalen Standards für Projektmanagement, um die Qualität zu gewährleisten. Die wissenschaftliche Qualität der Forschungsarbeiten wird sowohl durch eine sorgfältige Auswahl der Forschungsinstitution sichergestellt, als auch durch eine Evaluation der wissenschaftlichen Arbeiten und Erkenntnisse.

6.2 Qualitätssicherung

Der interdepartementale Koordinationsausschuss für die Ressortforschung des Bundes hat 2014 Richtlinien zur Qualitätssicherung in der Forschung der Bundesverwaltung erlassen, welche die drei Teilbereiche Forschungsmanagement, Berichterstattung und Wirksamkeitsprüfung umfassen. Die Umsetzung des Qualitätssicherungskonzeptes liegt in der Verantwortung der Bundesstellen und kann flexibel auf die Gegebenheiten angepasst werden.

Bei armasuisse wurden in der Periode 2021-2024 folgende Qualitätssicherungsmassnahmen umgesetzt:

- Die rechtzeitige Verfügbarkeit von Kompetenzen für die Erstellung von Expertisen, eine Hauptzielsetzung der Forschung, wurde im Rahmen der VA/IAFP-Zielsetzungen der Leistungsgruppe «Technologiemanagement und Expertisen» erhoben und hinsichtlich Erreichungsgrad beurteilt. Allenfalls wurden Massnahmen abgeleitet.
- Die ZUVA und das Konzept zur Weiterentwicklung der fähigkeitsorientierten Streitkräfteentwicklung (WE FOSKE) legten die Abstimmung der Forschungstätigkeiten mit dem Bedarf der militärischen Gesamtplanung fest.
- Die Prozesse der Forschung mit der entsprechenden Regelung der Zuständigkeiten, welche im integrierten Managementsystem (IMS) der armasuisse hinterlegt sind, wurden einem regelmässigen Review unterzogen und im Rahmen der Re-Zertifizierung (ISO 9001) von einer unabhängigen Stelle auditiert.
- Um eine angemessene Ausrichtung der Forschungsprogramme zu gewährleisten, wurden die entsprechenden Kompetenzfelder jährlich überprüft und während eines Workshops mit den Stakeholdern abgestimmt. Die Überprüfung des Forschungsprogramm-Portfolios und der prioritären Themenfelder erfolgte jährlich durch die Forschungsaufsicht.
- Für die Gewährleistung eines gezielten Aufbaus von Expertennetzwerken wurden potenzielle Forschungspartner systematisch evaluiert. Um die Effektivität der systematischen Bewertungen zu erhöhen, wird die «Technologie- und Marktmonitoring»-Applikation weiterentwickelt. Die neue Version sollte bis 2025 einsatzbereit sein.
- Die wissenschaftliche Qualität der Forschung wurde sichergestellt, indem vorzugsweise mit Forschungspartnern zusammengearbeitet wird, welche national und international einen ausgezeichneten Ruf geniessen und auch in anerkannten Fachzeitschriften und Fachkonferenzen regelmässig publizieren.
- Forschungsarbeiten wurden regelmässig mit internen und externen wissenschaftlich tätigen Experten diskutiert, so dass die Qualität der Forschungsresultate durch Zweit- und Drittmeinungen verifiziert werden konnten.
- Die Projektmanagementkompetenzen im Forschungsumfeld wurden gesteigert, indem für Mitarbeitende interne oder externe Weiterbildungsmassnahmen, wie die Erlangung eines Zertifikats der International Project Management Association (IPMA) oder die Absolvierung eines Lehrgangs in Certificate of Advanced Studies in Research Management, ermöglicht wurden.

Für die Periode 2025-2028 sind folgende Massnahmen vorgesehen:

- Die Qualitätssicherungsmassnahmen der Periode 2021-2024 werden beibehalten bzw. fortgeführt. Dazu gehören der Review interner Prozesse, die Erfassung und Beurteilung der Wirksamkeit von Forschungstätigkeiten, die Gewährleistung der bedarfsgerechten Ausrichtung der Forschungsthemen und die Sicherstellung der wissenschaftlichen Qualität von Resultaten und Erkenntnissen.
- Die Weiterbildung der wissenschaftlich tätigen Mitarbeitenden wird sowohl auf der Fach- als auch auf der Managementebene aktiv gefördert.
- Zur Steigerung der Attraktivität von armasuisse W+T als Arbeitgeber für talentierte junge Wissenschaftler werden in Kooperation mit akademischen Ausbildungsstätten gemeinsame Aktivitäten wie Fellowships, Wettbewerbe, Summerschools, Praktika oder Konferenzen gefördert.
- Die Qualität laufender wissenschaftlicher Arbeiten von externen Partnern wird mit Hilfe geeigneter Instrumente beurteilt. Neben externen Audits ist grundsätzlich auch eine Erhebung mittels eines internen Erhebungssystems denkbar.
- Die Qualität des Wissens- und Erkenntnistransfers aus der Forschung zur Förderung von Innovationen im Umfeld der Sicherheitskräfte wird verstärkt. Dies erfordert eine engere Zusammenarbeit zwischen armasuisse W+T und den verschiedenen Innovationsverantwortlichen im VBS, unter anderem durch Anwendung von modernen Kreativmethoden, agilem Projektmanagement sowie Think-Tank-Ansätzen.

