Sachdokumentation:

Signatur: DS 3886

Permalink: www.sachdokumentation.ch/bestand/ds/3886

Zitierweise für graue Literatur

Elektronische Broschüren und Flugschriften (DS) aus den Dossiers der Sachdokumentation des Sozialarchivs werden gemäss den üblichen Zitierrichtlinien für wissenschaftliche Literatur wenn möglich einzeln zitiert. Es ist jedoch sinnvoll, die verwendeten thematischen Dossiers ebenfalls zu zitieren. Anzugeben sind demnach die Signatur des einzelnen Dokuments sowie das zugehörige Dossier.

avenir suisse

avenir debatte

Perspektiven der Sicherheitspolitik

Realitätsbezogene Strategien zum Schutz der Schweiz

Lukas Rühli und Lisa Rogenmoser

Dank

Die Autoren bedanken sich bei den Mitgliedern der Programmkommission von Avenir Suisse, Prof. Dr. Karen Horn und Dr. Christian Casal, für das inhaltliche Lektorat. Unser Dank gilt auch den 19 Interviewpartnern: VBS-Mitarbeitern, Armeeangehörigen, Cyberexpertinnen und -experten, Dozenten und Diplomaten. Sie alle haben wertvolle Inputs und Vorschläge eingebracht, ohne die diese Publikation nicht möglich geworden wäre. Die Verantwortung für den Inhalt der Studie liegt allein bei den Autoren, Lisa Rogenmoser und Lukas Rühli sowie beim Direktor von Avenir Suisse, Peter Grünenfelder.

Autoren	Lukas Rühli und Lisa Rogenmoser
Internes Lektorat	Urs Steiner
Herausgeber	Avenir Suisse, *www.avenir-suisse.ch*
Gestaltung	Carmen Sopi, Olivia Vilarino

Bestellen	assistent@avenir-suisse.ch, Tel. 044 445 90 00
Download	*www.avenir-suisse.ch/publication/perspektiven-der-schweizer-sicherheitspolitik/*

Vorwort

Seit dem 24. Februar 2022, dem Tag, als Russland in einem Angriffskrieg auf das unabhängige, demokratisch regierte Nachbarsland Ukraine eine Zeitenwende in der europäischen Nachkriegsordnung einläutete, ist die Sicherheitspolitik auch hierzulande wieder in aller Munde. Doch statt eine fundierte Auslegeordnung über die aktuelle und zukünftige Schweizer Sicherheitsarchitektur vorzunehmen, verliert man sich vorschnell in parteipolitischen Positionsbezügen. Linke Kräfte sammeln – ungeachtet davon, dass die Schweizer Stimmberechtigten bereits am 27. September 2020 den Bundesbeschluss über die Beschaffung neuer Kampflugzeuge angenommen haben – Unterschriften für die Initiative gegen den F-35-A und fordern die energiepolitische Autarkie. Auf nationalkonservativer Seite wird die Lancierung einer Volksinitiative vorangetrieben, die unserem Land eine allumfassende Neutralität vorschreiben soll. Der Erlass von Wirtschaftssanktionen gegen kriegerische Regimes, in Abstimmung mit der internationalen Gemeinschaft, würde damit Bund und Kantonen verunmöglicht. Und parteiübergreifend werden in einem Akt der Symbolpolitik mehr Finanzmittel für die Armee gefordert, ohne zu konkretisieren, wohin diese Mittel fliessen sollen.

Was fehlt, ist der Blick auf das «grosse Ganze». Die vorliegende Sicherheitsstudie soll ihren Teil dazu beitragen. Die inhaltlichen Arbeiten begannen vor weit über einem Jahr und sind nicht der aktuellen Lage geschuldet. In den letzten 18 Monaten analysierten die Avenir-Suisse-Forscher in zahlreichen Gesprächsrunden und Interviews mit in- und ausländischen Experten die weltweite und europäische Bedrohungslage und hinterfragten Dogmen wie auch vorherrschende Meinungsbilder zur Schweizer Sicherheitspolitik. Dazu wurde die heutige Ausrichtung der Schweizer Sicherheitsarchitektur den aktuellen Gefährdungslagen gegenübergestellt. Es zeigt sich: Die Plausibilitäten für die einzelnen Konfliktarten sind höchst unterschiedlich. Doch nur in Ansätzen folgt die aktuelle Schweizer Sicherheitspolitik den oft stark divergierenden Eintretenswahrscheinlichkeiten von Gefährdungen für Gesellschaft und Wirtschaft. Gemäss meinen beiden Kollegen, Lisa Rogenmoser und Lukas Rühli, die Autorin und der Autor dieser neuen Studie, braucht es darum eine breitere Debatte über realitätsbezogene Strategien zum Schutz der Schweiz. Vorab gilt es, sich vom Denkmuster zu lösen, unser Land sei den Bedrohungslagen isoliert ausgesetzt und müsse diese demzufolge allein bewältigen. Wenn Verteidigungsanstrengungen im internationalen Verbund erfolgen, ist es sinnvoll, diese auch vorab im Verbund zu üben. Nur schon aus diesem Grund lässt sich eine bessere transnationale Abstimmung der Schweiz mit den kollektiven Verteidigungsstrukturen der Nato und der Sicherheitskooperation der europäischen Länder begründen. Die Schweizer Sicherheitspolitik muss zugleich ehrlicher als

bisher in den Spiegel schauen und eine Antwort darauf geben, ob angesichts der zahlreichen Bedrohungslagen unser Kleinstaat überhaupt in der Lage ist, auch mit allenfalls aufgestockten Sicherheitsbudgets für eine allumfassende Verteidigungsfähigkeit zu sorgen. Sind zukünftig nicht vermehrt Priorisierungen notwendig und die öffentlichen Gelder stärker gemäss den unterschiedlichen Eintretenswahrscheinlichkeiten auszurichten?

Der Krieg in Osteuropa macht es deutlich: Auch wenn die Schweiz von ihrer geografischen Lage mitten in Europa und vom Nato-Schutzschirm profitiert, kommt sie nicht um eine Weiterentwicklung ihrer Landesverteidigung herum – strukturell, aber auch sicherheits- und neutralitätspolitisch. Ein rein nach Innen gerichteter Fokus und damit letztlich ein alleiniger isolierter Ansatz abseits des Verteidigungsverbunds um uns herum würde sich als Irrweg erweisen.

In der vorliegenden Studie vermitteln die Autoren Denkanstösse für zukünftige Perspektiven der Schweizer Sicherheitspolitik, indem sie ungeachtet von Dogmen und Ideologien den Handlungsbedarf infolge der unterschiedlichen Bedrohungsbilder ableiten.

Peter Grünenfelder, Direktor von Avenir Suisse

Inhalt

Executive Summary

Die Welt ist unruhig. Nach Jahrzehnten des weitgehenden Friedens herrscht ein bewaffneter zwischenstaatlicher Konflikt in Europa. Der Angriffskrieg Russlands in der Ukraine verändert nicht nur die europäische, sondern die globale Sicherheitslage. Geopolitische Verschiebungen sowie gesellschaftliche und technologische Entwicklungen generieren neue Unsicherheiten. Das internationale Umfeld ist instabiler und unberechenbarer geworden, die Schutzwirkung des geographischen und politischen Umfelds der Schweiz lässt nach. Vor dem Hintergrund einer herausfordernden und komplexen sicherheitspolitischen Lage untersucht die vorliegende Publikation, was diese Entwicklungen für die Ausrichtung der schweizerischen Sicherheitspolitik bedeuten.

Eine direkte militärische Bedrohung durch einen terrestrischen Angriff auf die Schweiz ist gemäss Bundesrat weiterhin unwahrscheinlich. Ein konventioneller Konflikt dürfte eher Europa als Kollektiv im Rahmen einer gemeinsamen Verteidigungsanstrengung betreffen – und nicht isoliert die Schweiz. Die Schweiz hat sich zudem auch gegen Risiken zu wappnen, die sich nicht ausschliesslich mit militärischen Mitteln kontrollieren lassen: (kriminelle) Cyberangriffe, Pandemien, Strommangellagen, ein Ausfall des Mobilfunknetzes oder terroristische (Drohnen-) Angriffe gehören dazu. Im Rahmen der materiellen Kompletterneuerung der Armee während der nächsten zehn Jahre scheint allerdings ein Grossteil der Neuinvestitionen für konventionelle Mittel angedacht zu sein.

Angesichts der komplexen und vielfältigen Bedrohungslage ist es schwierig, sich in angemessener Weise gegen alle erdenklichen Bedrohungen zu wappnen. Gewisse Trade-Offs sind für die Schweiz als kleines Land unvermeidbar. Eine transparente Lagebeurteilung sowie eine Mittelallokation, die aktuelle und künftig plausible Bedrohungsbilder konsequent priorisiert, sind entscheidend, um eine effiziente und bedarfsgerechte Sicherheitspolitik zu gewährleisten.

- Beispielsweise sollte diskutiert werden, ob neben den geplanten Erneuerungsinvestitionen in bereits bestehende schwere Panzersysteme genügend Mittel vorhanden sind, um beispielsweise hybriden Bedrohungen im urbanen Gebiet angemessen begegnen zu können.
- Die Kampfjets F-35A, die beschafft werden sollen, sind spezifisch für Einsätze in einem militärischen Verbund (der Nato) konzipiert. Um ihr Potenzial voll auszuschöpfen, ist die transnationale Militärkooperation auszubauen, beispielsweise durch die Teilnahme an Nato-Übungen. Es gilt daher, neutralitätspolitische Fragen zu klären. Aufgrund der zunehmenden Relevanz von Drohnenangriffen sind zudem Schutzkonzepte in diesem Bereich angebracht.
- Die Schweizer Cybersicherheit muss erhöht werden – sowohl jene des Militärs als auch jene der kritischen Infrastrukturen. Die Aufgabentei-

lung bezüglich Cybersicherheit muss klar sein – zwischen Militär und anderen staatlichen Stellen, sowie zwischen Staat und Wirtschaft. Bei der Abwehr von nicht kriegerischen Cyberangriffen ist die Armee weiterhin nur subsidiär einzusetzen. Für Betreiber kritischer Infrastrukturen sollte der Bund Systemredundanzen, Backup-Konzepte und Meldepflichten (im Falle von Cyberangriffen) vorschreiben.

Die sicherheitspolitischen Strategien anderer europäischer Länder können interessante Anhaltspunkte für die Schweiz liefern. Das Vereinigte Königreich setzt beispielsweise vermehrt auf den Ausbau der Cyber- und Drohnenabwehr. Finnland und Schweden zeigen, dass kleine und neutrale, bzw. blockfreie Länder angesichts konventioneller Bedrohungen ihre Verteidigungsstrategien hin zu mehr transnationaler Kooperation ausrichten. Die Verteidigung im Ernstfall ist im Verbund am effizientesten, weshalb die Fähigkeiten vorab eingeübt und aufgebaut werden müssen.

Eine effiziente Sicherheitspolitik kann auch in Zukunft gewährleistet werden, indem der Sicherheitsetat bedarfsorientiert aufgrund effektiver Risiken und Bedrohungen auf die sicherheitspolitischen Instrumente verteilt wird.

1_Einleitung

Die militärische Invasion Russlands in die Ukraine stellt eine Zäsur dar. Europa, das über weite Strecken auf lange Jahrzehnte des Friedens zurückblickt, ist mit einer kriegerischen Auseinandersetzung konfrontiert. Die Eskalation der Ereignisse sorgte selbst bei vielen Expertinnen und Experten für Erstaunen, wenn nicht gar Entsetzen, doch sie spiegeln auch eine geopolitische Entwicklung, die sich schon seit längerem abzeichnet: Die Konkurrenz zwischen Gross- und mittelgrossen Mächten nimmt zu, das internationale Umfeld ist instabiler und unberechenbarer geworden und Konflikte werden sowohl mit konventionellen wie auch mit hybriden Mitteln wie Cyberangriffen und Desinformationskampagnen ausgefochten.

Der Angriffskrieg Russlands in der Ukraine hat – das steht ausser Frage – schwerwiegende und weitreichende Konsequenzen. In erster Linie für die Ukraine und ihre Bürgerinnen und Bürger aber auch für die westliche Allianz und die europäische Sicherheitsordnung. Was bedeutet das für die Schweiz?

Diese Frage war ursprünglich nicht Ausgangspunkt der vorliegenden Studie. Denn die Forschungsarbeiten daran begannen schon vor über einem Jahr – als ein derart expliziter territorialer Angriff Russlands sowohl vom Bundesrat als auch von der Nato für unwahrscheinlich betrachtet wurde und als die Vorstellung einer eigentlichen territorialen Bedrohung für viele europäische Länder in weiter Ferne lag. Die aktuelle kriegerische Aggression Russlands wird nun in den Untersuchungskontext eingebettet, der da lautet: Fliessen die Investitionen im Rahmen der schweizerischen Verteidigungspolitik angesichts der Gefahren des 21. Jahrhunderts in die richtigen Geräte und Massnahmen?

Die gesamteuropäische Sicherheitslage hat sich innert weniger Monate nachhaltig verändert und so auch das sicherheitspolitische Umfeld der Schweiz. Doch es bleibt festzuhalten: Als Land inmitten von Europa profitiert die Schweiz vom Schutzschirm der Nato und den sicherheitspolitischen Bemühungen der EU. Es ist aktuell weiterhin nicht damit zu rechnen, dass die Schweiz territorial direkt von den Geschehnissen in der Ukraine betroffen sein wird. Trotz der besorgniserregenden Ereignisse in der Ukraine soll der Blick auf das grosse Ganze nicht verloren gehen: Die Schweiz hat sich auch gegen Risiken wie (kriminelle) Cyberangriffe, Pandemien, Strommangellagen, ein Ausfall des Mobilfunknetzes und terroristische (Drohnen-)Angriffe zu wappnen (NDB 2020; NDB 2021; Babs 2015; Babs 2020). Diesen kann nicht ausschliesslich mit konventionellen militärischen Mitteln begegnet werden. Auf viele dieser Gefährdungen ist die Schweiz derzeit ungenügend vorbereitet.

Die gesamteuropäische Sicherheitslage hat sich innert weniger Monate nachhaltig verändert und so auch das sicherheitspolitische Umfeld der Schweiz.

Wir sind also mit einer komplexen und herausfordernden sicherheitspolitischen Lage konfrontiert, in der konventionelle militärische Bedro-

hungen und gleichzeitig auch unkonventionelle Bedrohungsszenarien relevant sind. Angesichts dieser Vielfalt ist es schwierig, sich in angemessener Weise gegen alle erdenklichen Bedrohungen zu wappnen. Gewisse Trade-Offs sind für die Schweiz als kleines Land unvermeidbar. Eine transparente Lagebeurteilung, sowie eine Mittelallokation, die aktuelle und künftig plausible Bedrohungsbilder konsequent priorisiert, sind entscheidend, um in effizienter Weise ein grösstmögliches Mass an Sicherheit zu gewährleisten.

Die aktuelle Situation verdeutlicht die Wichtigkeit des Themas Sicherheitspolitik und rückt dieses stärker ins Scheinwerferlicht der Schweizer Öffentlichkeit. Öffentliche Diskussionen sind wichtig, um in einer komplexen und herausfordernden sicherheitspolitischen Landschaft eine bedarfsgerechte und effiziente Schweizer Sicherheitspolitik zu gewährleisten. Wir hoffen, mit der vorliegenden Publikation einen Beitrag zu dieser Debatte leisten zu können.

Box 1

Die Bereitstellung von Sicherheit als ökonomische Frage

Sicherheit wird von Ökonomen als ein klassisches öffentliches Gut gewertet: Es besteht Nichtrivalität im «Konsum» (der Genuss von Sicherheit des einen schränkt nicht den Genuss von Sicherheit eines anderen ein) und fehlende Ausschliessbarkeit (ein Individuum auf Schweizer Boden kann auch bei fehlender Zahlungsbereitschaft nicht von der bereitgestellten Sicherheit ausgeschlossen werden). Daher zählt die Gewährung der äusseren und inneren Sicherheit eines Landes seit jeher zu den Kernaufgaben des Staates.

Sicherheit hängt, gerade in unserer heutigen komplexen und vernetzten Welt, von einer Vielzahl sich wandelnden und teils nur schwer vorhersehbaren Faktoren ab. Da das Sicherheitsbudget nicht unbegrenzt ist, ist die effiziente Herstellung von Sicherheit eine im Kern ökonomische Frage. Bei der Effizienz gibt es zum einen die produktive Effizienz. Sie beantwortet die Frage: Werden die Dinge richtig getan? Und es gibt die allokative Effizienz. Sie beantwortet die Frage: Werden die richtigen Dinge getan? Die zweite Frage ist Kernbestandteil der vorliegenden Publikation.

Ein Staat kann sich nicht gegen alle theoretisch erdenklichen Bedrohungen wappnen, sondern muss sich auf die wahrscheinlichen und plausiblen fokussieren. Im Sinne der allgemeinen Sicherheit, sowie der Legitimation der mit Steuern finanzierten Armee ist es wichtig, die militärische Mittelallokation konsequent an der Bedrohungslage auszurichten und dementsprechende Prioritäten zu setzen.

Während die Armee als sicherheitspolitisches Instrument der Landesverteidigung im Fokus steht, nimmt dieses Debattenpapier im Kern eine ganzheitliche sicherheitspolitische Perspektive ein. Die Schweizer Sicherheitspolitik soll anhand eines Vergleichs von identifizierten Bedrohungen und Mitteleinsatz betrachtet werden. Stand der vorliegenden Publikation in Sachen Ukraine-Krieg ist der 15. März 2022.

In Kapitel 2 und 3 wird das weltweite Bedrohungsbild sowie die Sicherheitslage der Schweiz skizziert, basierend auf den Bedrohungsanalysen des Bundes.

Kapitel 4 untersucht die Verteidigungsausgaben und die geplanten Investitionen der Schweizer Armee in den Bereichen «Boden», «Luft» und «Cyber» und stellt sie der aktuellen bzw. künftigen Bedrohungslage gegenüber.

Anhand von Fallstudien wird in Kapitel 5 die sicherheitspolitische Ausrichtung der Schweiz verglichen mit der Prioritätensetzung anderer (post-) neutraler Staaten in Europa (Schweden, Finnland und Österreich) und Grossbritanniens.

Die Thesen in Kapitel 6 sollen eine Grundlage für die Diskussion über eine bedarfsgerechte Schweizer Sicherheitspolitik liefern.

2_Die weltweite Bedrohungslage

Der Einmarsch Russlands in die Ukraine hat in Europa eine Episode von 66 Jahren zwischenstaatlichen «Friedens» beendet: Auf europäischem Boden hatte davor seit 1956 kein konventioneller zwischenstaatlicher Konflikt stattgefunden (vgl. Abbildung 2 auf S. 18). Die Mehrheit der bewaffneten Konflikte seit dem Zweiten Weltkrieg sind innerstaatlicher Natur – so auch in Europa, wo seit 1950 fast permanent einige solche Konflikte ausgetragen wurden (UCDP/PRIO 2021). [1]

Generell sind zwischenstaatliche Konflikte seit dem 2. Weltkrieg selten geworden (vgl. Abbildung 2 auf S. 18). Die Gründe für diese Abnahme sind vielfältig. Dem von den Siegermächten des Zweiten Weltkrieges, allen voran den USA, errichteten und dominierten internationalen System wird eine stabilisierende Wirkung zugeschrieben. Verteidigungsbündnisse wie die Nato haben ebenfalls eine abschreckende und somit stabilisierende Wirkung, während internationale Institutionen wie die UNO Mechanismen zur friedlichen Streitbeilegung bieten. Die potenzielle Vernichtungskraft von Nuklearwaffen hat bekanntlich zu einer gegenseitigen Abschreckung geführt, eine gewisse Eskalationsschwelle zu überschreiten. Je nach akademischer Lehre werden zudem die starke wirtschaftliche Verflechtung, sowie die Verbreitung des demokratischen Regierungsmodells für den Rückgang von zwischenstaatlichen Konflikten verantwortlich gemacht, da diese in beträchtlichen finanziellen Schäden, sowie Verlust von innen- und aussenpolitischem Kapital münden können. Einige dieser stabilisierenden Faktoren haben jedoch in den letzten Jahren an Stärke verloren.

Einige dieser stabilisierenden Faktoren haben in den letzten Jahren an Stärke verloren.

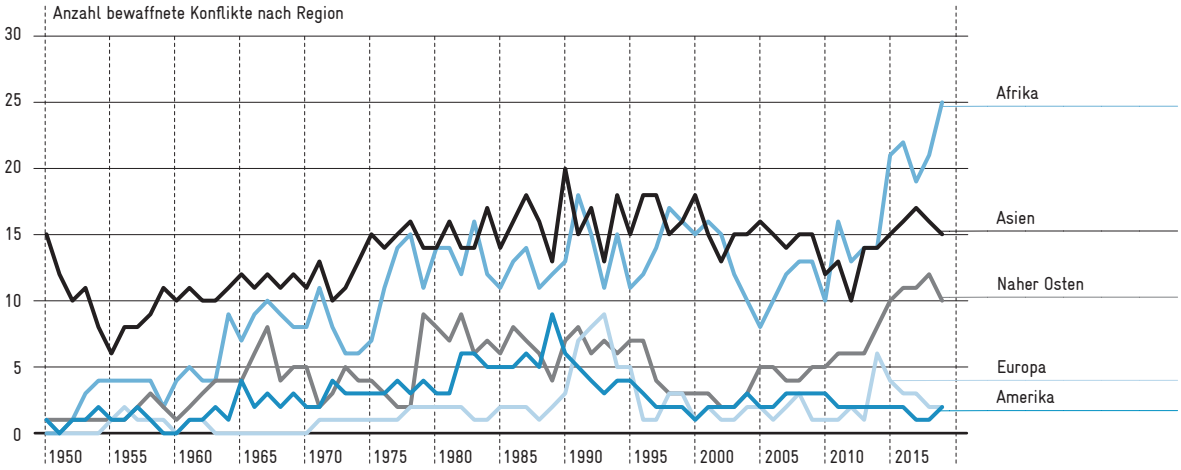
Der Nachrichtendienst des Bundes (NDB) hielt 2020 und 2021 fest, dass konventionelle bewaffnete Konflikte in Zentral- und Westeuropa aufgrund der stabilen Lage innerhalb der EU und Nato auch in Zukunft unwahrscheinlich bleiben. Diese Aussagen wurden wohlgemerkt vor Ausbruch des Konflikts in der Ukraine getroffen. Dieser beeinträchtigt die globale Sicherheitslage und ist eine Versinnbildlichung der Erosion der genannten Faktoren. Zudem sind weitere neuartige Bedrohungen festzustellen, die sowohl die globale Sicherheit beeinträchtigen, wie auch Unsicherheiten für die Schweiz generieren.

1 Bis 2019 (also noch ohne Russlands Krieg gegen die Ukraine) identifiziert die internationale Konfliktdatenbank UCDP/PRIO seit dem Ende des Zweiten Weltkrieges nur einen konventionellen zwischenstaatlichen Konflikt in Europa: Den ungarischen Volksaufstand gegen die sowjetische Besatzungsmacht im Jahr 1956. Innerstaatliche und hybride (Stellvertreter-) Konflikte tauchten phasenweise auf. Der starke Ausschlag in den 1990er Jahren ist auf die Jugoslawienkriege und die Konflikte in Nordirland sowie im spanischen Baskenland zurückzuführen. Beim zweiten Peak handelt sich um den Ukraine-Konflikt von 2014, der in der Annexion der Krim durch Russland mündete.

Abbildung 1a

Zunahme der Konflikte im Nahen Osten und in Afrika

Die meisten bewaffneten Konflikte fanden seit Ende des Zweiten Weltkriegs in Asien und Afrika statt. Deutlich zahlreicher sind die Konflikte im letzten Jahrzehnt in Afrika und im Nahen Osten geworden. In Europa erreichte die Zahl der Konflikte 1993 mit den Jugoslawienkriegen ein Maximum.

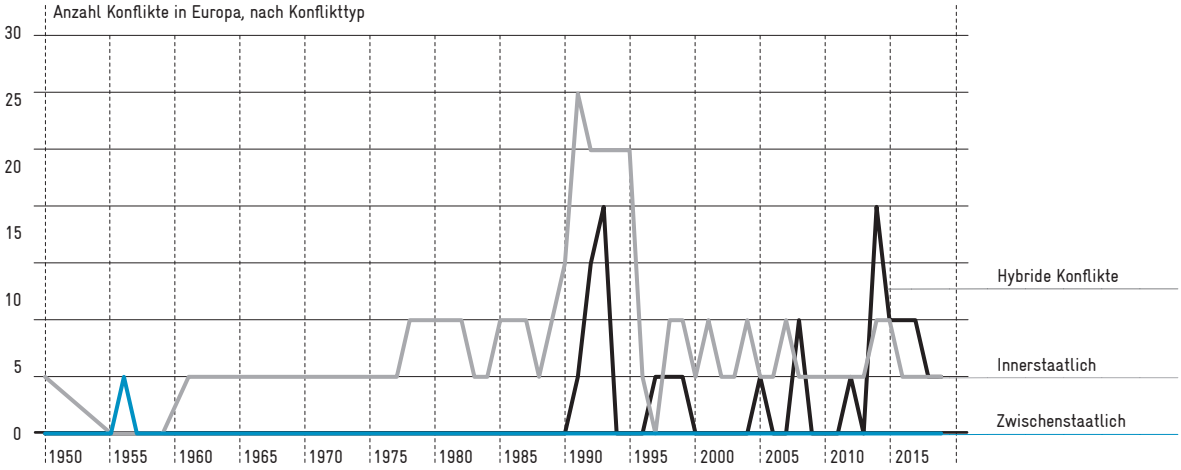


Quelle: UCDP/PRIO (2021), Gleditsch et al. (2002)

Abbildung 1b

Von 1955 bis 2022 kein konventioneller zwischenstaatlicher Konflikt in Europa

Die meisten Konflikte innerhalb von Europa waren seit dem 2. Weltkrieg innerstaatlicher oder hybrider Natur. Der Einmarsch Russlands in die Ukraine bedeutet den ersten konventionellen zwischenstaatlichen Konflikt auf europäischem Boden seit 1956.



Quelle: UCDP/PRIO armed conflict dataset (2021), Pettersson und Öberg (2020), Gleditsch et al. (2002)

2.1_ Mögliche Unsicherheitsquellen

Weltordnung – Konkurrenz der Grossmächte

USA und «The China Challenge»: Geopolitische Verschiebungen schwächen die durch die USA geprägte liberale Weltordnung. Die USA haben ihre Führungsrolle in den letzten Jahren nur noch selektiv wahrgenommen und ihre Dominanz verloren. Insbesondere China konnte seinen Einfluss wirtschaftlich, politisch, wie auch geographisch ausweiten. Die Grundlage des chinesischen Regierungshandelns ist, bis zum hundertsten Jahrestag der Gründung der Volksrepublik (1949) eine Macht mit globalem Einfluss zu werden.[2] Gemäss Experten ist der Aufstieg Chinas zu einer globalen Grossmacht so gut wie sicher (NDB 2021, S. 27). Die Übernahme bestehender internationaler Normen und Regeln dürfte nur erfolgen, wenn es im Interesse Chinas ist. Vielmehr möchte das Land der Mitte die internationale Weltordnung prägen und präsentiert sein autoritäres und staatskapitalistisches Regierungsmodell als alternative Regierungsform zur liberalen Demokratie. Während diese Absicht in den USA als konkrete Bedrohung wahrgenommen und entsprechend gekontert wird, ist man in Europa und auch in der Schweiz (zumindest öffentlich) zurückhaltender.[3] Angesichts der expansionistischen Ansprüche der Kommunistischen Partei Chinas (KPCh) und dem Nachdruck, mit welchem diese verfolgt werden, kann diese Zurückhaltung einschneidende Konsequenzen haben. Eine Schwächung liberaler und demokratischer Werte und Systeme ist nicht im Interesse von international stark eingebundenen Demokratien wie der Schweiz.

Auch wenn es aufgrund des Konflikts in der Ukraine derzeit nicht das brennendste Thema sein ist: Der Trend zu einer neuen Bipolarität wird sich wohl fortsetzen. Die Kluft zwischen dem vom Westen geprägten liberalen Modell und dem autoritären Staatskapitalismus wird laut NDB weiterwachsen und die Welt mehr und mehr vom strategischen Wettbewerb zwischen den USA und China geprägt sein (NDB 2020; NDB 2021). Europa und die Schweiz könnten künftig also gezwungen sein, sich wirtschaftlich zunehmend auf einen dieser Räume zu fokussieren, insbesondere wenn sich der Technologiewettstreit akzentuieren sollte. Auf globaler Ebene ist beispielsweise die Debatte um 5G stark von einer strategischen Perspektive geprägt und schlägt sich in der anhaltenden Kontroverse um chinesische Telekomzulieferer wie Huawei nieder. Besonders im immer

Der Trend zu einer neuen Bipolarität wird sich wohl fortsetzen.

