Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Schweizer Armee

GESAMTKONZEPTION CYBER

Konzeption der Weiterentwicklung der Fähigkeiten der Schweizer Armee
im Cyber- und elektromagnetischen Raum
bis Mitte der 2030er-Jahre

Inhalt

Zusammenfassung		**7**
1	**Einleitung**	**17**
2	**Umfeld und Entwicklungstendenzen**	**27**
3	**Organisatorische und rechtliche Grundlagen**	**49**
4	**Doktrin**	**59**
5	**Fähigkeiten**	**75**
6	**Weiterentwicklung und Umsetzung**	**87**
7	**Kooperation mit Partnern im Rahmen des SVS bzw. mit Dritten**	**101**
Anhang		**105**

Inhalt

1 Einleitung 18

1.1 Anlass 19

1.2 Ziel und Zweck 20

1.3 Völkerrechtliche Ausgangslage 21

1.4 Grundlagen und Rahmenbedingungen 22

2 Umfeld und Entwicklungstendenzen 28

2.1 Internationales Umfeld 29

2.2 Nationales Umfeld 35

2.3 Technologieentwicklung als Herausforderung 36

2.4 Erkenntnisse 45

3 Organisatorische und rechtliche Grundlagen 50

3.1 Einleitung 50

3.2 Organisatorische Entwicklungen 50

3.3 Bestehende Rechtsgrundlagen 54

3.4 Ausblick 56

4 Doktrin 60

4.1 Einführung 60

4.2 Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen im CER 60

4.3 Bedrohungen 63

4.4 Wissens- und Entscheidvorsprung 70

5 Fähigkeiten 76

5.1 Grundsätzliche Fähigkeitsanforderungen 76

5.2 Herleitung der Fähigkeiten 76

5.3 Fähigkeit CER-Eigenschutz 77

5.4 Fähigkeit Lageverständnis im Verbund 79

5.5 Fähigkeit Datenverarbeitung robust und sicher 80

5.6 Fähigkeit Führung im Verbund organisatorisch und technisch 81

5.7 Fähigkeit Aktionen im elektromagnetischen Raum 82

5.8 Fähigkeit Aktionen im Cyberraum 83

5.9 Handlungsbedarf 85

6 Weiterentwicklung und Umsetzung 88

6.1 Rahmen und Eckwerte der Optionsentwicklung 88

6.2 In allen Optionen umzusetzende Massnahmen 88

6.3 Option 1 90

6.4 Option 2 92

6.5 Option 3 94

6.6 Optionenbewertung 96

6.7 Eckwerte zur Umsetzung der Option 3 97

6.8 Umsetzung 98

7 Kooperation mit Partnern im Rahmen des SVS bzw. mit Dritten 102

7.1 Subsidiäre Unterstützung 102

7.2 Kooperation 102

7.3 Ausbildung 103

8 Anhang 106

8.1 Anhang 1: Zusammenstellung der zu schliessenden Fähigkeitslücken 106

8.2 Anhang 2: Werte der Ausprägungen in den Netzdiagrammen der Optionen in Kapitel 6 107

8.3 Anhang 3: Abkürzungsverzeichnis / Glossar 108

8.4 Anhang 4: Literaturverzeichnis 111

Inhalt

Abbildungen

1: Grafische Darstellung der drei Optionen 12

2: Umsetzungsschritte Option 3 14

3: Wirkungsräume 19

4: Der CER im Zusammenhang mit allen weiteren Wirkungsräumen 20

5: Cybersicherheit in der Bundesverwaltung (Strategie Cyber VBS, 2021) 22

6: Cyberdefence-Dispositiv VBS (Strategie Cyber VBS, 2021) 24

7: Prinzip eines Angriffs auf die Vertraulichkeit im Cyberraum 61

8: Prinzip eines Angriffs auf die Vertraulichkeit im elektromagnetischen Raum 61

9: Prinzip eines Angriffs auf die Integrität im Cyberraum 62

10: Prinzip eines Angriffs gegen die Verfügbarkeit im Cyberraum 62

11: Prinzip eines Angriffs gegen die Verfügbarkeit im elektromagnetischen Raum 62

12: Übersicht Akteure und Wirkungsräume 68

13: Prinzip Wissens- und Entscheidvorsprung 71

14: Fähigkeitsausprägung Option 1 90

15: Fähigkeitsausprägung Option 2 92

16: Fähigkeitsausprägung Option 3 95

17: Fokus der Investitionen 97

18: Schritte der Umsetzung Option 3 99

Tabellen

1: Operationelle Fähigkeiten CER und deren Einbettung in die Cyberdefence-Strategie VBS 77

2: Fähigkeitslücken CER-Eigenschutz 106

3: Fähigkeitslücken Lageverständnis im Verbund 106

4: Fähigkeitslücken Datenverarbeitung robust und sicher 106

5: Fähigkeitslücken Führung im Verbund 106

6: Fähigkeitslücken Aktionen im Elektromagentischen Raum 107

7: Fähigkeitslücken Aktionen im Cyberraum 107

Zusammenfassung

Die Gesamtkonzeption Cyber zeigt die Herausforderungen im Cyber- und elektromagnetischen Raum (CER) sowie in der Informations- und Kommunikationstechnologie (IKT) auf und beschreibt, welche Fähigkeiten die Schweizer Armee bis Mitte der 2030er-Jahre entwickeln muss, um auch künftigen Bedrohungen begegnen zu können

Diese Weiterentwicklung muss das Gesamtsystem «Armee» (Verwaltung, Fachbereiche, Truppengattungen und Dienstzweige) berücksichtigen, weil sie weite Teile der Armee betrifft.

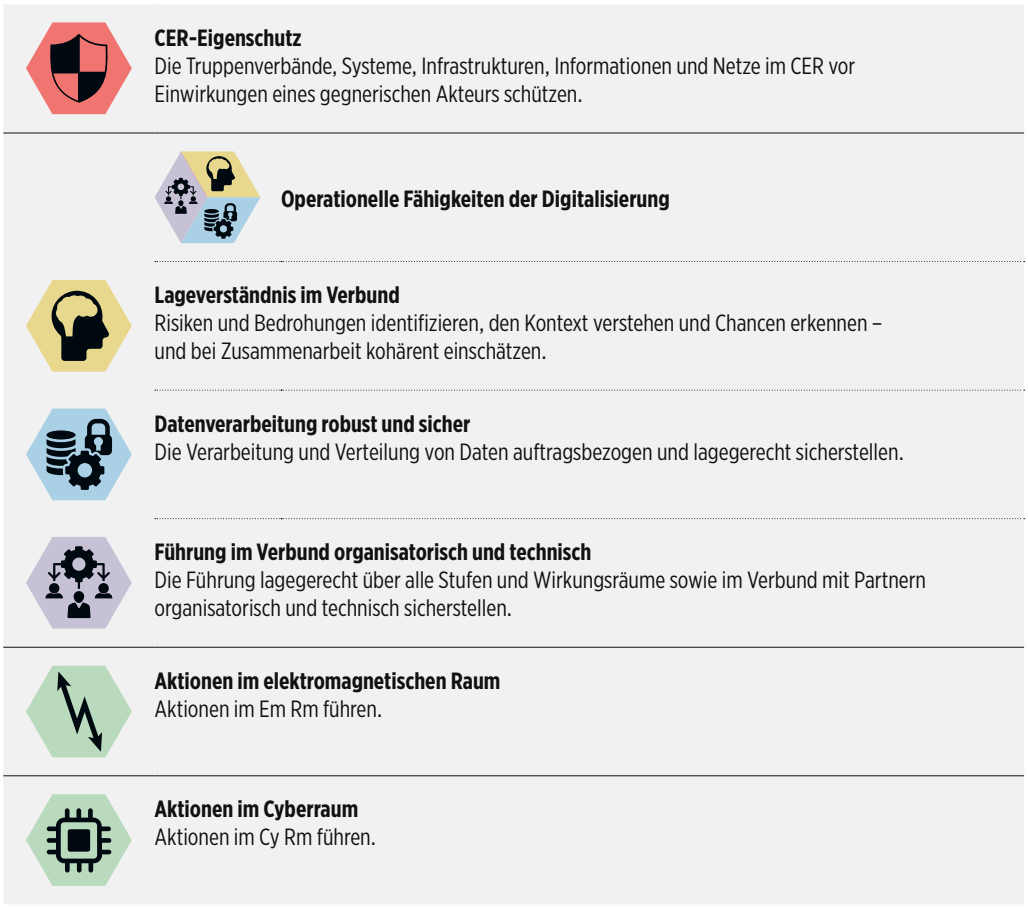
Der CER ist eine etablierte Dimension unter anderem zur Machtausübung, Konfliktvorbereitung und -führung, sowohl in zivilen als auch in militärischen Bereichen. In den letzten Jahren haben Staaten und nichtstaatliche Akteure Desinformation und Propaganda eingesetzt, die zivile Telekommunikation gestört und Attacken mit Malware durchgeführt. Vermehrt wurden auch Cyberangriffe gegen Energie-Infrastrukturen und Behörden durchgeführt. Gegenüber herkömmlichen Aktionen lassen sich Angriffe im CER schwieriger zurückverfolgen und einem Staat bzw. einem Urheber zuordnen. Dadurch wird eine Sanktion oft unmöglich, was die Hemmschwelle für Cyberangriffe senkt.

Der Cyberraum der Armee umfasst alle durch die Armee betriebenen und genutzten Informatiksysteme (IKT-Systeme). Alle Daten und Informationen sowie die Nutzer der IKT-Systeme gehören ebenfalls zum Cyberraum. Der elektromagnetische Raum dient insbesondere zur funkbasierten (elektromagnetischen) Übertragung von Informationen und zur räumlichen Ortung und Identifizierung von Objekten. Der CER ist das Bindeglied zwischen den physischen Wirkungsräumen (Boden, Luft, maritimer Raum, Weltall) und vernetzt diese. Es ist somit für jegliche Militäroperation von zentraler Bedeutung, die Fähigkeiten im CER zu unseren Gunsten einzusetzen und unter unserer Kontrolle zu behalten. Die operative Führung muss Armeeeinsätze deshalb ganzheitlich, über alle Wirkungsräume vernetzt und mit den passenden Mitteln planen, führen und steuern können, um jederzeit die erwartete Wirkung zu erzielen. Ob die Armee ihren Auftrag erfüllen kann, hängt deshalb mehr und mehr davon ab, wie sie ihre eigenen IKT-Systeme sowie die eigenen Daten und Informationen vor den vielfältigen Bedrohungen im CER schützen kann – und dies über alle Lagen in allen Teilen der Armee.

Die Gesamtkonzeption Cyber stellt als Grundprinzip den Wissens- und Entscheidvorsprung in den Fokus. Wer zuerst agiert, kann den gegnerischen Akteur in die Rolle des Reagierenden zwingen und so die Oberhand über das Geschehen erlangen. So ist im Einsatz wahrscheinlich jene Partei erfolgreich, die unter anderem rascher die richtigen Entscheidungen trifft. Um das Ziel zu erreichen, geht es also darum, einen Handlungsvorsprung zu erreichen und dafür die begrenzten eigenen Mittel zeitgerecht sowie präzis einzusetzen.

Die Armee steht in einem vielfältigen Spannungsfeld. Sie muss sich nicht nur ihren aktuellen Aufgaben stellen: Auch künftige Bedrohungen, Herausforderungen und die immer schnelleren Entwicklungen im CER muss sie rechtzeitig antizipieren. Zudem muss sie über rasche Abläufe verfügen, um Schritt halten zu können. Da Operationen der Armee in der Regel unter Einbezug aller Möglichkeiten im CER durchgeführt werden, muss sie sich gesamtheitliche Fähigkeiten über alle Wirkungsräume erarbeiten. Über diese Fähigkeiten verfügt die Armee heute noch nicht.

Die vorliegende Gesamtkonzeption beleuchtet die Frage, über welche Fähigkeiten die Armee im CER und in der IKT ab 2030 verfügen muss, um ihren Auftrag langfristig über alle Lagen erfüllen zu können. Zudem wird geklärt, in welchem Umfang die Armee auch Partner (z. B. BABS, SVS, andere Bundesstellen und Behörden sowie Partner in Wirtschaft und Gesellschaft) bei der Bewältigung dieser Herausforderungen unterstützen kann bzw. soll. In den ersten Kapiteln wurden aus dem nationalen und internationalen Kontext wichtige Umfeld- und Entwicklungstendenzen sowie doktrinelle Grundlagen für die Armee hergeleitet, die schliesslich in sechs grundlegende Fähigkeiten gefasst wurden:



Darauf aufbauend wurden drei Optionen ausgearbeitet, welche auf die Bedürfnisse der gesamten Armee eingehen. Zudem berücksichtigen sie die künftigen Entwicklungen und Erneuerungen aus den anderen Wirkungsräumen und integrieren die oben genannten operationellen Fähigkeiten in jeweils unterschiedlichen Ausprägungen. Alle Optionen können bis Mitte der 2030er-Jahre personalneutral, durch Umlagerung innerhalb der Gruppe Verteidigung, umgesetzt werden.

In der Option 1 werden die Cyber- sowie die elektromagnetischen Fähigkeiten auf Stufe Armee gebündelt. Das Schwergewicht der Weiterentwicklung liegt nahezu vollständig beim CER-Eigenschutz und bei den Fähigkeiten im Cyberraum. Auf einen Ausbau der entsprechenden Fähigkeiten bis auf die untere taktische Stufe (Bataillon und Kompanie) wird verzichtet, ebenso auf eine Ausrüstung von Kampfverbänden mit den dazu erforderlichen Mitteln. Dadurch fehlt aber eine adäquate Antwort auf eine mögliche hybride Konfliktführung in stark überbautem Gelände, wie es für die Schweiz charakteristisch ist.

Die Option 2 befähigt die Mehrheit der Verbände der Bodentruppen in ihren jeweiligen Einsatzräumen zu eigenständigen Einsätzen im Cyber- und elektromagnetischen Raum. Dazu werden in den Kampfkompanien kleine, spezialisierte Teams, bestehend aus jeweils rund zehn Armeeangehörigen, aufgebaut. Diese werden mit Systemen ausgerüstet, die es erlauben, kleine, einfache Angriffe im Cyber- und elektromagnetischen Raum durchzuführen. Eine solche Weiterentwicklung der Fähigkeiten in der Breite und Tiefe hätte jedoch ebenfalls bedeutende Nachteile: Sie wäre nicht nur teuer, sondern hätte auch technisch hohe Anforderungen, weil es dafür weitgehend automatisierte Systeme bräuchte, die im Cyber-Bereich heute noch nicht verfügbar sind. Zudem wäre es fraglich, ob die Armee genügend geeignete Milizangehörige und Berufspersonal rekrutieren könnte.

Option 3 zielt darauf ab, dass sich die Armee künftig umfassend vor Angriffen aus dem Cyber- und elektromagnetischen Raum schützen kann. Der Schutz bezieht sich sowohl auf permanent als auch auf temporär betriebene Systeme (z. B. Waffensysteme mit hohem IKT-Anteil). Vor allem der Eigenschutz gegen Bedrohungen aus dem elektromagnetischen Raum ist im Vergleich zu den anderen Optionen deutlich ausgeprägter. Der Eigenschutz soll grundsätzlich zentral gewährleistet werden, wofür die erforderlichen, qualitativ hochstehenden Fähigkeiten – wie heute – in einem spezialisierten Bataillon auf Stufe Armee zusammengefasst werden sollen. Ein punktueller, dezentraler Schutz von wichtigen Infrastrukturen soll jedoch ebenfalls möglich sein. Dazu können anderen Verbänden der Armee (oder bei Bedarf zivilen Partnern) bedarfsgerecht Mittel aus dem Cyber-Bataillon zugewiesen oder unterstellt werden. Mit dem ausgeprägten Eigenschutz setzt die Armee nicht zuletzt eine wichtige Forderung der NCS um, nämlich, dass alle Akteure für ihren eigenen Schutz die Verantwortung tragen und folglich in der Lage sein müssen, sich möglichst selbstständig vor Risiken und gegen Bedrohungen im Cyberraum zu schützen.

Einander gegenübergestellt sehen die drei Optionen folgendermassen aus:

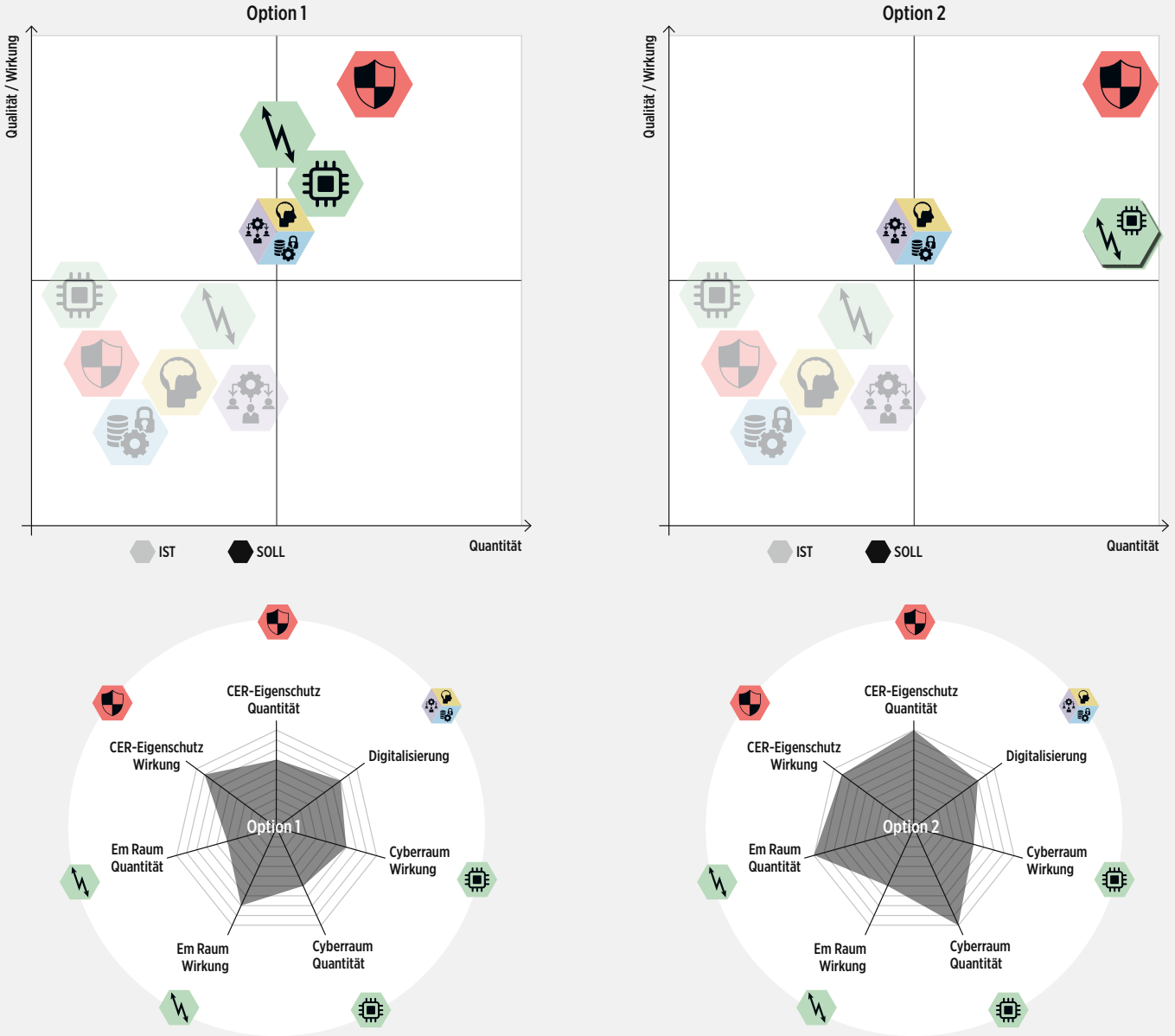
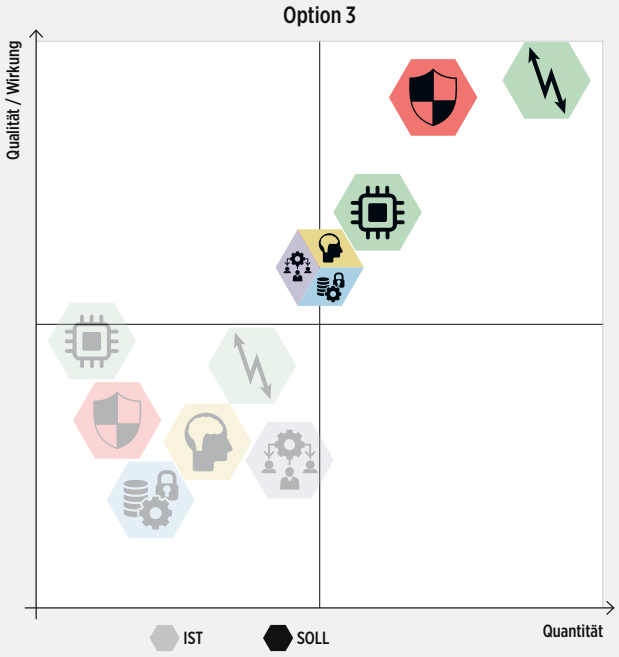
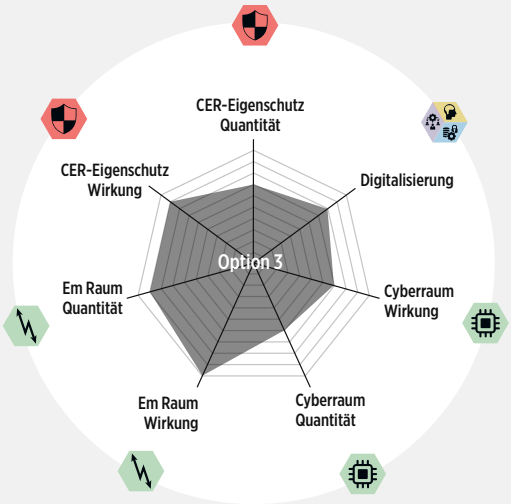
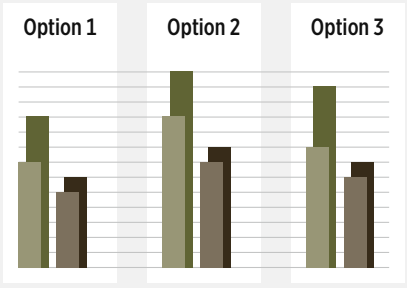


Abbildung 1: Grafische Darstellung der drei Optionen

Aufgrund der vorgenommenen Bewertung schlägt die Expertengruppe des VBS vor, die Option 3 zu wählen. Sie bietet einen höheren militärischen Nutzen, d. h. sie unterstützt in hohem Masse die militärische Auftragserfüllung. Entsprechend den Verhältnissen auf dem Schweizer Arbeitsmarkt wird der geschätzte Bedarf an qualifizierten Spezialistinnen und Spezialisten als realistisch eingeschätzt. Option 3 schafft zudem gute Voraussetzungen, um den künftigen Herausforderungen im CER begegnen zu können. Insgesamt bietet sie ein ausgeglichenes und zukunftsorientiertes Fähigkeits- und Leistungsprofil zur Erfüllung des Armeeauftrags ab 2030.







Option	Investitions-kosten Mia CHF	Truppe Ada
1	1,4 – 2,0	5000 – 6000
2	2,0 – 2,6	7000 – 8000
3	1,6 – 2,4	6000 – 7000

Betriebskosten/Jahr: ca. 15% der Investitions-kosten

Die Umsetzung der Option 3 soll in drei Schritten erfolgen. Nachfolgend sind die Grobziele für jeden Schritt ausgeführt:

Der Schritt 1 hat zum Ziel, den bestehenden CER-Eigenschutz primär zentral weiter auszubauen und die Fähigkeiten zu Aktionen im Cyber- und elektromagnetischen Raum zu erhalten bzw. in Teilen auszubauen. Zudem wird die Grundfähigkeit in der Anwendung von Data Science aufgebaut. Data Science befasst sich mit der Analyse von grossen Datenbeständen, die im Hinblick auf strategische oder operationelle Fragestellungen ausgewertet werden.

Der Schritt 2 hat zum Ziel, die Resilienz der Kerninfrastrukturen zum CER-Eigenschutz auszubauen. Die Fähigkeit zum dezentralen CER-Eigenschutz und zur Forensik im Einsatzraum wird aufgebaut. Nach Umsetzung dieses Schrittes soll – unter Berücksichtigung des Bedarfs, der sich aus der Führungsfähigkeit der Armee ergibt – eine lokale, autonome IKT-Infrastruktur für die Truppe zur Verfügung stehen, sogenannte Lokalknoten. Weiter werden die Fähigkeiten zu Aktionen im Cyber- und elektromagnetischen Raum erhalten und teilweise ausgebaut.

Der Schritt 3 hat zum Ziel, die Fähigkeiten der Bataillone und Kompanien zu eigenständigen Aktionen im elektromagnetischen Raum bis auf die gefechtstechnische Führungsstufe auszubauen. Bis auf dieselbe Führungsstufe wird die Fähigkeit zum Eigenschutz gegen Bedrohungen aus dem elektromagnetischen Raum aufgebaut. Ab 2032 sollen zudem die Grosssysteme der Bodentruppen erneuert werden. Dies dient dazu, Wirk- und Selbstschutzsysteme im elektromagnetischen Raum in die neuen Plattformen zu integrieren oder, minimal, aufeinander abzustimmen und damit Synergien zu nutzen. Im Cyberraum wird die Fähigkeit zur Aufklärung und Wirkung gegen militärische Systeme weiter ausgebaut und neuen Technologien angepasst.

Die Abbildung zeigt den ungefähren Zeithorizont der Umsetzungsschritte auf. Da gewisse Massnahmen über den gesamten Zeithorizont aufgebaut werden und gegenseitige Abhängigkeiten bestehen, können sie nicht eindeutig voneinander getrennt werden. Es wird daher beschrieben, welche Massnahmen als Hauptfokus pro Schritt umgesetzt werden sollen.

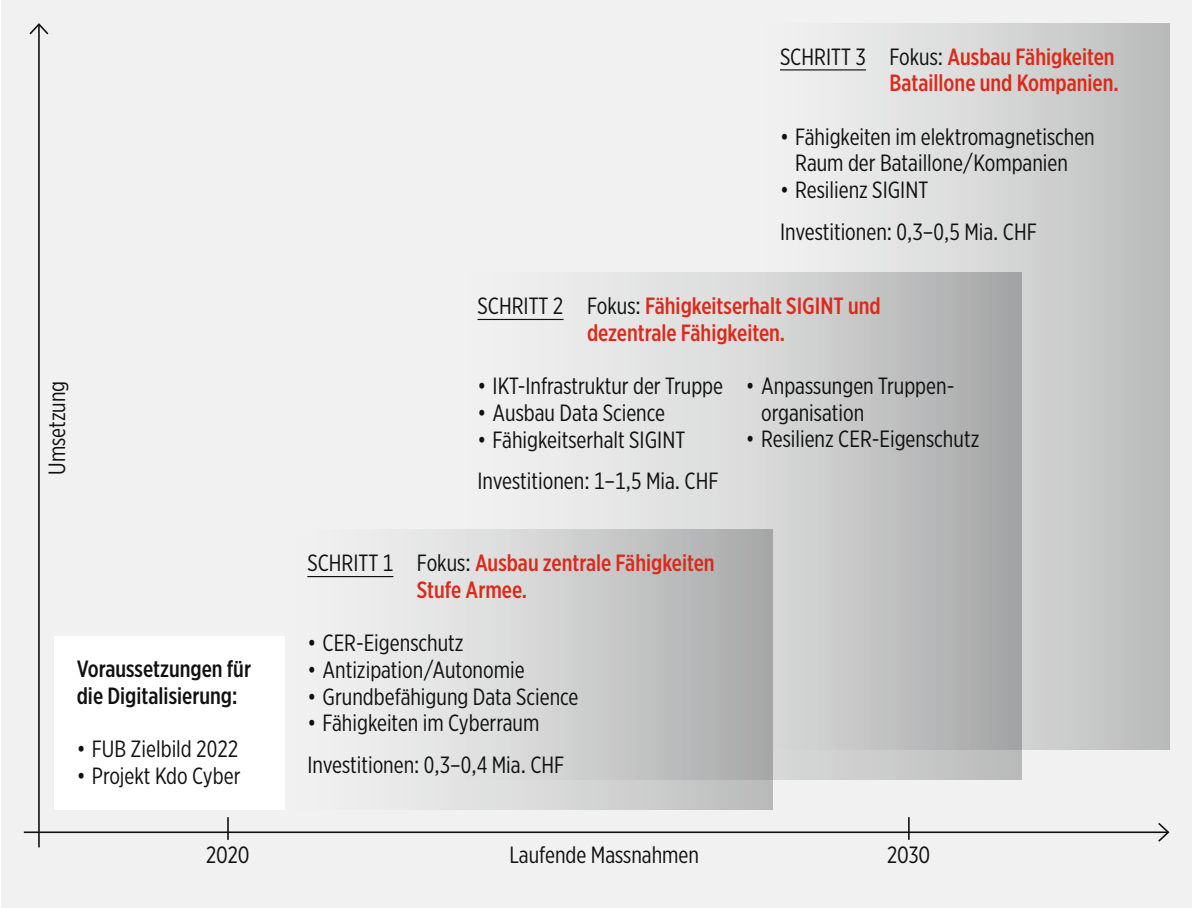


Abbildung 2: Umsetzungsschritte Option 3

1

Einleitung

Aktuelle Konflikte werden mit starkem Einbezug des Elektromagnetischen und des Cyberraums 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. Für die Weiterentwicklung der Armee ist die Berücksichtigung der Herausforderungen im CER notwendig.

1 Einleitung

Im Cyber- und im elektromagnetischen Raum (CER) gab es in den letzten Jahren bedeutende und schnell eintretende Veränderungen. Die Entwicklungen in diesen beiden Räumen beeinflussten sich gegenseitig stark, so dass sie immer näher zusammenrückten: Heute lassen sich Aktionen meistens nicht mehr eindeutig dem Cyber- oder elektromagnetischen Raum zuordnen. Geografische Grenzen, wie sie insbesondere auf dem Boden, aber auch im Luftraum bestehen, sind im CER kaum relevant. Aus diesen Gründen werden die zwei Wirkungsräume üblicherweise in einem einzigen Wirkungsraum zusammengefasst, dem CER.

CER

Der CER bezeichnet den Cyber- und den elektromagnetischen Raum, den gesamten IKT-Bereich sowie die Daten- und Informationslogistik [1].

Cyberraum der Armee

Der Cyberraum der Armee umfasst alle Daten und Informationen und die durch die Armee betriebenen oder genutzten IKT-Systeme – unabhängig vom Wirkungsraum, dem sie physisch zugeordnet sind.

Elektromagnetischer Raum

Der elektromagnetische Raum dient zur technischen Übertragung von Informationen (funkbasierte Signalübertragung), zur räumlichen Ortung von Objekten (Radar, Funkortung) und zur elektronischen Kriegführung (EKF) mittels elektromagnetischer Wellen verschiedener Frequenzen.

Die enge Verflechtung der Wirkungsräume innerhalb des CER ist eine Tatsache. Veränderungen in diesen Räumen erfolgen ausserordentlich schnell und beeinflussen meistens gleichzeitig beide Wirkungsräume. Zudem greifen die virtuellen Wirkungsräume im CER immer stärker auf die anderen, physischen Wirkungsräume über wie Boden, Luftraum, maritimer Raum und Weltraum. Der CER gewinnt dadurch zunehmend an Bedeutung.

Diese Entwicklung stellt Gesellschaft, Staat und Wirtschaft vor neue Herausforderungen. Die wechselseitigen Abhängigkeiten bringen eine hohe Komplexität mit sich. Die Gefahr von Störungen nimmt zu – physische und virtuelle Systeme werden verletzlicher. Dadurch wird die Forderung nach Eigenschutz stärker.

Ein moderner Konflikt ohne Aktionen im CER ist heute und in Zukunft undenkbar. Die Schweizer Armee muss in diesem Umfeld permanent fähig sein, Nachrichten zu beschaffen, sich zu schützen, (subsidiär) zu helfen sowie eigenständig zu kämpfen. Dies über alle Lagen und abgestimmt auf ihre Aktionen in anderen Wirkungsräumen.

Als Streitkraft geht es für die Armee darum, den CER als militärischen Wirkungsraum in die Planung und Durchführung ihrer Einsätze einzubeziehen und sich selbst zu schützen, sowie relevante Partner bei deren Schutz wo notwendig zu unterstützen.

1 Daten- und Informationslogistik: Dies beinhaltet die Bearbeitung, Speicherung und Verteilung von Informationen und Daten innerhalb der Schweizer Armee.

1.1 Anlass

Die Armee hat den Auftrag, die Schweiz und ihre Bevölkerung zu schützen und zu verteidigen, zivile Behörden zu unterstützen, die Lufthoheit zu wahren und Beiträge an die Friedensförderung zu leisten. Damit sie all diese Aufgaben erfüllen kann, muss sie die Kohärenz ihrer Aktionen über alle Wirkungsräume gewährleisten können (siehe Abbildung 3: Wirkungsräume).

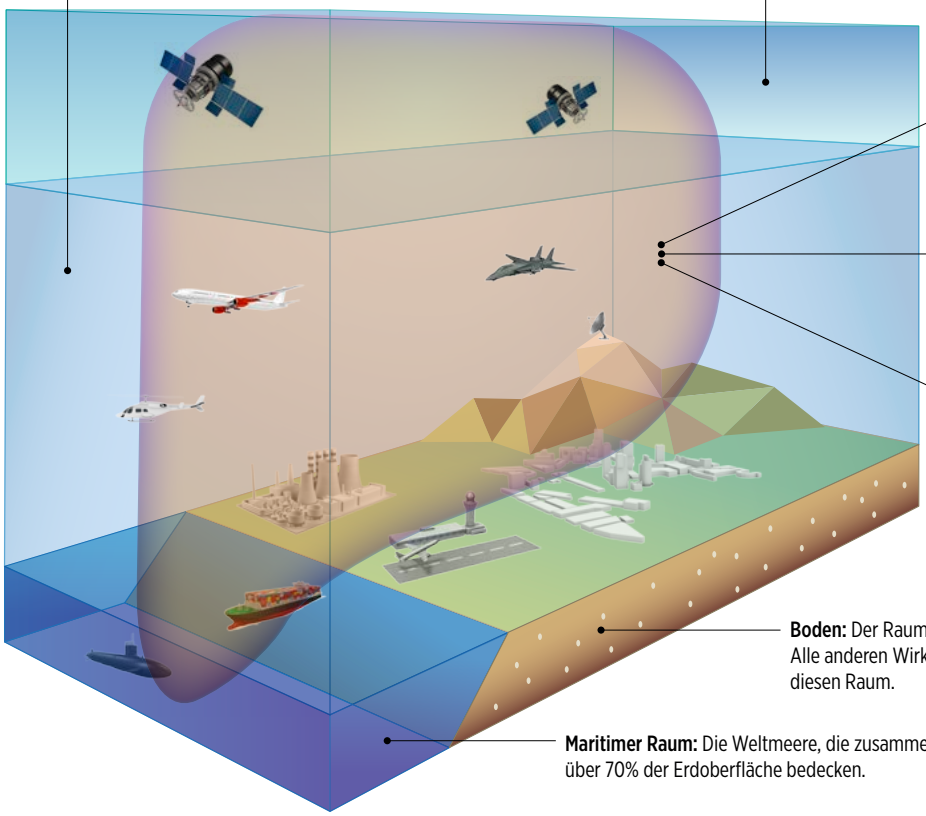


Abbildung 3: Wirkungsräume

Wie in der Abbildung 4 dargestellt, ist der CER ein Bindeglied zwischen dem Informationsraum und den physischen Wirkungsräumen Boden, Luftraum, maritimer Raum und Weltraum. Er ermöglicht den Austausch von Daten und Informationen zwischen Sensoren, Wirkmitteln und der Führung – auch wirkungsraumübergreifend. Nur mit der Nutzung des CER werden die immer komplexeren Einsätze der Armee plan- und führbar.

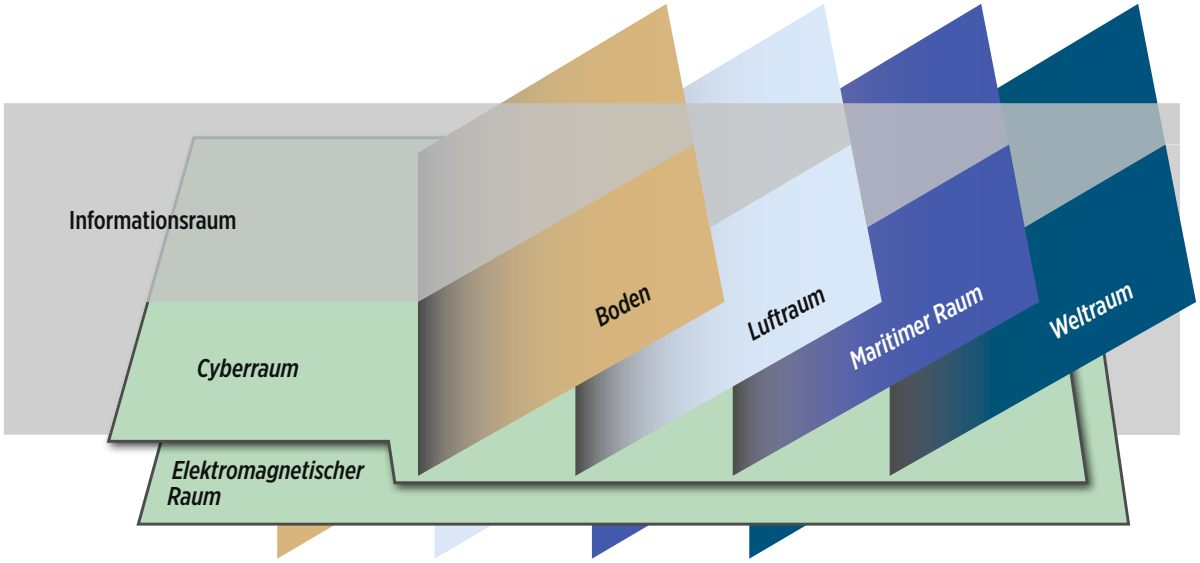


Abbildung 4: Der CER im Zusammenhang mit allen weiteren Wirkungsräumen

1.2 Ziel und Zweck

Die vorliegende Gesamtkonzeption dient dazu, die nötigen Massnahmen zur Weiterentwicklung der Fähigkeiten im Bereich des Cyberraums, des elektromagnetischen Raums sowie der Informations- und Kommunikationstechnologie (IKT) anzustossen. Sie soll eine gemeinsame Vorstellung in diesem Bereich schaffen und eine Vorgabe für die Planungen der 2020er- bis in die 2030er-Jahre darstellen.

Die Konzeption nimmt die Erkenntnisse zum CER und zur IKT aus den beiden vorhergehenden Berichten zur mittel- bis längerfristigen Weiterentwicklung der Armee, dem Bericht «Luftverteidigung der Zukunft» (2017) und dem Bericht «Zukunft der Bodentruppen» (2019) auf und vertieft bzw. konkretisiert sie. Des Weiteren stützt sie sich auf den Sicherheitspolitischen Bericht (Sipol B) 2021, die «Nationale Strategie der Schweiz vor Cyberrisiken» (2018) und auf die «Strategie Cyber des VBS» (2021).

Dabei geht es darum, die CER-Thematik und ihre Bedeutung für die zukünftige Ausrichtung der Armee sowie für die Zusammenarbeit mit Partnern in einem breiteren Kontext darzustellen. Zu beachten sind dabei insbesondere auch völkerrechtliche Aspekte sowie vorhandene Grundlagen und Rahmenbedingungen.

Im Zentrum steht die Frage, über welche Fähigkeiten die Armee im CER künftig verfügen muss, um ihren Auftrag längerfristig erfüllen zu können. Weiter wird die Frage zu beantworten sein, in welchem Umfang Partner unterstützt werden sollen und können.

Zur Beantwortung dieser Fragen gilt es, folgende Themen zu beleuchten:

a) Die nationale und internationale Situation und deren künftige Entwicklung haben einen wesentlichen Einfluss darauf, welche CER-Fähigkeiten die Armee aufbauen und wie sie mit Daten und Informationen umgehen will. Ebenfalls eine Rolle spielen Technologieentwicklung, Fragen der Digitalisierung, aber auch Rahmenbedingungen in der Bildungslandschaft und der Wirtschaft. Nicht zuletzt müssen sich die Konzepte der Armee in den Gesamtrahmen des Bundes einfügen, der beispielsweise in der Nationalen Strategie der Schweiz zur Abwehr von Cyber-Risiken (NCS) oder in der «Strategie Digitale Schweiz» beschrieben ist.

b) Verschiedene Akteure führen regelmässig Aktionen gegen Ziele in der Schweiz durch – auch gegen die Armee. Cyberangriffe gegen IKT-Systeme der Armee haben nachweislich stattgefunden. Auch Funk- und Kabelaufklärung sind eine Realität. Weltweit werden Aktionen durchgeführt, um Meinungen durch gezielte Informationsverbreitung zu beeinflussen. Die Fähigkeiten der Armee haben sich darum auch an der konkreten, täglichen Bedrohung im und aus dem CER auszurichten.

c) Die Anforderungen an die anstehenden Erneuerungen des Luftlage- und Einsatzsystems, der neuen Kampfflugzeuge und der bodengestützten Luftverteidigung zeigen auf, wie zentral die Vernetzung der Systeme ist: Damit die Armee ihre Mittel effizient einsetzen kann, müssen Aktionen zeitlich präzise aufeinander abgestimmt ablaufen. Voraussetzung dafür ist ein digitalisierter und flexibler Verbund von Sensoren, Wirkmitteln und Führung. Diese Entwicklung stellt hohe Anforderungen an eine einheitliche IKT-Architektur und zwingt zu standardisierten Anwendungen in der Armee und der Militärverwaltung.

1.3 Völkerrechtliche Ausgangslage

Die Schweiz ist an die Regeln des Völkerrechts gebunden – insbesondere an die verfassungs- und völkerrechtlich verankerten Grund- und Menschenrechtsgarantien «off- und online». Aus völkerrechtlicher Sicht gelten für Armee und Nachrichtendienst grundsätzlich die gleichen Regeln wie für andere staatliche Organe. Ihre Handlungen sind deshalb an die entsprechenden völkerrechtlichen Vorgaben gebunden.