6.3 Verbreitung des Wissens

Die verschiedenen Forschungsprogramme von armasuisse mit ihren zahlreichen Forschungsprojekten und Kooperationen produzieren eine grosse Menge an Wissen. Die Forschungsprojekte werden bei armasuisse W+T von Mitarbeitenden der Linienorganisation betreut. Damit ist sichergestellt, dass die wissenschaftlichen Kompetenzen an derjenigen Stelle in der Organisation aufgebaut werden, an der sie zur Erstellung von Expertisen erforderlich sind. Spezielle

interne Massnahmen für den Transfer von Erkenntnissen innerhalb von armasuisse W+T sind somit nicht mehr notwendig. Es ist jedoch wichtig, eine Strategie zu haben, um einen optimalen Wissenstransfer zu den verschiedenen beteiligten Partnern zu erreichen. Um dieses Ziel zu erreichen, werden die Ergebnisse so weit wie möglich zugänglich gemacht, und zwar in verschiedenen Formen wie z. B. in Jahresberichten, bei verschiedenen Veranstaltungen wie Workshops, Projektpräsentationen und Symposien, durch die Teilnahme an Konferenzen oder die Veröffentlichung in wissenschaftlichen Zeitschriften. Wichtig zu erwähnen ist auch, dass das Wissen aus der Forschung nicht nur für die fähigkeitsorientierte Streitkräfteentwicklung zur Verfügung gestellt wird, sondern auch für potenzielle Innovationsprojekte, deren Bewertung, Umsetzung und schliesslich den Transfer der Ergebnisse in die Truppe. Zudem soll so der Transfer der Forschungserkenntnisse über die Armeeplanung in die Armee sichergestellt werden. Die Realisierung einer Wissensmanagement-Plattform zur Verbreitung der Erkenntnisse aus der Forschung wird geprüft.

Projektinformationen wie umfassende Angaben zum jeweiligen Stand der Projekte und deren Resultate inkl. Forschungsberichte werden auf ARAMIS (Administration Research Actions Management Information System) elektronisch abgelegt und aktualisiert. ARAMIS ist das elektronische Informationssystem über die Forschungs- und Entwicklungsprojekte des Bundes. Für ein breiteres Publikum hat jedes Forschungsprogramm eine eigene Internetseite, auf der allgemeine Informationen wie Fact-Sheets, Kompetenzbereiche und verschiedene Berichte veröffentlicht werden.

Anhang 1: Abkürzungsverzeichnis

Abkürzung	Bedeutung
3D	Drei-Dimensional
5G	5. Generation (Mobilfunk)
A Stab	Armeestab
ABC	Atomar, Chemisch und Biologisch
AIS	Abteilung Internationale Sicherheit
AFM	Abteilung Frieden und Menschenrechte
AR	Augmentierte Realität
ar	armasuisse
ARAMIS	Administration Research Actions Management Information System
BABS	Bundesamt für Bevölkerungsschutz
BAZL	Bundesamt für Zivilluftfahrt
BFE	Bundesamt für Energie
BFI	Bildung, Forschung und Innovation
BFS	Bundesamt für Statistik
BKB	Beschaffungskonferenz des Bundes
BöB	Bundesgesetz über das öffentliche Beschaffungswesen
BV	Bundesverfassung
C2	Command and Control
CapTech	Capability Technology (Group of EVA)
CCDCoE	Cooperative Cyber Defence Centre of Excellence
CD&E	Concept Development and Experimentation
CER	Cyber- und elektromagnetischer Raum
CO_2	Kohlenstoffdioxid
COTS	Commercial off-the-shelf
COVID-19	Coronavirus-Erkrankung
CSS	Center for Security Studies (der ETH Zürich)
DACH	Deutschland, Österreich, Schweiz
DDoS	Distributed Denial of Service
DIANA	Defence Innovation Accelerator for the North Atlantic
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDF	European Defence Fund
EFD	Eidgenössisches Finanzdepartement
EMP	Elektromagnetischer Puls
ESA	European Space Agency
EPFL	École Polytechnique Fédérale de Lausanne
ETHZ	Eidgenössische Technische Hochschule Zürich
EU	Europäische Union
EVA	Europäische Verteidigungsagentur
fedpol	Bundesamt für Polizei (Federal Police)
FIFG	Forschungs- und Innovationsförderungsgesetz
FS Daten V	Funktionsstrategie Daten Verteidigung
FOSKE	Fähigkeitsorientierte Streitkräfteentwicklung
GEOINT	Geospacial Intelligence
GNSS	Global Navigation Satellite Systems
GO	Geschäftsordnung

