Strategie Cyber VBS

März 2021

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Impressum

Der Generalsekretär des VBS beauftragte die Erstellung der Strategie Cyber VBS. Die Verantwortung wurde an einen Projektausschuss mit den folgenden Vertreterinnen und Vertretern übertragen: Roger Michlig (Chef Digitalisierung und Cybersicherheit VBS, Vorsitz), Gérald Vernez (Delegierter Cyberdefence VBS, Projektleiter), Botschafterin Pälvi Pulli (Chefin Sicherheitspolitik VBS), Divisionär Alain Vuitel (Chef Führungsunterstützungsbasis FUB), Divisionär Jean-Paul Theler (bis 31.12.2020 Direktor BABS a.i., ab 1.1.2021 Chef A Stab), Dr. Thomas Rothacher (Vizedirektor armasuisse), Philipp Kronig (Vizedirektor NDB).

Für die operative Erarbeitung der Strategie hat der Projektausschuss eine Arbeitsgruppe eingesetzt, welche aus folgenden Personen besteht: Gérald Vernez (Delegierter Cyberdefence VBS, Projektleiter), Oberst i Gst Robert Flück (Projektleiter Cyber der Armee), Dr. Laura Crespo (Steuerungsverantwortliche Cyber NDB), Dr. Etienne Voutaz (armasuisse Wissenschaft und Technologie), Dr. Stefan Brem (Chef Risikogrundlagen und Forschungskoordination, BABS).

Die Strategie Cyber VBS wurde VBS-intern konsolidiert. Zusätzlich zu dieser Strategie konsultiert wurden der Vorsitzende der Kerngruppe Cyber, Florian Schütz (Delegierter für Cybersicherheit des Bundes und Chef NCSC), Nicoletta della Valle (Direktorin fedpol) und Dr. Jon Fanzun (Sondergesandter für Cyber-Aussen- und Sicherheitspolitik, EDA).

Genehmigt durch den Generalsekretär VBS im März 2021.

Premedia
Zentrum elektronische Medien ZEM
80.256 d 03.2021

Im Gleichschritt mit der Digitalisierung

Die fortschreitende Digitalisierung prägt unsere Gegenwart und unsere Zukunft. Ein rasanter technologischer Wandel hat unseren Alltag erfasst und bietet uns als Gesellschaft zahlreiche neue Chancen. Ein Trend, den die Corona-Pandemie zusätzlich beschleunigt hat.

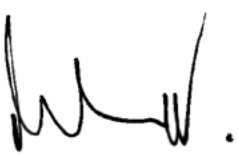
Mit dem Cyberraum ist auch eine neue Dimension, ein neues Mittel hinzugekommen, das Bedrohungen und Gefahren weiter verschärft. Missbrauch und Angriffe im Cyberspace können mit verschiedenen Absichten erfolgen: Beispielsweise zu Spionage- oder Sabotagezwecken, aus kriminellem Bestreben, als Teil von militärischen Operationen oder vermehrt auch in sogenannt «hybriden» Konflikten.

Wir alle sind auf funktionierende, zuverlässige IT-Infrastrukturen und -Daten angewiesen. Sie sind die Lebensnerven unserer Gesellschaft. Werden kritische Infrastrukturen – wie zum Beispiel die Energieversorgung – angegriffen, kann das gravierende Folgen haben. Deshalb schliesst eine moderne Sicherheitspolitik den virtuellen Raum mit ein.

Das Departement für Verteidigung, Bevölkerungsschutz und Sport VBS ist im Rahmen der Nationalen Strategie für Cybersicherheit zuständig für die Cyberdefence der Schweiz im Alltag, aber auch im Falle von Krisen und Konflikten. Das vorliegende Dokument legt die strategische Ausrichtung des Departementes im Bereich Cyberdefence für die kommenden Jahre dar.

Die Gruppe Verteidigung, der Nachrichtendienst des Bundes, armasuisse, das Bundesamt für Bevölkerungsschutz und das Generalsekretariat des VBS: Alle diese Bereiche im VBS tragen mit ihren spezifischen Aufgaben, ihren Kompetenzen und Verantwortungen täglich zur Cyberdefence unseres Landes bei. Sie haben die Strategie Cyber gemeinsam erarbeitet und dabei die neusten Entwicklungen berücksichtigt. Das Dokument zeigt, welche Fähigkeiten nötig sind, um den Bedrohungen aus dem virtuellen Raum erfolgreich zu begegnen. Dazu gehört, dass Bedrohungen, Risiken und Trends früh erkannt und technische Voraussetzungen gegeben sind. Dabei ist etwas klar: Trotz aller Digitalisierung – das zentrale Element für die erfolgreiche Umsetzung der Strategie bleibt der Mensch.

Ich bin überzeugt, dass die Strategie Cyber VBS ein gutes, wirkungsvolles Instrument ist, um den Bedrohungen im Cyberraum auch künftig und in Zusammenarbeit mit allen Partnern angemessen zu begegnen. Cyberverteidigung ist eine Verbundaufgabe – und eine sicherheitspolitische Priorität.



Bundesrätin Viola Amherd
Chefin Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport

Zusammenfassung

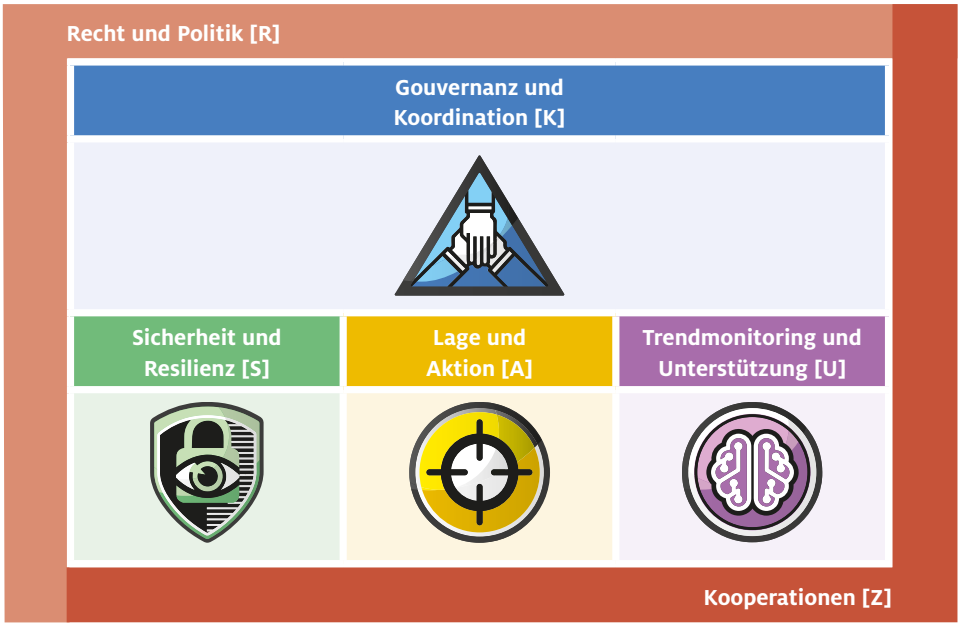
Die Strategie Cyber VBS beschreibt die Organisation und Vorgehensweise der Bereiche Cyber des VBS bis 2024. Sie ist die Fortsetzung und Weiterentwicklung des früheren Aktionsplans Cyberdefence. Bewährtes findet sich wieder: So der Beschrieb der Aktivitäten der verschiedenen Partner[1] im Bereich Cyber VBS im Alltag. Und ebenso die Erbringung von Sicherheitsleistungen zur Bewältigung von Cybervorfällen bei Spannungen und Konflikten. Gemeinsam tragen die Verwaltungseinheiten des VBS subsidiär dazu bei, kritische Infrastrukturen vor Cyberangriffen zu schützen und ihre Resilienz zu stärken.

Die Strategie integriert die Erkenntnisse der IST-Analyse, die laufenden Vorhaben im VBS[2] sowie die Zusammenarbeit mit Partnern im In- und Ausland. Sie zeigt auf, wie das VBS sich in die übergeordnete Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) einbringt.

Die Strategie fasst die allgemeine Stossrichtung des VBS im Cyberbereich zusammen:

«Wir tragen zum Schutz des Landes bei, verteidigen es im Cyberraum und erhöhen somit dessen Handlungsfreiheit massgeblich.»

Die Handlungen im VBS werden in vier Kernbereiche strukturiert:
- Gouvernanz und Koordination;
- Sicherheit und Resilienz;
- Lage und Aktion;
- Trendmonitoring und Unterstützung.



1 Generalsekretariat, Gruppe Verteidigung, Nachrichtendienst des Bundes, armasuisse, Bundesamt für Bevölkerungsschutz.
2 Insbesondere die Grundkonzeption Cyber der Schweizer Armee oder die Weiterentwicklung des Cyberdefence-Campus der armasuisse.

Wie diese konkret von den verschiedenen Verwaltungseinheiten des VBS bis 2024 umgesetzt werden, ist in zwei separaten, klassifizierten Katalogen beschrieben:

- Aufgaben, Kompetenzen und Verantwortungen der betroffenen Verwaltungseinheiten.
- Massnahmen zur Umsetzung der Strategie.

Die koordinierte Umsetzung der Strategie berücksichtigt folgende Handlungsgrundsätze: Subsidiarität, Institutionelle Zusammenarbeit, Internationale Zusammenarbeit, Aufgeschlossenheit, Offenheit und die Schaffung des Kommando Cyber der Armee. Die Steuerung der Umsetzung erfolgt im Rahmen der Konferenz «Cyberdefence VBS», welche unter der Leitung des Generalsekretärs VBS stattfindet.

Als national zuständige und kompetente Stelle für Cyberdefence setzt das VBS die folgenden **Ziele** für die Erfüllung seiner Aufgaben:

- **Antizipation und Früherkennung** von allgemeinen Herausforderungen und Entwicklungen im Cyberraum und den sich daraus ergebenden Bedrohungen, Chancen und Risiken (inkl. der Möglichkeiten der Digitalisierung zwecks kontinuierlicher Optimierung und Modernisierung), um sich dadurch agil daran anpassen zu können.
- **Bedrohungen und Angriffe**, welche die Aufgabenerfüllung des VBS beeinträchtigen, nationale Auswirkungen haben oder nationale Interessen gefährden, vorbeugen[3], selbstständig und – wo erforderlich – im Verbund rechtzeitig und in allen Lagen frühzeitig erkennen, stören, verhindern und attribuieren.
- Bereitstellung eines **Aus- und Weiterbildungsinstrumentariums** für die zivilen und militärischen Mitarbeitenden (Lohnbezüger) sowie für die Angehörigen der Miliz (Soldbezüger), um diese auf die sich entwickelnden Cyberherausforderungen vorzubereiten. Dieses ist, wo nötig und gemäss Vereinbarung, zugunsten anderer Leistungsbezüger auf Stufe von Bund, Kantonen und Betreibern kritischer Infrastrukturen zur Verfügung zu stellen.
- In Belangen der Cybersicherheit basierend auf einem Risikomanagementansatz **resistent sein** und ein hohes Mass an **Resilienz erreichen.**
- Zum Zweck der Resistenz und der Resilienz das **Asset-Management** beherrschen, auf aktuellem, technischem Stand halten, die **Lieferketten** und ihre Sicherheit kennen und ein angemessenes Mass an **Autonomie** durch die Reduktion der Abhängigkeiten von Dienstleistern und Lieferanten erreichen.
- Im Bereich Cyberdefence als Vorreiter und Vorbild auftreten und damit als attraktiver Arbeitgeber in Erscheinung treten.