Es gilt zu unterscheiden zwischen den allgemeinen Regeln des Völkerrechts, die insbesondere in Friedenszeiten Anwendung finden einerseits, und den Regeln des humanitären Völkerrechts andererseits[2]. Letztere gelten ausschliesslich in bewaffneten Konflikten und werden innerhalb der Armee auch als Kriegsvölkerrecht bezeichnet. Das allgemeine Völkerrecht gilt für alle Gegenmassnahmen der Armee und des Nachrichtendienstes als Reaktion auf einen internationalen Cybervorfall, wenn dieser unterhalb der Schwelle eines bewaffneten Angriffs auf Informationssysteme der Armee oder kritische Infrastrukturen der Schweiz erfolgt.[3] Auf staatliche Operationen im Cyberraum sind insbesondere die völkerrechtlichen Prinzipien der staatlichen Souveränität[4], des Interventionsverbots[5] und des Gewaltverbots[6] anwendbar. Während bewaffneten Konflikten kommt zudem das humanitäre Völkerrecht (Kriegsvölkerrecht) als lex specialis zur Anwendung (Gewohnheits- und Vertragsrecht). Es muss auch bei Operationen im CER respektiert werden. In Bezug auf die Kriegführung sind dies insbesondere die Grundsätze der Unterscheidung, der Vorsicht und der Verhältnismässigkeit. Auch

2 Abgeleitet aus: https://www.eda.admin.ch/content/dam/eda/de/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_DE.pdf
3 Vgl. Erläuterungen Verordnung über die militärische Cyberabwehr MCAV (SR 510.921); UNO Charta, Artikelentwürfe der Völkerrechtskommission (International Law Commission – ILC) über die Verantwortlichkeit von Staaten für völkerrechtswidriges Handeln aus dem Jahre 2001 (ILC Artikelentwürfe). Die Artikelentwürfe stellen grösstenteils Völkergewohnheitsrecht dar.
4 Vgl. Art. 2 Ziff. 1 UNO-Charta.
5 Abgeleitet aus Art. 2 Ziff. 1 UNO-Charta und nach Völkergewohnheitsrecht.
6 Vgl. Art. 2 Ziff. 4 UNO-Charta.

weitere Bestimmungen des Kriegsvölkerrechts mit gewohnheitsrechtlichem Charakter sind für Aktionen im CER relevant und müssen respektiert werden. Beispiele sind das Verbot der Heimtücke[7] oder der besondere Schutz gewisser Personen und Objekte[8]. Bei der Prüfung, Entwicklung, Beschaffung oder Einführung neuer Waffen, Mittel oder Methoden der Kriegführung ist zudem zu prüfen, ob ihre Verwendung stets oder unter bestimmten Umständen durch das Kriegsvölkerrecht oder durch andere anwendbare Regeln des allgemeinen Völkerrechts verboten wäre.[9] Darunter fallen auch Cyberwaffen sowie Mittel und Methoden der Cyberkriegführung.

Bei Aktionen im inhärent internationalen Cyberraum stellen sich zahlreiche Fragen der Rechtsanwendung auf allen Führungsebenen. Auf strategischer Stufe muss die Zulässigkeit von Massnahmen überhaupt beurteilt werden (allgemeines Völkerrecht). Auf operativer Stufe muss der anwendbare Rechtsrahmen eruiert werden (Menschenrechte, Kriegsvölkerrecht), und auf taktischer Stufe müssen konkrete Fragen der Rechtsanwendung geklärt werden: im Kontext eines bewaffneten Konflikts beispielsweise die Pflicht zur Unterscheidung von legitimen militärischen Zielen (militärische Objekte, Kombattanten, bewaffnete Gruppen, direct participation in hostilities etc.) oder die Abgrenzung zwischen erlaubter Kriegslist und verbotener Heimtücke. Dabei muss auch eine unité de doctrine über alle Wirkungsräume sichergestellt werden.

1.4 Grundlagen und Rahmenbedingungen

Botschaft zur Legislaturplanung 2019–2023

Die Digitalisierung als eines der Hauptziele in der Legislaturplanung bezieht sich grundsätzlich auf die Bundesverwaltung, den Service Public und die Wirtschaft.

Sicherheitspolitischer Bericht 2021

Der Sicherheitspolitische Bericht 2021 fordert unter anderem die Verstärkung des Schutzes vor Cyberbedrohungen und eine stärkere Ausrichtung der Armee auf das hybride Konfliktbild.

Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS 2.0) 2018–2022

Die NCS wurde vom Bundesrat verabschiedet und ist zurzeit die wichtigste Leitlinie auf Bundesebene. Sie gliedert sich wie in folgender Abbildung dargestellt:

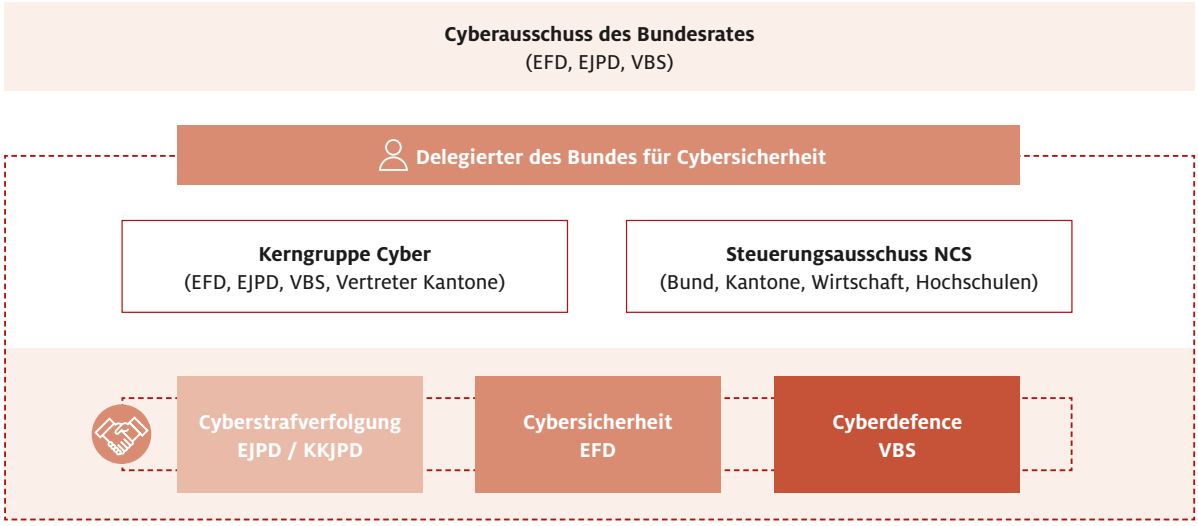


Abbildung 5: Cybersicherheit in der Bundesverwaltung (Strategie Cyber VBS, 2021)

7 Vgl. Art. 37 Zusatzprotokoll I zu den Genfer Abkommen.
8 Beispielsweise der Schutz von Kulturgut (Art. 53 Zusatzprotokoll I), von Anlagen und Einrichtungen, die gefährliche Kräfte enthalten (Art. 56 Zusatzprotokoll I) oder von Sanitätseinrichtungen (Art. 12 Zusatzprotokoll I).
9 Vgl. Art. 36 Zusatzprotokoll I sowie Art. 11 Materialverordnung VBS (MatV).

Die politische Führung obliegt dem Cyber-Ausschuss des Bundesrates, der vom Vorsteher des eidgenössischen Finanzdepartementes präsidiert wird. Unter der Leitung des Delegierten des Bundes für Cybersicherheit stehen der Steuerungsausschuss NCS und die Cyber-Kerngruppe. Ebenfalls ersichtlich sind die drei Säulen der NCS: Cyberstrafverfolgung, Cybersicherheit und Cyberdefence mit den jeweils verantwortlichen Organisationen.

Die NCS beinhaltet folgende, für die Armee wesentliche Treiber:

— Zentrale (thematische) Führung – dezentrale Ausführung (föderaler Ansatz) der Umsetzung.
— Einfache und direkte Zusammenarbeit aller Beteiligten und auf allen notwendigen Stufen.
— Anspruch an die Armee, ihre Cybermittel zur subsidiären Unterstützung zur Verfügung zu stellen.

Die Armee ist als Teil des nationalen Gesamtdispositivs in der NCS 2.0 eingebunden. Die darin festgelegten Aufgaben sind für die Armee verbindlich. Sie zeigen bereits eine Richtung auf, welche die Gesamtkonzeption Cyber einschlagen wird.

IKT-Strategie des Bundes 2020–2023[10]

Die aktuelle IKT-Strategie formuliert Massnahmen und Ziele entlang von vier Stossrichtungen. Für die Armee bedeutend ist hier primär der Grundsatz der spezifischen und komplementären Leistungserbringung als interner Leistungserbringer des Bundes.

Der Bund hat sich ferner das Ziel gesetzt, Supportprozesse und IKT-Grundleistungen zu bündeln. Die zukünftig zuständige Organisationseinheit muss hier die spezifischen Anforderungen der Armee berücksichtigen. Zu diesem Zweck ist eine eigene Verordnung für die Armee im Bereich Informatik geplant (Armeeinformatik-Verordnung).

Strategie des Bundesrates für eine digitale Schweiz

Die Strategie des Bundesrates für eine digitale Schweiz verfolgt primär das Ziel, die digitalen Infrastrukturen zu erhalten, auszubauen und zu fördern. Zudem soll sie den erforderlichen Sicherheitsaspekten Rechnung tragen und den Schutz vor Cyberrisiken gewährleisten. Dazu ist zurzeit eine Studie in Erarbeitung. Die Armee ist in Teilbereichen ebenfalls betroffen.

Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022

Diese Strategie definiert 17 Massnahmen, mit denen der Bundesrat die Versorgungssicherheit in der Schweiz erhalten und in wesentlichen Bereichen verbessern will. Den zuständigen Aufsichts- und Regulierungsbehörden hat er den Auftrag erteilt, in allen Sektoren der kritischen Infrastrukturen zu prüfen, ob es erhebliche Risiken für gravierende Versorgungsstörungen gibt. Geeignete Massnahmen sollen solche Risiken reduzieren.

Grundlagenberichte Bodentruppen und Luftverteidigung der Zukunft

Die beiden Berichte «Zukunft der Bodentruppen» und «Luftverteidigung der Zukunft» ergeben die Grundlage und den Rahmen bezüglich Streitkräfteentwicklung in den kommenden Jahren.

Strategie Cyber VBS 2021-2024

Cyberdefence ist ein Teil der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS). Der Aktionsplan Cyberdefence VBS (APCD) aus dem Jahr 2017 definierte zum ersten Mal übergreifend die Aufgaben, Kompetenzen und Prozesse der VBS-Ver-

10 Durch den Beschluss A2021-008_B2021-031 zur digitalen Transformation und IKT-Lenkung Bund vom 4. Oktober 2021 wird das Papier neu als «Digitalisierungsstrategie des Bundes» bezeichnet.

waltungseinheiten im Umgang mit Cyberdefence. Die darin festgelegten Massnahmen wurden bis Ende 2020 umgesetzt. Die Strategie Cyber VBS baut auf den Erkenntnissen des APCD auf. Sie dient dem VBS und seinen Verwaltungseinheiten dazu, sich gezielt und ganzheitlich auf die sich ständig ändernden Anforderungen vorzubereiten.

Das Cyberdefence-Dispositiv des VBS ist in der Abbildung mit ihren Hauptbereichen unten dargestellt. Im Zentrum stehen vier Kernbereiche, in denen die Strategie mit Massnahmenfeldern und Pflichtenheften die konkreten Ziele bis 2024 festlegt.

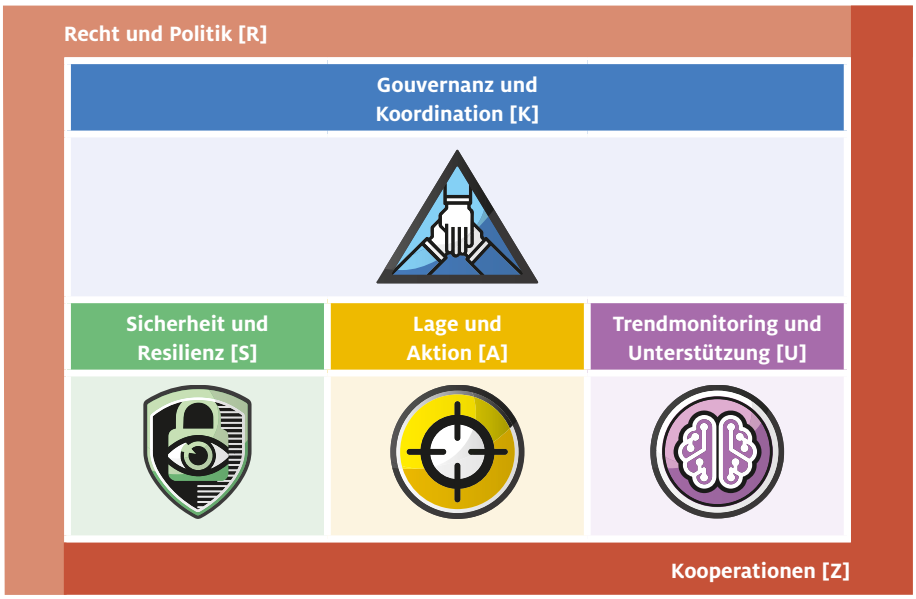


Abbildung 6: Cyberdefence-Dispositiv VBS (Strategie Cyber VBS, 2021)

2

Umfeld und Entwicklungstendenzen

Parallel zur Digitalisierung und zunehmenden Vernetzung der Gesellschaft haben sich die Wirkungsräume Cyber und Elektromagnetik als zusätzliche Dimensionen zur Machtausübung im zivilen und militärischen Bereich etabliert.

Die meisten Streitkräfte haben die neuen militärischen Opportunitäten und Herausforderungen in diesen Gebieten erkannt und systematisch personelle, materielle und immaterielle Fähigkeiten aufgebaut.

2 Umfeld und Entwicklungstendenzen

Im Zuge der Digitalisierung und zunehmenden technischen Vernetzung der Gesellschaft haben sich die Wirkungsräume Cyber und Elektromagnetik als zusätzliche Dimensionen zur Machtausübung im zivilen und militärischen Bereich etabliert. Die meisten Streitkräfte haben die neuen militärischen Opportunitäten und Herausforderungen auf diesen Gebieten erkannt und systematisch personelle, materielle und immaterielle Fähigkeiten aufgebaut. Auch der Sicherheitspolitische Bericht 2021 betont, dass der Einsatz von Cyber- und Informationsmitteln für machtpolitische Zwecke bereits heute Standard sei und in den kommenden Jahren durch eine steigende Zahl staatlicher wie nichtstaatlicher Akteure zunehmen dürfte. Cyber- und Informationsmittel könnten zur Zermürbung als Vorbereitung eines Angriffs dienen und schliesslich in bewaffnete Konflikte herkömmlicher Art münden.[11] Die Doktrin der verschiedenen Länder zeigt, dass die Realisierung eines solchen Ansatzes eine neue ganzheitliche Sichtweise erfordert.

Streitkräfte müssen die notwendigen CER-Fähigkeiten aufbauen, erhalten und bedrohungsgerecht weiterentwickeln. Dies ist bereits heute eine Herausforderung, weil sich der CER stetig wandelt. Werden beispielsweise Angriffswerkzeuge wie etwa eine Schadsoftware von der Gegenseite entdeckt, verlieren sie ihre Wirkung, weil Sicherheitslücken in Zielsystemen ausgebessert werden. Angriffswerkzeuge können ihre Wirkung auch durch die reguläre Systempflege (z. B. Updates, Patching) verlieren.

Eine weitere Herausforderung ist es, zu erkennen, wie sich die Technologie weiterentwickelt. Diese Entwicklung muss in das militärische Umfeld integriert werden, damit sich neue Fähigkeiten aufbauen lassen.

Ausserdem benötigen immer stärker vernetzte IKT-Systeme alle fünf bis sechs Jahre eine umfassende Erneuerung, weil sich Anforderungen stetig verändern und die Nutzungsdauer von Hard- und Software immer kürzer wird. Zeitgemässe Systeme müssen überdies den jeweiligen aktuellen Sicherheitsanforderungen genügen und damit selbst ausreichend vor Cyberangriffen geschützt sein. Um Erneuerungszyklen möglichst kurz zu halten, bedarf es agiler und flexibler Beschaffungs-, Integrations- und Betriebsprozesse.

All dies stellt Streitkräfte vor grosse Herausforderungen, die zu neuen Ansätzen zwingen und einen Kulturwandel herbeiführen: Über Jahrzehnte lag der Fokus auf klassischen militärischen Einsätzen mit schweren Mitteln (z. B. Panzer), deren Nutzungsdauer sich in der Regel über mehrere Dutzend Jahre erstreckte. Heute müssen Informatiksysteme in weit engeren Abständen erneuert werden. Damit stehen die hochdynamischen Anforderungen in den neuen Wirkungsräumen in Kontrast zu den eher langfristig orientierten Vorbereitungen von herkömmlichen militärischen Einsätzen.

11 Die Sicherheitspolitik der Schweiz – Bericht des Bundesrates vom 24.11.2021, Seite 6.

2.1 Internationales Umfeld [12]

2.1.1 Neue Wirkungsräume als Mittel der Machtpolitik

Die neuen Wirkungsräume werden mehr und mehr dazu genutzt, um machtpolitische Interessen unterhalb der militärischen Konfliktschwelle zu verfolgen und durchzusetzen – etwa im Fall von politischen und wirtschaftlichen Spannungen sowie regionalen oder strategischen Rivalitäten. Insbesondere werden im Cyber- und elektromagnetischen Raum Nachrichten beschafft (z. B. Spionagetätigkeiten) sowie Beeinflussungs- und Informationsoperationen durchgeführt. Diese Aktionen sind in der Regel weder Einzelaktionen noch handeln die Akteure isoliert. Im Gegensatz zu cyberkriminellen Operationen streben Spionage- und Beeinflussungsoperationen in den meisten Fällen das Erlangen einer vorteilhaften Machtposition an.

Staatliche Cyberfähigkeiten werden international laufend ausgebaut. Dazu kommt eine steigende Zahl nichtstaatlicher, mehr oder weniger professionell agierender Akteure sowie automatisierte Verfahren, die stetig zu schnelleren und effektiveren Cybermitteln weiterentwickelt werden. Staatliche wie auch nichtstaatliche Akteure betreiben systematisch Wirtschafts- und Industriespionage und führen Aktionen zur Beeinflussung politischer Prozesse durch, um im wachsenden Wettbewerb der Weltwirtschaft bestehen zu können. In diesen Wirkungsräumen existieren auf internationaler Ebene erst wenige Abkommen zur rechtlichen Regelung und Sanktionierung. Dies erlaubt es, Aktionen zu verschleiern und Sanktionen zu umgehen.

Staatlich gesteuerte Spionagetätigkeit und politische Einflussnahme gibt es in verschiedenen Ländern. Sie reichen bis zur Unterdrückung der eigenen Bevölkerung, der politischen Opposition und von Minderheitsgruppierungen mit Cybermitteln, vor allem im Informationsraum. Beispiele sind die Zensur von Social-Media-Kanälen, die Sperrung des Internetzugangs, Propaganda und andere psychologische Operationen. Eine Studie zum Thema «Global Disinformation Order» der Universität Oxford (GB) stellt u.a. fest, dass im Jahr 2019 siebzig Staaten organisierte Social-Media-Kampagnen durchgeführt haben.[13]

12 In den folgenden Abschnitten wird die internationale Einbettung des Cyberthemas in Sicherheits-, Wirtschafts- und Machtpolitik sowie in militärischen Konflikten behandelt. In der Sicherheitspolitik liegt das Hauptaugenmerk auf Westeuropa und der Schweiz. Die nachfolgenden Ausführungen stützen sich vorwiegend auf:
Baezner Marie, Cordey Sean (2019): Nationale Cybersicherheitsstrategien im Vergleich – Herausforderung für die Schweiz, März 2019, Center for Security Studies (CSS), ETH Zürich. Zitiert als Baezner, Cordey (2019).
Dewar Robert S.: Trend Analysis: Contextualising Cyber Operations, May 2018, Center for Security Studies (CSS), ETH Zürich. Zitiert als Dewar (2018).
Der Abschnitt Westeuropäische Cyberstreitkräfte stützt sich im Wesentlichen auf Sean Cordey, Robert S. Dewar, ed. (2019): National Cybersecurity and Cyberdefense Policy Snapshots: Update Collection 2, Center for Security Studies (CSS), ETH Zürich. Folgende Länder wurden näher beleuchtet und, wenn möglich, ein Zusammenhang mit der Schweiz hergestellt: Finnland, Frankreich, Deutschland (ebenfalls bei Baezner, Cordey 2019) und Grossbritannien.

13 University of Oxford: The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation (2019); S. 2ff. Zitiert als "University of Oxford: The Global Disinformation Order (2019)".

Tendenz: Es ist davon auszugehen, dass

- Aktionen im CER bei allen Formen zwischenstaatlicher Spannung als Mittel der ersten Wahl eingesetzt werden – von politischen und wirtschaftlichen Rivalitäten bis hin zu militärischen Konflikten;
- Fähigkeiten im CER zukünftig von einer steigenden Zahl von Staaten in unterschiedlich ausgeprägter und ausgebauter Form genutzt werden, um eigene Interessen zu untermauern, zu verteidigen und durchzusetzen;
- auch kleinere Staaten mit einem geringeren machtpolitischen Potenzial über sehr anspruchsvolle Cyber-Überwachungsmittel verfügen, deren Technologie von Partnern zur Verfügung gestellt werden (in der Regel im Rahmen der Stärkung diplomatischer Beziehungen) und diese Mittel zunutze machen werden.

2.1.2 Neue Wirkungsräume in Konflikten[14]

Staaten und Armeen haben in Konflikten schon immer die neusten und effektivsten Mittel eingesetzt, um taktische und strategische Vorteile gegenüber ihren Gegnern zu erlangen. Der systematische und gezielte Einsatz von Aktionen im Cyber- und elektromagnetischen Raum kommt deshalb nicht überraschend. Sie werden heute als gebräuchliches Kampfmittel in Konflikten angewendet und gehören zu modernen militärischen Konfliktbildern. Solche Aktionen können einen physischen Angriff vorbereiten. Sie werden aber auch als alleiniges Mittel genutzt, um Infrastrukturen und Systeme zu stören, zu zerstören oder zu destabilisieren. Zur Vorbereitung und Unterstützung militärischer Aktionen finden Aktivitäten im Cyber- und elektromagnetischen Raum oft bereits Wochen oder Monate vor den eigentlichen Operationen in den herkömmlichen physischen Wirkungsräumen statt. Dazu gehören etwa die Störung und Unterbrechung von militärischen und zivilen Kommunikations-, Versorgungs- und Steuerungssystemen oder die Durchführung von Desinformations-, Propaganda- und Beeinflussungskampagnen.[15]

Dass einem militärischen Konflikt oft eine länger andauernde machtpolitische Auseinandersetzung vorausgeht, zeigt beispielsweise der Konflikt zwischen Russland und der Ukraine ab 2014. Aktionen im Cyber- und elektromagnetischen Raum spielten auch hier vor und während des Konflikts eine wichtige Rolle. Beide Seiten machten intensiv Gebrauch von Desinformation und Propaganda, Störung der zivilen Telekommunikation, Unterbrechung der Energieversorgung und Attacken mit Malware. Solche Vorgehensweisen gehören in heutigen Konflikten zum Standardprozedere. Künftig dürften Aktionen im Cyberraum, im elektromagnetischen Raum und im Informationsraum mit stets neuen, noch wirkungsvolleren Technologien und Instrumenten geführt werden, denen sich ein entsprechendes Verteidigungsdispositiv mit einer ebenso rasch voranschreitenden Entwicklung von Gegenmassnahmen wird entgegenstellen müssen.

Cybermächte, d. h. Staaten, die über hochentwickelte militärische Cyberfähigkeiten verfügen, werden weiterhin tonangebend sein. Denn sie besitzen auch die finanziellen und personellen Möglichkeiten, um hochkomplexe Cyberwaffen zu konzipieren und einzusetzen.

---

14 Unter Konflikten werden offene, internationale oder innerstaatliche Auseinandersetzungen mit militärischer Komponente verstanden.

15 Bsp. Computerwurm Stuxnet (2010 entdeckt) und dessen Folgeentwicklungen. Seither sind keine vergleichbaren Einsätze von hochentwickelten Cyberwaffen mehr öffentlich bekannt geworden. Wahrscheinlich ist dies auf ein ungleiches Kosten-Nutzen-Verhältnis zurückzuführen. Der Einsatz derartiger Waffen zahlt sich nur gegen entsprechend hochwertige Ziele aus und erfordert einen enormen Aufwand an Technologie, Personal und Entwicklungszeiten. In der Regel werden für Angriffe häufig Cybertools bevorzugt, die günstig im Preis, einfach zu handhaben und effektiv in der gewünschten Wirkung sind.

Ein weiterer wichtiger Faktor in den Auseinandersetzungen im Cyber- und elektromagnetischen Raum sind nichtstaatliche Akteure. In fast allen internationalen Konflikten der vergangenen Jahre haben Gruppierungen, die den Konfliktparteien nahestehen, mit Cyberangriffen von sich reden gemacht. Derartige Gruppierungen handeln teilweise in staatlichem Auftrag, aus eigener Motivation oder beides. Es ist davon auszugehen, dass konfliktführende Staaten auch in Zukunft nichtstaatliche Gruppen engagieren werden, weil diese über hochentwickelte Fähigkeiten verfügen und ad hoc gezielt für entsprechende Aktionen eingesetzt werden können. Die Gruppierungen führen Cyberaktionen oft inoffiziell, jedoch gut organisiert, höchst professionell und meist mit relativ einfachen, aber wirkungsvollen Cybertools aus. Für die dahinterstehenden Staaten hat dies den Vorteil, dass sie als Auftraggeber kaum mit den Akteuren in Verbindung gebracht werden können. Sie tragen aber auch das Risiko der fehlenden Kontrolle über die Führung und die möglichen Konsequenzen derartiger Aktionen, sobald sich eine Gruppierung in einem zwischenstaatlichen Konflikt auf eigene Faust beteiligt.

Die Schwierigkeit, Aktionen zurückzuverfolgen und ihren Auftraggebern zuzuweisen, sorgt dafür, dass kaum mit Vergeltung zu rechnen ist. Dies wiederum senkt die Hemmschwelle zur Durchführung solcher Aktionen. Die Entwicklung hin zu vermehrter Einmischung nichtstaatlicher Akteuren und besonders auch von Einzelakteuren könnte gemäss neueren Studien zu einem Schlüsselaspekt in zukünftigen innerstaatlichen Konflikten werden[16].

Die klassischen Grundsätze der Abschreckung sind in einem solch diffusen Umfeld nicht unmittelbar anwendbar. Nebst dem Problem, dass ein Angriff oft keinem Aggressor zugeschrieben werden kann (Attribution), sind die Proportionalität und die Kontrollierbarkeit digitaler Gegenreaktionen nicht gegeben.

Tendenz: Es ist davon auszugehen, dass
- Staaten, nichtstaatliche Akteure und Einzelpersonen bei einem Konflikt vermehrt anonym und zeitlich weit im Voraus breit angelegte Aktionen im CER durchführen, um den Verlauf des eigentlichen, nachfolgenden Konfliktes zu beeinflussen;
- die klassischen Grundsätze der Abschreckung im CER kaum mehr Geltung haben.

2.1.3 Cybersicherheitsstrategien[17]

Die meisten westlichen Staaten haben in den vergangenen 10 bis 15 Jahren ein ausgeprägtes Bewusstsein für Cybersicherheit entwickelt. Die weltweite digitale Transformation mit den einhergehenden Chancen und Risiken hat diese Bewusstseinsbildung befördert. Das Resultat sind zahlreiche nationale Strategien zur Cybersicherheit und darauf basierende Konzepte zur militärischen und polizeilichen Cyberabwehr.

Allen betrachteten Strategien ist ein ganzheitlicher Ansatz gemeinsam, der verschiedene, national-sozioökonomische Anliegen miteinschliesst. Sie sind jeweils in einer umfassenden nationalen Sicherheitsstrategie eingebettet und grundsätzlich auf defensive Cyberfähigkeiten ausgerichtet. Zudem steht die politisch-strategische Führung im Bereich Cybersicherheit in allen Strategien in unmittelbarer Nähe zur obersten Regierungsebene[18]. In allen untersuchten Strategien werden die militärische und zivile Cy-

16 Dewar (2018), S. 9.
17 Baezner Marie, Cordey Sean (2019): Nationale Cybersicherheitsstrategien im Vergleich – Herausforderung für die Schweiz, März 2019, Center for Security Studies (CSS), ETH Zürich. Zitiert als Baezner, Cordey (2019).
18 Zur Organisation in den einzelnen Ländern siehe Baezner, Cordey (2019), S. 10.

berabwehr getrennt geführt. Sie messen der internationalen Kooperation und der Zusammenarbeit mit dem privaten Sektor einen hohen Stellenwert bei und setzen auf eine umfassende Sensibilisierung, Information und Bildung.

In allen Strategien ist die Frage zentral, wie nationale Cybersicherheit vertikal (durch eine effiziente Steuerung nationaler Ressourcen) und horizontal (durch die Koordination verschiedener Stellen) gewährleistet werden soll. Auf nationaler Ebene braucht es die richtige Mischung aus Zentralisierung und dezentraler Nutzung von Kompetenzen. Auf internationaler Ebene muss definiert werden, wie die zwischenstaatliche Zusammenarbeit gestaltet werden soll. Hinzu kommen weitere Themenfelder, denen sich die Staaten annehmen müssen. Dazu gehören solide und belastbare Strukturen für das Krisenmanagement, eine wirksame Krisenkommunikation, die Entwicklung einer guten Reaktionsfähigkeit auf gravierende Vorfälle, ein geeignetes Lagebild und eine präzise Bedrohungsanalyse. Ferner stellt sich die Frage, wie zukünftige Bildungsangebote ausgestaltet werden, um dem Mangel an Spezialistinnen und Spezialisten im Cyberbereich zu begegnen. Für die Zusammenarbeit mit der Privatwirtschaft ist ein Rahmen gefragt, der Innovationen zulässt und die nationale Sicherheit fördert. Ein nicht zu unterschätzendes Thema ist die Harmonisierung der Gesetzgebung – auch im Hinblick auf interdisziplinäre und internationale Zusammenarbeit. Schliesslich braucht es in Zukunft wirksame Strategien zur Bekämpfung von Cyberkriminalität.

Die markantesten Abweichungen innerhalb der in diesem Kapitel betrachteten Beispiele gehen vorwiegend aus dem jeweiligen historischen Bezugsrahmen, der Kultur sowie der Organisation und der Struktur der einzelnen politischen Systeme hervor. Weitere Unterscheidungsmerkmale ergeben sich aus der politischen Positionierung, dem Selbstverständnis und den Interessenbereichen der einzelnen Staaten innerhalb der globalen Staatengemeinschaft.[19]

Tendenz:
- Allen untersuchten Cybersicherheitsstrategien ist gemeinsam, dass die nationale Führung der Cybersicherheit unter ziviler Leitung erfolgt – heute und auch in Zukunft.
- Die Nutzung des eigenen nationalen Potenzials einzelner Staaten wird in Zukunft an Bedeutung gewinnen.

2.1.4 Cyber-Streitkräfte der Grossmächte USA, Russland und China[20]

Die Grossmächte USA, Russland und China verfügen seit etwa zwei Jahrzehnten über wirksame Cyberfähigkeiten und -mittel für defensive und offensive Cyberaktionen. Die jeweiligen Cybersicherheitsstrukturen sind abhängig von der geschichtlichen Entwicklung, den politischen Systemen, dem jeweiligen Selbstverständnis sowie den Absichten und Interessen, welche diese Staaten im globalen Kontext verfolgen.

Es kann davon ausgegangen werden, dass die Cyber-Streitkräfte aller drei Staaten mit personellen und finanziellen Mitteln gut alimentiert sind. China dürfte sogar über mehrere zehntausend Personen verfügen, die ausschliesslich für die militärische Cyber Defence und Offence arbeiten. Alle drei Staaten verfügen über eigene, offizielle Einheiten

19 Siehe dazu Baezner, Cordey (2019), S. 7.
20 Militärstrategische Angaben: Powerpoint-Dokumentationen «Cyber-Fähigkeiten» FUB / ZEO / CYD (30.08.2018). Der elektromagnetische Raum wird hier mangels aussagekräftiger, öffentlich zugänglicher Quellen nicht behandelt.

für militärische Cyberoperationen. Sie haben ausserdem die Fähigkeiten und Mittel, hochanspruchsvolle Cyberwaffen herzustellen und einzusetzen.[21]

Mit hoher Wahrscheinlichkeit unterhalten die drei Grossmächte mehr oder weniger offizielle Verbindungen zu diversen nichtstaatlichen Gruppierungen, die Aktionen und Angriffe in ihrem Sinne führen. Insbesondere für Russland und China sind mehrere solche Gruppen von «Patriotic Hackers» und «Hacktivisten» bekannt, die fest oder temporär mit staatlichen Aufträgen betraut sind.

Die Verbindung bzw. die Kontrolle solcher Gruppierungen erlaubt es sogar, nichtstaatliche Cyberkräfte für staatliche Überwachung, Spionage oder gar Sabotage einzusetzen. Es handelt sich vor allem um Unternehmen, die Hardware, digitale Dienstleistungen[22] und Monitoring-Technologien produzieren.

Die hier behandelten Grossmächte machen zusätzlich systematisch Gebrauch von Informationsoperationen, um ihre Interessen durchzusetzen[23].

Tendenz:
- Es ist davon auszugehen, dass Grossmächte ihre Potenziale im Cyber-, elektromagnetischen und Informationsraum weiter ausbauen und systematisch nutzen werden.

2.1.5 Westeuropäische Cyber-Streitkräfte und Cyberverteidigungsstrategien

Die in diesem Kapitel betrachteten westeuropäischen Staaten[24] verfügen alle über moderne Cyber-Streitkräfte, deren jeweilige Zuständigkeiten und Aufgaben in Cyberverteidigungsstrategien definiert sind. Diese wiederum sind in übergeordnete Cybersicherheitsstrategien integriert oder werden als eigenständiges Rahmenwerk parallel dazu geführt.

Hervorzuheben ist, dass alle Cybersicherheitsstrategien die militärische Cyberabwehr von den zivilen Aufgaben wie zum Beispiel der Abwehr von Cyberkriminalität klar abgrenzen. In den Cybersicherheits- und -verteidigungsstrategien lässt sich durchwegs erkennen, dass es sowohl auf politischer als auch auf militärstrategischer Ebene eine zentrale Führung braucht, um die offensichtlich komplexen Strukturen zu koordinieren. Diese Führungsstelle ist jeweils in der Nähe der obersten Führungsstufe (Verteidigungschef, Oberkommando) angesiedelt. Die untersuchten Länder haben auch erkannt, dass die militärische Cyberverteidigung am besten als zentrale (Kommando-) Stelle etabliert werden sollte.[25] Diese Position auf der höchsten Kompetenzebene erlaubt es der Cyber-Streitkräfteführung, unmittelbar, auf dem kürzesten Dienstweg und auf Augenhöhe mit gleichwertigen Partnern innerhalb und ausserhalb der Armee zu agieren und das Tempo ihrer Aktionen bei Bedarf zu erhöhen. Weil es so viele verschiedene Beteiligte auf diversen Ebenen gibt, erfolgt die Ausführung jedoch idealerweise dezentral – wo nötig mit eigenen Kompetenzen und Verantwortungen der ausführenden Stellen.

---

21 Vgl. dazu Baezner Marie, Robin Patrice (2017), Hotspot Analysis: Stuxnet, October 2017, Center for Security Studies (CSS), ETH Zürich.

22 Dienstleistungen wie beispielsweise Suchmaschinen, Office-Produkte, soziale Kommunikations- und Mitteilungsdienste, soziale Netzwerke, Online-Bezahldienste, Videoplattformen, Online-Shopping, Cybersecurity-Firmen.

23 Siehe dazu Cordey Sean (2019), Cyber Influence Operations: An Overview and Comparative Analysis, Cyber Defence Trend Analysis, Center for Security Studies, ETH Zurich; University of Oxford: The Global Disinformation Order (2019).

24 Baezner, Cordey (2019): Im Rahmen der nationalen Cyber-Sicherheitsstrategien wurden auch die Einbettung der Cyberverteidigungs-Strategien beleuchtet, und zwar für die Staaten Finnland, Frankreich, Deutschland, Italien und Niederlande. Im folgenden Abschnitt werden aus den Erkenntnissen von Baezner, Cordey (2019) mögliche Gemeinsamkeiten mit der Schweiz hervorgehoben. Details zu den einzelnen Streitkräften siehe Anhang.

25 Deutschland, Frankreich, Finnland, Niederlande, Grossbritannien (ab 2020 in Umsetzung).

Die Cyberkommandos westeuropäischer Cyber-Streitkräfte orientieren sich oft am Vorbild der NATO-Kommandoorganisation. Auch Staaten wie Finnland, die zwar nicht der NATO angehören, jedoch gewisse Berührungspunkte mit ihr haben, haben die Schaffung von Cyber-Kommandostellen in Betracht gezogen. Die Zentralisierung, Strukturierung, Führung und Überwachung defensiver und offensiver Cyberkräfte unter einem einheitlichen Cyberkommando nach NATO-Vorbild könnte einem Trend entsprechen.[26]

Die Verschärfung der sicherheitspolitischen Lage in den vergangenen Jahren hat dazu geführt, dass Streitkräfte vermehrt offensive Fähigkeiten entwickeln. Verschiedene Staaten haben sich in jüngster Vergangenheit offiziell zu ihren offensiven militärischen Cyberfähigkeiten bekannt.

Alle Streitkräfte verfügen mindestens über IT-Notfallteams, sogenannte Computer Emergency Response Teams (CERT). Offensive Cyberfähigkeiten sind für die Niederlande, Frankreich und Österreich ausgewiesen.

Die Zusammenarbeit der Streitkräfte mit zivilen Behörden, der Industrie und der Privatwirtschaft (kritische Infrastrukturen wie Stromversorgung, Telekommunikation usw.) spielt in praktisch allen Ländern eine entscheidende Rolle – gerade auch im Rahmen subsidiärer Hilfeleistungen an Dritte sowie im Bereich der Bildung und Forschung.

Eine engere Zusammenarbeit zwischen militärischen und zivilen Stellen lässt sich in den untersuchten Ländern anhand mehrerer Beispiele beobachten. Sie kommt beispielsweise bei der Erarbeitung eines gemeinsamen Lagebildes vor, im Informationsaustausch sowie bei der Sensibilisierung und der Führung gemeinsamer Operationen. Um eine enge Zusammenarbeit zu fördern und die Vorteile kurzer Informationswege zu nutzen, sind in manchen Ländern zivile und militärische Cybereinheiten räumlich in denselben Gebäuden untergebracht – beispielsweise in den Niederlanden.[27]

Alle untersuchten Streitkräfte betonen die Wichtigkeit der internationalen Zusammenarbeit.

Wie die Cybersicherheitsstrategien unterscheiden sich auch die untersuchten Cyberverteidigungskonzepte vorwiegend durch ihre jeweiligen politisch-historischen Hintergründe und den geopolitischen Kontext, in dem sie stehen.

Tendenz: Es zeigt sich, dass

- etablierte westeuropäische Cyber-Streitkräfte zentral geführt und dezentral eingesetzt werden;
- aus militärischer Sicht sowohl die Zusammenarbeit mit zivilen Behörden wie auch die internationale Kooperation als wichtig erachtet wird;
- Wirkungen für militärische Zwecke im Cyber-, elektromagnetischen und Informationsraum – gleich wie physische Wirkungen – auf der operativen Stufe geführt werden.

26 Vgl. dazu Cordey Sean, Dewar Robert S. ed. (2019): National Cybersecurity and Cyberdefense Policy Snapshots: Updated Collection 2, 2019, Center for Security Studies (CSS), ETH Zürich. S. 167, Punkt 5; S. 168, Punkt 7.
27 Baezner, Cordey (2019), S. 10.

2.2 Nationales Umfeld

2.2.1 Politik

Wie in vielen anderen Staaten wurden auch in der Schweiz die Chancen und Risiken der Digitalisierung erkannt. Der Bundesrat hat entsprechende Ziele festgelegt.[28]

Unter den zahlreichen parlamentarischen Vorstössen zum Cybersicherheitsthema sind insbesondere zwei Motionen für den weiteren Ausbau der Cyberfähigkeiten der Armee zu erwähnen.[29] Sie verfolgen im Wesentlichen sechs Ziele:

1. Bildung eines Cyber-Kompetenzzentrums Bund und Schaffung eines Cyber-Kommandos Armee zur Bündelung und zum Ausbau der Cyberfähigkeiten;
2. Aufstockung von personellen und finanziellen Ressourcen für Bund und Armee;
3. Selbstschutz der armeeeigenen Systeme und Infrastrukturen und Aufbau autonomer Fähigkeiten für den Verteidigungsfall;
4. subsidiäre Unterstützung;
5. Kooperation zwischen Bildung, Forschung, Wissenschaft, Industrie und Wirtschaft sowie Betreibern kritischer Infrastrukturen;
6. Austausch, Kommunikation und Information auf nationaler und internationaler Ebene.

Die zweite «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (2018–2022)» erfasste die Situation ganzheitlich, im Gegensatz zu ihrer Vorgängerin (2012–2017). Sie berücksichtigte zahlreiche Schnittstellen und bindet die Armee entsprechend ihrem Auftrag besser ein. Zudem hat sie neue Massnahmen definiert, um der Bedrohungslage besser zu entsprechen.

Tendenz: Es zeigt sich, dass

- die Bedeutung des Cyberthemas in der schweizerischen sicherheitspolitischen Diskussion erkannt und etabliert ist;
- eine politische Erwartungshaltung besteht, wonach die Schweiz diesbezüglich ihre eigenen Fähigkeiten verstärkt, um der internationalen Entwicklung Rechnung zu tragen.

2.2.2 Wirtschaft, Bildung und Forschung

International lassen sich verschiedene Wege beobachten, wie Wirtschaft, Bildung und Forschung zusammenarbeiten. Ziel ist es, die Vorteile aus dem Cyberraum, dem elektromagnetischen Raum und dem Informationsraum systematisch zu nutzen und gleichzeitig die Sicherheit der eigenen Infrastrukturen zu verbessern. Je nach Land spielen dabei Institutionen des zivilen und militärischen Sicherheitsapparats eine unterschiedliche Rolle. Unabhängig von der gewählten Lösung verfolgen diese Staaten das Ziel, nationale Potenziale zu bündeln, um die jeweiligen Wirtschafts- und Sicherheitsinteressen möglichst wirksam und eigenständig zu wahren.

Im Hinblick auf die Entwicklung und Nutzung von Schlüsseltechnologien (siehe Kapitel 2.3) im Cyber- und elektromagnetischen Raum spielen die Schweizer Wirtschaft und die Bildungslandschaft für die Armee eine grosse Rolle. Sie sind wichtige Treiber und Lieferanten zugleich. Will die Armee mit der technologischen Entwicklung Schritt hal-

28 Ziele des Bundesrates 2020.
29 Motion Eder Joachim 1735.08, Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund (abgeschrieben). Motion Dittli Josef, 1735.07, Ein Cyberdefence-Kommando mit Cybertruppen für die Schweizer Armee (abgeschrieben).

ten und Synergien nutzen, so ist es unumgänglich, Partnerschaften und gemeinsame Entwicklungsprogramme aufzubauen und zu fördern.

Im Bereich Bildung und Forschung werden in der Schweiz Fachkräfte für Berufe in Zusammenhang mit dem CER auf hohem Niveau ausgebildet. Dieses Fachpersonal ist für die Personalalimentierung der Armee eine entscheidende Ressource. Die Armee unterstützt den Bildungssektor mit eigenen Ausbildungsprogrammen, beispielsweise mit dem Cyberlehrgang oder der beruflichen Grund- und Weiterausbildung.

Tendenz: Es ist davon auszugehen, dass
- nationale Kooperationen in Bildung, Forschung und Wirtschaft künftig ein wesentliches Element bilden, um angemessene staatliche Fähigkeiten und die Eigenständigkeit im Cyber-, elektromagnetischen und Informationsraum zu stärken und zu erhalten;
- Streitkräfte diese Zusammenarbeit verstärkt nutzen werden;
- die Armee verstärkt eine nationale (partnerschaftliche) Zusammenarbeit mit Wirtschaft, Bildung und Forschung anstreben wird. Nur so wird sie die technologischen Entwicklungen antizipieren sowie ihre Personalgewinnung auf aktuelle und zukünftige Herausforderungen ausrichten können.