2 Die expansionistischen Ansprüche der KPCh drücken sich in vielfältigen und weitreichenden Tätigkeiten aus: Militärisches Aufrüsten (von konventionellen Waffensystemen zu einem Nuklearprogramm), orchestrierte Hacking-Angriffe, aggressive Diplomatie und gezielte Desinformationskampagnen, kompromisslose Territorialansprüche im Süd- und Ostchinesischen Meer oder gegenüber Taiwan, starke Repressionen und Menschenrechtsverletzungen in Xinjiang und Hongkong, versuchte Einflussnahme auf andere Länder u.a. durch an Konditionen geknüpfte Entwicklungshilfe, ambitionierte Infrastrukturprojekte (bspw. die Belt and Road Initiative) oder Versuche der verstärkten Allianzbildung (bspw. der 17+1 Gipfel mit osteuropäischen Staaten) *(Foreign Affairs 2022)*.

3 Vgl. z.B. folgenden Abschnitt aus dem sicherheitspolitischen Bericht des *Bundesrates (2021a, S. 14)*: «Es ist aber noch offen, inwieweit China wirklich eine globale Führungsrolle sucht […].»

wichtiger werdenden Bereich der Digitalisierung ist es im Interesse der Schweiz, dass die internationalen Normen und Standards den Werten der Schweiz entsprechen.[4]

Um weiterhin eine glaubwürdige Verfechterin von Demokratie, Rechtsstaatlichkeit und des Völkerrechts zu sein, könnte die Schweiz in einem sich verstärkenden Systemkonflikt vermehrt in Situationen geraten, in denen ein Positionsbezug erwartet wird. In Bezug auf die Beziehungen zu China könnte ein Abwägen zwischen Prinzipen, dem Anspruch, vermittelnd, neutral und unvoreingenommen aufzutreten, sowie wirtschaftlichen Überlegungen notwendig werden.

Russlands (militärische) Aggressionen: Putins Invasion der Ukraine hat weltweit Beunruhigung und Bestürzung ausgelöst. Die diplomatischen Bemühungen haben bisher nicht die erhoffte deeskalierende Wirkung gezeigt. Wie sich der Krieg weiterentwickeln wird, ist (Stand 15. März 2022) schwer zu prognostizieren. Dasselbe gilt für das Ausmass der Involvierung von Drittländern. Die Situation verändert sich von Tag zu Tag und die vollen Auswirkungen werden sich wohl erst noch zeigen. Klar ist, dass der Krieg schwerwiegende und weitreichende Konsequenzen haben wird. Dies in erster Linie für die Ukraine und ihre Bürgerinnen und Bürger aber auch im weiteren Sinne für alle involvierten Personen und Parteien, die westliche Allianz und die europäische Sicherheitsordnung.

Der Krieg und insbesondere ein allfälliger «Triumph» Putins kann auch eine nicht zu vernachlässigende geopolitische Wirkung haben. Je nach Weiterentwicklung des Konflikts kann dieser die politische Durchsetzungskraft und militärische Abschreckung der westlichen Allianz empfindlich in Frage stellen. Geht man von einem Systemkonflikt aus, schwächt dies liberale demokratische Werte und die darauf aufbauende internationale Ordnung zusätzlich, was den Machtanspruch (anderer) autoritärer Staaten weiter befeuern könnte. Russlands Aggression könnte jedoch im Gegenteil auch ein Zusammenrücken und eine stärker geeinte Front der westlichen Länder nach sich ziehen.

Russlands Aggression könnte jedoch auch ein Zusammenrücken der westlichen Länder nach sich ziehen.

Der Bund hat vorgängig an verschiedenen Stellen festgehalten, dass die territoriale Integrität der Schweiz mit grosser Wahrscheinlichkeit kurz- und mittelfristig weder vom generell aggressiven militärischen Verhalten Russlands, noch von einer allfälligen Auseinandersetzung zwischen der Nato und Russland beeinträchtigt wird (Bundesrat 2021, NDB 2021, Armeebotschaft 2022). Der Konflikt in der Ukraine beeinflusst jedoch die gesamteuropäische Sicherheitslage und schafft Unsicherheiten – auch für die Schweiz. Neben den unmittelbaren, beispielsweise humanitären und wirtschaftlichen Konsequenzen des Konflikts sind für die Schweiz auch politische Veränderungen im internationalen Umfeld relevant. Die

4 Beispiele hierfür sind die Anwendung von Völkerrecht im Cyberraum, ein zufriedenstellender Datenschutz, oder den Missbrauch von künstlicher Intelligenz zu verhindern.

Schweiz ist eine starke Verfechterin des Völkerrechts, welches mit Russlands Einmarsch in einen souveränen Staat schwerstens verletzt wurde. Des Weiteren hat die Schweiz u.a. im Sinne ihrer eigenen Sicherheit ein starkes Interesse an einer stabilen, kollektiven europäischen Sicherheitsordnung, sowie einem auf Regeln und demokratischen Werten basierendem internationalen System mit funktionierenden multilateralen Institutionen.

EU – gemeinsame Verteidigungsinitiativen mit unklarer Durchsetzungskraft: Aufgrund beträchtlicher wirtschaftlicher Stärke sowie wichtigen Soft-power-Elementen[5] hat die EU das Potenzial zu globalem Einfluss. Die komplizierte innere Konsensfindung erschwert jedoch die aussenpolitische Positionierung der EU. Der aktuelle Krieg in der Ukraine stellt diesbezüglich einen herausfordernden Test für die EU dar; könnte aber auch als Katalysator dienen, um in Zukunft geeinter und stärker für gemeinsame Interessen einzustehen und die sicherheitspolitische Kooperation zu erhöhen. Bisher hat die EU sich entschlossen gezeigt, beispielsweise durch die strengen Sanktionen gegenüber Russland.

Die komplizierte innere Konsensfindung erschwert die aussenpolitische Positionierung der EU.

In der Verteidigungspolitik hat die EU auf internationaler Ebene bis anhin eine untergeordnete Rolle gespielt. Verschiedene konkrete Initiativen zeugen jedoch vom politischen Willen, die Verteidigungsfähigkeit der Union zu stärken. Diese Bemühungen liefen bisher eher schleppend voran. Die kriegerischen Geschehnisse in der Ukraine mögen der Thematik nun jedoch zusätzliche Dringlichkeit verleihen. Die Emanzipation von den USA sowie die Möglichkeit einer effizienteren Verteidigungspolitik der einzelnen Länder durch verstärkte Organisation im Verbund sind weitere Gründe für die erhöhte Attraktivität einer gemeinsamen Verteidigungspolitik.

Die kumulierten jährlichen Verteidigungsausgaben der EU-Länder betragen 219 Mrd. € (Eurostat 2021). In Folge des Konflikts in der Ukraine hat zum Beispiel Deutschland verkündet, seine Verteidigungsausgaben um 100 Mrd. € zu erhöhen. Obwohl die Verteidigungsausgaben so vermutlich steigen dürften, bestehen Herausforderungen in Verbindung mit Doppelspurigkeiten und Hindernissen bei der Beschaffung. Bisher wurden jährlich schätzungsweise rund 26 Mrd. € aufgrund solcher Probleme verschlungen (Europäisches Parlament 2019). Zudem besitzt Europa als Ganzes 160 verschiedene Waffensysteme, während die USA mit 60 auskommen. Die europäischen Länder kämpfen derzeit also weniger mit einem Mangel an Sicherheitsressourcen als mit organisatorischen und sicherheitspolitischen Herausforderungen (Lago und Schnell 2020).

Diese sollen angegangen werden: Der sogenannte strategische Kompass zielt darauf ab, die Grundlagen für eine gemeinsame Vision für die

5 Soft-power beruht nicht auf militärischer Macht, sondern Vorbildfunktion und Attraktivität von Normen und Werten.

Sicherheit und Verteidigung zu festigen. Aufbauend auf einer gemeinsamen Bedrohungsanalyse für die gesamte EU sollen das Ausmass der strategischen Autonomie geklärt, das Ambitionsniveau der EU definiert und der strategische, operative und fähigkeitsbezogene Bedarf der EU verbessert werden (Europäisches Parlament 2021). Die Pesco [6] und die Europäische Verteidigungsagentur sind neue Instrumente, um Ineffizienzen in Ausbildung, Training und Beschaffung zu beseitigen. Dabei ist man bestrebt, nicht in Konkurrenz zur Nato zu treten, sondern den Beitrag Europas zur Verteidigungsfähigkeit des eigenen Kontinents zu erhöhen (Economist 2019). Die Nato ist die wichtigste kollektive Verteidigungsstruktur für Europa und dürfte es auf absehbare Zeit auch bleiben.

Ehrgeizige Regionalmächte und lokale Brandherde: Die Türkei, die in der Vergangenheit selektiv mit Russland kooperierte, jedoch auch ein Nato-Mitglied und ein wichtiger Partner der EU in Migrationsfragen ist, strebt unter den Regionalmächten am aggressivsten nach einer Ausdehnung der Einflusssphäre.

Ebenso wird der Iran weiterhin um Einfluss ringen. Obwohl Iran Interesse an Verhandlungen mit den USA haben dürfte, ist nicht mit der verlangten Beschränkung des Nuklearprogrammes zu rechnen. Im Hinblick auf Nordkoreas Rüstungsprogramm sind ebenfalls keine signifikanten Erfolge absehbar. Wie der NDB ausführt (2021, S. 65/68), ist die Schweiz jedoch ausser Reichweite der derzeit relevantesten ballistischen Lenkwaffen beider Länder.

Destabilisierungen am Horn von Afrika oder südlich der Sahara dürften Auswirkungen auf Europa und die Schweiz haben. Dies allerdings primär im Bereich der Migration, des Terrorismus und des gewalttätigen Extremismus.

In Libyen und Syrien ist kein Ende der innerstaatlichen bewaffneten Konflikte absehbar. Auch hier dürften sich die Auswirkungen auf die Schweiz aber auf die oben genannten Bereiche beschränken.

Unsichere Zukunft internationaler Institutionen und des Multilateralismus

Autoritäre Staaten mit einem zunehmenden Machtanspruch stellen liberale demokratische Werte und das darauf aufbauende internationale System in Frage. Die verstärkte Konkurrenz zwischen den Staaten erhöht den Fokus auf die eigenen Interessen, was Multilateralismus erschwert und die Handlungsfähigkeit von internationalen Institutionen reduziert.

Autoritäre Staaten mit einem zunehmenden Machtanspruch stellen liberale demokratische Werte und das darauf aufbauende internationale System in Frage.

6 Permanent structured cooperation (ständige strukturierte Zusammenarbeit) existiert seit 2017 und bezeichnet die Zusammenarbeit von Mitgliedstaaten der Europäischen Union (EU) hinsichtlich der gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP). Man beabsichtigt beispielsweise, die Interoperabilität zwischen EU-Mitgliedsstaaten im Wehrbereich zu stärken, indem nationale Streitkräftestrukturen synchronisiert oder gemeinsame Rüstungsprojekte durchgeführt werden. Langfristiges Ziel der EU ist es, ein «militärisches Schengen» bzw. eine europäische Verteidigungsunion zu schaffen.

Streitbeilegung und kollektive Krisenbewältigung werden beispielsweise durch Dissens zwischen den Staaten und Ausübung des Vetorechts behindert. Die Relevanz und der Nutzen der Nato, der Vereinten Nationen und der OSZE (Organisation für Sicherheit und Zusammenarbeit in Europa) werden teilweise öffentlich angezweifelt. Je nach Weiterentwicklung des Konflikts in der Ukraine könnte sich dieser Trend beschleunigen.

Nachdem die Trump-Administration vielen langjährigen Partnern der USA die kalte Schulter gezeigt hat, beteuert Präsident Biden regelmässig Amerikas Rückkehr zum Multilateralismus. Tatsächlich besteht eine Intensivierung der transatlantischen Beziehung zu Amerika als Hauptstandbein der Nato. Gleichzeitig wird aber auch Biden eine faire Lastenverteilung und höhere Verteidigungsausgaben seiner Nato-Verbündeten fordern. Des Weiteren ist die Administration stark von innenpolitischen Herausforderungen absorbiert. Gerade in einer Zeit, die von globalen Herausforderungen verschiedenster Art (bspw. Klimawandel, Pandemiebekämpfung oder expansionistische Ansprüche autoritärer Staaten) geprägt ist, bleibt wirksames multilaterales Handeln also schwierig und internationale Institutionen werden geschwächt.

Gesellschaftliche Polarisierung

Eine Welt, die so globalisiert und vernetzt ist wie noch nie zuvor und zudem einem raschen gesellschaftlichen Wandel unterliegt, führt in nennenswerten Teilen der Bevölkerung zu gewissen Gegenreaktionen. Die letzten Jahre haben eine Erstarkung von Identitätspolitik gesehen: Eigenschaften wie Geschlecht, Ethnie, Sprache, Herkunft oder politische Ausrichtung werden zunehmend in den Vordergrund gestellt. Statt eine offenere und diverse Gesellschaft zu begrüssen, verlangen bestimmte Gruppen Abschottung. Dies kann zu Polarisierung und Fragmentierung der Gesellschaft führen. Die durch die Corona-Pandemie bedingte Verschiebung in den virtuellen Raum erhöht das Risiko von politischer Radikalisierung. Ebenso hat die Pandemie bekanntlich weltweit zu Ausschreitungen und Protesten gegen die Staatsgewalt geführt. Die Gewaltbereitschaft hat sich über verschiedene Gruppen hinweg erhöht (Bundesrat 2021a).

Die durch die Corona-Pandemie bedingte Verschiebung in den virtuellen Raum erhöht das Risiko von politischer Radikalisierung.

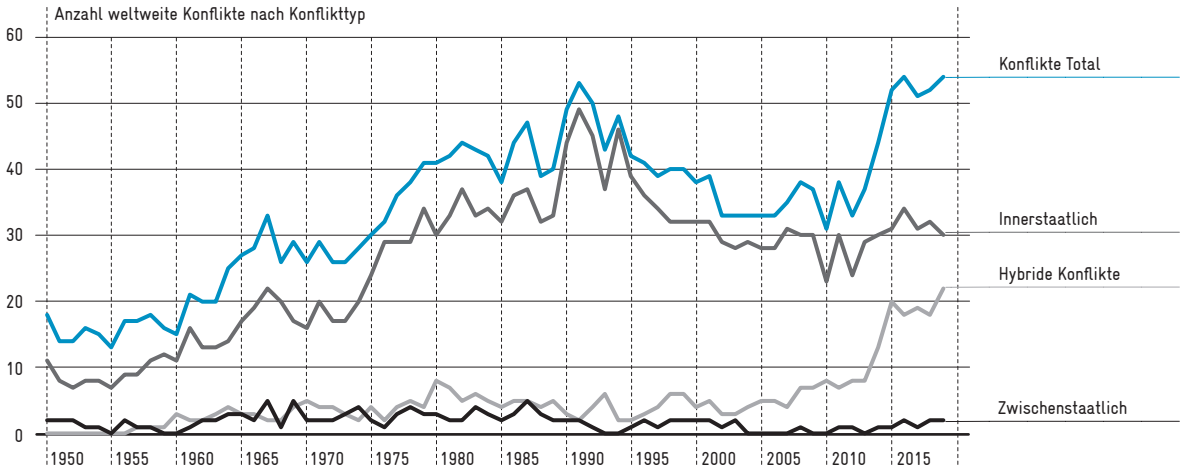
Technologischer Fortschritt

Während politische und wirtschaftliche Regionalisierungstendenzen bemerkbar sind, ist die Welt gleichzeitig aufgrund des technologischen Fortschrittes immer stärker vernetzt. Die Nutzung von Daten und neuen Technologien bietet einen enormen Wettbewerbsvorteil, aber auch Missbrauchspotenzial. Automatisierte Entscheidungen, die kritische Prozesse betreffen, werfen politische, rechtliche und ethische Fragen auf. Autonom gesteuerte Waffen können aufgrund tieferer personeller Risiken die Konfliktbereitschaft und somit das Eskalationspotential erhöhen. Des

Abbildung 2

Hybride Konflikte werden weltweit häufiger

Die Zahl der weltweiten Konflikte lag 2019 bei 53, was seit dem 2. Weltkrieg einem Höchststand entspricht. Die meisten Konflikte sind innerstaatlicher Natur. Neu ist der relativ grosse Anteil hybrider Konflikte.



Quelle: UCDP/PRIO (2021)

Weiteren können Staaten in Abhängigkeit von Akteuren geraten, die führend im Technologiebereich sind, was diesen nicht-staatlichen Akteuren grosse Bedeutung verleiht. Forschungsstätten und Unternehmen im technologischen Bereich werden vermehrt Ziel von Spionageaktivitäten, so auch in der Schweiz (Bundesrat 2021a).

Hybride Konfliktformen

Die beschriebenen machtpolitischen, technologischen und gesellschaftlichen Entwicklungen haben zum Aufstieg eines Konfliktbildes geführt, das oft als «hybrid» bezeichnet wird. Lag die Zahl hybrider Konflikte über Jahrzehnte weltweit im (tiefen) einstelligen Bereich, liegt sie seit 2015 bei rund 20. Damit machen die hybriden Konflikte neu 40 % aller Konflikte aus.

Box 2

Die «hybride» Bedrohung – ein unscharfer Begriff

Hybride Konflikte sind eine Konfliktform, bei der strategische Ziele mit unkonventionellen Mitteln verfolgt werden. Aggressoren handeln in der Grauzone zwischen bewaffnetem Konflikt und Frieden. So sollen Staat, Wirtschaft und Gesellschaft unterhalb der Kriegsschwelle destabilisiert werden. Die verwendeten Mittel sind politischer, wirtschaftlicher, militärischer, nachrichtendienstlicher, informationeller oder krimineller Natur, sollen solange wie möglich unentdeckt bleiben und kommen häufig in Kombination vor. Der Einbezug moderner Waffen und Technologien, insbesondere im Informations- und Cyberbereich, zeichnet hybride Konfliktführung besonders aus. Konkrete Beispiele diesbezüglich sind Cyberangriffe oder Desinformationskampagnen, die darauf abzielen, politische Prozesse zu manipulieren, Institutionen zu unterminieren oder die gesellschaftliche Kohäsion zu schwächen. Verantwortlichkeiten

sollen verschleiert, Einmischungen geleugnet und so Vergeltungsmassnahmen minimiert werden (Torossian et al. 2020).

Obwohl sich hybride Konflikte unter dem Radar des formellen Krieges (nach völkerrechtlicher Definition) abspielen, kann ein offener, bewaffneter Konflikt auch Teil eines hybriden Konflikts sein oder werden. Dies gilt aber als die unwahrscheinlichste, letzte Eskalationsstufe.

Definition als auch Verwendung des Begriffes «hybrid» sind nicht eindeutig, und die Abgrenzung zu anderen Bedrohungskategorien ist schwierig. So betont der Bundesrat im neusten sicherheitspolitischen Bericht, dass neue Bedrohungen die konventionellen nicht ersetzen, sondern zu ihnen hinzukommen (Bundesrat 2021a). Ein künftiger Konflikt könne sowohl im Cyberraum als auch mit konventionellen militärischen Mitteln ausgefochten werden – und zwar gleichzeitig. Die begriffliche Unschärfe begünstigt eine inkonsequente Festlegung von Investitionsprioritäten (vgl. Box 6). *Bezeichnenderweise verwendet das amerikanische Verteidigungsdepartement den Begriff aufgrund seiner Unschärfe in neueren Dokumenten nicht mehr. Er wurde von angelsächsischen Think Tanks so extensiv angewendet, dass seine Begriffsschärfe zunehmend verwässerte.*

2.2_ Weltweite Zunahme der Cyberangriffe

Die Bedrohungslandschaft im Cyberraum ist vielfältig und es ist oftmals eine Vermischung staatlicher (potenziell kriegerischer) Motivationen mit finanziellen Motiven krimineller Organisationen beobachtbar (Torossian et al. 2020).

Die Anzahl weltweit durchgeführter Cyberangriffe ist schwierig zu messen und es muss von einer hohen Dunkelziffer ausgegangen werden. Erstens bleiben viele Angriffe unentdeckt, zweitens melden betroffene Unternehmen auch erkannte Angriffe oft nicht, oder Staaten wollen einen Angriff nicht offiziell anerkennen (Torossian et al. 2020). Doch schon die verfügbaren Daten zu Angriffen auf kritische Infrastrukturen [7] zeichnen ein deutliches Bild: Die Zahl der gegen sie gerichteten und als folgenreich klassifizierten, bekannten Cyberangriffe stieg von sechs im Jahr 2008 auf 49 im Jahr 2018 (vgl. Abbildung 3) (UCDP/PRIO 2021).

Die Attribution von Cybervorfällen ist schwierig und politisch heikel, vor allem wenn kriminelle Organisationen im Auftrag eines Staates operieren. Das Ausmass der staatlichen Beteiligung kann dabei oft nicht eindeutig abgeschätzt werden. Des Weiteren stellt sich die Frage der Verantwortlichkeit von Staaten, die wissentlich Cyberkriminelle von ihrem Territorium aus agieren lassen. Staaten hüten sich davor, Cyberangriffe als bewaffnete Angriffe zu deklarieren, aus Furcht vor einer Eskalation bis hin zu einer Kriegserklärung inklusive Auslösung allfälliger Beistandsverpflichtungen (z.B. Artikel 5 der Nato). Die Zahlen in Abbildung 3 sind entsprechend als konservative Schätzung staatlicher Beteiligung bei Cyberangriffen zu verstehen.

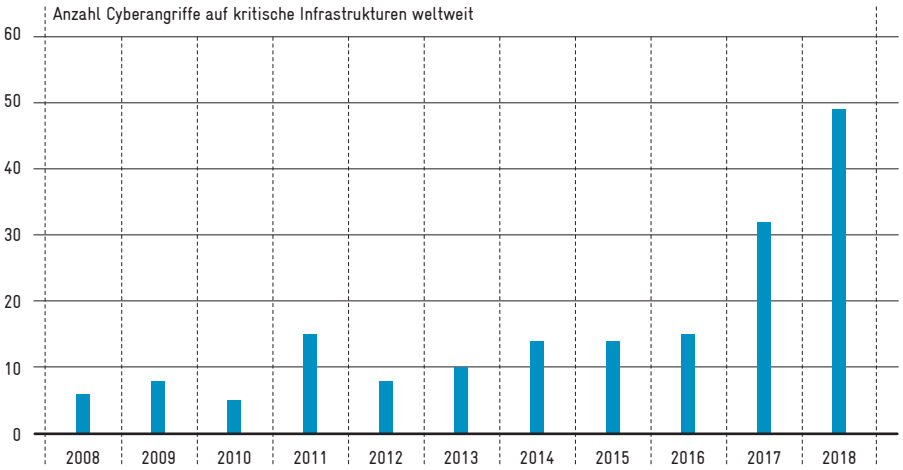
Die Attribution von Cybervorfällen ist schwierig und politisch heikel, vor allem wenn kriminelle Organisationen im Auftrag eines Staates operieren.

7 Systeme, die bspw. Wasser, Energie, Transport, Kommunikation, Lebensmittel oder das Gesundheitswesen betreffen.

Abbildung 3

Die Cyberangriffe werden weltweit häufiger

Die Abbildung zeigt die Entwicklung der Anzahl «folgenreicher», [8] sichtbarer und gemeldeter Cyberangriffe auf kritische Infrastrukturen [9], bei denen das Mitwirken fremder Staaten vermutet wird.



Quelle: CSIS (2021), Torossian et al. (2020)

Beispiele von Cyber-Angriffen

Hybride Cyberbedrohungen können ein erhebliches Risiko für die nationale Sicherheit darstellen. Im Dezember 2020 wurde beispielsweise die gross angelegte Cyberspionagekampagne «Sunburst» öffentlich bekannt (NDB 2021, S. 86): Die Firmen FireEye und Microsoft meldeten, dass unbekannte Täter über den Zulieferer Solarwinds einen Angriff auf zahlreiche Behörden und Unternehmen auf der ganzen Welt lanciert hatten. Insgesamt wurden rund 18 000 der 300 000 Kunden von Solarwinds infiziert. Betroffen waren Regierungsbehörden und Firmen aus den Sektoren Energie, Technologie und Telekommunikation in Nordamerika, Europa, Asien und dem Nahen Osten. Die Angreifer haben unter anderem Penetrationssoftware der profilierten Cybersicherheitsfirma FireEye ausspioniert, die dazu dient, Angriffe auf Behörden und kritische Infrastrukturen zur Erhöhung der Cybersicherheit zu simulieren. FireEye betont, dass Expertise und verwendete Techniken darauf hindeuten, dass der Angreifer von einem Nationalstaat unterstützt wurde (Mandia 2020). Es wird vermutet, dass die Hacker in Verbindung mit dem russischen Geheimdienst standen. Schlagzeilen machte insbesondere der Cyberangriff auf

8 Als folgenreich gelten alle Cyberangriffe auf Regierungsbehörden, Verteidigungs- und High-Tech-Unternehmen sowie Wirtschaftsverbrechen mit Schäden von mehr als 1 Mio. $ *(CSIS 2021)*.

9 Ein Cyberangriff auf kritische Infrastrukturen ist definiert als die Gefährdung, Zerstörung oder der unbefugte Zugriff auf Systeme, die Wasser, Energie, Transport, Kommunikation, Lebensmittel oder das Gesundheitswesen betreffen.

das amerikanische Finanz- und Handelsministerium, der ebenfalls mit der ausspionierten Software von FireEye in Verbindung gebracht wird (NZZ 2020a). Auch mehrere Schweizer Firmen waren von den Sunburst-Hacks betroffen (NDB 2021, S. 87). Jedoch gibt es keine Anzeichen dafür, dass die Angriffe fortgeführt wurden. Demnach waren Schweizer Unternehmen in diesem Fall bisher nur Zufallsopfer eines Cyberangriffs, der prioritär gegen andere gerichtet war.

Das Center for Strategic and International Studies führt eine Liste über bekannte signifikante Cyberangriffe (CSIS 2021), hier zur Illustration bloss ein paar weitere Beispiele:

- Im September 2021 wurde Russland von der EU beschuldigt, Teil einer Cyberkampagne zu sein, die Wahlen und das politische System mehrerer EU-Mitgliedsländer sabotierte, indem seit 2017 mehrere Social-Media-Konten von Regierungsvertretern und Nachrichten-Portalen gehackt wurden, um Misstrauen gegenüber den USA und den Nato-Streitkräften innerhalb Europas zu schüren.
- Ebenfalls im September 2021 meldete die norwegische Regierung eine Reihe von Cyberangriffen auf private und staatliche IT-Infrastrukturen von Akteuren, die von China gesponsert wurden und von dort aus operierten. Die Hacker hätten versucht, geheime Informationen über Norwegens Militär und den Nachrichtendienst zu ergattern.
- Im April 2020 wurden in den Netzwerken der australischen Regierung chinesische Bots entdeckt, kurz nachdem Australien eine unabhängige internationale Untersuchung über die Herkunft des Coronavirus gefordert hatte.
- Im Mai 2021 erfolgte ein Ransomware-Angriff auf die Colonial Pipeline, die grösste Treibstoff Pipeline der USA. Das vorübergehende Abschalten der Pipeline hatte eine unmittelbare Benzinknappheit zur Folge. Hunderte Tankstellen hatten keinen Treibstoff mehr und Bilder von langen Warteschlangen und tätlichen Auseinandersetzungen um das wenige noch vorhandene Benzin gingen um die Welt. Die Auswirkungen der Verwundbarkeit von kritischen Infrastrukturen wurden deutlich vor Augen geführt. Eine aus Russland operierende Hacker Gruppe wurde für den Angriff verantwortlich gemacht.

Eine aus Russland operierende Hacker Gruppe wurde für den Angriff verantwortlich gemacht.

2.3_ Implikationen für die Schweiz

Auch wenn die Schweiz von vielen globalen Entwicklungen nicht direkt betroffen ist: Als neutrales Land inmitten von Europa ist sie von ihrem internationalen Umfeld abhängig, das instabiler, unübersichtlicher und unberechenbarer geworden ist. Stabilisierende Faktoren, die für den Rückgang zwischenstaatlicher Konflikte verantwortlich gemacht werden, sind nicht mehr oder nur noch teilweise vorhanden. Gleichzeitig sind neue Unsicherheitsquellen entstanden. Bewaffnete Konflikte und Krisen an der Peripherie Europas dauern an, haben sich aufgrund machtpoliti-

schen Ringens teilweise noch verschlimmert (Fiott, 2020; NDB, 2020) oder sind gar zu einem offenen bewaffneten Konflikt eskaliert. Die Sicherheitslage in Europa hat sich aufgrund des Krieges in der Ukraine nachhaltig verändert – es sind wesentliche und nicht zu unterschätzende Unsicherheiten entstanden. Eine weitere Eskalation des Konflikts oder der Einbezug weiterer Staaten kann nicht ausgeschlossen werden. Die Nato-Bündnisstärke trägt jedoch dazu bei, dass west- und zentraleuropäische Staaten mit grosser Wahrscheinlichkeit nicht mit einer konkreten territorialen Bedrohung rechnen müssen. Nicht zu vergessen sind aber auch die strategischen und taktischen Atomwaffen Russlands, die zu mehr als nur Droh- und Druckmittel taugen.