---

3 Vorsorgliche Massnahmen sind u. a. in den Bereichen Technologie, Prozesse sowie Personen zu treffen.

Inhaltsverzeichnis

1

1 Einleitung

1.1 Veranlassung

Mit der zunehmenden Digitalisierung wachsen auch die Komplexität und die Herausforderungen im Cyberraum. Das VBS hat unterschiedliche Aufgaben zu erfüllen hinsichtlich Schutz und Verteidigung vor Angriffen im Cyberraum sowie der Unterstützung bei der Bewältigung solcher Ereignisse.

Cyberdefence ist ein Teil der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS). Der Aktionsplan Cyberdefence VBS (APCD) aus dem Jahr 2017 definierte zum ersten Mal übergreifend die Aufgaben, Kompetenzen und Prozesse der Verwaltungseinheiten des VBS im Umgang mit Cyberdefence. Die darin festgelegten Massnahmen wurden bis Ende 2020 umgesetzt. Die vorliegende Strategie Cyber VBS baut auf den Erkenntnissen des APCD auf. Sie dient dem VBS und seinen Verwaltungseinheiten dazu, sich gezielt und ganzheitlich auf die sich ständig ändernden Anforderungen vorzubereiten. Mit Massnahmenfeldern und Pflichtenheften für die Verwaltungseinheiten legt sie die konkreten Ziele bis 2024 fest.

Die Strategie Cyber VBS wurde unter Berücksichtigung verschiedener Verordnungen erarbeitet. Es geht dabei um die Verordnung vom 27. Mai 2020[1] über den Schutz vor Cyberrisiken in der Bundesverwaltung (CyRV) und das neue IKT-Lenkungsmodell zur Steuerung der Digitalisierung sowie die Verordnung vom 25. November 2020[2] über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung (VDTI). Berücksichtigt wurden ebenfalls die laufenden Vorhaben im VBS[3] und in der Bundesverwaltung sowie die Zusammenarbeit mit Partnern im In- und Ausland.

1.2 Struktur des Dokumentes

Die Strategie besteht aus vier Hauptteilen:

- Kapitel 2 reflektiert die Bedrohungslage, die Herausforderungen und die Trends.
- Kapitel 3 analysiert die Situation innerhalb des Bundes und den Beitrag des VBS nach der Umsetzung des Aktionsplans Cyberdefence.
- Kapitel 4 beschreibt die strategischen Aktivitäten.
- Kapitel 5 beschreibt die Methode zur Umsetzung der Strategie.

---

1 SR **120.73**
2 SR **172.010.58**
3 Insbesondere die Grundkonzeption Cyber der Schweizer Armee oder die Weiterentwicklung des Cyberdefence-Campus der armasuisse.

1.3 Zielgruppen

Die Strategie berücksichtigt folgende Zielgruppen:

- Das **VBS-Personal** aller Stufen (ziviles und militärisches Personal) und **Milizangehörige**, um die für ihre Dienstleistungen erforderliche Sicherheit und Resilienz zu erreichen sowie für die Sicherstellung der benötigten Fähigkeiten und Kompetenzen;
- die **Betreiber kritischer Infrastrukturen**, insbesondere diejenigen, die es dem VBS ermöglichen, seinen Beitrag zur Sicherheit und Verteidigung des Landes in allen Lagen zu erbringen;[4]
- die **Bevölkerung,** als Beitrag für die Initiativen des Bundes, der Kantone und des Privatsektors, um das Bewusstsein für die Cyberherausforderungen zu schärfen sowie zur Gewinnung von hochqualifiziertem Personal.

4 Das VBS ist auf zentrale Dienstleistungen wie den Zugang zu Energie oder Telekommunikation angewiesen. Um seine Aufgaben jederzeit und in allen Lagen erfüllen zu können, arbeitet es eng mit diesen Akteuren zusammen und schliesst mit ihnen einen Dienstleistungsvertrag ab.

2 Bedrohungen und Herausforderungen im Cyberraum

Die Analyse der Bedrohungen und allgemeinen Herausforderungen im Cyberraum ist eine Momentaufnahme in einem dynamischen Umfeld. Es werden jeweils die erwarteten Entwicklungen beschrieben, die in den nächsten Jahren im Cyberbereich an Relevanz gewinnen werden. Die nachfolgende Analyse bildet die Basis, auf der die Massnahmenfelder (vgl. Kapitel 4.5) aufgebaut werden.

2.1 Bedrohungen im Cyberraum[5]

Mit der Absicht, sich finanziell zu bereichern oder politische Interessen durchzusetzen, nutzen Staaten und nichtstaatliche Akteure zunehmend die Möglichkeiten von Informations- und Kommunikationstechnologien (IKT). Mit der fortschreitenden Digitalisierung erweitern sich die Angriffsvektoren, um an sensible Informationen zu gelangen. Dies zum Zweck der Spionage, oder um die Integrität von kritischen Infrastrukturen zu schwächen (Sabotage). Die Art, wie Informationen ausgetauscht und gespeichert werden sowie der steigende Wert digitaler Informationen bieten zusätzliche Anreize für kriminelle Geschäftsmodelle.

Der Nachrichtendienst des Bundes (NDB) beobachtet eine «deutliche Zunahme von Cyberangriffen auf Schweizer Interessen im In- und Ausland».[6] Zu den Zielen gehören unter anderem die Behörden, die Armee, die in der Schweiz angesiedelten internationalen Organisationen und ausländische Vertretungen sowie der Finanz- und Technologiesektor. Der NDB zählt Angriffe mit Verschlüsselungstrojanern zu den grössten Bedrohungsformen, welche die kritischen Infrastrukturen der Schweiz und Unternehmen betreffen. Das Schadenspotenzial ist bei den kritischen Infrastrukturen am grössten, da sie wesentliche Dienstleistungen erbringen, die für das Funktionieren der Gesellschaft zentral sind. Bis jetzt waren die kritischen Infrastrukturen der Schweiz nicht direktes Ziel eines staatlich durchgeführten Sabotageaktes. Der NDB geht zurzeit auch nicht davon aus, dass die Schweiz ein direktes Ziel von Cybersabotage werden wird. Dennoch können in der Schweiz Kollateralschäden eintreten, nämlich dann, wenn Schweizer Zulieferer als Angriffsinfrastruktur genutzt werden, um Dritte anzugreifen.

---

5 Die Erkenntnisse aus der Covid-19-Krise seit Anfang 2020 sind in die Analyse eingeflossen; erste Resultate zeigen, dass die im Cyberraum erfolgten Ereignisse die Lagebeurteilung nicht wesentlich beeinflusst haben. Folgende Erkenntnisse wurden gezogen: Erhöhter Bedarf im Bereich des *Business Continuity Managements* aufgrund der Vergrösserung der Cyberangriffsflächen; Anpassungen notwendig in der *Arbeitsorganisation*; Erhöhung der *Abhängigkeiten* (z. B. Lieferketten); Bedarf an mehr *Antizipation*.

6 Jahresbericht NDB 2020, S. 83, https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-80848.html

Erwartete Entwicklung

Böswillige Handlungen werden vermehrt automatisiert und gestützt auf künstliche Intelligenz ausgeführt. Unzureichende Sicherheitskonfigurationen einer immer komplexeren System- und Infrastrukturumgebung mit vielen Systemen verschiedener Generationen (Legacy Systems) werden systematisch ausgenutzt. Der Missbrauch des Cyberraums für Manipulation, Desinformation und Destabilisierung dürfte mit der wachsenden Bedeutung von sozialen Medien und der Hyperkonnektivität weiter zunehmen. Dieser Trend steht auch im Zusammenhang mit den wachsenden geopolitischen Spannungen, die zusätzlich verschärfend wirken.

2.2 Herausforderungen im Cyberraum

2.2.1 Technologische Entwicklungen, Abhängigkeiten und Machtpolitik

Die technologische Entwicklung steht zunehmend im Mittelpunkt vieler Politikfelder (*Policies*) von Staaten und der Wirtschaft. Staaten, die sich in einer multipolaren Weltordnung stark positionieren wollen, treiben die technologische Entwicklung besonders rasch voran, wie zum Beispiel im Bereich Quantencomputing[7]. Zu berücksichtigen ist ebenfalls das zunehmende Bemühen von Staaten, sich durch rechtliche und politische Instrumente einen privilegierten Zugang zu Schlüsseltechnologien und Daten zu verschaffen, von denen auch das VBS abhängig ist.[8]

Wegen des wachsenden Einflusses grosser Technologiefirmen werden Staaten, Unternehmen und Einzelpersonen durch die laufende Weiterentwicklung von Systemen und Plattformen zu neuen Investitionen und Kapazitäten gezwungen. Auch bezüglich der Auswertung grosser Datenmengen oder im Bereich der Nachrichtenbeschaffung, wo die Technologiegiganten über eine Vielzahl an Sensoren und Daten in Echtzeit verfügen, werden solche Unternehmen zunehmend bedeutende internationale Akteure. Diese Technologiegiganten kaufen zudem innovative Unternehmen auf und erschweren damit den Markteintritt von neuen Mitbewerbern.

Aus diesem Wettlauf resultieren vermehrte Spionageaktivitäten, einschliesslich der Cyberspionage[9], insbesondere in strategisch relevanten Bereichen wie der medizinischen Forschung (z. B. bezüglich Impflösungen für die Bewältigung der Corona-Krise). Die Frage sicherer und zuverlässiger Lieferketten hat sich im Rahmen der Covid-19-Krise verschärft.

---

7 Immer wieder kommt es zu Fortschritten im Bereich Quantencomputing. Die Entwicklung dieser Hochleistungsmaschinen sollte noch längere Zeit andauern.

8 Die internationale, rechtliche Lage hat auch Auswirkungen auf die Geschäftstätigkeiten des VBS, so z. B. der CLOUD Act der USA (Clarifying Lawful Overseas Use of Data Act), die General Data Protection Regulation (GDPR) der Europäischen Union oder das chinesische Gesetz zur Cybersicherheit und das Multi-Level Protection System (MLPS).

9 Lagebericht 2020 des Nachrichtendienstes des Bundes, S. 12.

Erwartete Entwicklung

Im technologischen Bereich ist mit steigendem Druck einzelner Staaten und Hersteller zu rechnen. Investitionen in Technology Foresight und in die Forschung und Entwicklung proprietärer[10] Lösungen werden an Relevanz gewinnen. Starke Leistungen in Forschung und Ausbildung (z. B. für Simulationen) sowie der aktuellste Wissensstand auf Gebieten wie Big Data, künstliche Intelligenz, Quantencomputing, Energieerzeugung und -speicherung, Blockchain und Raumfahrttechnologien sind in Bezug auf Cyberrisiken und IT-Dienstleistungen relevant. Diese Entwicklungen begünstigen eine immer engere Zusammenarbeit mit Hochschulen und der Wirtschaft, insbesondere in der Trust Economy, die in der Schweiz mit der kürzlich erfolgten Lancierung des Trust Valley eine internationale Dimension erhält.

Die vorherrschenden Technologieunternehmen dürften weiter an Macht gewinnen und durch die laufende Weiterentwicklung System- und Plattformwechsel erzwingen. Dadurch wird sich die Frage der Lieferketten und Lebenszyklen als grundlegendes Thema für die Cybersicherheit voraussichtlich weiter akzentuieren.