2.3 Technologieentwicklung als Herausforderung

Die Entwicklung von Informations- und Kommunikationstechnologien beeinflusst massgeblich die Möglichkeiten im Cyberraum. Relevante Entwicklungen finden gegenwärtig in folgenden Bereichen statt:

— Verdichtung der Rechenleistung;
— künstliche Intelligenz;
— Big Data;
— umfassende Vernetzung;
— autonome Plattformen;
— zunehmende Dominanz grosser Technologiefirmen.

Technologie befindet sich ständig im Fluss. Was vor zehn Jahren «Hightech» war, ist heute eine Selbstverständlichkeit. Geräte, die auf einer veralteten Technologie basieren, sind in den IKT-Systemen der Armee noch weitgehend vorhanden. Dies stellt bezüglich Betriebsaufwand und Sicherheit eine besondere, kaum vermeidbare Herausforderung dar. Um bestehende Fähigkeiten zu erhalten, aufzubauen oder Lücken zu schliessen, muss sich eine Armee technisch stetig weiterentwickeln. Sie muss sich zwingend mit künftigen Technologien, technischen Anwendungen und Systemen auseinandersetzen.

Bei Beschaffungen muss die Schweizer Armee eine Abwägung zwischen dem Potenzial einer angebotenen technologischen Lösung und den daraus resultierenden Risiken vornehmen. Eine allfällige Abhängigkeit von Lieferanten und deren Herkunft muss ebenfalls beurteilt werden. Neue Technologien, technische Anwendungen und Systeme sollen den geforderten zukünftigen Fähigkeiten entsprechen. Sie müssen in ihren Gesamtzusammenhang gestellt und im Rahmen eines umfassenden Lifecycle Managements bewirtschaftet werden. Dazu gehören auch Prozesse im Bereich Supply Chain Risk Management, mit denen über die gesamte Nutzungsdauer eines Systems dessen Sicherheit beurteilt sowie Risiken bewertet und antizipiert werden.

Technologieveränderungen führen entweder zu schrittweisen Verbesserungen oder zu grossen Entwicklungssprüngen, die bisherige Systeme vollständig ablösen. Ihre Integration erfordert ein flexibles und vernetztes Vorgehen und intensive Partnerschaften mit Wirtschaft und Wissenschaft. Zusätzlich braucht es rasche und einsatznahe Beschaffungsverfahren sowie flexible Projektorganisationen.

Tendenz: Es ist davon auszugehen, dass

- der Zwang zur Systemerneuerung wegen der beschleunigten Technologieentwicklung weiter zunimmt und die Nutzungsdauer von Systemen mit hohem Technologiegrad kürzer werden wird;
- die Integration moderner technischer Anwendungen und Systeme ein flexibles und vernetztes Vorgehen verlangt, was einen zeitnahen Beschaffungsprozess und gezielte Technologie-Partnerschaften voraussetzt;
- zukünftige Systeme noch eingehender auf Potenzial und Risiken überprüft werden müssen, damit die eigenen Ressourcen im Rahmen des System-Portfolios optimal eingesetzt werden können.

Cyberraum

IKT-Komponenten wie Smartphones und Rechenzentren sind bereits heute oft an Clouds angeschlossen. Diese speichern und verarbeiten Daten, sind über die ganze Welt verteilt und global vernetzt.

Neuartige Satellitennetzwerke (z. B. OneWeb, Starlink) und neue satellitengestützte Kommunikationsverfahren werden Internetzugänge künftig auch in entlegenen Regionen und Orten bereitstellen, wo es keinen terrestrischen Breitbandzugang gibt. Die drahtgebundene Kommunikation, z. B. mittels Glasfaserkabel, wird zudem Gebäude mit sehr hohen Datenraten erschliessen. Interkontinentale Verbindungen werden noch redundanter und mit beinahe unbeschränkter Leistung gewährleistet[30].

In den letzten Jahren haben verschiedene Entwicklungen zu einem neuen Innovationsschub im Cyberraum geführt. Dazu gehören die Automatisierung von Wirtschaftsprozessen, die zunehmende Vernetzung und Verfügbarkeit neuartiger Methoden der künstlichen Intelligenz und die Verarbeitung riesiger Datenmengen (Big Data). Unter dem Stichwort «Digitalisierung» oder «Industrie 4.0» wird die Interaktion zwischen Mensch und Maschine neu gestaltet: Die Tätigkeitsbereiche der Menschen verschieben sich zunehmend von repetitiven Aufgaben hin zu Aufgaben der Programmierung und Steuerung von automatisierten Prozessen.

Der militärische Cyberraum hinkt in weiten Teilen den zivilen Entwicklungen hinterher. Er setzt deshalb oft kommerziell verfügbare Technologien ein und ergänzt diese mit spezifischen Entwicklungen. Im Bereich der Telekommunikation hingegen ist die Armee aufgrund der notwendigen Verfügbarkeit, Robustheit und Sicherheit auf eigene Verfahren angewiesen, die jedoch deutlich kleinere Datenmengen transportieren als zivile.

Die Entwicklung im Cyberraum ist rasant. Der gesamte Bereich wächst kontinuierlich und wird immer komplexer und unübersichtlicher. Der technologische Aufbau ruht allerdings auf einem Fundament, das konzeptionell bereits veraltet ist. Die grundlegen-

30 Eine einzelne Glasfaser in einem Glasfaserkabel kann Datenraten von Dutzenden Tbit/s transportieren. Gebäude in Ballungszentren können mit bis zu 10 Gbit/s versorgt werden.

den Technologien wurden nicht für so grosse Nutzungsdimensionen konzipiert wie z. B. die weltweite Vernetzung, die Datenverarbeitung in Smartphones, Notebooks oder Datenzentren. Deshalb ist der Cyberraum hinsichtlich Sicherheit fragil – vollständige Sicherheit ist unerreichbar und wird es nie geben.[31]

Da der Cyberraum ein von Menschen erschaffener Raum ist, besteht ein grosser Teil der Risiken und Bedrohungen in menschlichen Aktivitäten. Cyberangriffe nutzen häufig auch die Schwächen des Menschen, der hinter der Maschine sitzt. Der Cyberraum wird von einer breiten Gemeinschaft auch kommerziell genutzt. Daraus entstehen stets neue Felder, in denen neuartige Verfahren und Werkzeuge zur Durchführung von offensiven Cyberaktionen entwickelt werden. Die besten Angriffswerkzeuge und -verfahren unterliegen allerdings einer strengen Geheimhaltung. Sie sind auf konventionellen Märkten nicht erhältlich.

Die Anfälligkeit der digitalisierten Systeme in Zusammenhang mit einer sich stetig weiterentwickelnden Bedrohung setzt Sicherheitstechnologien und eine entsprechende Sicherheitsorganisation voraus. Streitkräfte wappnen sich mit immer leistungsfähigeren Schutz- und Erkennungstechnologien. Sie bilden Teams, die für den Eigenschutz gegen Angreifer sorgen. Sowohl Angreifer als auch Verteidiger wenden Methoden zur Tarnung und Täuschung an. Eine wichtige Rolle bei Schutz- und Erkennungstechnologien spielt zunehmend auch die künstliche Intelligenz. Das Tempo von Aktionen im Cyberraum wird dadurch massiv erhöht.

Um ihre Handlungsfreiheit zu erhalten, muss die Schweizer Armee im Cyberraum auch in Krisenzeiten oder während eines bewaffneten Konflikts bestehen können. Dies soll mit einer robusteren IKT und mit einer geschickten Trennung der eigenen von öffentlichen Netzen erreicht werden. Gegnerische Aktivitäten im Cyberraum abzuwehren, ist somit eine vollwertige militärische Tätigkeit geworden – vergleichbar etwa mit dem Objektschutz oder der Luftverteidigung. Sind offensive Cyberfähigkeiten verfügbar, kann dies den Erfolg einer militärischen Aktion erheblich begünstigen. Um zukünftige, heute noch nicht vorhersehbare Bedrohungen zu erkennen und wirksame Gegenmassnahmen einzuleiten, muss die Armee bereits heute eigene technologische Entwicklungsfähigkeiten aufbauen.

Im militärischen Bereich sind zusätzlich folgende Aspekte zu berücksichtigen:

— Die Digitalisierung im militärischen Umfeld ist ein unumkehrbarer Trend. So werden beispielsweise mehr und mehr autonome Systeme zur Anwendung gelangen. Diese Entwicklung eröffnet sowohl Chancen als auch Risiken, da sich auch neue Möglichkeiten eröffnen, in gegnerische IKT-Systeme einzudringen und damit Entscheidungsprozesse zu beeinträchtigten.
— Cyberangriffe können auch dazu genutzt werden, falsche Informationen zu transportieren, um Bevölkerung und Truppe zu verunsichern. Die dafür verwendeten Infrastrukturen befinden sich meistens nicht in der Verantwortung der Armee. Es ist deshalb wichtig, dass die Armee mit den relevanten Organisationen zusammenarbeitet. Nur so kann sie derartige Angriffe frühzeitig erkennen und die Zuverlässigkeit der eigenen Daten aufrechterhalten.
— Militärische Systeme sind nicht zwangsläufig an das Gesamtnetzwerk angebunden, sondern bilden manchmal autonome «Stand-alone-Netze» (lokal begrenzt einzelne, nicht vernetzte Informatiksysteme). In diesem Fall kann ein Akteur versuchen, bereits weit im Voraus der eigentlichen Aktion in lokale IKT-Systeme einzudringen oder an sicherheitsrelevante Komponenten wie Telekommunikations- oder Verschlüsselungsgeräte zu gelangen. Er kann dies z. B. bei der Wartung eines Systems tun. Spezialkräfte, Mini-Drohnen, Flugzeuge oder Satelliten können ebenfalls zu diesem Zweck genutzt werden.

31 Beispiele wie die grundlegenden Schwächen in Routing-Protokollen des Internets und in der Architektur moderner Prozessoren (Spectre, Meltdown) verdeutlichen diese Aussage.

Tendenz: Es ist davon auszugehen, dass

- die zivilen technischen Entwicklungen die treibenden Kräfte der Vernetzung, Datenübertragung und Verarbeitung sind;
- die technischen Entwicklungen zu einem noch umfassenderen, aber weiterhin fragilen Cyberraum führen werden;
- die nicht vorhersehbaren Bedrohungen die eigenen, teilweise selbst entwickelten Sicherheitstechnologien und die eigene Sicherheitsorganisation permanent herausfordern und unter Zugzwang setzen werden;
- der militärische Cyberraum als Teilmenge des gesamten Cyberraums auch in Zukunft als nicht absolut sicher gelten und ständigen Angriffsversuchen ausgesetzt sein wird;
- der Erfolg militärischer Aktionen mit eigenen, offensiven Cyberfähigkeiten gesteigert werden kann;
- die Notwendigkeit grösser wird, autonome Waffenplattformen und «Stand-alone-Netze», z. B. autonome Waffensysteme, mit geeigneten Mitteln zu schützen.

Daten und Informationen

Der Erfolg einer militärischen Aktion wird durch den Einsatz geeigneter Kräfte (z. B. ein militärischer Verband oder ein Kampfflugzeug) am richtigen Ort zur richtigen Zeit bestimmt. Um dies planen und führen zu können, muss der verantwortliche Kommandant zeitgerecht über die dafür notwendigen Informationen (Lagebild) verfügen. Die Bedeutung von Informationen war und ist gerade auch im militärischen Kontext ausgesprochen hoch.[32] Durch die Technologieentwicklung hat die Informationsmenge deutlich zugenommen. Es sind immer mehr Informationen über einen Sachverhalt verfügbar und Veränderungen zeigen sich darin rasch. War es früher die Schwierigkeit, überhaupt an die benötigten Informationen zu gelangen, besteht heute die Herausforderung darin, in der grossen Menge an Informationen die wichtigen zu erkennen.

Um wichtige Erkenntnisse in einem Lagebild aufzeigen zu können, braucht es eine möglichst kontinuierliche Datenanalyse. Die Resultate fliessen direkt in die Aktionsplanung ein. Die so gesammelten Daten und Informationen bilden den Kern der Digitalisierung des Aktionsführungsprozesses.

Die Trends in diesem Bereich umfassen:

— Die Qualitätsverbesserung und Temposteigerung in der Aktionsführung durch qualitativ gute, relevante und für alle Beteiligten gleichzeitig verfügbare Daten zur Unterstützung des präzisen Einsatzes der knappen Mittel;
— das Ermöglichen der Zusammenarbeit durch gemeinsame Grundlagen, Sprache und Doktrin;
— das Vermeiden von Informationsüberflutung;
— den Erhalt der Integrität von Informationen / Daten.

Der Mensch, die IKT und die Cybersicherheit spielen eine zentrale Rolle. «Träger» der Daten ist die IKT. Sie stellt die notwendige Verarbeitungslogik und -leistung zur Verfügung und ermöglicht den Datenaustausch. Weiter braucht es eine Kultur, die das Infor-

32 Wirkungen im Informationsraum, beispielsweise im Rahmen von Armeeoperationen, sind nicht Gegenstand der vorliegenden Gesamtkonzeption. Diese werden in den Grundlagen zur längerfristigen Ausrichtung der Armee beschrieben.

mation Sharing und die Zusammenarbeit fördert. Gleichzeitig müssen die eigenen Daten geschützt werden: Stichworte sind hier Vertraulichkeit, Integrität und Verfügbarkeit der Information sowie Authentizität, Verbindlichkeit, Zurechenbarkeit und Resilienz. Im Rahmen des Informationsmanagements werden Regeln definiert, die von allen Beteiligten diszipliniert eingehalten und von der IKT unterstützt werden.

Für die Führung künftiger militärischer Einsätze sind digitalisierte Informationen über Organisations- und Systemgrenzen hinweg ein Schlüsselfaktor zum Erfolg. Die Verfügbarkeit der notwendigen Daten ist ein kritischer Faktor; er hängt direkt vom Erfolg im Kampf um den Wissensvorsprung, dem Eigenschutz im Cyberbereich und der IKT-Betriebsführung ab. Dieser Vorsprung bedeutet, vereinfacht ausgedrückt, dass die eine Partei mehr als die andere über den gleichen Sachverhalt weiss.

Die Gesetzgebung zu Informationssicherheit und Datenschutz spielt dabei eine grosse Rolle. Da in Governance-Bereichen oft unterschiedliche Regeln gelten und Vereinbarungen (Trust-Beziehungen) fehlen, sollten Partner ihre Datenaustauschbeziehungen mit entsprechenden Verträgen regeln. Jede beteiligte Organisation behält dabei jedoch die Informations- und Datenhoheit in ihrem Verantwortungsbereich. Sie entscheidet also selbst, welche Informationen sie mit wem teilt.

Tendenz: Es ist davon auszugehen, dass

- das Information Sharing an Bedeutung gewinnen und dessen Effektivität ein geeignetes menschliches Verhalten und eine Kultur der Zusammenarbeit voraussetzen wird;
- die Aktionsführung von stark vernetzten variablen Datenflüssen und einer grossen Datenflut begleitet wird, die eine Priorisierung und sowie den Einsatz von Informationslogik erfordern werden;
- die Zusammenarbeit mit externen Partnern zunehmen wird, was zu einem flexiblen und erweiterbaren, föderierten Informationsraum führen wird, in dem Zusammenarbeitsverträge (Governance und Trust-Beziehungen) gefragt sind.

Elektromagnetischer Raum

Der elektromagnetische Raum ermöglicht die drahtlose Datenkommunikation zwischen zwei oder mehreren Komponenten von IKT-Systemen, die Lokalisation und die Steuerung von Geräten wie etwa Flugdrohnen oder Sprengsätzen. Dank der Unabhängigkeit von physischen Leitern (z. B. Kabeln) bietet der elektromagnetische Raum eine Vielzahl kostengünstiger, rasch umsetzbarer und räumlich flexibler Anwendungsmöglichkeiten. Bei der mobilen Führung von militärischen Verbänden und Systemen im Gelände oder in der Luft ist die funktechnische[33] Datenkommunikation die einzig anwendbare Technologie.

Die Schweizer Armee nutzt eine wachsende Zahl von verschiedenen Funksystemen mit unterschiedlichen Technologien. Deren Lebensweg- und Sicherheitsmanagement ist eine Herausforderung, zumal die verwendete Funktechnik häufig vom Hersteller eines Waffensystems bestimmt wurde. Im Umfeld der Armee werden zurzeit Funksysteme mit gerichteten (Richtfunk) und ungerichteten elektromagnetischen Ausstrahlungen (z. B. taktische Funkgeräte) in verschiedensten Frequenzbereichen und Signalarten genutzt. Vermehrt kommen sogenannte Software Defined Radios (SDR) zum Einsatz, mit

33 Funktechnik: «Teilgebiet der Nachrichtentechnik mit allen technischen Verfahren und Geräten zur drahtlosen Übermittlung von Signalen mithilfe von Funkwellen.» Duden, https://www.duden.de/rechtschreibung/Funktechnik

denen Teile der Funktionen eines Funksenders oder -empfängers durch Software (digitalisiert) wahrgenommen wird. Die SDR können in der Regel zentral verwaltet werden und sind als «Kleincomputer» durchaus auch Ziele von Cyber-Angriffen.

Die für Aktionen im elektromagnetischen Raum notwendigen Ausrüstungen und Technologien orientieren sich daran, welche Systemen es aufzuklären und zu bekämpfen gilt. Immer dann, wenn neue Signale oder Verfahren zur Informationsübertragung zum Einsatz kommen, müssen auch die Systeme der elektronischen Aufklärung und Störung technisch nachgerüstet werden. Geschieht dies nicht, verlieren diese Systeme unter Umständen in kurzer Zeit vollständig ihre Wirksamkeit[34]. Umso wichtiger ist es, neue Signale und Verfahren im elektromagnetischen Spektrum permanent zu erfassen und zu analysieren (Signalaufklärung) und die Entwicklung in der Funktechnik laufend zu beobachten.

Der «elektronische Kampf» dient auch künftig dazu, gegnerische Funk-, Radar- und Satellitennavigationssysteme am Boden und in der Luft zu erkennen, zu lokalisieren und durch elektronische Gegenmassnahmen in ihrer Funktionalität einzuschränken oder diese ganz aufzuheben. Gleichzeitig gilt es, die eigenen Funksysteme der gegnerischen Aufklärung zu entziehen oder die eigenen Aufklärungs- und Störsysteme zu schützen. Hierzu können auch Angriffe gegen gegnerische elektronische Aufklärungssysteme geführt werden.[35]

Eine zukunftsträchtige Untergruppe an Waffensystemen im elektromagnetischen Raum sind die sogenannten Hochenergiewaffen. Dabei handelt es sich um eine neue Generation von Wirkmitteln, die gebündelte Energie nutzen. Sie werden im militärischen Kontext dazu eingesetzt, gegnerische Ausrüstung, Einrichtungen und Personal ausser Gefecht zu setzen, zu beschädigen, zu deaktivieren oder zu vernichten. Sie kommen in vielen Bereichen zum Einsatz und werden mit der steten Technologieentwicklung immer leistungsfähiger. Beispiele solcher Waffen sind Partikelstromwaffen, Plasmakanonen, Ultraschallwaffen sowie elektromagnetische Strahlenwaffen (Hochenergielaser oder Blendwaffen). Letztere sind für die vorliegende Konzeption von Bedeutung.

Im elektromagnetischen Raum verfügen elektronische Aufklärungs- und Störsysteme mit ihren Sensoren und Wirkmitteln sowie den dazugehörigen Operationszentralen über einen eigenen Sensoren-, Nachrichten-, Führungs- und Wirkungsverbund (SNFW). Dieser wiederum ist in den wirkungsraumübergreifenden Führungsverbund der Armee eingebunden. In der zukünftigen Signalumwelt wird es deutlich mehr Sensoren brauchen, da aufgrund moderner Signalcharakteristiken eine Erfassung nur mehr aus einem relativ nahen Bereich möglich sein wird. Diese Tendenz gilt grundsätzlich auch für Wirkmittel. Aufgrund der hohen Anzahl ausgestrahlter Funksignale und der Leistungsfähigkeit der Sensoren und Wirkmittel ist das Datenvolumen im elektromagnetischen Raum sehr hoch. Wahrscheinlich können in naher Zukunft nur noch moderne Technologien wie künstliche Intelligenz oder Big Data Analytics wertvolle Informationen in nützlicher Zeit auswerten. Zudem wird sich die Schnittstelle zwischen Mensch und System verändern müssen, beispielsweise mit Augmented Reality. Nur so kann die Armee mit der operationellen Geschwindigkeit im SNFW Schritt halten und komplexe Daten in der erforderlichen Zeit bearbeiten.

Hybride Konfliktführung und der Umstand, dass die Armee im Konfliktfall voraussichtlich in überbautem Gelände eingesetzt würde, erfordern eine erhöhte Flexibili-

34 Denkbar ist zum Beispiel, dass ein gegnerischer Akteur kurz vor einem Angriff neue und unbekannte Signale und Verfahren auf seinen Funksystemen (Software Defined Radio) implementiert und so elektronische Aufklärungs- und Störsysteme unwirksam werden lässt. Umgekehrt würde das bedeuten, dass die Schweizer Armee in Friedenszeiten sinnvollerweise andere funktechnische Signale und Verfahren verwenden würde als im Konflikt.

35 Stellen als Teil des elektronischen Kampfes die eigene Nutzung des elektromagnetischen Raums trotz gegnerischer elektronischer Kriegführung sicher. Sie umfassen aktive und passive Massnahmen.

tät bei technischen Konfigurationen und Fähigkeiten der Systeme. Militärisch sollten sie in der Lage sein, auch von der Gegenseite verwendete zivile Funksysteme zu erfassen und zu bekämpfen. Im heutigen Einsatzumfeld braucht es kleine, teils tragbare elektronische Aufklärungs- und Störsysteme, die sich einfach und rasch in ein übergeordnetes Gesamtsystem integrieren lassen. So sollte auch die Fähigkeit ausgebaut werden, mit elektronischen Gegenmassnahmen sogenannte Improvised Explosive Devices (IED) zu bekämpfen. Die Fähigkeit zur Abwehr solcher Sprengsätze besteht zwar in Ansätzen schon heute im Bereich Kampfmittelbeseitigung und Minenräumung (KAMIR). Sie wird aber gegenwärtig weder vernetzt noch im Rahmen einer Gesamtoperation geplant und eingesetzt.

Tendenz: Es ist davon auszugehen, dass

- Systeme zur Erfassung und Wirkung im elektromagnetischen Raum permanent betrieben und basierend auf neuen Bedrohungsszenarien kontinuierlich weiterentwickelt werden müssen;
- Akteure über das gesamte Spektrum im elektromagnetischen Raum (auch nicht militärisch) agieren werden, um ihre Ziele zu erreichen – ohne Berücksichtigung der schweizerischen Regulationen;
- der elektronische Kampf mit degradierbaren, zielorientierten und vernetzten Sensoren und Effektoren genutzt sowie mit dem SNFW-Verbund wirkungsraumübergreifend auf Stufe Armee geführt wird;
- wirkungsraumübergreifende, kombinierte Wirkungen die Kampfunterstützung nachhaltig und wirksam verbessern werden;
- der Faktor Zeit in Kombination mit hohen Datenvolumen die Anwendung neuer Technologien erforderlich machen wird (Data Science);
- sich die Schnittstelle zwischen Mensch und System vom einfachen Computerarbeitsplatz hin zu einer mehrdimensionalen Interaktionsplattform weiterentwickeln wird (Augmented Reality).

Informations- und Kommunikationstechnologie

Die Informations- und Kommunikationstechnologie (IKT) durchdringt alle Tätigkeitsbereiche der Gesellschaft und bildet so den Cyberraum. Als Querschnittsbereich beeinflusst sie die Möglichkeiten im CER massgeblich. Die IKT verarbeitet permanent Informationen, steuert Systeme, warnt vor Gefahren und lässt Menschen und Maschinen miteinander kommunizieren.

Treiber für die Entwicklung in der IKT sind[36]:

— Degradationsfähigkeit (Funktionstüchtigkeit von herausgetrennten IKT-Komponenten oder ganzen Teilen von Netzwerken), Dezentralisierung, Digitalisierung, permanenter Bedarf von Verbindung und Informationsaustausch;
— Modularisierung, Integration, Föderation, Kooperation, Standardisierung, Automatisierung und Technologie;
— steigende Cyberbedrohungen, Informationssicherheit, nationale Interessen, Gesetze, Demografie und Rechtslagen.

36 Aus der IKT-Architektur 4.0 abgeleitet und dort präzisiert wiedergegeben.

Damit verlässliche Informationen verfügbar sind, ist eine effektive und effiziente IKT-Unterstützung entscheidend.

Ein wichtiger Wirkungsbereich der IKT ist daher die nahezu gleichzeitige und ortsunabhängige Bereitstellung von Informationen, welche die angestrebte Informationsüberlegenheit überhaupt möglich macht. Weitere Wirkungsbereiche sind die Prozessbeschleunigung (Effizienzsteigerung) und die Automatisierung repetitiver Prozesse (Verarbeitung von Massendaten). Dank neueren Entwicklungen von Algorithmen können heute beispielsweise militärische Kommandanten für die Vorbereitung ihrer Entscheide auch Simulationen und Formen der künstlichen Intelligenz nutzen.

Damit die Armee die notwendigen Daten im Einsatz bereitstellen kann, ist für den Informationsaustausch eine umfassende Vernetzung nötig. Eine solche Vernetzung muss jederzeit sicher und robust funktionieren. Voraussetzungen für Sicherheit und Robustheit sind ein einheitliches Informationsmanagement, eine Prozess- und Datenstandardisierung und eine definierte Sicherheitsarchitektur.

Die Armee muss fähig sein, die Anwendung der IKT mit entsprechenden organisatorischen und gesetzgeberischen Massnahmen mitzubestimmen. Die nötigen Schritte, die zum erfolgreichen Einsatz der IKT führen, muss sie in eigenen Prozessen festhalten. Für eine reibungslose und dauernde Leistungserbringung der IKT ist eine hohe Automatisierung sowohl in der IKT-Betriebsführung als auch im IKT-Betrieb notwendig.

Um mögliche Lücken in der militärischen IKT-Leistungserbringung zu schliessen oder auch einzelne Silo-Systeme anzubinden, können zivile Telekommunikationsmittel ergänzend genutzt werden.

Tendenz: Es ist davon auszugehen, dass

- die Erfassung, Verarbeitung, Speicherung und Verbreitung von immer grösser werdenden Datenmengen entsprechende Technologien sowie Automatisierungs- und Standardisierungsverfahren erfordert;
- die nutzerorientierte, zeitgerechte, gebündelte und automatisierte Bereitstellung von Informationen zu Informationsüberlegenheit führt und damit den nötigen Entscheidvorsprung generiert;
- die zukünftige IKT ortsunabhängig, degradierbar, modularisiert und standardisiert sein muss, um die nutzerorientierten Bedürfnisse decken zu können;
- das Technologie-Management, d. h. die Technologie und ihre Handhabung, einer der wesentlichen Erfolgsfaktoren der zukünftigen IKT in Bezug auf Automatisierung und Digitalisierung sein wird;
- die IKT weitreichende automatisierte Supportleistungen benötigt, die zumindest teilweise miliztauglich sein müssen;
- der IKT-Betrieb wegen gegnerischen Wirkungen hochsicher, robust, redundant, armeeweit und bis auf die untere taktische Stufe ausgelegt werden sollte.

Kryptologie

Nur mit Kryptologie können Daten sicher aufbewahrt und übermittelt werden. Sie spielt deshalb im CER eine wichtige Rolle. Die Kryptologie befasst sich mit der Konzeption, Konstruktion und Analyse von sicheren Informationssystemen. Sie unterscheidet zwischen den Begriffen Kryptografie und Kryptoanalyse.

Bei der Kryptografie geht es um die Realisation von sicheren Kryptosystemen. Die zentralen Schutzziele in der Kryptografie sind Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit. Ein bestimmtes Kryptosystem muss nicht notwendigerweise all diese Ziele erfüllen.

Dem gegenüber steht die Kryptoanalyse. Sie zielt darauf ab, Kryptosysteme zu brechen, d. h. deren Sicherheit zu kompromittieren, beispielsweise durch ein unberechtigtes Eindringen in Computersysteme und Ausspähen und Manipulieren von Daten. Die Armee kann die Kryptoanalyse im Falle erhöhter Spannungen und in einem Konflikt als offensives Mittel zu ihren Gunsten einsetzen. Im Alltag wird sie vorwiegend zur Aufklärung angewendet, beispielsweise von verschlüsselten Nachrichten.

Bei der technologischen Entwicklung der Zukunft werden grosse, universelle Quantencomputer eine wichtige Rolle spielen. Für ihre Forschung und Entwicklung wird heute weltweit viel Aufwand betrieben. Solche Quantencomputer arbeiten im Gegensatz zum gängigen Computer nicht auf der Basis der klassischen Physik, sondern aufgrund von quantenmechanischen Zuständen. Mit ihrer Hilfe könnte es künftig möglich werden, einige der bekanntesten Chiffrier-Algorithmen und Schlüsselaustauschverfahren zu brechen. Zurzeit müssen in der Entwicklung noch einige grundlegende Probleme gelöst werden, etwa die hohen Fehlerraten und die Dekohärenz (irreversible Veränderungen durch Wechselwirkungen). Daher sind Prognosen schwierig und unsicher, wann Quantencomputer zur Verfügung stehen werden, um Angriffe auf gängige kryptografische Verfahren zu ermöglichen.

In der Informationssicherheit sind kryptografische Komponenten (z. B. datenverarbeitende Systeme) allgegenwärtig. Sie können u. a. Informationen und Systeme wirksam schützen. Allerdings hat die Komplexität von datenverarbeitenden Systemen derart zugenommen, dass standardisierte Kryptoverfahren kein Garant mehr sind für Sicherheit.

Drei Eigenschaften bilden die zentralen Voraussetzungen, damit Kryptografie ein System wirkungsvoll absichern kann:

1. Ein kryptografisches Einsatzkonzept – denn die sichersten Krypto-Algorithmen nützen wenig, wenn diese konzeptionell falsch eingesetzt werden.
2. Die korrekte Ausführung der kryptografischen Funktionen: Bereits kleine Fehler in der Implementation können fatale Folgen haben.
3. Eine über die gesamte Einsatzdauer geschützte Integrität. Nur so können die kryptografischen Funktionen korrekt zur Anwendung kommen.

Für einen Staat oder eine Armee ist es deshalb zentral, über eigene kryptografische Kompetenzen zu verfügen. Es wäre äusserst riskant, sich auf die Fachkompetenz anderer Staaten oder bestimmter Organisationen zu verlassen.

Die Kryptografie und die Kryptoanalyse sind voneinander abhängig und werden gemeinsam weiterentwickelt. Denn kryptografische Systeme werden umso besser, je eingehender sie mit kryptoanalytischen Fähigkeiten und Instrumenten geprüft wurden. Umgekehrt profitiert die Kryptoanalyse vom Know-how der Kryptografie, wenn kryptografische Konzepte in die Analyse miteinbezogen werden können. Daher kann das Potenzial auf diesem Gebiet nur durch die Kombination beider Kompetenzen voll ausgeschöpft werden.

Tendenz: Es ist davon auszugehen, dass

- kryptografische Funktionen zunehmend in Software- sowie Hardwarelösungen integriert werden;
- zukünftige technische Entwicklungen einzelne existierende Verschlüsselungsverfahren unbrauchbar machen werden;
- nur eigene kryptografische Kompetenzen und das Management der technischen kryptografischen Funktionen die nötige Sicherheit ermöglichen;
- mit dem Einsatz der Kryptografie und der Kryptoanalyse zukünftige, eigene Systeme überprüft und effektiv abgesichert werden können;
- die Kryptografie und die Kryptoanalyse sich ergänzen und nur kombiniert ihr volles Potenzial ausschöpfen können.

2.4 Erkenntnisse

Damit die Armee ihre Aufgaben[37] erfüllen kann, muss sie ganzheitlich über alle Wirkungsräume operieren können. Die Kernleistung der Armee im CER besteht darin, Informationen und Services auf der eigenen IKT ortsunabhängig zur Verfügung zu stellen und zu schützen. Dabei soll sie angebundene Partner nicht gefährden und damit ihre eigene Führungsfähigkeit und jene ihrer Partner in allen Lagen sicherstellen. Weil Cyberangriffe täglich erfolgen, muss die Armee diesen Schutz permanent, also auch im Alltag, gewährleisten können. Weiter muss sie fähig sein, militärische Operationen und Einsätze in anderen Wirkungsräumen mit Aktionen im Cyber- und elektromagnetischen Raum zu unterstützen.[38] Die sogenannten «Cyber Electromagnetic Activities» (CEMA) erlauben dabei wirksame Massnahmen bis auf die taktische Stufe, um den Wissensvorsprung zu erreichen.[39]

Treiber aus bestehenden konzeptionellen Grundlagen[40]

In den bestehenden konzeptionellen Grundlagen lassen sich zusammenfassend fünf grundsätzliche Treiber ableiten.

— Erstens wird ein Schwergewicht auf die Fähigkeit zur technischen und prozessualen Zusammenarbeit mit Partnern gelegt, die föderalistisch organisiert ist.
— Zweitens kommt die Forderung nach Digitalisierung in allen untersuchten Konzepten vor, jedoch ohne dass der Begriff «Digitalisierung» auf die Armee bezogen präzis definiert wird.
— Drittens wird die nationale Bedeutung des Schutzes vor Cyberrisiken auch in der Armee immer wieder hervorgehoben.
— Viertens bindet die NCS mit den drei Säulen Cyberstrafverfolgung, Cybersicherheit und Cyberverteidigung die Armee mit konkreten Aufgaben in das nationale Cyberdispositiv ein. Drei Forderungen an die Armee sind dabei zentral: sich selbst zu schützen, mit zivilen Partnern zusammenzuarbeiten und die Behörden subsidiär zu unterstützen.
— Fünftens verlangen die Konzepte zur längerfristigen Ausrichtung der Armee, wie sie insbesondere in den Berichten zur Zukunft der Luftverteidigung und der Bodentrup-

37 Die Schweiz und ihre Bevölkerung zu schützen und zu verteidigen, die zivilen Behörden nach Bedarf subsidiär zu unterstützen, die Lufthoheit zu wahren sowie Beiträge an die Friedensförderung zu leisten.
38 Siehe Kapitel 5 Fähigkeiten.
39 UK Ministry of Defence, Joint Doctrine Note 1/18, Cyber and Electromagnetic Activities, 2018.
40 Siehe Kap. 1 Einführung: Botschaft zur Legislaturplanung 2019–2023; Sicherheitspolitischer Bericht des Bundesrates 2016; Digitalisierungsstrategie des Bundes; Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS 2.0) 2018–2022; IKT-Strategie des Bundes 2020–2023; Strategie des Bundesrates für eine digitale Schweiz; Grundlagenberichte Bodentruppen und Luftverteidigung der Zukunft; Cyber-Strategie VBS 2020; Zielbild FUB 2022, LAA.

pen dargestellt werden, allesamt einen digitalisierten Führungsverbund auf und zwischen allen Führungsstufen.

CER in Operationen und Einsätzen

Die geforderte Leistung kann nicht erst bei Spannung oder im Falle eines Konflikts erbracht werden. Sie muss bereits im Alltag verfügbar sein, denn Cyberangriffe finden bereits dann statt, anonym und ortsunabhängig. Dieser Umstand hat einen wesentlichen Einfluss darauf, wie die Einsatzelemente und die erforderlichen Fähigkeiten ausgestaltet werden. Im Einsatz können lokal begrenzt einzelne, nicht vernetzte Informatiksysteme (Stand-alone-Systeme) von gegnerischen CEMA angegriffen werden und dadurch im schlimmsten Fall ihren Auftrag nicht mehr erfüllen. Dieser neuen «Dimension» des gegnerischen Einflusses auf eigene Systeme wird heute noch nicht genügend Rechnung getragen. Um eine Kompromittierung ihrer Systeme durch Cyberangriffe zu verhindern und eigene, auch offensive Cyberaktionen durchführen zu können, muss die Armee ihre Systeme in Zukunft permanent schützen.

Die Armee muss sowohl Anforderungen aus Sicht der Unterstützung als auch der Bedrohungen gerecht werden. Ihre Leistungen im CER soll sie permanent, degradier- und skalierbar, modular, auftragsorientiert, vernetzt, ortsunabhängig, über alle Lagen und wirkungsraumübergreifend erbringen können.

Nationale Vernetzung

Die Armee ist im Alltag bereits sehr engmaschig national vernetzt. Es wird erwartet, dass sie sich vor Bedrohungen im CER selbst nachhaltig schützen kann und nicht zu einem nationalen Sicherheitsrisiko wird. Die zunehmende technische Vernetzung mit zivilen Partnern erfordert zudem gemeinsame Standards – unter anderem zu dem Zweck, dass die Armee die zivil getriebene Entwicklung (Technologie, Recht, Prozesse usw.) nachvollziehen kann. Eine enge Vernetzung kann sich sowohl unterstützend als auch einschränkend auswirken. Deshalb ist es wichtig, dass die Armee dieses Umfeld aktiv begleiten und mitgestalten kann. Zudem muss sie Möglichkeiten finden, mit denen sie das nationale Potenzial in Bezug auf Know-how, Technologie, Arbeitskräfte usw. besser nutzen kann.

Gesellschaft und Politik

Im Zentrum steht die politische Forderung, nach der sich die Armee dem Thema Cyberdefence wirksam anzunehmen hat. Sie soll sich selbst schützen und im Verteidigungsfall autonom Cybermassnahmen ergreifen können. Zudem wird gefordert, dass die Armee die Miliz aktiv in Cyberaufgaben einbindet.

Nicht zuletzt muss sich die Armee auch gegen die Cyberkriminalität schützen können, die teilweise sehr hochentwickelte Werkzeuge einsetzt. Sie muss aber auch verhindern, dass ihre Systeme für illegale Aktionen missbraucht werden.

Technologie

Die Technologien und Systeme im CER entwickeln sich rasch und andauernd weiter. Dabei sind die zivilen technologischen Entwicklungen die treibenden Kräfte der Vernetzung, der Datenübertragung und der intelligenten Verarbeitung. Sie führen zu einem wachsenden, aber auch fragilen Cyberraum. Die Entwicklungsgeschwindigkeit ist so hoch, weil die globale Nachfrage aus der Gesellschaft und Wirtschaft für neue Lösungen stetig steigt. Die jeweilige Sicherheitsorganisation wird laufend vorangetrieben und steht unter Zugzwang: Sie muss sich auf neue Bedrohungen ausrichten und veraltete Sicherheitstechnologien ersetzen.

Die IKT-Komponenten neuer Rüstungsgüter basieren oft auf neuen oder weiterentwickelten Technologien und Systemen. Sie sind nicht der einzige Grund, wieso die Schweizer Armee ihre IKT-Systeme regelmässig anpassen muss: Auch bestehende, veraltete Technologien können neue militärische Anforderungen nicht mehr erfüllen. Die Technologiekonzerne geben der Armee indirekt vor, welche Hard- und Software für sie

am Markt verfügbar ist und welche Komponenten sie ersetzen muss. Der Technologiewandel in der Armee im CER wird also stark von aussen getrieben. Für die Armee ist es daher unabdinglich, diese Entwicklungen verfolgen zu können – so kann sie Chancen nutzen und Gefahren und Risiken frühzeitig erkennen. Zu diesem Zweck benötigt die Armee ein Technologie-Management und ein Technologie-Portfolio. Diese erlauben ihr, moderne Technologien rechtzeitig für sich nutzbar zu machen und die erforderlichen automatisierten Supportleistungen zu erbringen. Das Ziel ist, Informationen kundenorientiert, zeitgerecht und gebündelt (automatisiert) bereitzustellen, um eine Informationsüberlegenheit und den nötigen Entscheidvorsprung zu generieren. Um die CER-Schlüsselfähigkeiten sicherzustellen, müssen moderne Technologien schnell beschafft und nutzbar gemacht werden.

Internationales Umfeld

Das im Kapitel 2.1 beschriebene Konfliktbild macht deutlich, dass Aktionen im Cyber- und elektromagnetischen Raum in allen zeitgenössischen Konflikten verstärkt und selbstverständlich als Machtmittel eingesetzt werden. In diesem Bereich findet auch ein stetiger Aus- und Aufbau dieser Mittel statt. CER-Aktionen werden oft zeitlich weit im Voraus durchgeführt, also bereits in Friedenszeiten vor dem eigentlichen Konflikt.

Damit die Armee ihre Aufgaben erfüllen kann, muss sie ihre Leistungen sowohl bei erhöhten Spannungen als auch in einem Konflikt in allen Wirkungsräumen koordiniert erbringen können. Der permanente Schutz vor Cyberbedrohungen bereits im Alltag ist die Voraussetzung dafür.

Die unterschiedlichen Cyber-Verteidigungsstrategien anderer Streitkräfte sind für die Schweizer Armee keine direkten Treiber. Sie zeigen jedoch auf, dass Wirkungskräfte im CER in einer Organisation tendenziell zusammengelegt und auf operativer Stufe geführt werden sollten.

3

Organisatorische und rechtliche Grundlagen

Das rechtliche Regelwerk für die Weiterentwicklung im CER bedarf dem Verständnis der organisatorischen Entwicklung und deren rechtlichen Rahmenbedingungen.

3 Organisatorische und rechtliche Grundlagen

3.1 Einleitung

Gemäss Art. 5 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV) ist das Recht Grundlage und Schranke staatlichen Handelns. Staatliches Handeln muss im öffentlichen Interesse liegen und verhältnismässig sein.[41]

Weiter legt die Bundesverfassung die Aufgaben für die Schweizer Armee fest. Die Armee dient der Kriegsverhinderung und trägt zum Erhalt des Friedens bei; sie verteidigt das Land und seine Bevölkerung. Sie unterstützt die zivilen Behörden bei der Abwehr schwerwiegender Bedrohungen der inneren Sicherheit und bei der Bewältigung anderer ausserordentlicher Lagen. Das Gesetz kann weitere Aufgaben vorsehen.[42]

Nachfolgend wird aufgezeigt, wie die heutigen organisatorischen Strukturen innerhalb der Militärverwaltung und der Armee entstanden sind, und wie dort Daten bearbeitet[43] werden. Organisatorische Strukturen und ihre rechtlichen Grundlagen sind ein Abbild der Umstände sowie der gesellschaftlichen und politischen Entwicklungen ihrer Zeit, wobei zukünftige Änderungen stets von letzteren abhängig sind bzw. angestossen werden.

Die Strukturen wiederum geben vor, welche fachkundigen Stellen innerhalb der Bundesverwaltung welche Leistungen erbringen und wie andere Stellen diese beziehen können.

Für die Leistungserbringung im CER sowie für den Betrieb von IKT-Systemen gilt diese Aussage ohne Ausnahme. Erst die Betrachtung der Strukturen und Entwicklungen in diesen Bereichen *ex post* ermöglicht es, die geltenden Rahmenbedingungen zu erfassen und Herausforderungen zu erkennen, die es beim Erfüllen von zukünftigen Bedürfnissen zu bewältigen gilt.

