Bern, den 20. September 2024

VBS. Subsidiarität und Cybersicherheit

Bericht des Bundesrates in Erfüllung des Postulates 22.3368 Sicherheitspolitische Kommission NR vom 9. Mai 2022

Inhaltsverzeichnis

Zusammenfassung

Das Subsidiaritätsprinzip ist ein zentrales Element des schweizerischen Staatsrechts. Es besagt, dass Aufgaben primär von der untersten Staatsebene übernommen werden. Der Bund übernimmt demnach nur Aufgaben, welche die Kräfte der Kantone übersteigen. Das Subsidiaritätsprinzip ist in der Bundesverfassung verankert und gilt sowohl für die Aufgaben- und Kompetenzverteilung zwischen Bund, Kantonen und Gemeinden sowie die Ausübung der Kompetenzen. Im Bereich der inneren Sicherheit sind Bund und Kantone gemeinsam zuständig, wobei die Verantwortung grundsätzlich bei den Kantonen liegt. Die Armee unterstützt die zivilen Behörden nur, wenn deren Mittel nicht ausreichen und die Voraussetzungen zur Unterstützung gemäss Artikel 67 Militärgesetz[1] erfüllt sind. Aufgrund der föderalen Kooperation nach Artikel 44 Bundesverfassung[2] sind die Kantone und der Bund zur gegenseitigen Unterstützung verpflichtet. Artikel 14 Regierungs- und Verwaltungsorganisationsverordnung[3] verpflichtet die Verwaltungseinheiten des Bundes zur Zusammenarbeit. (Kapitel 2)

Der Schutz vor Cyberbedrohungen ist eine gemeinsame Verantwortung von Wirtschaft, Gesellschaft und Staat. Grundsätzlich sind alle Akteure für ihre eigene Sicherheit verantwortlich. Innerhalb des VBS nehmen die Ämter verschiedene Aufgaben im Bereich der Cybersicherheit wahr. Nur zwei Leistungen erfolgen im Bereich Cybersicherheit subsidiär: der Assistenzdienst der Armee und die subsidiäre technische Unterstützung von privaten Betreiberinnen kritischer Infrastrukturen durch das Bundesamt für Cybersicherheit. Die übrigen Cyberaufgaben, die durch das VBS wahrgenommen werden, lassen sich in zwei Kategorien einteilen: (1) Bei Leistungen, die gegenüber Dritten erbracht werden, wurde die Subsidiaritätsabwägung bereits bei Erlass des entsprechenden Gesetzes vorgenommen. (2) Bei Leistungen, welche die Ämter des VBS für den Bund selbst erbringen, muss keine Subsidiaritätsabwägung getroffen werden. (Kapitel 3)

Das VBS verfügt sowohl im militärischen als auch im zivilen Bereich über umfassende Cyberkompetenzen. Die Erkenntnisse aus dem Bericht zeigen jedoch, dass eine Zusammenarbeit zwischen dem militärischen Teil des Kommando Cyber und dem Bundesamt für Cybersicherheit nur unter den Voraussetzungen des Assistenzdienstes der Armee erfolgen kann. Der Bundesrat entscheidet über den Assistenzdienst. Dieser prozessuale Weg über den Bundesrat erschwert die gleichzeitig effiziente und rechtlich abgestützte Zusammenarbeit zwischen dem BACS und dem Kommando Cyber, da im Cyberbereich spezialisierte Mitarbeitende schnell und gezielt eingesetzt werden müssen. Der Assistenzdienst bei Katastrophen im Inland kann hingegen vom VBS alleine entschieden werden. Es fehlt an einer Rechtsgrundlage, damit das Kommando Cyber auf einem solchen vereinfachten Weg Unterstützungsleistungen der Armee an das Bundesamt für Cybersicherheit erbringen kann. Um diese Problematik anzugehen und die zeitnahe Erbringung von Unterstützungsleistungen aus dem Kommando Cyber an das Bundesamt für Cybersicherheit sicherzustellen, soll die Schaffung einer rechtlichen

[1] Bundesgesetz über die Armee und die Militärverwaltung vom 3. Februar 1995 (Militärgesetz, MG; SR 510.10).
[2] Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV; SR 101).
[3] Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998 (RVOV; SR 172.010.1).

Grundlage geprüft werden, die einen effizienten und zeitnahen Einsatz ermöglicht. Aus diesem Grund leitet der Bericht folgende Handlungsmassnahme ab:

Das Bundesamt für Cybersicherheit (BACS) prüft in Zusammenarbeit mit dem Kommando Operationen, dem Kommando Cyber, dem Generalsekretariat VBS (GS-VBS), dem Staatssekretariat für Sicherheitspolitik (SEPOS) und dem Sicherheitsverbund Schweiz (SVS) die Schaffung von Rechtsgrundlagen für vereinfachte Unterstützungsleistungen des Kommando Cyber zugunsten des BACS. Das BACS unterbreitet dem Bundesrat bis Ende 2026 Varianten zum weiteren Vorgehen. (Kapitel 4)

Abkürzungsverzeichnis

Abs.	Absatz
armasuisse	Bundesamt für Rüstung
Art.	Artikel
BA	Bundesstaatsanwaltschaft
BABS	Bundesamt für Bevölkerungsschutz
BACS	Bundesamt für Cybersicherheit
BAZG	Bundesamt für Zoll und Grenzsicherheit
BBl	Bundesblatt
BevSV	Verordnung über den Bevölkerungsschutz (Bevölkerungsschutzverordnung; SR 520.12)
BGE	Entscheidungen des Schweizerischen Bundesgerichts
BORS	Behörden und Organisationen für Rettung und Sicherheit
bspw.	beispielsweise
Bst.	Buchstabe
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (SR 101)
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit vom 21. März 1997 (SR 120)
BZG	Bundesgesetz über den Bevölkerungsschutz und den Zivilschutz (Bevölkerungs- und Zivilschutzgesetz; SR 520.1)
bzw.	beziehungsweise
ca.	circa
CCD CoE	Cooperative Cyber Defence Centre of Exellence in Tallinn
CEA	Dienst für Cyber- und elektromagnetische Aktionen
CERT	Computer Emergency Response Team
CSS	Center for Security Studies
CTC	Cyber Training Center
CYD Campus	Cyber-Defence Campus
E.	in BGE Erwägung
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
et al.	et alii = und weitere
etc.	et cetera
f./ff.	und folgende (Seite/Seiten)
fedpol	Bundesamt für Polizei
Fn.	Fussnote
gem.	gemäss
GS-VBS	Generalsekretariat des VBS
Hrsg.	Herausgeber, Herausgeberin
IKT	Informations- und Kommunikationstechnik
inkl.	inklusive
insb.	insbesondere
ISG	Bundesgesetz über die Informationssicherheit beim Bund vom 18. Dezember 2020 (Informationssicherheitsgesetz; SR 128)
ISV	Verordnung über die Informationssicherheit in der Bundesverwaltung und der Armee vom 8. November 2023 (Informationssicherheitsverordnung; SR 128.1)
KKJPD	Kantonale Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren

KKPKS	Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten der Schweiz.
MCAV	Verordnung über die militärische Cyberabwehr
MELANI	Melde- und Analysestelle Informationssicherung
MG	Bundesgesetz über die Armee und die Militärverwaltung vom 3. Februar 1995 (Militärgesetz, SR 510.10)
MSK	mobiles, breitbandiges Sicherheitskommunikationssystem
N	Randnote(n)
NCS	Nationale Cyberstrategie
NCSC	Nationales Zentrum für Cybersicherheit
NDB	Nachrichtendienst des Bundes
NDG	Bundesgesetz über den Nachrichtendienst vom 25. September 2015 (Nachrichtendienstgesetz; SR 121)
NDV	Verordnung über den Nachrichtendienst Nachrichtendienstverordnung vom 16. August 2017 (Nachrichtendienstverordnung; SR 121.1)
NEOC	National Emergency Operations Center, früher NAZ
NFA	Neugestaltung des Finanzausgleichs und der Aufgaben zwischen Bund und Kantonen
OV-VBS	Organisationsverordnung für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport vom 7. März 2003 (SR 172.214.1)
Po.	Postulat
ResMaB	Ressourcenmanagement Bund
revISG	Revidiertes Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), Änderung vom 29. September 2023, BBl 2023 2296
RVOG	Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997 (SR 172.010)
RVOV	Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998 (SR 172.010.1)
Rz.	Randziffern(n)
S.	Seite(n)
SDVN+	Sicheres Datenverbundnetz Plus
SEPOS	Staatssekretariat für Sicherheitspolitik
SGK	St. Galler Kommentar
SKI-Strategie	Nationale Strategie zum Schutz von kritischen Infrastrukturen
SR	Systematische Sammlung des Bundesrechts (Systematische Rechtssammlung)
SVS	Sicherheitsverbund Schweiz
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
VEKF	Verordnung über die elektronische Kriegführung und die Funkaufklärung vom 17. Oktober 2012 (SR 510.292)
vgl.	Vergleiche
VmKI	Verordnung über die militärische Katastrophenhilfe im Inland vom 21. November 2018 (SR 513.75).
WEP 2030	Werterhalt Polycom
z. B.	zum Beispiel
Ziff.	Ziffer

1 Ausgangslage

1.1 Auftrag des Postulats

Der vorliegende Bericht beantwortet das am 9. Mai 2022 überwiesene Postulat 22.3368 «VBS. Subsidiarität und Cybersicherheit», das am 21. März 2022 von der Sicherheitspolitischen Kommission des Nationalrats eingereicht wurde. Das Postulat lautet:

> *Der Bundesrat wird beauftragt in einem Bericht darzulegen, wie der Subsidiaritätsbegriff im VBS neu geprüft wird und wie dieser insbesondere in der Zusammenarbeit mit den Sicherheitsdienstleistungen im Cyberbereich anzuwenden ist.*
>
> *Die Lage in der Ukraine zeigt, dass der Sicherheitsbegriff breiter aufgefasst werden muss, insbesondere im Cyberbereich. Bei einer Verschlechterung der Lage können schnell verschiedene Bereiche betroffen sein: Wirtschaft, Gesellschaft, Verteidigung, Versorgung und weitere. Um den vielschichtigen Gefahren effektiv zu begegnen, müssen auf Bundesebene die vorhandenen Kompetenzen gezielt eingesetzt und Doppelspurigkeiten vermieden werden. Das VBS verfügt über Kompetenzen sowohl im zivilen wie im militärischen Bereich. Eine Trennung von militärischen und zivilen Kompetenzen ist nicht mehr zukunftsfähig.*

Der Bundesrat versteht diesen Auftrag so, dass die Anwendung des Subsidiaritätsprinzips im Cyberbereich an sich nicht in Frage gestellt wird. Die Anwendung des Subsidiaritätsprinzips ist eine staatspolitische Grundsatzfrage, deren Änderung dem Verfassungsgeber obliegt.

Der Auftrag des Postulats lässt sich in zwei Teile gliedern. Im ersten Teil verlangt das Postulat eine Auseinandersetzung mit dem Subsidiaritätsbegriff in Bezug auf die Cybersicherheit (mit Fokus auf das VBS). Es soll dargelegt werden, was unter dem Subsidiaritätsprinzip zu verstehen ist. Im zweiten Teil verlangt das Postulat eine Auseinandersetzung mit den bestehenden Cyberkompetenzen. Zudem soll aufgezeigt werden, wie die Zusammenarbeit gestärkt werden kann.

1.2 Aufbau des Berichts

Im vorliegenden Bericht wird zuerst das Subsidiaritätsprinzip erläutert (Kapitel 2). Danach wird der Begriff der Cybersicherheit erklärt, auf die Verantwortlichkeiten im Rahmen der Cybersicherheit eingegangen und die Cyberaufgaben der Bundesämter im VBS beschrieben (Kapitel 3). Darauf aufbauend wird der Handlungsbedarf in diesem Bereich aufgezeigt (Kapitel 4).

2 Das Subsidiaritätsprinzip

Das Subsidiaritätsprinzip besagt, dass Aufgaben nur dann einer übergeordneten Staatsebene (wie dem Bund) übertragen werden sollen, wenn diese die Aufgaben nachweislich besser erfüllen kann als die untergeordneten Staatsebenen (wie Kantone

oder Gemeinden).[4] In der Schweiz ist das Subsidiaritätsprinzip in Artikel 5a BV[5] und Artikel 43a Absatz 1 BV verankert.

Das Subsidiaritätsprinzip ist ein zentrales Element des schweizerischen Staatsrechts. Das folgende Kapitel vertieft die oben aufgeführte Definition und beleuchtet dabei drei zentrale Dimensionen des Subsidiaritätsprinzips in der Schweiz: «Staat zu Privaten», «Bund zu Kantonen und Gemeinden» und «Armee zu zivilen Behörden». Danach werden weitere Formen der gegenseitigen Unterstützung aufgeführt. Das Kapitel endet mit einer Zusammenfassung der wichtigsten Erkenntnisse.

2.1 Subsidiarität im Verhältnis «Staat zu Privaten»

Das Subsidiaritätsprinzip im Verhältnis zwischen Staat und Privaten reflektiert das Verständnis von Autonomie und Eigenverantwortung. Das Subsidiaritätsprinzip besagt, dass die öffentliche Hand nur dann tätig werden soll, wenn Private oder die Gesellschaft nicht in der Lage sind, die notwendigen Aufgaben selbst zu erfüllen. Der Staat soll nur solche Aufgaben übernehmen, die im öffentlichen Interesse liegen und so wichtig sind, dass sie auch dann erfüllt werden müssen, wenn sie nicht durch Private erfüllt werden (können).[6]

Das Subsidiaritätsprinzip zwischen Staat und Privaten ist ansatzweise auch in der Bundesverfassung verankert. Gemäss Artikel 6 BV nimmt jede Person Verantwortung für sich selbst wahr und trägt nach ihren Kräften zur Bewältigung der Aufgaben in Staat und Gesellschaft bei. Nur wer in Not gerät und nicht in der Lage ist, für sich selbst zu sorgen, hat nach Artikel 12 BV Anspruch auf Hilfe.[7] Nach Artikel 41 Absatz 1 BV stehen die Sozialziele «in Ergänzung zu persönlicher Verantwortung und privater Initiative».