2.2.2 Knappheit natürlicher Ressourcen

Im IKT-Bereich stehen Mineralressourcen (wie seltene Erden, Kobalt, Lithium, Aluminium) im Zentrum der Herstellung vieler Ausrüstungsgegenstände, von denen das VBS (insbesondere die Armee für wichtige Ausrüstungen) abhängig ist. Ebenso wichtig ist die Stromversorgung. Aufgrund der Marktlage und der internationalen Spannungen kann es zu kurzen oder langfristigen negativen Auswirkungen kommen. Die Entwicklung und Tätigkeiten der Verwaltungseinheiten im VBS könnten dadurch stark beeinträchtigt werden.

Erwartete Entwicklung

Mit der Vervielfachung von Technologien, die auf spezifische und seltene Grundstoffe und auf Energie angewiesen sind (der Verbrauch wird diesbezüglich in den nächsten Jahren voraussichtlich ansteigen), sind internationale Spannungen zu erwarten, die sich beispielsweise in Versorgungsschwierigkeiten oder Preisvolatilität äussern können.

10 Herstellergebundene und nicht einsehbare Technologie oder Software.

2.2.3 Ausbildungsbedarf und Engpässe bei den Fachkräften

Mit der fortschreitenden Digitalisierung der Gesellschaft steigen nicht nur die Anforderungen an die Fähigkeiten aller Mitarbeitenden bei der Nutzung von Informations- und Kommunikationstechnologien und deren Sicherheit, sondern auch der Bedarf an IKT-Fachkräften.

Die Erhebung der Bildungsangebote zeigt, dass das VBS über ein breites internes[11] und externes Angebot zur Sensibilisierung sowie Aus- und Weiterbildung im Bereich Cybersicherheit verfügt. Weitere Initiativen werden laufend entwickelt, wie zum Beispiel das Programm ICT Warrior Academy der FUB für die Förderung von Fachkarrieren. Die Erhebung zeigt Lücken bei der Festlegung der Bildungsziele sowie der Messung der Wirksamkeit der Bildungsprodukte. Die Weiterbildungsangebote z. B. von CAS und DAS Cybersicherheit der ETHZ[12], die primär für das VBS entwickelt wurden, werden noch wenig genutzt. Nebst der seit 2018 laufenden Ausbildung im Rahmen des Cyberlehrganges[13] hat die FUB für die Gruppe Verteidigung (Gruppe V) und die Armee ein Ausbildungskonzept erstellt. Ein ähnliches Konzept für die Bedürfnisse aller anderen Verwaltungseinheiten des VBS ist noch ausstehend.

Bis jetzt sind bei den verfügbaren VBS-Stellen noch keine erheblichen Probleme spürbar. In Bezug auf qualifizierte IKT-Fachleute sind aber mittelfristig Rekrutierungsschwierigkeiten zu erwarten. Eine Anstellung im Bereich Cyberdefence beim VBS ist zwar inhaltlich attraktiv, jedoch wirtschaftlich und ortsabhängig nicht immer wettbewerbsfähig. Der Frauenanteil in der Cybersicherheit ist gering: in der IKT-Branche beträgt er nur ca. 14,5 Prozent. Eine Ursache davon ist ist, dass Frauen allgemein in Fächern wie Mathematik, Physik und Informatik deutlich untervertreten sind. Der Ausschöpfung dieser Potenziale ist besondere Beachtung zu schenken.

Erwartete Entwicklung

Weltweit wird in den nächsten Jahren qualifiziertes Personal im IKT-Bereich fehlen. In der Schweiz werden gemäss ICT-Berufsbildung Schweiz[14] im Jahr 2026 fast 20% des Bedarfs an qualifiziertem IKT-Personal fehlen, davon bis 25% im Sicherheitsbereich. Dieser Trend dürfte unter anderem zu einem Anstieg der Personal- und Dienstleistungskosten und zu einer Abwanderung der besten Talente zu den meistbietenden Unternehmen führen. Innovative und agile Arbeitsweisen sowie attraktive Arbeitsmethoden[15] werden es ermöglichen, qualifiziertes Personal und einen höheren Anteil an Frauen zu rekrutieren.

---

11 U. a. verfügt das VBS über ca. 40 Lektionen zur integralen Sicherheit, Informationssicherheit und Cyberdefence.

12 CAS in Cyber Security (https://inf.ethz.ch/de/weiterbildung/cas-cybersecurity.html) und DAS in Cyber Security (https://inf.ethz.ch/de/weiterbildung/das-cybersecurity.html) der ETH Zürich. Fachhochschule Nordwestschweiz: CAS Cybersecurity und Information Risk Management (CISSP / BSI / ISO) | FHNW

13 Kann zu einem zivil anerkannten Eidgenössischen Fachausweis EFA Cyber Security Specialist führen.

14 Quelle: ICT-Berufsbildung Schweiz (www.ict-berufsbildung.ch).

15 Zu diesen Ansätzen gehören Wettbewerbe wie «Swiss Cyber Storms», «Cyber 9/12 Strategic Challenge» mit dem GCSP, «Capture the Flag», «Cyber Challenges» oder Data-Science-Wettbewerbe.

3

3 Cybersicherheit in der Bundesverwaltung

Mit dem Beschluss des Bundesrates zur Nationalen Strategie zum Schutz vor Cyberrisiken (2018) sowie der CyRV wurde ein umfassendes System aufgebaut. Es besteht aus den drei Bereichen Cybersicherheit, Cyberdefence und Cyberstrafverfolgung. Der Delegierte des Bundes für Cybersicherheit sorgt für eine optimale Abstimmung der überdepartementalen Arbeiten der Bereiche Cybersicherheit, -defence und -strafverfolgung und ist für die Koordination der interdepartementalen Gremien zuständig.

3.1 Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS)

Die NCS für die Jahre 2018–2022[16] gibt die strategischen Ziele zum Schutz vor Cyberrisiken in zehn Handlungsfeldern vor. Zwischen den Bereichen bestehen inhaltliche Überschneidungen und gegenseitige Abhängigkeiten. Deshalb ist eine enge Zusammenarbeit besonders wichtig. Zu diesem Zweck sind mit der **Kerngruppe Cyber** (zur Koordination innerhalb des Bundes unter Einbezug der Kantone) und dem **Steuerungsausschuss NCS** (zur Koordination der Umsetzung der NCS unter Einbezug aller Akteure, sei es innerhalb oder ausserhalb der Bundesverwaltung) zentrale Gremien geschaffen worden. Beide stehen unter der Leitung des Delegierten des Bundes für Cybersicherheit, der sicherstellt, dass die Arbeiten eng koordiniert stattfinden und Synergien optimal genutzt werden.[17] In weiteren Gremien werden beispielsweise technische Angelegenheiten sowie internationale Beziehungen koordiniert.

3.2 Aufgabenteilung innerhalb der Bundesverwaltung

Die Organisation der Bundesverwaltung zum Schutz vor Cyberrisiken sowie die Aufgaben und Zuständigkeiten der verschiedenen Stellen im Bereich Cybersicherheit sind in der CyRV festgelegt.

Cybersicherheit

Für die Koordination des Bereichs Cybersicherheit ist das Nationale Zentrum für Cybersicherheit (NCSC) zuständig. Das NCSC ist verantwortlich für die Gesamtheit der Massnahmen, welche der Prävention, der Bewältigung von Vorfällen und der Verbesserung der Resilienz gegenüber Cyberrisiken dienen. Zu diesem Zweck soll auch die internationale Zusammenarbeit gestärkt werden. Das EDA koordiniert die internationalen Kontakte in enger Abstimmung mit dem NCSC und dem VBS.

---

16 Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) für die Jahre 2018–2022 (https://www.ncsc.admin.ch/ncsc/de/home/strategie/strategie-ncss-2018-2022.html)

17 Weitere Informationen zur NCS unter www.ncsc.admin.ch/ unter NCS-Strategie.

Cyberdefence

Für Cyberdefence ist das VBS zuständig.[18] Dazu gehört die Gesamtheit der nachrichtendienstlichen und militärischen Massnahmen zu folgenden Zwecken: dem Schutz der für die Sicherheit des Landes kritischen Systeme, der Abwehr von Cyberangriffen, der Gewährleistung der Einsatzbereitschaft der Armee in allen Lagen und dem Aufbau von Kapazitäten und Fähigkeiten zur subsidiären Unterstützung ziviler Behörden. Dazu zählen aktive Massnahmen zur Erkennung von Bedrohungen, zur Identifikation von Angreifern und zur Störung und Unterbindung von Angriffen.

Cyberstrafverfolgung

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

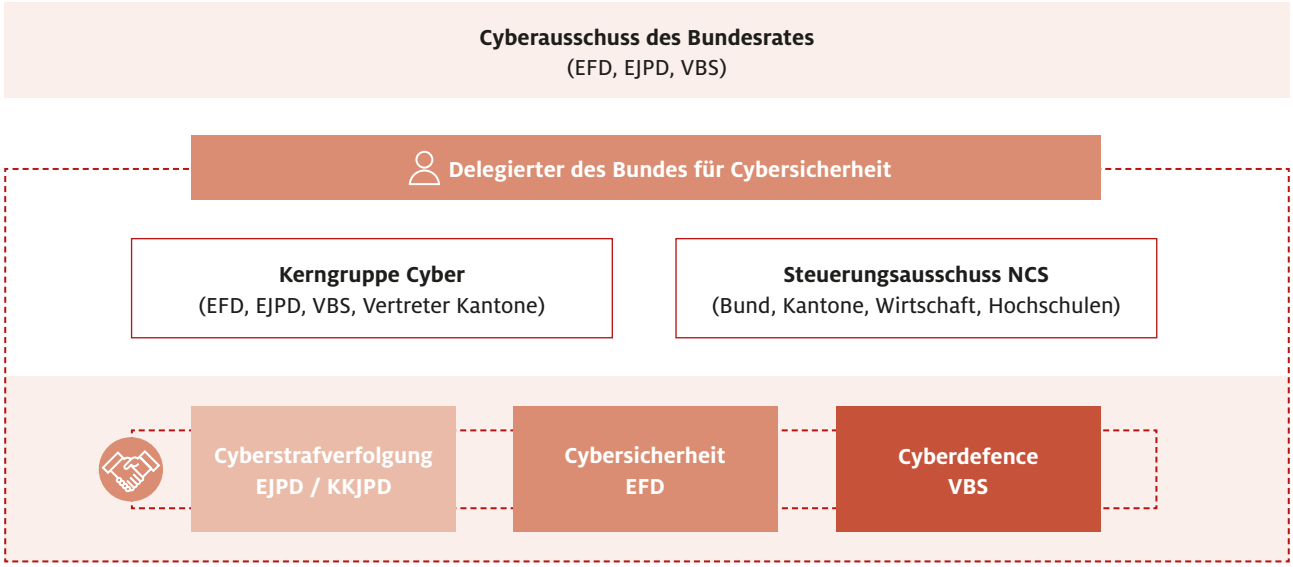


Abbildung 1 – Cybersicherheit in der Bundesverwaltung

3.3 Aktuelle VBS-Leistungen im Cyberraum

Die Bundesverwaltung wurde mehrmals Opfer von Cyberangriffen. Nach dem Angriff auf die RUAG 2016 erteilte der damalige Chef VBS den Auftrag, einen Aktionsplan Cyberdefence (APCD) für die Periode 2017–2020 zu erstellen. Im Rahmen der Ausarbeitung dieses Aktionsplans wurden die Aufgaben definiert, welche das VBS im Bereich Cyberdefence erfüllen soll.