3.2 Organisatorische Entwicklungen

3.2.1 Nachrichtendienstliche Leistungen

Im Jahr 2008 beauftragte die Bundesversammlung den Bundesrat, die beiden Dienststellen, welche Aufgaben des zivilen Nachrichtendienstes erfüllten, dem gleichen Departement zu unterstellen:[44] Aus den nachrichtendienstlichen Teilen des Dienstes für Analyse und Prävention (DAP) des Eidgenössischen Justiz- und Polizeidepartements (EJPD) und dem Strategischen Nachrichtendienst (SND) im Departement VBS entstand 2010 der Nachrichtendienst des Bundes (NDB). Er basiert heute auf dem Bundesgesetz vom 25. September 2015 über den Nachrichtendienst (Nachrichtendienstgesetz, NDG; SR 121).[45] Die bis anhin verwendeten gesetzlichen Grundlagen des SND und des DAP wurden ausser Kraft gesetzt.[46] Vor dieser Zusammenführung war der SND für die Beschaffung von Informationen im Ausland und deren Auswertung verantwortlich – der

41 Art. 5 Abs. 1 und 2 BV.
42 Art. 58 Abs. 2 BV. Die weiteren Aufgaben sind in Art. 1 MG festgehalten.
43 Vgl. Art. 3 lit. e des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG), SR 235.1, der das Bearbeiten von Personendaten als jeglichen Umgang unabhängig der angewandten Mittel und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten, definiert.
44 Art. 2 des Bundesgesetzes vom 03. Oktober 2008 (ausser Kraft) über die Zuständigkeit im Bereich des zivilen Nachrichtendienstes (ZNDG).
45 Vgl. Botschaft zum Nachrichtendienstgesetz vom 19. Februar 2014 BBl 2013-2794, S. 2016 (nachfolgend Botschaft NDG).
46 Vgl. Anhang I NDG (AS 2017 4134).

DAP seinerseits für den Inlandnachrichtendienst.[47] Diese Zuständigkeit ergab sich für den DAP aus dem Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit. Die Zuständigkeit des SND basierte auf Art. 99 Abs. 1 des Bundesgesetzes vom 3. Februar 1995 über die Armee und die Militärverwaltung (Militärgesetz MG), Stand 1. Januar 2004. Letzterer wurde durch die Verordnung vom 4. Dezember 2000 über den Nachrichtendienst im VBS (Nachrichtendienstverordnung, VND; SR 510.91) ergänzt.[48]

2004 nahm die Armee das Satellitenaufklärungssystem «ONYX» in Betrieb. Die neue Fähigkeit zur Satellitenaufklärung bedeutete einen Eingriff in die Grundrechte, der eine Anpassung der rechtlichen Grundlagen erforderte. Als Resultat wurde die Verordnung über die elektronische Kriegführung (VEKF)[49] in Kraft gesetzt.[50] Technisch wurde die Fähigkeit zur Satellitenaufklärung in der Abteilung Elektronische Kriegführung (AEKF)[51] aufgebaut.[52] Durch das MG und die VEKF wurde definiert, dass die Schweiz betreffende Informationen im Allgemeinen nicht an den SND weitergeleitet werden durften,[53] da dieser nicht berechtigt war, Aufklärungsarbeiten im Inland zu betreiben.[54]

Nebst der Funkaufklärung wurde in der Folge auch die Kabelaufklärung[55] vom Zentrum elektronische Operationen betrieben (ZEO, ehemals FUB-EKF bzw. AEKF), denn nur dieses darf über die notwendigen technischen Anlagen verfügen.[56] Dadurch, dass das ZEO nicht direkt mit dem Leistungsbezüger verbunden war, wollte der Gesetzgeber die Grundrechte schützen.[57] Bei der Kabelaufklärung werden bestimmte Datenströme auf internationalen Fernmeldekabeln erfasst und ähnlich wie bei der Funkaufklärung nach Inhalten abgesucht, triagiert und der Auswertung zugeführt. Im Gegensatz zur Fernmeldeüberwachung im Inland, die als genehmigungspflichtige[58] Beschaffungsmassnahme gilt, ist die Kabelaufklärung ein Mittel der Auslandaufklärung. Auch sie ist genehmigungspflichtig.[59]

Um knappe Ressourcen effizient zu nutzen, hat der NDB bei der Umsetzung des NDG bewusst darauf verzichtet, Fachwissen auszubauen, das bereits beim ausführenden Dienst ZEO vorhanden war. Entsprechend wird dieser jeweils vom NDB beauftragt, bewilligungs- bzw. genehmigungspflichtige Beschaffungsmassnahmen nach Art. 26 Abs. 1 lit. d und Art. 37 NDG durchzuführen, um in Computersysteme und Computernetzwerke einzudringen. Ein Eindringen bezweckt dabei die Beschaffung von Informationen oder soll den Zugang zu Informationen stören, verhindern oder verlangsamen.

---

47 Vgl. Satellitenaufklärungssystem des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (Projekt «ONYX»); Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte vom 10. November 2003, BBl 2003-2615, 4.2, S. 1512 (Projekt «ONYX»); Effizientere Bekämpfung von Terrorismus und organisiertem Verbrechen; Bericht des Bundesrates in Erfüllung des Postulates der Sicherheitspolitischen Kommission SR (05.3006) vom 9. Juni 2006, BBl 2006-0523, 3.2.2, S. 5708.

48 Die Verordnung hielt fest, dass der SND «den ständigen Auslandnachrichtendienst sicher(stellt)».

49 Inkraftsetzung am 01. November 2012.

50 Vgl. Rechtmässigkeit und Wirksamkeit des Funkaufklärungssystems «Onyx»; Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte vom 09. November 2007, 5.5.1, S. 12.

51 Eine Abteilung der Untergruppe Führungsunterstützung des Generalstabes.

52 Vgl. Projekt «ONYX», 4.4, S. 1514.

53 Der SND konnte auf Basis der Militärgesetzgebung die AEKF als technischen Dienstleister für Abklärungsaufträge beauftragen (vgl. Rechtliche Grundlagen der elektronischen Aufklärung des Bundes vom 24. April 2003, Bundesamt für Justiz, 3., S. 6f.).

54 Vgl. Projekt «ONYX», 4.2, S. 1513.

55 Vgl. Botschaft NDG, 1.3, S. 2178: «Die Verlagerung der Fernmeldekommunikation von drahtlosen Mitteln (Funk) auf leitungsgebundene Netze (der Verständlichkeit halber hier als Kabel bezeichnet) hat sich in den letzten Jahren mit dem Ausbau der sehr leistungsfähigen Glasfasernetze intensiviert. Gleichzeitig nehmen die Möglichkeiten, Erkenntnisse aus der Funkaufklärung zu gewinnen, etwas ab.»

56 Vgl. Botschaft NDG, 1.3, S. 2177.

57 Vgl. Botschaft NDG, 1.3, S. 2179.

58 Genehmigungspflichtige Massnahmen sind Inlandbeschaffungen, die nicht in Selbstkompetenz des NDB durchgeführt werden können, vgl. Art. 26 Abs. 1 Bst. b, Art. 38 NDG.

59 Art. 39 ff. NDG.

3.2.2 Militärische Sicherheit gemäss Art. 100 MG

Die nachrichtendienstlichen Fähigkeiten der Armee sind im MG definiert und unterscheiden sich von jenen des Dienstes für militärische Sicherheit[60]. In der Botschaft zum MG[61] (3. Kapitel, S. 93) führt der BR aus, dass «eine Trennung geschaffen werden [soll], sowohl zwischen dem Dienst für militärische Sicherheit und dem militärischen Nachrichtendienst als auch zwischen den militärischen Diensten und dem zivilen Abwehr- und – allenfalls – dem Nachrichtendienst, unter klarer Regelung des Informationsaustausches. Mit dieser Trennung ist es möglich, die jeweiligen Aufgaben und Kompetenzen besser zu definieren und zuzuweisen.» Mit dieser Trennung machte der Gesetzgeber deutlich, dass der Dienst für militärische Sicherheit in der ordentlichen Lage keinerlei nachrichtendienstliche Aufgaben wahrzunehmen hatte.[62] Seine Aufgaben lagen in der Beurteilung der Sicherheitslage und im Schutz von militärischen Objekten und Informationen.[63]

Auch mit der Weiterentwicklung der Armee behielt der Gesetzgeber die Teilung bei zwischen dem militärischen Nachrichtendienst (MND) und der militärischen Sicherheit[64]. Er schuf im Rahmen der Änderung des MG vom 18. März 2016 unter anderem[65] die Grundlage für die militärische Cyberabwehr in Art. 100 Abs. 1 lit. c MG.[66] Dadurch wurde dem VBS die Pflicht übertragen, Cyberangriffe gegen militärische Systeme und Netzwerke mit geeigneten Massnahmen abzuwehren.[67] Mit der Verordnung vom 1. Januar 2019 über die militärische Cyberabwehr (MCAV) trat am 1. März 2019 die Ausführungsverordnung zu Art. 100 Abs. 1 lit. c MG in Kraft.[68]

Die heutigen Strukturen sind folglich grösstenteils politisch entstanden. Die genannten Stellen finden sich im NDB und in der Gruppe V innerhalb des VBS. Der NDB dient als Nachrichtendienst mit dem Auftrag, Informationen zu beschaffen und zu bearbeiten, um wichtige Landesinteressen zu wahren (Art. 2 i. V. m. Art. 3 i. V. m. Art. 6 NDG). Innerhalb der Gruppe Verteidigung ist das ZEO der FUB unterstellt. Als durchführender Dienst stellt es seinen Auftrag auf Grundlage des NDG und des MG sicher.

3.2.3 Sensorfähigkeiten

Ziviler Nachrichtendienst

Zugunsten und im Auftrag des NDB erbringt das ZEO Leistungen im Bereich der Beschaffung von Daten aus der Kommunikationsaufklärung. Das ZEO bearbeitet Daten, die im Rahmen von Funk- und Kabelaufklärungsaufträgen erfasst wurden, und stellt sie dem NDB zur weiteren Auswertung zur Verfügung.

Das ZEO hat Fähigkeiten im Bereich der Funk- und Kabelaufklärung sowie der Beschaffung von Informationen in fremden Computersystemen und -netzwerken aufgebaut,

---

60 Der Dienst für militärische Sicherheit wurde vormals in Art. 105 MG geregelt (1993). Er zeigte sich zuständig für die Beurteilung der militärischen Sicherheitslage, den Schutz von militärischen Informationen und Objekten, die Erfüllung von kriminal- und sicherheitspolizeilichen Aufgaben im Armeebereich, Massnahmen zur präventiven Sicherung der Armee vor Spionage, Sabotage und anderen rechtswidrigen Handlungen. Er beschaffte Nachrichten, wenn seine Angehörigen zu Assistenz- oder Aktivdienst aufgeboten waren und schützte die Mitglieder des Bundesrates, den Bundeskanzler und weitere Personen, wenn seine Angehörigen zu Assistenz- oder Aktivdienst aufgeboten waren. Mit der MG-Revision vom 1. Januar 2018 wurden Teile der Aufgaben des Dienstes für militärische Sicherheit innerhalb des VBS von der Militärpolizei und vom Dienst für präventiven Schutz der Armee (DPSA) übernommen.

61 Botschaft betreffend das Bundesgesetz über die Armee und die Militärverwaltung sowie den Bundesbeschluss über die Organisation der Armee vom 8. September 1993, BBl 1993-626.

62 Vgl. Botschaft MG 1993, 3. Kapitel, S. 94: «Nicht Aufgabe der Organe der militärischen Sicherheit in der ordentlichen Lage und damit auch nicht Teil der Beurteilung der militärischen Sicherheitslage ist hingegen die aktive Nachrichtenbeschaffung.»

63 Vgl. Botschaft MG 1993, 3. Kapitel, S. 94f.

64 Vgl. Botschaft zur Änderung der Rechtsgrundlagen für die Weiterentwicklung der Armee vom 3. September 2014, BBl 2014-6955, S. 7017.

65 Auf Art. 100 MG basiert auch die Verordnung vom 21. November 2018 über die militärische Sicherheit (VMS). Die Verordnung zusammen mit der Schaffung des MND und des DPSA zeigt die neuen Schwergewichte auf.

66 Art. 100 Abs. 1 lit. c MG war im Entwurf des Bundesrates nicht vorgesehen. Erst in der parlamentarischen Debatte wurde die Norm in der heutigen Form eingeführt. Daher bestehen zu dieser Norm keine Materialen, die konsultiert werden könnten.

67 Vgl. Ständerat Kuprecht und Bundesrat Maurer, AB S 2015 708.

68 Die Verordnung regelt die Massnahmen zum Eigenschutz und zur Selbstverteidigung der Armee und der Militärverwaltung im Falle eines Angriffes auf ihre eigenen Informationssysteme und Informatiknetzwerke in der normalen Lage (vgl. Verordnung über die militärische Cyberabwehr, Erläuterung der einzelnen Bestimmungen, S. 1).

damit es seinen Auftrag erfüllen kann.[69] Gesetzliche Grundlagen dazu finden sich in Art. 26 Abs. 1 lit. d Ziff. 1 NDG und Art. 37 Abs. 2 NDG für die Beschaffung von Informationen in fremden Computersystemen und Computernetzwerken, in Art. 38 NDG für die Funkaufklärung und in Art. 39 ff. NDG für die Kabelaufklärung.

Militärischer Nachrichtendienst (MND)

Der MND ist berechtigt (Art. 99 Abs. 1bis MG), Aufträge zur Funkaufklärung gemäss Art. 38 NDG zu erteilen. Diese Aufträge führt das ZEO aus – unabhängig von den Aufträgen des NDB. Daneben steht dem MND die strategische Funkaufklärung gemäss Art. 99 Abs. 1ter MG zur Verfügung.

3.2.4 Wirkungsfähigkeiten

Nachrichtendienstliche Wirkungen

Im Auftrag des NDB kann das ZEO in fremde Computersysteme und Computernetzwerke eindringen, um den Zugang zu Informationen zu stören, zu verhindern oder zu verlangsamen (Art. 26 Abs. 1 lit. d Ziff. 2 und 37 Abs. 1 NDG). Diese Massnahmen bedürfen bei einem Ziel im Inland der Genehmigung durch das Bundesverwaltungsgericht und einer Freigabe durch die Vorsteherin oder den Vorsteher des VBS – dies nach Konsultation der Vorsteherin oder des Vorstehers des EDA und des EJPD (Art. 26 Abs. 1 lit. d Ziff. 2 NDG). Bei einem Ziel im Ausland braucht es die Zustimmung des Bundesrates (Art. 37 Abs. 1 NDG). Solche Massnahmen werden nur bei Angriffen gegen kritische Infrastrukturen in Erwägung gezogen.

Militärische Wirkungen

Die Beeinträchtigung des elektromagnetischen Spektrums[70] und die elektronische Kriegführung (EKF) erfolgt durch das ZEO und durch die Führungsunterstützungsbrigade 41 (FU Br 41). Wichtig ist, dass die Armee nur militärische Frequenzen selbstständig beeinträchtigen kann. Will sie zivile Frequenzen stören, auch innerhalb des Sicherheitsbereiches von geschützten militärischen Anlagen, braucht sie im Alltag die Genehmigung der Vorsteherin bzw. des Vorstehers VBS.[71]

Im Auftrag der FUB kann das ZEO in fremde Computersysteme und -netzwerke eindringen, um Cyberangriffe gegen eigene Systeme und Netzwerke in der normalen Lage mit Mitarbeitenden der Militärverwaltung zu unterbinden (Art. 100 Abs. 1 lit. c MG i. V. m. Art. 2 Abs. 1 MCAV). Die Bewilligung dafür erteilt der Bundesrat.[72]

Einem politischen Entscheid zu einer militärischen Operation, ob in Friedenszeiten oder in Zeiten von Spannung oder Konflikt, liegen stets sämtliche in Betracht kommenden Vorgaben (z. B. der zivilen Luftfahrt) und Konsequenzen für die zivile Bevölkerung, die Wirtschaft und die Bundesverwaltung zugrunde.

3.2.5 Infrastruktur

Die Grundlage für sämtliche Fähigkeiten im nachrichtendienstlichen wie auch im militärischen Kontext ist die Infrastruktur.[73] Mit dem Aufbau von Fähigkeiten werden auch entsprechende digitalisierte Infrastrukturen geschaffen und betrieben. Neue fähigkeitsbezogene Systeme werden jeweils in ein Gesamtsystem integriert. Ihr Schutz[74]

---

69 Die territoriale Abgrenzung ist zur Qualifizierung nicht erheblich.

70 Das elektromagnetische Spektrum umfasst grundsätzlich die Gesamtheit aller elektromagnetischen Wellen verschiedener Wellenlängen, d. h. von Radiowellen über Infrarotstrahlung (Wärmestrahlung), sichtbarem Licht bis hin zur Gammastrahlung. Die Abgrenzung zwischen militärischen und zivilen Frequenzen ist im Nationalen Frequenzzuweisungsplan geregelt.

71 Art. 12 VEKF.

72 Die Bewilligung für eine solche Massnahme wird durch den Bundesrat erteilt (Art. 7 MCAV).

73 Der Betrieb der Infrastruktur, unbesehen des Entwicklungsstandes, bedarf hochqualifizierten Personals. Daher besteht in der Fähigkeit zur Personalrekrutierung und -förderung eine Bindung durch die Vorgaben des Bundes.

74 Schutz als Fähigkeit ergibt sich indirekt aus der MCAV. Weiter bestehen Grundlagen, die den Chef FUB mit dem Schutz der militärischen Systeme und Netzwerke beauftragen. Die Fähigkeit zum Schutz von Systemen beinhaltet diverse weitere, beispielsweise kryptoanalytische Fähigkeiten.

muss jederzeit sichergestellt werden. Der Betrieb der einzelnen Systeme basiert auf verschiedenen, nicht verknüpften rechtlichen Grundlagen.[75] Diese definieren jeweils den Zugang zum System, die Berechtigung zur Datenbearbeitung und deren Zweck.

3.2.6 Militärische Strafverfolgung

Die Strafverfolgung im Zusammenhang mit Cyberkriminalität obliegt den zivilen und militärischen Strafverfolgungsbehörden. Die Militärjustiz ist zuständig, wenn eine mutmassliche Täterschaft gegen das Militärstrafgesetz vom 13. Juni 1927 (MStG) verstossen hat und damit der militärischen Gerichtsbarkeit untersteht. Auch Zivilpersonen können für einige Delikte dem Militärstrafgesetz unterstehen, etwa bei Sabotage i.S.v. Art. 86a MStG. Widerhandlungen ausschliesslich gegen einschlägige Bestimmungen des Schweizerischen Strafgesetzbuchs vom 21. Dezember 1937 (StGB) fallen in den Zuständigkeitsbereich der zivilen Strafverfolgungsbehörden. Liegen gleichzeitig Verstösse sowohl gegen Bestimmungen des MStG als auch des StGB vor, koordinieren die militärischen und zivilen Strafverfolgungsbehörden ihr Vorgehen. Sie treffen in der Regel eine Absprache, damit das gesamte Verfahren durch eine einzige Strafbehörde geführt werden kann.

3.3 Bestehende Rechtsgrundlagen

3.3.1 Bearbeitung von Daten

Die Bearbeitung von Daten ist von militärischem Handeln und der täglichen Arbeit in der Militärverwaltung nicht mehr wegzudenken. Wobei die Bearbeitung von personenbezogenen Daten stets einer gesetzlichen Grundlage bedarf.[76] Ohne Daten mit Informatikmitteln über Netzwerke und Systeme zu bearbeiten, kann die Armee weder ihre tägliche Arbeit erledigen noch militärische Operationen planen oder führen. Rechtliche Grundlagen regeln, welche Daten bzw. Informationen mit welchem Partner über welches System ausgetauscht werden dürfen.[77] Konkret werden Systeme zur Bearbeitung von Daten sowohl mit nationalen wie auch mit internationalen Partnern genutzt und die Aufbewahrung und Löschung dieser Daten festgelegt. Erst dann dürfen Daten überhaupt bearbeitet werden, so dass ein Verbund von Systemen und Netzwerken entstehen kann. Nebst der grundlegenden Möglichkeit des Datenaustauschs müssen die Daten sowohl vom Sender wie auch vom Empfänger kategorisiert werden. Zu diesem Zweck liegen Abkommen über den Schutz und Austausch von Daten mit internationalen Partnern vor. [78]

Das digitale Umfeld nimmt grossen Einfluss auf das Arbeiten in der Armee. Daher sind sowohl die zu nutzenden Systeme und Netzwerke[79] wie auch administrative Vorgänge zu regulieren.[80] Spezifische Systeme und Programme, beispielsweise zur Geschäftsführung, unterliegen Vorschriften, die den Umgang und somit die Rahmenbedingungen definieren.[81] Daten gibt es überall, und sie werden von der ganzen Gesellschaft genutzt. Für ihre Bearbeitung gelten bundesgesetzliche Regeln, die für die Militärverwaltung und die Armee bindend und verpflichtend sind.[82]

---

75 Zusätzlich grenzen sich Systeme durch den Nutzerkreis ab, z. B. FIS Heer und FIS LW.
76 Art. 5 Abs. 1 und Art. 36 Abs. 1 BV, Art. 6 Abs. 1 und Art. 34 Abs. 1 nDSG.
77 Bundesgesetz vom 03. Oktober 2008 über die militärischen Informationssysteme (MIG), 510.91; Verordnung vom 16. Dezember 2009 (MIV), 510.911.
78 Stand Juni 2021 liegen neun Abkommen über den Austausch und Schutz von klassifizierten Informationen mit div. europäischen Ländern vor. Daneben bestehen weitere spezifische Vereinbarungen bspw. mit der NATO (Federated Mission Networking, FMN).
79 Bspw. durch die Verordnung vom 16. August 2017 über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes (VIS-NDB).
80 Bspw. Verordnung vom 8. September 1999 zum Bundesgesetz über die Archivierung (Archivierungsverordnung, VBGA).
81 Bspw. Verordnung vom 3. April 2019 über die elektronische Geschäftsverwaltung der Bundesverwaltung (GEVER-Verordnung).
82 Bspw. DSG und das Informationssicherheitsgesetz (ISG) mit geplanter Inkraftsetzung 2023.

Der funkwellenbasierten Übertragung von Daten gilt besonderes Augenmerk.[83] Wie zuvor ausgeführt, ist der Armee ein Teil des in der Schweiz verfügbaren Frequenzbereiches zugewiesen. Diesen Frequenzbereich zu nutzen und zu regulieren, obliegt der alleinigen Verantwortung der Armee.[84] Der grösste Teil der in der Schweiz verfügbaren Frequenzen sind allerdings zivil und nicht militärisch. Über diese Frequenzen sollen der Bevölkerung und der Wirtschaft Fernmeldedienste[85] angeboten werden. Die Frequenzen werden den Anbietern von Fernmeldediensten mittels Konzessionen vergeben und sind folglich streng reguliert. Ein Anbieter darf nur jene Frequenz nutzen, die ihm zugewiesen ist. Nutzt er andere, wird dies von der zuständigen Stelle entsprechend geahndet.[86]

3.3.2 Organisation

Die Organisation der Departemente und der Bundesämter ergibt sich grundsätzlich aus dem Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997 (RVOG) sowie aus der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998 (RVOV). Diese Grundlagen gelten für die gesamte Bundesverwaltung und über alle Departemente und Bundesämter – unabhängig der Aufgaben, Fähigkeiten und Ausgestaltungen.

Spezifische Ziele, Funktionen und Aufgaben der einzelnen Bundesämter werden auf Basis der Departementsziele in Organisationsverordnungen festgehalten. Für das VBS sind sie in der Organisationsverordnung vom 7. März 2003 (OV-VBS; SR 172.214.1) nachzulesen.

Als Organisation ist die Armee nicht Teil der Bundesverwaltung, sondern eine staatliche Organisation sui generis. Sie bildet also eine Art «Sonderfall». Ihre Organisation ist in eigenen Rechtserlassen geregelt: Dies sind: Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (Art. 58 Abs. 1 und Art. 60 Abs. 1), Bundesgesetz vom 03. Februar 1995 über die Armee und die Militärverwaltung (MG, Sechster Titel: Organisation der Armee), die Verordnung der Bundesversammlung vom 18. März 2016 über die Organisation der Armee (AO), die Verordnung vom 29. März 2017 über die Strukturen der Armee (VSA) und die Verordnung des VBS vom 29. März 2017 über die Detailorganisation der Armee (VDA).

Die organisatorische Struktur der Militärverwaltung und der Armee sind teilweise spiegelgleich. So gibt es in beiden Strukturen einen Armeestab, ein Kommando Operationen, eine Logistikbasis der Armee, eine Führungsunterstützungsbasis und ein Kommando Ausbildung. Die Bundesämter der Gruppe Verteidigung erbringen nicht nur Leistungen zugunsten der Bundesverwaltung und der Armee. Sie müssen diese auch Dritten subsidiär zur Verfügung stellen können – beispielsweise den Blaulicht-Organisationen[87]. Zusätzlich müssen sie den notwendigen Austausch von Informationen und Daten im internationalen Umfeld sicherstellen können. Um diese Leistungen zu erbringen, braucht es entsprechende technische und rechtliche Grundlagen. Das Spektrum der Datenbearbeitung muss vor diesem Hintergrund vollumfänglich und ganzheitlich betrachtet werden.

3.3.3 Anforderungen an die Rechtsetzung

Die verfassungsmässigen Aufgaben der Armee sind der Ausgangspunkt für die weitere Rechtsetzung. Daneben legen Rechtserlasse wie das Datenschutzgesetz (DSG) und das Fernmeldegesetz (FMG) den Rahmen fest, in dem die Armee ihre Fähigkeiten entwi-

83 Zum elektromagnetischen Spektrum vgl. militärischer Wirkungen.
84 Art. 22 Abs. 4 des Fernmeldegesetzes (FMG) vom 30. April 1997, SR 784.10.
85 Art. 3 lit. b FMG: fernmeldetechnische Übertragung von Informationen für Dritte.
86 Art. 49ff. FMG.
87 Vgl. Art. 67 MG Assistenzdienst zur Unterstützung ziviler Behörden (sog. Subsidiarität).

ckeln kann. Es muss im Interesse der Leistungsbezüger sein, die gesetzlichen Rahmenbedingungen so zu gestalten, dass die Armee ihre Handlungsfreiheit behält.

Die Aufgaben der Armee sind komplex. Für die Rechtsetzung ist es eine Herausforderung, jeweils rechtzeitig die entsprechenden Rechtsgrundlagen sicherzustellen. Die IKT-Architektur 4.0 vom 09. Mai 2020 der FUB weist beispielsweise aus, dass der Verbund von Systemen aktuell und zukünftig die primäre Herausforderung darstellt. Durch diesen Verbund werden zwischen verschiedenen Leistungsbezügern und Partnern Daten[88] ausgetauscht und zur Verfügung gestellt, ohne Zeitverzug und räumlich unabhängig. Mit jedem neuen zivilen Partner vergrössert sich das zu überwachende und zu schützende Gesamtsystem.[89] Dadurch ergeben sich neue Schwachstellen und neue Ansprüche an die Geschwindigkeit der Datenübertragung und an die Schutzmassnahmen.[90] Aspekte, die es auch in künftigen Regularien zu berücksichtigen gilt.

Aus den Ausführungen im Kapitel 1.3 geht hervor, dass Daten auftrags- und fähigkeitsbezogen zur Verfügung stehen müssen. Die gesetzlichen Rahmenbedingungen müssen zukünftig derart ausgestaltet sein, dass Daten oder die daraus gewonnenen Erkenntnisse, die im Auftrag für einen Leistungsbezüger beschafft wurden, auch für andere Verwendungen eingesetzt werden können. Zusätzlich soll es eine Durchlässigkeit von Daten für verschiedene Zwecke geben, die in verschiedenen Stellen parallel aufgebaut wurden.[91]

3.4 Ausblick

Der Aufbau von Fähigkeiten und deren Betrieb müssen durch die bestehenden rechtlichen Grundlagen oder durch Rechtsanpassungen sichergestellt werden. Wobei die Weiterentwicklung von Fähigkeiten aus der Analyse des gesetzlichen Auftrages und der regulierenden Rahmenbedingungen hervorgeht. Der Verbund von Fähigkeiten, Partnern und Systemen sowie die enge Zusammenarbeit und Vernetzung zwischen Militärverwaltung und Armee muss zu entsprechend harmonisierten oder sogar einheitlichen Rechtsgrundlagen führen. Unterschiedliche Regelungen gilt es so weit als möglich zu verhindern.[92]

Aufgrund der bestehenden rechtlichen Grundlagen ist die Datenbearbeitung bis anhin nur eingeschränkt möglich. Dies, obwohl sie unter Einbindung sämtlicher Auswirkungen auf Systeme und Netzwerke eine zentrale Fähigkeit ist. Die Aufgaben sind so komplex, dass die Bearbeitung nicht nur innerhalb der Bundesverwaltung erfolgt, sondern auch föderal und ausserhalb mit nationalen und internationalen Partnern. Dazu müssen die entsprechenden rechtlichen Grundlagen geschaffen werden.

Für die Fähigkeiten der Armee braucht es weitreichende und spezifische Rechtsgrundlagen. Werden sie nicht stetig aktualisiert, ist die Nutzung von Fähigkeiten jederzeit und in allen Lagen gefährdet oder nur noch für eine begrenzte Zeit möglich.

Es gilt also, Abhängigkeiten und Entwicklungen eng zu verfolgen und die entsprechenden Rechtsgrundlagen wenn nötig anzupassen, damit die Armee ihre organisatorischen und fähigkeitsbezogenen Bedürfnisse erfüllen kann.[93]

---

88 Es handelt sich nachfolgend um technische und nicht personenbezogene Daten, die bspw. der Lageverfolgung oder Analyse von Programmen dient.
89 Partner finden sich nicht nur innerhalb der Bundesverwaltung (bspw. BABS und BIT), sondern auch ausserhalb im privatrechtlich organisierten Sektor (z. B. RUAG AG).
90 Exemplarisch ist hier die Problematik der Klassifizierung und der uneinheitlichen Sicherheitsstandards aufzuführen.
91 EKF der Armee und EKF der Luftwaffe. Beide Fähigkeiten basieren auf der VEKF, jedoch bestehen zwei unabhängige Weisungen. Die Weisung EKF der Armee sieht keinen Datenaustausch vor, die Weisung EKF der Luftwaffe hingegen schon (Weisungen jeweils gültig bis 31.12.2023).
92 Der Verbund von Systemen macht die militärische Nutzung von ziviler Infrastruktur alltäglich. In einem bewaffneten Konflikt wird militärisch genutzte zivile Infrastruktur deshalb zu einem legitimen militärischen Ziel.
93 Vorliegend wird exemplarisch auf die Revision des MG und der AO verwiesen. Nur durch diese Grundlagen können Anpassungen in der Struktur bzw. Gliederung der Armee und deren Auftrag vorgenommen werden.

Die Aktualisierung und Ergänzung von Rechtsgrundlagen müssen aus rechtsstaatlichen Gründen im Voraus erfolgen. Aufgaben dürfen erst an die Hand genommen werden, wenn die dafür notwendigen gesetzlichen Bestimmungen in Kraft sind. Inwieweit für die Umsetzung des Gesamtkonzepts Cyber bestehende Rechtsgrundlagen angepasst oder neue geschaffen werden müssen, ist daher bei den weiteren Arbeiten stets im Auge zu behalten und rechtzeitig in die Wege zu leiten.

4

Doktrin

Im Einsatz wird derjenige gewinnen, der rascher die richtige Entscheidung trifft und so den Handlungsvorsprung erreicht. Es geht für die Schweizer Armee im Kern also darum, den eigenen Wissens- und Entscheidvorsprung zu erreichen und zu halten – und dies bereits im Alltag.

4 Doktrin

Unter Doktrin werden all jene allgemeinen Prinzipien verstanden, nach denen die Armee ihre Aufgaben erfüllt, um die sicherheitspolitischen und militärstrategischen Ziele zu erreichen, und zwar sowohl im Alltag als auch bei erhöhten Spannungen und in einem Konflikt. Bezugspunkt sind dabei Bedrohungen und Risiken, auf welche die Doktrin – auch im CER – Antworten geben muss.

4.1 Einführung

4.1.1 Operativer Gesamtrahmen

Aktionen im CER dürfen nicht isoliert betrachtet werden. Die Armee führt ihre Einsätze in allen Wirkungsräumen, d. h. nicht nur im Cyberraum und im elektromagnetischen Raum, sondern insbesondere auch am Boden und im Luftraum; daneben nutzt sie Weltraumanwendungen (z. B. für die Präzisionsnavigation und die Nachrichtenbeschaffung) und wirkt mit ihren Aktionen im Informationsraum. Um die militärstrategischen und operativen Ziele zu erreichen, müssen militärische Aktionen in allen Räumen parallel durchgeführt werden. Diese Aktionen in verschiedenen Räumen ergänzen, verstärken oder substituieren sich in ihrer Wirkung. Das Kommando Operationen gewährleistet dabei die übergeordnete Gesamtsicht: Es verfolgt die Lage gesamtheitlich und koordiniert alle militärischen Aktionen über sämtliche Wirkungsräume.

4.1.2 CER

Wesentlich für erfolgreiche Armeeeinsätze ist die sogenannte operative Kohärenz, d. h. die zeitliche Synchronisation und Koordination von Wirkungen und Aktionen militärischer Verbände in allen Wirkungsräumen. Als Bindeglied zwischen dem Informationsraum und den physischen Räumen Boden, Luft, maritimem Raum und Weltraum spielt der CER dabei eine wichtige Rolle: In ihm werden Daten und Informationen für die Planung und Führung der Einsätze bereitgestellt und zeitverzugslos zwischen Verbänden und Systemen übermittelt. Zudem lässt sich im CER die gegnerische Führung beeinträchtigen, indem beispielsweise die Datenübertragung des Gegners gestört oder sogar unterbunden wird oder indem gegnerische Führungsinformationssysteme lahmgelegt werden.

Damit militärische Systeme wirken können, sind sie praktisch ausnahmslos auf IKT angewiesen. Ein Panzer beispielsweise ist nicht nur ein Waffensystem, mit dessen Kanonen sich Bodenziele bekämpfen lassen, sondern er ist über die IKT, die in ihm verbaut ist, auch mit dem Cyberraum verbunden. Erfolgt die Datenübertragung drahtlos, ist er zudem mit dem elektromagnetischen Raum vernetzt. Diese Vernetzung ist insbesondere für die Datenübermittlung, die Nachrichtenbeschaffung oder den elektronischen Kampf gegen Funksysteme von grosser Bedeutung.

4.2 Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen im CER

Für sämtliche Aktionen im CER sind drei Ansatzpunkte zentral, nämlich die Vertraulichkeit, die Integrität und die Verfügbarkeit von Daten und Informationen. Sie sind sowohl für den Eigenschutz relevant als auch für offensive und nachrichtendienstliche Aktionen.

1. Angriffe auf die **Vertraulichkeit** (Confidentiality): Wenn Daten gespeichert, übertragen und verarbeitet werden, muss ihre Vertraulichkeit stets geschützt werden. Dies lässt sich nur gewährleisten, wenn niemand unbefugt auf Informationen in einem System zugreifen kann. Angriffe auf die Vertraulichkeit können sowohl im elektromagnetischen Raum (z. B. bei der Funkaufklärung) als auch im Cyberraum erfolgen.

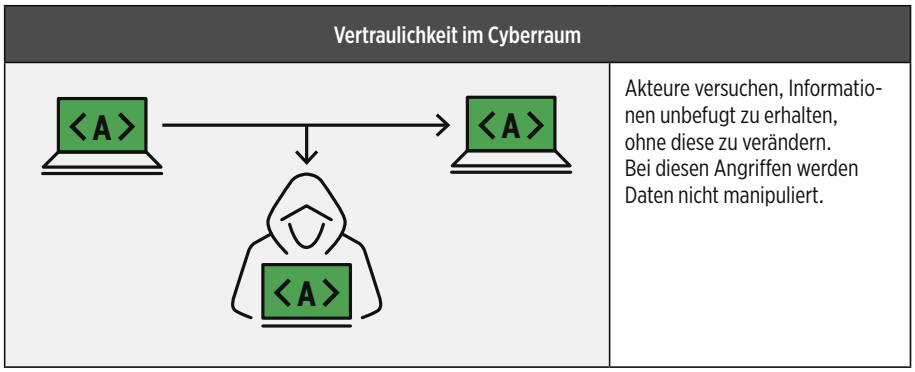


Abbildung 7: Prinzip eines Angriffs auf die Vertraulichkeit im Cyberraum

Im elektromagnetischen Raum können vertrauliche Informationen lediglich während eines beschränkten Zeitraums beschafft werden, nämlich dann, wenn sie über Funkwellen ausgestrahlt werden. Anders als bei Cyberangriffen ist es unmöglich, nur mit Mitteln der Funkaufklärung in Systeme einzudringen und dort nach vertraulichen Informationen zu suchen. Andere Informationen hingegen lassen sich mit Aktionen im elektromagnetischen Raum relativ leicht gewinnen, indem beispielsweise der Standort eines Senders mit Funkortung aufgeklärt wird.

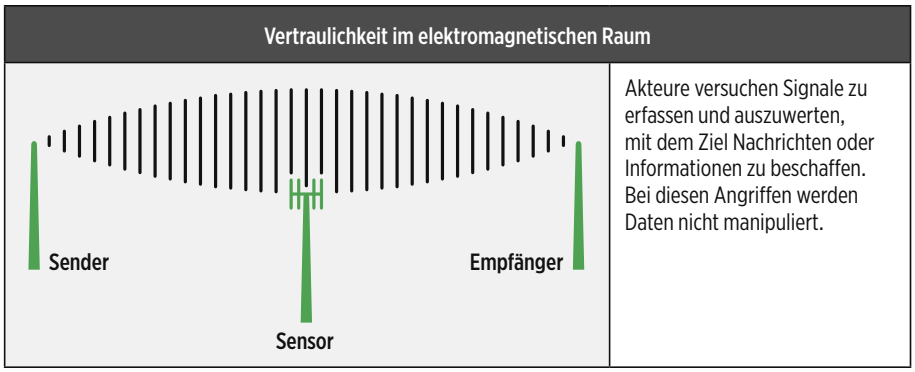


Abbildung 8: Prinzip eines Angriffs auf die Vertraulichkeit im elektromagnetischen Raum

2. Angriffe auf die **Integrität** (Integrity): Daten dürfen nicht unbefugt oder unbemerkt verändert werden. Alle Änderungen müssen nachvollziehbar sein. Integrität lässt sich gewährleisten, wenn verunmöglicht wird, dass Daten unberechtigt und unbemerkt verändert werden. Dieser Grundsatz gilt primär für den Cyberraum.

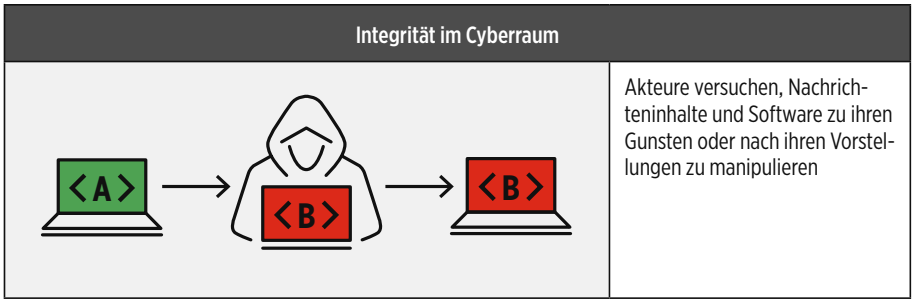


Abbildung 9: Prinzip eines Angriffs auf die Integrität im Cyberraum

3. Angriffe auf die **Verfügbarkeit** (Availability): Ein System gewährt Verfügbarkeit, wenn authentifizierte und autorisierte Zugriffe auf Daten erfolgen und die Dienste und Daten in der geforderten Qualität, unverzüglich und störungsfrei genutzt werden können.

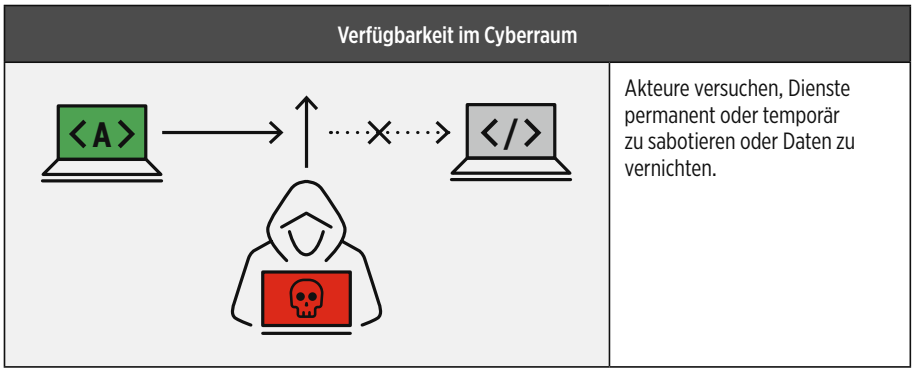


Abbildung 10: Prinzip eines Angriffs gegen die Verfügbarkeit im Cyberraum

Die Verfügbarkeit von Daten lässt sich durch Cyberangriffe beeinträchtigen, aber auch durch Aktionen im elektromagnetischen Raum, beispielsweise indem der Funk gestört wird. Dabei wird – zeitlich und räumlich begrenzt – der Empfang von Informationen verhindert, die über Funkwellen übermittelt werden. Die entsprechenden Aktionen richten sich folglich nicht gegen die eigentliche Verfügbarkeit der Informationen in den Systemen, sondern gegen die technische Fähigkeit, Signale zu empfangen.

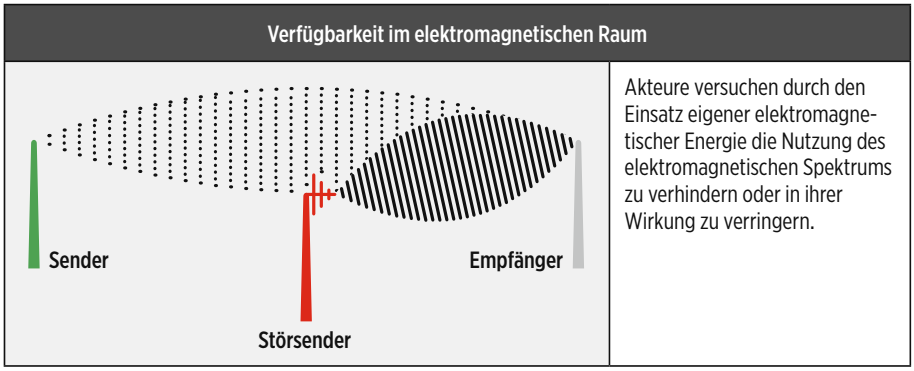


Abbildung 11: Prinzip eines Angriffs gegen die Verfügbarkeit im elektromagnetischen Raum

4.3 Bedrohungen

Risiken und Bedrohungen im Cyberraum sind vielfältig: Sie reichen von kriminellen Aktivitäten über Spionage, Manipulation und Desinformation bis hin zum Einsatz offensiver Cybermittel in einem bewaffneten Konflikt. Um vernetzte Gesellschaften zu destabilisieren oder zu schwächen, nutzen Angreifer immer häufiger Möglichkeiten, die sich aus der globalen Vernetzung und der Digitalisierung ergeben. Ein Akteur kann bereits im Alltag auf den CER eines Gegners einwirken, ohne dass er sich zweifelsfrei als Aggressor zu erkennen geben muss.