Der Grundsatz der Eigenverantwortung gilt in allen Lebensbereichen, auch im Bereich der Cybersicherheit. So hält die Nationale Cyberstrategie (NCS)[8] fest, dass der Schutz vor Cyberbedrohungen als gemeinsame Aufgabe von Gesellschaft, Wirtschaft und Staat verstanden wird. Dabei sind die Verantwortlichkeiten und Zuständigkeiten klar definiert und werden von allen Beteiligten gelebt. Die Umsetzung der NCS erfolgt daher nach föderalistischen Prinzipien dezentral und in gemeinsamer Verantwortung. Private sind für ihre eigene Cybersicherheit grundsätzlich selbst verantwortlich.[9]

2.2 Subsidiarität im Verhältnis «Bund zu Kantonen und Gemeinden»

Das Subsidiaritätsprinzip besagt, dass eine Aufgabe möglichst von der kleinsten Einheit zu erfüllen ist. Die übergeordnete Einheit soll nur dann eingreifen, wenn die untergeordnete Gebietskörperschaft die Aufgabe nicht allein oder gemeinsam mit anderen

[4] Botschaft vom 14. November 2001 zur Neugestaltung des Finanzausgleichs und der Aufgaben zwischen Bund und Kantonen (NFA), BBl 2002 2291, 2306 und 2547.
[5] Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV; SR 101).
[6] JOHAN ROCHEL, Kommentierung zu Art. 6 BV, in: Stefan Schlegel/Odile Ammann (Hrsg.), Onlinekommentar zur Bundesverfassung – Version: 01.09.2023, N 39 ff., <https://onlinekommentar.ch/fr/kommentare/bv6> (alle Internetquellen wurden zuletzt am 15.05.2024 besucht).
[7] JOHAN ROCHEL, Kommentierung zu Art. 6 BV (Fn. 6), N 34.
[8] Der Schweizerische Bundesrat, «Nationale Cyberstrategie (NCS)» vom April 2023 <https://www.newsd.admin.ch/newsd/message/attachments/76793.pdf>.
[9] Der Schweizerische Bundesrat, «Nationale Cyberstrategie (NCS)» (Fn. 8), S. 12.

bewältigen kann. Dieses Verständnis von Subsidiarität ist in der Bundesverfassung verankert.[10] Das folgende Kapitel erläutert das Zusammenspiel zwischen den verschiedenen Verfassungsartikeln.

Artikel 3 BV regelt die Kompetenzaufteilung zwischen Bund und Kantonen. Er hält fest, dass die Kantone alle Rechte ausüben, die nicht dem Bund übertragen sind. Staatliche Aufgaben fallen somit in der Schweiz nach der Bundesverfassung grundsätzlich in die Zuständigkeit der Kantone (Generalkompetenz). Der Bund ist nur dort zuständig, wo ihm die Bundesverfassung eine Einzelermächtigung erteilt. Die Bundesverfassung regelt somit die Zuständigkeiten und Aufgaben des Bundes abschliessend. Artikel 42 Absatz 1 BV hält dies ausdrücklich fest: «Der Bund erfüllt die Aufgaben, die ihm die Bundesverfassung zuweist.» Der Bund kann somit nur in den Bereichen zuständig sein, in denen ihn die Bundesverfassung für zuständig erklärt und ihm eine Kompetenz zum Handeln einräumt (Prinzip der Einzelermächtigung).[11] Im Umkehrschluss bedeutet dies, dass alle Kompetenzen, die nicht dem Bund zugewiesen sind, bei den Kantonen verbleiben (lückenlose Kompetenzaufteilung).[12]

Im Zusammenhang mit der Kompetenzzuweisung und -erfüllung ist das in Artikel 5*a* BV verankerte Subsidiaritätsprinzip zu beachten. Artikel 5*a* BV verpflichtet Bund und Kantone, bei der Zuweisung und Erfüllung staatlicher Aufgaben den Grundsatz der Subsidiarität zu beachten.

Artikel 43*a* BV konkretisiert diesen Grundsatz. Demnach soll der Bund nur jene Bereiche regeln, welche die Kraft der Kantone übersteigen oder die einer einheitlichen Regelung bedürfen.[13] Der Bund darf somit keine Aufgaben übernehmen, welche die Kantone ebenso gut selbst erfüllen können.[14] Auch das in Artikel 43*a* Absatz 5 BV verankerte Gebot der Bedarfsgerechtigkeit und Wirtschaftlichkeit bei der Erfüllung staatlicher Aufgaben führt nicht zu einer Verschiebung der verfassungsmässigen Aufgabenzuweisung: Selbst wenn der Bund eine Leistung volkswirtschaftlich effizienter erbringen kann als die Kantone, kann dies allein nicht bestimmend sein für eine Zuweisung der Aufgabe an den Bund.[15]

Zum Ausdruck kommt das Subsidiaritätsprinzip auch in der Grundregel, dass die Kantone das Bundesrecht umsetzen (Art. 46 Abs. 1 BV). Artikel 46 Absatz 3 BV verpflichtet den Bund, den Kantonen bei der Umsetzung des Bundesrechts eine möglichst grosse Gestaltungsfreiheit zu belassen und kantonalen Besonderheiten Rechnung zu tragen. Der Bund hat zudem die Eigenständigkeit und Organisationsautonomie der Kantone zu wahren und ihnen ausreichend eigene Aufgaben und Finanzierungsquellen zu belassen (Art. 47 BV).

[10] Botschaft NFA, BBl 2002 2291 (Fn. 4), 2306.
[11] Bericht des Bundesrates in Erfüllung des Postulats Malama 10.3045 vom 3. März 2010. Innere Sicherheit. Klärung der Kompetenzen vom 2. März 2012, BBl 2012 4459, 4479.
[12] Bericht Po. Malama, BBl 2012 4459 (Fn. 11), 4479.
[13] Bericht Po. Malama, BBl 2012 4459 (Fn. 11), 4479; Botschaft NFA, BBl 2002 2291 (Fn. 4), 2460 f.
[14] Bericht Po. Malama, BBl 2012 4459 (Fn. 11), 4479; Botschaft NFA, BBl 2002 2291 (Fn. 4), 2460 f.
[15] Bericht Po. Malama, BBl 2012 4459 (Fn. 11), 4479; Botschaft NFA, BBl 2002 2291 (Fn. 4), 2329 und 2460 f.

Das Subsidiaritätsprinzip ist Ausdruck der Aufgabenautonomie jeder Verwaltungsebene, über den Einsatz ihrer Mittel selbst zu entscheiden und die Aufgabenerfüllung unterschiedlich anzugehen. Diese Aufgabenautonomie ist in Artikel 43 BV ausdrücklich festgehalten: Die Kantone bestimmen, welche Aufgaben und wie sie diese Aufgaben im Rahmen ihrer Zuständigkeiten erfüllen wollen.[16] Das Subsidiaritätsprinzip trägt damit den Anliegen eines modernen Föderalismus Rechnung.[17]

Erst wenn die untere Staatsebene nicht (mehr) in der Lage ist, die Aufgabe sachgerecht zu erfüllen, soll die höhere Staatsebene die Aufgabe übernehmen. Bundeskompetenzen dürfen daher in ihrem Umfang und ihrer Intensität immer nur so weit gehen, wie dies notwendig ist. Die Erweiterung bestehender oder Einführung neuer Bundeskompetenzen bedarf stets einer besonderen Rechtfertigung und einer entsprechenden gesetzlichen Grundlage (vgl. Art. 3 BV).

Neben der Aufgabenzuweisung gilt das Subsidiaritätsprinzip auch für die Aufgabenerfüllung. Bei der Beurteilung, welche Aufgabenverteilung und -erfüllung in diesem Sinne sachgerecht ist, besteht ein politischer Ermessensspielraum.

2.3 Subsidiarität im Verhältnis «Armee zu zivilen Behörden»

Der Begriff «subsidiär» wird nicht nur im Rahmen der verfassungsrechtlichen Aufgabenteilung genannt. Wenn der Staat Leistungen gegenüber Dritten erbringt, die nur unter bestimmten Voraussetzungen erbracht werden, sprechen die Rechtsgrundlagen teilweise ebenfalls von subsidiärer Unterstützung. So unterstützt beispielsweise das Bundesamt für Cybersicherheit (BACS) Betreiberinnen kritischer Infrastrukturen, wenn Cybervorfälle ihre Funktionsfähigkeit gefährden. Eine solche Unterstützung erfolgt gegenüber Privaten subsidiär zu den IT-Leistungen, die auf dem Markt erhältlich sind (ausführlich dazu Kapitel 3.4.7).

Auch im Zusammenhang mit der Armee wird von subsidiären Einsätzen gesprochen, wenn die Armee zivile Behörden bei der Abwehr von schwerwiegenden Bedrohungen der inneren Sicherheit und bei der Bewältigung anderer ausserordentlicher Lagen unterstützt. Das folgende Kapitel geht vertieft auf die subsidiären Einsätze der Armee ein.

Bund und Kantone sorgen gemäss Artikel 57 BV im Rahmen ihrer Zuständigkeiten für die Sicherheit des Landes und den Schutz der Bevölkerung. Sie koordinieren ihre Anstrengungen im Bereich der inneren Sicherheit. Das bedeutet, dass sowohl der Bund als auch die Kantone für die Sicherheit zuständig sind.[18] Grundsätzlich tragen die Kantone die Verantwortung für die innere Sicherheit auf ihrem Gebiet (Polizeihoheit).[19] Der Bund nimmt auch hier nur jene Aufgaben wahr, die ihm die Bundesverfassung ausdrücklich zuweist (bspw. Art. 58 ff. BV und Art. 61 BV).

Die Armee und ihr Einsatz sind ausschliesslich Sache des Bundes (Art. 58 BV). Der Auftrag der Armee ist in Artikel 58 Absatz 2 BV umschrieben. Demnach (1) dient die

[16] Bericht Po. Malama, BBl 2012 4459 (Fn. 11), 4480.
[17] Botschaft NFA, BBl 2002 2291 (Fn. 4), 2305 und 2306.
[18] Botschaft über eine neue Bundesverfassung vom 20. November 1996, BBl 1997 I 1, 237; SGK BV-MÜLLER/MOHLER, Art. 57 N 1.
[19] Botschaft BV, BBl 1997 I 1 (Fn. 18), 237. Vgl. auch Art. 4 Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit vom 21. März 1997 (BWIS; SR 120).

Armee der Kriegsverhinderung und trägt zur Erhaltung des Friedens bei; (2) verteidigt sie das Land und seine Bevölkerung und (3) unterstützt sie die zivilen Behörden bei der Abwehr schwerwiegender Bedrohungen der inneren Sicherheit und bei der Bewältigung anderer ausserordentlicher Lagen. Im Folgenden wird vertieft auf den dritten Auftrag «Unterstützung der zivilen Behörden bei der Abwehr schwerwiegender Bedrohungen der inneren Sicherheit und bei der Bewältigung anderer ausserordentlicher Lagen» eingegangen.

Artikel 65 MG[20] unterscheidet zwischen drei Einsatzarten: Friedensförderungsdienst, Assistenzdienst und Aktivdienst.[21] Für die folgenden Ausführungen sind insbesondere der Aktivdienst und der Assistenzdienst von Interesse.

Aktivdienst wird geleistet, um die Schweiz und ihre Bevölkerung zu verteidigen (Landesverteidigungsdienst), die zivilen Behörden bei der Abwehr von schwerwiegenden Bedrohungen der inneren Sicherheit zu unterstützen (Ordnungsdienst) sowie bei steigender Bedrohung den Ausbildungsstand der Armee zu erhöhen (Art. 76 MG).[22]

Gemäss Artikel 173 Absatz 1 Buchstabe d BV ist die Bundesversammlung für die Anordnung von Aktivdienst zuständig. Nur in dringenden Fällen liegt diese Zuständigkeit beim Bundesrat, der aber die Bundesversammlung unverzüglich einberuft, wenn für einen Einsatz mehr als 4000 Angehörige der Armee aufgeboten werden oder ein Einsatz voraussichtlich länger als drei Wochen dauert (Art. 185 Abs. 4 BV).[23]

Die Armee unterstützt gemäss Artikel 1 Absatz 2 MG die zivilen Behörden, «wenn deren Mittel nicht mehr ausreichen» (Assistenzdienst). Im Folgenden wird vertieft auf diesen Assistenzdienst (Art. 67 MG) eingegangen.

Artikel 67 Absatz 1 Buchstaben a-e MG konkretisieren die Situationen, in denen die Armee zivile Behörden im Inland unterstützen kann:

- bei der Bewältigung ausserordentlicher Lagen, in denen die innere Sicherheit nicht schwerwiegend bedroht ist und die keinen Ordnungsdiensteinsatz erfordern;

- beim Schutz von Personen und besonders schutzwürdigen Sachen, insbesondere von Infrastrukturen, die für Gesellschaft, Wirtschaft und Staat unerlässlich sind (kritische Infrastrukturen);

- bei der Bewältigung von Aufgaben im Rahmen des Sicherheitsverbundes Schweiz und der koordinierten Dienste;

- bei der Bewältigung von Katastrophen, Spitzenbelastungen oder von Aufgaben, die die Behörden mangels geeigneter Personen oder Mittel nicht bewältigen können;

[20] Bundesgesetz über die Armee und die Militärverwaltung vom 3. Februar 1995 (Militärgesetz, MG; SR 510.10).
[21] Bericht Po. Malama, BBl 2012 4459 (Fn. 11), 4512.
[22] Bericht Po. Malama, BBl 2012 4459 (Fn. 11), 4515.
[23] Bericht Po. Malama, BBl 2012 4459 (Fn. 11), 4515.