18 swisstopo und das BASPO sind im Rahmen der Cyberdefence und der Cyberabwehr nicht betroffen.

Mit dem Schlussbericht vom 28. Januar 2021 wurde eine Beurteilung der Zielerreichung vorgenommen. Der Bericht legt ebenfalls dar, welche Lücken noch bestehen. Die Beurteilung basiert auf einer Selbsteinschätzung der Fachexperten und -expertinnen der Verwaltungseinheiten des VBS. In den folgenden Kapiteln werden die Ziele und Aufgaben des Aktionsplans sowie Verbesserungsvorschläge dargelegt.

3.3.1 Fokus des Aktionsplans Cyberdefence (APCD) VBS

Im Fokus des APCD standen die enge Zusammenarbeit mit Partnern der Wirtschaft und Hochschulen sowie die quantitativ und qualitativ ausreichenden Mittel für drei Hauptziele:

1. *«Dem VBS als Betreiber kritischer Infrastrukturen und innerhalb seiner Kompetenzen ermöglichen, die in Anzahl, Intensität und Komplexität zunehmenden Formen der Cyberbedrohung zu bewältigen, sowohl im Alltag als auch im Falle einer Krise oder eines Konflikts;*
2. *die Cyberaspekte des Bundesgesetzes vom 25. September 2015*[19] *über den Nachrichtendienst (NDG) und des Bundesgesetzes vom 3. Februar 1995*[20] *über die Armee und die Militärverwaltung (MG) konkret umsetzen;*
3. *in der Lage sein, die Betreiber kritischer Infrastrukturen, die Opfer von Cyberangriffen wurden, bei Bedarf wirksam und nachhaltig zu unterstützen.»*

3.3.2 Bewertung der Hauptbereiche des Cyberdefence-Dispositivs des VBS

Der generelle Auftrag «Cyberdefence» wurde im Rahmen des Aktionsplanes in vier Funktionen (Steuerung, Cyberschutz, Abwehr und Aktion im Cyberraum sowie Unterstützung) unterteilt. Abbildung 2 zeigt die Architektur des APCD und deren Einbettung in den rechtlich-politischen Rahmen sowie die Absicht der Zusammenarbeit mit verschiedenen Partnern.

Abbildung 2 – Hauptbereiche des Cyberdefence-Dispositivs des VBS

19 SR 121
20 SR 510.10

Nachfolgend wird die Zielerreichung dieser Hauptbereiche bewertet. Die Bewertung ist das Ergebnis einer Einschätzung durch die betroffenen Ämter und Organisationen.

- **Steuerung**: Mit der Koordination und strategischen Führung der Cyberdefence-Aktivitäten innerhalb des VBS durch das GS-VBS, der Schaffung der Stelle eines Delegierten VBS für Cyberdefence und seit Anfang 2020 der neuen Abteilung Digitalisierung und Cybersicherheit (DCS) wurden die erwarteten Ziele erreicht.
- **Cyberschutz**: Mit der Umsetzung der APCD-Ziele wurden massgebliche Fortschritte gemacht. Dazu zählen z. B. die Schaffung eines Chief Information Security Officer (CISO), welcher die Cybersicherheit führt und über ein Security Operations Center (SOC), das milCERT (militärische Computer Emergency Response Team) und das Cyber Operations Center (CyOC) verfügt; diese stellen die kontinuierliche Überwachung der eigenen Netzwerke und Systeme sicher.
- **Abwehr und Aktion im Cyberraum**: Der NDB hat die Kompetenz und die Fähigkeiten, sicherheitspolitisch relevante staatliche Cyberangriffe auf Schweizer Interessen frühzeitig zu erkennen. Er erstellt insbesondere in Zusammenarbeit mit der Armee, dem NCSC und fedpol eine umfassende Cyberlage, die er beispielsweise in die Kerngruppe Cybersicherheit einbringt. Die nachrichtendienstlichen Fähigkeiten zur Antizipation, Sensibilisierung, Vorbeugung und Attribution werden kontinuierlich ausgebaut (z. B. wird der Bereich Open Source Intelligence gestärkt).
  In der Gruppe V wurden nebst den APCD-Zielen zusätzliche Massnahmen angeordnet, welche in Überprüfung, in Vorbereitung oder im Aufbau sind. Dazu gehören die mobilen Einsatzmittel, die Koordination der Cyberoperationssphäre mit den anderen Operationssphären der Armee sowie die Schaffung des «Cyber Training Centres».
- **Unterstützung**: Neben dem Aufbau der eigenen Fähigkeiten von armasuisse Wissenschaft und Technologie konnte auch der neue Cyberdefence-Campus (CYD-Campus) zur Erweiterung des ursprünglich vorgesehenen Dispositivs umgesetzt werden. Die enge Zusammenarbeit mit den beiden ETH (mit der Schaffung von Aussenstellen in Zürich und Lausanne) wird es ermöglichen, den CYD-Campus rasch weiterzuentwickeln. Im Bereich der Sensibilisierung und Ausbildung wurden wesentliche Fortschritte erzielt. Die Analyse zeigt, dass eine gegenseitige Abstimmung innerhalb des Bildungssystems unerlässlich ist, um den Herausforderungen der Digitalisierung gerecht zu werden.

3.3.3 Bewertung der Hauptziele des VBS im Cyberraum

Innerhalb der oben aufgeführten Funktionen wurden verschiedene Aufgaben definiert. Die Erfüllung der für diese Aufgaben gesetzten Ziele wird wie folgt bewertet:

- **Sicherheit und Abwehr bei den eigenen IKT-Systemen und -Infrastrukturen in allen Lagen:** Die vorhandenen Mittel ermöglichen den Verwaltungseinheiten des VBS, den alltäglichen Cyberbedrohungen zu begegnen. Viele Massnahmen sind zur Stärkung der eigenen Cybersicherheit (qualitativ) im Aufbau. Aus heutiger Sicht reichen diese Mittel nicht aus, um mehreren gleichzeitig geführten Angriffen standzuhalten.

- **Aufgaben des NDB und der Armee**: Im Umgang mit Cyberrisiken leistet der NDB gestützt auf das NDG einen massgebenden Beitrag zur frühzeitigen Erkennung und Vorbeugung von Cyberangriffen auf Schweizer Interessen. Er hat die Fähigkeit, Cyberangriffe zu identifizieren und zuzuordnen (Attribution). Er bedient Entscheidungsträger auf föderaler und kantonaler Ebene mit umfassenden nachrichtendienstlichen Informationen und mit Beurteilungen der Cyberbedrohungen (Cyberlage).
  Die Armee verantwortet den Cyberschutz der IKT-Infrastrukturen VBS, die militärische Cyberabwehr und die Aktionen im Cyberraum im Rahmen von militärischen Operationen. Zudem erbringt sie subsidiäre Unterstützung zugunsten der zivilen Behörden. Es besteht Potenzial in der Abstimmung zwischen der Operationssphäre Cyber und den Sphären Boden, Luft, Weltraum, Elektromagnetik und Informationsraum.
- **Unterstützung der Betreiber kritischer Infrastrukturen bei Cyberangriffen**: Der NDB unterstützt die Betreiber kritischer Infrastrukturen im Rahmen des Public Private Partnership-Ansatzes. Der NDB stellt unter anderem sektorspezifische Lageradare zur Verfügung, ist rund um die Uhr erreichbar. Er bietet bei Bedarf, gestützt auf Artikel 6 Absatz 6 des NDG, sensiblen Unternehmen, Dienstleistern und Betreibern kritischer Infrastrukturen Sensibilisierungsarbeit an. Das Nachrichtendienstgesetz schafft zudem die gesetzlichen Rahmenbedingungen, um letztere im Fall von Cyberangriffen zu unterstützen.
- **Übungen:** Nationale und internationale Übungen ermöglichen es, die eigenen Kompetenzen und Prozesse[21] fortlaufend zu überprüfen und zu verbessern. Sie dienen der Stärkung der internationalen Kooperation. An den Übungen erkennt man oft besondere Talente, etwa bei jungen Mitarbeitenden. Auf strategischer und technisch-operativer Ebene nimmt das VBS an verschiedenen Übungen teil, wie zum Beispiel strategische Führungsübungen (SFU), Sicherheitsverbundsübungen (SVU) oder «Cyber Pakt» sowie «Locked Shields», «Cyber Coalition», «ENISA Cyber Europe Exercise» und «Cyberstorm» (International Watch and Warning Network, IWWN).
- **Internationale Zusammenarbeit:** Das VBS arbeitet im Bereich Cyberdefence mit zahlreichen internationalen Partnern zusammen.[22] Das GS-VBS funktioniert als Schnittstelle, um die internationalen Aktivitäten der einzelnen Verwaltungseinheiten zu erleichtern und aufeinander abzustimmen. Kooperationen sind zeitaufwändig und sollen demzufolge ressourcengerecht geplant und mit nachweisbarem Mehrwert durchgeführt werden. Die internationale Zusammenarbeit im Bereich Cyberdefence erfolgt multilateral und bilateral und, wo erforderlich, mit anderen Departementen,vor allem mit dem EDA. **Multilateral** kooperiert die Schweiz im Cyberbereich insbesondere mit der NATO (z. B. als *Contributing Nation* beim *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) in Tallinn) und mit der europäischen Verteidigungsagentur. **Multi- und bilateral** pflegt der NDB eine regelmässige Zusammenarbeit mit ausländischen Partnern. Die anderen Verwaltungseinheiten kooperieren in erster Linie mit Frankreich, Deutschland und Österreich. Diese Zusammenarbeit ist für die Einschätzung von Bedrohungen und Herausforderungen im Cyberbereich sowie im Hinblick auf Aufdeckung und Verhinderung von Cyberangriffen unverzichtbar.

---

21 Wie von der SVU19 bestätigt, besteht Verbesserungsbedarf bei der subsidiären Unterstützung durch die Armee, den operationellen Prozessen sowie den VBS-Beiträgen und der Armee in den Bereichen Ausbildung und Übungen.

22 Seit 2018 erstellt das VBS vierteljährlich einen Gesamtüberblick über die internationale Zusammenarbeit. Dazu gehört u. a. die Partnerschaft für den Frieden (PfP), ein Element der militärischen Kooperation.