3_ Die Sicherheitslage in der Schweiz

Anhand des sicherheitspolitischen Berichts des Bundesrates (NSB-BR), des Lageberichts des Nachrichtendienstes, sowie den Risikoeinschätzungen des Bundesamtes für Bevölkerungsschutz analysiert dieses Kapitel die Relevanz verschiedener Gefährdungen der Schweiz. Generell kann unterschieden werden zwischen sogenannten «nicht mutwilligen» Gefährdungen, also Zwischenfälle, die ohne absichtliches menschliches Einwirken passieren, und «mutwilligen Gefährdungen», also Ereignisse, die absichtlich herbeigeführt werden. Das Bundesamt für Bevölkerungsschutz (Babs) – das dem VBS zugehört – hat im «Bericht zur nationalen Risikoanalyse» die Relevanz verschiedenster Gefahren beider Kategorien zu quantifizieren versucht (Babs 2020).

3.1_ Nicht mutwillige Gefährdungen (Unfälle und Katastrophen)

Zwischenfälle, die nicht durch absichtliches menschliches Mitwirken herbeigeführt werden, wurden gewichtet, indem man das potenzielle Schadensausmass mit der angenommenen Eintretenshäufigkeit multipliziert (vgl. Abbildung 4).

Wie bereits im Risikobericht 2015 schätzt das Babs eine schwere Strommangellage als das grösste Risiko für die Schweiz ein. Unter der Annahme einer Stromunterversorgung von 30 % während mehrerer Monate im Winter wird mit aggregierten Schäden von über 180 Mrd. Fr. – entsprechend etwa 25 % des jährlichen BIP – gerechnet. Ein derartiges Ereignis wird als wahrscheinlicher als eine Pandemie eingestuft, und auf einmal in 30 bis 50 Jahren vorkommend geschätzt. Die Entwicklung dieses Risikos ist von diversen kurz- und mittelfristigen Faktoren abhängig. Kurzfristig könnten Versorgungsengpässe mit russischem Erdgas das mitteleuropäische Energienetz auf eine Probe stellen – wovon auch die Schweiz betroffen sein könnte. Mittelfristig sind mit der Umstellung auf neue erneuerbare Energie Herausforderungen bezüglich Stromversorgungssicherheit im Winter verbunden.

Das Bundesamt für Bevölkerungsschutz schätzt eine schwere Strommangellage als das grösste Risiko für die Schweiz ein.

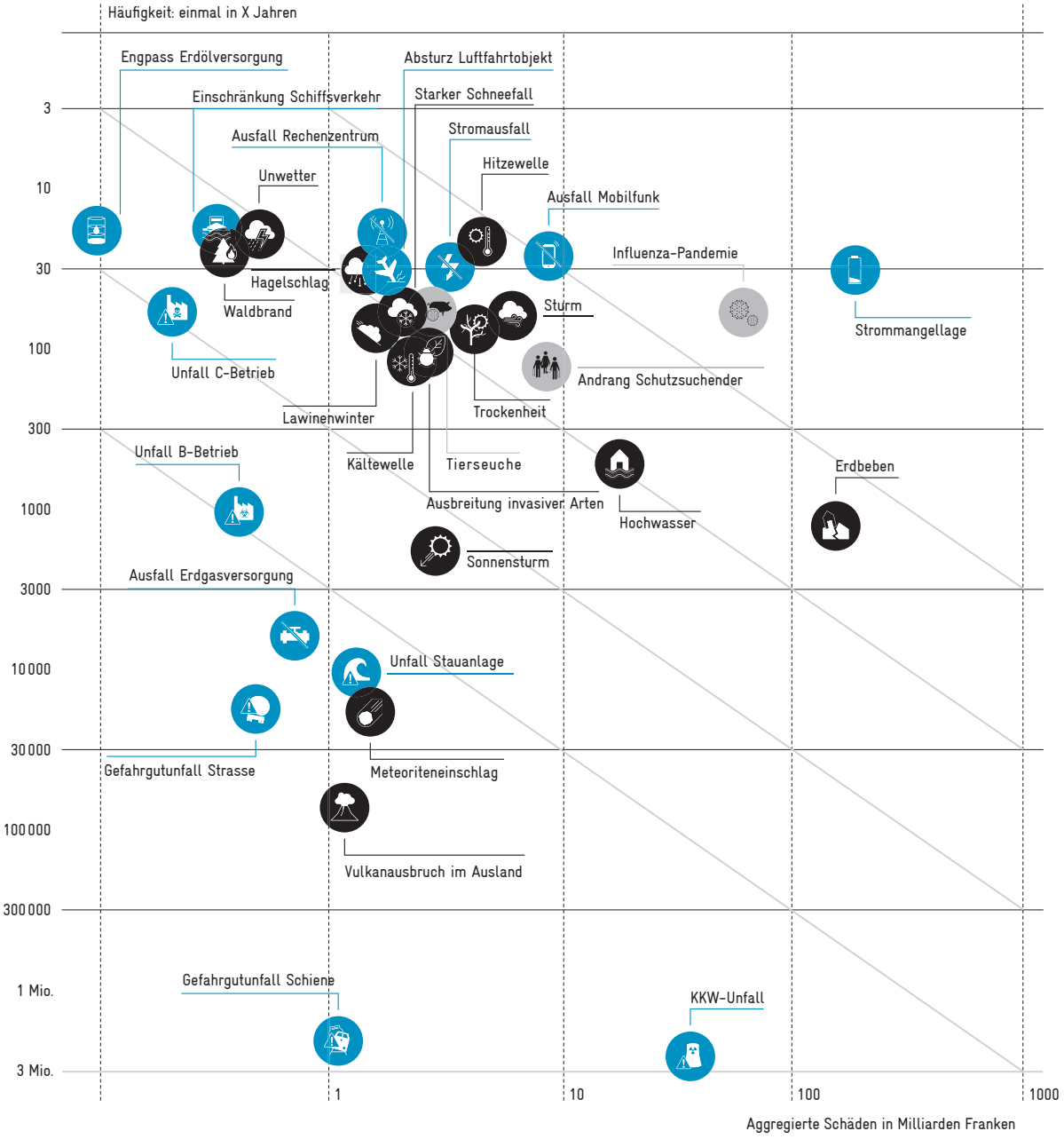
Eine Grippe-Pandemie stellt das zweitgrösste Risiko dar, mit einem Schadensausmass von ca. 60 bis 80 Mrd. Fr. und einer geschätzten Häufigkeit von einmal in 50 bis 80 Jahren. Die Tatsache, dass wir eine solche mit Sars-Cov-2 (auch wenn dieser genau genommen kein Grippevirus ist) gerade durchgemacht haben, garantiert leider (auch bei korrekter Häufigkeitsschätzung) nicht, dass jetzt wieder 50 bis 80 Jahre lang «Ruhe» von einer derartigen Krise herrscht.

Das drittgrösste Risiko stellt ein mindestens dreitägiger Komplettausfall des Mobilfunknetzwerkes in der ganzen Schweiz dar. Das aggregierte Schadensausmass betrüge 8 bis 10 Mrd. Fr. und die Häufigkeit wird auf einmal in 20 bis 30 Jahren geschätzt.

Abbildung 4

Strommangellage, Pandemie und Mobilfunkausfall als grösste Bedrohungen

Die vorstellbaren «nicht mutwillig herbeigeführten Bedrohungen», also im Wesentlichen Unfälle und Naturkatastrophen, hat das Babs nach Häufigkeit und Schadensausmass gewichtet. Je weiter rechts oben ein Punkt, desto relevanter die Gefahr.



Quelle: Bundesamt für Bevölkerungsschutz (Babs) (2020)

Die Armee käme in all diesen Szenarien aus der zivilen Domäne nur subsidiär zum Einsatz. Anders wäre es bei einem Konflikt auf Schweizer Boden.

3.2_ Mutwillige Gefährdungen

Für alle absichtlich herbeigeführten Ereignisse nimmt das Babs in seinem Risikobericht statt einer Einschätzung der Eintretenshäufigkeit eine Plausibilitätsschätzung vor. Dies wohl, weil solche Ereignisse, wie z.B. ein Anschlag mit Bakterien, stark von (schwer prognostizierbaren) geopolitischen und technologischen Entwicklungen abhängig sind und sich daher schlecht auf Basis historischer Erfahrungen quantifizieren lassen, wie dies z.B. für Erdbeben möglich ist. Die Plausibilitätseinschätzung findet jeweils im Rahmen einer Expertenbefragung statt. Die Experten bewerten dabei zwei massgebliche Leitindikatoren: Die «Absicht und Fähigkeiten der Täterschaft» und die «Realisierbarkeit bzw. Machbarkeit des Szenarios».

Bewaffneter Konflikt auf Schweizer Boden

Die Schweiz ist von befreundeten Nato-Staaten und dem neutralen Österreich umgeben. Der Osten Europas ist aktuell jedoch in einen bewaffneten Konflikt verwickelt und generell hat die Schutzwirkung des geografischen und politischen Umfelds der Schweiz abgenommen (Bundesrat 2021a). In der neusten Armeebotschaft (die zwar kurz vor Ausbruch des Krieges veröffentlicht wurde) wird festgehalten (2022, S. 8), dass die Wahrscheinlichkeit, dass in Europa ein bewaffneter Grosskonflikt ausbricht, in den auch die Schweiz verwickelt ist, trotz gestiegener Spannungen zwischen dem Westen und Russland eher gering ist. Bei einem Konflikt zwischen der Nato und Russland könnte die Schweiz allenfalls indirekt militärisch bedroht werden, wenn eine der Konfliktparteien mit militärischen Mitteln wirtschaftliche, politische oder militärische Konzessionen von der Schweiz erzwingen wollte. Jedoch schätzt der Bundesrat auch für das Szenario einer Eskalation zwischen Nato und Russland einen direkten terrestrischen Vorstoss gegen die Schweiz als unwahrscheinlich ein (Bundesrat 2021a). Zudem hielt der Nachrichtendienst vorgängig fest, dass die Schweiz territorial weder vom Streben Russlands, seine Einflusssphäre in Osteuropa zu stärken, noch von Chinas erhöhten militärischen Aktivitäten im Süd- und Ostchinesischen Meer betroffen ist (NDB 2021, S. 20).

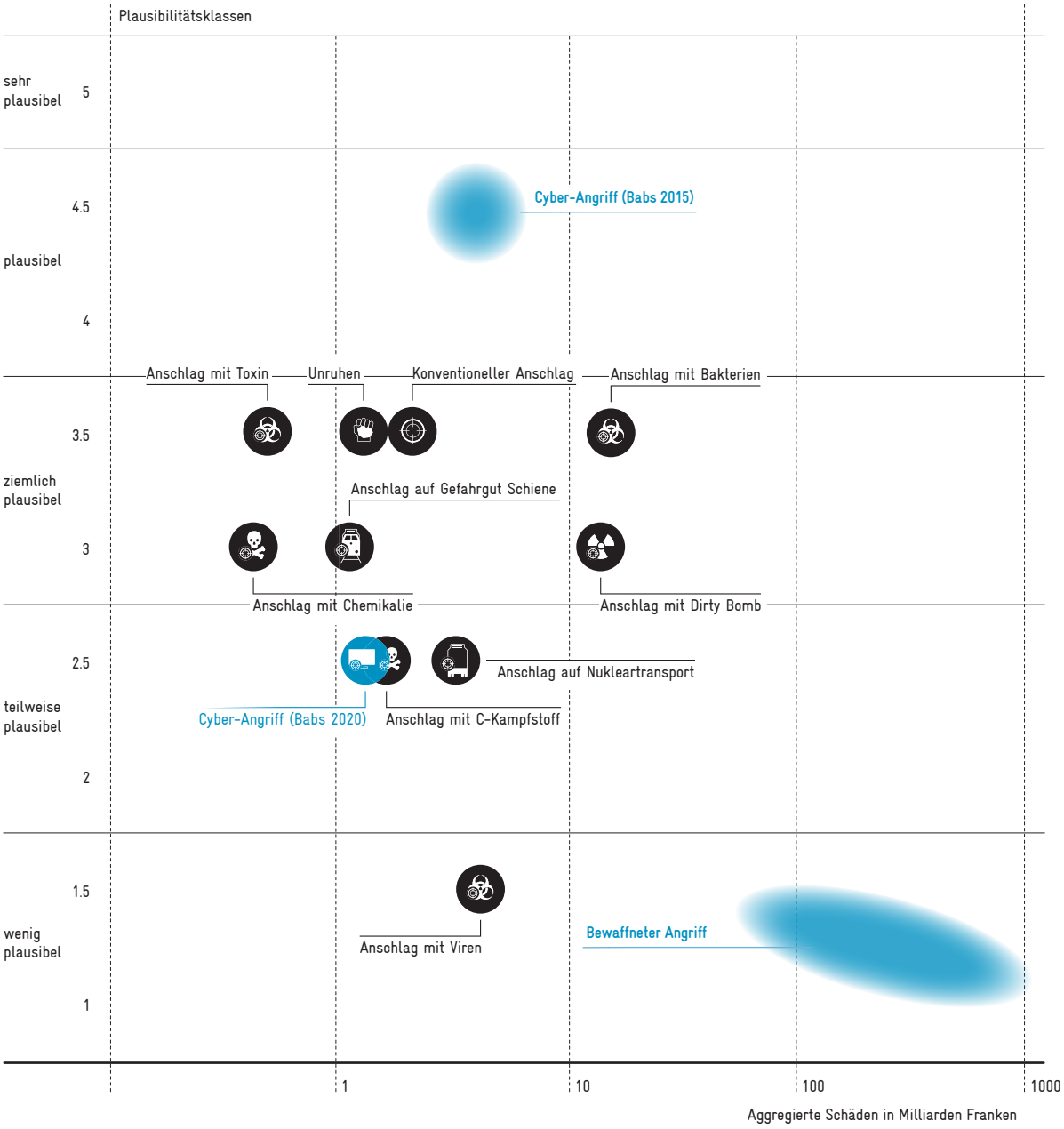
Der Bundesrat schätzt auch im Falle einer Eskalation zwischen Nato und Russland einen direkten terrestrischen Vorstoss gegen die Schweiz als unwahrscheinlich ein.

Diese Aussagen, welche wohlwissend vor Ausbruch des Kriegs in der Ukraine getroffen wurden, finden jedoch auch danach Anwendung, so wurde seitens VBS in diesem Kontext gesagt: «Mit einem direkten militärischen Angriff auf die Schweiz rechnen wir nicht» (VBS 2022). Aus Sicht des Bundesrates müsse das generelle Bedrohungsszenario eines bewaffneten Konfliktes auf Schweizer Boden – u.a. wegen der potenziell hohen Auswirkungen – dennoch ernst genommen werden. Die Höhe dieser Auswirkungen wird im NSB-BR nicht beziffert, während der Risikobericht des Babs sie auf mehrere 100 Mrd. Fr. schätzt (Babs 2020). Das Babs hat dieses Szenario allerdings nicht in der entsprechenden Risikografik (vgl. Abbildung 5) eingetragen (Babs 2020, S. 38) – weil eine Plausibilitätseinschätzung nicht möglich sei.

Abbildung 5

Keine Plausibilitätsschätzung für einen bewaffneter Konflikt in der Schweiz durch Babs und Armee

Das Szenario des bewaffneten Konflikts wurde vom Babs zusammen mit der Armee erarbeitet und wird im Risikobericht mit Verweis auf das potenziell hohe Schadensausmass behandelt. Jedoch wurde keine Plausibilitätseinschätzung veröffentlicht. Die blaue Ellipse entspricht der Einschätzung von Avenir Suisse. Zudem wurde das Szenario Cyberangriff entsprechend der Babs-Risikoeinschätzung von 2015 hinzugefügt und die Verortung des Cyberangriffs 2020 hervorgehoben (vgl. Ausführungen auf S. 30).



Quelle: Babs (2020), ergänzt um Einschätzungen Avenir Suisse

Es mag sein, dass die Plausibilität einer so groben Kategorie wie «bewaffneter Angriff» schwierig einzuschätzen ist. Hier würde es helfen, in Abstufungen zu denken: So ist beispielsweise ein Angriff auf ganz Europa bzw. eine kollektive Verteidigungsanstrengung Europas plausibler als ein alleiniger Angriff auf die Schweiz. Ebenso wäre ein Szenario mit einem isolierten, in seinem Umfang beschränkten bewaffneten Angriff plausibler als das eines grossflächigen territorialen Angriffs auf die Schweiz.

So ist beispielsweise ein Angriff auf ganz Europa bzw. eine kollektive Verteidigungsanstrengung Europas plausibler als ein alleiniger Angriff auf die Schweiz.

Laut NSB-BR muss aber ein bewaffneter Angriff auf die Schweiz nicht mehr zwingend als Vorstoss militärisch organisierter Streitkräfte verstanden werden. «Auch ein Cyberangriff kann demzufolge als bewaffneter Angriff qualifiziert werden, wenn er zu erheblichen Schäden an Personen und Objekten führt» (Bundesrat 2021a, S. 36f.). Schliesslich ist es wahrscheinlicher, dass ein Aggressor die Schweiz mit einer Cyberattacke angreift, also dass der Schutzschirm von befreundeten europäischen Staaten mit konventionellen militärischen Mitteln durchbrochen und die Schweiz territorial bedroht würde. Dies macht jedoch die möglichen Ausprägungen des Szenarios «bewaffneter Angriff» noch vielfältiger und erschwert es, Rüstungsinvestitionen gezielt auf das Risikoassessment eines «bewaffneten Angriffs» auszurichten. Es gilt also jeweils genau hinzuschauen, welche Art von bewaffnetem Angriff als Grundlage für die Investitionsentscheidung herangezogen wird.

Die Analyse des Babs kann trotz gewissen Fragezeigen eine nützliche Orientierungshilfe über mögliche Gefährdungen der Schweiz bieten. Aufgrund unterschiedlicher Zuständigkeiten werden weitere Risikofaktoren, welche in der Vergangenheit bereits eine konkrete Gefährdung dargestellt haben und/oder dies auch in Zukunft werden, jedoch von anderen Behörden thematisiert. Sicherheitsrelevante Ereignisse mit direkten Konsequenzen für die Schweiz fanden abgesehen vom Cyberraum bisher nämlich v.a. aufgrund terroristischer Bedrohungen und verbotenen nachrichtendienstlichen Tätigkeiten statt.

(Cyber-) Angriffe

Die meisten Cyberangriffe in der Schweiz haben einen kriminellen Hintergrund, keinen staatlich-kriegerischen. Gingen 2011 beim Bundesamt für Polizei (Fedpol) 5330 Meldungen im Bereich der Cyberkriminalität ein, sind es inzwischen über 10 000 pro Jahr. Zu den Vorfällen mit dem grössten Schadenspotenzial zählen Verschlüsselungstrojaner (Ransomware). Beispielsweise wurde im Juli 2021 der Vergleichsdienst Comparis Opfer einer Ransomware-Attacke. Um die blockierten Daten wiederherzustellen, bezahlte Comparis das Lösegeld in Höhe von $ 400 000 (NZZ 2021a). In der zweiten Jahreshälfte 2020 sind beim Nationalen Kompetenzzentrum für Cybersicherheit (NCSC) zu Ransomware-Attacken 34 Meldungen aus verschiedenen Wirtschaftssektoren eingegangen (NCSC 2021a). Rund 80 % der Meldungen betrafen KMU.

Die grössten bekannten Cyberangriffe auf die Schweiz, bei denen auch staatliche Motive vermutet werden, betreffen das Labor Spiez und das VBS, sowie die mit dem VBS verbundene Ruag. [10]

Ruag: 2016 wurde ein Cyberangriff auf die Bundesverwaltung über das Einfallstor der Ruag entdeckt. Es wird ein staatlicher Angriff zu Spionagezwecken vermutet. Die Attacke zeigt auf, dass solche Vorfälle lange unbemerkt bleiben können und ihre Attribution schwierig ist. Erst im Januar 2016, mehr als ein Jahr nach dem Eindringen, wurde der Cyberangriff entdeckt und die Bundesanwaltschaft informiert. Gemäss nachrichtendienstlichen Erkenntnissen begann der Angriff aber bereits im Dezember 2014. Der Ruag-Cyberspionagefall wurde durch die Melde- und Analysestelle Informationssicherung (Melani) analysiert (Bundesrat 2016a): Beim Angriff, bei dem mehr als 20 Gigabyte Daten entwendet wurden (SRF 2016), deute alles auf Wirtschaftsspionage hin, teilt die Melani mit. So sei konkret nach aktuell laufenden Projekten der Ruag gesucht worden. Urheberin des Angriffes sei eine Gruppierung im Auftrag eines Staates oder mehrerer Staaten gewesen. Auch fünf Jahre nach dem Cyberangriff gab es noch Sicherheitsmängel (vgl. Kapitel 4.5).

Erst im Januar 2016, mehr als ein Jahr nach dem Eindringen, wurde der Cyberangriff entdeckt und die Bundesanwaltschaft informiert.

Der Cyberangriff auf die Ruag war für die Schweiz ein Warnschuss und hat einige Reaktionen ausgelöst. Seither investiert der Bund verstärkt in die Cybersicherheit, hat nationale Strategien zur Cybersicherheit formuliert, das NCSC geschaffen und die Wichtigkeit der Cyberverteidigung innerhalb der Armee betont.

VBS: Das Verteidigungsdepartement wurde im Jahr 2017 Opfer eines Cyberangriffs (VBS 2017a). Das Communiqué wurde damals sehr kurzgehalten. Einzig bekannt ist, dass der Angriff entdeckt und gestoppt wurde. Die Malwarefamilie Turla sei im Spiel gewesen, welche auch beim Angriff gegen die Ruag im Einsatz stand. Durch diesen Angriff stellte die Führungsunterstützungsbasis, die neu auch für die IT-Systeme der Ruag verantwortlich ist, 2018 fest, dass ihre eigenen IT-Systeme militärischen Anforderungen nicht genügten. Die folgend beschlossenen Massnahmen wurden jedoch noch nicht vollständig umgesetzt. Schwachstellen aufgrund von älteren Systemen und Spezialanwendungen sollen bis 2026 im Rahmen eines Projektes, das neue Rechenzentren und robustere Netzwerkverbindungen umfasst, behoben werden (NZZ 2020b).

Labor Spiez: Im Jahr 2018 wurde auf das Labor Spiez, die schweizerische Fachstelle zum Schutz vor ABC-Angriffen, eine Cyberattacke verübt, die dem russischen Militärgeheimdienst GRU zugeordnet wird. Dessen Spuren wurden bereits 2016 und 2017 in der Schweiz festgestellt (NDB 2019).

10 Die Ruag ist ein Schweizer Technologiekonzern mit Sitz in Bern und hauptsächlich in den Märkten Luft- und Raumfahrt, Verteidigung und Sicherheit tätig.

Das Schweizer Forschungsinstitut war an einer Analyse im Fall des Ex-Doppelagenten Sergei Skripal beteiligt, auf den laut EU Russland einen Anschlag mit dem Nervengift Nowitschok ausgeübt hatte (Tages Anzeiger 2018). Zudem untersuchte das Labor Spiez die Giftgasangriffe im Syrien-Krieg.[11] Der Cyberangriff wurde jedoch vom NDB und dank internationaler Zusammenarbeit verhindert (NDB 2019, S. 79).

Diese Beispiele zeigen deutlich, dass vielfältige Bedrohungen aus dem Cyberraum in der heutigen Schweiz Realität sind. Auch in Zukunft muss laut Nachrichtendienst mit Cyberangriffen gerechnet werden (NDB 2020; NDB 2021). Der Nachrichtendienst hält in seinem neusten Sicherheitsbericht fest, dass der Digitalisierungsdruck aufgrund der Pandemie die Angriffsfläche für Cyberangriffe vergrössert hat, nicht zuletzt aufgrund vermehrter Fernzugriffe, etwa über das Homeoffice. Die zahlreichen Unternehmen in der Schweiz, die Zubehör und Dienstleistungen für die Betreiber kritischer Infrastrukturen im In- und Ausland anbieten, sind auch für Akteure mit staatlichem Hintergrund interessante Ziele (NDB 2021, S. 12). Die Betreiber kritischer Infrastrukturen stehen über alle Sektoren hinweg unter besonders hohem Digitalisierungsdruck (NDB 2021, S. 83):

Diese Beispiele zeigen deutlich, dass vielfältige Bedrohungen aus dem Cyberraum in der heutigen Schweiz Realität sind.

- Der Energiemarkt setzt auf intelligente Messsysteme und Stromnetze, und industrielle Kontrollsysteme werden aus der Distanz nicht nur bedient, sondern auch gewartet.
- Im Gesundheitswesen nimmt die Zahl und die Weiterentwicklung medizinischer Geräte zu, bis hin zu Analysegeräten, die die Patienten tragen und selbst betreiben.
- Die Abdeckung der Schweiz mit der neuesten Generation der Mobilfunktechnologie (5G) wird laufend vergrössert, und in den unterschiedlichsten Branchen wird erprobt, welches Potenzial künstliche Intelligenz bietet.

Weil die Sicherheitsvorkehrungen der Betreiber kritischer Infrastrukturen besser werden, werden Unternehmen, die Ausrüstung und spezialisierte Dienstleistungen für diese Betreiber anbieten, zum bevorzugten Ziel der Angreifer – nicht nur für kriminelle Organisationen, sondern auch für staatliche gesponserte Akteure (NDB 2021, S. 83f.).

Angesichts des Konfliktes in der Ukraine steigt die Relevanz von Bedrohungen aus dem Cyberraum – auch für die Schweiz. So könnte auch die Schweiz gemäss VBS vermehrt zum Ziel von russischen Cyberangriffen, Spionage oder Störungen der kritischen Infrastruktur werden. Hier stationierte ausländische Diplomaten und internationalen Organisationen könnten ebenfalls ein Ziel darstellen. Desinformationsaktivitäten seitens Russlands sind bereits beobachtbar (VBS 2022).

11 Das Labor Spiez arbeitete als Teil des UNO-Ausschusses zur Untersuchung von Chemiewaffeneinsätze in Syrien mit der Organisation für das Verbot chemischer Waffen (OPCW) zusammen.

Risikoeinordnung des Babs wirft Fragen auf: Im Risikobericht des Babs 2015 wies der Cyber-Angriff auf kritische Infrastrukturen noch die höchste Plausibilität aller untersuchten Szenarien auf (vgl. Abbildung 5). Bei der Neueinschätzung der Plausibilität wird im Bericht des Jahres 2020 dem Szenario eine deutlich tiefere Plausibilität zugeordnet als anderen (Babs 2020). Als Grund wird eine methodische Anpassung bei der Bestimmung der Plausibilität durch die Experten genannt.

Dass das Szenario neu bloss noch als «teilweise plausibel» eingestuft wird, ist nachvollziehbar: Das Szenario von 2020 skizziert einen orchestrierten, grossangelegten Cyberangriff, der mehrere Monate andauert und aus vielen einzelnen Cyberangriffen auf kritische Infrastrukturen besteht. Wenig nachvollziehbar angesichts eines so schwerwiegenden Szenarios eines grossangelegten Cyberangriffes ist hingegen das geringer geschätzte Schadensausmass von ca. 2 Mrd. Fr. im Jahr 2020 gegenüber den ca. 8 Mrd. Fr. im Jahr 2015. Gesprächen mit Cyber-Experten zufolge muss bei orchestrierten Cyberangriffen viel eher mit einem Schadenmass zwischen 10 und 100 Mrd. Fr. gerechnet werden.

Gesprächen mit Cyber-Experten zufolge muss bei orchestrierten Cyberangriffen mit einem Schadenmass zwischen 10 und 100 Mrd. Fr. gerechnet werden.

Es wäre wünschenswert, wenn das Szenario «Cyberangriff», stärker im Detail durchdekliniert werden würde. So könnte beurteilt werden, ob die Szenarien realistisch sind, und auf welcher Grundlage die Einschätzung von Plausibilität und Schadenausmass vorgenommen wurde.