Abkürzung	Bedeutung
GTP	Generative Pre-trained Transformers
HALE	High Altitude Long Endurance
HAP	High Altitude Platform
HEDI	Hub for EU Defence Innovation
HEFA	Hydroprocessed Esters and Fatty Acids
HPM	High Power Microwaves
HUMINT	Human Intelligence
IAFP	Integrierte Aufgaben und Finanzplanung
IED	Improvised Explosive Device
IKT	Informations- und Kommunikationstechnologien
IMINT	Image Intelligence
IMS	Integriertes Managementsystem
IoT	Internet of Things
IPMA	International Project Management Association
IschV	Informationsschutzverordnung
ISG	Bundesgesetz über die Informationssicherheit beim Bund
ISO	International Standardisation Organisation
ITPP	Individually Tailored Partnership
Kdo	Kommando
KMU	Kleine und mittlere Unternehmen
KI	Künstliche Intelligenz
LBA	Logistikbasis der Armee
LFP	Langfristiger Forschungsplan
MALE	Medium Altitude Long Endurance
MASINT	Measurement and Signature Intelligence
Mat-V	Verordnung des VBS über das Armeemeterial
MD DGA	Militärdoktrin Doktringrundlage der Armee
MG	Militärgesetz
MILAK	Militär Akademie
MOTS	Military off-the-Shelf
NATO	North Atlantic Treaty Organization
NATO/STO	NATO/Science and Technology Organisation
NASA	National Aeronautics and Space Administration
NAZ	Nationale Alarmzentrale
NCS	Nationale Cyber Strategie
NDB	Nachrichtendienst des Bundes
NDG	Nachrichtendienstgesetz
NDV	Nachrichtendienstverordnung
NFB	Neues Führungsmodell für die Bundesverwaltung
NFP	Nationale Forschungsprogramme
NFS	Nationale Forschungsschwerpunkte
OODA	Observe-Orient-Decide-Act
OSINT	Open Source Intelligence
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
OV	Organisationsverordnung
PESTEL	Political, Economic, Social, Technological, Legal, Environment
PfP	Partnership for Peace

Abkürzung	Bedeutung
PtX	Power-to-X
RADINT	Radar Intelligence
RDT&E	Research, Development, Test and Evaluation
RUAG	RüstungsUnternehmen-AktienGesellschaft
SAF	Sustainable Aviation Fuels
SAR	Synthetic Aperture Radar
SDR	Software Defined Radio
SDRZ	Schweizer Drohnen- und Robotikzentrum
SIGINT	Signal Intelligence
SNF	Schweizerischer Nationalfonds
SNFW	Sensor-Nachrichtendienst-Führungs-Wirkungsverbund
SOCMINT	Social Media Intelligence
SR	Systematische Sammlung des Bundesrechts
STIB	Sicherheitsrelevante Technologie- und Industriebasis
STO	Science and Technology Organisation (der NATO)
SWEET	Swiss Energy research for the Energy Transition
TRL	Technology Readiness Level
UAV	Unmanned Aerial Vehicle
UGV	Unmanned Ground Vehicle
UNO	United Nations Organisation
USA	United Staates of America
USB	Universal Serial Bus
V	Departementsbereich Verteidigung
VA/IAFP	Voranschlag mit integriertem Aufgaben- und Finanzplan
V-FIFG	Verordnung zum Bundesgesetz über die Förderung der Forschung und Innovation
V-NDA	Verordnung über den Nachrichtendienst der Armee
VBS	Departement für Verteidigung, Bevölkerungsschutz und Sport
VISINT	Visual Intelligence
VöB	Verordnung über das öffentliche Beschaffungswesen
WEA	Weiterentwicklung der Armee
W+T	Kompetenzbereich Wissenschaft und Technologie von armasuisse
ZUVA	Weisungen über die Zusammenarbeit der Departementsbereiche Verteidigung und armasuisse