3.3.4 Verbesserungsmassnahmen aus dem APCD

Aus der vorhergehenden Beurteilung ergeben sich folgende Erkenntnisse, die in die Erarbeitung der vorliegenden Strategie eingeflossen sind:

- **Steuerung**: Die Architektur soll vervollständigt, die Umsetzung der Massnahmen besser messbar und steuerbar und die Koordination sowie die Zusammenarbeit mit den Partnern gestärkt werden. Die Vorgaben sind zu vereinfachen und an die künftigen Herausforderungen der Digitalisierung anzupassen. Zudem sind die diesbezügliche Gouvernanz, die entsprechenden Aufgaben, Kompetenzen und Verantwortlichkeiten zu überarbeiten.
- **Cyberschutz**: Die Schutz- und Abwehrmassnahmen sollen gegenüber Angriffen mit hoher Intensität und langer Dauer in Einklang gebracht werden. Diese sollen in Zusammenarbeit mit den betroffenen Stellen der Bundesverwaltung erfolgen.[23]
- **Abwehr und Aktion im Cyberraum**: Die Fähigkeiten zur Früherkennung und Attribution sollen ausgebaut werden, sodass alle sicherheitspolitisch relevanten Cyberangriffe frühzeitig erkannt und zugeordnet werden können. Die Abstimmung des Cyberbereichs mit den militärischen Führungsprozessen anderer Operationssphären (Boden-, Luft-, Welt-, elektromagnetischer und Informationsraum) soll weiterentwickelt werden.
  Die Mittel der Armee werden primär für die eigene Auftragserfüllung eingesetzt und sollen in den folgenden Bereichen erweitert werden: Durchhaltefähigkeit, Frühwarnung und aktive Massnahmen. Damit können auch Betreiber kritischer Infrastrukturen besser unterstützt werden. Es kommt in Kooperation mit der Geschäftsstelle SKI des BABS zu einer Überarbeitung der Zusammenarbeitsvereinbarungen mit den Betreibern kritischer Infrastrukturen, welche für die Erfüllung der VBS-Aufgaben unerlässlich sind.
- **Unterstützung**: Es ist ein umfassenderes, auf Stufe Departement koordiniertes Ausbildungs- und Sensibilisierungssystem zu etablieren. Dieses wird mit den Sensibilisierungsmassnahmen des Bundes abgestimmt, um den künftigen Herausforderungen der Digitalisierung im Personalwesen gerecht zu werden. Zudem sollen bei Beschaffungen die Sicherheit von Lieferketten und Lebenszyklen im Zentrum stehen. Alle Akteure in den Prozessen sollen sich systematisch mit dieser Thematik befassen.
- **Kommunikation**: Um das VBS als attraktiven Arbeitgeber im Cyberbereich zu positionieren, soll auf die Ausbildungs- und Karriereangebote stärker aufmerksam gemacht werden. Diese Aktionen sind mit den anderen Institutionen wie NCSC zur Multiplikation der Nachrichten abzustimmen. Zusätzlich soll die Rolle des VBS im Bereich Cyberdefence bekannter werden.

---

23 Dazu gehören die Umsetzungen der Empfehlungen der EFK aus dem Jahr 2019. https://www.efk.admin.ch/de/publikationen/wirtschaft-verwaltung/informatikprojekte/3911-informatiksicherheit-fuehrungsunterstuetzungsbasis.html

4

4 Strategie Cyber VBS 2021–2024

Inhalt des nachfolgenden Kapitels sind die strategischen Aktivitäten Cyberdefence VBS und die Aufgabenteilung im VBS. Sie basieren auf den Erkenntnissen aus den vorangehenden Kapiteln, den identifizierten Herausforderungen sowie den rechtlichen Grundlagen.

4.1 Strategischer Rahmen

4.1.1 Einleitung

Die Herausforderungen des Cyberraums sind vielfältig und können insbesondere volatil, unsicher, komplex und mehrdeutig sein. Wenn eine Entität (Staat, Organisation, Unternehmen oder Individuum) diese Herausforderungen nicht rechtzeitig erkennt, versteht und behandelt, können sie sich zu Gefahren, Bedrohungen[24] und zu Risiken[25] entwickeln oder Chancen können verpasst werden.

4.1.2 Handlungsgrundsätze VBS

Die Funktionen und Aufgaben des VBS werden von den gesetzlichen Grundlagen vorgegeben (vgl. Kapitel 4.1.3). Zusätzlich legt das VBS bei der Erfüllung der Aufgaben folgende Handlungsgrundsätze fest:

- **Subsidiarität**: In der Praxis stellt sich regelmässig die Frage, ob die im VBS vorhandenen Cyberkompetenzen auch anderen Sicherheitsorganisationen[26] oder zivilen Akteuren zur Verfügung stehen. Was die Kompetenzen innerhalb der Armee betrifft, gilt gemäss Artikel 58 Absatz 2 der Bundesverfassung und gemäss Militärgesetz: Die Armee unterstützt die zivilen Behörden bei der Abwehr schwerwiegender Bedrohungen der inneren Sicherheit und bei der Bewältigung anderer ausserordentlichen Lagen, wenn deren Mittel nicht mehr ausreichen (Grundsatz der Subsidiarität gem. Artikel 1 und 67 des MG). Die Cybermittel der Armee müssen bereitgestellt werden, um zivile Behörden während möglichen Ereignissen subsidiär unterstützen zu können. Dafür muss die Armee laufend mit den zivilen Behörden zusammenarbeiten. Dies umfasst u. a. Wissenstransfer, Übungen und die Beteiligung an internationalen Aktivitäten.

---

24 Definition gem. Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz 2010 (Ziff. 3.2.1): Eine Bedrohung setzt einen Willen voraus, die Schweiz oder ihre Interessen zu schädigen oder zumindest eine solche Schädigung in Kauf zu nehmen. Eine Gefahr setzt keinen Willen zur Schädigung voraus (z. B. Naturgefahren und technische Gefahren).

25 Definition Risiko: Produkt der Eintretenswahrscheinlichkeit einer Gefahr oder Bedrohung und deren Auswirkungen.

26 Am Beispiel von fedpol, kantonalen Polizeikorps, Sicherheitsverbund Schweiz usw.

- **Institutionelle Zusammenarbeit**: Das VBS bringt seine Mittel in die Zusammenarbeit mit den anderen sicherheitspolitischen Partnern in der Schweiz ein. Der Artikel 4 der CyRV bestimmt die Grundsätze der Zusammenarbeit und des Informationsaustausches mit den Kantonen, den Gemeinden, der Wirtschaft, der Gesellschaft, der Wissenschaft und den internationalen Partnern, soweit diese dem Schutz der eigenen Sicherheitsinteressen entsprechen. Dieser Verordnung (Art. 6a CyRV) und der NCS (Ziff. 4.8 und 5.1) ist zudem zu entnehmen, dass das VBS für den Bereich Cyberdefence zuständig ist. Es koordiniert, unter Federführung des Delegierten für Cybersicherheit des Bundes, seine Aktivitäten mit den anderen Bereichsverantwortlichen (Cybersicherheit, Cyberstrafverfolgung) in der dafür vorgesehenen Kerngruppe Cyber, in der auch die Kantone vertreten sind. Im Steuerungsausschuss NCS beteiligt sich das VBS zudem aktiv an der laufenden Weiterentwicklung des nationalen Dispositivs.
- **Internationale Zusammenarbeit**: Die internationale Zusammenarbeit bei Cyberdefence sollte je nach Interessenlage und Möglichkeiten sowohl multilateral als auch bilateral fortgesetzt und gegebenenfalls verstärkt werden. Dies geschieht in Abstimmung mit den internationalen Tätigkeiten anderer Departemente (insbesondere EDA, EFD und EJPD). Die Wichtigkeit der internationalen Zusammenarbeit hat vor allem mit der Gewinnung eines umfassenden Bildes der Cyberbedrohungen und den neuen Herausforderungen im Cyberraum zu tun.
- **Aufgeschlossenheit / Offenheit**: Cybervorfälle finden täglich statt. Für deren Bewältigung sind Kooperationen und Wissensaustausch wichtig. Unter Berücksichtigung des Subsidiaritätsprinzips und den gesetzlichen Vorgaben sowie in enger Abstimmung mit dem Nationalen Zentrum für Cybersicherheit (NCSC) sollen die Kompetenzen, welche innerhalb des VBS zur Verfügung stehen, auch weiteren Partnern angeboten werden, sofern dies mit der Auftragserfüllung des VBS vereinbar ist. Weitergehende zusätzliche Leistungen des VBS werden auf Anfrage geprüft.
- **Kommando Cyber:** Der Bundesrat will mit Blick auf die aktuelle Bedrohungslage die FUB auf Anfang 2024 in ein Kommando Cyber weiterentwickeln. Die Digitalisierung und die damit einhergehende Modernisierung und Vernetzung sämtlicher Systeme der Armee schreiten rasch voran. Diese Entwicklung stellt hohe Anforderungen, insbesondere im Bereich Cyberschutz. Um diesen Anforderungen künftig besser gerecht zu werden, soll die FUB von einer breit gefächerten Unterstützungsorganisation in ein einsatzorientiertes Kommando weiterentwickelt werden. Das Kommando Cyber soll künftig über die militärischen Schlüsselfähigkeiten in den Bereichen militärisches Lagebild, Cyberabwehr, IKT-Leistungen, Führungsunterstützung, Kryptologie und elektronische Kriegsführung verfügen. Die Wichtigkeit des Bereichs macht es notwendig, dass das Kommando Cyber in der Armeeführung weiterhin vertreten bleibt. Nach aktueller Auffassung wird das Kommando Cyber auf Stufe Armee bestehen bleiben.

4.1.3 Rechtlicher Rahmen der VBS-Leistungen im Cyberraum

Der rechtliche Rahmen der Aktivitäten der Verwaltungseinheiten des VBS wird insbesondere durch das NDG, das MG und die CyRV festgelegt. Zudem müssen insbesondere folgende rechtliche Grundlagen berücksichtigt werden: das Bundesgesetz über die militärischen Informationssysteme vom 3. Oktober 2008[27] (MIG), die Verordnung vom 30. Januar 2019[28] über die militärische Cyberabwehr (MCAV), das Bundesgesetz vom 20. Dezember 2019[29] über den Bevölkerungs- und Zivilschutz (BZG), das Bundesgesetz vom 19. Juni 1992[30] über den Datenschutz (DSG) sowie die VBS-internen Vorgaben wie die Weisungen über die Führung und Organisation der Sicherheit (WeFOS). Auch wird das neue Informationssicherheitsgesetz (ISG) ab Inkrafttreten zentral sein. Die nachfolgende Tabelle bietet eine Übersicht über die Tätigkeiten des VBS im Cyberraum.

	Cyberschutz	Cyberabwehr	Aktion im Cyberraum
Bürger / Individuum	Eigenverantwortung. Keine VBS-Leistung.	Strafverfolgungskette bei Vorfällen. Keine VBS-Leistung.	Keine direkte VBS-Leistung.
Wirtschaft	Eigenverantwortung der Unternehmen. VBS-Leistungen im Rahmen der Sensibilisierung.	Strafverfolgungskette bei Vorfällen. VBS-Leistung nur bei besonders hoher Kritikalität für das Land.	
Betreiber kritischer Infrastrukturen	Eigenverantwortung der KI-Betreiber auf der Grundlage ihrer gesetzlichen Verpflichtungen und der Standards ihrer Wirtschaftsbereiche. Die VE-VBS tragen zur Sensibilisierung bei Cyberrisiken und zur Interoperabilität bei.	Eigenverantwortung der KI-Betreiber auf der Grundlage ihrer gesetzlichen Verpflichtungen. Im Fall eines Cyberangriffs kann der NDB (Art. 26 Bst. d NDG; Art. 37 Abs. 1 NDG) Betreibern helfen. Bei Bedarf kann die Verteidigung (Art. 67, Abs. 1 Bst. d MG) subsidiär unterstützen.[31]	
VBS	Eigenverantwortung des VBS auf der Grundlage der Sicherheitsverfahren und Informatiksicherheitsvorgaben Bund und der VBS-eigenen Vorgaben[32].	Abwehr bei eigenen IKT-Systemen und -Infrastrukturen (Art. 26 Abs. 1 Bst. d und 37 Abs. 1 NDG; Art. 100 Abs. 1 Bst. c MG). Der NDB (mit Unterstützung der Gruppe V) ist für die Cyberlage und Attribution zuständig.	Aktive Informationsbeschaffung (Art. 26 Abs. 1 Bst. d und 37 Abs. 1 NDG) und Wirkung im Cyberraum (gem. Kriegsvölkerrecht / humanitärem Völkerrecht).