Die Bedrohungslage im CER ist komplex. Neue Technologien werden laufend weiterentwickelt, ebenso deren technischen Anwendungen. Dies schafft ständig neue Abhängigkeiten. Mit der Digitalisierung wachsen im CER die Verwundbarkeit und das Missbrauchspotenzial. Aktionen gegen staatliche Institutionen und kritische Infrastrukturen können die Funktionsfähigkeit von Verwaltung, Streitkräften und Sicherheitsbehörden erheblich beeinträchtigen. Sie können sich damit direkt auf die öffentliche Sicherheit und Ordnung auswirken.[94] Virtuelle Werte wie Kryptowährungen, Datensammlungen usw. gewinnen an Bedeutung. Dies führt dazu, dass der Anreiz wächst, den CER auch für kriminelle Aktivitäten zu nutzen. Technologische Innovationen und das Ineinanderwachsen der physischen und virtuellen Wirkungsräume schaffen laufend neue Handlungsmöglichkeiten.[95]

Cyberangriffe nachzuverfolgen ist anspruchsvoll. Häufig lassen sie sich nur schwer einem Akteur zuordnen. Dies kann zu Fehlentscheidungen führen; das Risiko einer unkontrollierten Eskalation steigt. Akteure können ihre Identität und Absicht verschleiern oder ihre Handlungen unbeteiligten Dritten zuschreiben. Der tatsächliche Akteur handelt dabei unter falscher Flagge, wobei er typischerweise gezielt von Desinformation Gebrauch macht. Unterschiedliche, teils nicht kooperierende Rechtsordnungen erschweren es zusätzlich, solche Aktionen strafrechtlich zu verfolgen und zu verurteilen.[96] Landesgrenzen spielen im CER praktisch keine Rolle. Die staatliche Souveränität – und damit auch die Rechtsordnung – sind hingegen primär an das nationale Territorium gebunden. Weil sich die IKT-Infrastruktur meistens auf dem Territorium eines Staates befindet,[97] entzieht sich der CER allerdings nicht von vornherein der staatlichen Souveränität. Ausnahmen sind lediglich Infrastrukturen, die in Regionen betrieben werden, die keinem Staat zugeordnet sind (z. B. Mary-Byrd-Land in der Antarktis).

In einem Umfeld diffuser Bedrohungen ist es essenziell, das Bedrohungspotenzial ständig zu analysieren. Anders als herkömmliche Waffensysteme können Cyberwaffen jedoch weder gezählt noch direkt miteinander verglichen werden. Die Qualität moderner Waffensysteme bestimmt ausserdem nicht mehr ausschliesslich die Hardware, sondern zunehmend die Software und damit die Fähigkeit, Rohdaten in verwertbare Informationen umzuwandeln.

---

94 Vgl. Bundesministerium des Innern: Cyber-Sicherheitsstrategie für Deutschland, 2016, https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf [12.04.2020], S. 7.
95 Vgl. Swisscom: Cyber Security Report 2019: Der gezielte Angriff, 2019, https://www.swisscom.ch/content/dam/swisscom/de/about/unternehmen/portraet/netz/sicherheit/documents/security-report-2019.pdf.res/security-report-2019.pdf [14.04.2020], S. 12.
96 Vgl. Gaycken, Sandro/Talbot, David: Aufmarsch im Internet, in: Technology Review, 08.10.2010, https://m.heise.de/tr/artikel/Aufmarsch-im-Internet-1102301.html [12.04.2020],].
97 Vgl. Schulze, Sven-Hendrick: Cyber-»War» – Testfall der Staatenverantwortlichkeit, Tübingen, Deutschland: Mohr Siebeck, 2015, S. 113.

4.3.1 Akteure

Staatliche Akteure

In den meisten Staaten sind Wirkungen im CER primär für die zivilen Nachrichtendienste und die Streitkräfte von Bedeutung. Immer mehr Länder haben Vorgehensweisen entwickelt, mit denen sie ihre Interessen und Absichten auch im CER durchsetzen: Es sind nach wie vor in erster Linie Staaten, die Gesetze und Regularien erlassen, technische Standards festlegen und durchsetzen, Märkte regulieren und sich den Zugang zu den Netzen sichern.[98]

Nachrichtendienste

Viele Nachrichtendienste setzen Cybermittel ein, um Informationen zu beschaffen. Bei lohnenswerten Zielen setzen sie mitunter auf massgeschneiderte und zielgerichtete Aktionen (Advanced Persistent Threats), um dauerhaften Zugriff auf entsprechende Ressourcen zu erhalten. Das Ziel kann sein, strategische Vorteile zu erlangen, politische Ziele zu erreichen oder Technologieentwicklungen zu eigenen Gunsten zu beeinflussen.[99] Für Nachrichtendienste ist entscheidend, möglichst lange unentdeckt zu bleiben, um über einen längeren Zeitraum – etwa mehrere Monate – sensible Informationen auszuspähen oder anderweitig Schaden anzurichten. Dies geschieht in der Regel durch besonders zurückhaltendes und schwer nachvollziehbares Vorgehen. Solche Aktionen sind ressourcenintensiv und setzen erhebliche technische Fähigkeiten voraus.[100]

Mit der globalen Vernetzung werden Standards mehr und mehr vereinheitlicht. Diese Vereinheitlichung führt unter anderem dazu, dass nahezu alle Akteure die gleiche, serienmässig vertriebene Hardware benutzen. Dies eröffnet Nachrichtendiensten neue Möglichkeiten: Sie können kompromittierte (schädliche) Hardware einsetzen, die mit einer sogenannten Hintertüre versehen ist. Solche Hardware lässt sich meistens kaum identifizieren. Sie kann auf eine Art und Weise auf Daten zugreifen, die für die Software auf einem Computersystem unsichtbar ist.[101] Es besteht die Möglichkeit, weltweit genutzte Computerhardware mit kaum auffindbaren Schwachstellen zu versetzen, bei denen Cyberattacken leicht ansetzen können. Dies weckt bei Staaten Begehrlichkeiten, Hardware-Hersteller rechtlich zur Zusammenarbeit zu verpflichten – gerade auch, um solche Schwachstellen einzubauen. Es ist unwahrscheinlich, dass sich ein privatwirtschaftliches Unternehmen gegen seine Regierung stellt. Ein Nachrichtendienst kann Hintertüren auch zur Spionage oder im Krisenfall zur Sabotage nutzen. Cyberbedrohungen sind in der gesamten Lieferantenkette ein Problem.[102]

Streitkräfte

Der CER ist für militärische Operationen mittlerweile ebenso bedeutend wie die übrigen Wirkungsräume. CER-Fähigkeiten sind für Streitkräfte einerseits ein wichtiger Kräfte-Multiplikator, d. h. sie können herkömmliche militärische Fähigkeiten verstärken. Andererseits bilden sie eine unabhängige Handlungsalternative, um eigene Schwächen auszugleichen, weshalb beispielsweise zusätzliche Fähigkeiten zum elektronischen Kampf aufgebaut werden. Durch die zunehmende Digitalisierung und Vernetzung verschwimmen die Grenzen der Wirkungsräume zusehends.[103] Wenn Streitkräfte über offensive CER-Fähigkeiten verfügen, eröffnen sich ihnen zusätzliche militärische Optionen und Handlungsalternativen: Sie können Netzwerke, Computer- und Informa-

---

98 Vgl. Segal, Adam: The Hacked World Order, New York, United States: Public Affairs, 2016, S. 27.
99 Vgl. Swisscom: Cyber Security Report 2019: Der gezielte Angriff, 2019, https://www.swisscom.ch/content/dam/swisscom/de/about/unternehmen/portraet/netz/sicherheit/documents/security-report-2019.pdf.res/security-report-2019.pdf [14.04.2020], S. 17.
100 Vgl. Bundesministerium für Verteidigung: Abschlussbericht Aufbaustab Cyber- und Informationsraum, 2016, http://docs.dpaq.de/11361-abschlussbericht_aufbaustab_cir.pdf [07.04.2020], S. 45.
101 Vgl. Simonite, Tom: NSA's Own Hardware Backdoors May Still Be a "Problem from Hell", in: MIT Technology Review, 08.10.2013, https://www.technologyreview.com/2013/10/08/176195/nsas-own-hardware-backdoors-may-still-be-a-problem-from-hell/ [04.05.2020].
102 Vgl. Mäder, Lukas: Wenn der feindliche Zugang zum Computer gleich mitgeliefert wird, in: NZZ, 18.03.2019, https://www.nzz.ch/schweiz/wenn-der-feindliche-zugang-zum-computer-gleich-mitgeliefert-wird-ld.1467220 [03.05.2020].
103 Vgl. Smeets, Max: The Strategic Promise of Offensive Cyber Operations, in: Strategic Studies Quarterly, Vol. 12, 22.09.2018, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Smeets.pdf [03.05.2020], S. 90.

tionssysteme manipulieren, blockieren, stören, degradieren und zerstören. Aktionen im CER können ausserdem Effekte erzielen, die mit konventionellen Aktionen nicht möglich sind.

International gelten offensive CER-Fähigkeiten den defensiven als überlegen,[104] und zwar sowohl als kampfkraftverstärkender Faktor als auch als unabhängige Fähigkeit. **Es ist davon auszugehen, dass Gross-und Regionalmächte ihre offensiven Kräfte mit sechs- bis zehnmal mehr Finanzmitteln und Personal ausstatten als ihre defensiven Kräfte.**[105] Cyberaktionen sind häufig relativ risikoarme Handlungsalternativen: Die Hemmschwelle ist tiefer, IKT-Infrastrukturen im Cyberraum zu beeinträchtigen, als offene militärische Gewalt anzuwenden, um politische oder militärische Ziele zu erreichen.

Aktionen im CER können auch Schäden im physischen Raum verursachen, insbesondere an kritischen Infrastrukturen. Deren Störung, Ausfall oder Zerstörung kann sich gravierend auf die Gesellschaft, die Wirtschaft und den Staat auswirken. Für Streitkräfte sind insbesondere Cyberaktionen gegen Energie-Infrastrukturen problematisch, weil sie oftmals ebenfalls auf zivile Infrastruktur angewiesen sind, um ihre militärischen Systeme mit Energie zu versorgen.

Aktionen im Informationsraum dienen Streitkräften zur Destabilisierung und Subversion – also zur Unterminierung oder zum Umsturz staatlicher Ordnung. Sie zielen darauf ab, das Vertrauen in Behörden zu untergraben, Beziehungen zu stören, Autoritäten zu diskreditieren und staatliche Strukturen zu schwächen. Dass Informationen kontrolliert oder manipuliert werden, um politische oder militärische Ziele zu erreichen, ist zwar grundsätzlich nichts Neues. Die massive Verbreitung von Informations- und Kommunikationstechnologien hat die Wirkungsweise jedoch massgeblich verstärkt. Mit Aktionen im Informationsraum lässt sich der Einsatz konventioneller militärischer Mittel verringern; allenfalls kann eine offene bewaffnete Intervention überhaupt vermieden werden.[106]

Neben dem Cyberraum ist auch der elektromagnetische Raum für Streitkräfte von grosser Bedeutung. Drahtlose Verbindungen sind das Nervensystem moderner Streitkräfte. Nur wer den elektromagnetischen Raum kontrolliert, kann militärische Mittel erfolgversprechend einsetzen. Denn immer mehr Aufklärungs-, Führungs- und Wirksysteme sind über den elektromagnetischen Raum miteinander vernetzt. Die Kontrolle des elektromagnetischen Raums bildet die Voraussetzung für eine vernetzte Operationsführung in Echtzeit. Verschiedene aufstrebende Staaten wie Russland haben daher ihre Fähigkeiten auf diesem Gebiet in den letzten Jahren erheblich ausgebaut. Dass Konflikte auch im elektromagnetischen Raum ausgetragen werden, wird damit immer wahrscheinlicher.[107]

Neben den herkömmlichen Mitteln des elektronischen Kampfes haben verschiedene Streitkräfte neuartige Hochenergiewaffen oder zumindest deren Prototypen entwickelt. Sie erzeugen elektromagnetische Strahlung und können Ausrüstung, Einrichtungen oder Personal in ihrem Umfeld zeitweise deaktivieren, stören oder ganz zerstören. Wie sich solche Technologien auf heutige (kritische) Infrastruktursysteme auswirken würden und welche Kaskadeneffekte bei einem Einsatz möglich wären, ist derzeit nur wenig erforscht. Unbestritten ist jedoch, dass derartige Aktionen im elektromagneti-

---

104 Vgl. Slayton, Rebecca: What Is the Cyber Offense-Defense Balance? Conceptions, Causes and Assessment, in: International Security, Cambridge, United States; The MIT Press, Band 41, Ausgabe 3, 2017, S. 72–109.
105 Vgl. Ruhmann, Ingo: Aufrüstung im Cyberspace. Staatliche Hacker und zivile IT-Sicherheit im Ungleichgewicht, in: Wissenschaft & Frieden, Dossier 79, Ausgabe 3, 2015, https://wissenschaft-und-frieden.de/seite.php?dossierID=083 [09.04.2020].
106 Vgl. MacKenzie, Paul: Cyberspace and Cyber-Enabled Information Warfare, in: Joint Air Power Competence Centre, 2018, https://www.japcc.org/cyberspace-and-cyber-enabled-information-warfare/ [03.05.2020].
107 Vgl. Schürz, Torben: Der vernetzte Krieg. Warum moderne Streitkräfte von elektronischer Kampfführung abhängen, in: DGAPkompakt 17, 16.10.2015, https://dgap.org/system/files/article_pdfs/2019-17-DGAPkompakt.pdf [08.04.2020].

schen Raum Gesellschaften schwerwiegend und mit ungeahnten Folgen treffen könnten.[108]

Kontraktnehmer

Kontraktnehmer sind private Firmen, die Dienstleistungen in den Bereichen der nationalen Sicherheit, des Militärs und der Nachrichtendienste anbieten. Dabei gibt es auch Dienstleister, die Fähigkeiten staatlicher Auftraggeber im Cyber- und Informationsraum substituieren oder ergänzen. Solche Organisationen verfügen über Kompetenzen, die Staaten nicht oder nicht in genügendem Umfang bereitstellen wollen. Ihre Kompetenzen setzen sie entweder im Rahmen einer vertraglichen Vereinbarung mit dem entsprechenden Staat ein oder sie agieren autonom, aber mit ausdrücklicher Duldung des betreffenden Staats. Kontraktnehmer verfügen über die notwendigen Fähigkeiten, Organisation und Entschlossenheit, um selbst schwierigste Aktionen durchzuführen.

Durch das Zusammenspiel mit Kontraktnehmern verschaffen sich Staaten einen Vorteil; insbesondere jene, die unter rein militärischen Gesichtspunkten unterlegen wären oder mit den beauftragten Aktionen nicht in Verbindung gebracht werden wollen. Indem ein Staat einen Kontraktnehmer beauftragt, verdeckten Aktionen im Cyber- oder Informationsraum durchzuführen, kann er sich vor einer späteren Schuldzuweisung schützen. Unerkannt kann er so seine strategischen und politischen Ziele verfolgen, selbst wenn es zu einer Attribution durch einen anderen Staat kommen sollte. Denn die bezichtigte Regierung kann einfach behaupten, dass es sich um eine kriminelle Aktivität handelt, für die sie nicht verantwortlich ist.

Verschiedene Staaten befürworten die Ratifizierung eines verbindlichen Rechtsrahmens für Aktionen im Cyber- und Informationsraum. Für subversiv operierende Staaten bleibt es hingegen vorteilhaft, auf echte oder nur behauptete rechtliche Unklarheiten zu verweisen oder sogar Bemühungen aktiv zu untergraben, verbindliche Verhaltensnormen festzulegen. Selbst wenn es der internationalen Gemeinschaft gelingen würde, solche Aktionen in Übereinstimmung mit dem Völkerrecht zu kodifizieren und einzuschränken, bestünde mit dem Einsatz von Kontraktnehmern für CER-Aktionen immer noch eine rechtliche Grauzone.[109]

Nichtstaatliche Akteure

Staaten sind zwar im internationalen politischen Geschehen nach wie vor dominant. Wichtiger werden aber auch nichtstaatliche Akteure, die international ebenfalls um Einfluss und Anerkennung ringen. Als Folge des technologischen Fortschritts und der Verbreitung moderner Informations- und Kommunikationstechnologien gewinnen transnationale, nichtstaatliche Netzwerke an Bedeutung. Software mit hohem Schadenpotenzial ist vergleichsweise leicht erhältlich und kostengünstig. Dies führt dazu, dass nicht nur Staaten über wirksame Mittel verfügen, um Aktionen im CER durchzuführen. Auch terroristische Gruppierungen, kriminelle Organisationen und versierte Einzelpersonen können mit geringem Aufwand potenziell erheblichen Schaden anrichten.

Zu den nichtstaatlichen Akteuren, die im CER aktiv sind, gehören Cyberterroristen und -extremisten, Cyberkriminelle, sogenannte «Hacktivisten» und weitere Einzelpersonen.

Cyberterroristen / Cyberextremisten

Bei Terroristen und gewalttätigen Extremisten kann es sich um eine substaatliche Gruppe, ein Netzwerk aus Individuen oder ein einzelnes Individuum handeln. Terro-

---

108 Vgl. Österreichische Akademie der Wissenschaften: Digitaler Stillstand, Die Verletzlichkeit der digital vernetzten Gesellschaft, 2017, http://epub.oeaw.ac.at/0xc1aa5576_0x00358488.pdf [03.03.2020], S. 5–6.
109 Vgl. Sigholm, Johan: Non-State Actors in Cyberspace Operations, in: Journal of Military Studies, Volume 4, 2013.

risten oder Extremisten greifen mit Aktionen im CER unterschiedliche Ziele an, um damit ihre Ideologien zu verbreiten und ihren Einfluss zu erweitern.[110]

Dabei gilt es zwischen Cyberterrorismus und Terrorismus zu unterscheiden: Cyberterrorismus arbeitet einzig mit IKT und operiert nur im CER. Der Terrorismus nimmt die IKT zur Hilfe, um seine Aktionen zu planen, zu unterstützen und zu propagieren, oder um die elektronische Kommunikation zwischen einzelnen Zellen oder dem Führungskader sicherzustellen.

Es wird bisweilen befürchtet, Terroristen und gewalttätige Extremisten könnten umfangreiche Aktionen im CER durchführen, namentlich gegen kritische Infrastrukturen. Eine solche Aktion wäre nicht nur ein grosser propagandistischer Erfolg, sie hätte auch weitreichende Auswirkungen auf die betroffene Volkswirtschaft. Bisher ist allerdings kein Fall bekannt geworden, wo solche Gruppen ihre strategischen Ziele allein durch gezielte Aktionen im CER verfolgt und erreicht hätten. Ebenfalls wurde noch keine Terrororganisation identifiziert, die in der Lage wären, mit gezielten Aktionen im CER signifikanten physischen Schaden anzurichten.[111] Terroristinnen und Terroristen werden die Informations- und Kommunikationstechnologien aber weiterhin dazu nutzen, um sich zu organisieren, Personal zu rekrutieren, Propaganda zu verbreiten, Finanzmittel zu beschaffen, Informationen zu sammeln, Aktionen von Anhängern anzuregen und Operationen zu koordinieren.[112] Selbst wenn der reine Cyberterrorismus bisher ausgeblieben ist, darf diese Form der Bedrohung nicht kategorisch ausgeschlossen werden.

Cyberkriminelle

Streitkräfte können wie jede andere Organisation, die IKT nutzt, zum Ziel von Cyberkriminalität werden. Diese hat sich zu einem lohnenden und boomenden Geschäft entwickelt. Die Bandbreite reicht von einfacher Kleinkriminalität bis hin zu organisierter Cyberkriminalität mit hoher Arbeitsteilung. Die zunehmende Digitalisierung, die alles durchdringende Vernetzung, die explosionsartige steigende Anzahl vernetzter Geräte und die rasante Ausbreitung cloudbasierter Dienste schaffen eine grosse Angriffsfläche.

Das Ziel von Cyberkriminellen ist nicht per se, das Funktionieren von Gesellschaft, Staat oder Wirtschaft zu kompromittieren. Sie nehmen jedoch hohe Kollateralschäden in Kauf, um ihre kriminellen Ziele zu erreichen.[113] Sofern Fälle von Cyberkriminalität überhaupt entdeckt werden, bleibt eine beträchtliche Anzahl ihrer Aktivitäten ungestraft und viele Fälle werden nicht einmal angezeigt. Der Zugang zu elektronischen Beweismitteln ist oftmals schwierig und bei der Zulassung vor Gericht treten häufig Probleme auf. Komplexe Verfahren und rechtliche Herausforderungen in Zusammenhang mit dem grenzüberschreitenden Charakter von Cyberkriminalität ziehen Verfahren häufig in die Länge.[114] Derartige Verzögerungen machen damit einige Länder zu sicheren Zufluchtsorten für Cyberkriminelle.[115]

Hacktivisten

Hacktivisten nutzen Informations- und Kommunikationstechnologien als Protestmittel, um politische oder ideologische Ziele zu erreichen. Typische Aktionen sind das

---

110 Vgl. Post Jerrold; Ruby Keven; Shaw Eric: From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism, in: Terrorism and Political Violence, Volume 12, Issue 2, London, United Kingdom: Taylor & Francis Group, 2000, S. 100.
111 Vgl. Evan, Tamara: Cyber Terrorism Threat Intelligence and Loss Modelling, in: Cambridge Centre for Risk Studies 2018 Risk Summit, 2018, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/180620-slides-evan.pdf, [21.04.2020], S. 5.
112 Vgl. Coats, Daniel: World Wide Threat Assessment of the US Intelligence Community, 13.02.2018, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf [21.04.2020], S. 6.
113 Vgl. Informatiksteuerungsorgan des Bundes ISB: Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022, https://www.isb.admin.ch/dam/isb/de/dokumente/ikt-vorgaben/strategien/ncs/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_DE.pdf.download.pdf/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_DE.pdf [29.04.2020], S. 3–4.
114 Vgl. Europäisches Parlament: Entwurf einer Entschliessung des Europäischen Parlaments zur Bekämpfung der Cyberkriminalität, 25.7.2017, https://www.europarl.europa.eu/doceo/document/A-8-2017-0272_DE.html [27.04.2020], Artikel M.
115 Vgl. Microsoft: Moderne Verhinderung von Cyberkriminalität: Handlungsempfehlungen, https://news.microsoft.com/cloudforgood/_media/downloads/de/modern-cybercrime-prevention-de.pdf [27.04.2020], S. 1.

Verunstalten von Internetseiten, deren Überflutung mit Anfragen oder die Enthüllung vertraulicher Dokumente. Grössere Gruppierungen lancieren auch Kampagnen gegen Terrororganisationen oder gegen Staaten, die sich gegen die Unabhängigkeit des Internets stellen.

Hacktivisten streben in der Regel keine materiellen oder finanziellen Vorteile an. Die Motivation hinter ihren Aktionen ist die Einflussnahme.[116] Die Vorgehensweisen variieren – abhängig von den zur Verfügung stehenden Mitteln, den technologischen Fähigkeiten, dem Zielobjekt und der Motivation. Der dadurch entstandene Schaden wird in Kauf genommen oder sogar gesucht, um eine höhere Aufmerksamkeit zu erlangen. Oft sind Regierungen, Organisationen oder ganze Branchen von Hacktivisten-Aktionen betroffen.[117]

Weitere Einzelpersonen

Weitere Einzelpersonen (z. B. sogenannte Script Kiddies oder Recreational Hackers) sind meist Jugendliche, die trotz mangelnder Grundlagenkenntnisse versuchen, in fremde Computersysteme oder Netzwerke einzudringen oder sonstigen Schaden anzurichten. Ihr Handeln ist primär von Neugier, Experimentierfreudigkeit und Cybervandalismus geprägt. Sie wählen ihre Ziele unspezifisch aus, wobei auch vom Zufall abhängen kann, ob ein System angegriffen wird. Natürlich kommt es auch darauf an, wie gut ein System geschützt ist.

Einzelpersonen nutzen effiziente, gebrauchsfertige Schadsoftware-Baukästen oder automatisierte Angriffswerkzeuge, die im Internet problemlos verfügbar sind. Oftmals kennen sie weder die volle Funktionalität dieser Werkzeuge noch verstehen sie die technischen Zusammenhänge vollständig. Dies macht sie aber nicht weniger gefährlich: Einer der grössten Netzausfälle der Geschichte wurde von unbedachten Einzelpersonen im Oktober 2016 an der Ostküste der USA verursacht. Sie verwandelten eine Unzahl von vernetzten Haushaltgeräten in ein Angriffsnetzwerk und kappten so für Millionen von Haushalten den Zugang ins Internet (sogenannter Distributed Denial of Service Attack, DDoS).[118] Einige sehr anspruchsvolle und raffiniert ausgeführte Cyberangriffe können durchaus von Akteure durchgeführt werden, die dieser Gruppe zuzuordnen sind. Vereinzelt besteht hier ein durchaus ernstzunehmendes Bedrohungspotenzial.

	Staatliche Akteure			**Nichtstaatliche Akteure**			
Wirkungsräume der Akteure	Streitkräfte	Nachrichtendienste	Kontraktnehmer	Cyberterroristen Cyberextremisten	Cyberkriminelle	Hacktivisten	Individuen
Cyberraum	●	●	●	◌	●	●	●
Informationsraum	◐	●	●	◌	◐	●	●
Elektromagnetischer Raum	●	●	◐	◌	◐	◐	◐

● Hauptsächlich in Erscheinung getreten ◐ Teilweise in Erscheinung getreten ◌ Bisher nicht in Erscheinung getreten – Wird nicht erwartet

Abbildung 12: Übersicht Akteure und Wirkungsräume

116 Vgl. Bundesamt für Sicherheit in der Informatik: Cyber-Bedrohungen – ein Einstieg, 09.08.2012, BSI - Bundesamt für Sicherheit in der Informationstechnik [17.04.2020], S. 2.
117 Vgl. Gaycken, Sandro: Einführung Cyberwar: Was ist Cyberwar, 2013, https://www.inf.fu-berlin.de/groups/ag-si/pub/Cyberwar_SB1-5_V160114.pdf [28.04.2020], S. 18.
118 Vgl. Gilbert, David: A bunch of kids probably pulled off the biggest DDoS hack ever, in: Vice News, 04.11.2016, https://www.vice.com/en_us/article/3k58e5/a-bunch-of-kids-probably-pulled-off-the-biggest-ddos-hack-ever [29.04.2020].

4.3.2 Weitere Risiken

Neben gezielten und vorsätzlichen Aktionen können auch menschliches Unvermögen, technische Ausfälle oder Naturereignisse zu Beeinträchtigungen im CER führen. Geschehnisse dieser Art lassen sich letztlich nicht völlig vermeiden; sie kommen regelmässig und in unterschiedlichsten Ausprägungen und Grössenordnungen vor. Dahinter stehen oft nicht gezielte Aktionen, sondern eine Verkettung von unglücklichen Umständen, verbunden mit unzureichenden Schutz- und Vorbereitungsmassnahmen. Die Komplexität hat aufgrund der Vernetzung verschiedenster Bereiche zugenommen. Dies macht es schwierig, die Auswirkungen unbeabsichtigter oder unabwendbarer Ereignisse abzuschätzen und einzugrenzen.[119] Dennoch darf nicht ausser Acht gelassen werden, dass auch scheinbar unglückliche Umstände und Einzelereignisse Bestandteile einer gezielten Aktion sein könnten.

4.3.3 Infrastruktur

Bei CER-relevanten kritischen Infrastrukturen handelt es sich vor allem um Unternehmen der Stromversorgung und Datenübertragung, um Unternehmen in den (globalen) Güterversorgungsketten, aber auch um das nationale und internationale Gesundheitswesen. Bezogen auf den CER wird die Herausforderung am Beispiel der kabelgebundenen, weltweiten Datenübertragung fassbar: Grosse Teile des internationalen Daten- und Kommunikationsverkehrs werden heute über Unterseekabel abgewickelt. Würde ein einziges davon beschädigt, so könnte eine ganze Region während längerer Zeit vom CER abgekoppelt werden. Die Folge wäre eine erhebliche Beeinträchtigung der Wirtschafts- und Sicherheitsinteressen der betroffenen Staaten.[120]

4.3.4 Erkenntnisse

Der Staat trägt dazu bei, die Gesellschaft und Wirtschaft gegen Bedrohungen zu schützen. Im Zeitalter der Digitalisierung wird er dieser Aufgabe nur dann gerecht, wenn er auch im CER ein gewisses Mass an Schutz bieten kann. Dafür muss er in erster Linie seine eigenen Systeme ausreichend schützen können. Das digitale Innovationspotenzial ist riesig, sowohl mit Blick auf neue Anwendungen als auch für mögliche Bedrohungen. Umso wichtiger ist es, dass der Staat auf Basis einer entsprechenden Risikoanalyse mögliche Entwicklungen und neue Lösungsansätze erforscht und diese in politische Konzepte einbindet.[121] In der Schweiz wurde dazu die «Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken» (NCS) erarbeitet[122]. Darin ist die Armee in das nationale Gesamtdispositiv eingebunden.

Neue Bedrohungen müssen frühzeitig erkannt werden; ein wirksamer Schutz erfordert innovative Lösungen. Auch die Armee muss ihren Beitrag an die nationale CER-Sicherheitsarchitektur leisten. Dieser ist in der NCS dargelegt. Zwar wird die Schweiz beim Aufbau entsprechender Fähigkeiten kaum je mit weltweit agierenden Staaten mithalten können. Mit den neuen Handlungsspielräumen im CER, insbesondere in den technischen Bereichen, könnten jedoch auch für die Schweizer Armee neue militärische Möglichkeiten entstehen. Dabei muss die Sicherheit im Zeitalter der Digitalisierung global betrachtet werden. Damit Sicherheit gewährleistet werden kann, müssen die

---

119 Vgl. Informatiksteuerungsorgan des Bundes ISB: Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022, https://www.isb.admin.ch/dam/isb/de/dokumente/ikt-vorgaben/strategien/ncs/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_DE.pdf.download.pdf/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_DE.pdf [29.04.2020], S. 5.

120 Vgl. Patalong, Frank: Untersee-Kabel: Die fragilen Lebensadern des Internets, 02.02.2015, https://www.spiegel.de/netzwelt/web/untersee-kabel-die-fragilen-lebensadern-des-internets-a-1015809.html [29.04.2020].

121 Vgl. Bundesministerium des Innern: Cyber-Sicherheitsstrategie für Deutschland, 2016, https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf [12.04.2020], S. 4.

122 Vgl. Schweizer Bundesrat: Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS), 18.04.2018, https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html [01.09.2020].

nationalen Massnahmen ausgeweitet und gleichzeitig in regionale und internationale Prozesse eingebettet werden.[123]

Die technische und organisatorische Weiterentwicklung der Bedrohungen im CER ist für die Armee eine grosse und langfristige Herausforderung. Sie kann ihre eigene Handlungsfähigkeit schützen, indem sie ihre Resilienz stärkt und langfristige und vorausschauende Sicherheitsvorkehrungen trifft. Eine Voraussetzung dazu ist der Ausbau von CER-Fähigkeiten. Sie schaffen zusätzliche Handlungsoptionen, um Konflikte zu vermeiden und Krisen zu bewältigen.[124] Dabei ist es wesentlich, dass die Mittel so weiterentwickelt werden, dass die Armee ihren Schutz- und Verteidigungsauftrag auch im Zeitalter der Digitalisierung erfüllen und sich selbst wirksam gegen Aktionen im CER schützen kann.

Die Armee steht dabei in einem mehrdimensionalen Spannungsfeld: Sie muss sich bereits heute den Herausforderungen stellen, die aus aktuellen Konflikten und Bedrohungen entstehen. Gleichzeitig verfügt sie jedoch – trotz Fortschritten in den vergangenen Jahren – noch nicht über alle tatsächlich erforderlichen Fähigkeiten. Es gilt, eine Reihe neuer Fähigkeiten aufzubauen. Diese sollen die Armee befähigen, CER-Bedrohungen jeglicher Art umfassend zu antizipieren, abzuwehren und die dazu notwendigen Veränderungen rasch und laufend zu bewältigen. Im Vordergrund steht dabei die Fähigkeit zum Eigenschutz im CER – auch gegen zukünftige Bedrohungen. Ausserdem müssen Fähigkeiten ausgebaut werden, um im Rahmen der Verteidigung auch aktiv im CER wirken zu können.

4.4 Wissens- und Entscheidvorsprung

4.4.1 Grundsätzliches

Für den Erfolg von Armeeeinsätzen ist entscheidend, wie schnell Informationen für die Führung nutzbar gemacht werden können. Wer schneller entscheidet als ein Gegner, beispielsweise wo Verbände oder Waffenwirkungen zum Einsatz gelangen, behält die Überhand. International spricht man in diesem Zusammenhang vom sogenannten OODA-Loop. Es handelt sich dabei um eine Entscheidungsschleife mit dem Ziel, einen Gegner in die Rolle des Reagierenden zu zwingen. Dies wird erreicht, indem die vier Schritte Beobachten (Observe), Beurteilen (Orient), Entscheiden (Decide) und Handeln (Act) möglichst rasch durchlaufen werden.

Konkret geht es darum, gegenüber einem Gegner einen Wissens- und zeitlichen Entscheidvorsprung zu erreichen und zu halten, um mit begrenzten Mitteln die eigenen Ziele durchzusetzen. Ein Wissensvorsprung wird entweder mit dem eigenen Wissensvorsprung oder dem Wissensrückstand des Gegners erreicht. Ein eigener Wissensvorsprung entsteht, wenn Daten aktueller und besser verfügbar sind, wenn ihr Wahrheitsgehalt gewährleistet ist oder wenn sie rasch ausgewertet werden können. Ein gegnerischer Wissensrückstand lässt sich erzielen, indem beispielsweise eigene Mittel getarnt werden, indem der Gegner mit falschen Informationen getäuscht wird oder indem seine Führungssysteme mit Cyberangriffen beeinträchtigt werden.

123 Vgl. Kamasa, Julian: Transparente Sicherheitspolitik notwendig,17.06.2019, https://www.avenir-suisse.ch/transparente-sicherheitspolitik-notwendig [08.04.2020].
124 Vgl. Bundesministerium für Verteidigung: Abschlussbericht Aufbaustab Cyber- und Informationsraum, 2016, http://docs.dpaq.de/11361-abschlussbericht_aufbaustab_cir.pdf [07.04.2020], S. 1–2.

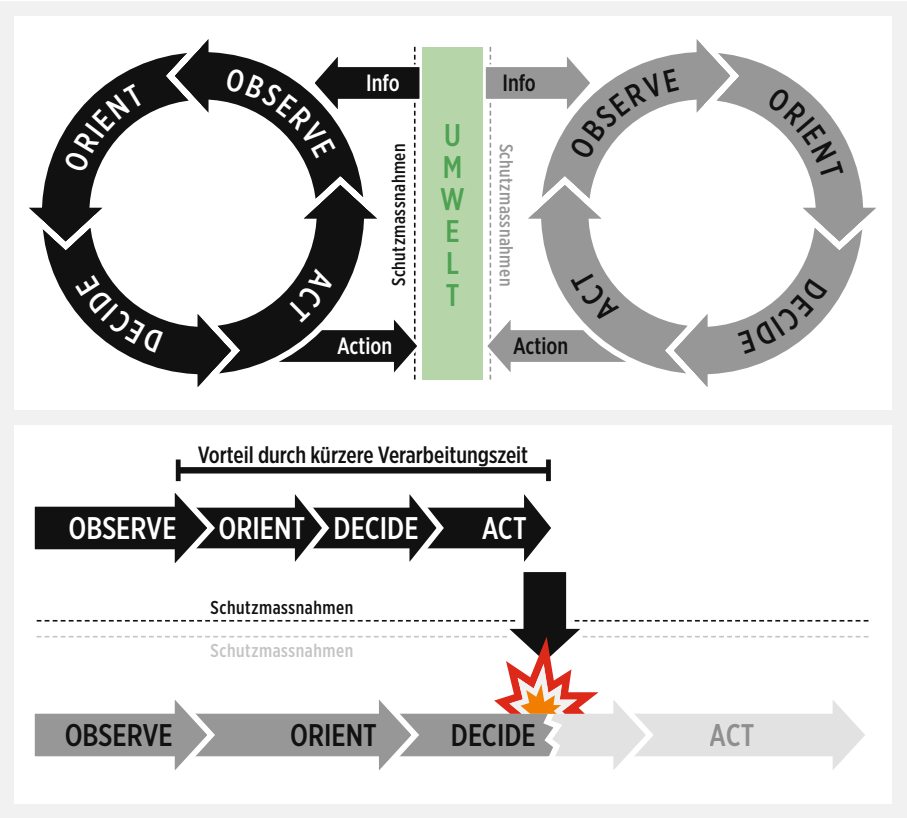


Abbildung 13: Prinzip Wissens- und Entscheidvorsprung

Neben dem Wissensvorsprung streben Streitkräfte auch einen Entscheidvorsprung gegenüber dem Gegner an. Dabei geht es darum, entweder rascher zu handeln als ein Gegner oder den Gegner in seinem Handeln aktiv zu verlangsamen. Diesbezüglich lassen sich zwei Ansätze unterscheiden: ein defensiver und ein offensiver.

Beim defensiven Ansatz geht es darum, die eigenen Systeme, die technische Infrastruktur und die eigenen Informationen jederzeit vor den Einwirkungen des Gegners zu schützen Dies kann in allen Wirkungsräumen erfolgen: EKF-Truppen beispielsweise können die Funkübertragungen zwischen Systemen abschirmen, Cyberspezialistinnen und -spezialisten können den Schutz von IKT-Systemen gewährleisten und die Bodentruppen und die Luftwaffe können ausgewählte (technische) Infrastrukturen vor gegnerischen Einwirkungen schützen. Ziel ist es zu verhindern, dass der Gegner einen Vorsprung erreichen kann.

Ein offensiver Ansatz zielt darauf ab, beim Gegner einen Wissens- und Entscheidrückstand zu verursachen. Auch dazu können verschiedenste Truppen eingesetzt werden: Cyberaktionen wirken in den informationsverarbeitenden Systemen des Gegners gegen Vertraulichkeit, Integrität und Verfügbarkeit von Daten. Aktionen im elektromagnetischen Raum dienen der Nachrichtenbeschaffung und dem Stören von Funksignalen. Mit Angriffe am Boden oder aus der Luft schliesslich können wichtige gegnerische Infrastrukturen oder verlegbare Systemteile ausgeschaltet werden.

4.4.2 Alltag

Im Alltag muss sich die Armee vor allem gegen Akteure mit kriminellen und nachrichtendienstlichen Absichten schützen. Ziel ist es, die Bereitschaft der Armee sicherzustellen. Zudem erfüllt die Armee im CER bei Bedarf subsidiäre Aufträge sowie Aufgaben, die ihr von Gesetzes wegen zugeteilt sind.

Der eigene Cyberraum umfasst die Daten, Informationen und IKT-Systeme der Armee. Er ist mit dem weltweiten Cyberraum verbunden. Eigenschutz im eigenen Cyberraum

bedeutet für die Armee, Cyberangriffe jederzeit zu erkennen und die Angreifer am Erreichen ihrer Ziele zu hindern. Im Cyberraum beschafft die Armee zugunsten der politischen und militärischen Führung Nachrichten über das Ausland, wobei sie die gesetzlichen Vorgaben jederzeit einhalten muss. Im Rahmen der militärischen Cyberabwehr hält sie sich zudem bereit, eigene Aktionen gegen fremde Systeme durchzuführen – dies jeweils mit Bewilligung des Bundesrates.

Die IKT-Systeme der Armee lassen sich mithilfe von Funksystemen standortunabhängig erweitern. Die Armee definiert und verwaltet dazu die Frequenzen, die sie zur Datenübertragung benötigt. In Zusammenarbeit mit den zivilen Instanzen stellt sie die Verfügbarkeit der eigenen Frequenzen sicher. Soweit es die gesetzlichen Vorgaben erlauben, beschaffen Armee und Militärverwaltung Nachrichten im Ausland für die politische, militärstrategische und operative Führung und zugunsten des zivilen Nachrichtendienstes (NDB). Zudem stellt die Armee die Bereitschaft zum elektronischen Kampf sicher.

In Alltag, Spannung und Konflikt verfolgt die Armee permanent die militärische Lage im CER. Zur Ergänzung und bei Vorfällen findet überall, wo dies gesetzlich vorgesehen ist, ein laufender Austausch bzw. eine Koordination mit dem für die Gesamtlage zuständigen NDB sowie mit Partnern statt. Die technischen Mittel müssen fähig sein, Leistungen während mehrerer Wochen oder Monate aus dem Stand zu erbringen.

Um die technologischen Herausforderungen im CER bewältigen und die benötigten Spezialistinnen und Spezialisten rekrutieren zu können, nutzt die Armee das nationale Potenzial in Bildung, Forschung und Wirtschaft. Dazu arbeitet sie mit Schweizer Technologieträgern (z. B. Firmen, Start-ups oder Hochschulen) zusammen, die über Know-how im CER verfügen. Schliesslich nutzt und fördert sie das in der Miliz vorhandene Know-how bereits ab der militärischen Grundausbildung.

Die Armee verfolgt die Technologieentwicklung im CER in vier Bereichen: künftige Entwicklungen, praktische Anwendung neuer Technologien, Weiterentwicklung der genutzten Technologien und Wiederverwendung alter, bewährter Technologien[125]. Der Fokus liegt dabei auf dem Ableiten von praktischen Massnahmen, um Fähigkeiten zu erhalten und weiter auszubauen. Dazu arbeitet die Armee eng mit ihren Partnern im Bund zusammen, insbesondere mit armasuisse.

4.4.3 Spannungen

Es kann sein, dass die Lage im CER bereits als «Spannung» gilt, lange bevor sich die Lage in den übrigen Wirkungsräumen verschärft. Akteure, die hybride Formen der Konfliktführung anwenden, streben danach, möglichst lange unentdeckt zu bleiben und ihre Ziele zu erreichen, ohne offene Gewalt einzusetzen. Cyberangriffe und Aktionen im elektromagnetischen Raum sind dafür ein ideales Mittel, weil sie aus der Distanz wirken und sich nur schwer zuordnen lassen. In einem durch hybride Konfliktführung geprägten Umfeld muss die Armee vor allem den eigenen Wissens- und Entscheidvorsprung behaupten. Zentral ist dabei der Eigenschutz.

Voraussichtlich bereits in dieser Lage stünden die Cybermittel der Armee zu grossen Teilen im Einsatz. Zusammen mit den Mitteln des IKT-Betriebs der Armee würden sie die militärische Cyberabwehr sicherstellen. Dies würde teilweise dezentral erfolgen, damit die Armee den Schutz bei einem Teilausfall der IKT mittels lokalen IKT-Teilsysteme sicherstellen könnte. Um den Eigenschutz zu erhöhen, würden die nicht einsatzrelevanten IKT-Systeme zudem abgekoppelt oder ausser Betrieb genommen.

125 Praktisches Beispiel: Für die sichere, robuste und dauerhafte Speicherung von grossen Datenmengen (vor allem bei Backups) werden heute wieder vermehrt magnetische Bandlaufwerke eingesetzt.

Die eigenen Massnahmen würde die Armee laufend mit Partnern auf Stufe Bund und im Rahmen des SVS koordinieren. Die Armee könnte mit ihren Cyberkräften überdies subsidiäre Unterstützung leisten. Gleichzeitig würde sie Aktionen durchführen, um fremde (virtuelle) Netzwerke im eigenen Cyberraum zu erkennen, in sie einzudringen und Nachrichten über gegnerische Akteure zu beschaffen. Für Aktionen gegen fremde Netzwerke ausserhalb des eigenen Cyberraums benötigt die Armee eine Bewilligung des Bundesrats.