- bei der Erfüllung anderer Aufgaben von nationaler oder internationaler Bedeutung.

Für einen subsidiären Einsatz der Armee im Bereich der inneren Sicherheit müssen folgende Voraussetzungen erfüllt sein (Art. 1 Abs. 2, Art. 67 Abs. 2 MG):[24]

- Alle geeigneten zivilen Mittel auf jeder Stufe sind im Einsatz und reichen dabei in personeller, materieller oder zeitlicher Hinsicht nicht aus, um die Lage zu meistern.

- Die Unterstützung erfolgt auf Gesuch der betroffenen Behörden von Bund oder Kantonen.

- Die Aufgabe liegt im öffentlichen Interesse.

Das bedeutet, dass sich die Armee darauf beschränken soll, ausserordentliche Belastungsspitzen zu brechen. Sie soll nicht permanent Lücken füllen.[25] Die Grundlast ist somit von den Kantonen zu tragen.[26] Schliesslich ist darauf hinzuweisen, dass grundsätzlich auch Bundesbehörden zivile Behörden im Sinne von Artikel 58 Absatz 2 BV sein können. Allerdings beschränkt Artikel 58 Absatz 2 BV die mögliche Unterstützung der Armee auf zivile Behörden, die im Bereich der Abwehr schwerwiegender Bedrohungen der inneren Sicherheit und bei der Bewältigung anderer ausserordentlicher Lagen tätig sind.[27]

Es wird zwischen der Armee und der Gruppe Verteidigung (Militärverwaltung) unterschieden. Diese Unterscheidung ist relevant, da für die beiden Organisationen unterschiedliche Rechtsgrundlagen existieren und daraus unterschiedliche Unterstützungsmöglichkeiten resultieren. Aus diesem Grund wird im folgenden Abschnitt auf die Struktur der Armee und der Gruppe Verteidigung und die unterschiedlichen Unterstützungsaufgaben eingegangen.

Struktur

- Die Armee ist nicht Teil der Bundesverwaltung, sondern eine staatliche Organisation sui generis.

- Die Gruppe Verteidigung hingegen ist Teil der Bundesverwaltung.

- Trotz dieser Unterscheidung ist die organisatorische Struktur der Gruppe Verteidigung teilweise identisch zur Armee aufgebaut.[28] Das führt zu einer Vermischung der Armeestrukturen mit jener der Gruppe Verteidigung. Das wiederum kann dazu führen, dass militärisches Personal Funktionen der Verwaltung ausführt.

[24] Bericht Po. Malama, BBl 2012 4459 (Fn. 11), 4512.
[25] Bericht Po. Malama, BBl 2012 4459 (Fn. 11), 4511.
[26] Bericht Po. Malama, BBl 2012 4459 (Fn. 11), 4512.
[27] Bericht Po. Malama, BBl 2012 4459 (Fn. 11), 4512.
[28] VBS, Gesamtkonzeption Cyber (GK Cyber) vom März 2022, S. 55 <Cyberfähigkeiten der Armee: Umfassender Eigenschutz und flexibler Einsatz (admin.ch)>.

Unterstützungsaufgaben

- Die im Militärgesetz festgehaltene Unterstützungsaufgabe zu Gunsten der zivilen Behörden ist der Armee zugewiesen und nicht der Gruppe Verteidigung.

- Die Gruppe Verteidigung unterstützt die Leistungserbringung der Armee und erbringt selbst keine direkten Leistungen zu Gunsten Dritter. Artikel 67 Absatz 3 MG hält ausdrücklich fest, dass die Unterstützung durch Truppen sowie Material und Versorgungsgüter der Armee erfolgen, Personal des Bundes kann lediglich beigezogen werden und nur soweit erforderlich.

- Die Gruppe Verteidigung untersteht, wie alle Verwaltungseinheiten des Bundes, dem RVOG[29] und der RVOV[30]. Die Unterstützungsmöglichkeiten auf der Grundlage des RVOG und der RVOV werden im folgenden Kapitel beschrieben. Die Gruppe Verteidigung hat grundsätzlich keine gesetzliche Grundlage, um subsidiär Leistungen zugunsten Dritter direkt zu erbringen. Dies im Gegensatz zu Artikel 67 Absatz 2 MG, welcher der Armee erlaubt, Assistenzdienst zu leisten.

Auf die Schwierigkeiten, die sich aus der beschriebenen Struktur und den unterschiedlichen Rechtsgrundlagen ergeben, wird im Kapitel 4 «Handlungsmassnahmen» eingegangen.

Zuständig für das Aufgebot zum Assistenzdienst ist grundsätzlich der Bundesrat (Art. 70 Abs. 1 Bst. a MG). Davon gibt es zwei Ausnahmen, die im Militärgesetz geregelt sind. Bei Katastrophen im Inland ist das VBS alleine zuständig für das Aufgebot und die Zuweisung an die zivilen Behörden (Art. 70 Abs. 1 Bst. b MG). Bei Katastrophen im Ausland, die einen dringenden Einsatz erfordern, ist das VBS auf Antrag des Eidgenössischen Departements für auswärtige Angelegenheiten (EDA) für das Aufgebot und die Zuweisung an die zivilen Behörden zuständig (Art. 70 Abs. 1 Bst. c MG).

Unabhängig von der Zuständigkeit für das Aufgebot muss ein Assistenzdienst jeweils von der Bundesversammlung bewilligt werden, wenn er länger als drei Wochen dauert oder mehr als 2000 Angehörige der Armee aufgeboten werden sollen (Art. 70 Abs. 2 MG).[31]

Im Kapitel 4 «Handlungsmassnahmen» wird auf den Einsatz bei Katastrophen im Inland Bezug genommen. Aus diesem Grund wird an dieser Stelle ausführlicher darauf eingegangen. Die Verordnung über die militärische Katastrophenhilfe im Inland (VmKl)[32] regelt die Details eines solchen Einsatzes. So hält Artikel 3 Buchstabe c VmKl fest, dass die militärische Katastrophenhilfe durch den Einsatz von Truppen sowie militärischem und zivilem Personal der Gruppe Verteidigung erfolgen kann. Somit können auf dieser Rechtsgrundlage sowohl die Armee als auch die Gruppe Verteidigung für die Unterstützungsleistungen eingesetzt werden.

[29] Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997 (RVOG; SR 172.010).
[30] Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998 (RVOV; SR 172.010.1).
[31] Bericht Po. Malama, BBl 2012 4459 (Fn. 11), 4514.
[32] Verordnung über die militärische Katastrophenhilfe im Inland vom 21. November 2018 (VmKl, SR 513.75).

Artikel 6 VmKI regelt das Verfahren und den Entscheid für einen solchen Einsatz. Die zivile Behörde richtet ihr Gesuch direkt an das Kommando Operationen. Dieses wiederum bereitet den Entscheid zuhanden des VBS vor (Art. 6 Abs. 1 VmKI). Bei zeitlicher Dringlichkeit kann das Kommando Operationen die militärische Katastrophenhilfe anordnen. Eine solche Anordnung ist dem VBS sobald als möglich zum Entscheid zu unterbreiten (Art. 6 Abs. 2 VmKI). Im Falle eines Landesverteidigungsdienstes gelten besondere Bestimmungen, auf die vorliegend nicht genauer eingegangen wird.

Kommt es zu einem solchen Einsatz, bestimmt gemäss Artikel 8 Absatz 1 VmKI die zivile Behörde den Einsatz der Mittel und den Auftrag im Einvernehmen mit dem Kommando Operationen. Artikel 8 Absatz 3 VmKI hält zudem fest, dass die zivile Behörde die Gesamtverantwortung für den Einsatz trägt.

Das Verfahren für einen Einsatz in Katastrophenfällen im Inland ist im Vergleich zu den anderen Assistenzdiensten vereinfacht, da nur das VBS über den Einsatz entscheidet und nicht der gesamte Bundesrat. Ein solcher vereinfachter Prozess existiert nicht für Unterstützungsleistungen bei Cybervorfällen. Auf diese Lücke wird im Kapitel 4 «Handlungsmassnahmen» eingegangen.

Der Sicherheitsverbund Schweiz (SVS) hat in seinem Bericht «Die Subsidiarität und die Grundsätze der Koordination von Milizmitteln der Armee, des Zivilschutzes und des Zivildienstes im Krisenfall» neun Voraussetzungen definiert, die erfüllt sein müssen, damit einem Gesuch um Assistenzdienst entsprochen werden kann.[33] Der Bericht befasst sich jedoch nicht mit der Situation bei einem Cybervorfall. Auch darauf wird im Kapitel 4 «Handlungsmassnahmen» eingegangen.

2.4 Weitere Formen der Unterstützung

Das Subsidiaritätsprinzip wird ergänzt durch den so genannten kooperativen Föderalismus.[34] Darunter versteht man Formen der Zusammenarbeit zwischen den Kantonen, aber auch zwischen Bund und Kantonen.[35] Sie ermöglicht es den Behörden, Ressourcen, Wissen und Informationen gemeinsam zu nutzen, um eine effiziente und effektive Aufgabenerfüllung zu gewährleisten.

Im Verhältnis zwischen Bund und Kantonen (vertikales Verhältnis), aber auch zwischen den Kantonen untereinander (horizontales Verhältnis)[36], verpflichtet Artikel 44 BV Bund und Kantone, sich bei der Erfüllung ihrer Aufgaben zu unterstützen und zusammenzuarbeiten. Das bedeutet, dass die Kantone untereinander zur gegenseitigen Hilfe verpflichtet sind.[37] Dies kann beispielsweise durch Konkordate erfolgen.[38]

---

[33] Sicherheitsverbund Schweiz, Die Subsidiarität und die Grundsätze der Koordination der Milizmittel der Armee, des Zivilschutzes und des Zivildienstes im Kriesenfall, Antwort auf Empfehlung Nr. 4 der Eidgenössischen Finanzkontrolle (20542), November 2023, S. 13 ff., <https://www.svs.admin.ch/de/themen-/krisenmanagement.html>.
[34] SGK BV- SCHWEIZER, Art. 44 N 6.
[35] ULRICH HÄFELIN et al., Schweizerisches Bundesstaatsrecht, 10. Auflage, Zürich 2020, Rz. 1242.
[36] ULRICH HÄFELIN et al. (Fn. 35), Rz. 1245 und 1254.
[37] Botschaft BV, BBl 1997 I 1 (Fn. 18), 209.
[38] PIERRE TSCHANNEN, Staatsrecht der Schweizerischen Eidgenossenschaft, 5. Auflage, Bern 2021, Rz. 556.

Auf Bundesebene verpflichtet Artikel 14 RVOV die Verwaltungseinheiten zur Zusammenarbeit. Sie unterstützen und informieren sich gegenseitig. Zudem koordinieren sie ihre Tätigkeiten und erteilen einander Auskünfte, soweit dies zur Erfüllung der gesetzlichen Aufgaben erforderlich ist. Dazu gehören auch die Leistungen der Gruppe Verteidigung.

2.5 Wichtigste Erkenntnisse

Das Subsidiaritätsprinzip ist ein zentrales Element des schweizerischen Staatsrechts. Es besagt, dass Aufgaben primär von der kleinsten staatlichen Ebene übernommen werden. Der Bund übernimmt demnach nur Aufgaben, welche die Kräfte der Kantone übersteigen. Das Subsidiaritätsprinzip ist in der Bundesverfassung verankert und beeinflusst die Aufgaben- und Kompetenzverteilung zwischen Bund, Kantonen und Gemeinden sowie die Ausübung der Kompetenzen. Im Bereich der inneren Sicherheit sind Bund und Kantone gemeinsam zuständig, wobei die Verantwortung grundsätzlich bei den Kantonen liegt. Die Armee unterstützt zivile Behörden nur, wenn deren Mittel nicht ausreichen und die Voraussetzungen gemäss Artikel 67 MG erfüllt sind. Aufgrund der föderalen Kooperation gemäss Artikel 44 BV sind die Kantone und der Bund zur gegenseitigen Unterstützung verpflichtet. Artikel 14 RVOV verpflichtet die Verwaltungseinheiten des Bundes zur Zusammenarbeit.

In der Folge wird vertieft auf den Begriff Cybersicherheit eingegangen und dargelegt, über welche Fähigkeiten und Kompetenzen die verschiedenen Bundesämter des VBS im Bereich Cyber verfügen.

3 Die Cybersicherheit

3.1 Der Begriff der Cybersicherheit

Unter dem Begriff der Cybersicherheit versteht man einen anzustrebenden Zustand, bei dem die Datenbearbeitung, insbesondere der Datenaustausch zwischen Personen und Organisationen, über Informations- und Kommunikationsinfrastrukturen wie beabsichtigt funktioniert.[39]

3.2 Verantwortlichkeiten Cybersicherheit

Cybersicherheit ist ein Querschnittsthema, das nicht einer einzelnen Behörde zugeordnet werden kann. Dies gilt besonders für die Schweiz, die durch föderalistische Strukturen geprägt ist. Obwohl digitale Interaktionen kaum territorial begrenzt sind, bleibt das verfassungsmässige Prinzip der föderalen Zuständigkeit auch im Cyberraum bestehen. Basierend auf diesem Prinzip haben der Bund und die Kantone jeweils ihre eigenen Cyberorganisationen entwickelt. Neben der Aufgabenverteilung zwischen den verschiedenen staatlichen Ebenen spielt die Zusammenarbeit zwischen öffentlichen und privaten Akteuren im Bereich Cybersicherheit eine entscheidende Rolle. Diese Zusammenarbeit ist vielfältig organisiert und erfolgt über Organisationen, die aus öffentlichen und privaten Akteuren bestehen. Sie beinhaltet auch die direkte Beteiligung von Ver-

[39] Der Schweizerische Bundesrat, «Nationale Cyberstrategie (NCS)» (Fn. 8), S. 37.

bänden und Unternehmen bei der Umsetzung von Massnahmen der Nationalen Cyberstrategie (NCS) sowie die tägliche Kooperation und den Erfahrungsaustausch zwischen privaten und öffentlichen Sicherheitsteams.[40]

Der Bund ergreift die nötigen Massnahmen zur Erhöhung seiner eigenen Cybersicherheit und trägt unter Berücksichtigung des Subsidiaritätsprinzips zur Verbesserung der Cybersicherheit der Wirtschaft und Gesellschaft bei. Dabei gewichtet er die zentrale Bedeutung der kritischen Infrastrukturen entsprechend. Zu den Massnahmen zählt auch die Förderung der internationalen Zusammenarbeit im Bereich Cybersicherheit.