Tabelle 1 – Rechtlicher Rahmen der VBS-Leistungen im Cyberraum

27 SR **510.91**
28 SR **510.921**
29 SR **520.1**
30 SR **235.1**
31 Es handelt sich um eine subsidiäre Unterstützung, die keine aktiven Gegenmassnahmen beinhaltet. Diese können nur vom NDB durchgeführt werden.
32 Im VBS wendet man das NIST-Framework an (National Institute of Standards and Technology), sowie die ISO 27000-Serie (International Organization for Standardization / Information Security Management Systems).

Es laufen Vorbereitungen zur Einführung einer Meldepflicht für Betreiber kritischer Infrastrukturen durch den Cyberdelegierten des Bundes bei einem Cybervorfall.[33] Das VBS (exkl. Armee) unterliegt den Bestimmungen der CyRV, wonach Cybervorfälle und Schwachstellen sowie Sicherheitsvorfälle gestützt auf Artikel 14 CyRV dem NCSC zu melden sind.

4.2 Strategie

Wir tragen zum Schutz des Landes bei, verteidigen es im Cyberraum und erhöhen somit dessen Handlungsfreiheit massgeblich.

Es liegt im sicherheitspolitischen Interesse der Schweiz, Handlungsfreiheit und Integrität des Staats, der Wirtschaft und der Bevölkerung auch im Cyberraum zu schützen und im Konfliktfall zu verteidigen. Das VBS ist, im Verbund mit seinen Partnern bei Bund und Kantonen, Wirtschaft und Hochschulen, sowie bei Bedarf internationalen Partnern, für die Cyberdefence der Schweiz zuständig. Es antizipiert und analysiert im Rahmen seiner Verantwortlichkeiten die Cyberherausforderungen und -bedrohungen und erbringt Sicherheitsleistungen zur Bewältigung von Cybervorfällen in Friedenszeiten, Spannungen und Konflikten. Das VBS trägt (subsidiär) dazu bei, kritische Infrastrukturen vor Cyberangriffen zu schützen und ihre Resilienz zu stärken.

4.3 Strategische Ziele

Damit das VBS die Erfüllung seiner Aufgaben sicherstellen und als die national zuständige und kompetente Stelle für Cyberdefence erfolgreich agieren kann, soll es folgende Ziele erreichen:

- **Antizipation und Früherkennung** von allgemeinen Herausforderungen und Entwicklungen im Cyberraum und den sich daraus ergebenden Bedrohungen, Chancen und Risiken (inkl. der Möglichkeiten der Digitalisierung zwecks kontinuierlicher Optimierung und Modernisierung), um sich dadurch agil darauf anpassen zu können.
- **Bedrohungen und Angriffen**, welche die Aufgabenerfüllung des VBS beeinträchtigen, nationale Auswirkungen haben oder nationale Interessen gefährden, vorbeugen[34], selbstständig und, wo erforderlich, im Verbund rechtzeitig und in allen Lagen frühzeitig erkennen, stören, verhindern und attribuieren.

---

33 Meldepflicht für Cybervorfälle: Die Schweiz kennt nur in einzelnen Sektoren Meldepflichten für Funktionsausfälle aber keine generelle Meldepflicht bei Cyberangriffen. Der Bundesrat hat daher basierend auf dem Bericht des NCSC (EFD) vom 11.12.2020 das EFD beauftragt, bis Ende 2021 eine Vernehmlassungsvorlage auszuarbeiten, welche die rechtlichen Grundlagen für eine Meldepflicht für kritische Infrastrukturen bei Cyberangriffen und bei der Entdeckung von Sicherheitslücken schafft. Auf Gesetzesstufe soll dabei eine zentrale Meldestelle bezeichnet und für alle Sektoren einheitlich bestimmt werden.

34 Vorsorgliche Massnahmen sind u. a. in den Bereichen Technologie, Prozesse sowie Personen zu treffen.

- Bereitstellung eines **Aus- und Weiterbildungsinstrumentariums** für die zivilen und militärischen Mitarbeitenden (Lohnbezüger) sowie für die Angehörigen der Miliz (Soldbezüger), um diese auf die sich entwickelnden Cyberherausforderungen vorzubereiten. Dies, wo nötig und gemäss Vereinbarung, zugunsten anderer Leistungsbezüger auf Stufe Bund, Kantone und Betreiber kritischer Infrastrukturen zur Verfügung stellen.
- In Belangen der Cybersicherheit basierend auf einem Risikomanagementansatz **resistent sein** und ein hohes Mass an **Resilienz erreichen.**
- Zum Zweck der Resistenz und der Resilienz das **Asset-Management** beherrschen, auf aktuellem, technischen Stand halten, die **Lieferketten** (inkl. ihre Sicherheit) kennen und durch die Reduktion der Abhängigkeiten von Dienstleistern und Lieferanten ein angemessenes Mass an **Autonomie** erreichen.
- Im Bereich Cyberdefence als Vorreiter und Vorbild auftreten und damit als attraktiver Arbeitgeber in Erscheinung treten.

4.4 Kernbereiche und Aufgaben des VBS

Die nachfolgende Abbildung 3 zeigt die Kernbereiche, in welchen das VBS tätig ist. Diese orientieren sich weitgehend an der Strukturierung der bisherigen Aufgaben (vgl. Kapitel 3.3). Das Cyberdefence-Dispositiv des VBS ist eingebettet in den rechtlichen und politischen Rahmen (Bereich [R]). In der Abbildung 3 erfasst sind zudem die externen Partner: Staaten, interne Organisationen, Leistungserbringer, Industriebasis, Unternehmen (Bereich [Z]). Diese Partnerschaften sind unerlässlich, da kein Akteur alleine die Herausforderungen im Cyberspace bewältigen kann.

Innerhalb der vier Kernbereiche nimmt das VBS verschiedene Aufgaben wahr. Nachfolgend wird einleitend der Kernbereich ausgeführt, bevor die dazugehörigen Aufgaben beschrieben werden.

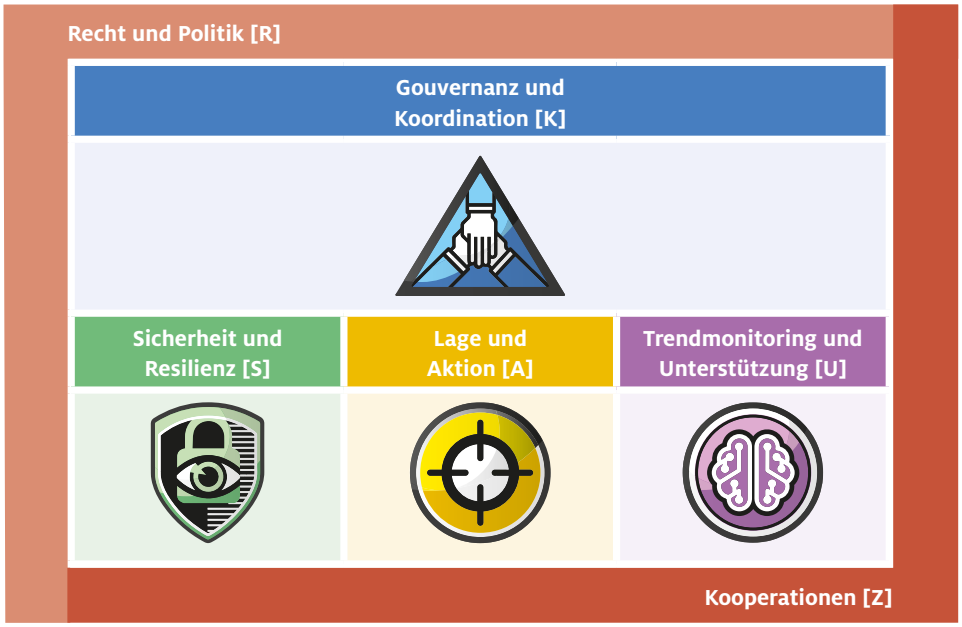
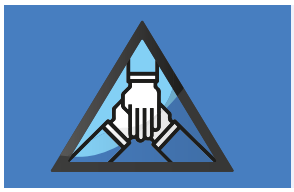


Abbildung 3 – Cyberdefence-Dispositiv des VBS



Gouvernanz und Koordination [K]:
Auf der strategischen Ebene jeder Verwaltungseinheit (VE) des VBS werden die Voraussetzungen für die Entwicklung und Nutzung aller notwendigen Ressourcen geschaffen. Der Fortschritt der Umsetzung wird überwacht und die Zusammenarbeit mit den Beteiligten koordiniert.

Aufgaben	Beschreibung
[K1] Policy, Management und Kontrolle	Die VE des VBS berücksichtigen die übergeordneten Strategien, Vorgaben und Standards. Gemäss den Informatiksicherheitsvorgaben des Bundes und den VBS-eigenen Vorgaben sollen die vorgesehenen Sicherheitsniveaus erreicht werden. Die Verwaltungseinheiten überprüfen die Umsetzung der Informationssicherheitsvorgaben auf allen Stufen, u. a. durch Audits und Reviews und die Bestimmung von Korrekturmassnahmen. Das GS-VBS steuert die Aktivitäten und überwacht den Fortschritt der Umsetzung gemäss der vorliegenden Strategie. Es übernimmt die Koordination mit den Partnern innerhalb und ausserhalb der Bundesverwaltung.
[K2] Kooperation und strategische Leitung	Die VE des VBS setzen die Strategien um. Sie schaffen Rahmenbedingungen für die Antizipation, frühzeitige Erkennung von Cyberrisiken und Verhinderung und Attribution von Cybervorfällen sowie deren Bewältigung. Wo sinnvoll, findet eine Koordination mit Partnern im In- und Ausland auf allen Stufen statt.
[K3] Organisationsentwicklung	Die VE erstellen eine Analyse der Herausforderungen im Cyberraum sowie eine Übersicht für die jeweiligen Stufen. Dazu werden die Ergebnisse aus den Bereichen [S] (Sicherheit und Resilienz), [A] (Lage und Aktion im Cyberraum) und [U] (Antizipation und Unterstützung) zusammengeführt. Diese Arbeiten bilden die Grundlagen für zeitgerechte Entscheidungen und Weiterentwicklungen der jeweiligen VE.

Tabelle 2 – Definition des Kernbereichs «Gouvernanz und Koordination» und seine Aufgaben

Sicherheit und Resilienz [S]:
Dieser Kernbereich strukturiert die Aufgaben, damit alle IKT-Systeme und -Infrastrukturen so organisiert und betrieben werden, dass die definierten Leistungen erbracht werden können. Damit soll erreicht werden, dass die VE des VBS ihre Aufgaben jederzeit und in allen Lagen erfüllen können. Diese reichen von der Risikoidentifikation und Risikominderung über die Überwachung und Störungserkennung bis hin zur Wiederherstellung der Dienste.