Terroristische Aktivitäten

2020 wurden in Europa mehr terroristische Gewalttaten als 2019 verzeichnet, wobei es sich mehrheitlich um Messeranschläge von Einzeltätern handelte (NDB 2020). Zu diesen Terroranschlägen gehören das Tötungsdelikt in der Schweiz in Morges (VD) am 12. September 2020 und der Anschlag in Lugano am 24. November 2020 (NDB 2021). In der Schweiz sind dies die ersten Anschläge seit 2011 (Swissnuclear in Olten SO) und die ersten mit dschihadistischer Motivation (Bundesanwaltschaft 2020). Die Terrorbedrohung in der Schweiz ist und bleibt laut NDB seit November 2015 erhöht. Sie wird weiterhin massgeblich durch die Kernorganisation des «Islamischen Staats» geprägt. Am wahrscheinlichsten werden jedoch Anschläge von autonom agierenden Personen oder Kleingruppen erachtet, deren gewalttätige Orientierung ebenso in persönlichen und psychischen Krisen wie in ideologischen Überzeugungen wurzelt. Da die Ideologie und die diese befeuernden gewaltsamen Konflikte auch in absehbarer Zeit lebendig bleiben, besteht weiterhin eine dschihadistisch motivierte Terrorbedrohung für die Schweiz. Sollte sich die Lage nicht massgeblich ändern (bspw. durch einen wahrgenommenen Anstieg von Feindseligkeit gegenüber Musliminnen, Muslimen oder dem Islam), bleibt die Schweiz aber weiterhin ein sekundäres Ziel für Anschläge. Die Rückkehr von dschihadistisch motivierten Reisenden stellt jedoch eine Herausforderung dar. Ebenso muss festgehalten werden, dass Terrorgruppierungen unterschiedlichen Hintergrunds das Territorium der Schweiz für logis-

tische und finanzielle Unterstützung, sowie Propaganda und Rekrutierungsaktivitäten nützen (Bundesrat 2021a).

Der relativ geringen Anzahl erfolgreicher Anschläge in Europa und der Schweiz stehen mehrere Verhaftungen von Terrorverdächtigen gegenüber. In der Schweiz wurden einige Personen wegen der Beteiligung an der Planung für Anschläge auf Schweizer Territorium verurteilt. Zudem verhing das Fedpol in 2020 gegen 144 Personen eine Einreisesperre aufgrund eines terroristischen Zusammenhangs und wies drei Personen aus, die eine Bedrohung für die innere Sicherheit der Schweiz darstellten (Fedpol 2020a). Massgebende Verhaftungen von Terrorverdächtigen erfolgten zum Beispiel auch im Dezember 2019 in Dänemark, im Januar 2020 in Frankreich und im April 2020 in Deutschland und Spanien. Dies zeigt, dass auch für die innere Sicherheit der Schweiz die transnationale Zusammenarbeit in Europa essenziell ist (Lago und Schnell 2020). Kernstück der transnationalen Polizeizusammenarbeit ist das Schengener Informationssystem (SIS), das gemeinsame elektronische Fahndungssystem. Die Anzahl Treffer auf schweizerische Fahndungen hat dank SIS um stattliche 151 % zugenommen, von 4265 im Jahr 2014 auf 10 725 im Jahr 2020 (Fedpol 2020b).

Die Schweizer Behörden identifizieren jedoch auch zunehmende Gewaltbereitschaft von spezifischen Szenen, wie beispielsweise jene des Links- und Rechtsextremismus. Gewaltpotential ist auch durch organisierte und schwere Kriminalität gegeben. Während Migration nicht in erster Linie eine sicherheitspolitische Herausforderung ist, ordnet ihr der Bundesrat jedoch in Zusammenhang mit gewalttätigem Extremismus, Terrorismus, Menschenhandel und Kriminalität ebenfalls sicherheitsrelevante Auswirkungen zu (Bundesrat 2021a).

Verbotener Nachrichtendienst

Laut dem Lageradar des NDB ist der feindliche Cybernachrichtendienst eine der wahrscheinlichsten Bedrohungen für die Schweiz (NDB 2020; NDB 2021). Während das Ausmass der nachrichtendienstlichen Tätigkeit im Cyberraum vom NDB als klassifizierte Information behandelt wird und eine Quantifizierung deshalb schwierig ist, gilt die Schweiz als einer der Hauptumschlagsplätze für physische nachrichtendienstliche Tätigkeit in Europa: Der NDB beziffert ein Drittel des derzeit akkreditierten Personals offizieller russischer Vertretungen als identifizierte oder verdächtigte Angehörige des russischen Nachrichtendienstes (NDB 2020). Hinzu kommen Informanten, Quellen und Offiziere unter nichtoffizieller Tarnung. Laut Nachrichtendienst des Bundes spioniert neben Russland insbesondere China in der Schweiz, jedoch weniger über den diplomatischen Corps, als unter nichtoffizieller Tarnung in Form von Offizieren, Forschenden, Studierenden und Geschäftsleuten.

Die Schweiz gilt als einer der Hauptumschlagsplätze für physische nachrichtendienstliche Tätigkeit in Europa.

Ein Grossteil der Aktivitäten fremder Nachrichtendienste zielen nicht direkt auf Schweizer Interessen ab. Vielmehr stehen Vertretungen ande-

rer Staaten und internationaler Organisationen im Fokus. Der NDB (2021) rechnet jedoch damit, dass vermehrt führende und in der Schweiz ansässige Unternehmen in den Bereichen Informations-, Chemie-, Pharmatechnologie, Mobilität, erneuerbare Energien und Rüstungstechnik ins Visier von fremden Nachrichtendiensten geraten könnten. Das spezifische Know-How von Schweizer Firmen in der Rüstungsindustrie sowie deren Herstellung von Schlüsselkomponenten machen die Schweiz zu einem attraktiven Ziel dafür (NDB 2021).

4_ Verteidigungsausgaben und geplante Investitionen der Armee

Dieses Kapitel zeigt zuerst vor dem Hintergrund eines internationalen Vergleichs auf, was sich die Schweiz ihre Landesverteidigung kosten lässt. Anschliessend werden die geplanten Investitionen am Boden, in der Luft und im Cyberraum aus ökonomischen und sicherheitspolitischen Gesichtspunkten anhand der Bedrohungslage eingeordnet.

4.1_ Die Kosten der Landesverteidigung

Im Jahr 2020 lagen die Ausgaben für die militärische Landesverteidigung | [12] auf Stufe Bund bei 5,3 Mrd. Fr. (EFV 2021). In den frühen 1990er-Jahren lag das Budget mit über 5,5 Mrd. Fr. höher als heute, gegenüber dem Minimum von 2006 entspricht es dagegen einem Anstieg um 27 %. Der Anteil der Militärausgaben gemessen am BIP hat sich von 2010 zu 2020 kaum verändert (SIPRI 2021). 2020 lag dieser bei 0,8 %. Damit gehört die Schweiz zu den europäischen Schlusslichtern (vgl. Tabelle 1). Pro Kopf berechnet liegt die Schweiz mit 659 $ allerdings im Mittelfeld.

Box 3

Vollkostenrechnung für die Landesverteidigung

Das für das Jahr 2020 offiziell ausgewiesene Militärbudget beträgt 5,3 Mrd. Fr. (EFV 2021). Die vollen Kosten für die Landesverteidigung dürften sich dagegen auf insgesamt rund 8,2 Mrd. Fr. belaufen. Sie kommen wie folgt zustande:

- *Bereits 2012 wies die Milizkommission VBS in ihrer Studie zur «Bedeutung der Armee für die Schweiz» darauf hin, dass weitere staatliche Zusatzkosten in Höhe von 1 bis 1,1 Mrd. Fr. zu berücksichtigen sind (Milizkommission C VBS 2012 S. 29f.). Darin enthalten sind u.a. die Militärausgaben der Kantone und Gemeinden, Budgetanteile VBS an bundesinternen Leistungsverrechnungen und die Militärversicherung.*
- *Zusätzlich fallen private Ausgaben in Höhe von 0,9 bis 1 Mrd. Fr. an, die sich aus den staatlich garantierten Erwerbsersatzzahlungen | [13] und den privaten Lohnfortzahlungen zusammensetzen.*
- *Weiter müssen volkswirtschaftliche (Opportunitäts-)Kosten des Milizsystems addiert werden: Für das Jahr 2012 schätzte die Milizkommission VBS diese auf 0,8 bis 1 Mrd. Fr., wobei als Berechnungsgrundlage der (zivile) Durchschnittslohn der Soldaten diente, und zudem angenommen wurde, | [14] dass die temporäre, wehrpflichtbedingte Bindung des Faktors Arbeit in der Armee die Produktivität der Volkswirtschaft durch ihre Abwesenheit am Arbeitsplatz dämpft.*

---

12 Dies sind ausschliesslich Ausgaben für die militärische Landesverteidigung nach dem GFS-Modell (Government Finance Statistics, international gemäss IMF), das die internationale Vergleichbarkeit gewährleistet. Nicht berücksichtigt sind z.B. die zivile Landesverteidigung oder F&E im Bereich Landesverteidigung. Die Prognosen für 2021 und 2022 belaufen sich auf rund 5,2 Mrd. Fr. *(EFV 2021)*.

13 Als Produkt einer volkswirtschaftlichen Umverteilung zählt die Milizkommission VBS den staatlich garantierten Erwerbsersatz zu den privaten Zusatzausgaben des Milizsystems *(Milizkommission C VBS 2012, S. 30)*.

14 Es wird weiter angenommen, dass die Wertschöpfung eines Arbeitstages dem dafür bezahlten Bruttolohn inklusive Lohnnebenkosten entspricht. Da für die Dauer der durch den Armeeeinsatz bedingten Abwesenheit das entsprechende Kapital keine Wertschöpfung erzielt, ist der erlittene Wertschöpfungsverlust grösser als die Summe der totalen Lohnkosten. Laut Milizkommission VBS bedeutet jeder Tag im Dienst der Armee einen Wertschöpfungsverlust und damit volkswirtschaftliche Kosten in Höhe von Faktor 1,21 des Lohns *(Milizkommission C VBS, S. 37)*.

Berücksichtigt man alle Posten der Vollkostenrechnung (vgl. Box 3), so kumulieren sich die jährlichen Kosten für die Landesverteidigung auf etwa 8,2 Mrd. Fr., was 1,16 % des Schweizer BIP entspricht. Damit würde die Schweiz ins europäische Mittelfeld vorrücken, in Nachbarschaft von Schweden (1,2 % des BIP), Belgien (1,1 %) und Deutschland (1,4 %) – wenn auch zur korrekten Vergleichbarkeit für andere Länder mit Wehrpflichtarmee an sich die gleiche Rechnung gemacht werden müsste. Der Pro-Kopf-Verteidigungsaufwand der Schweiz beliefe sich so gerechnet auf 1013 $. Wir lassen uns unsere Landesverteidigung also – trotz Milizsystem – einiges kosten.

Die jährlichen Kosten für die Landesverteidigung kumulieren sich auf etwa 8,2 Mrd. Fr., was 1,16 % des Schweizer BIP entspricht.

In Folge des Konflikts in der Ukraine wollen allerdings einige europäische Länder massiv aufrüsten. So hat beispielsweise Kanzler Scholz eine Aufstockung der Mittel für die Bundeswehr um 100 Mrd. Euro angekündigt, mit Hilfe derer der Verteidigungsetat mittelfristig auf 2 % des BIP erhöht werden soll, womit er die von den USA wiederholt eingeforderte Nato-Quote erfüllen würde. Die Pro-Kopf-Ausgaben stiegen damit auf 900 $. Auch unter Schweizer Politikern und Politikerinnen werden Forderungen laut, die Verteidigungsausgaben zu erhöhen.

Tabelle 1

Schweiz bei den Verteidigungsausgaben im europäischen Mittelfeld

Verteidigungsausgaben 2020	*absolut (in Mrd. $)*	*pro Kopf (in $)*	*% des BIP*	*% der gesamten Staatsausgaben*
Schweiz (offizielles Militärbudget)	5,7	659	0,80	2,16
Schweiz (gesamte volkswirtschaftliche Kosten)	8,75	1013	1,16	3,08
Irland	1,1	232	0,29	0,98
Österreich	3,6	400	0,84	1,43
Belgien	5,5	471	1,08	1,78
Schweden	6,5	639	1,22	2,29
Deutschland	52,8	630	1,40	2,60
Holland	12,6	734	1,42	2,93
Finnland	4,1	738	1,53	2,55
Frankreich	52,7	808	2,07	3,29
UK	59,2	873	2,25	4,23

Quelle: SIPRI (2021), Eurostat (2021), eigene Berechnungen.

4.2_ Die geplanten Investitionen

Bis im Jahr 2032 ist die Erneuerung aller grossen militärischen Systeme in der Luft und am Boden geplant, gleichzeitig soll die Verteidigung im Cyberraum ausgebaut werden (Armeebotschaft 2020, S. 2273). Um die prognos-

tizierten Investitionen von rund 18,5 Mrd. Fr. über die nächsten zehn Jahre zu finanzieren, wird das Militärbudget auch in Zukunft um 1,4 % pro Jahr erhöht (Armeebotschaft 2022, S. 15). Box 4 zeigt die Aufteilung dieser Investitionen und dient als Basis für die in diesem Kapitel vorgenommene Einordnung der zukünftigen Ressourcenausrichtung der Armee.

Box 4

Die Erneuerung der grossen Armeesysteme innerhalb der nächsten zehn Jahre

Bodentruppen: 7–7,5 Milliarden Franken

Basierend auf dem VBS-Bericht über die Zukunft der Bodentruppen (VBS 2019) entschied der Bundesrat im Mai 2019, dass die Bodentruppen sich stärker auf das «hybride» Konfliktbild ausrichten sollen, und dafür mobiler und modularer einsetzbar sein müssen (Bundesrat 2019a). Mit insgesamt 7–7,5 Mrd. Fr. sollen die Bodentruppen auf Einsätze in überbautem Gelände ausgerichtet werden, anstatt wie bisher abseits von Strassen und Wegen eine weniger mobile Verteidigung zu führen (Hauser et al. 2020).

Die Rüstungsausgaben der Jahre 2018 bis 2021 wurden hier nicht mitgerechnet. Für weitere 3 Mrd. Fr. hat die Armee unter anderem ein neues Aufklärungssystem beschafft und die Nutzungsdauer des Schützenpanzers 2000 verlängert. Unter Einbezug dieser Investitionen käme man bis 2032 auf rund 10,5 Mrd. Fr. für die Bodentruppen.

Luftverteidigung: 8 Milliarden Franken

Die aktuell 30 Kampfflugzeuge des Typs F/A-18 werden 2030 das Ende ihrer Nutzungsdauer erreichen. Basierend auf dem VBS-Expertenbericht über die «Luftverteidigung der Zukunft» (2017b) hat der Bundesrat entschieden, die Mittel der Luftwaffe vollständig zu erneuern und plant die Beschaffung neuer Kampfflugzeuge und Mittel für die bodengestützte Luftverteidigung im Umfang von rund 8 Mrd. Fr. Der Bundesrat legt den eidgenössischen Räten mit der Armeebotschaft 2022 u.a. die Beschaffung von 36 Kampfflugzeugen des Typs F-35A des US-Herstellers Lockheed Martin (für 6,035 Mrd. Fr.) und die Beschaffung von 5 Feuereinheiten des Typs Patriot des US-Herstellers Raytheon (für 1,987 Mrd. Fr.) vor. Laut Bundesrat erzielten die beiden Systeme in der Evaluation den höchsten Gesamtnutzen und gleichzeitig die tiefsten Gesamtkosten (Bundesrat 2021b).

Modernisierung Führungsinfrastruktur (inklusive Cyberanteil): 3,3 Milliarden Franken

Bis ca. 2030 sollen die Führungsinfrastruktur, die IT und die Anbindung an die bestehende Netzinfrastruktur der Armee modernisiert werden (Programm FITANIA). Dafür sollen mit rund 3,3 Mrd. Fr. neue Rechenzentren, ein zusammenhängendes, autonomes Übertragungsnetz («Führungsnetz Schweiz») und ein mobiles Kommunikationsnetz («Telekommunikation der Armee») aufgebaut werden (Armeebotschaft 2020). Ziel ist eine eigene, krisenresistente informations- und kommunikationstechnische Infrastruktur für die Armee, die je nach Lage ergänzend zur zivilen Infrastruktur betrieben würde (Hauser et al. 2020). Ausserdem soll die Führungsunterstützungsbasis (FUB) bis 2024 zu einem Cyberkommando umgebaut werden, um die militärischen Systeme besser schützen zu können.

Von den rund 18,5 Mrd. Fr. an Investitionen werden ca. 15–15,5 Mrd. Fr. für Mittel und militärische Systeme ausgegeben, die vor allem für konventionelle bewaffnete Bedrohungen relevant sind. Nur ein kleiner Anteil der Ausgaben fliesst in die Cyberabwehr zum Schutz der eigenen Militärinfrastruktur. Ob diese Investitionen zur Errichtung einer robusten Cyberabwehr reichen, wird sich zeigen müssen.

4.3_ Bodentruppen

Der Bundesrat hat am 15. Mai 2019 einen Richtungsentscheid für die Modernisierung der Bodentruppen gefällt (Bundesrat 2019a). Die Bodentruppen sollen in Zukunft leichter und mobiler gemacht werden, um sie stärker auf ein hybrides Konfliktumfeld zu fokussieren.

Anstatt jedoch primär auf mobil einsetzbare Systeme zu setzen, die beispielsweise der Abwehr von Terroranschlägen auf das internationale Genf dienen könnten, wird vor allem die Nutzungsdauer bestehender konventioneller Systeme (Schützenpanzer, Radschützenpanzer, Bergepanzer) verlängert. Für die Jahre 2021 bis 2024 ist die Revision der Fahr- und Lenkgetriebe an den Panzern 87 Leopard sowie die Verlängerung der Nutzungsdauer der Bergepanzer 01 vorgesehen (Armeebotschaft 2020). Die geplanten Investitionen fliessen also zu grossen Teilen in schwere Panzersysteme und in die Artillerie. Begründet wird dies mit dem Grundlagenbericht zur Zukunft der Bodentruppen, wo auf das Konzept des «hybriden Konfliktes» verwiesen wird, innerhalb dessen die Armee aber auf die klassischen bewaffneten Anteile hybrider Konflikte am Ende des Eskalationsspektrums fokussiert (vgl. Box 5). So wird die Verlängerung der Nutzungsdauer der Schützenpanzer 2020 beispielsweise folgendermassen begründet (Armeebotschaft 2020, S. 2288 ff.): Die mechanisierten Verbände brauchen die 154 Schützen- und 32 Kommandoschützenpanzer auch in Zukunft, denn «reguläre (gegnerische) Verbände, ausgerüstet mit Panzern und Artillerie, könnten an den Grenzen aufmarschieren» und so die Schweiz bedrohen (VBS 2019, S. 30; siehe auch VBS 2019, S. 99 ff.). Das Konzept der Territorialverteidigung mag angesichts der aktuellen Geschehnisse in der Ukraine wieder an Brisanz gewonnen haben. Trotzdem wäre eine Erörterung dazu, wie ein solches Szenario im gesamteuropäischen Kontext realistischerweise auf Schweizer Boden entstehen soll, hilfreich, wenn damit so umfassende Investitionen begründet werden.

Die geplanten Investitionen fliessen zu grossen Teilen in schwere Panzersysteme und in die Artillerie.

Die beantragte Lösung ist laut Armeebotschaft die wirtschaftlichste, weil die Alternativen zum selben Preis mit Ausrüstungslücken oder einer Reduktion von Kampfverbänden verbunden wären. Eine solche Alternative zu den Schützenpanzern wären zum Beispiel die leichteren und mobileren Radschützenpanzer, die dem gegenwärtigen Stand der Technik, dem Einsatzumfeld und der bewaffneten Bedrohung in urbanem Gebiet besser entsprächen (Armeebotschaft 2020, S. 2288 ff.). Dass zum gleichen Preis weniger Radschützenpanzer beschafft als Schützenpanzer ersetzt werden könnten, könnte gerechtfertigt werden, wenn mit den Radschützenpanzern der urbane Kampf wendiger geführt werden kann, wie die Rüstungsexperten der Armee darlegen. Falls das Militärbudget für die erstrebte Fähigkeit tatsächlich nicht ausreicht, dann sollten die Militärplaner dies transparent darlegen (und womöglich Zusatzmittel beantragen), statt die Schützenpanzer als eine passable Alternative zu bezeichnen. Nur so kann ein Fähigkeitsdialog entstehen. Ob dann tatsächlich Radschützenpanzer beschafft würden, sei dahingestellt.

Box 5

Fokus auf konventionelle Rüstungsausgaben in Folge der Unschärfe der «hybriden Bedrohung»

Dass hybride Bedrohungen aus konventionellen und unkonventionellen Anteilen bestehen, und diese gleichzeitig und vermischt auftreten können, bestreitet niemand. Allerdings können begriffliche Unschärfen in hybriden Sicherheitskonzepten in Lagebeurteilungen die sicherheitspolitische Prioritätensetzung behindern. Wenn in «hybrid» ausgerichteten Sicherheitsstrategien alle möglichen Eskalationsstufen und Arten eines Konfliktes, unabhängig von der Lagebeurteilung, gleichermassen abgedeckt werden sollen, besteht die Gefahr, dass die konventionelle Aufrüstung übergewichtet wird.

So betont das VBS in den Lagebeurteilungen seiner Armeebotschaften (2020; 2021; 2022) zwar, dass der Cyberraum einen prioritären Stellenwert innehat, um künftige Beschaffungen im Rahmen «hybrider» Bedrohungen zu rechtfertigen. Die Mittelaufteilung spiegelt aber nicht wirklich eine derartige Prioritätensetzung.

4.4_ Luftverteidigung

Die Schweiz muss ihren Luftraum sowohl in der normalen als auch in einer mittleren Spannungslage[15] schützen können, um ihren Beitrag für die kollektive Sicherheit in Europa zu leisten. Die Gewährleistung einer effektiven Luftverteidigung ist für die Schweiz als Zentrum internationaler Organisationen, Gipfel (bspw. das WEF in Davos) und als Mediationsstandort von besonderer Bedeutung. Ohne ein Dach über dem Kopf liessen sich zudem die Bodentruppen, die übrigen Teile der Armee und die anderen sicherheitspolitischen Instrumente nicht mit Aussicht auf Erfolg einsetzen.

Ohne ein Dach über dem Kopf liessen sich die übrigen Teile der Armee nicht mit Aussicht auf Erfolg einsetzen.

Dafür sollen für 8 Mrd. Fr. neue Kampfjets und eine bodengestützte Luftverteidigung beschafft werden. Bei den Jets handelt es sich um 36 Flugzeuge des Typs F-35A des US-Herstellers Lockheed Martin. Weitere europäische Länder wie Finnland, das Vereinigte Königreich, Italien, Holland, Norwegen, Dänemark, Polen, Belgien und zuletzt Deutschland haben Interesse an den F-35 Jets bekundet, oder diese bereits erworben (Lockheed Martin 2022). Die Kompatibilität der europäischen Luftwaffen kann die Möglichkeiten zur effektiven Zusammenarbeit erhöhen.

Ordnungspolitisch fragwürdige Offsetgeschäfte

Der Kauf der Schweizer Jets wurde wie üblich an die Bedingung umfangreicher Offsetgeschäfte geknüpft. Statt wie bisher das Rüstungsgeschäft mit 100 % zu kompensieren, hat sich das Parlament bei der Beschaffung der neuen Kampfflugzeuge im Umfang von rund 6 Mrd. Fr. zwar auf eine Quote von «bloss» 60 % geeinigt. Doch auch das dürfte die Kampfjetbeschaffung um 150 Mio. bis 600 Mio. Fr. verteuern (vgl. Box 6). Der Steu-

15 Damit sind beispielsweise Flugzeugentführungen, unbefugtes Eindringen in den Schweizer Luftraum, Terroranschläge aus der Luft oder Luftschläge geringer Intensität gemeint.

erzahler bezahlt hier für industriepolitische Partikularinteressen, die mit einem überholten merkantilistischen Weltbild – möglichst viel Wertschöpfung im Land zu bewahren – begründet werden.

Box 6

Offsets verteuern die Rüstungsgeschäfte

Offsets sind Gegengeschäfte, beziehungsweise Kompensationsgeschäfte, die auch bei Rüstungsbeschaffungen im Ausland die Wertschöpfung sicherheitsrelevanter Technologien im Inland sicherstellen sollen. Ein ausländischer Anbieter willigt also in Geschäfte mit Firmen aus dem Land des Käufers ein. Nur wenige Länder mit Offsets kennen eine hundertprozentige Kompensation, neben der Schweiz sind es v.a. Dänemark, Norwegen, Kanada und Brasilien. Letztlich widerspricht diese Praxis den Grundsätzen des freien Handels.

Gemäss Armasuisse (2021) sollen Gegengeschäfte die sicherheitsrelevante Technologie- und Industriebasis (STIB) der Schweiz stärken. Dazu zählen Forschungseinrichtungen und Unternehmen, die in der Schweiz über Kompetenzen, Fähigkeiten und Kapazitäten im sicherheits- und wehrtechnischen Bereich verfügen. Dies sind insbesondere die Maschinen- und Metallindustrie, die Bereiche Elektronik und Elektrotechnik sowie Optik. In Frage kommen auch die Uhrenindustrie, der Fahrzeug- und Waggonbau, die Bereiche Gummi und Plastik, die Chemieindustrie, Luft- und Raumfahrtindustrie sowie Informatik- und Software-Unternehmen. Tatsächlich entfallen die Gegengeschäfte allerdings zu 40% auf indirekte Offsets ohne Sicherheitsrelevanz, zu weiteren 40% auf indirekte Offsets innerhalb der STIB, aber ohne direkten Bezug zum Rüstungsgeschäft, und bloss zu 20% auf direkte Offsets innerhalb der STIB, wo die Hersteller direkt mit dem Rüstungsgut in Verbindung stehende Gegengeschäfte eingehen, z.B. einzelne Komponenten der neuen Kampfjets herstellen. Die Etablierung eines F-35 Cyber Centers zur Evaluierung von Cyber-Bedrohungen ist jedoch ein erwähnenswerter Bestandteil der vorgesehenen Offset Geschäfte. Dies stärkt die Fähigkeiten der Schweiz in der Cyberverteidigung und adressiert somit eine der relevantesten Gefährdungen.

Fragwürdig ist jedoch die strikte Verteilung der Offsets nach regionalpolitischen Kriterien: Generell sollen 65% der Geschäfte von Firmen aus der Deutschschweiz, 30% aus den französisch- und 5% aus den italienischsprechenden Landesteilen kommen. Damit entlarven sich die Offset-Geschäfte zu Teilen als Industrie- und Standortpolitik.

Die Offsetgeschäfte verteuern Rüstungsbeschaffungen: Grüter (2019) schätzt, dass Offsetgeschäfte die Kosten für Rüstungsbeschaffungen in der Schweiz um 5% bis 20% des Volumens der Offsets erhöht. Das liegt zum einen daran, dass die Handelspartner die Verpflichtung zu Gegenschäften in Preisaufschlägen abbilden. Zudem entstehen bei Offset-Geschäften Transaktionskosten (Aufwand der Offset-Verpflichteten und des Schweizer Controllings).

Aufholbedarf beim Schutz gegen Drohnen

Moderne Konflikte sind nicht mehr so stark territorial gebunden und werden zuweilen auch von nichtstaatlichen Akteuren ausgetragen. Moderne Luftkriege werden nicht nur mit Kampfflugzeugen, sondern auch mit Drohnen, Marschflugkörpern und Raketen ausgefochten. Dies hat der Berg-Karabach-Konflikt exemplarisch aufgezeigt: Drohnen und (Boden-Boden-)Lenkwaffen schalteten in grossem Stil armenische Panzer aus und waren kriegsentscheidend (CSIS 2020). Teure und schwer mechanisierte Kräfte wie Panzer werden vermutlich vermehrt von den viel kostengünstigeren Drohnen und Lenkwaffen angegriffen, die nicht nur billiger sind als Kampfjets, sondern auch nahezu risikofrei ihre Wirkung

entfalten. So werden beispielsweise auch Drohnen benutzt, um im Konflikt in der Ukraine wichtige russische Infrastruktur wie Flugabwehreinheiten ausser Gefecht zu setzen. Bei solchen Drohnen handelt es sich nicht nur um grosse, unbemannte Kampfdrohnen, sondern auch um kleine, wendige «Suizid- oder Kamikaze-Drohnen», die Freizeitdrohnen ähneln. Diese Drohnen, die man sich als fliegende Kleinstbomben vorstellen kann, können einzeln eingesetzt werden, um unbemerkt konkrete menschliche Ziele oder militärische Hardware anzufliegen – oder auch in Schwärmen, mit dem Ziel, dass mindestens einige der Drohnen ihr Attentatsziel erreichen. Weil die Drohnen günstig beschafft werden können, könnten sie auch von mittelstarken Mächten oder von Terrorgruppierungen und Aufständischen eingesetzt werden. Je militarisierter und ausstattungsstärker ein Gegner ist, desto stärker werden Alltagsdrohnen künftig zu eigentlichen Kampfrobotern ausgerüstet, bis zur künstlichen Intelligenz mit Gesichtserkennung, die es erlaubt, gezielt Offiziere, Terroristen und gegnerische Soldaten vollautonom zu neutralisieren. Deshalb gewinnen beispielsweise für Grossbritannien (vgl. Kapitel 5.1) Drohnen im Vergleich zu Kampfjets und Panzer an Bedeutung (UK Verteidigungsministerium 2021; UK Government 2021).