Das BACS ist verantwortlich für die Kernaufgaben im Bereich Cybersicherheit sowie die Koordination mit allen beteiligten Stellen.[41] Die Aufgaben des Bundesamts konzentrieren sich ausschliesslich auf die zivile Cybersicherheit und sind damit klar abgegrenzt von den Zuständigkeiten der Armee im Bereich der Cyberdefence.[42] Das BACS übernimmt keine Aufsichts- oder Regulierungsaufgaben von Fachbehörden in den Sektoren. Diese Fachbehörden bleiben für die Zulassung und laufende operative Aufsicht von Industrieunternehmen und konzessionierten Firmen in Bezug auf sektorspezifische Cybersicherheitsanforderungen zuständig.[43]

Das BACS arbeitet eng mit den Fachämtern zusammen und stellt ihnen sein Fachwissen im Bereich Cybersicherheit zur Verfügung. Die Zuständigkeit für die Cyberstrafverfolgung liegt hauptsächlich bei den Kantonen. Auf Bundesebene sind das Bundesamt für Polizei (fedpol) und die Bundesanwaltschaft (BA) dafür verantwortlich. Die rechtlichen Grundlagen der Organisationen präzisieren die Kompetenzen der jeweiligen Stellen. Gleichzeitig sorgen die Verwaltungseinheiten dafür, innerhalb des gesetzlichen Rahmens einen kontinuierlichen Informations- und Erfahrungsaustausch zu gewährleisten, um eine optimale Abstimmung und die Nutzung von Synergien zu ermöglichen.[44]

Die Kantone gestalten ihre Organisation der Cybersicherheit eigenständig und passen sie an ihre individuellen Bedürfnisse an. Dabei können sie sich an der "Empfehlung für die Umsetzung zur kantonalen Cyber-Organisation" orientieren, die vom SVS erarbeitet und 2020 von der Kantonalen Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) verabschiedet wurde.[45]

Die übergeordnete interkantonale Koordination zu Themen der Cybersicherheit erfolgt über die KKJPD. Dies schliesst jedoch nicht aus, dass sich andere Regierungskonferenzen im Rahmen ihrer Zuständigkeitsgebiete mit Cyberaspekten befassen. Die Zusammenarbeit mit dem Bund wird durch den SVS koordiniert und gefördert.[46]

[40] Der Schweizerische Bundesrat, «Nationale Cyberstrategie (NCS)» (Fn. 8), S. 9.
[41] Vgl. zu den Aufgaben des BACS Kapitel 3.4.7.
[42] Ein Überblick über die Bekämpfung der Cyberkriminalität in der Schweiz: Bericht des Bundesrates in Erfüllung der Postulate 22.3145, Andri Silberschmidt, 16. März 2022, und 22.3017, Sicherheitspolitische Kommission des Nationalrates, 15. Februar 2022, «Wie fit sind die Kantone in der Cyber-Strafverfolgung?».
[43] Der Schweizerische Bundesrat, «Nationale Cyberstrategie (NCS)» (Fn. 8), S. 9 f.
[44] Der Schweizerische Bundesrat, «Nationale Cyberstrategie (NCS)» (Fn. 8), S. 9 f.
[45] Der Schweizerische Bundesrat, «Nationale Cyberstrategie (NCS)» (Fn. 8), S. 10.
[46] Der Schweizerische Bundesrat, «Nationale Cyberstrategie (NCS)» (Fn. 8), S. 10.

3.3 Nationale Cyberstrategie (NCS)

Die NCS spielt eine Schlüsselrolle im Umgang mit Cyberbedrohungen. Sie dient als Leitlinie für den Bund, die Kantone, die Wirtschaft und die Gesellschaft.

Die Cybersicherheit betrifft nahezu alle Lebens-, Wirtschafts- und Verwaltungsbereiche. Alle müssen handeln und stehen gemeinsam in der Verantwortung für den Schutz der Schweiz vor Cyberbedrohungen. Die NCS bestärkt diese gemeinsame Verantwortung, indem sie die Akteure mit den benötigten Kompetenzen in die Pflicht nimmt und die bestehenden Strukturen nutzt. Daraus ergibt sich eine dezentrale Umsetzung, welche aber zentral durch die strategische Führung der NCS gesteuert wird und eine klare Aufgaben- und Rollenverteilung ausweist.

Aus der gemeinsamen Verantwortung ergibt sich auch die gemeinsame Umsetzung der NCS. Bund, Kantone, Wirtschaft und Gesellschaft sollen die Massnahmen der NCS in enger Zusammenarbeit umsetzen und dabei ihre jeweiligen Kompetenzen einbringen. Der zur Strategie gehörende Umsetzungsplan definiert die Zuständigkeiten und Umsetzungsverantwortung für die in der Strategie bestimmten Massnahmen.

Die NCS geht von einem ganzheitlichen, risikobasierten Ansatz aus, mit dem Ziel, die Resilienz der Schweiz hinsichtlich Cyberrisiken zu verbessern. Dies impliziert die Annahme, dass kein vollständiger Schutz vor Cyberbedrohungen möglich ist, die Risiken aber soweit behandelt werden können, dass das verbleibende Risiko tragbar ist. In einem umfassenden Ansatz werden alle relevanten Verwundbarkeiten und Bedrohungen berücksichtigt.

Zusammenfassend: Der NCS liegt ein Verständnis einer subsidiären und partnerschaftlichen Rolle des Staates zugrunde. Dies bedeutet, dass der Staat erst dann eingreift, wenn das Wohlergehen der Gesellschaft wesentlich bedroht ist und private Akteure nicht in der Lage oder nicht willens sind, das Problem selbständig zu lösen. Der Staat kann in diesem Fall unterstützend wirken, Anreize setzen oder regulativ eingreifen, wobei er die entsprechenden Massnahmen in engem Austausch mit den betroffenen Akteuren bestimmt und eine enge Zusammenarbeit mit diesen anstrebt.[47]

3.4 Organisation und Zuständigkeiten im VBS

Die Organisation und die Zuständigkeiten auf Bundesebene im Bereich Cyber sind in drei Hauptbereiche gegliedert.[48]

Im Bereich der *Cybersicherheit* konzentrieren sich alle Massnahmen darauf, präventive Schritte zu unternehmen, mit Zwischenfällen umzugehen und die Resilienz gegenüber Cyberrisiken zu verbessern. Gleichzeitig wird die internationale Zusammenarbeit in diesem Kontext gestärkt.

Der Bereich der *Cyberdefence* umfasst die nachrichtendienstlichen und militärischen Massnahmen, die dem Schutz der für die Landesverteidigung kritischen Systeme, der Abwehr von Cyberangriffen, der Gewährleistung der Einsatzbereitschaft der Armee in

[47] Der Schweizerische Bundesrat, «Nationale Cyberstrategie (NCS)» (Fn. 8), S. 12.
[48] Der Schweizerische Bundesrat, «Nationale Cyberstrategie (NCS)» (Fn. 8), S. 9.

allen Lagen und dem Aufbau von Kapazitäten und Fähigkeiten zur subsidiären Unterstützung ziviler Behörden dienen; dazu zählen auch aktive Massnahmen zur Erkennung von Bedrohungen, zur Identifikation von Angreifern und zur Störung und Unterbindung von Angriffen.

Der Bereich der *Cyberstrafverfolgung* umfasst sämtliche Massnahmen der Polizei und Staatsanwaltschaft auf Bundes- und Kantonsebene, die darauf abzielen, Cyberkriminalität zu bekämpfen. Hierbei wird eine koordinierte Vorgehensweise auf verschiedenen Ebenen verfolgt, um effektiv gegen Cyberkriminalität vorzugehen. Auf Bundesebene sind insbesondere das Bundesamt für Polizei fedpol und die Bundesanwaltschaft zuständig. Das VBS hat in diesem Bereich keine Kompetenzen.

In der Folge wird auf die Cyberzuständigkeiten der Bundesämter im VBS und der Armee eingegangen. Zu den berücksichtigten Organisationseinheiten gehören das Generalsekretariat VBS (GS-VBS), das Staatssekretariat für Sicherheitspolitik (SEPOS), der Nachrichtendienst des Bundes (NDB), das Kommando Cyber, der Cyber-Defence Campus des Bundesamtes für Rüstung armasuisse (CYD Campus), das Bundesamt für Bevölkerungsschutz (BABS) und das Bundesamt für Cybersicherheit (BACS).

3.4.1 Generalsekretariat VBS

Im VBS sind sieben Ämter respektive Gruppen (inkl. das GS-VBS) im Cyberbereich aktiv. Um eine Gesamtübersicht und ein einheitliches Vorgehen sicherzustellen, nimmt das GS-VBS eine koordinative und politisch beratende Rolle im Bereich Cyber auf Stufe Departement ein. In dieser Rolle unterstützt es die Departementschefin VBS bzw. den Departementschef VBS und die Generalsekretärin VBS bzw. den Generalsekretär VBS. Konkret nimmt das GS-VBS die folgenden Aufgaben wahr:

1. *Politische Beratung und Unterstützung*: Das GS-VBS unterstützt die Departementschefin VBS bzw. den Departementschef VBS und die Generalsekretärin VBS bzw. den Generalsekretär VBS bei der politischen Planung, Steuerung und Koordination der departementalen Tätigkeiten im Cyberbereich. Dabei stellt es eine Gesamtübersicht über die Tätigkeiten und Herausforderungen des Departements im Cyberbereich sicher. Zudem stellt das GS-VBS sicher, dass die verschiedenen Handlungen, die auf politischer und strategischer Ebene im Cyberbereich ergriffen werden, sowohl mit den strategischen Prioritäten der Departementschefin VBS bzw. des Departementschef VBS als auch mit der strategischen Weiterentwicklung des Departements übereinstimmen. Das GS-VBS sorgt dafür, dass die Planungen und die Tätigkeiten des Departements mit denjenigen der anderen Departemente und des Bundesrates koordiniert werden. Bei departementsübergreifenden Fragen erarbeitet das GS-VBS eine konsolidierte Position für das Departement und unterstützt eine einheitliche Kommunikation. Es vertritt das Departement in Cyberangelegenheiten in der Bundesverwaltung sowie in nationalen Gremien (bspw. im Steuerungsausschuss der NCS).

2. *Politische Geschäfte*: Das GS-VBS begleitet politische Geschäfte (Departements-, Bundesrats- und Parlamentsgeschäfte) im Cyberbereich auf Stufe Departement. Dabei übernimmt es die politische Beratung und die operative Koordination der Arbeiten.

3. *Referate*: Das GS-VBS nimmt die Referate für die Gruppen respektive die Ämter wahr. Dies tut es auch im Cyberbereich. In dieser Rolle unterstützt es die Departementschefin VBS bzw. den Departementschef VBS und berät sie bzw. ihn bei der Führung der Ämter mit Cyberfähigkeiten.

4. *Aufsichtsfunktion*: Das GS-VBS nimmt die Controlling-Funktion für departementale Strategien wahr, so z. B. auch für die Strategie Cyber VBS. Zudem nimmt das GS-VBS seine Aufsichtsfunktion im Bereich der militärischen Cyberdefence wahr und stellt dafür das Sekretariat.

5. *Sicherheitsmanagement*: Das GS-VBS berät die Generalsekretärin VBS bzw. den Generalsekretär VBS sowie die Verwaltungseinheiten des VBS in Sicherheitsfragen, führt auf Auftrag Audits und Kontrollen durch, koordiniert die Bewältigung von Sicherheitsvorfällen im Departement und leitet die operativen Sicherheitsgremien des VBS.

3.4.2 Staatssekretariat für Sicherheitspolitik

Das SEPOS sorgt in Zusammenarbeit mit weiteren Verwaltungseinheiten des Bundes dafür, dass der Bund über übergeordnete konzeptionelle Grundlagen für eine kohärente Sicherheitspolitik verfügt (Art. 7 Abs. 1 OV-VBS[49]). Es stellt in Zusammenarbeit mit weiteren Verwaltungseinheiten des Bundes eine gesamtheitliche und vorausschauende Sicherheitspolitik auf strategischer Ebene sicher (Art. 7 Abs. 2 OV-VBS), wozu auch die Cyber-Sicherheitspolitik gehört. Es erarbeitet und begleitet die Grundlagen und Vorgaben, koordiniert zwischen den zuständigen Stellen innerhalb des VBS und bezieht weitere Stellen in- und ausserhalb der Bundesverwaltung mit ein.

1. *Koordination*: Das SEPOS koordiniert die sicherheitspolitischen Tätigkeiten des VBS allgemein und damit auch im Cyberbereich auf konzeptioneller Ebene. Dies beinhaltet unter anderem das Monitoring der Strategie Cyber VBS.