Im elektromagnetischen Raum müssten Angriffswege erkannt und nötigenfalls geschlossen werden. Eigene Frequenzen würden zugeteilt, überwacht und Störungen behoben. Die Bereitschaft der Armee und Systeme würde erhöht, und zwar abhängig vom Vorgehen der gegnerischen Akteure und von der möglichen Lageentwicklung. Ferner ginge es darum, Funkstörungen gegen eigene Systeme (z. B. im Nahbereich eines Flugplatzes) zu erkennen und angemessene Schutz- und Abwehrmassnahmen einzuleiten. Im Inland würde sich die Armee bereithalten, Behörden subsidiär mit Leistungen im elektromagnetischen Raum zu unterstützen – beispielsweise das BAKOM im Frequenzmonitoring.

armasuisse würde die Armee verstärkt mit Expertisen und Fachkräften unterstützen. Sie würde überdies für die Armee bei Bedarf rasch zusätzliche Mittel wie Soft- und Hardware oder spezialisierte Leistungen der Industrie beschaffen. Spezialistinnen und Spezialisten von armasuisse könnten direkt in die Militärverwaltung integriert werden und diese vor Ort unterstützen. Mit Analysen – beispielsweise von neuartigen Angriffswerkzeugen oder elektromagnetischen Übertragungsverfahren – würde sie die Militärverwaltung zusätzlich entlasten.

4.4.4 Konflikt

Auch im Konflikt ginge es für die Armee darum, gegenüber gegnerischen Akteuren einen Wissens- und Entscheidvorsprung zu erlangen und zu behaupten. Dazu müsste sie Mittel aus allen Teilen einsetzen. IKT-Infrastrukturen des Gegners könnten beispielsweise mit geeigneten Mitteln zerstört werden, etwa mit präzisen Angriffen aus der Luft oder mit direkten Aktionen von Spezialkräften. Es müsste damit gerechnet werden, dass nicht direkt involvierte Akteure die Konfliktsituation nutzen, um z. B. ihre kriminellen Ziele zu erreichen. Auch sie könnten im CER weiterhin Druck auf die Armee ausüben oder diesen verstärken. Die Armee würde deshalb den Betrieb aller nicht einsatzrelevanten IKT-Systemen einstellen, um sich besser zu schützen.

Die Cyberkräfte würden zusätzlich dezentrale, offensive Leistungen zur Kampfunterstützung erbringen müssen. Im Vordergrund stünden dabei kombinierte Cyber- und elektromagnetische Aktionen gegen Systeme des Gegners. Zusätzlich könnten mittels Einsatzforensik Nachrichten beschafft werden: Dazu würden aufgefundene oder erbeutete IKT-Geräte (z. B. Smartphones oder Datenträger) vor Ort ausgewertet.

Im Konflikt würden die notwendigen Wirkungen im elektromagnetischen Raum mit dem kombinierten Einsatz aller EKF-Kräfte fortlaufend sichergestellt. Der Fähigkeit der eigenen Aufklärung kommt dabei eine besondere Bedeutung zu. Es ginge darum, diese vor der Wirkung der weitreichenden Waffen zu schützen. Zusätzlich würden Ausweichstandorte für die Einsatzzentralen sowie der Ersatz für zerstörte Sensoren bereitgestellt und im Bedarfsfall eingesetzt.

5

Fähigkeiten

Die Fähigkeiten im Elektromagnetischen und Cyberraum ersetzen nicht diejenigen am Boden oder in der Luft. Sie verstärken und ergänzen diese und machen sie effektiver, aber auch gefährlicher.

Die Schweizer Armee verfügt im Kern schon heute über alle für die Zukunft notwendigen CER-Fähigkeiten, teilweise jedoch nicht auf dem notwendigen Niveau.

5 Fähigkeiten

Dieses Kapitel beschreibt, über welche Fähigkeiten die Armee im CER für den Zeithorizont über 2030 hinaus verfügen muss, um ihren Auftrag langfristig und lageunabhängig erfüllen zu können. Die Fähigkeiten leiten sich von den Umfeld- und Entwicklungstendenzen aus Kapitel 2 und den doktrinellen Überlegungen aus Kapitel 4 ab.

5.1 Grundsätzliche Fähigkeitsanforderungen

Die technische Basis für den eigenen Wissens- und Entscheidvorsprung ist eine moderne, sichere und robuste IKT. Sie schafft überdies die Voraussetzungen für den digitalisierten Führungsverbund der Armee. Diese wichtige Grundlage der Führungsfähigkeit muss die Armee permanent schützen. Damit folgt sie auch einer wichtigen Forderung der NCS und des sicherheitspolitischen Berichts 2021, nämlich dass alle Akteure für ihren eigenen Schutz die Verantwortung tragen und folglich in der Lage sein müssen, sich möglichst selbstständig vor Risiken und gegen Bedrohungen im Cyberraum zu schützen. Um einen Gegner im CER bekämpfen und Nachrichten beschaffen zu können, muss die Armee militärische Handlungen selbstständig planen und durchführen können. Dabei muss es technisch möglich sein, auch Partner flexibel einzubinden. Die Abstimmung von Wirkungen über alle Räume («Multi-Domain») stellt das Kommando Operationen sicher. In Zukunft soll die Armee ihre Fähigkeiten zudem vermehrt auch Partnern innerhalb des Sicherheitsverbunds Schweiz (SVS), anderen Bundesstellen und Behörden, Partnern in Wirtschaft und Gesellschaft sowie Dritten zur Verfügung stellen können, beispielsweise Betreibern von Objekten der kritischen Infrastruktur. Die Unterstützung erfolgt immer auf Gesuch hin und nur, wenn die Mittel der zivilen Behörden ausgeschöpft oder nachweislich nicht vorhanden sind und auch nicht von kommerziellen Leistungserbringern im erforderlichen Umfang und zeitgerecht erbracht werden können (Subsidiaritätsprinzip).

Die Aufgaben sind Teil des übergeordneten Gesamtrahmens, bestehend aus:
— dem rechtlichen Rahmen und der politischen Entscheide[126];
— dem Kooperations-Netzwerk in und ausserhalb der Schweiz für den Informationsaustausch;
— dem Netzwerk der in der Schweiz verfügbaren Kompetenzen[127].

5.2 Herleitung der Fähigkeiten

Aus den grundsätzlichen Fähigkeitsanforderungen ergeben sich drei eigenständige Fähigkeiten: der CER-Eigenschutz, Aktionen im Cyberraum und Aktionen im elektromagnetischen Raum. Der CER-Eigenschutz umfasst alle technischen, betrieblichen, organisatorischen und taktischen Vorkehrungen, um sich vor Bedrohungen zu schützen. Zu den Aktionen im Cyber- und elektromagnetischen Raum gehören sowohl passive als auch aktive Massnahmen. Passive Massnahmen sind beispielsweise die Funkaufklärung, aktive das Eindringen in ein fremdes Computersystem oder die Funkstörung

Drei Bereiche ermöglichen den eigenen Wissens- und Entscheidungsvorsprung: Erstens benötigt die Armee Mittel, um Daten transportieren und verarbeiten zu können. Dies wird durch die IKT-Infrastruktur gewährleistet. Zweitens sind technische und or-

126 Bundesratsentscheide, Befehle, Weisungen, parlamentarische Vorstösse, Empfehlungen der Aufsichtsorgane, Strategien und Auflagen aus dem sicherheitspolitischen Bericht, Nationale Strategie zum Schutz der Schweiz gegen Cyberrisiken und Nationale Strategie zum Schutz der kritischen Infrastrukturen, Aktionsplan Cyberdefence VBS
127 In erster Linie in der Technologie- und Industriebasis, in den Universitäten und Hochschulen, in enger Zusammenarbeit mit der Abteilung Wissenschaft und Technologie von armasuisse.

ganisatorische Massnahmen erforderlich, um über alle Stufen und mit allen Partnern koordiniert führen zu können. An dritter Stelle stehen Massnahmen und Werkzeuge, um aus Daten und Informationen Wissen zu gewinnen und ein gemeinsames Lageverständnis zu ermöglichen (z. B. Software-Anwendungen, technische Hilfsmittel, Methoden der Daten- und Informationsauswertung usw.).

Daraus ergeben sich drei weitere Fähigkeiten im CER, die auch als Fähigkeiten zur Unterstützung der Digitalisierung bezeichnet werden:

— Lageverständnis im Verbund;
— Datenverarbeitung robust und sicher;
— Führung im Verbund organisatorisch und technisch.

Die nachfolgende Tabelle führt alle Fähigkeiten CER mit einer Kurzbeschreibung auf. Sie stellt deren Bezug zu den Handlungsfeldern der Strategie Cyber VBS her.

	CER-Eigenschutz Die Verbände, Systeme, Infrastrukturen, Informationen und Netze im CER vor Einwirkungen eines gegnerischen Akteurs schützen. Betrifft folgende Handlungsfelder der Strategie Cyber VBS: 2, 3, 5, 7b, 8, 9, 10, 12, 15.
	Operationelle Fähigkeiten der Digitalisierung
	Lageverständnis im Verbund Risiken und Bedrohungen im Verbund identifizieren, den Kontext verstehen und Chancen erkennen. Betrifft folgende Handlungsfelder der Strategie Cyber VBS: 3, 5, 7b, 8a, 8b, 9, 16, 18.
	Datenverarbeitung robust und sicher Daten auftragsbezogen und lagegerecht verarbeiten und verteilen. Betrifft folgende Handlungsfelder der Strategie Cyber VBS: 2, 3, 4, 5, 7b, 8a, 8b, 16.
	Führung im Verbund organisatorisch und technisch Die Führung lagegerecht über alle Stufen und Wirkungsräume sowie im Verbund mit Partnern organisatorisch und technisch sicherstellen. Betrifft folgende Handlungsfelder der Strategie Cyber VBS: , 4, 5, 7a, 8a, 8b, 18
	Aktionen im elektromagnetischen Raum Aktionen im elektromagnetischen Raum führen. Betrifft folgende Handlungsfelder der Strategie Cyber VBS: 2, 16.
	Aktionen im Cyberraum Aktionen im Cyberraum führen. Betrifft folgende Handlungsfelder der Strategie Cyber VBS: 8a, 8b, 12, 14, 15, 18.

Tabelle 1: Operationelle Fähigkeiten CER und deren Einbettung in die Cyberdefence-Strategie VBS

5.3 Fähigkeit CER-Eigenschutz

5.3.1 Beschreibung

Der CER-Eigenschutz umfasst alle Fähigkeiten, die es braucht, um armeeeigene Verbände, Systeme, Infrastrukturen, Daten, Informationen und Netze gegen Bedrohungen im CER über alle Lagen zu schützen. Dabei kann es sich um gegnerische Einwirkungen, um technisches oder menschliches Versagen oder um Umwelteinflüsse handeln.

Teil des CER-Eigenschutzes ist das integrale Sicherheitsmanagement. Es umfasst technische, organisatorische und betriebliche Massnahmen, um die IKT zu schützen. Ein wichtiges Element dabei ist das sogenannte IKT-Schwachstellenmanagement. Es dient dazu, allfällige Verwundbarkeiten zu erkennen und vorsorglich zu beheben. Damit Bedrohungen antizipiert werden können, braucht es überdies eine sogenannte Cyber Threat Intelligence und Technological Foresight. Ebenfalls zum CER-Eigenschutz gehört zudem die Bereitschaft, Partner oder Dritte im Rahmen der Subsidiarität zu unterstützen.

Ein weiterer wichtiger Bestandteil des Eigenschutzes ist das Erkennen und Abwehren von Angriffen auf die IKT der Armee. Ist der Angriff abgewehrt, muss der entstandene Schaden festgestellt und das Vorgehen des Angreifers analysiert werden. Zusätzlich werden weitere Informationen beschafft – etwa zu den eingesetzten Software-Tools, den Absichten und den Angriffszielen. Die IKT-Systeme werden anschliessend in den Normalzustand zurückversetzt und die vom Angreifer genutzten Sicherheitslücken dauerhaft geschlossen.

Zahlreiche Sensoren und Waffensysteme der Armee nutzen den elektromagnetischen Raum. Die Handlungsfreiheit im elektromagnetischen Raum ist darum für die Führung und den Waffeneinsatz in anderen Wirkungsräumen (insbesondere am Boden und in der Luft) entscheidend. Entsprechend zentral ist der Eigenschutz. Er beruht im Wesentlichen darauf, gegnerische elektromagnetische Aktivitäten zu erfassen, eigene Truppen zu warnen und Gegenmassnahmen einzuleiten, sofern solche notwendig sind.

Im elektromagnetischen Raum geht es weiter darum, die eigenen Emissionen – also das eigene elektromagnetische Strahlungsbild – zu kontrollieren. Dies erlaubt es, sich der gegnerischen Funkaufklärung zu entziehen oder diese zu täuschen. Weiter gilt es zu verhindern, dass sich eigene Sensoren und Effektoren im elektromagnetischen Raum gegenseitig stören. Das elektromagnetische Strahlungsbild wird dazu mittels taktischer, organisatorischer, technischer oder betrieblicher Massnahmen gesteuert.

5.3.2 Künftige Ausprägung

Künftig muss die Armee den CER-Eigenschutz zentral führen und ganzheitlich über alle CER-Teilbereiche hinweg sicherstellen. Folgende zwei Ausprägungen bilden dazu die Voraussetzung: Der umfassende CER-Eigenschutz und die Antizipation von Bedrohungen und Risiken.

Umfassender CER-Eigenschutz

Den CER-Eigenschutz zu gewährleisten, ist heute aus zwei Gründen schwierig: Zum einen, weil die Armee über sehr viele unterschiedliche Systeme verfügt. Zum anderen, weil die Armee IKT-Systeme betreibt, die nicht permanent mit dem Gesamtnetz verbunden sind. Zudem besteht eine Vielzahl von Inselsystemen. Dies gilt insbesondere auch für Waffensysteme. Die Armee muss also die Fähigkeit aufbauen, künftig alle ihre Systeme zu schützen.

Gegenwärtig legt die Armee den Fokus hauptsächlich auf den zentral sichergestellten Schutz von IKT-Systemen und Netzen, die permanent mit dem Gesamtnetz verbunden sind. Die dafür genutzte Operationszentrale des CER-Eigenschutzes soll künftig mit Ausweichstandorten ergänzt werden. Weiter ist derzeit ein dezentraler Schutz von Systemen und wichtigen Infrastrukturen, wie z. B. ein Armeelogistikcenter, kaum möglich. Diesbezüglich geht es darum, dass die Armee die Fähigkeit erlangt, einen wirkungsvollen Schutz vor Ort (dezentral) sicherzustellen.

Es ist möglich, dass die Armee gleichzeitig mehreren Angriffen im CER ausgesetzt ist. Um diese abwehren zu können, muss die Überwachung der Systeme ausgebaut und die personelle Durchhaltefähigkeit erhöht werden. In der Überwachung geht es vor allem darum, eigenschutzrelevante Ereignisse im CER armeeweit und permanent zu erken-

nen und zu verfolgen. Ausserdem müssen armeeweite Prozesse etabliert werden, die es erlauben, auch Angriffe auf isolierte Waffensysteme zu bewältigen.

Ebenfalls noch nicht durchgängig gesichert ist die Lieferkette (Supply-Chain) für die IKT-Systeme der Armee. Um diese Fähigkeitslücke zu schliessen, müssen die Komponenten über alle zugänglichen Schnittstellen kontrolliert werden können. Dies gilt sowohl für Software als auch für Hardware.

Mit der heute üblichen Verschlüsselung von Kommunikationskanälen kommt der Spionage wieder dort grössere Bedeutung zu, wo die Informationen noch nicht verschlüsselt sind, z. B. in Sitzungszimmern oder Führungsräumen. Zur Informationsbeschaffung werden beispielsweise versteckte Abhörwanzen oder Mikrokameras eingesetzt. Die Fähigkeit der «Lauschabwehr» zum Finden solcher Geräte ist derzeit sehr eingeschränkt; sie muss vor allem personell ausgebaut werden.

Der CER-Eigenschutz erstreckt sich auch in den elektromagnetischen Raum. Dabei ist insbesondere in Rechnung zu stellen, dass verschiedenste Akteure im elektromagnetischen Raum permanent aufklären, und zwar bereits im Alltag. Um sich vor dieser Bedrohung zu schützen, ist es wesentlich, das eigene Strahlungsbild zu kontrollieren. Diese Fähigkeit ist heute kaum etabliert und muss ausgebaut werden. Dazu sind die dafür notwendigen Planungs- und Führungsprozesse zu entwickeln und auszubilden.

Antizipation von Bedrohungen und Risiken

Die Armee muss Bedrohungen und Risiken im CER künftig besser antizipieren, indem sie ihre eigenen gesammelten Daten und Beiträge von Partnern noch schneller und aktiver nutzt. Dazu muss sie in der Lage sein, innerhalb der eigenen (militärischen) Systeme Daten zu gewinnen und diese Daten mithilfe moderner Methoden auszuwerten. Dies erlaubt es, präventive Schutzmassnahmen zeitgerecht anzuordnen.

Es ist absehbar, dass Truppen in einem Einsatz mit digitalen Spuren eines Gegners in Berührung kommen, beispielsweise, wenn sie Datenträger findet. Diese können entscheidende Informationen enthalten und müssen möglichst rasch ausgewertet werden. Dies geschieht am besten direkt auf dem Feld, und zwar unverzüglich und automatisiert. Die Fähigkeit «Forensik im Einsatzraum» ist aktuell nicht vorhanden und soll aufgebaut werden.

5.4 Fähigkeit Lageverständnis im Verbund

5.4.1 Beschreibung

Das Lageverständnis im Verbund ermöglicht auf allen Führungsstufen, den Kontext eines Einsatzes zu verstehen. Es sind dabei Risiken, Gefahren und Bedrohungen zu identifizieren und Chancen zu nutzen. Um mit der steigenden Datenmenge umgehen zu können, braucht es die Automatisierung, Digitalisierung und Anwendung von Data Science. Durch diese Techniken können komplexe Zusammenhänge rascher vertieft analysiert werden. Ziel ist es, ein militärisches Gesamtlagebild und parallel dazu spezifische, bedürfnisorientierte Lagebilder zu erstellen. Dazu müssen Daten und Informationen gewonnen, übertragen und verarbeitet sowie die Informationsaufbereitung und -darstellung automatisiert werden.

5.4.2 Künftige Ausprägung

Ein fusioniertes, aktuelles Lagebild ist eine entscheidende Voraussetzung für den Erfolg im Einsatz. Um dieses Ziel zu erreichen, soll sich die Lagedarstellung einfach den Bedürfnissen des Einsatzes anpassen lassen. Die Daten und Informationen werden mittels Data Science aufbereitet und anschliessend automatisiert stufen- und zeitgerecht in Lagebildern dargestellt. Zentrale Voraussetzungen hierzu sind eine einheitliche Informations- und Datenarchitektur, eine moderne IKT und entsprechendes Fachperso-

nal. Um dies über alle Lagen sicherzustellen, benötigt Data Science besondere IKT-Systeme (High Performance Computing (HPM) Cluster).

In der Armee wurden in den letzten Jahren in einigen spezialisierten Bereichen erste Data-Science-Fähigkeiten aufgebaut, beispielsweise in der Funkaufklärung. Diese Fähigkeiten sind allerdings lediglich für einen spezifischen Einsatzbereich konzipiert und können deshalb nicht für andere genutzt werden. Aufgrund der vielen verschiedenen IKT-Systeme und der bestehenden Vielfalt von Datenformaten sind die Daten nur schwer austauschbar und können mittels Data Science nicht genutzt werden. Es besteht folglich in diesem Bereich eine bedeutende Fähigkeitslücke. Um sie zu schliessen, muss unter anderem eine Datenstrategie erarbeitet werden, die für alle Bereiche der Armee gilt. Sie soll es erlauben, in der gesamten Armee einheitliche Datenformate einzuführen. Zudem müssen die notwendigen IKT-Systeme beschafft und das erforderliche Fachpersonal angestellt werden. Weil die entsprechenden Kosten hoch und die erforderlichen Fachkräfte nur eingeschränkt verfügbar sind, wird sich die Data-Science-Fähigkeit lediglich in ausgewählten Bereichen der Armee aufbauen lassen. Diese Bereiche sollen ihre Leistungen dann den verschiedenen Bedarfsträgern zur Verfügung stellen. Systeme allein genügen indessen nicht: Was es braucht, ist überdies ein Kulturwandel, so dass Daten aus verschiedenen Bereichen der Armee ausgetauscht und gemeinsam genutzt werden können.

Neue und bereits bewährte Techniken zur Lagedarstellung nutzt die Armee, mit Ausnahme der Luftwaffe, noch zu wenig. Komplexe militärische Lagen werden in der Regel zweidimensional auf Bildschirmen oder ähnlichen Mitteln dargestellt. Dies erschwert es, Lagen rasch zu erfassen oder Systeme einfach zu steuern. Entscheidungsträger müssen aber intuitiv, rasch und einfach mit den Systemen interagieren können. Dafür sollen künftig auch Technologien wie Augmented oder Virtual Reality zur Anwendung kommen, um die Schnittstellen zwischen Mensch und System zu verbessern. Diese Lücke muss in den jeweiligen Rüstungsvorhaben geschlossen werden, beispielsweise wenn ein neues Führungssystem beschafft wird.

5.5 Fähigkeit Datenverarbeitung robust und sicher

5.5.1 Beschreibung

Die Fähigkeit zur robusten und sicheren Datenverarbeitung und -verteilung bedingt eine umfassend geschützt und, erweiterbare IKT-Infrastruktur. Dies ist eine der technischen Voraussetzungen zur Digitalisierung der Armee. Die dafür notwendige IKT-Infrastruktur soll so aufgebaut sein, dass sie auch bei Netzunterbrüchen oder Ausfall der Stromversorgung weiterhin funktioniert.

Wesentlich ist, dass die Vertraulichkeit, Integrität und Verfügbarkeit der Daten permanent gewährleistet ist. Dies erfordert, die Schutzmassnahmen laufend zu überprüfen und anzupassen. Die Identifikations- und Authentifizierungsdienste ermöglichen den sicheren technischen Zugriff auf die Daten.

IKT-Systeme zugunsten von Partnern mit besonderen Anforderungen werden hochsicher in isolierten Umgebungen betrieben. Dazu gehören z. B. jene der Nachrichtendienste.

5.5.2 Künftige Ausprägung

Eine Voraussetzung für die Digitalisierung und dadurch für den angestrebten digitalen Führungsverbund bilden das laufende Programm «Fitania» und die IKT-Architektur 4.0. Das laufende Programm Fitania besteht aus drei Komponenten: zusammenhängendes Übertragungsnetz, Rechenzentren und mobiles Kommunikationsnetz der Truppe. Die IKT-Architektur 4.0 definiert die langfristigen, übergeordneten Prinzipien und Standards der IKT in der Armee und in der Zusammenarbeit mit Partnern.

Das zusammenhängende Übertragungsnetz (Führungsnetz Schweiz) ist ein standortgebundenes, fixes Transportnetz. Es funktioniert auf der Basis von Glasfaserkabeln und Richtfunk-Verbindungen. Um seine Verfügbarkeit hoch zu halten, werden verschiedene Verbindungen redundant aufgebaut. Das ausgebaute Netz soll es ermöglichen, Daten zwischen jedem einzelnen Standort verschlüsselt zu transportieren. Durch den Bau von drei neuen Rechenzentren wird die vorhandene Infrastruktur den künftigen Anforderungen der Armee angepasst. Zwei der drei Zentren werden durch erhöhte Sicherheitsmassnahmen besser geschützt sein. Das dritte, mit tieferer Schutzkategorie, können auch zivile Bundesstellen nutzen.

Um Daten über das mobile Kommunikationsnetz der Truppe zu transportieren, braucht es eine geschützte Vernetzung. Dabei wird die zentrale Datenverarbeitung mit autonomen und teilmobilen IKT-Mitteln ergänzt, beispielsweise mit kleinen, transportierbaren Rechenzentren. Die Truppe kann diese Systeme im Einsatzraum flexibel einsetzen. Der Datenfluss ist durch eine Breitband-Anbindung auf allen Führungsstufen sichergestellt. Nach der Umsetzung von Fitania wird eine bedeutende Fähigkeitslücke bestehen bleiben – nämlich die Business Support Services (z. B. E-Mail, Fachanwendungen usw.) für die Truppen und Stäbe der Miliz am Einsatzstandort. Die dafür notwendigen Beschaffungsvorhaben befinden sich in der Initialisierung.

Smart Devices (Smartphones und ähnliches) sind in der Gesellschaft weit verbreitet. Dies bietet die Chance, IKT-Services der Armee kostengünstig vielen Armeeangehörigen zur Verfügung zu stellen, etwa mithilfe von Apps. Wenn es die Lage erlaubt, sollen künftig zivile und militärische Telekommunikationsnetze kombiniert für die Datenübertragung genutzt werden können. Damit wird die Armee in der militärischen Datenübertragung flexibler. Gleichzeitig können zivile Mittel natürlich auch neue Sicherheitsherausforderungen mit sich bringen, die bereits bei der Konzeption solcher Lösungen berücksichtigt werden müssen.

5.6 Fähigkeit Führung im Verbund organisatorisch und technisch

5.6.1 Beschreibung

Diese Fähigkeit zur Führung im Verbund stellt sicher, dass die verschiedenen Führungsstufen und Partner lagegerecht über die notwendigen Führungsinformationen verfügen, und zwar zur richtigen Zeit und im richtigen Detaillierungsgrad. Dazu braucht es organisatorische Massnahmen und technische Schnittstellen. Verschiedener Stäbe müssen beispielsweise inhaltlich und zeitlich koordiniert zusammenarbeiten und Systeme von Partnern müssen Daten austauschen können. Die Fähigkeit zur Führung im Verbund ermöglicht es, die Führungstätigkeiten zu koordinieren und das Vorgehen über alle Führungsstufen hinweg und mit Partnern abzustimmen.

Unentbehrlich ist dabei ein reibungsloser Informations- und Lageaustausch. Er erfolgt auf unterschiedlichen Stufen, mit unterschiedlichen Partnern und ist zeitlich flexibel. Die Fähigkeit, die dazu erforderlichen Informationen nach Möglichkeit automatisiert zu teilen, ist für die Auftragserfüllung und Koordination elementar.

5.6.2 Künftige Ausprägung

Die Digitalisierung führt zu einer starken Zunahme an Daten. Im digitalen Führungsverbund müssen diese Daten geteilt bzw. von einem System zum anderen übermittelt werden. Die daraus entstehenden, sehr variablen Datenflüsse fordern künftig ein wirkungsvolles Informations- und Datenmanagement. Diesbezüglich geht es darum, die Datenflüsse zwischen allen Berechtigten sicherzustellen – über alle Organisationen, Führungsstufen und Systeme hinweg.

Die Armee verfügt heute über Führungsinformationssysteme, die in der Regel sogenannte Silosysteme sind. Informationen fliessen nicht durchgängig; vielmehr gibt es

Brüche, die den Informationsaustausch umständlich, zeitraubend und fehleranfällig machen. Teilweise werden Daten von Hand aus einem System in ein anderes übertragen. Dies ist auch unter dem Aspekt der Sicherheit problematisch. Für die Armee geht es darum, die vorhandenen Silosysteme ausser Dienst zu stellen und mit neuen, modernen Lösungen zu ersetzen. Diese müssen den digitalen Führungsverbund ermöglichen. Dafür sind die technischen Voraussetzungen und rechtlichen Grundlagen zu schaffen sowie die notwendigen Funktionsträgerinnen und Funktionsträger in den Organisationen auszubilden.

5.7 Fähigkeit Aktionen im elektromagnetischen Raum

5.7.1 Beschreibung

Aktionen im elektromagnetischen Raum dienen dazu, die gegnerische Funkübertragung zu stören oder die Nutzung des Raumes durch den Gegner überhaupt zu unterbinden. Ziel ist nicht zuletzt, den gegnerischen Wissens- und Entscheidvorsprung zu beeinträchtigen. Die Fähigkeit umfasst aktive und passive Massnahmen. Passive Massnahmen sind beispielsweise die Funkstörung gegen Kommunikation, Ortung und Lenkung, passive die Funkaufklärung, Radarwarner oder Beiträge zur Luftlagedarstellung. Ausserdem werden alle Tätigkeiten dazugezählt, die nötig sind, um die Einsatzbereitschaft sicherzustellen und die eigene Handlungsfreiheit bereits im Alltag zu erhöhen, etwa indem unbekannte elektromagnetische Signale analysiert werden.

5.7.2 Künftige Ausprägung

Mit Aktionen im elektromagnetischen Raum kann die Armee auf die technischen Führungsfähigkeiten eines Gegners einwirken, ohne dabei physische Schäden oder gar Zerstörungen hervorzurufen und ohne Menschenleben zu gefährden. Dies gibt der Truppe unter anderem die Möglichkeit, den Gegner in seiner Führung einzuschränken, während sie Aktionen am Boden gegen ihn durchführt. Die Mittel für Aktionen im elektromagnetischen Raum ergänzen, unterstützen und verstärken die Gefechtsleistung eines Kampfverbandes damit deutlich. Weil diese Mittel auf Distanz wirken, wird die eigene Truppe zudem einem wesentlich geringerem Risiko ausgesetzt als bei einem konventionellen Waffeneinsatz. Mit den Mitteln für Aktionen im elektromagnetischen Raum wird die Truppe auch in die Lage versetzt, durch Funkstörung das Auslösen von Sprengsätzen des Gegners über Funk zu verhindern. Sie verfügt damit über ein weiteres Mittel zum Eigenschutz im Einsatzraum. Insgesamt erhält die Truppe mit diesen Mitteln zusätzliche Möglichkeiten, um völkerrechtskonforme und verhältnismässige Aktionen durchzuführen – im Alltag, in der Spannung und im Konflikt. Dies ist umso wichtiger, als dass militärische Einsätze immer häufiger in einem allenfalls dicht besiedelten Umfeld stattfinden.

Die Fähigkeit, Aktionen im elektromagnetischen Raum durchzuführen, ist heute primär auf die Abwehr eines bewaffneten Angriffs ausgerichtet. Die Armee ist gegenwärtig in der Lage, taktische Funksysteme aufzuklären, zu stören und zu beeinträchtigen. Dazu verfügt sie über verschiedene Grosssysteme, die ursprünglich mit Blick auf ein herkömmliches Konfliktbild konzipiert wurden. Sie sind so ausgestaltet, dass sie sich für Einsätze in überbautem Gelände und in einem hybriden Konfliktumfeld nicht gut eignen. Die bestehenden ortsfesten Sensoren würden in einem Konflikt voraussichtlich schon früh zerstört, da ihre Standorte bekannt sein dürften. Sie sind folglich ein leichtes Ziel für Abstandswaffen.

Die Armee muss ihre künftigen Mittel nicht nur auf die zentralisierte Abwehr herkömmlich agierender militärischer Kräfte ausgelegen, sondern auch auf Einsätze gegen neuartige Ziele in einem hybriden Konfliktumfeld. In Ergänzung zu den auch in Zukunft notwendigen Grosssystemen sind leichte und einfach einsetzbare Systeme für die Bodentruppen erforderlich. Weil international ständig neue Gegenmassnahmen entwickelt werden, muss die Armee zudem ihre Fähigkeiten zu Aktionen im elektromag-

netischen Raum schnell anpassen können. Weiter sind auch Mittel zur Führung des elektronischen Kampfes zu beschaffen, die im Radarfrequenzbereich wirken können. Die Kerninfrastrukturen der Funkaufklärung, wie z. B. die Infrastruktur der zentralen Auswertung, müssen zudem redundant ausgebaut werden.

Die Armee muss in Zukunft auch über Passivradare verfügen. Dies sind Radare, die Objekte erfassen können, selbst aber keine eigenen Signale aussenden. Die heutigen Radarsysteme senden starke elektromagnetische Signale aus. Sie können dadurch einfach geortet und mit Abstandswaffen zerstört werden. Ein Passivradar nutzt primär vorhandene, nicht selbst erzeugte Rundfunksignale (z. B. FM, DAB, DVB-T). Dadurch ist es beinahe unmöglich, ein Passivradar zu orten, um es anschliessend zu zerstören. Neben dem Passivradar soll auch die Technologie des bistatischen Radars vertieft untersucht werden. Es handelt sich dabei um ein Radarsystem, das auf einer örtlichen Trennung von Sender und Empfänger basiert.

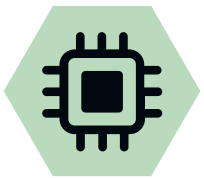
Eine weitere Fähigkeitslücke besteht in der Aufklärung von Kurzwellenfunksystemen. Solche Systeme werden genutzt, um Einsätze über grosse Distanzen zu führen, etwa solche von Spezialkräften. Sie werden in der Regel für die Aufklärung in der Schweiz und im nahen Ausland eingesetzt. Die heutigen Sensoren der Armee sind dafür ungeeignet.

Die Bedrohung durch selbstständig agierende Systeme und ferngesteuerte Drohnen hat zugenommen. Der Armee fehlt im elektromagnetischen Raum heute die Fähigkeit, sich gegen diese Bedrohungsarten zu behaupten. Diese muss neu aufgebaut werden.

Zurzeit stehen in der Armee keine Hochenergiewaffen im Einsatz, die elektromagnetische Strahlung als Waffen nutzen. Ob die Armee die Fähigkeit aufbauen soll, solche Waffen einzusetzen, muss grundsätzlich geklärt werden. Die direkte oder indirekte Waffenwirkung lässt sich je nach Frequenz und Abstrahlungsmethode nur beschränkt kontrollieren. Ein Einsatz solcher Waffen in einem dicht besiedelten Umfeld kann deshalb zu weitreichenden Kollateralschäden führen. Darum muss die Armee auch aus völkerrechtlicher Sicht beurteilen, welche dieser Waffensysteme mit welcher Ausprägung für sie infrage kommen könnten. In diesem Zusammenhang stellt sich auch die Frage nach möglichen Schutzkonzepten für Mensch und Systeme im Rahmen der Fähigkeit zum Eigenschutz.

5.8 Fähigkeit Aktionen im Cyberraum

5.8.1 Beschreibung



Mit Aktionen im Cyberraum kann ein gegnerischer Akteur daran gehindert werden, einen Wissens- und Entscheidvorsprung zu erlangen. Überdies lässt sich das Funktionieren seiner Waffensysteme beeinträchtigen oder gänzlich verhindern. Voraussetzung ist, dass Sicherheitslücken und Zugangsmöglichkeiten bekannt und spezifische Werkzeuge vorhanden sind, um die beabsichtigten Effekte in diesen Systemen zu erzeugen. Fähigkeiten zu Aktionen im Cyberraum können auch dazu dienen, Massnahmen in den eigenen IKT-Systemen umzusetzen, um Ziele und Absichten von eingedrungenen gegnerischen Akteuren zu erkennen. Aktionen im Cyberraum und im elektromagnetischen Raum lassen sich technisch kombinieren. Die damit gewonnenen Synergien führen zu neuen Möglichkeiten, um gegnerische Systeme wirkungsvoll zu bekämpfen.

5.8.2 Künftige Ausprägung

Heute sind die Fähigkeiten für Aktionen im Cyberraum vor allem nachrichtendienstlich ausgerichtet. Aktionen gegen militärische Ziele standen bisher eher im Hintergrund und müssen künftig verstärkt vorbereitet werden. Um Aktionen im Cyberraum führen zu können, muss sich die Armee rasch und eigenständig den Bedürfnissen der Leistungsbezüger, den Schutzmassnahmen in den Zielsystemen und neuen Technolo-

gien anpassen können. Dazu gehört die Fähigkeit, selbstständig Werkzeuge zu entwickeln und zielorientiert einzusetzen. Zudem sind spezialisierte Cyberteams zur Unterstützung der Bodentruppen oder der Luftwaffe erforderlich. Die Einsatzunterstützung dieser Verbände mit Aktionen im Cyberraum muss in das hybride und urbane Umfeld integriert werden können.

Eine Fähigkeitslücke besteht bei der Aufklärung und Wirkung gegen militärische Systeme. Hierbei geht es unter anderem darum, Aufbau, Funktionsweise und Schwachstellen z. B. militärischer Waffensysteme aufzuklären und diese in ihrer Funktion einzuschränken oder gar unbrauchbar zu machen. Bei Systemen mit einer funkbasierten Datenverbindung oder Anbindung an ein Netzwerk kann das Eindringen in die Systeme allenfalls über diese Verbindung erfolgen. Unter Umständen ist der direkte Zugang zu einem Zielsystem am Einsatzstandort notwendig, was in der Regel die Zusammenarbeit mit geeigneten Truppen (z. B. Spezialkräften) bedingt.

Aktionen im Cyberraum, mit denen sich militärische Systeme eines Gegners aufklären oder beinträchtigen lassen, führen zu einer deutlichen Verbreiterung des Fähigkeitsspektrums der Armee. Sie erlauben es künftig, Waffen- oder Führungssysteme auf weite Distanz zielgenau ausser Funktion zu setzen und Informationen zu beschaffen. Gleichzeitig können Kollateralschäden vermieden werden, und zwar sowohl an Menschen als auch an Infrastrukturen. Im kombinierten Einsatz mit Aktionen am Boden oder in der Luft, ergänzen, unterstützen und verstärken die Aktionen im Cyberraum die Wirkungen der Bodentruppen oder der Luftwaffe wesentlich. Je nachdem, welche Werkzeuge zur Anwendung gelangen, lassen sich sogar reversible Effekte erzeugen, etwa indem eine Verschlüsselungssoftware (Ransomware) eingesetzt wird. Solche Werkzeuge ermöglichen es, die entsprechenden Daten einfach wiederherzustellen, nachdem das militärische Einsatzziel erreicht ist. Wie bei Aktionen im elektromagnetischen Raum wirken solche Mittel überdies auf Distanz. Das Risiko für die eigene Truppe ist deshalb geringer, als wenn sie die militärischen Ziele mit konventionellen Waffen bekämpfen würde. Weil – anders als bei einem Waffeneinsatz – keine Kollateralschäden entstehen, eignen sich Cybermittel besonders gut für verhältnismässige Einsätze in überbauten und besiedelten Gebieten, wie sie für das Schweizer Mittelland charakteristisch sind.

Um die Ziele in einem Einsatz zu erreichen, kann es notwendig sein, Aktionen im Cyber- und elektromagnetischen Raum kombiniert durchzuführen. Aktionen im Cyberraum können beispielsweise den Zugang zu Systemen erfordern, die ausschliesslich über Funk kommunizieren. In diesem Fall wird die Funkverbindung genutzt, um mit einem Cyberangriff in das Zielsystem einzudringen.

Diese kombinierten Aktionen müssen in der Regel mit viel Aufwand für jedes Ziel einzeln konzipiert werden. Technische Lösungen, die dabei erarbeitet werden, lassen sich später häufig nicht ohne Anpassungen für andere Einsätze verwenden. Solche Aktionen werden durch Teams konzipiert, die sich aus besonders geschulten Spezialistinnen und Spezialisten aus den Bereichen Kryptologie, Cyberaktionen und elektronischer Kampf zusammensetzen. Meistens werden diese Teams mit Spezialistinnen und Spezialisten aus anderen Teilen der Armee ergänzt, beispielsweise aus den Spezialkräften oder aus der Luftwaffe. Solche Einsätze erfordern eine umfassende Vorbereitung und Einsatzsysteme mit einem hohen Automatisierungsgrad.

5.9 Handlungsbedarf

CER-Eigenschutz

Im Zentrum der angestrebten Weiterentwicklung muss der Ausbau des CER-Eigenschutzes stehen. Ziel ist es, auch temporär vernetzte Systeme und wichtige Infrastrukturen dezentral schützen zu können, die Sicherheit in der Supply Chain zu gewährleisten und die Fähigkeit zur Antizipation von Bedrohungen auszubauen. Zudem soll die

Resilienz der Operationszentralen CER-Eigenschutz verbessert werden. Weiter muss die personelle Durchhaltefähigkeit so weit ausgebaut werden, dass die Armee gleichzeitig mehrere Angriffe aus dem CER bewältigen kann.

Fähigkeiten zur Unterstützung der Digitalisierung

Mit Blick auf das Lageverständnis im Verbund müssen Fähigkeiten insbesondere im Bereich der Data Science, der Automatisation und der Lagedarstellung erweitert werden. Es ist absehbar, dass moderne technische Lösungen die Interaktion zwischen Mensch und System künftig vereinfachen. Mit Blick auf die Zusammenarbeit mit Partnern sollen die notwendigen rechtlichen und technischen Voraussetzungen geschaffen bzw. – wo sie bereits bestehen – ausgebaut werden.

Damit die Daten auch bei der Truppe im Einsatz resilient verarbeitet werden können, muss die dafür notwendige (verlegbare) Digitalisierungsinfrastruktur beschafft werden. Darüber hinaus müssen künftig gemeinsame Standards festgelegt und durchgesetzt werden. Generell gilt es, eine IKT-Führung zu etablieren, die stärker auf die Einsatzbedürfnisse der Armee ausgerichtet ist.

Um die notwendigen technischen und organisatorischen Voraussetzungen für eine digitalisierte Führung im Verbund zu schaffen, ist es nötig, künftige Führungssysteme so auszugestalten, dass ein durchgängiger Datenfluss möglich ist.

Aktionen im Cyber- und elektromagnetischen Raum

Für Aktionen im Cyber- und im elektromagnetischen Raum muss in jedem Fall die Fähigkeit ausgebaut werden, künftige Entwicklungen (kombiniert mit Kryptologie) zu antizipieren. Dies gilt insbesondere für die Antizipation der Technologieentwicklung und der Bedrohung. Gleichzeitig bedingt dies eine deutliche Stärkung der Fähigkeit, neue technologische Möglichkeiten in die bestehende Systemlandschaft zu implementieren. Zudem soll die Fähigkeit gestärkt werden, technische Gegenmassnahmen (Reaktionen) auf die eigenen Aktionen zu erkennen, zu analysieren und zu kompensieren.

6

Weiterentwicklung und Umsetzung

Die Optionen zur Weiterentwicklung der Schweizer Armee im CER müssen sich in das Gesamtsystem einbetten. Sie berücksichtigen die anstehenden Fähigkeitsentwicklungen in den anderen Wirkungsräumen und verstärken bzw. ergänzen diese. Dabei ist zu betonen, dass insbesondere der Fähigkeitsausbau im Cyberraum nicht primär durch neue Systeme, sondern durch eine höhere Anzahl von Fachspezialisten sichergestellt werden kann.

6 Weiterentwicklung und Umsetzung

Massnahmen lassen sich nur dann kohärent planen und umsetzen, wenn eine klare Zielvorstellungen darüber besteht, in welche Richtung die einzelnen Fähigkeiten – aufeinander abgestimmt – weiterentwickelt werden sollen. Der Ausbau von CER-Fähigkeiten muss dabei stets mit der Weiterentwicklung des Gesamtsystems Armee in Einklang stehen. Die nachfolgend beschriebenen Optionen berücksichtigen, wie die Fähigkeiten in den anderen Wirkungsräumen weiterentwickelt und wie die entsprechenden Mittel erneuert werden.

6.1 Rahmen und Eckwerte der Optionsentwicklung

Bei allen Entwicklungsoptionen sind die personellen, finanziellen, rechtlichen und technologischen Rahmenbedingungen gebührend in Rechnung zu stellen. Ein wichtiger Eckwert sind überdies die laufenden CER-relevanten IKT-Vorhaben und Projekte (z. B. Fitania).