Ist die Schweiz auf einen Terroranschlag mit Lenkwaffen oder Drohnen gegen einen Flughafen oder während eines internationalen Gipfels (beispielsweise in Genf) vorbereitet? Hochfliegende, grosse Drohnen lassen sich gemäss VBS mit Kampfflugzeugen sowie der bodengestützten Luftverteidigung abwehren. Tiefliegende kleine Drohnen, die künftig vermehrt auch in Schwärmen eingesetzt werden dürften, seien jedoch schwer zu erfassen und abzuwehren (Armeebotschaft 2022, S. 13). Der ehemalige Armeechef Blattmann weist darauf hin, dass die Schweiz gegen Drohnenangriffe im untersten Luftraum zurzeit wehrlos ist (NZZ 2021b). Dies wird vorerst auch so bleiben, wie das VBS selbst bestätigt: Das neue Bodluv-System des Typs Patriot des US-Herstellers Raytheon, das für knapp 2 Mrd. Fr. beschafft werden soll, kann die Schweiz weder gegen Drohnen im unteren Luftraum noch gegen Lenkwaffen schützen (VBS 2021a). Die Beschaffung von Systemen für die bodengestützte Luftverteidigung kleinerer Reichweite sollen «aufgrund der Ressourcenlage» erst gegen Ende der 2020er Jahre eingeleitet werden (VBS 2017b, S. 162).

Der ehemalige Armeechef Blattmann weist darauf hin, dass die Schweiz gegen Drohnenangriffe im untersten Luftraum zurzeit wehrlos ist.

Gemäss Armeebotschaft 2022 (S. 13) prüfe der Bund aktuell, welche Auswirkungen die Drohnentechnologie auf die Sicherheit der Schweiz habe, wie sich die Schweiz gegen Angriffe, die mit Drohnen geführt werden, schützen kann und welche Behörden in diesem Bereich zuständig sind. Das VBS beantragt einen Kredit zur Prüfung von Möglichkeiten eines Systems, das Mini-Drohnen ortet, identifiziert und allenfalls neutralisiert (Armeebotschaft 2022, S. 62). Der Schutz vor Drohnenangriffen fällt bislang in die Zuständigkeit der Kantone, solange die Drohnen weniger als 20 Kilogramm schwer sind (Bundesrat 2019b). Die Kantone stehen in ihrer Planung jedoch noch am Anfang. Potenziell ist die (Luft-)Sicherheit der Schweiz

in Frage gestellt, weil Drohnen und Lenkwaffen im Konfliktfall die Luftwaffe der Schweiz funktionsuntüchtig machen könnten, da sie unter dem Radar gezielt militärische Luftstützpunkte angreifen könnten.

Transnationale Kooperation

In der Armeebotschaft 2022 wird festgehalten, dass eine Krise im Luftraum mit hoher Wahrscheinlichkeit nicht nur die Schweiz, sondern auch die Nachbarstaaten und das weitere Umfeld betreffen würde. Eine völlig autonome Luftverteidigung gegen einen Angriff eines mächtigen Gegners, der seinen Angriff auf die Schweiz konzentriert, sei zudem aus Ressourcengründen nicht realistisch. Wird die Schweiz militärisch angegriffen, könne die Luftverteidigung demnach zusammen mit Kooperationspartnern geführt werden (Armeebotschaft 2022, S. 12). Die Schweiz wird im Ernstfall ihren Luftraum also im Verbund schützen, weshalb Investitionen in die Luftsicherheit im Sinne der kollektiven Sicherheit gedacht werden sollten. Deshalb ist es plausibel, dass die Schweiz den Kampfjettyp F-35 beschafft, denn dieser wird nicht nur von mehreren europäischen Staaten benutzt, sondern ist spezifisch für Angriffs-Einsätze in einem militärischen Verbund (der Nato) konzipiert (US-Kongress 2012). Um das Potenzial des neuen Kampfjets mit dem grösstmöglichen Nutzen auszuschöpfen, sollte aber eine ernsthafte transnationale Verteidigungspolitik im Rahmen der Nato angestrebt werden. Dies würde eine stärkere Annäherung an die Nato und die europäischen Verteidigungsinitiativen und damit einen pragmatischeren Umgang mit der Neutralität bedeuten (vgl. Kapitel 6). Dazugehören könnten gemeinsame militärische Übungen und Einsätze, wie dies auch andere neutrale und blockfreie Staaten wie Schweden (vgl. Kapitel 5) praktizieren. Zudem könnte sich die Schweiz so des Verdachtes entledigen, als Freerider vom Nato-Schutzschirm profitieren zu wollen.

Die Schweiz wird im Ernstfall ihren Luftraum im Verbund schützen, weshalb Investitionen in die Luftsicherheit im Sinne der kollektiven Sicherheit gedacht werden sollten.

Das VBS verzichtet aber darauf, die Beschaffung der neuen Kampfjets in erster Linie mit der kollektiven Verteidigung innerhalb eines Verbundes zu begründen. Die Schweiz müsse das Ziel haben, das ganze Spektrum der Luftverteidigung abzudecken, vom Polizeidienst in der normalen Lage bis zum konventionellen Luftkrieg (VBS 2017b, S. 68). Der ausschlaggebende Faktor für die bundesrätliche Bestimmung der zukünftigen Flotten-Mindestgrösse von 30 Kampfflugzeugen (Bundesrat 2019c) war die Forderung, dass die Schweiz auch einen Luftkrieg bei einer «langanhaltenden Spannung» [16] für mindestens vier Wochen alleine führen können muss. Obwohl die Nato zum gegenwärtigen Zeitpunkt nicht vorhat, in den Krieg in der Ukraine militärisch direkt einzugreifen, kann ein bewaffneter Konflikt zwischen Russland und der Nato nicht mehr mit Sicherheit ausgeschlossen werden. Die Schweiz wäre von einem solchen

16 Damit ist die Verteidigung vor Angriffen im und aus dem Luftraum, bis hin zu einem Luftkrieg oder einen kombinierten Luft-/Landkrieg gemeint *(Bundesrat 2019c, S. 21; VBS 2017b, S. 68)*.

aber nicht spezifisch oder alleinig betroffen. Ein realistischer Worst-Case würde eine Verteidigungsanstrengung im Verbund bedingen.

Die Schweiz muss ihren Luftraum schützen können. Die Investitionen in Verbundkampfflugzeuge entfalten aber ihren vollen Nutzen nur, wenn die Schweiz sich stärker neutralitätskompatibel in die transnationalen kollektiven Nato-Strukturen einbindet und das plausibelste Angriffsszenario vorab üben kann (vgl. Kapitel 6.2).

4.5_ Cyberverteidigung

Russland hat sich beim Einmarsch der Ukraine sowohl auf konventionelle militärische Hardware wie auch auf unkonventionelle Mittel wie Cyberangriffe verlassen. Gemäss Expertenmeinungen seien die Cyberangriffe bisher jedoch relativ unkoordiniert gewesen und hätten zu einem Grossteil aus Desinformationskampagnen bestanden. So wird die Relevanz und der strategische Nutzen von Cyberangriffen in einem tatsächlichen kriegerischen Konflikt hinterfragt, da diese den hohen Erwartungen oftmals nicht gerecht werden (Maschmeyer 2021). Obwohl der Stellenwert von Cyberangriffen in einem Konfliktfall unklar sein mag, sind sie aufgrund ihrer zunehmenden Häufigkeit und potenziellem Schadensausmass ein ernstzunehmendes Bedrohungsszenario. Des Weiteren hält das VBS spezifisch fest, dass die Schweiz vom Angriffskrieg Russlands in der Ukraine durch Cyberattacken und Spionage indirekt betroffen werden könnte (VBS 2022). Aus diesem Grund ist der Schweizer Cyberverteidigung nicht nur im Kontext der aktuellen Situation im Osten Europas besondere Aufmerksamkeit zu widmen.

Die 3,3 Mrd. Fr. für die Modernisierung der Führungsinfrastruktur fliessen primär in den Aufbau einer krisenresistenten Informations- und Kommunikationsinfrastruktur, die im Jahr 2035 gänzlich abgeschlossen sein wird. Unter dem Projektnamen Fitania wird die ganze Informatik erneuert, inklusive dem Führungsnetz und den Funk- und Kommunikationssystemen der Armee (Schweizer Armee 2021a). Zudem wird die Führungsunterstützungsbasis (FUB) der Armee bis Anfang 2024 in ein Kommando Cyber weiterentwickelt. Des Weiteren will die Armee mit dem Kommando Cyber langfristig den Cyberschutz der IKT-Infrastrukturen des VBS garantieren und gleichzeitig Kapazitäten und Fähigkeiten aufbauen, um subsidiäre Unterstützungsleistungen zugunsten ziviler Behörden anzubieten. Letzteres wird vom VBS in der neuen Cyberstrategie als ein Ziel der Cyberverteidigung definiert. Offen ist, inwiefern die subsidiären Aufgaben der Armee mit den Kernaufgaben des Nachrichtendienstes überlappen. Die Armee möchte sozusagen in neue (zivile) Gebiete expandieren: Im Falle eines Sabotageversuchs mit Cyberangriffen gegenüber der Energieversorgung möchte das Militär beispielsweise in Zukunft die Netz- oder Kraftwerksbetreiber unterstützen (NZZ 2021c), was aber eigentlich in den Verantwortungsbereich des NDB in Absprache mit dem NCSC fällt. Zudem hat die VBS-Vorsteherin eine Cyber-Interventions-

Offen ist, inwiefern die subsidiären Aufgaben der Armee mit den Kernaufgaben des Nachrichtendienstes überlappen.

truppe andiskutiert (Tages Anzeiger 2020), die neben den Betreibern kritischer Infrastrukturen auch Privatunternehmen bei der Abwehr von Attacken unterstützen soll. Die neuste Armeebotschaft betont ebenfalls die Wichtigkeit der Cyberverteidigung und sieht in verschiedenen Bereichen Investitionen darin vor.

Die Cybersicherheit der Armee

Die Modernisierung der Informatikinfrastruktur der Armee wird erst in 2035 abgeschlossen sein (Schweizer Armee 2021a). Wobei die Einhaltung dieser Frist nicht garantiert ist. Die Personalressourcen reichen laut Armee nicht aus, um die jährlichen Ziele des Modernisierungsprojekts zu erfüllen. Für Informatikprojekte verfüge sie über ca. 100 Vollzeitstellen. Benötigt würden laut Armeesprecher weitere 300 Mitarbeiter für die Integration, den Unterhalt und den Betrieb der IT-Systeme. Für die Erfüllung wichtiger Projektmeilensteine wurden externe Dienstleister beauftragt. 2021 wird das Informatikbudget laut dem Armeesprecher um rund 100 Mio. Fr. überschritten (Tages Anzeiger 2021). Dies sei kein temporärer Engpass, sondern habe mit einer chronischen Überlastung der Armee-Informatik zu tun. Laut Prognosen der Armee könnten deshalb die Informatikausgaben – statt der bisherigen 460 Mio. Fr. – auf jährlich über 600 Mio. Fr. steigen. Rund 3,3 Mrd. Fr. für die Modernisierung der Informatikinfrastruktur reichen bis 2035 unter Umständen also nicht aus.

Um die militärisch heiklen Daten und IT-Systeme in Zukunft besser zu schützen, beschloss der Bundesrat im März 2018, die Ruag und ihre IT-Systeme per 1. Januar 2020 in Ruag Schweiz (Ruag MRO) und Ruag International aufzuspalten (Bundesrat 2020a). Die IT-Sicherheit der Ruag Schweiz, die unter anderem die Kampfjets wartet, sollte erhöht werden, indem sie neu in die Verantwortung der FUB gestellt wurde. Dies ist die Organisation, die zum Cyberkommando und zur krisenresistenten Kommunikationsinfrastruktur der Armee und des Bundes heranwachsen soll (NZZ 2020c). Die FUB selbst war mit Cybersicherheitsproblemen konfrontiert. So waren die Festplatten auf den Rechnern nicht verschlüsselt, weshalb sie im Fall eines Diebstahls nicht geschützt gewesen wären. Ausserdem waren potenzielle Eintrittspforten ins FUB-Netzwerk und damit in die Bundesverwaltung offen. Die Armee habe zudem den Bund ungenügend über den Vorfall informiert, und erhöhte damit das Sicherheitsrisiko für die ganze Bundesverwaltung. Die FUB müsste eigentlich die IT-Sicherheitsvorgaben des Bundes erfüllen und dem Cyberdelegierten des Bundes Rechenschaft ablegen. Die Armeeführung sagte aber, dass sie auch in Zukunft ihre Cyber-Schwachstellen dem Bund nicht kommunizieren möchte, weil die FUB bzw. das neue Cyberkommando selber für ihre IT-Sicherheit sorge und die Kommunikation von Schwachstellen ein Risiko für die Armee darstelle (NZZ 2021d).

Die Armeeführung sagte, dass sie auch in Zukunft ihre Cyber-Schwachstellen dem Bund nicht kommunizieren möchte.

Ein Prüfbericht der Eidgenössischen Finanzkontrolle legte 2021 offen, dass auch die Ruag Schweiz selbst fünf Jahre nach dem letzten Cyberan-

griff nicht genügend vor Cyberangriffen geschützt war (EFK 2021): Seitens FUB wurde bisher die flächendeckende Umsetzung der Sicherheitsvorgaben nicht überprüft. Dadurch bestehe bei Anwendungen mit Internetzugang ein Risiko. Zudem sei die Ruag Schweiz nicht genügend auf Ereignisfälle wie IT-Probleme und Cyberangriffe vorbereitet. Mängel gäbe es auch beim sogenannten Business Continuity Management (BCM), also der Planung, wie im Störungsfall der Betrieb dennoch aufrechterhalten werden kann.

Gemäss Rundschau wurde die Ruag International im Mai 2021 mutmasslich Opfer von Hacker-Angriffen (Rundschau 2021). Zwar konnte der Hack selber nicht verifiziert werden, aber es wurde ersichtlich, dass weiterhin Verbindungen zur Ruag Schweiz bestehen, so dass potenziell heikle militärische Daten der Schweiz entwendet werden könnten. Die Ruag International musste nach einer externen Untersuchung tatsächlich ernstzunehmende IT-Sicherheitslücken zugeben (NZZ 2021d). Unter anderem war Software nicht aktualisiert worden, und die Überwachung der Systeme genügte den Anforderungen nicht. Somit stellen Angriffe auf die Ruag International weiterhin ein Sicherheitsrisiko für die Infrastrukturen des VBS dar.

Auch die E-Learning-Plattform der Armee stellte Anfang 2021 eine Gefährdung für die Schweiz dar. Aufgrund gravierender Sicherheitslücken waren 400 000 Datensätze einsehbar, die wertvoll sind für Cyberangriffe: Zugänglich waren unter anderem Kontaktangaben des Armeechefs, von Bundesräten sowie Namen und Koordinaten von Mitarbeitern des Nachrichtendienstes und des Bundesamtes für Polizei, inklusive AHV-Nummern, die in vielen Bereichen der Verwaltung zur Identifikation eingesetzt werden (NZZ 2021e).

Die Armee verfolgt in ihren Strategiepapieren zur Zukunft der Luft- und Bodenkriegsführung den Multidomain-Ansatz, also dass man sich sowohl am Boden, in der Luft und im Cyberraum gleichzeitig verteidigen können muss. Es wird betont, dass die neuen Bedrohungen aus dem Cyberraum die alten am Boden und in der Luft nicht ersetzen, sondern lediglich ergänzen, und das ganze Spektrum der hybriden Bedrohungen abgedeckt sein müsse. Der Cyberanteil nimmt innerhalb der gesamten Zukunftsinvestitionen der Armee aber einen eher geringen Stellenwert ein. Für 2022 war die Schaffung eines Cyber-Bataillons und eines Cyber-Fachstabs geplant, womit der Bestand in der Miliz von 206 auf 575 Armeeangehörige wächst. Ob diese Massnahmen für den Cyber-Eigenschutz reichen werden, lässt sich schwer beurteilen. Ebenso ist unklar, welcher Anteil der Übernahme subsidiärer Aufgaben gilt: Die genaue Mittelverwendung in Bezug zur Bedrohungslage ist wenig transparent.

Der Cyberanteil nimmt innerhalb der gesamten Zukunftsinvestitionen der Armee einen eher geringen Stellenwert ein.

Die Abwehr von Cyberbedrohungen ausserhalb der Armee

Ob die Armee überhaupt Cyberschutz für zivile Behörden und Infrastruktur anbieten soll, ist per se eine offene Frage.

Zum einen ist hier eine staatliche Intervention nur zu rechtfertigen, wenn der Schutz den Charakter eines öffentlichen Guts hat, oder anders ausgedrückt: Wenn die cybertechnische Kompromittierung einer Behörde, eines Unternehmens oder einer Infrastruktur deutliche negative externe Effekte aufweist, weil der mögliche Schaden deutlich über das Unternehmen und seine direkten Stakeholder hinausreicht. Falls dies gegeben ist, stellt sich zum anderen die Frage, ob die Armee die richtige staatliche Institution ist, um diese Aufgabe zu übernehmen, oder ob hier nicht eher der Nachrichtendienst oder betroffene öffentliche Behörden selbst in der Verantwortung stehen. Cyberbedrohungen können laut Bundesrat in fünf Kategorien unterteilt werden (Bundesrat 2018, S. 3 ff.):

Eine staatliche Intervention ist nur zu rechtfertigen, wenn der Schutz den Charakter eines öffentlichen Guts hat.

- Cyber-Konflikte: Während ein ausschliesslich im Cyber-Raum geführter Krieg (Cyber-War) gegenwärtig als unrealistisches Szenario betrachtet wird, hat sich gezeigt, dass Cyber-Angriffe aller Arten als Mittel der Kriegführung in verschiedenen Konflikten eingesetzt werden.
- Bei der Cyber-Kriminalität steht das Motiv der Bereicherung im Vordergrund. Sie geht von privaten Akteuren aus. Es werden Straftaten mit Hilfe von Informations- und Kommunikationstechnologie (IKT) verübt oder Schwachstellen dieser Technologien ausgenutzt.
- Cyber-Spionage ist eine Tätigkeit, um im Cyber-Raum für politische, militärische oder wirtschaftliche Zwecke Informationen zu stehlen. Akteure können sowohl staatliche als auch nicht-staatliche Akteure sein. Im Fokus der Angreifer stehen sowohl Unternehmen als auch staatliche, gesellschaftliche oder internationale Institutionen.
- Bei Cyber-Sabotage und Cyber-Terrorismus geht es nicht nur darum, möglichst grosse Schäden zu erzielen, sondern auch um Machtdemonstration und Einschüchterung, verbunden mit der Absicht, eine Organisation oder sogar die ganze Gesellschaft zu destabilisieren. Daher muss sowohl der tatsächliche Schaden eines Cyberangriffs, wie auch dessen Effekt in der Öffentlichkeit in Betracht gezogen werden. Letzterer kann unter Umständen sogar einen grösseren und langanhaltenderen Schaden anrichten (NZZ 2022). Während auf internationaler Ebene verschiedene Sabotageakte, unter anderem auf die Energieversorgung von Staaten, getätigt wurden, sind in der Schweiz bisher keine grösseren Fälle bekannt. Die Relevanz dieser Bedrohung wird mit der digitalen Vernetzung von physischen Geräten über das Internet der Dinge zunehmen.
- Desinformation und Propaganda: Die Bedrohung durch gezielte Verbreitung von Falschinformationen oder von illegal über Cyber-Angriffe beschafften Informationen mit dem Zweck der Diskreditierung von politischen, militärischen oder zivilgesellschaftlichen Akteuren hat stark an Bedeutung gewonnen. In verschiedenen Ländern wurden vor wichtigen Wahlen solche Aktivitäten beobachtet. Auch in der Schweiz muss damit gerechnet werden, dass staatliche oder nicht-staatliche Ak-

teure versuchen könnten, das Vertrauen der Bürgerinnen und Bürger in Staat und Institutionen zu unterminieren.

Die Analysekategorien verschwimmen in der Realität, weil im Rahmen hybrider Konflikte Cyber-Angriffe aller Arten kombiniert werden und die Urheber und Motivationen schwierig zu eruieren sind (Torossian et al. 2020). Deshalb ist es schwierig, die Cybersicherheit als öffentliches Gut klar von der digitalen Verantwortung der Privaten abzugrenzen. Die kritische Infrastruktur kann dabei als Ausgangspunkt für die Beurteilung staatlicher Eingriffe dienen.

Als kritische Infrastrukturen werden laut Bundesamt für Bevölkerungsschutz (Babs) Prozesse, Systeme und Einrichtungen bezeichnet, die essenziell für das Funktionieren der Wirtschaft oder das Wohlergehen der Bevölkerung sind. Sie betreffen folgende Sektoren (Babs 2017):

- Energie: Erdgasversorgung, Erdölversorgung, Fern- und Prozesswärme, Stromversorgung
- Verkehr: Luftverkehr, Schienenverkehr, Schiffsverkehr, Strassenverkehr
- Gesundheit: Chemie und Heilmittel, Labordienstleistungen, medizinische Versorgung
- Nahrung: Lebensmittelversorgung, Wasserversorgung
- Entsorgung: Abfälle, Abwasser
- Information und Kommunikation: IT-Dienstleistungen, Medien, Postdienste, Telekommunikation
- Finanzen: Finanzdienstleistungen, Versicherungsdienstleistungen
- Behörden: Forschung und Lehre, Kulturgüter, Parlament, Regierung, Justiz, Verwaltung
- Öffentliche Sicherheit: Armee, Blaulichtorganisationen (Polizei, Feuerwehr, Sanität), Zivilschutz

Grundsätzlich müssen in der Schweiz die Betreiber von kritischen Infrastrukturen diese selber vor Cyberangriffen schützen, analog zu Unternehmen und Individuen (VBS 2021b, S. 27). Präventiv und im Ereignisfall kommt dem Staat *dann* eine Rolle zu, wenn ein Angriff auf die kritischen Infrastrukturen als relevante Gefahr für das Funktionieren von Wirtschaft und Gesellschaft gesehen werden kann und ein Ausfall verheerende volkswirtschaftliche Folgen hätte (Babs 2017).

Grundsätzlich müssen in der Schweiz die Betreiber von kritischen Infrastrukturen diese selber vor Cyberangriffen schützen.

Ein länger andauernder, landesweiter Strom-Blackout oder ein Ausfall der Telekommunikation (u.a. der Internet-Verbindungen) würde beispielsweise zu einem unmittelbaren Stillstand von nahezu der gesamten Schweizer Wirtschaft führen, Ausfälle der übrigen kritischen Infrastrukturen (z.B. der Lebensmittelversorgung oder des Finanzwesens) verursachen und die Bevölkerung in schwerwiegendem Masse beeinträchtigen (z.B. Ausfall der Wasserversorgung, Abwasserentsorgung oder der Heizungen). Strategische Cyberangriffe mit dem militärischen oder nachrichtendienstlichen Ziel, einen Staat, seine Wirtschaft und Gesellschaft

zu destabilisieren, können auch über kriminelle Hackerorganisationen in staatlichem Auftrag erfolgen. Kriegerische und kriminelle Motive können sich mischen, wenn viele kleine Hackerangriffe auf private Firmen verübt werden, und in der Summe die Volkswirtschaft eines Staates destabilisiert wird.

Die Relevanz von Cyberbedrohungen im zivilen Bereich kombiniert mit der Tatsache, dass die Systeme vieler Firmen nicht robust genug sind und teilweise auch das spezifische Know-How fehlt, um diesen Bedrohungen angemessen zu begegnen, rechtfertigt keine Ausdehnung staatlicher – oder militärischer – Aktivität in private Sphären, sie erfordert aber die Schaffung geeigneter staatlicher Rahmenbedingungen. Dazu gehört beispielsweise die Schaffung eines verpflichtenden Meldesystems zu Cyberangriffen oder konkrete Orientierungshilfen zu besserer Cybersicherheit.

Zu regelnde Verantwortlichkeiten

Das Nationale Kompetenzzentrum Cyber (NCSC) ist das Kompetenzzentrum des Bundes für Cyberrisiken und koordiniert die Arbeiten des Bundes im Bereich Cybersicherheit. Es betreibt die nationale Anlaufstelle für Cyberrisiken, die Meldungen aus der Bundesverwaltung, der Wirtschaft, den Kantonen und der Bevölkerung entgegennimmt (NCSC 2021b).

Für die Cyberstrafverfolgung auf Stufe Bund sind das Eidgenössische Justiz- und Polizeidepartement (EJPD) und die Bundesanwaltschaft (BA) zuständig. Dieses Aufgabengebiet umfasst die Gesamtheit aller polizeilichen und Strafverfolgungs-Massnahmen zur Bekämpfung der Cyberkriminalität, auch auf kantonaler Ebene. Hervorzuheben ist die internationale Zusammenarbeit (sowohl bilateral als auch multilateral), in welcher das Bundesamt für Polizei Fedpol eine zentrale Rolle einnimmt.

Die Aufgaben und Verantwortlichkeiten der Armee im Bereich Cyberverteidigung wurden im Nachgang des Cyberangriffs auf die Ruag im Rahmen des Aktionsplans Cyberdefence ausgearbeitet (vgl. Kapitel 3) (VBS 2017c). Seit dem Ruag-Vorfall gilt offiziell, dass die Armee primär für die Verteidigung der eigenen IKT-Systeme und -Infrastrukturen verantwortlich ist. Innerhalb des VBS ist der Nachrichtendienst für die Abwehr von Cyberangriffen auf kritische Infrastrukturen zuständig, wie auch für die frühzeitige Erkennung und Prävention (VBS 2017c). So wird ein Angriff auf einen Energieversorger von Spezialisten innerhalb des NDB in Absprache mit dem nationalen Kompetenzzentrum (NCSC) vereitelt. Die Cybersoldaten kämen subsidiär zum Einsatz, wenn die Aufgabe im öffentlichen Interesse liegt und auf Gesuch ziviler Behörden erfolgt, deren eigene Mittel nicht ausreichen (Art. 58 Bundesverfassung, Art. 1 & 67 Militärgesetz).

Seit dem Ruag-Vorfall gilt offiziell, dass die Armee primär für die Verteidigung der eigenen IKT-Systeme und -Infrastrukturen verantwortlich ist.

Es gilt zu klären, ob und ab wann der Armee eine aktive Rolle bei der Cyberabwehr zukommt, die über den Eigenschutz hinausgeht, ob dafür kriegerische Motive massgebend sind und inwiefern die Cybersicherheit

kritischer Infrastrukturen oder privater Unternehmen nicht bereits durch den Nachrichtendienst, und das nationale Zentrum für Cybersicherheit sichergestellt wird.

Die Cyber-Bedrohungen sind in der Schweiz bisher vor allem ziviler Natur (vgl. Kapitel 3). Möchte man beispielsweise mehr in die präventive Cybersicherheit investieren, dann sollte man dafür sorgen, dass die zivilen Kapazitäten nicht zu schnell ausgeschöpft werden. Dies analog zur Polizei und Feuerwehr, wo die Armee selbst für schwere Kriminaldelikte, vereinzelte (Terror)Anschläge und folgenschwere Unwetterschäden nicht als primäres Instrument herbeigezogen wird. Der Armee kann im zivilen Cyberbereich primär eine subsidiäre Rolle eingeräumt werden – alleine deshalb, weil die meisten Firmen die Armee in Friedenszeiten, auch während eines Cyberangriffs, nicht in ihren Räumen und schon gar nicht in ihren IT-Systemen wissen wollen.

Die Cyber-Bedrohungen sind in der Schweiz bisher vor allem ziviler Natur.

Generell sollte die Festlegung des konkreten Bedarfs an Cyberfähigkeiten ganzheitlich und bedarfsgerecht über alle sicherheitspolitischen Instrumente hinweg erfolgen, und es sollten die überlappenden Kompetenzen und Verantwortungen geklärt werden. Ein erster Schritt in Richtung Bedarfs- und Ressourcentransparenz wäre eine bessere Übersicht der Cybersicherheitsbudgets über alle Departemente hinweg. Ressourcen sollen den benötigten Fähigkeiten gegenüberstellt und somit Doppelspurigkeiten innerhalb und zwischen Departementen sichtbar gemacht werden. Dies wäre insbesondere für die Bildung eines Cyberbundesamtes wichtig, und für die Entscheidung, wo ein solches zukünftig angegliedert werden sollte.