2. *Internationale und nationale Vernetzung und Zusammenarbeit*: Das SEPOS stellt die Kohärenz der Governance in den Beziehungen des VBS zu nationalen und internationalen Partnern im Rahmen der definierten Sicherheitspolitik sicher. Das SEPOS ist die sicherheitspolitische Anlaufstelle für nationale und internationale Partner des VBS. Das SEPOS ist verantwortlich für die Koordination der entsprechenden internationalen Beziehungen zwischen den verschiedenen Ämtern innerhalb des Departements sowie mit dem EDA. Es stärkt die internationalen bi- und multilateralen Beziehungen mit den Partnern und führt mit ihnen den Dialog auf strategischer Ebene, zum Beispiel dem Cooperative Cyber Defence Centre of Exellence (CCD CoE) in Tallinn.

3. *Steuerung CSS*: Das SEPOS nimmt die Beziehung des VBS zum Center for Security Studies (CSS) der ETH im Bereich Cyber wahr, steuert dieses und stellt die Vertretung sicher.

4. Die *Fachstelle des Bundes für Informationssicherheit:* Die Fachstelle des Bundes für Informationssicherheit nimmt verschiedene Aufgaben im Rahmen der Informationssicherheit wahr. Sie berät und unterstützt die durch das Informationssicherheitsgesetz

[49] Organisationsverordnung für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport vom 7. März 2003 (OV-VBS; SR 172.214.1).

(ISG)[50] verpflichteten Behörden, deren Informationssicherheitsbeauftragte und die Kantone beim Vollzug des ISG. Zudem gibt sie Empfehlungen ab, wenn die Informationssicherheit des Bundes gefährdet ist. Sie kann auf Antrag Überprüfungen durchführen, die Risiken für die Informationssicherheit beim Einsatz neuartiger Technologien beurteilen und die Informationssicherheit bei wichtigen behördenübergreifenden Projekten steuern und koordinieren. Zudem ist sie Ansprechstelle für Fachkontakte mit inländischen, ausländischen und internationalen Stellen und erstattet dem Bundesrat jährlich Bericht über den Stand der Informationssicherheit des Bundes.[51] Die Fachstelle des Bundes für Informationssicherheit verhandelt Informationsschutzabkommen und sorgt für deren Umsetzung. Sie übernimmt dabei die Rolle der für die Umsetzung der Sicherheitsmassnahmen zuständigen Stelle (National Security Authority) und dient als nationale Anlaufstelle, die einheitliche Standards festlegt und die Eignung der Systeme bestätigt (Security Accreditation Authority).[52]

3.4.3 Nachrichtendienst des Bundes

Der NDB ist ein sicherheitspolitisches Instrument der Schweiz. Seine Aufgaben sind in Artikel 6 NDG[53] definiert. Die Kernaufgaben des NDB sind die Prävention und die Lagebeurteilung zuhanden der politischen Entscheidungstragenden. In diesem Zusammenhang befasst sich der NDB mit der Früherkennung und Bekämpfung von Terrorismus, gewalttätigem Extremismus, Spionage, der Verbreitung von Massenvernichtungswaffen und deren Trägertechnologie, Cyberangriffen auf kritische Infrastrukturen und sicherheitspolitischen Vorgängen im Ausland.

Im Bereich Cybersicherheit nimmt der NDB folgende Aufgaben wahr:

1. *Cyberbedrohungslage*: Der NDB verfolgt und analysiert laufend die Cyberbedrohungslage sowie allfällige Konsequenzen für die Schweiz (Art. 6 Abs. 2 NDB). Die Datenbeschaffung und -bearbeitung zur Beurteilung der Bedrohungslage gemäss Artikel 6 Abs. 2 NDG ist in den Kapiteln 3 und 4 des NDG geregelt.[54] Der NDB beurteilt die Bedrohungslage im Cyberbereich und informiert die verschiedenen Bundesstellen und kantonalen Vollzugsbehörden laufend über allfällige Bedrohungen.[55] Die fortlaufende Beurteilung von Cyberbedrohungen führt zu Produkten, um die breite Öffentlichkeit zu informieren. Hier ist insbesondere der Jahresbericht des NDB zu nennen: Sicherheit Schweiz.

Gemäss Massnahme 3 der NCS sind der NDB und das BACS für die Weiterentwicklung der Lageverfolgung zuständig. Aufgrund der zunehmenden Digitalisierung von Prozessen in verschiedenen Wirtschaftssektoren steigt der Bedarf nach spezifischen, auf diese Sektoren ausgerichtete Einschätzungen zur Bedrohungslage. Diesem Bedarf wird über eine zielgruppengerechte Aufarbeitung der bedrohungsrelevanten Information entgegengekommen.[56] Das BACS gewährt dem NDB zum Zweck des frühzeitigen

[50] Bundesgesetz über die Informationssicherheit beim Bund vom 18. Dezember 2020 (Informationssicherheitsgesetz, ISG; SR 128).
[51] Art. 83 ISG.
[52] Botschaft vom 22. Februar 2017 zum Informationssicherheitsgesetz, BBl 2017 2953, 3090.
[53] Bundesgesetz über den Nachrichtendienst vom 25. September 2015 (Nachrichtendienstgesetz, NDG; SR 121).
[54] Botschaft vom 19. Februar 2014 zum Nachrichtendienstgesetz, BBl 2014 2105, 2144.
[55] Der Schweizerische Bundesrat, «Nationale Cyberstrategie (NCS)» (Fn. 8), S. 16.
[56] Der Schweizerische Bundesrat, «Nationale Cyberstrategie (NCS)» (Fn. 8), S. 16.

Erkennens und Verhinderns von Bedrohungen der inneren oder äusseren Sicherheit, zur Beurteilung der Bedrohungslage und zur nachrichtendienstlichen Frühwarnung zum Schutz kritischer Infrastrukturen nach Artikel 6 Absatz 1 Buchstabe a Ziffer 2 und 5 NDG Zugriff auf Informationen, welche die Identität und die Vorgehensweise der Verursachenden von Cyberangriffen betreffen.[57]

2. *Vorfallsbearbeitung*: Im Rahmen der Vorfallsbearbeitung untersucht der NDB Fälle, die gemäss NDG in seinen Zuständigkeitsbereich fallen. Dabei hat er Zugang zu verschiedenen Informationsquellen. Die in Kapitel 3 und 4 NDG geregelten Beschaffungsmassnahmen sind auch auf Cybervorfälle anwendbar. Insbesondere befasst sich der NDB mit den Themen Spionage mittels Cybermitteln und Bedrohung kritischer Infrastrukturen.[58] Der NDB hat die Aufgabe, zuhanden der Stelle, die sich mit Cyberangriffen befasst, die notwendigen Informationen über drohende oder bereits erfolgte Angriffe zu beschaffen und die Abwehr von Angriffen zu unterstützen.[59]

3. *Analyseprodukte*: Der NDB erstellt Analyseprodukte zuhanden der Bundesverwaltung und für politische Entscheidungstragende. Durch punktuelle mündliche Briefings gibt der NDB die Ergebnisse aus seinen Recherchen und Analysen an die entsprechenden Stellen weiter.

4. *Attribution von sicherheitspolitisch bedeutsamen Cybervorfällen*: Attribution, das heisst die Identifikation der Täterschaft, beschreibt einen ganzheitlichen interdisziplinären Prozess, der die Analyse technischer Eigenschaften eines Cybervorfalls umfasst, den geopolitischen Kontext berücksichtigt und das gesamte nachrichtendienstliche Spektrum zur Informationsbeschaffung nutzt. Attribution ist eine Kernaufgabe des NDB gemäss NCS.[60]

5. *Sensibilisierung*: Der NDB sensibilisiert Unternehmen, Hochschulen und Forschungsinstitutionen der Schweiz und aus Lichtenstein für Bedrohungen im Zusammenhang mit Spionage und Proliferation. Die Sensibilisierung erstreckt sich auch auf die möglichen Bedrohungen, die durch Cyberangriffe verursacht werden können.[61]

6. *Zusammenarbeit*: Der NDB kann sowohl mit anderen Dienststellen des Bundes, mit Dienststellen der Kantone sowie mit Privatpersonen, Unternehmen und Organisationen zusammenarbeiten. Auch die Zusammenarbeit mit der Armee und dem Ausland ist erwünscht.[62] Die Zusammenarbeit zwischen Bund und Kantonen hat einen hohen Stellenwert. Aus diesem Grund verpflichtet das NDG den Bund, zuständige kantonale Behörden über besondere Ereignisse im Aufgabengebiet des NDB und über die Bedrohungslage zu informieren. Dieser Austausch erfolgt vor allem über die KKPKS[63] und

[57] Art 76a Abs. 2 revISG, abrufbar unter: Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), Änderung vom 29. September 2023, BBl 2023 2296. Die Referendumsfrist ist am 18. Januar 2024 unbenutzt abgelaufen.
[58] Art. 6 Abs. 1 Buchstabe a Ziff. 4 und Art. 6 Abs. 5 NDG.
[59] Botschaft NDG, BBl 2014 2105 (Fn. 54), 2144.
[60] Der Schweizerische Bundesrat, «Nationale Cyberstrategie (NCS)» (Fn. 8), S. 15.
[61] Art. 6 Abs. 6 NDG.
[62] Art. 9-12 NDG; Art. 1 Abs. 1 Verordnung über den Nachrichtendienst Nachrichtendienstverordnung vom 16. August 2017 (Nachrichtendienstverordnung, NDV; SR 121.1).
[63] Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten der Schweiz.

die KKJPD[64]. Der NDB kann Informationen an die Bundesanwaltschaft zum Zweck der Strafverfolgung bereitstellen, wenn der NDB im Rahmen seiner Abklärungen den Verdacht hat, dass strafbare Handlungen vorliegen.[65] Das BACS unterstützt den NDB mit periodischen Auswertungen zu Anzahl, Art und Ausmass von Cyberangriffen sowie, auf Anfrage, mit technischen Analysen von Cyberbedrohungen.[66]

7. *Amtshilfe*: Der NDB ist grundsätzlich wie jede andere Amtsstelle berechtigt und verpflichtet, Amtshilfe in den Bereichen zu leisten, wo er sowohl zuständig als auch personell und fachlich dazu in der Lage ist. Der NDB kann hier besondere operative Mittel und Methoden zur Verfügung stellen, beispielsweise Übermittlungs-, Transport- und Beratungsleistungen, über die andere Amtsstellen nicht verfügen.[67]

3.4.4 Kommando Cyber

Die Funktionen und Zuständigkeiten des Kommando Cyber sind in Artikel 96 und Artikel 100 Absatz 1 Buchstabe c MG, Artikel 11 Buchstabe d OV-VBS und in der Verordnung über die militärische Cyberabwehr (insb. Art. 4 MCAV[68]) geregelt.

Die Leistungen des Kommandos Cyber sind auf den Cyber Eigenschutz und auf Aktionen im Cyberraum ausgerichtet. Zudem ist es alleiniger Erbringer von einsatzkritischen IKT Leistungen der Armee. Es erbringt diese Leistungen mit Personen aus der Militärverwaltung und seinen unterstellenten Milizverbänden in allen Lagen. Unter Berücksichtigung des operativen resp. wirkungsraumübergreifenden Gesamtrahmens werden Leistungen des Kommando Cyber im Rahmen von Operationen, Einsätzen und Unterstützungsleistungen durch das Kommando Operationen koordiniert.

Dabei können die Funktionen des Kommandos Cyber in folgende Bereiche unterteilt werden:

1. *Informations- und Kommunikationstechnologie*: Das Kommando Cyber plant und betreibt die einsatzkritische IKT zugunsten der Armee, sowie der Landesregierung und des nationalen Krisenmanagements. Zudem stellt es die in informations- und kommunikationstechnische Bereitschaft der Infrastrukturen und der Truppen zur Aufrechterhaltung der Führungsfähigkeit der Armee sicher.[69]

2. *Zusammenarbeit mit Dritten*: Das Kommando Cyber kann im Einvernehmen mit dem Bereich DTI[70] der Bundeskanzlei Leistungen aus seinem Leistungskatalog zugunsten der Bundesverwaltung erbringen. Es kann informations- und kommunikationstechnische Leistungen zur Aufrechterhaltung der Führungsfähigkeit von Dritten erbringen, sofern dafür eine gesetzliche Grundlage besteht.[71]

[64] Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren.
[65] Art. 60 NDG; Botschaft NDG, BBl 2014 2105 (Fn. 54), 2164.
[66] Art 76a Abs. 1 revISG (Fn. 57).
[67] Art. 69 NDG; Botschaft NDG, BBl 2014 2105 (Fn. 54), 2197.
[68] Verordnung über die militärische Cyberabwehr (MCAV; SR 510.921).
[69] Art. 96 MG; Art. 11 Bst. d Ziff. 1- 3 OV-VBS.
[70] Bereich Digitale Transformation und IKT-Lenkung.
[71] Art. 11 Bst. d Ziff. 4 und 5 OV-VBS.

3. *Militärische Cyberdefence*: Das Kommando Cyber ist zuständig für die Abwehr von Cyberangriffen gegen militärische Systeme und Netzwerke.[72] Unter militärischen Cyberdefence versteht man umfassende Aktionen im Cyberraum mit dem Ziel, die einsatzkritischen IKT-Leistungen der Armee auf militärstrategischer und operativer Führungsstufe zu schützen und zu verteidigen. Folgende Aktionen sind darin enthalten:[73]

- Cyberverteidigung: Aktionen im Cyberraum mit dem Ziel, Angriffe und Cyberaufklärung zu identifizieren und die eigenen Ressourcen zu schützen.
- Cyberaufklärung: Aktionen im Cyberraum mit dem Ziel, Nachrichten im Cyberraum zu gewinnen.
- Cyberangriff: Aktion im Cyberraum mit dem Ziel, gegnerische Ressourcen und Fähigkeiten im oder durch den Cyberraum zu stören, zu behindern oder zu verlangsamen.