Anhang 2: Gesetzliche Grundlagen und strategische Dokumente

Stufe Bund

- Bundesverfassung (BV) SR 101, Art. 2 Zweck, Art. 57-60 Sicherheit, Landesverteidigung, Art 64. Forschung, 01. Januar 2024
- Bericht des Bundesrates, Die Sicherheitspolitik der Schweiz, 24. November 2021
- Bericht des Bundesrates, Zusatzbericht zum Sicherheitspolitischen Bericht 2021 über die Folgen des Krieges in der Ukraine, 07. September 2022
- Nationale Cyberstrategie (NCS), 13. April 2023
- Bundesgesetz über die Förderung der Forschung und Innovation (FIFG), SR 420.1, insb. Art. 16, Art 42, Art 45, 01. Juli 2023
- Verordnung zum Bundesgesetz über die Förderung der Forschung und der Innovation (V-FIFG), insb. Art. 24-25, SR 420.11, 01. September 2023
- Verordnung über das Informationssystem ARAMIS über Forschungs- und Innovationsprojekte des Bundes (ARAMIS-Verordnung), SR 420.171, 01. Januar 2014.
- Bundesgesetz über die Informationssicherheit beim Bund (ISG), SR 128, 01. Januar 2024
- Verordnung über den Schutz von Informationen des Bundes (ISchV), SR 510.411, 01. September 2023
- Bundesgesetz über das öffentliche Beschaffungswesen (BöB), SR 172.056.1, 01. Januar 2024
- Verordnung über das öffentliche Beschaffungswesen (VöB), SR 172.056.11, 01. September 2023
- Qualitätssicherung in der Ressortforschung des Bundes - Richtlinien, 1. Revision vom 26. März 2014
- Grundsätze für die Erstellung der Konzepte 2025-2028 betreffend die Forschungsaktivitäten der Bundesverwaltung in den 11 Politikbereichen, Oktober 2022
- Weltraumpolitik 2023, 19. April 2023
- Bundesgesetz zur Nutzung des Weltraums (in Erarbeitung)

Stufe VBS

- Bundesgesetz über die Armee und die Militärverwaltung (Militärgesetz, MG), SR 510.10, 1. Januar 2024
- Verordnung des VBS über die Beschaffung, die Nutzung und die Ausserdienststellung von Material (MatV), SR 514.20, 18. August 2020
- Weisungen über die Zusammenarbeit der Departementsbereiche Verteidigung und armasuisse (ZUVA), 28. März 2018
- Organisationsverordnung für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (OV-VBS), SR 172.214.1, 01. Januar 2024
- Geschäftsordnung VBS (GO-VBS), 01. Januar 2024
- Strategie Cyber VBS 2021-2024, März 2021
- Verordnung über die militärische Cyberabwehr, SR 510.921, 01. Januar 2024
- Bundesgesetz über den Nachrichtendienst (Nachrichtendienstgesetz, NDG), SR 121, 01. Januar 2024
- Verordnung über den Nachrichtendienst (Nachrichtendienstverordnung, NDV), SR 121.1, 01. Januar 2024
- Grundsätze des Bundesrates für die Rüstungspolitik des VBS, 24. Oktober 2018
- Rüstungsstrategie VBS, 01. Januar 2020
- Departementsstrategie VBS, Vision, Handlungsfelder und strategische Initiativen, 15. September 2022
- Aktionsplan Energie und Klima VBS, Juni 2021

Stufe Departementsbereich Verteidigung

- Die Verteidigungsfähigkeit stärken – Zielbild und Strategie 2023, Zentrum für digitale Medien der Armee DMA, 81.298d
- Grundlagenbericht Luftverteidigung der Zukunft, Sicherheit im Luftraum zum Schutz der Schweiz und ihrer Bevölkerung, Mai 2017
- Grundlagenbericht Zukunft der Bodentruppen, Weiterentwicklung der Fähigkeiten der Bodentruppen, Mai 2019
- Grundlagenbericht Gesamtkonzeption Cyber, Konzeption der Weiterentwicklung der Fähigkeiten der Schweizer Armee im Cyber- und elektromagnetischen Raum bis Mitte der 2030er-Jahre, Februar 2022
- Grundlagenbericht Gesamtkonzeption Weltraum (in Erarbeitung)
- Militärdoktrin 2017 - Doktringrundlagen der Armee (MD 17 DGA), 07. Juli 2019
- Doktrinale Grundlage Cyberraum und elektromagnetischer Raum (CER), Entwurf, Stand 31. März 2023
- Verordnung über den Nachrichtendienst der Armee (V-NDA), SR 510.291, 01. September 2023
- Investitionsplanung der Armee 2023 bis 2035, 07. September 2022
- Armeebotschaft (jährlich)

Stufe Departementsbereich armasuisse

- Geschäftsordnung Bundesamt für Rüstung, 15. August 2017
- Managementsystem armasuisse (IMS ar): Technologie- und Forschungsmanagement (Prozess Id 2.20.25 und Dok Id 40031)
- IAFP: Integrierte Aufgaben und Finanzplanung armasuisse 2025-2027, Band 2A, Leistungsgruppe Technologiemanagement und -Expertisen (S. 347-351), 24. August 2023
- Langfristiger Forschungsplan 2021-2024 (Wissenschaft und Technologie, armasuisse), 30. November 2020