Zurzeit sind die die Cyberbudgets wenig transparent. Zwar kommunizierte der Bundesrat bei der Beantwortung einer Interpellation (20.3496) die Anzahl Cyber-Mitarbeitenden der Bundesverwaltung, aufgeschlüsselt nach sicherheitspolitischem Instrument (Bundesrat 2020b): Zusätzlich zu den 575 Armeeangehörigen, die im Rahmen des Cyberkommandos ausgebildet werden, verfügt das VBS über 175 fachspezifische Stellen (wobei in der Stellungnahme nicht nach Nachrichtendienst und Armee differenziert wurde). Für das nationale Zentrum für Cybersicherheit sind bis Ende 2021 nur 43 Stellen geplant, unterstützt durch 26 dezentrale Stellen in den Departementen EDA, EDI, UVEK und WBF. Im Rahmen der Strafverfolgung besetzt das Fedpol 41,5 Vollzeitstellenäquivalente mit Cyberspezialisten. Das NCSC und das Fedpol scheinen im Vergleich zum VBS unterdotiert.

5_Internationale Fallstudien – Ein Vergleich der militärischen Prioritätensetzung

Für die Schweiz als eher kleines Land inmitten von Europa ist transnationale Kooperation besonders wichtig. Während der Schweizer Nachrichtendienst und die Polizei eng mit ihren europäischen Partnerinstitutionen vernetzt sind, ist das Schweizer Militär weniger international eingebettet: Die transnationale Kooperation existiert vor allem bilateral zwischen der Schweiz und ihren unmittelbaren Nachbarn, allen voran Deutschland, Frankreich und Österreich. Institutionalisierte Kooperationen gibt es auf Nato- und EU-Ebene. Jedoch beschränken sich die Arten der transnationalen Militärkooperationen auf konzeptionelle Kooperationen im Sinne von Ausbildungskooperationen, ohne wirkliche Truppeneinsätze im Verbund.

Ausbaufähige transnationale militärische Kooperation

Während sich die anderen neutralen und blockfreien Staaten in Europa – Österreich, Finnland und Schweden – an den EU-Battlegroups, den bataillonsstarken Kräften der EU, beteiligen und Finnland und Schweden regelmässig an Nato-Übungen und Missionen teilnehmen, waren in der Schweiz im Jahr 2020 nur ca. 250 Armeeangehörige für militärische Friedensmissionen im Einsatz (Schweizer Armee 2021b). Das Ziel des vorgängigen sicherheitspolitischen Berichtes (2016b), «weiterhin gleichzeitig bis zu 500 Angehörige der Armee im Ausland einsetzen zu können», wurde damit verfehlt.

Die militärische Zusammenarbeit der Schweiz mit der EU beschränkt sich in erster Linie auf die Unterstützung der Operation Eufor Althea in Bosnien-Herzegowina mit einer Handvoll mobiler Ausbildungsteams und Stabsoffizieren im Hauptquartier der Eufor (Hauser et al. 2020, S. 128 f.). Darüber hinaus führt die Schweiz einen regelmässigen Dialog mit der EU über gemeinsame aussen- und sicherheitspolitische Themen und nimmt mit zivilen Experten an Friedensmissionen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) teil. Ein formelles Rahmenabkommen zur sicherheitspolitischen Kooperation zwischen der EU und der Schweiz besteht bisher nicht. Zurzeit prüft die Schweiz, welche Beteiligungsmöglichkeiten es als Drittstaat an Pesco gäbe und inwieweit diese von Interesse für die Schweiz seien. Von Truppeneinsätzen ist bisher nicht die Rede (NZZ 2021f).

Ein formelles Rahmenabkommen zur sicherheitspolitischen Kooperation zwischen der EU und der Schweiz besteht bisher nicht.

Umfangmässig ist die schweizerische Sicherheitskooperation mit der Nato wesentlich bedeutender als jene mit der EU, allerdings involviert auch sie insgesamt weniger als 1 % des personellen Gesamtbestandes und der Verteidigungsausgaben (Hauser et al. 2020). Unter Leitung der Nato, im

Rahmen der KFOR Mission im Kosovo, ist für die Schweiz weiterhin eine Einheit in Kompaniestärke, die SWISSCOY, im Einsatz. Diese wurde jedoch 2018/2019 von 235 auf 165 Mann reduziert (Hauser et al. 2020).

Eine stärkere transnationale Kooperation der Schweizer Armee mit europäischen Partnern könnte u.a. allfällige zwischenzeitliche Fähigkeitslücken in den mechanisierten Verbänden kompensieren. Das würde jedoch eine Debatte zur Schweizer Neutralitätspolitik nötig machen. Ansätze dazu sind im Neutralitäts-Exkurs von Kapitel 6 ausgeführt.

Folgend wird die Prioritätensetzung der anderen (post-)neutralen Staaten in Europa (Finnland und Schweden, Österreich) und jene Grossbritanniens diskutiert. Daraus ergeben sich für die Schweiz teilweise wertvolle Denkanstösse, wie die Armeeressourcen effizienter an der Bedrohungslage ausgerichtet werden können und wie dank transnationaler Kooperation zu den kollektiven Verteidigungsstrukturen beigetragen werden kann, ohne dabei die eigene Neutralität zu kompromittieren.

5.1_ Vereinigtes Königreich – Ausbau der Cyberverteidigung

Das Vereinigte Königreich hat im Jahr 2021 zwei neue Weissbücher über die Neuausrichtung der Aussen- und Sicherheitspolitik veröffentlicht: «Defence in a competitive age» (UK Verteidigungsministerium 2021) und «Global Britain in a competitive age» (UK Government 2021). Darin zeigt London auf, wie es hybriden Konflikten unterhalb der Kriegsschwelle begegnen und die militärischen Fähigkeiten für die «Kriegsführung im Informationszeitalter» verbessern möchte. Es findet eine Schwerpunktverschiebung von robusten Mitteln wie schweren Panzern zu neuen Technologien wie der Cyberabwehr und Drohnen mit künstlicher Intelligenz statt. Schützenpanzer werden zunehmend ausgemustert und durch leichtere hochmobile Radfahrzeuge ersetzt. [17] Die Anzahl Kampfpanzer wird von 227 auf 148 [18] reduziert, Diskussionen wurden auch bezüglich einer Reduktion der Anzahl Kampfjets geführt. Für den Sollbestand der Soldaten war (Stand 2021) bis 2025 eine Reduktion von 82 040 auf 76 000 bis 72 500 vorgesehen.

Diese Umdisponierungen machen Ressourcen frei für Investitionen in unkonventionelle Mittel, die 34 % aller Neuinvestitionen bis 2025 ausmachen: Von den Neuinvestitionen [19] in Höhe von 24 Mrd. £ sollen mindestens 6,6 Mrd. £ in die Cyberabwehr, den Aufbau militärischer Kapazitäten im Weltraum und die Erforschung künstlicher Intelligenz fliessen. Zudem werden 1,5 Mrd. £ in Technologien für die Datenaufbereitung und -analyse investiert, um ein «digitales Rückgrat» aufzubauen.

Diese Umdisponierungen machen Ressourcen frei für Investitionen in unkonventionelle Mittel.

17 Das geplante gepanzerte Fahrzeug «Boxer» gilt nicht als Eins-zu-eins-Ersatz, sondern als leichteres, hochmobiles Radfahrzeug, das modular aufgebaut werden kann *(Financial Times 2021, Rheinmetall Defence 2021)*.

18 Und die übrig gebliebene Panzerflotte wird mit 1,3 Mrd. £ aufgerüstet.

19 Dies ist das erste Investitionspaket für die Neuausrichtung bis 2030. Es erhöht das britische Militärbudget der nächsten vier Jahre auf insgesamt 188 Mrd. £ über den 4-Jahreszeitraum. Weitere Investitionen in die neuen Technologien werden grösstenteils erst gegen Ende des Jahrzehnts erfolgen *(NZZ 2021g)*. Die Investitionen gegen unkonventionelle Bedrohungen werden bis 2032 also noch höher ausfallen.

Für die Modernisierung der Luftabwehr (Future Combat Air System, FCAS) wurden ebenfalls zusätzliche 2 Mrd. £ gesprochen. Mit dem FCAS soll eine innovative Mischung aus bemannten, unbemannten und autonomen Plattformen umgesetzt werden, einschließlich Drohnenschwärmen. Dabei wird in den Weissbüchern auf den jüngsten Konflikt zwischen Armenien und Aserbaidschan um Nagorni Karabach verwiesen. Im Konflikt spielten die aserbaidschanischen Drohnen eine entscheidende Rolle, weil sie mittels künstlicher Intelligenz oder über Fernsteuerung das Feuer eröffneten und den feindlichen Panzern überlegen waren.

Sicherheitspolitische Einordnung

Grossbritannien orientiert sich bei seiner militärischen Ressourcenausrichtung konsequent an den militärischen Bedrohungen aus Russland und China im Rahmen eines hybriden Konfliktes. Die Verteidigung im Cyber- und Informationsraum sowie die Kriegsführung unter Zuhilfenahme künstlicher Intelligenz werden besonders stark gewichtet. Die Nutzung von künstlicher Intelligenz in Waffensystemen führt jedoch zu wichtigen ethischen, rechtlichen und politischen Fragen. Um moralische Verantwortung und Rechenschaftspflicht zu gewährleisten, müssen internationale Normen implementiert werden.

Grossbritannien begründet die Priorisierung mit einem erweiterten und sich ergänzenden Gefahrenspektrum: Weil sich das Spektrum der Kriegsführung erweitert, herrscht in London die Einsicht, dass Prioritätensetzungen nötig sind. Deshalb dürfte auch die Partnerschaft mit den USA und der Nato an Bedeutung gewinnen, um allfällige Fähigkeitslücken zu kompensieren. Innerhalb der Verteidigungsallianz wird der britische Weg die Tendenz hin zu mehr transnationaler Kooperation verstärken.

Weil sich das Spektrum der Kriegsführung erweitert, herrscht in London die Einsicht, dass Prioritätensetzungen nötig sind.

Die sicherheitspolitische Ausrichtung Grossbritanniens, mit weniger schwerer konventioneller Ausrüstung hin zu mehr Cyberfähigkeiten, gilt als progressiver Ansatz – wenn auch seine geografische Situation als Insel natürlich nicht ganz vergleichbar ist mit der Situation mitteleuropäischer Länder.

5.2_ Schweden und Finnland – (post-)neutral und transnational kooperierend

Sicherheitspolitisch können Finnland und Schweden nur eingeschränkt mit der Schweiz verglichen werden, weil die Sicherheitsstrategien der nordeuropäischen Länder von der besonderen Bedrohungslage als Grenz- bzw. Nachbarländer Russlands geprägt sind. Jedoch zeigen sie exemplarisch auf, dass sich kleine Länder nur innerhalb kollektiver Verteidigungsstrukturen glaubwürdig gegen konventionelle Bedrohungen wappnen können. Beiden Ländern ist eine stark institutionalisierte transnationale Kooperation gemein, die als essenzielle Doktrin für die nationale Sicherheit gilt.

Schweden

Schweden gilt als neutral im Sinne von bündnisfrei und ist geprägt durch seine Nähe zu Russland. Schweden rüstet konventionell auf, weil es Russland seit der Annexion der Krim und der Aggression gegen die Ukraine in seinen Bedrohungsanalysen als ein zentrales Sicherheitsrisiko wahrnimmt (Schwedische Regierung 2020). Diese Wahrnehmung dürfte sich seit der russischen Invasion der Ukraine nochmals verstärkt haben.

Die schwedische Regierung verabschiedete im Oktober 2020 ihre Verteidigungsprioritäten für die Jahre 2021 bis 2025. Die Verteidigungsausgaben sollen bis 2025 um 2,7 Mrd. auf 8,9 Mrd. € erhöht werden, was einem Anstieg von 45 % entspricht. Insgesamt sollen die Verteidigungsausgaben damit auf 1,5 % des BIP steigen. Die Streitkräfte (Berufssoldaten, Milizsoldaten und Reservisten) werden von 60 000 auf 90 000 Personen erhöht. Hinzu kommt eine Modernisierung der Kampfflugzeuge, ein neues U-Boot und die Schaffung einer neuen mechanisierten Brigade (Schwedische Regierung 2020).

Strategisch und finanziell sollen nicht nur konventionelle Mittel priorisiert werden, sondern auch der Nachrichtendienst, die Cyberverteidigung und der Zivilschutz (IISS 2021). Die Cyberfähigkeiten sollen in Zukunft sowohl defensive als auch offensive Kapazitäten umfassen (Schwedische Regierung 2020). Die zivile Verteidigung wird in Zukunft die Bereiche Cybersicherheit, Stromversorgung und Gesundheitssystem priorisieren.

Schweden hält sich aus militärischen Bündnissen heraus und ist keinen militärischen Beistandsklauseln verpflichtet, beteiligt sich aber seit dem Ende des Kalten Krieges äusserst engagiert in Gefässen der transnationalen Kooperation. Die Bedeutung der transnationalen Kooperation hat seit der russischen Annexion der Krim und dem Brexit zugenommen (Zandee et al. 2020). Aufgrund Russlands aggressivem Verhalten intensiviert Stockholm die Nato-Kooperationen. Der Schwerpunkt liegt auf der Gewährleistung der Sicherheit im Ostseeraum. Dazu gehören u.a. ein Informationsaustausch über die hybride Kriegsführung und die Entwicklung eines gemeinsamen Lagebewusstseins, um Gegenmassnahmen gemeinsam entwickeln zu können (Nato 2021a). Gemeinsam mit Finnland beteiligt sich Schweden an der Nato-Response-Force[20] (NRF). Darüber hinaus hat Schweden ein Memorandum of Understanding unterzeichnet, das die logistische Unterstützung alliierter Streitkräfte, die sich auf ihrem Territorium befinden oder dieses durchqueren, während Übungen oder im Krisenfall ermöglicht. Abgesehen vom Engagement im Rahmen von Friedensmissionen im Kosovo (KFOR), engagierte sich Schweden in Missionen in Afghanistan (International Security Assistance Force ISAF), Libyen (Operation Unified Protector OUP) und im Irak (Nato 2021a). In Li-

Schweden beteiligt sich seit dem Ende des Kalten Krieges äusserst engagiert in Gefässen der transnationalen Kooperation.

20 Die Nato-Reaktionsstreitmacht ist eine Eingreiftruppe der NATO, die in zeitlich hoher Verfügbarkeit durch ihren modularen Aufbau in einem breiten Spektrum möglicher Operationen eingesetzt werden kann. Sie besteht aus Kontingenten von Bodenstreitkräften, Luftstreitkräften, Marineeinheiten und Spezialeinheiten.

byen waren beispielsweise bis zu 122 Soldaten und 8 Gripen Kampfjets im Einsatz.

Sicherheitspolitische Einordnung

Die nordische Solidaritätsdeklaration [21] sowie diverse bilaterale und regionale Verteidigungskooperationen, inklusive Nato-Zusammenarbeit, reizen die Möglichkeiten von Schwedens Neutralität im Sinne der Bündnisfreiheit aus, ohne dass das Land formelle Beistandserklärungen eingehen müsste (Hellquist und Lundholm 2021). Im Lichte des Kriegs in der Ukraine hat das – der Meinung einiger nach veränderte – Neutralitätsverständnis Schwedens weltweit zu reden gegeben. Kurz nach dem Einmarsch Russlands gab Schweden bekannt, dem ukrainischen Militär direkte militärische Unterstützung in Form von Panzerabwehrwaffen, Helme und Schutzwesten zur Verfügung zu stellen. [22] Schweden hat damit die bisherige Doktrin gebrochen, keine Waffen an Länder zu schicken, die sich in einem aktiven Konflikt befinden (Reuters 2022a).

Im Lichte des Kriegs in der Ukraine hat das Neutralitätsverständnis Schwedens weltweit zu reden gegeben.

Obwohl bündnisfrei richtet Schweden, genau wie Finnland – als (bevölkerungsmässig) kleines Land in geopolitisch exponierter Lage – angesichts konventioneller Bedrohungen seine Verteidigungsstrategie hin zu transnationaler Kooperation aus, auch wenn es im Kern neutral bleiben und nicht in bewaffnete Konflikte involviert werden möchte. Die Verteidigung ist im Ernstfall im Verbund am erfolgversprechendsten, weshalb die entsprechenden Fähigkeiten für potenzielle Kriegszeiten vorab eingeübt und aufgebaut werden müssen. So schreibt die schwedische Verteidigungsagentur (als wissenschaftliches Sprachrohr der schwedischen Armee) in ihrer neusten Studie, dass gerade in der neuen Multipolarität mit asymmetrischen Bedrohungen und globalem Terrorismus Verteidigungspolitik automatisch immer auch eine internationale Dimension habe und transnationale Lösungen brauche. Gerade weil die konventionelle und hybride militärische Bedrohung für Schweden zugenommen hat, ist die transnationale Verteidigungskooperation das wichtigere Prinzip geworden für die nationale Sicherheit als die Neutralität (Hellquist und Lundholm 2021). Schwedens pragmatischer Umgang mit der Neutralität kann als Inspiration dienen, indem die transnationale Verteidigungskooperation verstärkt als Mittel betrachtet wird, um sowohl konventionellen wie auch hybriden Bedrohungen zu begegnen.

Finnland

Geopolitisch ist Finnland geprägt von seiner unmittelbaren Nachbarschaft zu Russland, mit dem es eine 1300 Kilometer lange Grenze teilt.

21 Unterschrieben durch Dänemark, Finnland, Island, Norwegen und Schweden, darin bekennen sich die Mitgliedsländer der nordischen Solidaritätsdeklaration zu sicherheitspolitischer Beistandshilfe: Sollte ein Mitgliedsland bedroht sein, dann schreiten die anderen Länder auf dessen Ersuchen hin zur Hilfe.

22 Natürlich unterstützen auch noch andere Länder (insbesondere die Nato, USA und Grossbritannien) die Ukraine militärisch. Für eine Übersicht und weitere bilaterale Unterstützungsleistungen s. *Military assistance to Ukraine since the Russian invasion (2022)*.

Die Sorge eines Überraschungsangriffs, beispielsweise durch Marschflugkörper in Finnlands Reichweite, hat nach der russischen Übernahme der Krim im Jahr 2014 zugenommen (IISS 2021). In Folge jüngster Geschehnisse in der Ukraine dürfte sich diese Bedrohungswahrnehmung nochmals wesentlich verschärft haben. Der Angriffskrieg Russlands hat auch bei Finnland zu einem Policy Shift geführt – so unterstützt Finnland die Ukraine mit Waffen (z.B. Sturmgewehre und Panzerabwehrwaffen) und Munition (Reuters 2022b).

Vor dem Hintergrund einer russischen Bedrohung rüstet Finnland selbst stark konventionell auf, im Rahmen einer sicherheitspolitischen Abschreckungsstrategie, und um ein glaubwürdiger internationaler Partner zu sein (Finnische Regierung 2020). Mit dem Budgetvoranschlag 2021 wurde das Verteidigungsbudget gegenüber 2020 um 1,7 Mrd. auf insgesamt 5,2 Mrd. € erhöht. Die Budgeterhöhung ist ein erster Schritt, um für die zwei grossen Beschaffungen bis 2028 zusätzliche Mittel bereitzustellen: 64 neue Kampfjets für 10 Mrd. € im Rahmen des Kampfflugzeugprogramms, und 4 neue Kriegsschiffe für 1,3 Mrd. € (IISS 2021; Frisell & Pallin 2021).

Vor dem Hintergrund einer russischen Bedrohung rüstet Finnland selbst stark konventionell auf.

Aufgrund einer umfassenden Neubewertung der Bedrohungslage und der politischen und ökonomischen Zugehörigkeit zu Westeuropa mit seinen liberalen Werten entwickelte Finnland nach dem Ende des Kalten Krieges sein Neutralitätsverständnis weiter und verwendete ab dann nur noch den Begriff der Bündnisfreiheit.[23] Zudem wurden die transnationalen Kooperationen institutionalisiert. Finnland trat 1995 der EU bei, ist Teil der Nato-Partnerschaft für den Frieden (PfP) und beherbergt das gemeinsame EU-Nato-Zentrum für die Bekämpfung hybrider Bedrohungen (Centre for Countering Hybrid Threats) (Baezner 2020). Die transnationale Kooperation hat sich nach der Annexion der Krim durch Russland zusätzlich verstärkt.

Es besteht eine weitgehende Verteidigungskooperation Finnlands mit Schweden, einschliesslich einer bilateralen Einsatzplanung. Finnland kooperiert zudem im Rahmen der Nordefco mit Dänemark, Island, Norwegen und Schweden. Ziel von Nordefco ist es, die Interoperabilität zu erhöhen und rechtliche und politische Grundlagen zu schaffen, um militärische Einheiten und Material über die Grenzen hinweg verschieben und lagern zu können.

Die EU-Mitgliedschaft gilt in Finnland als zusätzlicher Sicherheitsfaktor, weil im europäischen Verbund die eigene Verteidigung gestärkt wird. Deshalb ist Finnland den militärischen Solidaritäts- und Beistandsklauseln im Vertrag von Lissabon beigetreten (Artikel 222 und 42). Um die

23 Wobei auch der Begriff «Bündnisfreiheit» ähnlich wie die «Neutralität» unscharf ist. So schreibt beispielsweise die ETH in einer Publikation vom bündnisfreien Finnland *(Locher 2010)* und in einer anderen vom neutralen Finnland *(Baezner 2020)*. Ob die beiden Terminologien tatsächlich Synonyme sind, mag bezweifelt werden. Jedoch unterstreicht dies einmal mehr, dass das Neutralitätsverständnis immer auch politisch konstruiert wird und über die rein völkerrechtliche Definition hinausgeht. Dies ermöglicht unter Umständen eine pragmatische, kontextabhängige Auslegung, kann sie aber auch verhindern.

Abschreckungsstrategie im Verbund noch glaubhafter zu machen und die Interoperabilität[24] in Europa und über den Atlantik zu erhöhen, hat Finnland ausserdem bilaterale Verteidigungsabkommen mit folgenden Staaten geschlossen: Dänemark, Estland, Frankreich, Deutschland, Norwegen, Polen, Schweden, Grossbritannien und den USA. Finnland nimmt auch an der von Grossbritannien geführten Joint Expeditionary Force teil und stellt Soldaten für die EU-Battlegroups.

Finnland ist ein aktiver Nato-Partner, seit 1994 Mitglied der Partnerschaft für den Frieden, und auch als «erweiterter» Partner aktiv («enhanced opportunities partner»). Elementare Bereiche der finnischen Streitkräfte, insbesondere Einheiten der Marine und der Luftstreitkräfte, werden ausgebildet, um den Interoperabilitäts-Standards der Nato zu entsprechen. Die Beziehung zur Nato wird auch über die bilaterale Kooperation mit den USA bzw. trilateralen Abkommen mit den USA und Schweden gestärkt. Insgesamt partizipiert Finnland jährlich an ca. 70 internationalen militärischen (Nato-)Übungen (Finnisches Verteidigungsministerium 2021). Auch an Nato-Missionen beteiligt sich Finnland, etwa an der Beratungs-, Ausbildungs- und Kapazitätsaufbaumission der Nato im Irak (Nato 2021b). Russland würde einer vollen Mitgliedschaft Finnlands in der Nato mit wenig Begeisterung begegnen. Finnische Politiker und Politikerinnen diskutieren aktuell jedoch einen solchen Nato-Beitritt (Politico 2022). Die Annäherung Finnlands und Schwedens an die Nato drückt sich auch darin aus, dass Nato-Generalsekretär Stoltenberg kürzlich verkündet hat, die Koordination und den Austausch mit den beiden Ländern zu vertiefen. Beide Staaten nehmen so auch an den Nato-Sitzungen zur Krise in der Ukraine teil (Defense News 2022).

Insgesamt partizipiert Finnland jährlich an ca. 70 internationalen militärischen (Nato-) Übungen.

Sicherheitspolitische Einordnung

Im Gegensatz zur Schweiz ist Finnland geografisch an der Peripherie Europas und deshalb auch stärker möglichen bewaffneten Anteilen hybrider Bedrohungen ausgesetzt als die europäischen Binnenländer. Insofern ist Finnlands sicherheitspolitische Strategie Vorbild für alle kleinen, bündnisfreien bzw. neutralen Staaten, die sich effektiv vor konventionellen Bedrohungen schützen wollen oder müssen. Finnland zeigt exemplarisch auf, dass ein kleines Land sich hauptsächlich mit transnationaler Kooperation vor dem Ernstfall eines konventionellen Konfliktes wappnen kann.

Für kleinere binneneuropäische Länder wie die Schweiz macht es zwar aufgrund der Bedrohungslage und der Arbeitsteilung innerhalb der Nato weniger Sinn, so stark in konventionelle Mittel zu investieren wie Finnland. Eine ausgeprägtere transnationale Militärkooperation, die über bestehende bilaterale Ausbildungskooperationen hinausgeht, könnte aber zu einem grösseren Nutzen von Investitionen in konventionelle Mittel

24 Interoperabilität bedeutet die Fähigkeit zur Zusammenarbeit verschiedener Systeme, Techniken oder Organisationen.

und die Territorialverteidigung führen. Finnlands Fokus auf Interoperabilität sowie die intensive Zusammenarbeit nicht nur mit der Nato, sondern auch mit Europa und den unmittelbaren Nachbarsländern, können Anhaltspunkte für eine stärkere Akzentsetzung der Schweiz bieten.

5.3_ Österreich – pragmatisch neutral

Unser östlicher Nachbar – mit traditionell geringer militärischer Durchschlagskraft – verzichtet auf eine komplette Erneuerung der konventionellen Mittel am Boden und in der Luft, die insgesamt 16,2 Mrd. € kosten würde (Bundesministerium für Landesverteidigung 2019). Schwere Waffensysteme werden bis auf einen Restbestand für Ausbildungszwecke abgebaut, um sie bei Bedarf wieder hochfahren zu können (Hauser et al. 2020). Fähigkeits- und Sicherheitslücken will Österreich mit einer starken transnationalen Kooperation und einer Ausrichtung auf die kollektive Sicherheit in Europa decken.

Von den bloss 640 Mio. €, die im Bundesfinanzrahmen 2021–2024 als Sonderpakete für Neuinvestitionen genehmigt wurden, fliessen 31 % als Zusatzmittel der Miliz zu, 38 % werden für unkonventionelle Mittel wie die Cyber-, Terror- und ABC-Abwehr verwendet und 31 % für den Ausbau von Zivilschutzaufgaben (im Rahmen des Sanitäts- und Katastrophenschutz-Pakets). Es wird auf die Terror-, Cyber-, ABC- und Drohnenabwehr sowie auf Auslandeinsätze und Blackout-Vorbereitungen fokussiert. Schwere Waffengattungen werden in Österreich dagegen auf das Minimum reduziert.

Es wird auf die Terror-, Cyber-, ABC- und Drohnenabwehr sowie auf Auslandeinsätze und Blackout-Vorbereitungen fokussiert.

Die österreichische Neutralität wird pragmatisch ausgelegt, als «engagierte Neutralität» (Gärtner 2018). Damit ist ein starkes Bekenntnis zur Nichtbeteiligung an Militärbündnissen gemeint, bei gleichzeitig starkem Einsatz für eine engagierte, im Gegensatz zu einer passiven Sicherheitspolitik. Die Mitgliedschaft in der EU und die gemeinsame Aussen-, Sicherheits- und Verteidigungspolitik der EU sind für Österreich nicht nur mit der engagierten Neutralität vereinbar, sondern spiegeln zentrale Prioritäten der österreichischen Aussen- und Sicherheitspolitik. Im Gegensatz zu einer rein kollektiven Verteidigung ist die EU auf ein umfassendes Sicherheitskonzept ausgerichtet, nicht nur in militärischer Hinsicht, sondern basierend auf breit abgestützten politischen Bemühungen zur Konfliktverhütung und einem umfassenden Krisenmanagement inklusive Friedensoperationen.

Sicherheitspolitische Einordnung

Aufgrund der ähnlichen Landesgrösse und Einwohnerzahl, einem ähnlichen Bedrohungsbild im Alpenraum inmitten von Europa, dem Milizsystem und der Neutralität würde sich Österreich an sich – seine EU-Mitgliedschaft abgesehen – für einen militärischen Vergleich mit der Schweiz aufdrängen. Jedoch gilt die österreichische Armee als wenig durchschlagskräftig, ist von Sparmassnahmen getrieben und hat einen viel geringeren

Stellenwert als in der Schweiz. Während die Zielgerichtetheit der Investitionen für die Schweiz daher nicht überbewertet werden sollte, beinhaltet die Ausrichtung der politischen Neutralität für einen Vergleich im Alpenraum durchaus interessante Aspekte.

Österreichs Sparkurs ist nur möglich dank dem pragmatischen Umgang mit der Neutralität. Seit der «Euro-Atlantisierung» Mitteleuropas [25] und der Gründung einer Europäischen Sicherheits- und Verteidigungspolitik (ESVP) im Jahr 1999 hat sich Österreichs Neutralitätspolitik zu einer umfassenden militär- und sicherheitspolitischen Kooperation in und um Europa entwickelt (Hauser et al. 2020). Als EU-Mitglied interpretiert Österreich die Neutralität politisch als «kernneutral», d.h. als Nichtbeitritt zu einem Militärbündnis sowie als Verbot der Duldung von Stützpunkten fremder Staaten auf österreichischem Staatsgebiet.