4. *Funkaufklärung:* Das Kommando Cyber, bzw. der Dienst für Cyber- und elektromagnetische Aktionen (CEA), ist zuständig für die Funkaufklärung zugunsten des NDB und des Nachrichtendienstes der Armee.[74]

5. *Kabelaufklärung*: Das Kommando Cyber, bzw. der Dienst CEA, ist der durchführende Dienst für die Kabelaufklärung zugunsten des NDB.[75]

6. *Kryptologie*: Das Kommando Cyber betreibt den kryptografischen Dienst der Armee. Dieser ist im Rahmen des ISG Ansprechpartner für die Fachstelle des Bundes für Informationssicherheit für technische Fragestellungen bezüglich kryptografischer Lösungen.[76]

Die Aufgaben des Kommandos Cyber werden in Artikel 4 Abs. 2 MCAV weiter konkretisiert. Dazu gehören die Ausführung von Cyberraumaktionen, Schutzmassnahmen für einsatzkritischer IKT-Leistungen der Armee, die rechtliche und praktische Überprüfung von neuen Aktionen, die Zugangsunterbrechung einsatzkritischer IKT-Leistungen der Armee, die Sicherstellung der Verfügbarkeit technischer Informationen, die Auswertung kompromittierter Systeme, die Pflege von Kontakten zu Fachstellen sowie die Unterstützung beim Einsatz und Ausbildung im Bereich der Cyberdefence und die Dokumentation von bewilligungspflichtigen Massnahmen.

3.4.5 Bundesamt für Rüstung (armasuisse) – Cyber-Defence Campus

Das Bundesamt für Rüstung stellt als Technologiezentrum des VBS wissenschaftlich-technische Kompetenzen für die Armee und das VBS sicher und deckt deren Bedarf in den Bereichen Wissenschaft, Technologie und Innovation.[77] Zuständig hierfür ist der Bereich «Wissenschaft und Technologie W + T» (armasuisse W + T). Um seinen Kompetenzen im Bereich Cyber gerecht zu werden und Cyberentwicklungen schneller zu antizipieren, gründete armasuisse W + T den Cyber-Defence Campus (CYD Campus).

[72] Art. 100 Abs. 1 Bst. c MG; Art. 11 Bst. d Ziff. 6 OV-VBS; Art. 4 Abs. 1 MCAV.
[73] Art. 1 Abs. 2 MCAV.
[74] Art. 1 und Art. 3 Verordnung über die elektronische Kriegführung und die Funkaufklärung vom 17. Oktober 2012 (VEKF; SR 510.292).
[75] Art. 24 ff. NDV.
[76] Vgl. Art. 21 und 23 Verordnung über die Informationssicherheit in der Bundesverwaltung und der Armee vom 8. November 2023 (Informationssicherheitsverordnung, ISV; SR 128.1).
[77] Art. 12 Abs. 1 Bst. b OV-VBS.

Der CYD Campus stellt dem VBS eine Antizipations- und Wissensplattform zur Verfügung für die Erkennung und Bewertung technologischer, wirtschaftlicher und gesellschaftlicher Cybertrends. Er dient als Bindeglied zwischen dem VBS, der Industrie und der Wissenschaft in Forschung, Entwicklung und Ausbildung für die Cyberabwehr. Der CYD Campus arbeitet eng mit nationalen und internationalen Partnern zusammen, um Wissen und Ressourcen im Bereich der Cybersicherheit zu teilen. Zu diesen Partnern gehören sowohl Hochschulen als auch Industriepartner.

Der CYD Campus konzentriert sich auf drei Aufgaben zur Stärkung der Schweizer Cyberabwehr:

1. *Früherkennung von Trends im Cyberbereich*: Der CYD Campus monitort Technologien und den Markt umfassend. Dazu gehört, dass der CYD Campus eine Cyber Technologie Monitoring Plattform entwickelt und betreibt sowie Technologie Reviews und Trendanalysen publiziert, dynamische Dashboards darstellt und zu Technologie Roadmaps/Radars beiträgt. Der CYD Campus spürt interessante Technologien und Firmen (vor allem Startups) in internationalen Innovationsräumen wie Trust Valley, Silicon Valley, Israel, Vereinigtes Königreich, etc. auf und pflegt ein Kooperationsnetzwerk.

2. *Erforschung und Innovation von Cybertechnologien*: In Zusammenarbeit mit Wissenschaft und Industrie erkennt der CYD Campus neu entstehende Cyberrisiken und entwickelt innovative Lösungen, um den Bedrohungen im Cyberraum wirksam begegnen zu können. Darüber hinaus stellt der CYD Campus die Sicherheit und Resilienz bestehender Cybersysteme sicher und verbessert diese.

3. *Ausbildung von Cyberspezialistinnen und -spezialisten*: Beim CYD Campus werden Talente auf Master-, PhD- und Postdoc-Stufe sowie Hochschulpraktikantinnen und -praktikanten und Personen aus dem Cyber Lehrgang in Form von Praktika, Masterarbeiten oder Fellowships (ca. 50 pro Jahr) für zukünftige Herausforderungen geschult. Zudem definieren und betreuen Expertinnen und Experten des CYD Campus zahlreiche studentische Projekte.

Ferner transferiert der CYD Campus neuartige Cybertechnologien ins VBS und entwickelt Demonstratoren, um sie besser zu verstehen und kennenzulernen. Er ist auch für Penetrations-Tests und Beratung zuständig. Dabei untersucht er IKT-Systeme auf ihre Sicherheit und berät bei komplexen Sicherheitsfragestellungen und Data Science Themen in der Beschaffung.

Um das Wissen zu verbreiten und einen Austausch zu fördern, organisiert und führt der CYD Campus unterschiedliche Veranstaltungen durch:

- *Cyber Startup Challenge* (jährlich), um interessante Cyber Startups aufzuspüren und einen Proof-of-Concept mit ihnen in einer Einsatzumgebung des VBS umzusetzen.
- *Hackathons* (mehrmals pro Jahr) zu diversen Cybersicherheits und Data Science Themen (z. B. E-Autos, industrielle Kontrollsysteme, Satellitenkommunikation, Internet of Things), um die Schweizer Cyber Community zusammenzubringen.

- *Cyber Konferenzen, Retreats und Seminare* zu diversen Cybersicherheit und Data Science Themen (z. B. Lunch Seminare).
- *Cyber Training* im Rahmen vom CTC Pilotprojekt.

3.4.6 Bundesamt für Bevölkerungsschutz

Das BABS trägt zu einem umfassenden Schutz der Bevölkerung und ihrer Lebensgrundlage sowie der Kulturgüter vor den Auswirkungen von Schadenereignissen grosser Tragweite, Katastrophen, Notlagen und bewaffneten Konflikten bei. Bei bevölkerungsschutzrelevanten Ereignissen von nationaler Tragweite koordiniert es die Zusammenarbeit zwischen Kantonen, Gemeinden und Dritten und trägt zur Bewältigung solcher Ereignisse bei. [78]

Das BABS setzt sich mit Cyber Unsicherheit im Rahmen seiner Kernleistungen auseinander. Das sind insbesondere:

1. *Nationale Risikoanalyse von Katastrophen und Notlagen*: Das BABS führt in regelmässigen Abständen eine nationale Risikoanalyse von Katastrophen und Notlagen durch.[79] Bei der letzten Durchführung wurden 44 Gefährdungen in den Bereichen Natur, Technik und Gesellschaft untersucht. Auch ein Cyberangriff war Bestandteil der untersuchten Gefährdungen. Zu jeder der 44 Gefährdungen existiert ein Gefährdungsdossier.[80] Diese Dossiers enthalten systematisch aufgebaute Szenarien sowie das erwartete Schadensausmass, das anhand von zwölf Schadensindikatoren abgeschätzt wird. Der Risikobericht sowie die Gefährdungsdossiers dienen als Grundlage zur vorsorglichen Planung und Ereignisvorbereitung. Dadurch können mit geeigneten präventiven und vorsorglichen Massnahmen die Eintrittswahrscheinlichkeit respektive das potentielle Schadensausmass reduziert werden.

2. *Nationale Strategie zum Schutz von kritischen Infrastrukturen (SKI-Strategie)*: Die nationale SKI-Strategie hat zum Ziel, die Ausfall- und Versorgungssicherheit von essenziellen Gütern und Dienstleistungen (z. B. Stromversorgung oder Telekommunikation) zu verbessern. Unter anderen hat der Bundesrat die jeweils zuständigen Aufsichts- und Regulierungsbehörden beauftragt, in allen kritischen Sektoren zu prüfen, ob Risiken für gravierende Ausfälle oder Störungen bestehen und Massnahmen zur Verbesserung der Resilienz zu treffen. In enger Abstimmung mit der NCS werden dabei auch Cyber-Risiken (wie ein Cyber-Angriff auf die Stromversorgung oder den Schienenverkehr) untersucht. Falls es notwendig sein sollte, zusätzliche Vorgaben für die Betreiber zu erlassen (z. B. hinsichtlich der Cyber-Sicherheit), erfolgt dies über die Anpassung der sektoriellen, spezialgesetzlichen Rechtsgrundlagen unter der Verantwortung der zuständigen Fachämter. Das BABS ist für die Koordination bei der Umsetzung der nationalen SKI-Strategie verantwortlich. Dabei wird es durch den Bundesratsausschuss Energie, Umwelt und Infrastruktur begleitet.[81] Als weiteren Schwerpunkt der

[78] Art. 14 OV-VBS.
[79] BABS, Nationale Risikoanalyse von Katastrophen und Notlagen <https://www.babs.admin.ch/de/natgefaehrdanalyse>.
[80] BABS, Gefährdungsdossiers und Szenarien < https://www.babs.admin.ch/de/gefahrdungsdossiers-und-szenarien>.
[81] BABS, Nationale Strategie zum Schutz kritischer Infrastrukturen <https://www.babs.admin.ch/de/nationale-strategie-zum-schutz-kritischer-infrastrukturen>.

nationalen SKI-Strategie führt das BABS das periodisch aktualisierte Inventar der kritischen Infrastrukturen. Dieses dient als wichtige Planungs- und Entscheidungsgrundlage bei der Bewältigung von Katastrophen, Notlagen und bewaffneten Konflikten (z. B. auch bei umfangreichen Cyberangriffen). Zudem betreibt das BABS Plattformen zur Verbesserung der sektorübergreifenden Zusammenarbeit auf Seiten der Behörden und der Betreiberinnen national kritischer Infrastrukturen.

3. *Führungs- und Einsatzkommunikationssysteme*[82]:

- Das BABS ist zusammen mit dem Bundesamt für Zoll und Grenzsicherheit (BAZG) für den Werterhalt Polycom (WEP 2030)[83] verantwortlich. Polycom ist das flächendeckende Sicherheitsfunknetz der Behörden und Organisationen für Rettung und Sicherheit (BORS).[84] Dessen Betrieb soll bis mindestens 2030 sichergestellt werden. Ein grosser Teil der im System Polycom genutzten Komponenten muss aufgrund des Technologiewandels erneuert werden. Dafür sind werterhaltende Massnahmen notwendig.
- Das BABS koordiniert das Projekt rund um die Konzipierung und Realisierung eines sicheren Datenverbundnetzes (SDVN+). Das Ziel von SDVN+ liegt in der Einführung eines sicheren, hochverfügbaren und vor Cyberangriffen geschützten Systems für eine zeitgemässe Alarmierung und Information der Bevölkerung und eine effiziente Führungs- und Einsatzkommunikation der BORS. Das SDVN+ soll insbesondere in Katastrophenfällen oder Notlagen den breitbandigen Datenaustausch zwischen den Partnern im Bevölkerungsschutz sicherstellen. Durch die Isolation von allen anderen Netzten soll der Schutz vor Cyberangriffen signifikant erhöht werden. Das Netz soll aber auch für sicherheitsrelevante Anwendungen in der normalen Lage benutzt werden können

Der Bundesrat hat entschieden ein neues, zukunftsgerichtetes, mobiles, breitbandiges Sicherheitskommunikationssystem (MSK) einzuführen.[85] Polizei, Feuerwehr, Sanität, Betreiber kritischer Infrastrukturen und weitere Organisationen des Bevölkerungsschutzes sind für die Erfüllung ihres Auftrags darauf angewiesen, Bilder und Videos sicher zu übermitteln und geschützt auf Datenbanken zuzugreifen. Dies muss auch dann möglich sein, wenn die bestehenden Mobilfunknetze überlastet oder beschädigt sind, etwa nach Naturkatastrophen, einem Cyberangriff, bei Stromausfällen oder einem Terroranschlag. Der Bundesrat hat das VBS beauftragt, bis Mitte 2024 eine Vernehmlassungsvorlage mit einer MSK-Kombi-Variante auszuarbeiten. Ein MSK wird das nationale sichere Datenverbundnetz (SDVN+) nutzen und ab 2030 das Sicherheitsfunksystem Polycom sukzessive ersetzen. Dadurch kann ein bedeutender Gewinn an Sicherheit und Funktionalitäten für die Blaulichtorganisationen und weitere Partner des Bevölkerungsschutzes erzielt werden, da diese mit einem MSK ihre Aufgaben nicht nur

[82] Kapitel 4 Verordnung über den Bevölkerungsschutz (Bevölkerungsschutzverordnung, BevSV; SR 520.12).
[83] BABS, Werterhalt Polycom (WEP 2030) <https://www.babs.admin.ch/de/werterhalt-polycom-wep-2030>.
[84] Ausführlich dazu: BABS, Führungs- und Einsatzkommunikationssysteme <https://www.babs.admin.ch/de/kommsysteme>.
[85] Art. 20 Bundesgesetz über den Bevölkerungsschutz und den Zivilschutz (Bevölkerungs- und Zivilschutzgesetz, BZG; SR 520.1) und Art. 5 BevSV.

bei Katastrophen oder Terroranschlägen besser wahrnehmen, sondern sich bereits im Alltag auf eine sichere breitbandige Kommunikation verlassen können.[86]

Daneben betreibt das BABS das NEOC (National Emergency Operations Center, früher NAZ), in welchem das Ressourcenmanagement Bund (ResMaB) angesiedelt ist.[87] ResMaB ist eine koordinative Aufgabe und ein Instrument des Bundes zum Ausgleich zusätzlich erforderlicher Ressourcen bei Gefahren- und Schadenlagen, insbesondere bei komplexen Ereignissen und im Speziellen bei interkantonalen, nationalen und internationalen Ereignissen. Die Ressourcenkoordination und die Vermittlung von Leistungen erfolgt nach dem Subsidiaritätsprinzip und unter Einbezug der in die Ereignisbewältigung involvierten Akteure, sowie unter Anwendung definierter Kriterien und Prioritäten im Rahmen eines konsultativen Prozesses durch das Gremium Teilstab ResMaB. Die Ressourcenkoordination und die Ressourcenallokation dienen dem zielgerichteten Einsatz von Ressourcen zum Schutz der Bevölkerung und dem Erhalt ihrer Lebensgrundlagen. ResMaB funktioniert grundsätzlich szenariounabhängig. Dennoch lag der Fokus bislang nicht auf dem Thema «Cyber».