Auch wenn die Rahmenbedingungen in den nächsten Jahren herausfordernder werden, ergibt sich ein gewisser Spielraum für neue Optionen. Durch technologische Lösungen, insbesondere durch die Automatisation, können beispielsweise auch nichtspezialisierte Truppenteile für Tätigkeiten im CER ausgebildet werden. Indem die Armee auf den Betrieb ihrer eigenen militärischen IKT fokussiert, lassen sich bestehende Funktionen in der Militärverwaltung auf neue Aufgaben im CER ausrichten. Dabei ist zu berücksichtigen, dass Cyberwirkungen nicht primär auf teuren militärischen Systemen basieren. Sie sind vielmehr vor allem davon abhängig, wie viele Spezialistinnen und Spezialisten zur Verfügung stehen und welches Wissen sie mitbringen.

Bei der Weiterentwicklung der Fähigkeiten ist in Rechnung zu stellen, dass in Teilen des CER gegenwärtig ein spannungsähnlicher Zustand herrscht. Das heisst, dass schon heute Cyberangriffe zu bewältigen oder Massnahmen gegen Funkaufklärung fremder Akteure umzusetzen sind. Deshalb müssen sich die Optionen auch an akuten und real bestehenden Bedrohungen ausrichten.

6.2 In allen Optionen umzusetzende Massnahmen

Verschiedene Massnahmen müssen unabhängig von der Optionenwahl umgesetzt werden. Geschieht dies nicht, so wäre die zukünftige Auftragserfüllung der Armee grundlegend gefährdet. Handlungsbedarf besteht insbesondere beim CER-Eigenschutz, im Bereich der Digitalisierung und bei den Fähigkeiten für Aktionen im Cyber- und elektromagnetischen Raum.

CER-Eigenschutz

Beim CER-Eigenschutz geht es in allen Optionen darum, in den kommenden Jahren die Voraussetzungen für eine umfassende und armeeweite Überwachung der eigenen IKT-Mittel zu schaffen. Dies betrifft sowohl einzelne Elemente (z. B. Waffensysteme mit IKT-Anteil) als auch ganze Teilbereiche (z. B. elektromagnetisches Spektrum). Der zentrale Teil der Infrastruktur (Operationszentralen) muss künftig über Ersatzstandorte verfügen.

Um den CER-Eigenschutz zu verbessern, ist es ferner erforderlich, die Fähigkeiten zum Lageverständnis und zur Antizipation künftiger Entwicklungen und Bedrohungen auszubauen. Ebenfalls zur Verstärkung des CER-Eigenschutzes muss die Fähigkeit zur Lauschabwehr ausgebaut werden – primär auf personeller Ebene. Falls Teile der IKT vom Gesamtnetz abgetrennt werden, braucht es dezentrale Schutzleistungen. Die armee-

weite Fähigkeit, das eigene Strahlungsbild im elektromagnetischen Raum zu kontrollieren, muss komplett neu aufgebaut werden. Auch die heute noch fehlende Supply Chain Security muss die Armee von Grund auf neu entwickeln. Damit diese Aufgaben rund um die Uhr erfüllt werden können, braucht es Anpassungen in der Berufsorganisation.

Fähigkeiten zur Unterstützung der Digitalisierung

Ein integrales Lageverständnis entsteht, wenn Lageinformationen aus allen Wirkungsräumen und Funktionsbereichen der Armee und von Partnern zusammengetragen und fusioniert werden. Eine zentrale Voraussetzung dazu ist, dass sich die dafür notwendigen Daten automatisiert aufbereiten und darstellen lassen. Zudem braucht es die Fähigkeit, Informationsflüsse auftrags- und lagebezogen zu planen und zu führen, dies mit Unterstützung von Technologien aus dem Bereich der Data Science. Die bereits bestehenden Fähigkeiten bezüglich Data Science werden in Zusammenarbeit mit dem Kompetenzzentrum Data Science des Bundesamtes für Statistik weiter ausgebaut. In einem ersten Schritt soll die Anzahl der Fachspezialistinnen und Fachspezialisten erhöht werden. Danach wird die bestehende IKT-Infrastruktur für Data Science basierend auf Fitania gegen Ende der 2020er-Jahre erweitert.

Das Programm Fitania bildet die technische Grundlage für eine robuste und sichere Datenverarbeitung und somit auch für den digitalen Führungsverbund der Armee. Des Weiteren muss die Truppe befähigt werden, allenfalls verfügbare zivile Übertragungsmöglichkeiten als Redundanz zu den militärischen zu nutzen. Um die Führungs- und Zusammenarbeitsfähigkeit der Truppe im Einsatz robust sicherzustellen, muss die Truppe zudem über lokale, vernetzungsfähige und standardisierte IKT-Plattformen mit Arbeitsplatzgeräten verfügen. Dadurch wird die Vielfalt von Plattformen im digitalen Führungsverbund weiter reduziert und der Betrieb vereinfacht.

Auf dem Verbund dieser Plattformen nutzen die Stäbe der Truppen die IKT-Services für die Führung, das Datenmanagement und für weitere Aufgaben. Zudem wird auch die Möglichkeit geschaffen, Einsatzsysteme und Partner anzubinden.

Zusätzlich müssen künftige IKT-Mittel und Applikationen für die militärische Führung so ausgelegt werden, dass sich Daten einfach austauschen lassen. Dies schafft eine weitere Voraussetzung für eine digitalisierte Führung im Verbund. Dabei muss die Prozess-, Informationsfluss- und Systemintegration organisatorisch und technisch sichergestellt werden.

Der digitale Führungsverbund wird laufend ausgebaut, indem Sensor-, Führungs- und Waffensysteme integriert werden. Für den Verbund mit internen und externen Partnern müssen die Zusammenarbeitsform und die dazugehörigen Schnittstellen definiert werden. Zusätzlich braucht es für diese Zusammenarbeit ein organisationsübergreifendes Regelsystem (Governance).

Aktionen im Cyber- und elektromagnetischen Raum

Für Aktionen im Cyber- und im elektromagnetischen Raum benötigt die Armee die Fähigkeit, zukünftige technologische Entwicklungen[128] und Bedrohungen zu antizipieren, und zwar unter Einbezug kryptologischer Fähigkeiten. Nur so können neue Bedürfnisse der Armee und des NDB rasch umgesetzt werden. Gleichzeitig wird damit die Fähigkeit verstärkt, neue technologische Möglichkeiten zu implementieren, und Gegenmassnahmen auszugleichen. Die dazu notwendige, spezialisierte IKT-Infrastruktur ist Teil der Data-Science-Infrastruktur. Weiter ausgebaut werden soll überdies die Fähigkeit zum Einsatz verlegbarer und luftgestützter Sensoren. Die Infrastruktur für die strategische Funkaufklärung soll in wichtigen Bereichen redundant ausgebaut werden. Schliesslich gilt es, Fähigkeiten zur elektronischen Kriegführung zugunsten des Luftraums zu

128 Das Monitoring der Technologieentwicklung erfolgt zusammen mit Partnern innerhalb des VBS.

erhalten und in Anlehnung an die Beschaffungen weiterzuentwickeln, wie sie im Rahmen des Programms Air2030 vorgesehen sind.

Die im folgenden beschriebenen Optionen legen qualitativ und quantitativ unterschiedliche Schwergewichte bei den Fähigkeiten im Cyberraum einerseits und bei jenen im elektromagnetischen Raum andererseits. Sie zeigen also auf, wie sich die CER-Fähigkeiten in welcher Tiefe und Breite weiterentwickeln lassen.

6.3 Option 1

Mit der Option 1 würde die Armee im Vergleich zu heute insbesondere den Eigenschutz im Cyber- und elektromagnetischen Raum stärken. Dieser Eigenschutz würde grundsätzlich zentral gewährleistet, wofür die erforderlichen, qualitativ hochstehenden Fähigkeiten – wie heute – in einem spezialisierten Bataillon auf Stufe Armee zusammengefasst werden. Darüber hinaus wäre auch ein punktueller, dezentraler Schutz bis auf Stufe Bataillone und Kompanien möglich. Dazu könnten den Kampfverbänden der Armee (oder bei Bedarf zivilen Partnern) bedarfsgerecht Mittel aus dem spezialisierten Bataillon zugewiesen oder unterstellt werden. Nach der Umsetzung dieser Option würden sie über die Fähigkeit verfügen, mehrere Aktionen gegen militärische Ziele gleichzeitig und vollständig zu entwickeln und durchzuführen. Die Truppen für militärische Einsätze im Cyber- und im elektromagnetischen Raum sowie für den dezentralen Eigenschutz wären auf Stufe Armee in spezialisierten Bataillonen zusammengefasst – analog den bestehenden EKF-Abteilungen und dem Cyber-Bataillon.

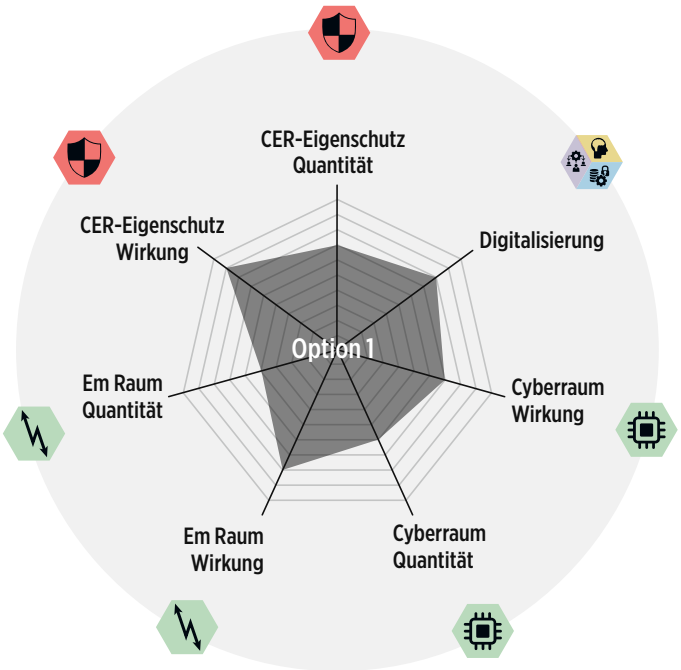


Abbildung 14: Fähigkeitsausprägung Option 1

6.3.1 Leistungen

CER-Eigenschutz

Mit der Umsetzung dieser Option wäre es möglich, wichtigen Infrastrukturen dezentral und punktuell zu schützen. Dazu könnten anderen Verbänden der Armee (oder bei Bedarf zivilen Partnern) bedarfsgerecht Mittel aus einem spezialisierten Bataillon der Stufe Armee zugewiesen oder unterstellt werden.

Fähigkeiten zur Unterstützung der Digitalisierung

Die Truppe würde mit verlegbarer IKT-Infrastruktur bis Stufe Bataillon ausgerüstet, um Daten selbstständig und allenfalls autonom zu verarbeiten. Dadurch würden bis auf diese Stufe die Voraussetzungen für eine digitalisierte Führung im Verbund geschaffen.

Aktionen im elektromagnetischen Raum

Für Aktionen im elektromagnetischen Raum würde die autonome Entwicklung von elektromagnetischen Signalen für Einsätze ausgebaut. Zum Zweck der Schwergewichtsbildung oder zur Sicherstellung der Handlungsfreiheit wären spezialisierte Bataillone auf Stufe Armee verfügbar.

Aktionen im Cyberraum

Die Fähigkeiten der Armee zur Führung von Aktionen im Cyberraum würden ausgebaut. Die dazu erforderlichen Werkzeuge würden weitgehend durch die Armee selbst entwickelt, wodurch sich ihre Fähigkeit zur Wirkung gegen militärische Zielsysteme verbessern liesse. Die Armee wäre dadurch in der Lage, gleichzeitig mehrere Angriffe gegen Systeme eines Gegners zu planen, die nötigen Wirkinstrumente zu entwickeln und die Einsätze zu führen. Zudem würde in den Truppen die Fähigkeit aufgebaut, Untersuchungen von IKT-Komponenten durchzuführen (z. B. aufgefundene Datenträger). Dafür wäre ein spezialisiertes Bataillon vorgesehen, das mit punktuellen militärische Aktionen im Cyberraum andere Truppen unterstützen und die Forensik im Einsatzraum durchführen könnte.

6.3.2 Erforderliche Investitionen

Die Investitionen für Option 1 würden sich zusammengefasst auf rund 1,4 bis 2 Milliarden Franken belaufen. Der Personalbestand bliebe unverändert. Der Bestand an Milizpersonal ergibt sich aus dem Bedarf an Spezialistinnen und Spezialisten sowie an Doppelfunktionärinnen und Doppelfunktionären, also Armeeangehörigen, die neben ihrer Hauptfunktion auch Aufgaben im Bereich der Cyberabwehr wahrnehmen. Er beträgt insgesamt rund 5000–6000 Armeeangehörige. Insgesamt beansprucht Option 1 von allen geprüften Optionen am wenigsten finanzielle und personelle Ressourcen.

6.3.3 Vor- und Nachteile

Option 1 basiert auf den laufenden Vorhaben (z. B. Fitania). Der zentrale Teil des CER-Eigenschutzes würde redundant ausgebaut. Zudem würden Mittel geschaffen, die es erlauben, den Schutz punktuell und dezentral zu erweitern. Die technische Grundlage der Führungsfähigkeit der Armee wäre dadurch deutlich besser geschützt als heute.

Die technischen Voraussetzungen für eine digitalisierte Führung würden es ermöglichen, das Tempo in einem Einsatz zu erhöhen. Gleichzeitig würden moderne Technologien bis auf Stufe Bataillon eingesetzt (z. B. Augmented Reality in der Logistik oder bei Einsatzkräften).

Die Fähigkeiten im Bereich der Data Science würden in Option 1 so aufgebaut, dass sie in der ganzen Armee angewendet werden könnten. Dies würde das gemeinsame Lageverständnis armeeweit stärken. Die Unabhängigkeit der Armee im Cyber- und im elektromagnetischen Raum würde so weit ausgebaut, dass sie nur noch punktuell auf Dritte angewiesen wäre. Die Armee würde dadurch flexibler und autonomer. Zudem würde sie ihre Handlungsfreiheit erhöhen. Die teilweise redundante Infrastruktur würde zudem die Resilienz der strategischen Funkaufklärung verbessern.

Mit der Umsetzung von Option 1 könnte die Truppe bis auf Stufe Bataillon im Einsatz mit CER-Wirkungen unterstützt werden, dies allerdings nur in beschränktem Umfang und priorisiert durch die Stufe Armee. Der Fähigkeitsbedarf, der sich aus dem hybriden Konfliktbild ableitet, würde dadurch nur beschränkt abgedeckt.

Der wesentliche Nachteil von Option 1 besteht somit in der eingeschränkten Fähigkeit, die Truppen mit Cyber- und elektromagnetischen Wirkungen im Einsatz zu unterstützen. Die Stufe Armee könnte mit den auf ihrer Stufe verfügbaren Verbänden lediglich zeitlich begrenzte Schwergewichte bilden. Zudem wäre die Fähigkeit, den CER-Schutz dezentral zu verdichten, nur punktuell vorhanden.

6.4 Option 2

Mit der Option 2 würde die Mehrheit der Bataillone und Kompanien umfassend zu selbständigen Aktionen im CER und zum selbstständigen CER-Eigenschutz befähigt. Dazu würden diese Verbände mit Spezialistinnen und Spezialisten sowie mit den erforderlichen Systemen ergänzt. Zusätzlich wären auf Stufe Armee spezialisierte Bataillone für Einsätze im Cyber- und im elektromagnetischen Raum verfügbar. Über eigenständige Fähigkeiten im Cyber- und im elektromagnetischen Raum würde die Armee nur in Kernbereichen verfügen. Sie wäre diesbezüglich auf die Unterstützung durch die Industrie angewiesen.

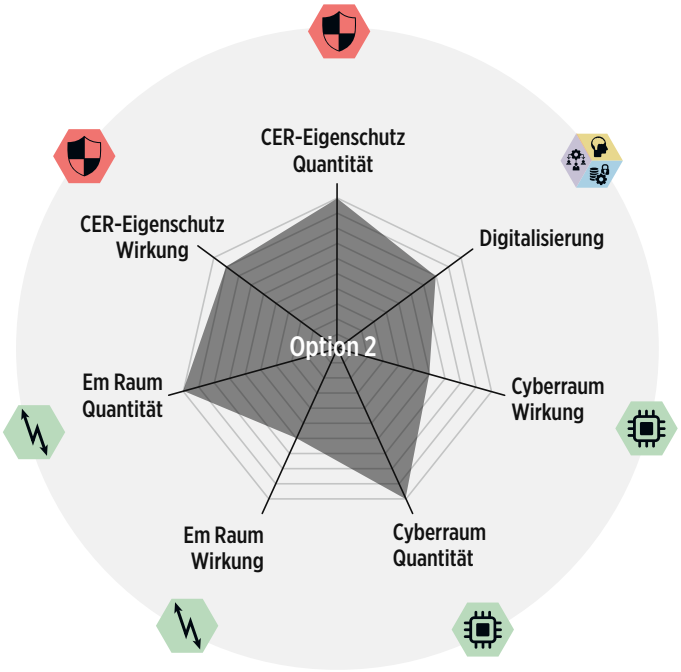


Abbildung 15: Fähigkeitsausprägung Option 2

6.4.1 Leistungen

CER-Eigenschutz

In der Option 2 würden die Mehrheit der Bataillone und Kompanien mit Spezialistinnen und Spezialisten sowie mit Systeme für den CER-Eigenschutz ausgestattet, die den dezentralen Schutz sicherstellen könnten. Diese Verbände wären dadurch in der Lage, ihre IKT-Systeme im Einsatzraum selbstständig zu schützten. Weiter würde ein spezialisiertes Bataillon zur Schwergewichtsbildung auf Stufe Armee gebildet.

Fähigkeiten zur Unterstützung der Digitalisierung

Wie in Option 1 würde die Truppe mit verlegbarer IKT-Infrastruktur bis Stufe Bataillon ausgerüstet, um Daten selbstständig und allenfalls autonom zu verarbeiten. Zusätzlich würden auch die Kompanien mit reduzierten Systemen ausgerüstet. Dadurch würden bis auf diese tiefe Führungsstufe die Voraussetzungen für eine digitalisierte Führung im Verbund geschaffen.

Aktionen im elektromagnetischen Raum

Für Aktionen im elektromagnetischen Raum würde die autonome Entwicklung von elektromagnetischen Signalen für Einsätze ausgebaut. Weiter wären spezialisierte Bataillone für militärische Aktionen im elektromagnetischen Raum auf Stufe Armee verfügbar. Diese würden auch über bodengestützte Mittel verfügen, um gegnerische Radarsysteme zu stören. Die Verbände auf Stufe Armee würden dazu dienen, Schwergewicht zu bilden und die Handlungsfreiheit zu wahren.

In der Option 2 würde die Mehrheit der Bataillone und Kompanien über eigene Spezialistinnen und Spezialisten sowie über Systeme verfügen, um Aktionen im elektromagnetischen Raum durchzuführen. Diese Systeme müssten einen hohen Automatisierungsgrad aufweisen, damit sie die Truppe einfach einsetzen könnte. Allerdings wären sie nicht besonders gut gegen herkömmliche Waffenwirkungen geschützt.

Aktionen im Cyberraum

Die Fähigkeiten der Armee für Aktionen im Cyberraum würden in dieser Option zwar ebenfalls ausgebaut, jedoch auf einem qualitativ tieferen Niveau als in der Option 1. Dafür könnten sehr viele Bataillone und Kompanien mit Mitteln für selbstständige Aktionen im Cyberraum ausgerüstet werden. Um Werkzeuge und Angriffsverfahren zu entwickeln, wäre die Armee in der Regel darauf angewiesen, von der Industrie unterstützt zu werden.

Auf Stufe Armee wäre ein spezialisiertes Bataillon zur Schwergewichtsbildung oder zur Sicherstellung der Handlungsfreiheit verfügbar. Wie für die Aktionen im elektromagnetischen Raum würde die Mehrheit der Bataillone und Kompanien darüber hinaus über eigene Spezialistinnen und Spezialisten sowie über die notwendigen Systeme verfügen. Auch diese Systeme wären in hohem Masse automatisiert, damit sie durch die Truppe einfach eingesetzt werden könnten.

Automatisierung

Die technische Einsatzbereitschaft muss bereits im Alltag laufend den neusten Entwicklungen angepasst werden. Dies dauert erfahrungsgemäss Monate oder sogar Jahre. Systeme können deshalb nicht erst kurz vor einem Einsatz beschafft und bei der Truppe eingeführt werden. Um die technische Einsatzbereitschaft der Systeme sicherzustellen, würde in Option 2 ein besonderer Bereich in der Berufsorganisation geschaffen.

6.4.2 Erforderliche Investitionen

Die Investitionen für Option 2 würden sich zusammengefasst auf rund 2 bis 2,6 Milliarden Franken belaufen. Option 2 wäre folglich teurer als Option 1, dies vor allem deshalb, weil für die Ausrüstung der Bataillone und Kompanien eine grosse Zahl von Systemen beschafft werden müsste. Der Personalbestand bliebe unverändert. Der Bestand an Milizpersonal würde 7000–8000 Armeeangehörige betragen; dabei handelt es sich vor allem um CER-Spezialistinnen und -Spezialisten sowie um Doppelfunktionärinnen und Doppelfunktionäre, die neben ihrer Hauptfunktion auch Aufgaben im Bereich der Cyberabwehr erfüllen würden. Die Option 2 bedeutet bezüglich Anzahl der Systeme den umfassendsten Fähigkeitsausbau. Deshalb handelt es sich auch um die ressourcenintensivste Option, und zwar sowohl mit Blick auf die erforderlichen Investitionen als auch hinsichtlich des zur Umsetzung notwendigen Berufs- und Milizpersonals.

6.4.3 Vor- und Nachteile

Option 2 basiert auf den laufenden Vorhaben, wie sie insbesondere mit dem Programm Fitania realisiert werden. Die Hauptunterschiede zur Option 1 liegen im Bereich der Ausgestaltung des CER-Eigenschutzes sowie der Aktionen im Cyber- und im elektromagnetischen Raum. Der dezentrale CER-Eigenschutz würde stark erweitert und es würde eine grosse Zahl von Mitteln beschafft. Dadurch könnte die Armee den überwiegenden Teil ihrer IKT-Infrastruktur auch dann schützen, wenn diese vom Gesamtnetz abgekop-

pelt würde. Die Fähigkeiten für Einsätze im Cyber- und im elektromagnetischen Raum würden vor allem bezüglich der Anzahl Systeme deutlich ausgebaut. Zur Schwergewichtsbildung auf Stufe Armee würden spezialisierte Bataillone zur Verfügung stehen.

Die Stärke der Option 2 liegt darin, dass primär die Bodentruppen zu einfachen Aktionen im Cyber- und elektromagnetischen Raum befähigt würden. Mit dem deutlich ausgebauten dezentralen CER-Eigenschutz würde ausserdem die technische Führungsfähigkeit der Armee umfassend geschützt. Ein solch umfassender Schutz wäre eine adäquate Antwort auf die spezifische Bedrohung, wie sie sich aus der möglichen hybriden Konfliktführung eines Gegners ergibt. Zudem würde die Stufe Armee in diesem Bereich deutlich an Handlungsfreiheit gewinnen. Es stellt sich im Vergleich mit den anderen Optionen jedoch die Frage, ob die zusätzliche Schutzwirkung den erheblich grösseren Mitteleinsatz rechtfertigt, der für die Umsetzung der Option erforderlich wäre.

Der Betrieb, Unterhalt und die Automatisation der sehr hohen Anzahl von Systemen würde viel Personal aus der Berufsorganisation erfordern. Diese Spezialistinnen und Spezialisten würden dann jedoch fehlen, wenn es darum ginge, vor allem anspruchsvolle Aktionen im Cyberraum gegen höherwertige und besser geschützte militärische Ziele zu planen und durchzuführen.

Der bedeutende Ausbau der CER-Elemente hätte personelle Auswirkungen auf andere Truppenteile, weil er bei gleichbleibendem Armeebestand zulasten anderer Teile der Armee erfolgen müsste. Die Anzahl benötigter Fachkräfte für die Berufsorganisation wäre hoch und am Schweizer Arbeitsmarkt wahrscheinlich nur mit sehr viel Aufwand zu rekrutieren. Zudem müssten zahlreiche neue Systeme beschafft werden, was zu zusätzlichen Kosten führen würde.

Gewisse Risiken bestehen auch im Bereich der Technologie. Besonders herausfordernd wäre dabei vor allem die Beschaffung von Systemen für automatisierte Wirkungen im Cyberraum für die Verbände der unteren taktischen Stufe. Es müssten zahlreiche Mittel beschafft werden, die durch ihre grundlegende Konstruktion und aufgrund der Technologie nicht weiterentwickelt werden könnten und damit für einen künftigen Einsatz möglicherweise ungeeignet wären. Dies hätte zur Konsequenz, dass sie in kurzen Intervallen erneuert werden müssten; der Fähigkeitserhalt würde damit teuer.

6.5 Option 3

Option 3 zielt darauf ab, dass sich die Armee künftig umfassend vor Angriffen aus dem Cyber- und elektromagnetischen Raum schützen könnte. Der Schutz bezieht sich sowohl auf permanent als auch auf temporär betriebene Systeme (z. B. Waffensysteme mit hohem IKT-Anteil). Vor allem der Eigenschutz gegen Bedrohungen aus dem elektromagnetischen Raum wäre im Vergleich zu den anderen Optionen deutlich ausgeprägter. Er würde grundsätzlich zentral gewährleistet, wofür die erforderlichen, qualitativ hochstehenden Fähigkeiten in einem spezialisierten Bataillon auf Stufe Armee zusammengefasst würden, analog dem Anfang 2022 geschaffenen Cyber-Bataillon. Ein punktueller, dezentraler Schutz von wichtigen Infrastrukturen wäre jedoch ebenfalls möglich. Dazu könnten anderen Verbänden der Armee (oder bei Bedarf zivilen Partnern) bedarfsgerecht Mittel aus dem Cyber-Bataillon zugewiesen oder unterstellt werden.

Neben dem Eigenschutz würden im Cyber-Bereich auch aktive Massnahmen aufgebaut, damit die Armee Bedrohungen angemessen abwehren könnte, auch solche, die von einem gegnerischen Waffensystem ausgehen (z. B. die Führungs- und Steuerungssysteme weitreichender Artillerie oder bodengestützter Luftverteidigung). Die Option sieht diesbezüglich den Aufbau von Fähigkeiten vor, um mehrere anspruchsvolle Angriffe gegen militärische Ziele gleichzeitig und vollständig zu planen und durchzuführen.

Ein Schwergewicht würde die Armee mit Option 3 auf die Wirkung und den Eigenschutz im elektromagnetischen Raum legen: In diesen Bereichen würde die Mehrheit der Bataillone und Kompanien zu selbstständigen Einsätzen befähigt und dazu mit den notwendigen, einfach einsetzbaren Systemen ausgerüstet. Dadurch wären die Verbände in der Lage, den gegnerischen funkbasierten Datenaustausch in ihrem Einsatzraum eigenständig zu unterdrücken und die gegnerische Führungsfähigkeit auch auf taktischer Stufe zu beeinträchtigen. Im Einsatz könnten die Kampfverbände damit das Fehlen eigener Cyber-Mittel weitgehend kompensieren. Für grössere Einsätze im elektromagnetischen Raum würde zudem eine geringe Zahl an spezialisierten Truppenkörpern gebildet bzw. weiterentwickelt, analog den beiden vorhandenen EKF-Abteilungen.

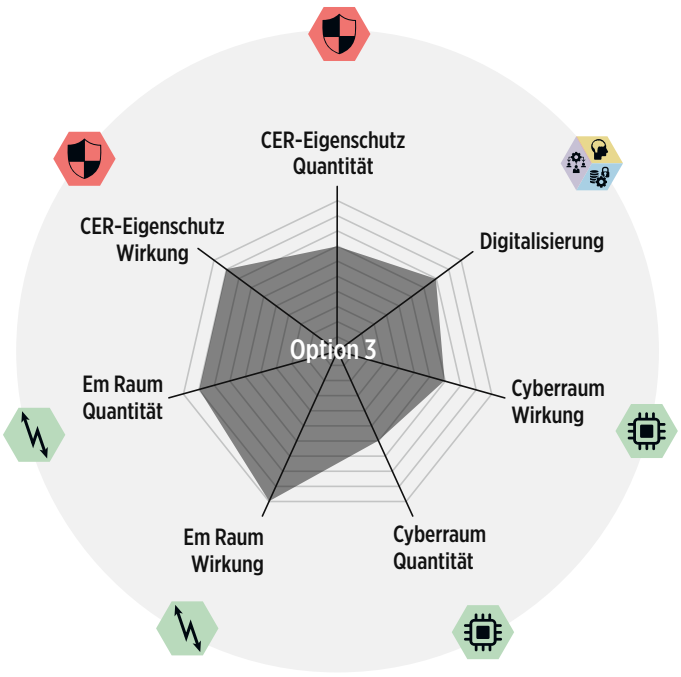


Abbildung 16: Fähigkeitsausprägung Option 3

6.5.1 Leistungen

CER-Eigenschutz

Beim CER-Eigenschutz besteht zur Option 1 kein Unterschied. Möglich wäre insbesondere ein punktueller, dezentraler Schutz von wichtigen Infrastrukturen. Dazu könnten anderen Verbänden der Armee (oder bei Bedarf zivilen Partnern) bedarfsgerecht Mittel aus dem Cyber-Bataillon zugewiesen oder unterstellt werden.

Fähigkeiten zur Unterstützung der Digitalisierung

Auch bei der Unterstützung der Digitalisierung besteht zur Option 1 kein Unterschied. Die Truppe würde mit verlegbarer IKT-Infrastruktur bis Stufe Bataillon ausgerüstet, um Daten selbstständig und allenfalls autonom zu verarbeiten. Dadurch würden bis auf diese Stufe die Voraussetzungen für eine digitalisierte Führung im Verbund geschaffen.

Aktionen im elektromagnetischen Raum

Analog zur Option 1 würde für Aktionen im elektromagnetischen Raum die autonome Entwicklung von elektromagnetischen Signalen für Einsätze ausgebaut. Zur Schwergewichtsbildung und zur Wahrung der Handlungsfreiheit wären spezialisierte Bataillone auf Stufe Armee verfügbar. Diese würden, wie in Option 2, auch über bodengestützte Mittel verfügen, um generische Radarsysteme zu stören.

Zusätzlich würde der Mehrheit der Bataillone und Kompanien eigene Spezialistinnen und Spezialisten sowie die erforderlichen Systeme zugeteilt. Die Waffenplattformen

(z. B. Panzer) dieser Verbände würden im elektromagnetischen Raum über hochgradig automatisierte und integrierte Selbstschutz- und Wirksysteme verfügen.

Aktionen im Cyberraum

Für Aktionen im Cyberraum würden die Fähigkeiten der Armee wie in Option 1 ausgebaut. Die Armee würde die dazu notwendigen Werkzeuge weitgehend selbst entwickeln und damit ihre Fähigkeit zur Wirkung gegen militärische Zielsysteme verbessern. Sie wäre dadurch in der Lage, gleichzeitig mehrere Angriffe gegen Systeme eines Gegners zu planen und die Einsätze zu führen. Zudem würde in den Truppen die Fähigkeit aufgebaut, Untersuchungen von IKT-Komponenten durchzuführen (z. B. aufgefundene Datenträger). Dafür wäre ein spezialisiertes Bataillon vorgesehen, das mit punktuellen militärische Aktionen im Cyberraum andere Truppen unterstützen und die Forensik im Einsatzraum durchführen könnte.

6.5.2 Erforderliche Investitionen

Die Investitionen für Option 3 würden sich zusammengefasst auf rund 1,6 bis 2,4 Milliarden Franken belaufen; sie liegen folglich zwischen den Optionen 1 und 2. Der Investitionsbedarf ergibt sich vor allem aus der Beschaffung der Mittel für die Einsatzunterstützung der Bataillone und Kompanien. Der Personalbestand bliebe unverändert. Beim Milizpersonal müssten vor allem zusätzliche CER-Spezialistinnen und Spezialisten sowie Doppelfunktionärinnen und Doppelfunktionäre rekrutiert werden. Der Bedarf an Milizpersonal würde rund 6000–7000 Armeeangehörigen betragen; er liegt damit zwischen den beiden anderen Optionen.

6.5.3 Vor- und Nachteile

Auch die Option 3 basiert auf den laufenden Vorhaben wie z. B. Fitania. Sie entspricht bezüglich Lageverständnis im Verbund und Datenverarbeitung robust und sicher der Option 1. Ebenfalls ausgebaut würden die Fähigkeiten für Aktionen im Cyber- und im elektromagnetischen Raum. Die Mehrheit der Verbände würde über Elemente verfügen, um Aktionen im elektromagnetischen Raum durchzuführen. Dies entspricht dem Fähigkeitsbedarf, der sich aus dem hybriden Konfliktbild ableitet. Die Waffenplattformen in den Einsatzverbänden würden mit integrierten elektromagnetischen Selbstschutz- und Wirksysteme ausgerüstet. Die Mittel für den CER-Eigenschutz und für Aktionen im Cyberraum wären auf Stufe Armee in spezialisierten Bataillonen zusammengefasst und könnten den Kampfverbänden bedarfsgerecht zugewiesen werden. Im Vergleich zur Option 2 könnten allerdings deutlich weniger Verbände und Infrastrukturen geschützt werden. Zur Schwergewichtsbildung für Aktionen im elektromagnetischen Raum würde die Stufe Armee über spezialisierte Bataillone verfügen. Sie würde so an Handlungsfreiheit gewinnen. Zwar wären die Mittel für Aktionen im Cyberraum anzahlmässig reduziert und auf Stufe Armee zusammengefasst; dies liesse sich jedoch dadurch kompensieren, indem die Mehrheit der Bataillone und Kompanien mit Mitteln für Aktionen im elektromagnetischen Raum ausgestattet würde. Bei den Fähigkeiten für Aktionen im Cyberraum stünde die Qualität im Vordergrund; diese könnte erhöht werden, weil auf einen umfassenden quantitativen Ausbau verzichtet würde.

6.6 Optionenbewertung

Jede Option gibt Antworten auf Erfordernisse, die sich aus dem sich verändernden Konfliktbild und dem technologischen Fortschritt ergeben. Sie schaffen allesamt gute Voraussetzungen, um die Digitalisierung in der Armee voranzutreiben. Alle Optionen ermöglichen zudem die Weiterentwicklung der übrigen Fähigkeiten der Armee, wie sie in den beiden Berichten zur Zukunft der Bodentruppen und zur Luftverteidigung der Zukunft beschrieben sind.

In der Gesamtbeurteilung schneidet die Option 3 am besten ab. Sie weist das beste Fähigkeitsspektrum und Leistungsvermögen auf. Dies ist der Tatsache geschuldet, dass in Option 3 die CER-Fähigkeiten in unterschiedlicher Kombination auf den verschiedenen Führungsstufen deutlich ausgebaut werden. Die Mittel für Aktionen im Cyberraum werden zugunsten der Qualität in der Anzahl reduziert und auf Stufe Armee zusammengefasst. Die dadurch scheinbar entstehende Schwäche der Bataillone und Kompanien bei der Cyberabwehr wird durch Mittel für Aktionen elektromagnetischen Raum weitgehend ausgeglichen. Diese Mittel versetzen die Kampfverbände in die Lage, den gegnerischen funkbasierten Datenaustausch in ihrem Einsatzraum eigenständig zu unterdrücken und die gegnerische Führungsfähigkeit auch auf taktischer Stufe zu beeinträchtigen. Im Einsatz können die Verbände damit das Fehlen eigener Cyber-Mittel weitgehend kompensieren. Der Aufbau von Fähigkeiten für Aktionen im Cyberraum auf Stufe Bataillon und Kompanie würde nur einen geringen zusätzlichen militärischen Nutzen bringen und unverhältnismässig viele Ressourcen binden.

In der Option 2 verfügt zwar die Mehrheit der Bataillone und Kompanien über qualitativ beschränkte eigenständige Fähigkeiten, um einfache Aktionen im Cyberraum durchzuführen. Dies bindet aber personellen Ressourcen für die Automatisation und die technische Einsatzbereitschaft der sehr zahlreichen Systeme, was sich negativ auf die erreichbare Qualität der Aktionen im Cyberraum der Armee auswirkt. Option 2 ist damit weniger geeignet als Option 3, um die CER-Fähigkeiten der Armee zukunftsgerichtet weiterzuentwickeln. Hinzu kommt, dass bei Option 3 der Eigenschutz gegen Bedrohungen aus dem elektromagnetischen Raum deutlich ausgeprägter ist. Durch das ausgewogene und in sich stimmige Leistungsprofil bietet sie zudem die beste Ausgangslage, um flexibel auf künftige Herausforderungen und Bedrohungen reagieren zu können. Schliesslich schneidet Option 3 auch in Bezug auf den Personalbedarf, die Kosten und das Technologierisiko im Vergleich zu den anderen Optionen besser ab und ermöglicht so das ausgewogenste Gesamtpaket.

6.7 Eckwerte zur Umsetzung der Option 3

Bis Anfang der 2030er-Jahre stehen in der Rüstungsbeschaffung die neuen Kampfflugzeuge und die Mittel für die bodengestützte Luftverteidigung grösserer Reichweite im Zentrum. Gleichwohl müssen auch die Cyberfähigkeiten angemessen weiterentwickelt werden. Dabei ist der Fokus auf den CER-Eigenschutz zu legen. Anschliessend sollen die Beschaffungen über alle Fähigkeitsbereiche wieder gleichmässiger erfolgen.

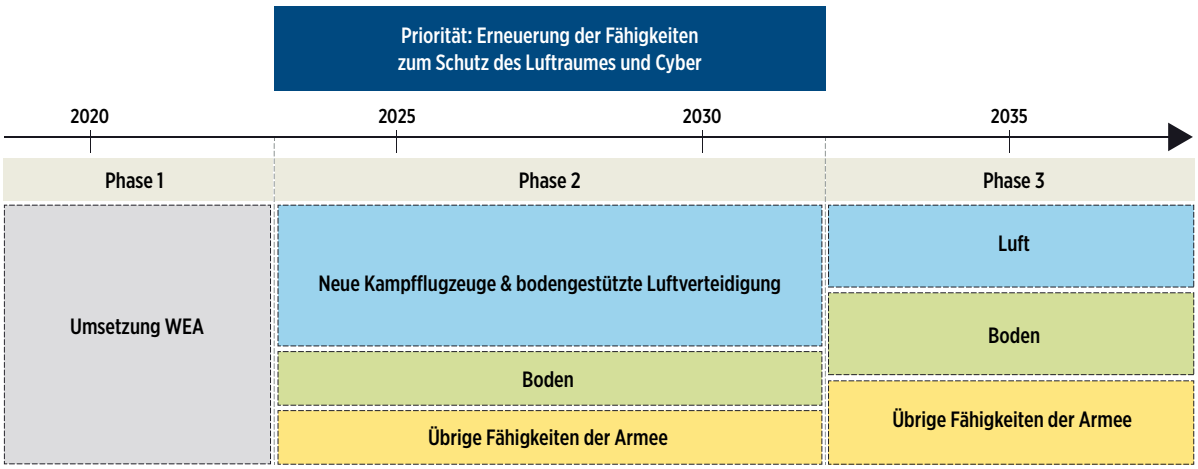


Abbildung 17: Fokus der Investitionen[129]

129 Vgl. Bericht Zukunft der Bodentruppen, S 133.

Bis 2030 können bereits weitere zeitliche Eckwerte abgeleitet werden. Die Voraussetzungen zur Digitalisierung der Armee werden in den Jahren 2024/2025 mit dem Abschluss der ersten Migration von Anwendungen auf die beiden Landesknoten geschaffen. Weiter bildet die Armee zu Beginn des Jahres 2024 das Kdo Cyber. Der volle Kapazitätsausbau in geschützten Rechenzentren ist für die Jahre 2028/2029 geplant. Schliesslich werden die Telekommunikationsmittel der Armee bis Anfang der 2030er-Jahre durch das Vorhaben TK A ersetzt. Die Umsetzung von neuen, grösseren Immobilienvorhaben ist nach aktuellem Stand ab 2028/2029 möglich.

Diese zeitlichen Eckwerte haben für die Umsetzung der Option folgende Konsequenzen:

— Die in der Option ausgewiesene Verdichtung des Führungsnetzes Schweiz ist ab 2030 vorgesehen.
— Die technische Ausgestaltung der Datenübertragung (fasergebunden und funkbasiert) ist mit dem Abschluss von TK A bis in die 2040er-Jahre zu grossen Teilen gegeben; sie bildet einen festen Rahmen für die Umsetzung der Option.
— Die breite Einführung der Digitalisierungsinfrastruktur erfolgt idealerweise nach Abschluss des Rechenzentren-Verbundes und der Regional- und Lokalknoten ab 2028.
— Der primäre Vollausbau der IKT-Infrastruktur für Data Science kann nach Abschluss des Rechenzentren-Verbundes umgesetzt werden.
— Die CER-relevanten Fähigkeiten bei den grossen Bodensystemen (z. B. Selbstschutz) sollte erst im Rahmen ihres vorgesehenen Ersatzes zu Beginn der 2030er-Jahre umgesetzt werden. So können kostenintensive Nachrüstungen bestehender Systeme umgangen werden.

6.8 Umsetzung

Aus den im vorangehenden Kapitel abgeleiteten Eckwerten lassen sich grob drei Umsetzungsschritte ableiten und so ein ungefährer Zeithorizont aufzeigen (vgl. Abbildung 20). Weil gewisse Massnahmen über den gesamten Zeithorizont aufgebaut werden und gegenseitige Abhängigkeiten bestehen, können die Schritte nicht eindeutig voneinander getrennt werden. Es wird daher lediglich skizziert, welche Massnahmen als Hauptfokus pro Schritt umgesetzt werden sollten. Mit diesem Vorgehen kann der jeweils nächste Schritt bereits beurteilt, den sich ändernden Rahmenbedingungen angepasst und mit Blick auf allfällige Technologieentwicklungen bei Bedarf adaptiert werden.

Im **Schritt 1** geht es darum, die zentralen CER-Fähigkeiten und die Fähigkeiten auf Stufe Armee auszubauen. Im **Schritt 2** sollen die dezentralen Fähigkeiten bis zur unteren taktischen Führungsstufe, teilweise bis auf die gefechtstechnische Führungsstufe, aufgebaut werden; beispielsweise die robuste und sichere Datenverarbeitung innerhalb der Bataillone und Kompanien. Ein weiteres Schwergewicht dieses Schrittes bildet der Resilienzausbau der einsatzrelevanten Kerninfrastruktur im CER-Eigenschutz. Ebenfalls in diesem Schritt wird die Organisation der Verbände angepasst. Im **Schritt 3** kann schliesslich der Fähigkeitsausbau für Aktionen im elektromagnetischen Raum bei den Manöververbänden erfolgen: Zum einen soll dabei im Rahmen der Erneuerung der Bodensysteme die Fähigkeit der taktischen Führungsstufe zur Wirkung im elektromagnetischen Raum ausgebaut werden. Zum anderen geht es darum, die dannzumal bestehende Grundfähigkeit zu Aktionen im Cyberraum auf Stufe Armee weiter auszubauen.