Österreichs Sparkurs ist nur möglich dank dem pragmatischen Umgang mit der Neutralität.

Vor diesem Hintergrund soll das Bundesheer mindestens 1100 Soldaten als Dauerleistung für Auslandseinsätze sicherstellen, damit eine präventive Sicherheitswirkung erzielt werden kann. Ausserdem werden im Rahmen einer gemeinsamen europäischen und transatlantischen Verteidigungsstrategie Synergieeffekte genutzt. Seit 2011 beteiligt sich Österreich regelmässig mit bis zu 600 Soldaten an den EU-Battlegroups [26] (Hauser et al. 2020). Im Jahr 2020 übten österreichische Soldaten einen EU-Battlegroup-Einsatz zusammen mit Soldaten der anderen Neutralen (Finnland, Schweden und Irland) sowie wie mit Deutschland, Kroatien, Lettland, den Niederlanden und der Tschechischen Republik.

25 Damit ist die Aufnahme von Polen, der Tschechischen Republik und Ungarns in die Nato im März 1999 bzw. der Slowakei und Slowenien im Mai 2004 gemeint. Diese Länder, davon vier Nachbarländer Österreichs, gehen bei der Formulierung ihrer Verteidigungsziele von den Bestimmungen des Nordatlantikvertrages und des strategischen Konzeptes der Nato vom November 2010 aus *(Hauser et al. 2020)*.

26 Eine EU-Battlegroup ist eine für jeweils ein halbes Jahr aufgestellte militärische Formation der Krisenreaktionskräfte der Europäischen Union (EU) in hoher Verfügbarkeit. Sie besteht im Kern aus einem Infanterieverband in Bataillonsstärke und einem Führungselement. Sie ist für Erstmissionen in einer Krisenregion gedacht und schafft die nötigen Voraussetzungen für einen weiteren Einsatz (z. B. im Rahmen der UNO) *(Europäische Union 2017)*.

6_Fünf Thesen zur Weiterentwicklung der schweizerischen Landesverteidigung

Die Schweiz ist geschützt durch den Nato-Schutzschirm und ihre Lage inmitten Europas. Sollte in Europa ein konventioneller Konflikt mit Einbezug west- und zentraleuropäischer Länder ausbrechen, dann stellt die kollektive Verteidigung gegen einen gemeinsamen Feind das plausibelste Szenario dar.

Die Schweiz hat sich aber auch gegen Risiken zu wappnen, denen nicht ausschliesslich mit konventionellen militärischen Mitteln begegnet werden kann: (kriminelle) Cyberangriffe, Pandemien, Strommangellagen, ein Ausfall des Mobilfunknetzes und terroristische (Drohnen-)Angriffe. Bei den militärischen Bedrohungen sind in erster Linie unkonventionellen Aspekte wie Cyberangriffe auf militärische oder andere kritische Infrastrukturen das relevante Bedrohungsbild. Die vollen jährlichen Kosten der Landesverteidigung summieren sich auf rund 8,2 Mrd. Fr. bzw. 1,16 % des BIP (vgl. Kapitel 4.1). Für die Legitimation der Armee ist es wichtig, die militärische Mittelallokation konsequent an der Bedrohungslage auszurichten. Die folgenden Thesen sollen eine Grundlage für eine Debatte über eine bedarfsgerechte Schweizer Armee- und Sicherheitspolitik schaffen.

These 1

Boden: Orientierung an neuen Bedrohungsbildern Die Schweiz sollte sich bei den geplanten Neu- und Erneuerungsinvestitionen am Boden konsequenter an tatsächlichen Bedrohungsbildern orientieren. Leichte und mobile Mittel, um unkonventionellen Bedrohungen zu begegnen, dürfen nicht vernachlässigt werden.

Trotz der jüngst erhöhten Bedrohungslage in Europa ist es wenig wahrscheinlich, dass die Schweiz alleine mit einem bewaffneten Territorialangriff durch feindliche Bodentruppen konfrontiert ist. Die derzeitige Priorisierung der mechanisierten Verbände am Boden sollte in Bezug zur Durchsetzungsfähigkeit der übrigen Kräfte gestellt werden. Die Erneuerungsinvestitionen fliessen derzeit vor allem in die schweren Mittel wie Kampf- und Schützenpanzer. Sind diese in diesem Umfang sinnvoll angesichts des Bedarfs an leichten und ungeschützten Radfahrzeugen, ergänzt durch schwere geschützte Fahrzeuge? Auch die Artillerie könnte stärker auf die Fähigkeit zur Feuerunterstützung auf kurze oder mittlere Distanz fokussiert werden. Dies würde es erlauben, sich besser gegen unkonventionelle Bedrohungen unterhalb der Kriegsschwelle zu wappnen, und den Schutzgrad der heutigen Infanterie gegen diese Bedrohungsart zu verbessern.

Die derzeitige Priorisierung der mechanisierten Verbände am Boden sollte in Bezug zur Durchsetzungsfähigkeit der übrigen Kräfte gestellt werden.

Luft: Mehr transnationale Kooperation für effizienten Kampfjeteinsatz Die zu beschaffenden Kampfjets des Typs F-35 sind konzipiert für Angriffs-Einsätze in einem militärischen Verbund (Nato). Dies ist angesichts der Plausibilität der in Frage kommenden bewaffneten Bedrohungen sinnvoll: Es ist plausibler, dass ein konventioneller Konflikt Europa als Kollektiv im Rahmen einer gemeinsamen Verteidigungsanstrengung betreffen wird, als dass sich die Schweiz alleine verteidigen müsste. Der tatsächliche Verteidigungsnutzen von Kampfjets hängt mit dem Ausmass der transnationalen Kooperation zusammen. Die transnationale Militärkooperation sollte ausgebaut werden, beispielsweise über eine Teilnahme an Nato-Übungen zur kollektiven Verteidigung. Die Kampfjet-Investitionen generieren einen höheren Nutzen, wenn die Schweiz sich stärker, aber neutralitätskompatibel in die kollektiven Nato-Strukturen einbindet. Es gilt daher, strategische und neutralitätspolitische Fragen zu klären.

Mit einer stärkeren Beteiligung an den kollektiven Nato-Verteidigungsstrukturen liesse sich nicht nur die Beschaffung von 36 Kampfjets des Typs F-35 besser begründen. Die Schweiz könnte darüber hinaus auch sicherheitspolitische Verantwortung wahrnehmen und einem möglichen Image als Freerider des kollektiven Nato-Schutzschirmes vorbeugen. Ein stärkeres sicherheitspolitisches Engagement auf internationaler Ebene würde die Schweiz auch zu einem wichtigeren aussenpolitischen Partner machen. Die «Guten Dienste», sprich die ausgeprägten Vermittlungs- und Mediationstätigkeiten, die die Schweiz anbietet, sind heute kein Alleinstellungsmerkmal mehr. Während die Fallbeispiele (post-) neutraler europäischer Staaten zwar interessante Anhaltspunkte bieten, ist die Neutralität und ausgeprägte Mediationstätigkeit der Schweiz nicht nur ein Kernpfeiler der Schweizer Aussenpolitik, sondern auch ein Faktor, der durch Schaffung von Dialog zur europäischen und internationalen Stabilität beiträgt. Es soll daher nicht für eine Abkehr vom Neutralitätsprinzip plädiert werden, sondern der Gedanke eines engagierter ausgelegtem Neutralitätsverständnis aufgebracht werden.

Ein solches Vorgehen ist kompatibel mit dem Neutralitätsrecht (vgl. Exkurs). Prüfenswert wäre insbesondere eine stärkere Kooperation mit den Nachbarländern, die über Ausbildungskooperationen und Trainingsflüge hinausgeht, beispielsweise im Rahmen eines gemeinsamen Luftpolizeidiensts oder einer Beteiligung an einem Verbund von Aufklärungs-, Kommunikations-, Führungs- und Waffensystemen.

Ein solches Vorgehen ist kompatibel mit dem Neutralitätsrecht.

Durch Kooperationssynergien würden in Zukunft allenfalls Mittel frei, um beispielsweise ein mehrschichtiges Bodluv-System für kurze, mittlere und grosse Distanz (wie z.B. Israel es hat) zu beschaffen, mit dem Drohnen und Marschflugkörper abgewehrt werden können. Basierend auf den Erkenntnissen des Nagorni-Karabach-Konflikts und des Krieges in Liby-

en sollte das VBS, wie in der neusten Armeebotschaft vorgesehen, darlegen, ob und wie die Schweiz sich vor Drohnen und Lenkwaffen im unteren Luftraum schützen kann. Zu evaluieren ist auch, ob die Schweiz selber Drohnen (Kampfdrohnen, Schwarmdrohnen) braucht, um sich besser gegen Angriffe jeder Art zu schützen.

Exkurs

Die Schweizer Neutralität: Möglichkeiten neutralitätskompatibler Kooperation

Die Beschaffung der neuen Kampfjets wäre eine Chance, die Neutralitätsdebatte in der Schweiz konstruktiv zu führen, entlang der alles entscheidenden Frage: Welche Art der politischen Neutralitätsauslegung bietet uns angesichts der aktuellen Bedrohungslage den grössten Gewinn an Sicherheit?

Rechtlich gesehen bedeutet die Schweizer Neutralität bereits heute nichts anderes als «die Nichtteilnahme an Kriegen, Gleichbehandlung der Kriegführenden, Selbstverteidigung, keine Söldner für Kriegsparteien, und keine Zurverfügungstellung des Territoriums für die Kriegsparteien» (VBS und EDA 2004). Jedoch wurde die Neutralitätspolitik, also die politische Auslegung über das Neutralitätsrecht hinaus, in der Schweiz bisher sehr eng ausgelegt, teilweise nämlich als regelrechte Nichteinmischungspolitik. Dieses Verständnis könnte pragmatisch weiterentwickelt werden, hin zu einer Kooperationsstrategie, die im Rahmen der rechtlichen Neutralitätsauslegung möglich wäre. Ob sich die Schweiz bei einer Intensivierung der Kooperation eher in Richtung EU oder Nato orientieren sollte, wäre Bestandteil einer solchen Neutralitätsdebatte. Unter Experten ist noch unklar, welches Potenzial die europäischen Verteidigungsinitiativen tatsächlich haben. Entweder werden die Initiativen rund um Pesco rein konzeptioneller, organisatorischer Natur bleiben oder sich tatsächlich in Richtung einer gemeinsamen sicherheitspolitischen Strategie aller EU-Mitglieder weiterentwickeln. So oder so ist die EU bemüht, die Nato-Strukturen nicht zu konkurrieren, sondern lediglich zu ergänzen bzw. zu vereinfachen. Dies macht auch Sinn, wäre eine Doppelspurigkeit doch hochgradig ineffizient. So gesehen wäre eine stärkere Kooperation mit der Nato für die Schweiz militärstrategisch sinnvoller, eine mit der EU unter Umständen politisch realistischer.

Ob sich die Schweiz bei einer Intensivierung der Kooperation eher in Richtung EU oder Nato orientieren sollte, wäre Bestandteil einer solchen Neutralitätsdebatte.

Naheliegend wäre eine stärkere Kooperation mit der EU, weil sie einen zivil-militärischen Strategieansatz verfolgt, der nicht nur militärischer Natur ist, sondern auf breit abgestützten politischen Bemühungen zur Konfliktverhütung beruht. Die Schweiz überprüft zurzeit, welche Beteiligungsmöglichkeiten es als Drittstaat an Pesco gibt, beschränkt sich jedoch auf Projekte im Sanitäts- und Logistikbereich. Es wäre zu überprüfen, inwiefern die Schweiz einen Beitrag mit Truppeneinsätzen liefern könnte. Die Schweiz könnte auch von den neutralen Staaten Schweden, Finnland, Irland und Österreich lernen und gezielt EU-Battlegroups beitreten, um ein transnationales militärisches (Nischen-)Profil aufzubauen und ein ernstzunehmender europäischer Partner in diesem Bereich zu werden. Das Truppenkontingent im Ausland könnte auch im Rahmen eines Ausbaus der transnationalen militärischen Friedensförderung erhöht werden. Die Soldaten im Ausland würden so in einem transnationalen Verbund im Sinne der Interoperabilität üben, und könnten ihre Fähigkeiten in realistischeren Szenarien testen, als dies beispielsweise in einem WEF-Einsatz der Fall ist. Die militärische Friedensförderung ist zusammen mit der zivilen der grösste Hebel der Schweiz, um etwas gegen die instabile Lage an der Peripherie Europas zu unternehmen, die laut Bundesrat eines der grösseren (indirekten) militärischen Risiken für die Schweiz darstellt (Bundesrat 2021a).

Die Nato ist und bleibt für die Schweiz, wie für ganz Europa, die wichtigste kollektive Verteidigungsallianz. Die Schweiz nimmt zwar bereits an Nato-Übungen teil, jedoch hauptsächlich als Beobachterin und nicht mit Truppenkontingenten oder wenn darin die kollektive Verteidigung eingeübt wird. Eine Teilnahme an Nato-Übungen mit eigenen Truppen würde der Schweiz erlauben, das plausibelste konventionelle Szenario, die Verteidigung im Verbund,

einzuüben. VBS und Bundesrat könnten überprüfen, inwiefern das Milizsystem für solche Kooperationsvorhaben ausreicht, oder ob es dafür vereinzelte Berufstruppen bräuchte.

Die Frage der Neutralität sollte ehrlich auf den Tisch gelegt werden: Die Neutralität findet erst dort ihre Grenzen, wo die Schweiz in internationale militärische Planungen involviert würde. Solange keine Beistandsverpflichtungen (Artikel 5 der Nato) eingegangen werden, ist solch ein Vorgehen kompatibel mit dem Neutralitätsrecht.

These 3

Cybersicherheit: Mängel beheben und klare Aufgabenteilung

Die Schweizer Cybersicherheit muss erhöht werden – sowohl jene des Militärs selber als auch beispielsweise jene der kritischen Infrastrukturen. Das nationale Kompetenzzentrum für Cybersicherheit (NCSC) trägt die Gesamtverantwortung (Ownership) für die staatliche Cybersicherheit der Schweiz. Die nachgelagerten subsidiären Strukturen sind so zu erarbeiten, dass es die Armee bei der Abwehr von nicht kriegerischen Cybergefahren so wenig wie möglich braucht. Die Departementalisierung sollte gebremst werden, indem geklärt wird, wie und aufgrund welcher Bedarfsanalyse von Cyberfähigkeiten die Ressourcenabstimmung zwischen NCSC, NDB und Armee geschieht.

Ein gemeinsames Cybersicherheitsbudget über alle Departemente hinweg könnte es ermöglichen, auf der Bedrohungslage abgestützt eine bedarfsgerechte Ressourcenverteilung auf die sicherheitspolitischen Instrumente vorzunehmen. Dies wäre insbesondere wichtig mit Blick auf ein Bundesamt für Cybersicherheit und der Frage nach dessen Angliederung.

Zu klären ist die Aufgabenteilung bei den Bemühungen um Cybersicherheit – nicht nur zwischen Militär und anderen staatlichen Stellen, sondern auch zwischen Staat und Wirtschaft. Auf die staatlichen Behörden bezogen scheinen das NCSC und das Fedpol im Vergleich zum VBS unterdotiert, zumal die zivilen Cyberrisiken aktuell die militärischen Cyberbedrohungen übertreffen (vgl. Kapitel 3).

Die Armee kommt nur bei einem grossangelegten militärischen Cyberangriff zum Einsatz, und auch hier in erster Linie subsidiär, d.h. auf Anfrage von einem Kanton oder im Auftrag des Bundes, wenn die zivilen Mittel nicht mehr ausreichen. Diese subsidiäre Funktion soll beibehalten werden. Innerhalb einer gesamtheitlichen Cybersicherheitsstrategie der Schweiz hat die Armee vor allem die Aufgabe, sich selbst effektiv gegenüber Cyberangriffen zu verteidigen. Wenn die Schweizer Cybersicherheit gesamthaft gestärkt werden soll, dann sollten Investitionen in die zivilen Instrumente getätigt werden – beispielsweise polizeiliche Massnahmen. Analog zur Terrorismusabwehr können so Verdrängungseffekte von der zivilen hin zur militärischen Sphäre vorgebeugt werden.

Wenn die Schweizer Cybersicherheit gesamthaft gestärkt werden soll, dann sollten Investitionen in die zivilen Instrumente getätigt werden.

Handlungsbedarf existiert beim Schutz von kritischen Infrastrukturen. Diese werden mehrheitlich von Unternehmen in Staatsbesitz (Bund,

Kantone, Gemeinden) betrieben. Es liegt an sich in der Verantwortung dieser Unternehmen, sich genügend gegen Cyberattacken zu schützen. Ein Angriff auf eine kritische Infrastruktur ist aber nicht nur für das betroffene Unternehmen ein Risiko, sondern meist auch für die Bevölkerung – zum Teil in erheblichem Mass. Hier liegt die staatliche Aufgabe deshalb in der Errichtung geeigneter Rahmenbedingungen, um das Entstehen solcher negativer Externalitäten unwahrscheinlicher zu machen. Erstens braucht es Vorgaben für Redundanzen in den entsprechenden Systemen, damit auch ein erfolgreicher Cyberangriff nicht ohne weiteres beispielsweise die Kommunikationsinfrastruktur der Swisscom lahmlegen oder die Stromversorgung eines Netzbetreibers unterbrechen kann. Kollektive Verpflichtungen zu regelmässigen Sicherungen und Backup-Konzepten sind angezeigt. Zweitens gilt es das Meldewesen auszubauen. Unternehmen – vor allem, aber nicht ausschliesslich Betreiber kritischer Infrastrukturen – sollten Cyberangriffe obligatorisch einer Bundesstelle melden müssen. Nur umfassende Kenntnis über Umfang und Art von Cyberangriffen erlaubt es, sich gegen solche künftig besser zu wappnen. Wird dies unterlassen, wäre die Schweiz als Land mit vielen zahlungskräftigen, aber IT-technisch oftmals schlecht geschützten Akteuren ein willkommenes Angriffsziel für kriminell wie auch militärisch motivierte Cyberangriffe. Die Meldung kann unter Ausschluss der Öffentlichkeit geschehen, um befürchtete Reputationsschäden zu vermeiden.

Kollektive Verpflichtungen zu regelmässigen Sicherungen und Backup-Konzepten sind angezeigt. Zweitens gilt es das Meldewesen auszubauen.

Beim NCSC als Kompetenzzentrum laufen alle Fäden zusammen, weshalb sich auch die Armee mit dem NCSC abzusprechen hat. So kann frühzeitig erkannt werden, wenn die Systeme der Armee oder ein Angriff darauf ein Risiko für die restliche Bundesverwaltung darstellen. Sicherheitsrisiken in Zusammenhang mit dem Informatiksystem der Armee sollten auch in Zukunft dem Cyberdelegierten des Bundes gemeldet werden müssen.

These 4

Mut zur (Fähigkeits-)Lücke und konsequente Priorisierung
Die Ausrichtung der Investitionsplanung auf Risiken gemäss der eigentlichen Risikoanalyse findet in der Schweiz nicht genug systematisch statt. Dies kann zu einer ineffizienten Bereitstellung des öffentlichen Gutes «äussere Sicherheit» führen. Mit einem zielgerichteteren Einsatz der verfügbaren Gelder könnte sich die Schweiz besser gegen reale künftige Risiken schützen.

Die Zukunft ist schlecht prognostizierbar. Deshalb muss die Armee auch in Zukunft vor allem anpassungsfähig, flexibel einsetzbar und modular aufgebaut sein. Dies ist primär über eine anpassungsfähige Führung umsetzbar. Bei allem Mangel an Prognostizierbarkeit bleibt eines sicher: Das Armeebudget ist begrenzt, weshalb Priorisierungen auf die plausibleren

Bedrohungsszenarien unumgänglich sind. Das VBS und der Bundesrat sollten künftige sicherheitspolitische Lagebeurteilungen in Priorisierungskonzepte münden lassen, inklusive transparenter Darstellung der finanziellen Konsequenzen für die sicherheitspolitischen Instrumente. Dies betrifft nicht nur die Armee: Die Schweiz braucht eine sicherheitspolitische Strategie, die bedarfsorientiert das Sicherheitsetat aufgrund der Risiken und Bedrohungen aus ganzheitlicher Perspektive auf die sicherheitspolitischen Instrumente verteilt. Investitionen in die militärische Anpassungsfähigkeit könnten so abgewogen werden gegen Investitionen in die militärische Hard- oder Software, den Ausbau des Nachrichtendienstes, den Bevölkerungsschutz oder die Unterstützung des transnational kooperierenden Bundesamtes für Polizei (Fedpol). Das würde aber bedingen, dass die eidgenössischen Räte nicht separate Budgets pro Sicherheitsorgan, sondern ein pauschales umfassendes Sicherheitsbudget betrachten müssen.

Als Grundlage für eine Defizitanalyse könnte die Risikoanalyse des Bundesamtes für Bevölkerungsschutz dienen, da dieses viele der relevanten Risiken systematisch nach Schadensausmass und nach Eintretenswahrscheinlichkeit bzw. Plausibilität gewichtet. Jedoch müssten die im Kapitel 3 identifizierten Unklarheiten der Risikoanalyse zuerst angegangen werden. Grundsätzlich gilt es, die Szenarien möglichst gut auszudifferenzieren, um eine sinnvolle Plausibilitätseinschätzung zu ermöglichen.

Grundsätzlich gilt es, die Szenarien möglichst gut auszudifferenzieren, um eine sinnvolle Plausibilitätseinschätzung zu ermöglichen.

Aus solch einer differenzierteren Risikoanalyse, ergänzt durch nachrichtendienstliche und militärische Lagebeurteilungen, liessen sich die Fähigkeitslücken der sicherheitspolitischen Instrumente ableiten und ein Priorisierungs- und Umsetzungskonzept erarbeiten, so dass eine bedarfsgerechte Vorsorgeplanung möglich wird. Das Pandemiemanagement der Schweiz hat exemplarisch aufgezeigt, dass es dabei nicht nur um finanzielle Ressourcen, sondern auch um den Aufbau von Strukturen und Kompetenzen geht.

These 5

Transparenz beim Fähigkeitsdialog Beim geplanten Fähigkeitsdialog mit dem Parlament könnte die Armee mehr Transparenz in der zugrundeliegenden Lagebeurteilung schaffen und bei der Begründung der benötigten Fähigkeiten die zugrundeliegenden Bedrohungsszenarien so detailliert wie möglich darlegen.

Um eine bedarfsgerechte und effiziente Sicherheitspolitik zu gewährleisten, wäre es von Nutzen, wenn sich das Parlament und das VBS stärker auf die allgemeinen Fähigkeiten, welche die Armee besitzen muss, einigen würden. Dies, anstatt wie bisher v.a. über Einzelsysteme zu diskutieren (VBS 2021c).

Tatsächlich wird das Parlament 2024 erstmals eine Armeebotschaft erhalten, die die erforderlichen militärischen Fähigkeiten mit einem Zeithorizont von zwölf Jahren beschreibt und auch die geplanten Investitionsausgaben aufführt. Laut VBS führt diese Änderung zur Stärkung der Rolle des Parlaments bei der grundsätzlichen Ausrichtung der Armee und ihrer Fähigkeiten. Entscheidend wird in diesem Zusammenhang die konkrete Ausgestaltung des Fähigkeitsdialogs sein und die sicherheitspolitische Fachkompetenz des Parlaments.

Wichtig wäre es, dass das Parlament verschiedene Szenarien und Fähigkeiten debattieren kann und nicht nur vorgefertigte Lösungen akzeptieren muss. Dabei ist eine klare und transparente Lagebeurteilung seitens VBS entscheidend. Damit Prioritäten gesetzt und die entsprechenden Mittel gesprochen werden können, müssen Bedrohungsszenarien detailliert dargelegt werden. Um eine Plausibilitätseinschätzung vornehmen zu können, müssten die Szenarien u.a. folgenden Konzeptionskriterien entsprechen: [27]

Wichtig wäre es, dass das Parlament verschiedene Szenarien und Fähigkeiten debattieren kann und nicht nur vorgefertigte Lösungen akzeptieren muss.

- Die Szenarien sollten erstens so formuliert sein, dass alle potenziellen Eskalationsstufen einzeln plausibilisiert werden können. Werden alle Eskalationsstufen eines hybriden Konfliktes in ein einziges, überfrachtetes Szenario gepackt, kann es von Expertinnen und Experten oder Parlamentariern kaum sinnvoll bewertet werden. Während beispielsweise ein Truppeneinmarsch in die Schweiz auf absehbare Zeit als wenig plausibel eingestuft werden kann, muss ein Drohnenangriff eher als plausibel betrachtet werden.
- Zweitens sollten in den Szenarien das Ausland miteinbezogen werden. Dies, um konkret aufzuzeigen, wie ein bewaffneter Konflikt auf west-/zentraleuropäischem Boden zustande kommen könnte und mit welcher Wahrscheinlichkeit die Schweiz dabei einem Gegner alleine (ohne Beistand des Auslands) gegenüberstünde. In diesem Zusammenhang sollte auch aufgezeigt werden, inwiefern Investitionen in eine transnationalere Schweizer Sicherheitspolitik einen präventiven Sicherheitsgewinn für die Schweiz darstellen.
- Drittens ist die Täterschaft und die Motivation so konkret wie möglich zu beschreiben, beispielsweise welche Akteure und Länder als Täter bzw. Angreifer in Betracht gezogen werden könnten. Zudem soll erörtert werden, ob der Angriff der Schweiz alleine oder einem Staatenverbund als Ganzes gilt und inwiefern das politische Neutralitätsverständnis der Schweiz, das über die rechtlichen Neutralitätspflichten hinausgeht, ein Sicherheitsgewinn darstellt.

27 Es ist selbstverständlich klar, dass die VBS-internen Bedrohungsanalysen wesentlich detaillierter als die öffentlichen Dokumente sind. Da die Mittelallokation jedoch von der Politik abhängig ist, ist es trotzdem wichtig, die Bedrohungsanalyse (zumindest gegenüber den Entscheidungsträgern) so klar wie möglich zu kommunizieren, um die verschiedenen sicherheitspolitischen Instrumente möglichst effizient auf die identifizierten Bedrohungen auszurichten.

Schlusswort

Angesichts der komplexen und vielfältigen Bedrohungslage ist es schwierig, sich in angemessener Weise gegen alle erdenklichen Bedrohungen zu wappnen. Gewisse Trade-Offs sind für die Schweiz als kleines Land unvermeidbar. Eine transparente Lagebeurteilung sowie eine Mittelallokation, die aktuelle und künftig plausible Bedrohungsbilder konsequent priorisiert, sind entscheidend, um eine effiziente und bedarfsgerechte Sicherheitspolitik zu gewährleisten.

Gewisse Trade-Offs sind für die Schweiz als kleines Land unvermeidbar.

Die Armee fokussiert in ihrer Investitionsplanung zu grossen Teilen auf konventionelle militärische Bedrohungen und plant, innerhalb der nächsten zehn Jahre weiter stark in klassische «Hardware» wie Kampfpanzer zu investieren. Dabei könnte der geografischen Lage inmitten von Europa stärker Rechnung getragen werden. Während russische Panzer und Kampfflugzeuge den Nato- und EU-Schild kaum durchbrechen können, ist die Schweiz russischen oder chinesischen Cyberangriffen potenziell genau gleich stark ausgesetzt wie ein Nachbarland der beiden Staaten. Des Weiteren müssen auch angemessene Kapazitäten bestehen, um unkonventionelle Bedrohungen in städtischem Gebiet zu adressieren. Bei den Investitionen in die Territorialverteidigung am Boden oder in der Luft sollte der Verteidigung im Kontext des gesamten europäischen Kontinents ein höheres Gewicht zugemessen werden.

Mit einer Strategie, die den Sicherheitsetat bedarfsorientiert und pragmatisch aufgrund effektiver Risiken und Bedrohungen auf die sicherheitspolitischen Instrumente verteilt, kann die Schweiz auch in einer Zukunft, die vermutlich von mehr geopolitischen Unruhen geprägt sein wird als die letzten drei Jahrzehnte, ein hohes Mass an Sicherheit für ihre Bürgerinnen und Bürger schaffen.

armasuisse, Bundesamt für Rüstung armasuisse (2021): Sicherheitsrelevante Technologie- und Industriebasis (STIB). *www.ar.admin.ch/de/beschaffung/ruestungspolitik-des-bundesrates/sicherheitsrelevante-technologie-und-industriebasis-stib.html*. Zugriff: 02.12.2021.