Artikel 3 Absatz 1 und 2 BZG[88] halten fest, dass im Rahmen des Bevölkerungsschutzes die Führungsorgane, Partnerorganisationen und Dritte in der Vorsorge und der Ereignisbewältigung zusammenarbeiten. Die Partnerorganisationen Bevölkerungsschutz sind die Polizei, die Feuerwehr, das Gesundheitswesen, die technischen Betriebe sowie der Zivilschutz. Artikel 3 Absatz 3 BZG hält zudem fest, dass weitere Stellen und Organisationen beigezogen werden können. Für Cyberthemen kann somit beispielsweise das BACS beigezogen werden.[89]

3.4.7 Bundesamt für Cybersicherheit

Das BACS ist das Kompetenzzentrum des Bundes für Cybersicherheit und damit erste Anlaufstelle für die Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen.[90]

Die organisatorischen Bestimmungen und Beschreibungen der Aufgaben des BACS finden sich in Artikel 15a OV-VBS. Mit der Revision des Kapitels 5 im ISG hat das Parlament eine neue gesetzliche Grundlage für das BACS erlassen, welche auch dessen Aufgaben definiert. In der Folge wird vertieft auf die zehn Aufgaben des BACS eingegangen, wie sie sich aus der OV-VBS ergeben. Diese Ausführungen werden mit den Informationen zum revidierten ISG (revISG) ergänzt.

[86] VBS, Bundesrat trifft Grundsatzentscheid für mobile Breitbandkommunikation in Krisenlagen <https://www.vbs.admin.ch/de/nsb?id=99545>.
[87] Art. 10 BZG und Art. 6 BevSV.
[88] Bundesgesetz über den Bevölkerungsschutz und den Zivilschutz (Bevölkerungs- und Zivilschutzgesetz, BZG; SR 520.1).
[89] Botschaft vom 21. November 2018 zur Totalrevision des Bevölkerungs- und Zivilschutzgesetzes, BBl 2019 521, 539. In der Botschaft wird noch von MELANI gesprochen, MELANI wurde am 1. Juli 2020 Teil des NCSC. Das NCSC ist seit dem 1. Januar 2024 das Bundesamt für Cybersicherheit (BACS).
[90] Vgl. Art. 15a Abs. 1 OV-VBS wo das BACS als Kompetenzzentrum bezeichnet wird.

1. Koordination: Das BACS koordiniert die Arbeiten des Bundes im Bereich Cybersicherheit.[91]

2. Erstellung von technischen Analysen: Das BACS erstellt technische Analysen zur Bewertung und Abwehr von Cybervorfällen und Cyberbedrohungen sowie zur Identifikation und Behebung von Schwachstellen beim Schutz der Schweiz vor Cyberbedrohungen.[92] Zu dieser Aufgabe gehört auch das Suchen nach infizierten Webseiten oder Schwachstellen.[93]

3. Entgegennahme von Meldungen zu Cybervorfällen und Cyberbedrohungen: Das BACS nimmt Meldungen zu Cybervorfällen und Cyberbedrohungen entgegen. Es betreibt dazu die nationale Anlaufstelle für Cyberbedrohungen.[94] Diese Meldestelle wurde auf der Grundlage von MELANI aufgebaut und wird von Unternehmen sowie der Bevölkerung rege genutzt.[95] Sie nimmt sowohl freiwillige Meldungen zu Cybervorfällen und Cyberbedrohungen entgegen wie auch Meldungen zu Cyberangriffen, die unter die Meldepflicht fallen.[96]

4. Analyse von Meldungen zu Cybervorfällen und Cyberbedrohungen: Das BACS analysiert die eingegangenen Meldungen bezüglich ihrer Bedeutung für den Schutz der Schweiz vor Cyberbedrohungen.[97] Auf Anfrage der meldenden Stelle kann das BACS basierend auf der Analyse Einschätzungen zum Vorfall und Empfehlungen für das weitere Vorgehen abgeben.[98]

5. Veröffentlichung von Informationen zu Cybervorfällen: Das BACS veröffentlicht Informationen zu Cybervorfällen, soweit dies dem Schutz vor Cyberbedrohungen dient. Diese Informationen dürfen nur dann Daten über natürliche oder juristische Personen enthalten, wenn diese eingewilligt und es sich um missbräuchlich verwendete Identifikationsmerkmale und Adressierungselemente handelt, wie beispielsweise im Falle des Missbrauchs von Logos bei Phishing-Angriffen.[99] Zudem kann das BACS Informationen zu Schwachstellen unter Angabe der betroffenen Hard- oder Software veröffentlichen, sofern die Herstellerin einwilligt oder die Schwachstelle nicht innert Frist behoben wurde. Das kann notwendig sein, um weitere Cyberangriffe zu verhindern. Das BACS ist international als Fachstelle für Schwachstellen anerkannt und arbeitet für eine koordinierte Veröffentlichung von gefundenen Schwachstellen mit ausländischen und internationalen Fachstellen zusammen.[100]

6. Sensibilisierung und Warnung von Behörden, Organisationen und Personen: Das BACS trägt mit gezielten Informationen zur Sensibilisierung der Bundesverwaltung und der Öffentlichkeit in Bezug auf Cyberbedrohungen bei, informiert über die aktuelle Lage und gibt Anleitungen für präventive und reaktive Massnahmen heraus. Das BACS

[91] Art. 15a Abs. 2 Bst. a OV-VBS.
[92] Art. 15a Abs. 2 Bst. b OV-VBS, Art. 73a Abs 1 revISG (Fn. 57).
[93] Botschaft vom 2. Dezember 2022 zur Änderung des Informationssicherheitsgesetzes (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), BBl 2023 84, 25.
[94] Art. 15a Abs. 2 Bst. c OV-VBS, Art. 73a Abs. 2 Bst. d und Art. 73b Abs. 1 revISG (Fn. 57).
[95] Botschaft Meldepflicht, BBl 2023 84 (Fn. 93), 25.
[96] Botschaft Meldepflicht, BBl 2023 84 (Fn. 93), 26.
[97] Art. 15a Abs. 2 Bst. c OV-VBS, Art. 73a Abs. 2 Bst. d und Art. 73b Abs. 2 revISG (Fn. 57).
[98] Art. 73b Abs. 2 revISG (Fn. 57); Botschaft Meldepflicht, BBl 2023 84 (Fn. 93), 26.
[99] Art. 73c Abs. 1 revISG (Fn. 57); Botschaft Meldepflicht, BBl 2023 84 (Fn. 93), 27.
[100] Art. 73c Abs. 2 revISG (Fn. 57); Botschaft Meldepflicht, BBl 2023 84 (Fn. 93), 27.

warnt betroffene Behörden, Organisationen und Personen vor unmittelbaren Cyberbedrohungen oder laufenden Cyberangriffen.[101] Zudem veröffentlicht das BACS gestützt auf den eingegangenen Meldungen und Analysen regelmässig Statistiken und Berichte zu den aktuellen Cyberbedrohungen, um die Öffentlichkeit zu sensibilisieren, Betroffene zu warnen und Empfehlungen zu erstellen.

7. Präventive Unterstützung der Betreiberinnen von kritischen Infrastrukturen beim Schutz vor Cyberbedrohungen: Das BACS unterstützt die Betreiberinnen von kritischen Infrastrukturen beim Schutz vor Cyberbedrohungen präventiv. Das BACS stellt den Betreiberinnen kritischer Infrastrukturen Hilfsmittel unentgeltlich zur Verfügung. Den Betreiberinnen kritischer Infrastrukturen ist es freigestellt, ob sie die Unterstützung des BACS in Anspruch nehmen wollen. Die Hilfsmittel werden mithin zur freien Nutzung angeboten. Die wichtigsten Hilfsmittel werden beispielhaft aufgelistet. Es handelt sich um eine nicht abschliessende Aufzählung.[102]

- *Cyber Security Hub*: Das BACS bietet eine Kommunikationsplattform, über welche Organisationen und Behörden mit Sitz in der Schweiz mit dem BACS und unter sich Informationen zu Cybervorfällen und Cyberbedrohungen austauschen können. Dadurch verfügen die Verantwortlichen stets über den aktuellsten Wissenstand. Das BACS nutzt diesen geschützten Informationskanal auch dazu, die kritischen Infrastrukturen frühzeitig über Angriffsmuster zu informieren, die noch nicht öffentlich bekannt sind und vom BACS aus Sicherheitsgründen auch nicht veröffentlicht werden können.[103]

- Das BACS stellt den Betreiberinnen von kritischen Infrastrukturen technische Informationen zu aktuellen Cyberbedrohungen (z. B. Schwachstellen) sowie Empfehlungen zu präventiven und reaktiven Massnahmen gegen Cybervorfälle zur Verfügung. Diese Hilfsmittel beschränken sich auf Inhalte, die für kritische Infrastrukturen allgemein nützlich sein können. Es wird keine unternehmensspezifische Beratung durchgeführt.[104]

- Als weiteres Hilfsmittel bietet das BACS auch technische Instrumente und Anleitungen für die Früherkennung von Cybervorfällen. Solche Instrumente können beispielsweise Detektionsregeln für die Erkennung von potenziell schädlichen Netzwerkflüssen und Dateien sein, Listen mit technischen Indikatoren für bereits erfolgte oder versuchte Angriffe («Indicators of Compromise») oder spezialisierte Anwendungen für die Entdeckung von Angriffsmustern und den Schutz vor solchen Angriffen.[105]

Diese Hilfsmittel werden teilweise so konzipiert, dass sie für alle kritischen Infrastrukturen hilfreich sind. Sie können aber auch spezifisch für gewisse Gruppen von kritischen Infrastrukturen oder für bestimmte Tätigkeitsbereiche zugeschnitten sein. Sie ersetzen nicht die Schutzdispositive der jeweiligen Infrastruktur, sondern müssen in diese eingebunden werden.[106]

[101] Art. 15a Abs. 2 Bst. e OV-VBS, Art. 73a Abs. 2 Bst. b revISG (Fn. 57).
[102] Art. 15a Abs. 2 Bst. f OV-VBS, Art. 74 ISG; Botschaft Meldepflicht, BBl 2023 84 (Fn. 93), 30.
[103] Art. 74 Abs. 2 lit. a revISG (Fn. 57); Botschaft Meldepflicht, BBl 2023 84 (Fn. 93), 30.
[104] Art. 74 Abs. 2 lit. b revISG (Fn. 57); Botschaft Meldepflicht, BBl 2023 84 (Fn. 93), 30.
[105] Art. 74 Abs. 2 lit. c revISG (Fn. 57); Botschaft Meldepflicht, BBl 2023 84 (Fn. 93), 30 f.
[106] Botschaft Meldepflicht, BBl 2023 84 (Fn. 93), 31.

8. Unterstützung der Betreiberinnen von kritischen Infrastrukturen bei der Bewältigung von Cyberbedrohungen: Das BACS führt ein «Computer Emergency Response Team» (CERT); dieses ist die nationale Fachstelle für die technische Vorfallbewältigung und unterstützt Betreiberinnen kritischer Infrastrukturen bei Cybervorfällen.

Die Form der Unterstützung unterscheidet sich je nach Betroffenheit der Funktionsfähigkeit sowie je nach Trägerschaft der kritischen Infrastruktur. Diese Unterscheidung ist für die Subsidiaritätsthematik relevant:

- *Technische Beratung*: Das BACS kann in jedem Fall Betreiberinnen kritischer Infrastrukturen bei der Bewältigung von Cybervorfällen und der Behebung von Schwachstellen mit technischer Beratung unterstützen.[107] Die Unterstützung des BACS erfolgt auf Anfrage und in enger Zusammenarbeit mit den Betroffenen.[108]

- *Technische Unterstützung*: Das BACS kann Betreiberinnen kritischer Infrastrukturen technisch unterstützen, wenn Cybervorfälle die Funktionsfähigkeit der betroffenen kritischen Infrastruktur gefährden. Wenn es sich um eine private Betreiberin handelt, erfolgt die Unterstützung subsidiär zu den IT-Leistungen, die auf dem Markt erhältlich sind. Das bedeutet, dass keine gleichwertigen Marktleistungen zeitnah verfügbar sein dürfen.[109] Ob es sich um eine private oder öffentliche Betreiberin handelt, entscheidet sich nach der Trägerschaft und nicht nach der Rechtsform der kritischen Infrastruktur.[110] Handelt es sich um eine öffentliche Betreiberin, erfolgt die Unterstützung ohne Subsidiaritätsabwägung.