Aufgaben	Beschreibung
[S1] Identifizierung	Identifikation von geschäftskritischen Systemen (inklusive Management der Assets und Lieferketten), Daten und Funktionen. Damit bestimmen die VE, wie sie die unternehmenswichtigen Leistungen schützen und welche Vorkehrungen hinsichtlich der Risiken zu treffen sind.
[S2] Schutz	Angemessene Schutzmassnahmen sind zu entwickeln und zu implementieren; wo nötig, sind proprietäre Systeme zu entwickeln. Damit sollen Auswirkungen möglicher Cybersicherheitsvorfälle begrenzt und eingedämmt werden.
[S3] Detektion	Überwachung der eigenen IKT-Systeme, Erfassung und Analyse der Informationen über Anomalien sowie Identifikation von Cyberbedrohungen (inkl. Korrelation und Aggregation). Erkennung sicherheitsrelevanter Ereignisse.
[S4] Reaktion	Beschaffung und Analyse von Informationen über Cybervorfälle (inkl. Forensik First Level Support) und deren Handhabung.
[S5] Wiederherstellung	Die VE entwickeln geeignete Massnahmen zur Wiederherstellung der Sicherheit und der Dienste, die im Rahmen eines Vorfalls beeinträchtigt werden. Im Minimum geht es darum, so rasch wie möglich einen vereinbarten Betrieb (gem. BCP[35]) wieder zu etablieren, damit die VE ihre Aufträge erfüllen können.

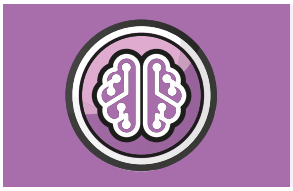
Tabelle 3 – Definition des Kernbereichs «Sicherheit und Resilienz» und seine Aufgaben

35 Business Continuity Planning.

Lage und Aktion im Cyberraum [A]:
Dieser Kernbereich erfasst alle Aufgaben, die zur Antizipation, frühzeitigen Erkennung, Verhinderung und Attribution von sicherheitspolitisch relevanten Cyberangriffen nötig sind. Er umfasst auch die Bedrohungsbeurteilung und Darstellung der Lage. Hinzu kommen die nachrichtendienstliche Informationsbeschaffung und die Durchführung von Cyberoperationen (Gegenmassnahmen im Rahmen der Cyberabwehr wie auch die aktive Wirkung im Cyberraum in konfliktähnlichen Lagen).

Aufgaben	Beschreibung
[A1] Cyberlage und Attribution	Es wird eine umfassende Bedrohungsbeurteilung und Lagedarstellung der staatlichen und nichtstaatlichen sicherheitspolitisch relevanten Cybervorfälle auf Schweizer Interessen erstellt. Dazu gehört die Attribution (Täteridentifikation), die sich aus der Analyse technischer Eigenschaften eines Cybervorfalls und dem geopolitischen Kontext ergibt. Das nachrichtendienstliche Spektrum zur Informationsbeschaffung wird genutzt.
[A2] Defensive Cybergegenmassnahmen	Gesamtheit der defensiven Massnahmen bei einem Angriff gegen die eigenen IKT-Systeme und -Infrastrukturen. Beinhaltet (gem. NDG und MG) das genehmigungspflichtige Eindringen in Computersysteme und Computernetzwerke, die für solche Angriffe verwendet werden, um den Zugang zu Informationen zu stören, zu verhindern oder zu verlangsamen.
[A3] Cyberdefence kritischer Infrastrukturen	Gesamtheit der (aktiven und passiven) Cyberabwehrmassnahmen (gem. NDG; wo nötig, mit subsidiärer Unterstützung der Armee) zugunsten der Betreiber kritischer Infrastrukturen, welche Cyberangriffe erleiden.
[A4] Cyberoperationen	Gesamtheit aller offensiven Aktionen gemäss NDG und MG (zus. gem. Kriegsvölkerrecht in konfliktähnlichen Lagen), die vom NDB (in allen Lagen) oder von der Armee zur Unterstützung einer militärischen Operation und zur Beschaffung relevanter Nachrichten erbracht werden.

Tabelle 4 – Definition des Kernbereichs «Lage und Aktion im Cyberraum» und seine Aufgaben



Trendmonitoring und Unterstützung [U]:
Die für den Aufbau der technischen, fachlichen und personellen Mittel der VE des VBS erforderlichen Schlüsselkompetenzen werden aufgebaut und zur Verfügung gestellt. Der Wissensaufbau und -transfer erfolgt in Zusammenarbeit mit den Hochschulen und der Industrie.

Aufgaben	Beschreibung
[U1] Technologie- und Markt-Monitoring	Verfolgung der technologischen Entwicklung im digitalen Bereich, um Trends zu erkennen und daraus zeitgerecht Konsequenzen für die Organisations- und Mittelentwicklung im VBS abzuleiten.
[U2] Forschung, Entwicklung und Innovation	Gesamtheit der Forschungs- und Innovationsaktivitäten (wo erforderlich, u. a. mit Industrie, Hochschulen und ausländischen Institutionen), um sich mit neuen technischen Lösungen und Abwehrverfahren vertraut zu machen. Diese können zwecks angemessener Autonomie oder auch für die Sicherheitsprüfung von Systemen entwickelt werden.
[U3] Personal und Kompetenz	Sicherstellung – qualitativ und quantitativ – der erforderlichen Personalkompetenzen zugunsten sämtlicher Bereiche des VBS. Diese erfolgt in enger Zusammenarbeit mit den Hochschulen und Berufs- / Fachverbänden und umfasst die Stärkung der Interoperabilität des VBS mit seinen Partnern.
[U4] Beschaffung und Bewirtschaftung von Leistungen und Systemen	Die VE beschaffen und verwalten sichere Produkte und Dienstleistungen zugunsten der Leistungsbezüger. Dafür werden Vertragsbedingungen definiert, welche die Cybersicherheit in den Mittelpunkt stellen sowie ein Lieferketten- und Lebenszyklusmanagement ermöglichen.
[U5] Beratung	Unterstützung der Fach-, Aufsichts- und Regulierungsbehörden bei der Analyse von Cyberrisiken. Unterstützung der Betreiber kritischer Infrastrukturen zur Verbesserung ihrer Resilienz.

Tabelle 5 – Definition des Kernbereichs «Trendmonitoring und Unterstützung» und seine Aufgaben

4.5 Massnahmen zur Umsetzung der Strategie

Um den in Kapitel 2 abgeleiteten Erkenntnissen Rechnung zu tragen und den kommenden Herausforderungen und Trends gerecht zu werden, sollen bis Ende 2024 die unten aufgelisteten Massnahmen umgesetzt werden. Die Umsetzung der Massnahmen und Ziele erfolgt im Rahmen der bestehenden Gesamtressourcen des VBS, des Rechtsrahmens und der NCS-Ziele.

	Massnahmenfelder	Ziele
1	**VBS-interne Vorgaben [K1]**	Die Anzahl Vorgaben vereinfachen, aktualisieren und zukunftsfähig machen.
2	**ISMS VBS [K1]**	Das aktuelle ISMS zu einem praxisnahen, bedarfsgerechten und einsatztauglichen System weiterentwickeln.
3	**Messbarkeit [K1]**	Den genauen Zustand des VBS-Dispositivs systematisch und dynamisch beurteilen.
4	**Internationale Zusammenarbeit [K2]**	Stärkung (im Verbund mit den nationalen Partnern) der eigenen Fähigkeiten und Kompetenzen durch internationale Kooperation.
5	**Nationale Zusammenarbeit [K2]**	Beitrag zur Stärkung des Schutz des Landes vor Cyberrisiken, insbesondere durch den Ausbau der Zusammenarbeit mit den systemkritischen Leistungserbringern.
6	**Kommando Cyber [K3]**	Weiterentwicklung der FUB von einer Unterstützungsorganisation zu einem einsatzorientierten militärischen Kommando.
7	**Vorausschau im digitalen Raum [K3]**	Strategische Herausforderungen im Cyberbereich frühzeitig und systematisch erkennen.
8	**Security Operation [S4]**	Stärkung der Fähigkeit, mehrere komplexe, gleichzeitige und andauernde Cybervorfälle zu bewältigen.
9	**Cyberlage [A1]**	Die Beurteilung aller sicherheitspolitisch relevanten Cyberbedrohungen vornehmen und diese in Lagedarstellungen abbilden.
10	**Attribution [A1]**	Stärkung der Analyse technischer Eigenschaften von Cybervorfällen, der Beurteilung des internationalen Kontextes und der Nutzung des gesamten nachrichtendienstlichen Spektrums zur Informationsbeschaffung.
11	**Beobachtung der Beeinflussung im Cyberraum [A1]**	Ausländische Beeinflussungskampagnen im Cyberraum gegen sicherheitspolitisch bedeutsame Interessen der Schweiz und der Armee entdecken, analysieren und den zuständigen Stellen melden.
12	**Cyber Threat Intelligence [A1]**	Ausbau der Beschaffung und Auswertung von Informationen über Cyberangriffe.
13	**Cyber ND [A1]**	Stärkung des nationalen und internationalen Netzes zur Beschaffung von Informationen.
14	**Joint Cyber Technical Analysis Center (JCTAC) [A1]**	Stärkung der technischen Analysefähigkeiten bezüglich Cyberbedrohungen und -ereignissen.
15	**Deep Forensic [A2]**	Bereitstellung einer fortgeschrittenen Fähigkeit zur logischen und physischen Analyse und Reverse-Engineering von Angriffsvektoren.
16	**Operative Data Science [A2]**	Fähigkeit[36], mit den wachsenden Massendaten automatisch umzugehen und Phänomene und Bedrohungen zu erkennen und Handlungsempfehlungen abzuleiten, welche mit manuellen Methoden unentdeckt bleiben würden.

36 Diese Massnahme hat hauptsächlich mit dem Cyberbereich zu tun, ist aber nicht auf dieses Thema eingeschränkt zu verstehen und ist mit analogen Aktivitäten in den anderen Ämtern des VBS und der Bundesverwaltung zu koordinieren.

	Massnahmenfelder	Ziele
17	**OIC MELANI+ [A3]**	Bei Cyberangriffen auf Betreiber kritischer Infrastrukturen subsidiär unterstützen. Angriffe besser antizipieren. Weiterentwicklung von Kompetenzen und Durchhaltefähigkeit für diese Aufgaben.
18	**Cyberoperationen [A4]**	Einen spannungsähnlichen oder einen zeitlich begrenzten, konfliktähnlichen Zustand mit mehreren Operationen flexibel und parallel behandeln.
19	**CYD-Campus+ [U1]**	Ständige Weiterentwicklung des CYD-Campus auf das Niveau des nationalen technischen Kompetenznetzwerks für Cyberdefence mit Hochschulen und Industrie.
20	**Forschung und Innovation [U2]**	Mittels wissenschaftlicher Erkenntnisse neue Bedrohungen identifizieren und innovative Lösungen zugunsten der operativen Einheiten zur Verfügung stellen.
21	**Education und Training [U3]**	Das Cyberpersonal entlang seiner Einsatzdauer im Bereich Cybersicherheit auf die steten Veränderungen des Cyberumfeldes vorbereiten.
22	**Berufliche Grundausbildung [U3]**	Dem wachsenden Mangel an Basis-IKT-Sicherheitsfachkräften entgegenwirken.
23	**Cybertalente für die Armee [U3]**	Talente möglichst früh erkennen und fördern.
24	**Cyberfellowships [U3]**	Weiterentwicklung des CYD-Fellowship-Programms, um wissenschaftliche Cybertalente möglichst früh zu erkennen und zu fördern sowie Schaffung eines Frührekrutierungsdispositivs.
25	**Cyber-MA 4.0 [U3]**	Etablierung eines systemischen Transformationsprozesses zur Befähigung des VBS-Personals entlang seiner Einsatzdauer für die Herausforderungen der Digitalisierung.
26	**Cyberkaderlehrgang [U3]**	Bereitstellung von neuen professionellen Kaderkursen und Laufbahnen für das Berufspersonal (ziv. / mil., evtl. für bestimmte ausländische Teilnehmende).
27	**Cyberzeitmilitär [U3]**	Junge Talente früh in der militärischen und fachlichen Karriere fördern und für Berufsorganisationen gewinnen.
28	**Cybersichere Rüstungsbeschaffung [U4]**	Stärkung der Bewirtschaftung der Cybersicherheit von Produkten und Leistungen entlang der Lieferketten und Lebenszyklen.
29	**Cybersichere logistische Prozesse [U4]**	Stärkung des Bewirtschaftungsprozesses des Armeematerials, wenn dieses an die Truppe oder Dritte (z. B. für Wartungszwecke) abgegeben wird.
30	**Resilienz kritischer Infrastrukturen gegenüber Cyberangriffen [U5]**	Unterstützung der Betreiber kritischer Infrastrukturen bei der systematischen Umsetzung der vereinbarten Massnahmen zur Verbesserung ihrer Resilienz.