Armeebotschaft (2022): Armeebotschaft vom 16. Februar 2022. *www.vbs.admin.ch/de/sicherheit/armee/armeebotschaften/armeebotschaft-2022.detail.document.html/vbs-internet/de/documents/verteidigung/armeebotschaften/2022/Armeebotschaft-2022-d.pdf.html*. Zugriff: 19.02.2022.

Armeebotschaft (2021): Armeebotschaft vom 2. März 2021. *www.vbs.admin.ch/de/sicherheit/armee/armeebotschaften/armeebotschaft-2021.html#dokumente*. Zugriff: 10.11.2021.

Armeebotschaft (2020): Armeebotschaft vom 19. Februar 2020. *www.vbs.admin.ch/content/vbs-internet/de/sicherheit/die-schweizer-armee/die-armeebotschaften-des-vbs/die-armeebotschaft-2020-des-vbs.download/vbs-internet/de/documents/verteidigung/armeebotschaften/2020/Armeebotschaft-2020-d.pdf*. Zugriff: 10.05.2021.

Babs, Bundesamt für Bevölkerungsschutz (2020): Katastrophen und Notlagen Schweiz 2020 – Bericht zur nationalen Risikoanalyse. *www.babs.admin.ch/content/babs-internet/de/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse/_jcr_content/contentPar/tabs/items/fachunterlagen/tabPar/downloadlist/downloadItems/109_1604480153059.download/KNSRisikobericht2020-de.pdf*. Zugriff: 09.04.2021.

Babs, Bundesamt für Bevölkerungsschutz (2017): Hintergrundbericht zur nationalen Strategie zum Schutz kritischer Infrastrukturen 2018-2022. 08.12.2017. *www.babs.admin.ch/content/babs-internet/de/aufgabenbabs/ski/publikationen/_jcr_content/contentPar/accordion/accordionItems/nationale_ski_strate/accordionPar/downloadlist/downloadItems/9_1518536145610.download/20171208_HintergrundbNatSKI-Strategie2018-2022_de.pdf*. Zugriff: 14.10.2021.

Babs, Bundesamt für Bevölkerungsschutz (2015): Katastrophen und Notlagen Schweiz – Technischer Risikobericht 2015. *www.newsd.admin.ch/newsd/message/attachments/40200.pdf*. Zugriff: 09.04.2021.

Baezner, Marie (2020): Study on the Use of Reserve Forces in Military Cybersecurity. Report. CSS Cyberdefense Reports. ETH Zurich. *doi:10.3929/ethz-b-000413590*.

Bundesanwaltschaft (2020): Update zum Tötungsdelikt in Morges. Medienmitteilung der Bundesanwaltschaft vom 16.09.2020. *www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-80428.html*. Zugriff: 25.06.2021.

Bundesministerium für Landesverteidigung (2019): Unser Heer 2030: Bericht zum Zustand des Bundesheeres. *www.bundesheer.at/archiv/a2019/unserheer2030/index.shtml#*. Zugriff: 25.06.2021.

Bundesrat (2021a): Die Sicherheitspolitik der Schweiz – Bericht des Bundesrates. *www.newsd.admin.ch/newsd/message/attachments/66420.pdf*. Zugriff: 09.12.2021.

Bundesrat (2021b): Air2030: Bundesrat beschliesst Beschaffung von 36 Kampfflugzeugen des Typs F-35A. Medienmitteilung des Bundesrates vom 30.06.2021. *www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-84275.html*. Zugriff: 04.07.2021.

Bundesrat (2020a): Entflechtung und Weiterentwicklung der RUAG nach dem Cyberangriff auf Kurs. Medienmitteilung des Bundesrates vom 24.02.2020. *www.vbs.admin.ch/content/vbs-internet/de/vbs/bundesnahe-betriebe/ruag-holding-ag.detail.nsb.html/78198.html*. Zugriff: 05.06.2021.

Bundesrat (2020b): Stellungnahme des Bundesrates vom 19.08.2020 zur Interpellation Martin Min Li (20.3496) – Aufgaben- und Rollenteilung in den Bereichen Cybersicherheit und -abwehr. *www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20203496*. Zugriff: 05.06.2021.

Bundesrat (2019a): Bundesrat fällt Richtungsentscheid für Modernisierung der Bodentruppen. Medienmitteilung des Bundesrates vom 16.05.2019. *www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-75062.html*. Zugriff: 09.12.2021.

Bundesrat (2019b): Stellungnahme des Bundesrates vom 06.11.2019 zur Interpellation Dittli Josef (19.4091) – Kampfdrohneneinsätze in Saudi-Arabien. Was bedeutet das für die Sicherheit der Schweiz? *www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20194091*. Zugriff: 08.08.2021.

Bundesrat (2019c): Botschaft zu einem Planungsbeschluss über die Beschaffung neuer Kampfflugzeuge. Botschaft des Bundesrates vom 26.06.2019. *www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-75578.html*. Zugriff: 14.04.2021.

Bundesrat (2018): Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022. 18. April 2018. *www.ncsc.admin.ch/dam/ncsc/de/dokumente/strategie/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.* Zugriff: 10.10.2021.

Bundesrat (2016a): Erkenntnisse im Zusammenhang mit Cyber-Spionage-Angriff auf RUAG. Medienmitteilung des Bundesrates vom 23.05.2016. *www.ncsc.admin.ch/ncsc/de/home/dokumentation/medienmitteilungen/newslist.msg-id-61788.html*. Zugriff: 12.04.2021.

Bundesrat (2016b): Die Sicherheitspolitik der Schweiz – Bericht des Bundesrates vom 24.08.2016. *www.fedlex.admin.ch/eli/fga/2016/1678/de*. Zugriff: 09.12.2021.

CSIS, Center For Strategic & International Studies (2021): Significant Cyber Incidents. *www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents*. Zugriff: 08.04.2021.

CSIS, Center For Strategic & International Studies (2020): The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense. Von Shaan Shaikh und Wes Rumbaugh. 8.12.2020. *www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense*. Zugriff: 08.04.2021.

Defense News (2022): NATO brings Finland, Sweden on board for all Ukraine conflict discussions. Von: Vivienne Machi. 04.02.2022. *https://www.defensenews.com/global/europe/2022/03/04/nato-brings-finland-sweden-on-board-for-all-ukraine-conflict-discussions/*. Zugriff: 08.03.2022.

Detsch, Jack (2021): The U.S. Army Goes to School on Nagorno-Karabakh Conflict – Off-the-shelf air power changes the battlefield of the future. Foreignpolicy report vom 30.03.2021. *https://foreignpolicy.com/2021/03/30/army-pentagon-nagorno-karabakh-drones/*. Zugriff: 07.04.2021.

Economist (2019): How Nato is shaping up at 70. Economist Special Report Mar 16th 2019 edition. *www.economist.com/special-report/2019/03/14/how-nato-is-shaping-up-at-70*. Zugriff: 12.04.2021.

EFK, Eidgenössische Finanzkontrolle (2021): Prüfung der Informatiksicherheit – RUAG MRO Holding AG. Prüfbericht vom 22.02.2021, Bern. *www.efk.admin.ch/images/stories/efk_dokumente/publikationen/_sicherheit_und_umwelt/verteidigung_und_armee/20431/20431BE-Endgueltige-Fassung-V04.pdf*. Zugriff: 12.04.2021.

EFV, Eidgenössische Finanzverwaltung (2021): Ausgaben nach Aufgabengebiet. Datencenter der EFV. *www.efv.admin.ch/efv/de/home/finanzberichterstattung/daten/datencenter.spa.EIS.app/eisui/index.html?#!/revenueExpenses/expensesAdminist-*

rativeUnits?spa_from=2014&spa_to=2020&spa_series=JE_S_VJETD002_Q921_0016. Zugriff: 10.08.2021.

Europäisches Parlament, European Parliament (2021): The European Union's strategic compass process. EPRS, European Parliamentary Research Service. *www.europarl.europa.eu/EPRS/graphs/EPRS_Strategic_Compass_final.pdf*. Zugriff: 03.12.2021.

Europäisches Parlament, European Parliament (2019): Defence: is the EU creating a European army? *www.europarl.europa.eu/news/en/headlines/security/20190612STO54310/eu-army-myth-what-is-europe-really-doing-to-boost-defence*. Zugriff: 20.05.2021.

Europäische Union, European Union, External Action Service (2017): EU Battlegroups. *https://eeas.europa.eu/headquarters/headquarters-Homepage/33557/eu-battlegroups_en*. Zugriff: 20.05.2021.

Eurostat (2021): General government expenditure by function (COFOG) – Defence. Eurostat Data Browser. h*ttps://ec.europa.eu/eurostat/databrowser/view/GOV_10A_EXP__custom_1273557/default/table?lang=en*. Zugriff: 07.07.2021.

Fedpol (2020a): Jahresbericht 2020 Terrorismus. *https://fedpol.report/de/terrorismus/zum-schutz-der-schweiz*. Zugriff: 10.01.2022.

Fedpol (2020b): Jahresbericht 2020 (Transnationale Kriminalität). *https://fedpol.report/de/transnationale-kriminalitaet/wanted*. Zugriff: 10.01.2022.

Financial Times (2021): UK military makes sweeping cuts as focus moves to technological warfare. *www.ft.com/content/125a82ca-883f-4dcd-84e5-68b98ae45f92*. Zugriff: 12.10.2021.

Finnische Regierung, Finnish Government, Ministry for Foreign Affairs (2020): Government Report on Finnish Foreign and Security Policy 2020 – security and global responsibility sharing go hand in hand. 29.10.2020. *https://valtioneuvosto.fi/en/-/government-report-on-finnish-foreign-and-security-policy-2020-security-and-global-responsibility-sharing-go-hand-in-hand-1*. Zugriff: 12.10.2021.

Finnisches Verteidigungsministerium, The Finnish Defence Forces (2021): International Exercises. *https://puolustusvoimat.fi/en/international-exercises*. Zugriff: 12.10.2021.

Fiott, Daniel (2020): Uncharted Territory? – Towards a common threat analysis and a strategic compass for EU security and defence. Brief 16/ July 20 of the European Union Institute for Security Studies. *www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2016%20Strategic%20Compass_0.pdf*. Zugriff: 14.05.2021.

Foreign Affairs (2022): Xi Jinping's New World Order – Can China Remake the International System?. Von: Elizabeth Economy. *https://reader.foreignaffairs.com/2021/12/14/xi-jinpings-new-world-order/content.html*. Zugriff: 10.01.2022.

Frisell, Eva Hagström und Pallin, Krister (2021): Western Military Capability in Northern Europe 2020 – Part I: Collective Defence. Swedish Defence Research Agency "FOI" Report vom Februar 2021.

Gärtner, Heinz (2018): Austria: Engaged Neutrality. In: A. Cottey (Hrsg.), The European Neutrals and NATO, New Security Challenges. *https://doi.org/10.1057/978-1-137-59524-9_6*. S. 129–149.

Gleditsch, Nils Petter; Wallensteen, Peter; Eriksson, Mikael; Sollenberg, Margareta und Strand, Håvard (2002): Armed Conflict 1946-2001: A New Dataset. In: Journal of Peace Research, 39(5), S. 615–637. *doi: 10.1177/0022343302039005007*

Grüter, Kurt (2019): Die Beurteilung von Offsets bei Rüstungsbeschaffungen. Bericht von Kurt Grüter zuhanden von Frau Bundesrätin Viola Amherd vom 30. April 2019, Bern. *www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi_rLeUweD0AhVag_0HHW-5JBLUQFnoECAYQAQ&url=https%3A%2F%2Fwww.newsd.admin.ch%2Fnews-*

d%2Fmessage%2Fattachments%2F56767.pdf&usg=AOvVaw01dfvKOXzPStMXkusID3G2. Zugriff: 02.05.2021.

Hauser, Gunther; Mantovani, Mauro; Krause, Dan und Staack, Michael (2020): Deutschland – Österreich – Schweiz Sicherheitspolitische Zielsetzungen – militärpolitische Ausrichtungen. (Gunther Hauser, Hrsg.). Schriftenreihe der Landesverteidigungsakademie, Republik Österreich.

Hellquist, Elin und Lundholm, Kajsa Tidblad (2021): National Defence and International Military Missions – The Swedish Armed Forces at home and abroad 1958–2020. Swedish Defence Research Agency "FOI" Report vom Februar 2021.

IISS, The International Institute of Strategic Studies (2021): The military balance 2021. (James Hackett, Hrsg.). *www.taylorfrancis.com/books/9781003177777.* Zugriff: 01.04.2021.

Lago, Pascal und Schnell, Fabian (2020): Die Zukunft der Sicherheitspolitik in Europa – Avenir Suisse International Think Tank Report on Security in Europe. *https://cdn.avenir-suisse.ch/production/uploads/2020/01/International_Think_Tank_Report_on_Security_in_Europe_2020.pdf*. Zugriff: 12.07.2021.

Locher, Anna (2010). EU-Mitgliedschaft, Krisenmanagement und Territorialverteidigung: Die finnische Sicherheits- und Verteidigungspolitik im Wandel. In Bulletin 2010 zur schweizerischen Sicherheitspolitik (S. 27–53). Center for Security Studies (CSS), ETH Zürich.

Lockheed Martin (2022): F-35 Global Partnership. *www.lockheedmartin.com/en-us/products/f-35/f-35-global-partnership.html*. Zugriff: 06.02.2022.

Mandia, Kevin (2020): FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community. FireEye Stories Blog, 08. Dezember. *www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html*. Zugriff: 09.12.2021.

Maschmeyer, Lennart (2021): The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. In: International Security, 46(2), S. 51–90. *https://doi.org/10.1162/isec_a_00418*. Zugriff: 14.3.2022

Milizkommission C VBS (2012): Die Bedeutung der Armee für die Schweiz – Eine ganzheitliche volkswirtschaftliche Analyse von Nutzen und Kosten. *www.newsd.admin.ch/newsd/message/attachments/27797.pdf*. Zugriff: 12.04.2021.

NATO, North Atlantic Treaty Organization (2021a): Relations with Sweden. *www.nato.int/cps/en/natohq/topics_52535.htm*. Zugriff: 12.04.2021.

NATO, North Atlantic Treaty Organization (2021b): Relations with Finland. *www.nato.int/cps/en/natohq/topics_49594.htm*. Zugriff: 12.04.2021.

NCSC, Nationales Kompetenzzentrum für Cybersicherheit (2021a): Informationssicherung – Lage in der Schweiz und International. Halbjahresbericht 2020/2, Bern: Mai 2021. *www.ncsc.admin.ch/dam/ncsc/de/dokumente/dokumentation/lageberichte/NCSC_2020-2_HJB_DE.pdf.download.pdf/NCSC_2020-2_HJB_DE.pdf*. Zugriff: 09.12.2021.

NCSC, Nationales Kompetenzzentrum für Cybersicherheit (2021b): Das NCSC. *www.ncsc.admin.ch/ncsc/de/home/ueber-ncsc/das-ncsc.html*. Zugriff: 12.04.2021.

NDB, Nachrichtendienst des Bundes (2021): «Sicherheit Schweiz 2021»: Lagebericht des Nachrichtendienstes des Bundes. *www.newsd.admin.ch/newsd/message/attachments/67044.pdf*. Zugriff: 09.12.2021.

NDB, Nachrichtendienst des Bundes (2020): «Sicherheit Schweiz 2020»: Lagebericht des Nachrichtendienstes des Bundes. *www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-80848.html*. Zugriff: 09.04.2021.

NDB, Nachrichtendienst des Bundes (2019): «Sicherheit Schweiz 2019»: Lagebericht des Nachrichtendienstes des Bundes. *www.newsd.admin.ch/newsd/message/attachments/57073.pdf*. Zugriff: 09.12.2021.

NZZ, Neue Zürcher Zeitung (2022): «Cyberangriffe in der Ukraine: «Die grösste Wirkung ist, dass man Panik in die Gesellschaft injiziert». Von: Lukas Mäder. 27.01.2022. *www.nzz.ch/technologie/cyberangriffe-in-der-uk-*

raine-die-groesste-wirkung-ist-dass-man-panik-in-die-gesellschaft-injiziert-ld.1665344. Zugriff: 07.02.2022.

NZZ, Neue Zürcher Zeitung (2021a): «Bezahle oder leide!»: Erst sah es so aus, als würde Comparis der Cyberattacke standhalten. Nun haben sich die Verantwortlichen aber erpressen lassen – aus praktischen Gründen. Von: Gioia da Silva. 30.07.2021. *www.nzz.ch/technologie/comparis-bezahlt-nun-doch-loesegeld-an-cyber-erpresser-ld.1638153?reduced=true*. Zugriff: 10.08.2021.

NZZ, Neue Zürcher Zeitung (2021b): Noch vor den Sommerferien fällt der Bundesrat den Entscheid für den neuen Kampfjet. Nun kommt Kritik von unerwarteter Seite. Von: Georg Häsler Sansano. 21.06.2021. *www.nzz.ch/schweiz/schweiz-kritik-am-kampfjet-von-unerwarteter-seite-ld.1630834*. Zugriff: 05.07.2021.

NZZ, Neue Zürcher Zeitung (2021c): Interview mit Armeechef Thomas Süssli und Divisionär Alain Vuitel – «Ein Cyberangriff der Armee würde Monate oder Jahre dauern». Von Lukas Mäder, Georg Häsler Sansano. Bern 06.01.2021. *www.nzz.ch/technologie/cyberangriffe-ist-die-armee-fuer-den-cyberkrieg-gewappnet-ld.1590150*. Zugriff: 05.07.2021.

NZZ, Neue Zürcher Zeitung (2021d): Externe Untersuchung bei der Ruag: «Wir haben ernstzunehmende Sicherheitsmängel gefunden». Von Lukas Mäder, Georg Häsler Sansano. Bern 03.06.2021. *www.nzz.ch/technologie/externe-untersuchung-bei-der-ruag-wir-haben-ernstzunehmende-sicherheitsmaengel-gefunden-ld.1628529*. Zugriff: 05.07.2021.

NZZ, Neue Zürcher Zeitung (2021e): Daten von hohen Offizieren waren im Internet zugänglich – und die Armee spielt die Brisanz herunter. Von Lukas Mäder, Georg Häsler Sansano. Bern 09.03.2021. w*ww.nzz.ch/technologie/daten-von-hohen-offizieren-waren-im-internet-zugaenglich-und-die-armee-spielt-die-brisanz-herunter-ld.1605744*. Zugriff: 05.07.2021.

NZZ, Neue Zürcher Zeitung (2021f): Die Schweiz will sich am EU-Militärprojekt Pesco beteiligen. Von Daniel Steinvorth. Brüssel 21.10.2021. *www.nzz.ch/schweiz/die-schweiz-will-sich-am-eu-militaerprojekt-pesco-beteiligen-ld.1651490*. Zugriff: 24.10.2021.

NZZ, Neue Zürcher Zeitung (2021g): Cyberversicherungen: «Dass häufig Lösegeld bezahlt wird, heizt das Businessmodell der Erpresser an». Von: Lukas Mäder. 20.08.2021. *www.nzz.ch/technologie/cyberversicherungen-dass-haeufig-loesegeld-bezahlt-wird-heizt-das-businessmodell-der-erpresser-an-ld.1642315*. Zugriff: 10.01.2022.

NZZ, Neue Zürcher Zeitung (2020a): Hacker dringen in US-Regierungsbehörden ein. Von: Marie-Astrid Langer. 14.12.2020. *www.nzz.ch/international/usa-finanz-und-handelsministerium-sind-opfer-des-cyberangriffs-ld.1592158?reduced=true*. Zugriff: 06.06.2021.

NZZ, Neue Zürcher Zeitung (2020b): Die Armee kämpft mit Sicherheitsproblemen – und das voraussichtlich noch Jahre. Von: Lukas Mäder. 31.08.2020. *www.nzz.ch/schweiz/armee-it-maengel-bleiben-noch-jahre-bestehen-ld.1573971?reduced=true*. Zugriff: 06.06.2021.

NZZ, Neue Zürcher Zeitung (2020c): Die Armee hat Lücken bei der IT-Sicherheit – und verschweigt dies der internen Aufsicht. Von: Lukas Mäder. 03.07.2020. *www.nzz.ch/schweiz/schweizer-armee-luecken-in-it-sicherheit-werden-verschwiegen-ld.1564138*. Zugriff: 08.06.2021.

Politico (2022): Finnish lawmakers to discuss potential NATO membership. Von: Melissa Heikkilä. 28.02.2022. *https://www.politico.eu/article/finland-nato-membership-sanna-marin-ukraine-russia/*. Zugriff: 08.03.2022.

Rheinmetall Defence (2021): Boxer – Armoured transport vehicle. A heavy weight champion for current operating environments. *www.rheinmetall-defence.com/en/rheinmetall_defence/systems_and_products/vehicle_systems/armoured_wheeled_vehicles/boxer/index.php*. Zugriff: 15.10.2021.

Reuters (2022a): Sweden to send military aid to Ukraine - PM Andersson. Von: Johan Ahlander. 27.02.2022. *https://www.reuters.com/world/europe/sweden-send-military-aid-ukraine-pm-andersson-2022-02-27/*. Zugriff: 08.03.2022.

Reuters (2022b): Finland sends weapons and ammunition to Ukraine in policy shift. Von: Essi Lehto. 28.02.2022. *https://www.reuters.com/world/europe/finland-sends-weapons-ammunition-ukraine-2022-02-28/*. Zugriff: 08.03.2022.

Rundschau, Schweizer Radio und Fernsehen (2021): Angriff auf Bundesbetrieb – Hacker dringen ins Ruag-Netzwerk ein. Von: Nadine Woodtli und Nina Blaser. 19.05.2021. *www.srf.ch/news/schweiz/angriff-auf-bundesbetrieb-hacker-dringen-ins-ruag-netzwerk-ein*. Zugriff: 15.11.2021.

Schwedische Regierung, Swedish Government, Government Offices (2020): Objectives for Swedish Total defence 2021–2025 - Government bill 'Totalförsvaret 2021–2025' - Government.se. The Government of Sweden. *www.government.se/government-policy/defence/objectives-for-swedish-total-defence-2021-2025---government-bill-totalforsvaret-20212025/*. Zugriff: 06.04.2021.

Schweizer Armee (2021a): IKT-Systeme der Armee. *www.vtg.admin.ch/de/aktuell/themen/programme-projekte/ikt-systeme-der-armee.html#ui-collapse-377*. Zugriff: 11.11.2021.

Schweizer Armee (2021b): Missionen – Militärische Friedensförderung seit 1953. *www.vtg.admin.ch/de/aktuell/einsaetze-und-operationen/militaerische-friedensfoerderung/missionen.html*. Zugriff: 11.11.2021.

SIPRI, Stockholm International Peace Research Institute (2021): SIPRI Military Expenditure Database. *www.sipri.org/databases/milex*. Zugriff: 15.08.2021.

SRF, Schweizer Radio und Fernsehen (2016): Cyber-Angriff auf Ruag: Mehr als 20 Gigabyte entwendet. *www.srf.ch/news/schweiz/cyber-angriff-auf-ruag-mehr-als-20-gigabyte-entwendet*. Zugriff: 22.05.2021.

SWI (2022): NATO says Russia still adding troops to Ukraine build-up. Von: Phil Stewart und Sabine Siebold, 16.02.2022. *www.swissinfo.ch/eng/nato-says-russia-still-adding-troops-to-ukraine-build-up/47352782*. Zugriff: 16.02.2022.

Tages Anzeiger (2021): Finanzloch von 100 Millionen – Jetzt muss die Armee sogar bei der Munition sparen. Von Markus Häfliger, 18.10.2021. *www.tagesanzeiger.ch/das-100-millionen-problem-von-armeechef-suess-li-585288818179*. Zugriff: 10.11.2021.

Tages Anzeiger (2020): Interview mit Bundesrätin Viola Amherd – «Die Gefahr durch rechte und linke Extremisten wächst». Von Beni Gafner und Markus Häfliger, 31.01.2020. *www.tagesanzeiger.ch/schweiz/standard/die-gefahr-durch-rechte-und-linke-extremisten-waechst/story/24988380*. Zugriff: 08.04.2021.

Tages Anzeiger (2018): Russische Hacker greifen Labor Spiez an. *www.tagesanzeiger.ch/schweiz/standard/russische-hacker-greifen-labor-spiez-an/story/10982180*. Zugriff: 08.04.2021.

Torossian, Bianca; Fagliano, Lucas und Görder, Tara (2020): Hybrid Conflict: Neither War, Nor Peace. Hague Centre for Strategic Studies.

UCDP/PRIO armed conflict dataset, Peace Pesearch Institute (2021): UCDP/PRIO Armed Conflict Dataset - PRIO. *www.prio.org/Data/Armed-Conflict/UCDP-PRIO/*. Zugriff: 08.04.2021.

UK Government (2021): Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy. Policy Paper vom 16. März 2021. *www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy*. Zugriff: 07.04.2021.

UK House of Commons (2022): Military assistance to Ukraine since the Russian invasion. Report vom 03.03.2022. *https://researchbriefings.files.parliament.uk/documents/CBP-9477/CBP-9477.pdf*. Zugriff: 08.03.2022.

UK Verteidigungsministerium, UK Ministry of Defence (2021): Defence in a Competitive Age. Report vom März 2021. *www.gov.uk/government/publications/defence-in-a-competitive-age*. Zugriff: 07.04.2021.

US Kongress (2012): F-35 Joint Strike Fighter (JSF) Program. Congressional Research Service Report for Congress von Jeremiah Gertler vom 16.02.2012. *https://apps.dtic.mil/sti/pdfs/ADA590244.pdf*. Zugriff: 15.09.2021.

VBS, Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (2022): «Spionage und Cyberattacken sind in der Schweiz denkbar». Interview mit Pälvi Pulli. *https://www.vbs.admin.ch/de/home.detail.news.html/vbs-internet/wissenswertes/2022/220224.html*. Zugriff: 08.03.2022.

VBS, Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (2021a): Air2030: «Wir stellen die Weichen für die nächsten 40 Jahre». *www.vbs.admin.ch/de/aktuell/meldungen/wissenswertes.detail.news.html/vbs-internet/wissenswertes/2021/200118a.html*. Zugriff: 08.07.2021.

VBS, Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (2021b): Strategie Cyber VBS. März 2021. *www.newsd.admin.ch/newsd/message/attachments/66200.pdf*. Zugriff: 08.07.2021.

VBS, Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (2021c): Bundesrat stärkt Einbezug des Parlamentes in die längerfristige Ausrichtung der Armee. Medienmitteilung des Bundesrates vom 04.06.2021. *www.vbs.admin.ch/de/aktuell/medienmitteilungen.detail.nsb.html/83828.html*. Zugriff: 08.07.2021.

VBS, Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (2019): Grundlagenbericht Zukunft der Bodentruppen vom 05. 2019. *www.vbs.admin.ch/de/sicherheit/armee/bodentruppen.detail.document.html/vbs-internet/de/documents/verteidigung/bodentruppen/Grundlagenbericht-Zukunft-Bodentruppen-d.pdf.html*. Zugriff: 23.04.2021.

VBS, Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (2017a): Cyberangriff auf die Bundesverwaltung entdeckt und Massnahmen ergriffen. Medienmitteilung des VBS vom 15.09.2017. *www.vbs.admin.ch/de/aktuell/medienmitteilungen.detail.nsb.html/68135.html*. Zugriff: 23.04.2021.

VBS, Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (2017b): Luftverteidigung der Zukunft - Bericht der Expertengruppe Neues Kampfflugzeug vom 05. 2017. *www.vbs.admin.ch/de/dokumente/suche.detail.document.html/vbs-internet/de/documents/verteidigung/sicherheitluftraum/Bericht-Luftverteidigung-der-Zukunft-d.pdf.html*. Zugriff: 23.04.2021.

VBS, Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (2017c): Aktionsplan für Cyber-Defence APCD vom 09.11.2017. *www.vbs.admin.ch/de/home/suche/suchmaske.detail.document.html/vbs-internet/de/documents/verteidigung/cyber/Aktionsplan-Cyberdefense-d.pdf.html*. Zugriff: 23.04.2021.

VBS, Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport und EDA, Eidgenössisches Departement für auswärtige Angelegenheiten (2004): Die Neutralität der Schweiz. *www.eda.admin.ch/eda/de/home/das_eda/publikationen/alle-publikationen.html/publikationen/de/eda/schweizer-aussenpolitik/die-neutralitaet-der-schweiz*. Zugriff: 04.04.2021.

Zandee, Dick; Deen, Bob; Kruijver, Kimberley und Stoetman, Adája (2020): European strategic autonomy in security and defence. Clingendael Report vom Dezember 2020, The Hague, Netherlands. Netherlands Institute of International Relations “Clingendael”.

avenir suisse

Zürich
Rotbuchstrasse 46
8037 Zürich
Tel +41 44 445 90 00
Fax +41 44 445 90 01

Lausanne
Chemin de Beau-Rivage 7
1006 Lausanne
Tel +41 21 612 66 10

www.avenir-suisse.ch
info@avenir-suisse.ch