Die Unterstützung des BACS bei der Bewältigung von Vorfällen besteht in der technischen Analyse des Angriffs. Diese hat zum Ziel, möglichst rasch zu verstehen, welche Angriffsvektoren die Angreifenden verwenden, welche Methoden und Taktiken sie anwenden und welche Ziele sie verfolgen. Diese Erkenntnisse ermöglichen es, die geeigneten Gegenmassnahmen zu bestimmen und umzusetzen. Das BACS arbeitet dabei eng mit den betroffenen Behörden und Organisationen und ihren allfälligen Sicherheitsdienstleistern zusammen. Es hilft zudem bei der Koordination zwischen den an der technischen Bewältigung beteiligten Akteuren. Es kann nötigenfalls auch Unterstützung direkt vor Ort bei der betroffenen Behörde oder Organisation leisten. Die Unterstützung des BACS erfolgt im Sinne einer Soforthilfe im Notfall. Bei den nach der Vorfallbewältigung nötigen Arbeiten zur Wiederherstellung der Daten und Wiederaufbau der Systeme unterstützt das BACS nur beratend.[111]

9. Unterstützung für Behörden: Artikel 76a revISG klärt die Rollenteilung zwischen dem BACS und dem NDB. Zudem führt er aus, welche Informationen und wie diese an den NDB, die Strafverfolgungsbehörden und die kantonalen Stellen, die für Cybersicherheit zuständig sind, übermittelt werden. Das BACS unterstützt den NDB, in dem es Auswertungen zu Anzahl, Art und Ausmass von Cyberangriffen sowie technische Analysen

[107] Botschaft Meldepflicht, BBl 2023 84 (Fn. 93), 31.
[108] Botschaft Meldepflicht, BBl 2023 84 (Fn. 93), 31.
[109] Botschaft Meldepflicht, BBl 2023 84 (Fn. 93), 31.
[110] Botschaft Meldepflicht, BBl 2023 84 (Fn. 93), 31.
[111] Botschaft Meldepflicht, BBl 2023 84 (Fn. 93), 31.

von Cyberbedrohungen zur Verfügung stellt («Lagebilder»).[112] Auch den Strafverfolgungsbehörden und den kantonalen Stellen, die für Cybersicherheit zuständig sind, gewährt das BACS Zugriff auf Informationen. Hierbei kann es sich auch um personenbezogene Informationen handeln.[113]

10. Nationale Cyberstrategie: Das BACS erarbeitet zuhanden des Bundesrates die Nationale Cyberstrategie (NCS) und koordiniert deren Umsetzung. Es führt als Geschäftsstelle der NCS ein strategisches Controlling durch und bereitet die Sitzungen des Strategischen Ausschusses NCS vor. Die NCS legt in Abstimmung mit den Kantonen den strategischen Rahmen für die Verbesserung der Prävention, Früherkennung, Reaktion und Resilienz zum Schutz der Schweiz vor Cybervorfällen und Cyberbedrohungen fest.[114]

3.5 Wichtigste Erkenntnisse

Der Schutz vor Cyberbedrohungen ist eine gemeinsame Verantwortung von Wirtschaft, Gesellschaft und Staat. Grundsätzlich sind alle Akteure für ihre eigene Sicherheit verantwortlich. Innerhalb des VBS nehmen die Ämter verschiedene Aufgaben im Bereich Cyber wahr.

Dabei erfolgen nur zwei Leistungen subsidiär: Der Assistenzdienst der Armee gemäss MG und die subsidiäre technische Unterstützung für private Betreiberinnen kritischer Infrastrukturen durch das BACS gemäss revISG. Wenn es sich um eine private Betreiberin handelt, erfolgt die Unterstützung des BACS subsidiär zu den IT-Leistungen, die auf dem Markt erhältlich sind. Das bedeutet, dass keine gleichwertigen Marktleistungen zeitnah verfügbar sein dürfen. Die technische Unterstützung, die das BACS gegenüber öffentlichen Betreiberinnen erbringt, erfolgt nicht subsidiär. Die übrigen Aufgaben, die durch das VBS wahrgenommen werden, lassen sich in zwei Kategorien einteilen. (1) Bei Leistungen, die gegenüber Dritten erbracht werden, wurde die Subsidiaritätsabwägung bereits dann vorgenommen, als das entsprechende Gesetz erlassen wurde. (2) Bei Leistungen, die die Ämter des VBS für den Bund selbst erbringt, muss keine Subsidiaritätsabwägung getroffen werden.

4 Handlungsmassnahme

Die vorangehenden Kapitel haben das Subsidiaritätsprinzip erklärt und ausgeführt welche Aufgaben die verschiedenen Ämter im Bereich Cyber erbringen. Das VBS verfügt sowohl im militärischen als auch im zivilen Bereich über umfassende Cyberkompetenzen. Um die Zusammenarbeit zwischen diesen beiden Bereichen zu vereinfachen, wurde die folgende Handlungsmassnahme ausgearbeitet:

Das Bundesamt für Cybersicherheit (BACS) prüft in Zusammenarbeit mit dem Kommando Operationen, dem Kommando Cyber, dem Generalsekretariat VBS (GS-VBS), dem Staatssekretariat für Sicherheitspolitik (SEPOS) und dem Sicherheitsverbund

[112] Botschaft Meldepflicht, BBl 2023 84 (Fn. 93), 50.
[113] Botschaft Meldepflicht, BBl 2023 84 (Fn. 93), 50.
[114] Art. 15a Abs. 2 Bst. g OV-VBS.

Schweiz (SVS) die Schaffung von Rechtsgrundlagen für vereinfachte Unterstützungsleistungen des Kommando Cyber zugunsten des BACS. Das BACS unterbreitet dem Bundesrat bis Ende 2026 Varianten zum weiteren Vorgehen.

Hintergrund dieser Massnahme ist die folgende Situation. Das BACS ist die zentrale Anlauf- und Unterstützungsstelle für kritische Infrastrukturen bei Cybervorfällen. Es kann kritische Infrastrukturen unterstützen. Kommt das BACS in eine Überlastungssituation, ist es möglich, dass andere zivile Bundesämter das BACS unter dem RVOG bzw. der RVOV unterstützen. Bei Unterstützungsleistungen durch das Kommando Cyber sieht die Situation anders aus.

Die Organisationsstruktur der Gruppe Verteidigung ist in weiten Teilen identisch zu derjenigen der Armee. Für die beiden Organisationen sind unterschiedliche gesetzliche Grundlagen anwendbar. Das Militärgesetz findet Anwendung auf die Armee und deren Kommando Cyber. Hingegen gilt für das Kommando Cyber der Militärverwaltung und deren Mitarbeitende das RVOG.

Die Armee kann zivile Behörden nur gemäss den Vorschriften des Militärgesetzes unterstützen. Das bedeutet, dass die Armee nur dann Unterstützungsleistungen gegenüber zivilen Behörden erbringen kann, wenn die Voraussetzung für den Assistenzdienst gemäss Artikel 67 MG erfüllt sind. Die Militärverwaltung kann hingegen nur gestützt auf das RVOG und die RVOV andere zivile Behörden innerhalb der Bundesverwaltung unterstützen.

Dies kann zur folgenden Schwierigkeit führen: Wenn das BACS Unterstützung gemäss RVOG bzw. RVOV anfordert, darf nur Personal des Bundes tätig werden. Damit die Armee das BACS unterstützen kann, muss Assistenzdienst beantragt werden. Gemäss Artikel 70 Absatz 1 Buchstabe a MG ist ein solcher Einsatz vom Bundesrat zu entscheiden.

Dieser prozessuale Weg über den Bundesrat erschwert die gleichzeitig effiziente und rechtlich abgestützte Zusammenarbeit zwischen dem BACS und dem Kommando Cyber, da im Cyberbereich spezialisierte Mitarbeitende schnell und gezielt eingesetzt werden müssen.

Um diese Problematik anzugehen und die zeitnahe Erbringung von Unterstützungsleistungen durch das Kommando Cyber an das BACS sicherzustellen, soll die Schaffung einer rechtlichen Grundlage geprüft werden, für einen vereinfachten Prozess für Cybervorfälle (bspw. ähnlich der Unterstützung bei Katastrophen im Inland).

Eine solche rechtliche Grundlage würde es dem BACS erleichtern, Unterstützung im Cyberbereich vom Kommando Cyber anzufordern und umgekehrt dem Kommando Cyber ermöglichen, seine Leistungen dem BACS anzubieten ohne das ein solcher Antrag über den Bundesrat laufen müsste. Zudem könnten mit einer solchen rechtlichen Grundlage sowohl die Armee als auch die Gruppe Verteidigung für die Unterstützungsleistungen eingesetzt werden.

Dabei soll auf die Eigenheiten des Cyberbereichs Rücksicht genommen werden. Beispielsweise geht es bei der Unterstützung im Cyberbereich seitens BACS darum, Schä-

den abzuwenden, noch bevor sie entstanden sind, bzw. das Schadenspotential einzugrenzen. Bei einer möglichen Unterstützung des BACS durch das Kommando Cyber ginge es denn um die schnelle Bewältigung von Spitzenbelastungen und die Möglichkeit, zeitnah auf geeignete Personen (Spezialfähigkeiten) zugreifen zu können (vgl. Art. 67 Abs. 1 Bst. d MG).

Bei Unterstützung des BACS durch das Kommando Cyber im Assistenzdienst verbleibt die Einsatzverantwortung beim BACS (vgl. Art. 71 MG), was auch für Unterstützungen gemäss RVOG gilt. Auch bei der Unterstützung von zivilen Behörden bei Katastrophen im Inland bestimmt die zivile Behörde den Einsatz der Mittel und den Auftrag im Einvernehmen mit dem Kommando Operationen. Die zivile Behörde trägt die Gesamtverantwortung für den Einsatz (vgl. Art. 8 VmKl). Dies muss bei der Prüfung einer rechtlichen Grundlage für die Unterstützung bei Cybervorfällen berücksichtigt werden, damit die Trennung zwischen zivilen und militärischen Interessen bestehen bleibt. Die Vereinfachung des Prozesses zum Assistenzdienst in Cyberangelegenheiten stellt keine Vermischung zwischen den zivilen und militärischen Cyberinteressen dar.

Insbesondere muss beachtet werden, dass die Vertraulichkeit von Meldungen an das BACS gewährleistet bleibt. Die Vertraulichkeit der Meldung ist eine wichtige Voraussetzung, damit überhaupt Meldungen eingehen und der Meldestelle Vertrauen entgegengebracht wird. Aus diesem Grund wurden für Mitarbeitende des BACS bestimmte Rechtsvorschriften angepasst, um die Vertraulichkeit zu gewährleisten.[115] Um eine vertrauensvolle Zusammenarbeit zu ermöglichen, müssen das BACS und das Kommando Cyber klären, wie sie sicherstellen können, dass die Rechtsvorschriften des BACS auch für die unterstützenden Fachpersonen aus dem Kommando Cyber gelten.

Für die Erarbeitung der Handlungsmassnahme werden folgende inhaltliche Punkte festgelegt:

- Erarbeitung von Szenarien und Darstellung des Ausmasses einer Überlastung, um aufzuzeigen, in welchen Situationen welche Unterstützungsleistungen notwendig sind.
- Anknüpfung an die Lagen im Cyberbereich, inkl. Abgrenzung zum Aktivdienst.
- Darstellung des vereinfachten Prozesses, inkl. Kompetenzaufteilung.
- Überprüfung, ob die neun SVS-Kriterien für den Assistenzdienst auch bei Cybervorfällen angewendet werden sollen.
- Prüfung einer Anpassung der Rechtsgrundlagen für eine einfache und zeitnahe Unterstützung des BACS durch das Kommando Cyber.
- Erarbeitung von Optionen zum weiteren Vorgehen zuhanden des Bundesrates.

[115] Die Anzeigepflicht für Straftaten wurde wegbedungen (vgl. 73d Abs. 3 ISG) und Informationen, welche das BACS in seiner Funktion als Meldestelle von Dritten erhält, sind vom Zugangsrecht nach BGÖ ausgenommen (vgl. Art. 4 Abs. 1bis ISG). Botschaft Meldepflicht, BBl 2023 84 (Fn. 93), 26.

Das BACS ist für die Umsetzung dieser Massnahme zuständig. Es arbeitet dafür zusammen mit dem Kommando Operationen, dem Kommando Cyber, dem GS-VBS, dem SEPOS und dem SVS. Die Massnahme wird bis Ende 2026 umgesetzt.

5 Schlussbemerkungen

Das Postulat «VBS. Subsidiarität und Cybersicherheit» hat den Bundesrat beauftragt, in einem Bericht darzulegen, wie der Subsidiaritätsbegriff im VBS neu geprüft wird und wie dieser insbesondere in der Zusammenarbeit mit den Sicherheitsdienstleistungen im Cyberbereich anzuwenden ist.

Der vorliegende Bericht hat aufgezeigt, wie das Subsidiaritätsprinzip funktioniert und zur Anwendung kommt. Zudem hat er ausgeführt wie Cybersicherheit im Bund verstanden wird und welche Zuständigkeiten die verschiedenen Ämter und Gruppen im VBS in diesem Bereich übernehmen. Diese Auslegeordnung hat gezeigt, dass die Zusammenarbeit zwischen dem zivilen und dem militärischen Bereich aus Subsidiaritätsüberlegungen verbessert werden kann. Aus diesem Grund wurde eine Handlungsmassnahme ergriffen. Diese prüft, ob eine Rechtsgrundlage für einen vereinfachten Prozess für Unterstützungsleistungen des Kommando Cyber zugunsten des BACS geschaffen werden kann.