Dieses Vorgehen ist zu wählen, weil

— alle Massnahmen mit den laufenden Vorhaben synchronisiert sind und den übergeordneten Rahmen berücksichtigen;
— der CER-Eigenschutz mit hoher Priorität ausgebaut wird und somit die technischen Voraussetzungen für die Führung der Armee gewährleistet werden;

— der Ausbau der CER-Fähigkeiten zuerst im zentralen und anschliessend im dezentralen Teil erfolgt und dadurch ein belastbares, durchgängiges und sicheres Gesamtsystem entsteht;
— dieses schrittweise Vorgehen es erlaubt, den jeweils nächsten Schritt den sich ändernden Rahmenbedingungen anzupassen und mit den allfälligen weiteren Technologieentwicklungen Schritt zu halten;
— sich mit der Erneuerung der Bodensysteme ab 2032 die Chance bietet, den Ausbau der Fähigkeit zu Aktionen im elektromagnetischen Raum auf taktischer Führungsstufe technisch mit der Neubeschaffung von Bodensystemen zu kombinieren und Synergien zu nutzen.

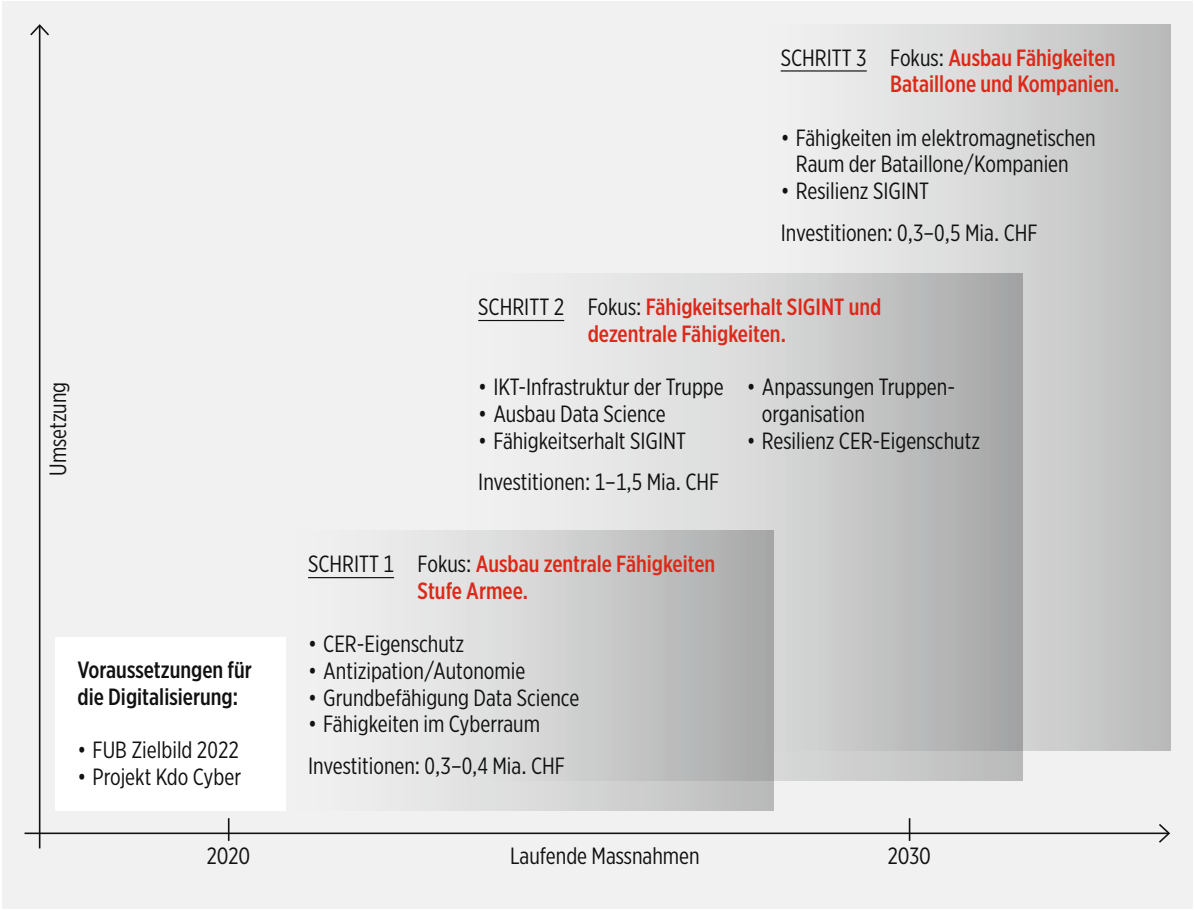


Abbildung 18: Schritte der Umsetzung Option 3

7

Kooperation mit Partnern im Rahmen des SVS bzw. mit Dritten

Mit Kooperationen im Bereich Cyber bringt sich die Armee aktiv im Sicherheitsverbund Schweiz ein und sie unterstützt Behörden im Bedarfsfall subsidiär. Mit ihrer Cyberausbildung leistet sie zudem einen Beitrag zur Reduktion des Fachkräftemangels in der Schweiz.

7 Kooperation mit Partnern im Rahmen des SVS bzw. mit Dritten

Mehrere Ereignisse zeigten in letzter Zeit, wie verwundbar kritische Infrastrukturen durch Cyberangriffe sein können. Der Cyberangriff auf die Colonial-Pipeline im Mai 2021 führte beispielsweise zu einem mehrtägigen Förderunterbruch an der Ostküste der USA und dadurch zu einem weiträumigen Versorgungsengpass an fossilen Brennstoffen. Schon nach kurzer Zeit wirkte sich diese Unterbrechung der Ölversorgung einschneidend auf die ganze Gesellschaft an der Ostküste der USA aus. Es stellt sich somit die Frage, was geschehen wäre, hätte dieser Angriff nicht der Colonial-Pipeline in den USA gegolten, sondern beispielsweise den Stromübertragungsnetzen in der Schweiz. Bei einem erfolgreichen Angriff wäre die Stromversorgung des Landes massgeblich eingeschränkt worden. Der Schluss liegt nahe, dass die verantwortlichen Stellen rasch auf alle geeigneten Ressourcen der Schweiz zur Bewältigung dieser Krise zurückgreifen würden – auch auf Spezialisten und Mittel der Armee.

Grundsätzlich erhöhen Kooperationen die Qualität der armeeeigenen Fähigkeiten. Die Armee erhält Zugang zu externem Fachwissen und kann von Erfahrungen Dritter profitieren. Zusätzliche Schnittstellen bergen aber immer auch Risiken und potenzielle Schwachstellen. Eine Zusammenarbeit ist darum in der Regel erst dann zweckmässig, wenn die entsprechenden Fähigkeiten in der Armee etabliert sind. Denkbar ist auch ein gemeinsamer Fähigkeitsaufbau im Rahmen einer Kooperation. Ein schrittweiser, priorisierter Ausbau der Kooperationen ist anzustreben.

7.1 Subsidiäre Unterstützung

Die Armee unterstützt zivile Behörden subsidiär auf der Grundlage des Militärgesetzes. Zivile Behörden können militärische Hilfe anfordern, wenn ihre Mittel ausgeschöpft oder die erforderlichen Mittel nachweislich nicht vorhanden sind und auch nicht von kommerziellen Leistungserbringern im erforderlichen Umfang und zeitgerecht erbracht werden können. Nach einem Cyber-Ereignis können auf Anfrage der zuständigen Behörden somit Elemente der Armee eingesetzt werden, um die eine oder andere Konsequenz des Ereignisses zu bewältigen (z. B. logistische Engpässe). Zudem können Cyberelemente subsidiär zum Einsatz gelangen, um beispielsweise Beiträge zur Analyse des Vorfalles bzw. zum «Wiederaufbau» zu leisten. Während der ganzen Zeit kann die Armee im Verbund mit den zuständigen Behörden Leistungen im Bereich der Beurteilung der allgemeinen und der besonderen Cyberlage gewährsleisten. Ein solcher Einsatz erfolgt auf Verlangen der zivilen Behörden.

Es wäre nicht zweckmässig, diese Fähigkeiten im Ereignisfall nicht zu nutzen, weil sie durch die Armee erbracht werden. Zudem trägt ihre sichere, robuste und flexibel erweiterbare IKT-Infrastruktur zur Resilienz der Schweiz bei. Sie kann für das Wiederanlaufen von Teilen der Gesellschaft oder von Betreibern kritischer Infrastrukturen nach einem grossangelegten und erfolgreichen Cyberangriff wesentliche Beiträge erbringen.

7.2 Kooperation

Ergänzend zu den heutigen Partnerschaften, die sich insbesondere auf den SVS fokussieren, soll die Zusammenarbeit mit anderen Bundesstellen oder Behörden sowie mit weiteren Partner in Wirtschaft und Gesellschaft gestärkt werden.

Die Armee kooperiert im CER bereits heute, in der alltäglichen Lage, mit verschiedenen Partnern, insbesondere im Rahmen des SVS. Dabei unterstützt sie SVS-Partner und Dritte darin, Aufgaben von nationaler Bedeutung zu erfüllen, ohne selbst Fähig-

keiten im CER aufbauen zu müssen. Kooperationen bestehen in Bereichen besonders geschützter IKT-Infrastruktur und permanenter oder zeitlich begrenzter IKT-Leistungen. Ihre Weiterentwicklung, insbesondere bei der Vernetzung von IKT-Infrastrukturen und -Diensten, sowie der Aufbau der dafür notwendigen Fähigkeiten ist in Planung und wird teilweise schon umgesetzt. Daran wird in allen Optionen festgehalten. Jede Option verfolgt im Minimum das Ziel, die Leistungen der Armee zugunsten der Partner qualitativ zu verbessern – insbesondere, was den Schutz vor Cyberbedrohungen und der Fähigkeit zur Zusammenarbeit (Interoperabilität) im Verbund betrifft. Die Armee kann von den Kooperationen ebenfalls profitieren, beispielsweise durch den Informationsaustausch über Bedrohungen im Cyberraum mit anderen Bundesstellen, Behörden oder Betreibern kritischer Infrastruktur.

Unabhängig von der gewählten Option bieten sich für die Armee weitere Kooperationen an, insbesondere in den Bereichen CER-Eigenschutz und Ausbildung. In welcher Art und in welchem Umfang dies erfolgen soll, wird die politische Stufe festlegen. Im CER-Eigenschutz erlangt die Armee mit der angestrebten Weiterentwicklung die Fähigkeit, in begrenztem Rahmen Schutzleistungen auch zugunsten Dritter zu erbringen. Zum einen gilt dies für die permanente Überwachung von IKT-Infrastrukturen sowie der Entdeckung und Abwehr von Cyberangriffen, zum anderen in der Unterstützung durch rasch einsetzbare Fachkräfte. Kooperationen können auch in den Bereichen Kryptologie, Computer-Forensik und Data Science erweitert werden – unter anderem mit dem Kompetenzzentrum für Datenwissenschaft (DSCC) des BFS. Im Rahmen solcher Übungen und mit Einbezug des Nationalen Zentrum für Cybersicherheit könnten künftig auch allgemein gültige Mechanismen und Entscheidprozesse für die Bewältigung von Cyberangriffen weiterentwickelt werden.

7.3 Ausbildung

Die Armee leistet in der Ausbildung einen Beitrag zur Reduktion des Fachkräftemangels, sei dies mit der Ausbildung in den Lehrgängen der Armee, sei dies in der beruflichen Grundausbildung von Lernenden in der Berufsorganisation. Mit dem Cyber-Lehrgang und der daraus abgeleiteten Berufsprüfung zum Cyber Security Specialist engagiert sich die Armee aktiv und nachhaltig in der schweizerischen Bildungslandschaft. Diese Kooperation will sie künftig ausbauen. Mit der vordienstlichen Cyber-Ausbildung baut sie das eher kleine Ausbildungsangebot für 16- bis 20-jährige Talente in der Schweiz aus. Die Absolventen der selektiven vordienstlichen Cyber-Ausbildung erwerben im Laufe des Programms Leistungsausweise, die es auch Stellen ausserhalb der Armee ermöglichen, das Potenzial eines Talents zu identifizieren. Die Armee strebt eine zivile Anerkennung dieser Leistungsausweise an. Die Arbeiten dazu mit Partnern in der Bildungslandschaft Schweiz laufen.

Durch den Aufbau des Cyber Training Center entsteht weiter die Möglichkeit, Fachspezialistinnen und Fachspezialisten bis hin zu Krisenstäben von Partnern/Dritten simulationsbasiert auszubilden. Im Rahmen solcher Übungen und mit Einbezug des NCSC könnten künftig auch allgemein gültige Mechanismen und Entscheidprozesse für die Bewältigung von Cyberangriffen weiterentwickelt werden.

Als Arbeitgeberin will die Armee verstärkt Talenten nach teilweise oder vollständig abgeschlossener Grundausbildung den Berufseinstieg erleichtern. Sie unterstützt dazu künftig vermehrt Abschlussarbeiten, beispielsweise für einen Masterabschluss. Gleichzeitig ermöglicht sie mittels Hochschulpraktika auch talentierten Quereinsteigerinnen und Quereinsteigern den Start in eine Karriere in allen CER-relevanten Berufsfeldern. Die Armee fördert die fachspezifische interne und externe Weiterbildung ihrer jungen Fachkräfte. Die Berufserfahrung, die sich diese Fachkräfte in der Armee aneignen, ist in ihrer Breite und Ausprägung einzigartig und auch im zivilen beruflichen Umfeld wertvoll. Die Armee sieht den üblichen späteren Wechsel von fertig ausgebildeten Fachkräften mit einigen Jahren Berufserfahrung in die Wirtschaft oder zu zivilen Behörden als indirekten Beitrag an die Sicherheit der Schweiz.

8

Anhang

8 Anhang

8.1 Anhang 1: Zusammenstellung der zu schliessenden Fähigkeitslücken

Fähigkeitslücke **CER-Eigenschutz**	Schritt 1	Schritt 2	Schritt 3
Schutz von militärischen Systemen dezentral sicherstellen		×	× (Em Rm)
Antizipation im CER-Eigenschutz	×		
Erkennen und Verfolgen von eigenschutzrelevanten Ereignissen	×		
Aufbau von Fähigkeiten in der Lauschabwehr	×		
Forensik im Einsatzraum sicherstellen		×	
Supply Chain Security	×		
Resilienz der Kerninfrastruktur CER-Eigenschutz aufbauen		×	
Kontrolle des eigenen Strahlungsbildes im elektromagnetischen Raum	×		

Tabelle 2: Fähigkeitslücken CER-Eigenschutz

Fähigkeitslücke **Lageverständnis im Bund**	Schritt 1	Schritt 2	Schritt 3
Datenmengen mittels Data Science auswerten	(×)	×	
Fusionierte Lageinformationen aus allen Wirkungsräumen und Funktionsbereichen der Armee und von Partnern ermöglichen ein gemeinsames, gleiches Lageverständnis.		×	

Tabelle 3: Fähigkeitslücken Lageverständnis im Verbund

Fähigkeitslücke **Datenverarbeitung robust und sicher**	Schritt 1	Schritt 2	Schritt 3
Datenflüsse degradationsfähig sicherstellen		×	

Tabelle 4: Fähigkeitslücken Datenverarbeitung robust und sicher

Fähigkeitslücke **Führung im Verbund**	Schritt 1	Schritt 2	Schritt 3
Informationsaustausch ohne Zeitverzug zwischen den Systemen verschiedener Teile der Armee sicherstellen		×	
Stufengerechtes Lagebild standardisiert, zeitgerecht und nutzerspezifisch erstellen		×	
Partner in den SNFW-Verbund einbinden		×	

Tabelle 5: Fähigkeitslücken Führung im Verbund

Fähigkeitslücke **Fähigkeitslücken Aktionen im Elektromagentischen Raum**	Schritt 1	Schritt 2	Schritt 3
Einsatzunterstützung auf taktischer Führungsstufe		×	×
Effektor im Radarfrequenzbereich aufbauen			×
Rasche und autonome Anpassung der Fähigkeiten zu Aktionen im Em Rm ermöglichen	×		
Redundante SIGINT-Kerninfrastruktur			×
Resiliente SIGINT/ESM-Sensoren	(×)	×	
Luftgestützte SIGINT/ESM	×		
Aufklärung von Kurzwellenfunksystemen (taktische Führungsstufe)		×	

Tabelle 6: Fähigkeitslücken Aktionen im Elektromagentischen Raum

Fähigkeitslücke **Fähigkeitslücken Aktionen im Cyberraum**	Schritt 1	Schritt 2	Schritt 3
Rasche und autonome Anpassung der Fähigkeiten zu Aktionen im Cyberraum ermöglichen	×		
Einsatzunterstützung bis taktische Führungsstufe	(×)	×	
Aufklärung und Wirkung gegen militärische Systeme	(×)	×	

Tabelle 7: Fähigkeitslücken Aktionen im Cyberraum

8.2 Anhang 2: Werte der Ausprägungen in den Netzdiagrammen der Optionen in Kapitel 6

Dimension	Wert	Beschreibung
CER-Eigenschutz (Qualität)	6	Ausbau Fähigkeit zur Antizipation von Bedrohungen und Ausbau der Durchhaltefähigkeit zur Abwehr von Angriffen aus dem CER (bspw. von Cyberangriffen)
	7	Zusätzlich: Flächendeckende Überwachung der Armeesysteme
	8	Zusätzlich: Resiliente Kerninfrastruktur für den CER-Eigenschutz
	9	Zusätzlich: Fähigkeit zum autonomen, dezentralen CER-Eigenschutz mit spezialisierten CER-Eigenschutz Elementen
	10	Zusätzlich: Spezialisierter Aufbau von Fähigkeiten zum Schutz vor Wirkungen von em Hochenergiewaffen.
CER-Eigenschutz (Quantität)	6	Dezentrale Leistungen zG der operativen Führungsstufe
	7	Zusätzlich: Dezentrale Leistungen zG der taktischen Führungsstufe (punktuell)
	8	Zusätzlich: Dezentrale Leistungen zG der taktischen Führungsstufe (umfassend)
	9	Zusätzlich: Leistungen zugunsten der gefechtstechnischen Führungsstufe (Eingreifkräfte, mittlere und schwere Kräfte)
	10	Zusätzlich: Leistungen zugunsten der gefechtstechnischen Führungsstufe (übrige Kräfte)
Digitalisierung (Quantität & Qualität)	7	Digitalisierte Prozesse, Data Science als Service zugunsten der Armee, Automatisation
	8–10	Nicht bewertet >>> Vorgaben GLP AFA
Cyber-Wirkungen[130] (Qualität)	6	Mässiger Ausbau der Fähigkeiten (Qualität)
	7	Deutlicher Ausbau der Fähigkeiten (Qualität)
	8–10	Ausbau bis Top-Level im Vergleich zu anderen Streitkräften

130 Die Klassifizierung INTERN des Dokuments lässt keine genauere Beschreibung der Cyber-Wirkungen zu. Gleiches gilt für die elektromagnetischen Wirkungen.

Dimension	Wert	Beschreibung
Cyber-Einsatztiefe (Quantität)	6	Wirkungen zugunsten der operativen Führungsstufe
	7	Zusätzlich: Wirkungen zugunsten der taktischen Führungsstufe (punktuell)
	8	Zusätzlich: Wirkungen zugunsten der taktischen Führungsstufe (umfassend)
	9	Zusätzlich: Wirkungen zugunsten der gefechtstechnischen Führungsstufe (Eingreifkräfte, mittlere und schwere Kräfte)
	10	Zusätzlich: Wirkungen zugunsten der gefechtstechnischen Führungsstufe (übrige Kräfte)
Elektromagnetische Wirkungen (Qualität)	6	Mässiger Ausbau der Fähigkeiten (Qualität)
	7	Deutlicher Ausbau der Fähigkeiten (Qualität)
	8	Zusätzlich: Ausbau Eigenschutz ausgewählter Verbände bzw. Systeme
	9	Zusätzlich: Ausbau Eigenschutz Eingreifkräfte, mittlere und schwere Kräfte
	10	Zusätzlich: Ausbau Eigenschutz (übrige Kräfte)
Elektromagnetische Einsatztiefe (Quantität)	6	Wirkungen zugunsten der operativen Führungsstufe
	7	Zusätzlich: Wirkungen zugunsten der taktischen Führungsstufe (punktuell)
	8	Zusätzlich: Wirkungen zugunsten der taktischen Führungsstufe (umfassend)
	9	Zusätzlich: Wirkungen zugunsten der gefechtstechnischen Führungsstufe (Eingreifkräfte, mittlere und schwere Kräfte)
	10	Zusätzlich: Wirkungen zugunsten der gefechtstechnischen Führungsstufe (übrige Kräfte)
Verbund (Quantität & Qualität)	7	Minimalbefähigung nach Zielbild 2030+ (Verbund innerhalb der Armee und zu externen Partnern)
	8–10	Nicht bewertet >>> Vorgaben GLP AFA

8.3 Anhang 3: Abkürzungsverzeichnis / Glossar

24 / 7	Bereitschaft rund um die Uhr, sieben Tage pro Woche
AdA	Angehörige der Armee
APT / Advanced Persistent Threats	Diese Bedrohung führt zu einem sehr hohen Schaden, der auf eine einzelne Organisation oder auf ein Land zielt. Der Angreifer ist bereit, sehr viel Zeit, Geld und Wissen in den Angriff zu investieren und verfügt in der Regel über grosse Ressourcen. Quelle: Glossar (admin.ch)
AI	Artificial Intelligence (künstliche Intelligenz)
AKV	Aufgaben, Kompetenzen, Verantwortung
Algorithmik	Verfahren zur schrittweisen Umformung von Zeichenreihen; Rechenvorgang nach einem bestimmten (sich wiederholenden) Schema Quelle: https://www.duden.de/rechtschreibung/Algorithmus
Asset	Ein IT-Asset ist eine Komponente (Hardware oder Software) innerhalb der IT-Umgebung
asymmetrisch	Siehe Hybrid
Attribution	Feststellen der Urheber von erfolgten Cyberangriffen
aufklären	In einem bestimmten Nachrichtenbeschaffungsraum bzw. -bereich aktiv Informationen über den Gegner, die Gegenseite oder weitere Akteure beschaffen
Augmented Reality	Deutsch: erweiterte Realität Sie beschreibt die computergestützte Erweiterung der Realitätswahrnehmung und kann alle menschlichen Sinne ansprechen.
BAKOM	Bundesamt für Kommunikation
Big Data Analysis	Big Data bezeichnet Datenmengen, die beispielsweise zu gross, zu komplex, zu schnelllebig oder zu schwach strukturiert sind, um sie mit manuellen und herkömmlichen Methoden der Datenverarbeitung auszuwerten.
Blockchain-Technologie	Eine Blockchain (auch Block Chain, englisch für Blockkette) ist eine kontinuierlich erweiterbare Liste von Datensätzen, «Blöcke“ genannt, die mittels kryptografischer Verfahren miteinander verkettet sind. Jeder Block enthält dabei typischerweise einen kryptografisch sicheren Hash (Streuwert) des vorhergehenden Blocks, einen Zeitstempel und Transaktionsdaten.
BORS	Behörden und Organisationen im Bereich Rettung und Sicherheit

Botnet / Social Bot	Eine Ansammlung von Computern, die mit Malicious Bots (Malware / Schadsoftware) infiziert sind. Diese lassen sich durch einen Angreifer (den Botnet-Besitzer) komplett fernsteuern. Je nach Grösse kann ein Botnet aus einigen Hundert bis Millionen kompromittierter Rechner bestehen. Quelle: Glossar (admin.ch)
CdA	Chef der Armee
CEMA	Cyber Electromagnetic Activities CEMA besteht aus Cyberspace-Operationen (CO), elektronischer Kriegsführung (EKF) und Spektrum-Management-Operationen (SMO). Es handelt sich um wirkungsraumübergreifende kombinierte Aktivitäten, die dazu genutzt werden, einen Vorteil gegenüber Gegnern sowohl im Cyber- als auch im elektromagnetischen Raum zu gewinnen, zu behalten und auszunutzen. Gleichzeitig wird die gegnerische Nutzung derselben herabgesetzt oder gar verweigert Aus dem Englischen von https://fas.org/irp/doddir/army/fm3-38.pdf
CERT	Computer Emergency Responce Team / IT-Notfallteam
CER	Cyber- und elektromagnetischer Raum
Cloud	Virtualisierte Ansammlung von Rechnerressourcen
CNS	Communication, Navigation, Surveillance / Kommunikation, Navigation, Überwachung
COMINT	Communication Intelligence Aufklärung von mittels elektromagnetischen Wellen übermittelten Signalen, die der Kommunikation dienen
Counter Intelligence	Gegenspionage
CTC	Cyber Training Center
Cyber- / Cyberraum	Das englische Wortbildungselement «Cyber» respektive das Synonym «Cybernetics» (Wissenschaft von den Steuerungs- und Regelungsvorgängen) leitet sich aus dem Griechischen kybernein (steuern) ab. Quelle: https://www.duden.de/rechtschreibung/cyber_ Cyber- bzw. Cyberraum bezeichnet die Gesamtheit der Informations- und Kommunikationsinfrastrukturen (Hard- und Software), die untereinander Daten austauschen, diese erfassen, speichern, verarbeiten oder in (physische) Aktionen umwandeln. Der Begriff steht auch für die dadurch ermöglichten Interaktionen zwischen Personen, Organisationen und Staaten. Quelle: Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–22
Cyberangriff	Beabsichtigte Handlung einer Person oder einer Gruppierung im Cyberraum, um die Integrität, Vertraulichkeit oder Verfügbarkeit von Informationen und Daten zu beeinträchtigen. Dies kann je nach Art des Angriffs auch zu physischen Auswirkungen führen. (Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–22). Im Kontext einer völkerrechtlichen Analyse müssen insbesondere die Regeln des humanitären und allgemeinen Völkerrechts (UNO-Charta) beachtet werden.
Cyber Threat Intelligence	Cyber-Bedrohungsaufklärung beschreibt den Vorgang der Informationssammlung über Bedrohungen und Bedrohungsakteure im Cyberraum und dient der Eindämmung von Cyberangriffen.
Data Science	Data Science ist ein interdisziplinäres Anwendungsgebiet, das Methoden und Prozesse zur Extraktion von Mustern und Erkenntnissen aus grossen, zu komplexen, zu schnelllebigen oder zu schwach strukturierten Datenmengen ermöglicht. Dabei werden Techniken und Theorien zur Automatisierung von intelligentem Verhalten und maschinellem Lernen angewandt.
Darknet	Das Darknet bezeichnet ein abgeschlossenes Netzwerk. Es enthält Webseiten, die nicht in normalen Suchmaschinen indexiert sind und über den Tor Browser zu finden sind. Tor Browser ermöglichen es, sich anonym im Internet oder im Darknet zu bewegen.
DDoS-Attacke	Unter Distributed Denial of Service (Verweigerung des Dienstes) versteht man einen Angriff auf Computer-Systeme mit dem erklärten Ziel, deren Verfügbarkeit zu stören. Quelle: Glossar (admin.ch)
degradierbar	Degradation bezeichnet die Separation von Komponenten aus IKT-Netzwerken. Die Funktionalität der abgetrennten Komponenten bleibt dabei vollständig erhalten.
Digitalisierung	Digitalisierung bezeichnet den Wandel hin zu elektronisch gestützten Prozessen mittels Informations- und Kommunikationstechnik. (Glossar BAKOM: Strategie Digitale Schweiz)
ECM	Electronic Counter Measures / Elektronische Gegenmassnahmen Teil des elektronischen Kampfes mit dem Ziel, die gegnerische Nutzung des elektromagnetischen Raums zu verhindern oder zu verringern
EFD	Eidgenössisches Finanzdepartement
Einsatzforensik / IT-Forensik	Bezeichnet das Sichern und Auswerten von Beweismitteln um festzustellen, was auf einem Gerät passiert ist.

EKF	Elektronische Kriegführung
elektronische Aufklärung	Teil der Signalaufklärung mit dem Ziel, Informationen durch Erfassen und Auswerten elektromagnetischer Ausstrahlungen fremder Ortungs- und Lenksysteme zu beschaffen.
elektronische Unterstützungsmassnahmen	Teil des elektronischen Kampfes zur Zielaufklärung, Wirkungsaufklärung und Bedrohungserkennung im elektromagnetischen Raum.
elektronischer Kampf	Teil der elektronischen Kriegführung mit dem Ziel, den elektromagnetischen Raum zu nutzen. Er umfasst elektronische Gegen-, Unterstützungs- und Schutzmassnahmen.
ELS	Einsatz- und Laufbahnsteuerungs-Modell
EPM	Electronic Protective Measures / Elektronische Schutzmassnahmen
ESM	Electronic Support Measures / Elektronische Unterstützungsmassnahmen
EW	Electronic Warfare / Elektronische Kriegführung
FITANIA	Mit dem Programm FITANIA erhalten Armee und zivile Sicherheitsorganisationen zukunftstaugliche IKT-Systeme. Die Abkürzung FITANIA steht für Führungsinfrastruktur, Informationstechnologie und Anbindung an die Netzinfrastruktur der Armee.
FMN	Federated Mission Networking zielt darauf ab, die Interoperabilität und Führungsfähigkeit durch verbesserten Informationsaustausch zwischen Partnern und Systemen sicherzustellen.
Föderation	Zusammenschluss von Organisationen, Bereichen oder Staaten
Friendly Force Tracking	Ein wirksames friendly force tracking liefert auf verschiedenen Ebenen den Standort der eigenen Streitkräfte sowie etwaiger Koalitionstruppen im Einsatzgebiet.
FUB	Führungsunterstützungsbasis
GLP AFA	Grundlagenpapier Aktionsführung der Armee
Honeypot	Als Honeypot (deutsch: Honigtopf) wird in der Computersicherheit ein Computerprogramm oder ein Server bezeichnet, der Netzwerkdienste eines Computers, eines ganzen Rechnernetzes oder das Verhalten eines Anwenders simuliert. Honeypots werden eingesetzt, um Informationen über Angriffsmuster und Angreiferverhalten zu erhalten. Quelle: Glossar (admin.ch)
Hybrid	Mischung aus zwei oder mehreren Komponenten. Quelle: https://www.duden.de/rechtschreibung/Hybrid Hybride Bedrohung bzw. hybrider Kampf ist der Ausdruck für eine flexible Mischform der offen und verdeckt zur Anwendung gebrachten regulären und irregulären, symmetrischen und asymmetrischen, militärischen und nicht-militärischen Konfliktmittel. Diese dienen dem Zweck, die Schwelle zwischen den völkerrechtlich angelegten binären Zuständen Krieg und Frieden zu verwischen. Quelle: Grundlagenbericht Zukunft der Bodentruppen (admin.ch)
IED	Improvised Explosive Device
IKT	Informations- und Kommunikationstechnologie
IKT-Systeme	Systeme in denen die IKT technisch angewendet respektive umgesetzt wird
Immersive Technologien	Immersive Technologien ermöglichen das Verschmelzen der physischen und digitalen Welt. Sie bilden die Realität entweder komplett virtuell ab (Virtual Reality) oder reichern die Umgebung mit digitalen Informationen an (Augmented Reality).
Informationsoperation	Informationsoperationen bezeichnen eine Art von Einsätzen durch Streitkräfte, bei denen Informationen des Gegners beeinflusst und gleichzeitig die eigenen Informationen und Informationssysteme gesichert werden.
IT	Informationstechnologie, Informatik
KI	Kritische Infrastrukturen. Als kritische Infrastrukturen werden Prozesse, Systeme und Einrichtungen bezeichnet, die für das Funktionieren der Wirtschaft bzw. das Wohlergehen der Bevölkerung essenziell sind.
Kryptosystem	Ein Kryptosystem ist ein System, das zur Verschlüsselung eingesetzt wird. Kryptografie bedeutet die Wissenschaft der Verschlüsselung von Informationen. Glossar (admin.ch)
LAA	Längerfristige Ausrichtung der Armee
LEIS	(Neues) Luftlage- und Einsatz-System
MG	Militärgesetz
MELANI	Melde- und Analysestelle Informationssicherung

MOTS	Merchandise off the Shelf / Geräte, die im Geschäft gekauft werden
MRO	Maintenance Repair Operations / Unterhalt, Reparatur, Betrieb
Multi-Domain-Operation	Militärische Operation, die das gesamte Spektrum der Wirkungsräume abdeckt
NATO	North Atlantic Treaty Organization / Organisation des Nordatlantikvertrags
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
PACD	Plan d›Action Cyber Défense / Einsatzplan Cyberverteidigung
Patriotic Hacker	Akteure die Aktionen im Sinne eines staatlichen Auftraggebers führen, die also fest oder temporär mit staatlichen Aufträgen betraut sind
Reach-Back-Verfahren	Der Effektor ist im Einsatzgebiet, die Waffenwirkung wird aus der Ferne gesteuert
Resilienz	Die Fähigkeit eines Systems, einer Organisation oder einer Gesellschaft, Störungen zu widerstehen und die Funktionsfähigkeit möglichst zu erhalten respektive rasch wieder zu erlangen. (Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–22)
Reverse Engineering	Deutsch: umgekehrt entwickeln Bezeichnet den Vorgang, von einem fertigen Produkt oder System durch Untersuchen der Struktur, des Zustandes, der Verhaltens- oder Funktionsweise die Konstruktionselemente zu verstehen.
SAR	Synthetic Aperture Radar
Signalaufklärung (SIGINT)	Teil der elektronischen Kriegführung mit dem Ziel, Informationen durch Erfassen und Auswerten fremder elektromagnetischer Signale zu beschaffen. Sie umfasst Funkaufklärung und elektronische Aufklärung.
SNFW-Verbund	Sensor-, Nachrichten-, Führungs- und Wirkungsverbund
Stuxnet	Stuxnet ist ein Computerwurm, der ursprünglich auf die Nuklearanlagen des Iran abzielte. Inzwischen ist er mutiert und hat sich auf andere Industrie- und Energieerzeugungsanlagen ausgebreitet. Quelle: https://www.mcafee.com/enterprise/de-de/security-awareness/ransomware/what-is-stuxnet.html
Supply Chain Security	Sicherheit in der Lieferkette oder Wertschöpfungskettensicherheit
SVS	Sicherheitsverbund Schweiz
VBS	Eidgenössisches Departement Verteidigung, Bevölkerungsschutz und Sport
Wargaming	Wargaming wird in den letzten Jahren vermehrt im Rahmen der Aktionsplanung zur Überprüfung der Varianten und insbesondere des Entschlusses eingesetzt.
WEA	Weiterentwicklung der Armee
ZEO	Zentrum Elektronische Operationen

8.4 Anhang 4: Literaturverzeichnis

Internet

Abschlussbericht Aufbaustab Cyber- und Informationsraum 2016. Bundesministerium für Verteidigung (DE) 2016.
http://docs.dpaq.de/11361-abschlussbericht_aufbaustab_cir.pdf

Gaycken Sandro, Talbot, David: Aufmarsch im Internet, in: Technology Review, 08.10.2010.
https://m.heise.de/tr/artikel/Aufmarsch-im-Internet-1102301.html

Gilbert David: A bunch of kids probably pulled off the biggest DDoS hack ever, in: Vice News, 04.11.2016.
https://www.vice.com/en_us/article/3k58e5/a-bunch-of-kids-probably-pulled-off-the-biggest-ddos-hack-ever

Kamasa Julian: Transparente Sicherheitspolitik notwendig, Avenir Suisse, 17.06.2019.
https://www.avenir-suisse.ch/transparente-sicherheitspolitik-notwendig

MacKenzie Paul: Cyberspace and Cyber-Enabled Information Warfare, in: Joint Air Power Competence Centre, 2018.
https://www.japcc.org/cyberspace-and-cyber-enabled-information-warfare/

Patalong Frank: Untersee-Kabel: Die fragilen Lebensadern des Internets, in: Der Spiegel, 02.02.2015.
https://www.spiegel.de/netzwelt/web/untersee-kabel-die-fragilen-lebensadern-des-internets-a-1015809.html

Ruhmann Ingo: Aufrüstung im Cyberspace. Staatliche Hacker und zivile IT-Sicherheit im Ungleichgewicht, in: Wissenschaft & Frieden, Dossier 79, Ausgabe 3, 2015.
https://wissenschaft-und-frieden.de/seite.php?dossierID=083

Sicherheitslücken im Internet, C.I.A. Prinzip, Universität Oldenburg (DE), 2020.
http://www.informatik.uni-oldenburg.de/~iug10/sli/index.html

Simonite Tom: NSA's Own Hardware Backdoors May Still Be a "Problem from Hell", in: MIT Technology Review, 08.10.2013.
https://www.technologyreview.com/2013/10/08/176195/nsas-own-hardware-backdoors-may-still-be-a-problem-from-hell/

Streitkräfte Deutschland:
https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum

Streitkräfte Finnland:
https://puolustusvoimat.fi/en/about-us/c5-agency

Streitkräfte Frankreich:
Direction générale de l'armement (defense.gouv.fr)

Streitkräfte Grossbritannien:
https://www.theguardian.com/technology/2020/feb/27/uk-to-launch-specialist-cyber-force-able-to-target-terror-groups;
https://www.independent.co.uk/news/uk/home-news/cyber-warfare-security-force-iran-crisis-ministry-of-defence-a9278591.html

Streitkräfte Niederlande
https://english.defensie.nl/topics/cyber-security/cyber-command

Publikationen

Aktionsplan Cyber-Defence VBS (APCD), Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport VBS (Hg.), Bern 2017.
Aktionsplan für Cyber-Defence APCD (admin.ch)

Baezner Marie, Cordey Sean: **Nationale Cybersicherheitsstrategien im Vergleich – Herausforderung für die Schweiz**, März 2019, Center for Security Studies (CSS), ETH Zürich 2019.
Risk and Resilience Reports – Center for Security Studies | ETH Zürich

Baezner Marie, Robin Patrice: **Hotspot Analysis**: Stuxnet, October 2017, Center for Security Studies (CSS), ETH Zürich 2017.
Risk and Resilience Reports – Center for Security Studies | ETH Zürich

Bericht des Bundesrates: Die Sicherheit der Schweiz 2016 (16.061), 24.08.2016, BBl 7763-7888.
Die Sicherheitspolitik der Schweiz – Bericht des Bundesrates (admin.ch)

Bericht des Bundesrates: **Effizientere Bekämpfung von Terrorismus und organisiertem Verbrechen**, Erfüllung des Postulates der Sicherheitspolitischen Kommission SR (05.3006) vom 09.06.2006, BBl 2006-0523.
BBl 2006 5693 (admin.ch)

Bericht GPDel: **Satellitenaufklärungssystem des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (Projekt «ONYX»)**, Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte vom 10.11.2003, BBl 2003-2615.
Satellitenaufklärungssystem des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (Projekt «Onyx»). Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte vom 10. November 2003 (parlament.ch)

Bericht: **Luftverteidigung der Zukunft**: Sicherheit im Luftraum zum Schutz der Schweiz und ihrer Bevölkerung, Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport VBS (Hg.), Bern 2017.
Luftverteidigung der Zukunft - Bericht der Expertengruppe Neues Kampfflugzeug (admin.ch)

Bericht: **Zukunft der Bodentruppen**: Grundlagenbericht über die Weiterentwicklung der Fähigkeiten der Bodentruppen, Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport VBS (Hg.), 2. Überarbeitete Auflage, Bern 2019.
Zukunft der Bodentruppen (admin.ch)

Botschaft zum Nachrichtendienstgesetz vom 19.02.2014, BBl 2013-2794.
Botschaft zum Nachrichtendienstgesetz (admin.ch)

Botschaft zur Änderung der Rechtsgrundlagen für die Weiterentwicklung der Armee, 03.09.2014, BBl 2014-6955.
BBl 2014 6955 (admin.ch)

Botschaft zur Legislaturplanung 2019–2023 (19.078), 29.01.2020, BBl 1777-1906.
Botschaft zur Legislaturplanung 2019–2023 (admin.ch)

Coats Daniel: **Worldwide Threat Assessment of the US Intelligence Community**, 13.02.2018.
https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

Cordey Sean, Dewar Robert S., ed.: **National Cybersecurity and Cyberdefense Policy Snapshots**: Update Collection 2, 2019, Center for Security Studies (CSS), ETH Zürich 2019.
Risk and Resilience Reports – Center for Security Studies | ETH Zürich

Cordey Sean: **Cyber Influence Operations**: An Overview and Comparative Analysis, Cyber Defence Trend Analysis, Center for Security Studies, ETH Zurich 2019.
Risk and Resilience Reports – Center for Security Studies | ETH Zürich

Cyber and Electromagnetic Activities: Joint Doctrine Note 1/18, Development, Concepts and Doctrine Centre, UK Ministry of Defence, Swindon (UK) 2018.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf

Cyber Electromagnetic Activities: Field Manual FM 3.38, Headquarters Department of the Army, Washington D.C.(US) 2014.
https://fas.org/irp/doddir/army/fm3-38.pdf

Dewar Robert S.: **Trend Analysis: Contextualising Cyber Operations**, May 2018, Center for Security Studies (CSS), ETH Zürich 2019.
Risk and Resilience Reports – Center for Security Studies | ETH Zürich

Digitaler Stillstand, Die Verletzlichkeit der digital vernetzten Gesellschaft, Österreichische Akademie der Wissenschaften 2017.
http://epub.oeaw.ac.at/0xc1aa5576_0x00358488.pdf

Evan Tamara: **Cyber Terrorism Threat Intelligence and Loss Modelling**, in: Cambridge Centre for Risk Studies 2018, Risk Summit 2018.
https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/180620-slides-evan.pdf

Gaycken, Sandro: **Einführung Cyberwar**: Was ist Cyberwar. 2013
https://www.inf.fu-berlin.de/groups/ag-si/pub/Cyberwar_SB1-5_V160114.pdf

Schörnig Niklas: **Resilienz stärken und Vertrauen bilden statt den Cyberwar herbeireden**, in: Werkner Ines-Jaqueline / Schörnig Niklas: Cyberwar – die Digitalisierung der Kriegsführung: Fragen zur Gewalt, Band 6, Wiesbaden (DE) 2019.

Schulze Sven-Hendrick: **Cyber-»War» – Testfall der Staatenverantwortlichkeit**, Tübingen (DE) 2015.

Schürz Torben: **Der vernetzte Krieg. Warum moderne Streitkräfte von elektronischer Kampfführung abhängen**, in: DGAPkompakt 17, 16.10.2015.
https://dgap.org/system/files/article_pdfs/2019-17-DGAPkompakt.pdf

Segal Adam: **The Hacked World Order**, New York, United States Public Affairs, 2016

Sigholm Johan: Non-State Actors in Cyberspace Operations, in: Journal of Military Studies, Volume 4, 2013.

Slayton Rebecca: **What Is the Cyber Offense-Defense Balance?** Conceptions, Causes, and Assessment, in: International Security; The MIT Press, Band 41, Ausgabe 3, Cambridge (US) 2017.

Smeets Max: **The Strategic Promise of Offensive Cyber Operations**, in: Strategic Studies Quarterly, Vol. 12, 22.09.2018.
https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Smeets.pdf

Strategie digitale Schweiz, Bundesamt für Kommunikation BAKOM, Biel 2020.
Digitalisierung (admin.ch)

Strategie: **Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022**, Informatiksteuerungsorgan des Bundes ISB (Hg.), Bern 2018.
Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) für die Jahre 2018-2022 (admin.ch)

Swisscom Cyber Security Report 2019: Der gezielte Angriff.
https://www.swisscom.ch/content/dam/swisscom/de/about/unternehmen/portraet/netz/sicherheit/documents/security-report-2019.pdf.res/security-report-2019.pdf

The Global Disinformation Order: **Global Inventory of Organized Social Media Manipulation**; University of Oxford (UK) 2019.
https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

Impressum

Herausgeber	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS)
Redaktion	Expertengruppe Gesamtkonzeption Cyber
Premedia	Zentrum digitale Medien der Armee (DMA), 86.084 d
Copyright	02.2022, VBS
Internet	www.armee.ch