Tabelle 6 – Massnahmen zur Umsetzung der Strategie

4.5.1 Aufgaben und Strukturen der VE des VBS

Zur Erfüllung der vorgängig aufgeführten Aufgaben, der Aufgaben des VBS im Rahmen der NCS und zur Unterstützung des NCSC verfügt das VBS über folgende Strukturen.

- **Generalsekretariat VBS**: Das GS-VBS trägt (gem. Organisationsverordnung vom 7. März 2003[37] für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport OV-VBS und der Verordnung vom 21. November 2018[38] über die militärische Sicherheit VMS) die Gesamtverantwortung für die Sicherheit des Departements; es stellt die Aufgabe des Informatiksicherheitsbeauftragten des Departementes sicher (ISBD; gem. Art. 13[39] CyRV). Das GS-VBS vertritt das Departement in der Kerngruppe Cybersicherheit. Mit der Abteilung Digitalisierung und Cybersicherheit stellt es die Gesamtkoordination der Aktivitäten der Verwaltungseinheiten im VBS, den Überblick über die Herausforderungen und die strategische Unterstützung der Departementsführung in Krisenlagen sicher. Zudem schafft es günstige Voraussetzungen für die Integration des Cyberbereiches in den grossen Übungen zur Erhöhung der Interoperabilität innerhalb des VBS und mit den externen Partnern.
- **Gruppe Verteidigung (Gruppe V)**
  - Der **Armeestab** (A Stab) plant Vorhaben und Beschaffungen; zudem ist er für die Koordination der Doktrin aller Operationssphären zuständig.
  - Das **Kommando Operationen** (Kdo Op) stellt[40] mit Hilfe der FUB die Integration des Cyberbereichs in die militärischen Operationen sicher. Für die Cybersicherheit bei der Truppe verfügt es im Cyberbereich u. a. über die Militärpolizei (Überprüfung der Sicherheitsmassnahmen bei bei einem erkannten Vorfall und Deliktbekämpfung) und die im GS angesiedelte Militärjustiz (mit dem Oberauditor).
  - Die **Logistikbasis der Armee** (LBA) koordiniert die Entwicklung und den Betrieb der IKT-Mittel der Logistik inklusive deren Sicherheit.
  - Die **Führungsunterstützungsbasis** (FUB, ab 1. Januar 2024 als Kommando Cyber vorgesehen) stellt die hochsicheren IKT-Leistungen der Gruppe V sicher und ist IKT-Leistungserbringer[41] zugunsten anderer Leistungsbezüger wie z. B. des Nachrichtendienstes des Bundes oder des Bundesamts für Bevölkerungsschutz. Der Chef FUB verantwortet die Operationssphäre Cyber und den elektromagnetischen Raum in der Gruppe V sowie in der Armee. Der Chef Kommando Operationen ist der Auftraggeber von Aktionen im Cyber- und elektromagnetischen Raum von militärischen Operationen und Einsätzen der Armee.
  - Das **Kommando Ausbildung** (Kdo Ausb) stellt die Integration des Cyberbereichs und dessen Inhalte in Schulen, Kursen und Lehrgängen sicher.
  - Die Intensivierung der Zusammenarbeit der Cyberdefence mit den Bereichen der IKT-Gouvernanz in Armee, Verwaltung und bei Partnern zur Schaffung günstiger Voraussetzungen (Führung, Lage, Projekte, Prozesse, Daten, IKT-Services) wird im Rahmen des Projekts Kommando Cyber betrachtet.

---

37 SR **172.214.1**
38 SR **513.61**
39 Die Verwaltungseinheiten stellen selber einen Informatiksicherheitsbeauftragten (ISBO) ihrer Einheit (gem. CyRV, Art. 14, Ziff. 1) zur Verfügung.
40 Das Kdo Op koordiniert sämtliche Aktionen in allen Wirkungsräumen, verfolgt diese und stimmt sie aufeinander ab, um die Gesamtsicht zu wahren.
41 Zu berücksichtigen ist die laufende Trennung zwischen den IKT-Basis- und -Spezialleistungen.

- **Nachrichtendienst des Bundes (NDB)**: Der NDB ist ein sicherheitspolitisches Instrument, das gestützt auf das NDG Informationen beschafft und bearbeitet, um Bedrohungen der inneren und äusseren Sicherheit frühzeitig zu erkennen und zu verhindern. Im Mittelpunkt der nachrichtendienstlichen Aufgaben stehen die Sensibilisierung und Antizipation von Cyberangriffen auf Schweizer Interessen (z. B. kritische Infrastrukturen). Der NDB ist für die umfassende Beurteilung der Cyberbedrohungen zuständig. Die Beurteilungen und Lagedarstellungen werden dem Bundesrat, den Departementen und der militärischen Führung mit Beiträgen (z. B. Analysen) und mit einem Lageradar zur Verfügung gestellt. Zu den Kernaufgaben des NDB gehört die Attribution, d. h. die Identifikation eines Cyberangriffs, die Zuordnung des Angriffs zum Urheber.[42] Dazu beschafft der NDB Informationen aus öffentlichen und nichtöffentlichen Quellen, führt vertiefte Akteur- und Umfeldanalysen durch und nutzt technische Instrumente sowie Fernmeldeüberwachung. Der NDB kann unter bestimmten Umständen zusammen mit der FUB offensive Cyberoperationen durchführen. Der NDB ist in der Kerngruppe Sicherheit sowie der Kerngruppe Cyber vertreten. Das Operations- und Informationszentrum der Melde- und Analysestelle Informationssicherung unterstützt die Betreiber der kritischen Infrastrukturen subsidiär.
- **Bundesamt für Rüstung (armasuisse)**: Das Amt ist innerhalb des Departements für Beschaffungen von Cyberprodukten und Leistungen sowie für die Forschung zuständig. Der CYD-Campus bei armasuisse Wissenschaft und Technologie stellt die Zusammenarbeit mit der Wissenschaft (insbesondere mit den beiden ETH und den dort angesiedelten Aussenstandorten) und der Wirtschaft sicher. Unter anderem setzt er sich für die Entschlackung und Vereinfachung bestehender IKT-Services, den Abbau von Legacy Systemen und den Bau von einfach handhabbaren Systemen mit hohem Eigenschutz ein. Der CYD-Campus erfüllt Unterstützungsaufgaben zugunsten des NCSC gemäss der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken.
  Weiter beschäftigt sich der CYD-Campus mit der Rekrutierung von Talenten, der Ausbildung, Weiterentwicklung und Unterstützung von Studenten mit hohem Potenzial.
- **Bundesamt für Bevölkerungsschutz (BABS)**: Das BABS verantwortet die Koordination und Umsetzung der nationalen Strategie zum Schutz kritischer Infrastrukturen. Durch die NCS ist das BABS mit weiteren Aufgaben im Bereich Risiko- und Verwundbarkeitsanalysen sowie Resilienz-Management kritischer Infrastrukturen (KI) betraut. Dies betrifft insbesondere den Bereich der Beratung von KI-Betreibern sowie der zuständigen Aufsichts- und Regulierungsbehörden zur Verbesserung der (Cyber-)Resilienz von kritischen Infrastrukturen.

42 Siehe Massnahme 22 der NCS und seines Umsetzungsplanes.

5 Umsetzung der Strategie Cyber VBS

5.1 Strategie als Prozess

Die gemeinsame Veränderung und Ausrichtung braucht eine klare Strategie, festgelegte Meilensteine und Vorgaben, welche Ziele erreicht werden sollen. Die Prozesse müssen von der Führung angestossen und gesteuert werden. Eine wichtige Frage aus dem Blickwinkel des Strategiemanagements lautet: Was ist heute zu tun, um der Zukunft wirkungsvoll zu begegnen?

Entscheidend sind dabei nicht nur Visionen, sondern vor allem ihre Verwirklichung. Das Ziel ist, eine hohe Wirksamkeit in allen Aktivitäten zu erreichen. Mit der vorliegenden Strategie ist der Prozess nicht beendet. Dieser unterliegt einer ständigen Weiterentwicklung. Die Umsetzungsführung der Strategie wird auf Stufe der Konferenz «Cyberdefence VBS» sichergestellt.

5.2 Gouvernanz: dezentrale, koordinierte Umsetzung

Für die Umsetzung der Massnahmen innerhalb des VBS sind die einzelnen Ämter, bzw. die Gruppe V verantwortlich. Es gilt das AKV-Prinzip (Prinzip der Kongruenz von Aufgabe, Kompetenz und Verantwortung). Nach dem Kongruenzprinzip wird eine Verwaltungseinheit zusammen mit der Übergabe einer Aufgabe mit den nötigen Kompetenzen ausgestattet, damit die zuständige Stelle die Verantwortung übernehmen kann. Das GS-VBS (Bereich DCS) überprüft die Zielerreichung im Auftrag der Chefin VBS, koordiniert die Arbeiten und stellt die institutionelle Zusammenarbeit mit den Partnern sicher.

A

Anhang 1 – Verzeichnisse

Abkürzungsverzeichnis

APCD	Aktionsplan Cyberdefence VBS
BABS	Bundesamt für Bevölkerungsschutz
CAS	Certificate of Advanced Studies
CYD	Cyberdefence
CyRV	Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung
DAS	Diploma of Advanced Studies
DCS	Digitalisierung und Cybersicherheit
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
ENISA	European Union Agency for Cybersecurity
EFD	Eidgenössisches Finanzdepartement
EFK	Eidgenössische Finanzkontrolle
ETHZ	Eidgenössische Technische Hochschule Zürich
FUB	Führungsunterstützungsbasis
Gruppe V	Gruppe Verteidigung
GS-VBS	Generalsekretariat des VBS
IKT	Informations- und Kommunikationstechnologie
ISMS	Information Security Management System
ISO	International Organization for Standardization
KI-Betreiber	Betreiber kritischer Infrastrukturen
OIC MELANI	Operation Information Center der Melde- und Analysestelle Informationssicherung
MG	Bundesgesetz über die Armee und die Militärverwaltung (Militärgesetz)
MIG	Bundesgesetz über die militärischen Informationssysteme
NATO	North Atlantic Treaty Organization
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken
NDB	Nachrichtendienst des Bundes
NDG	Bundesgesetz über den Nachrichtendienst (Nachrichtendienstgesetz)
OIC	Operation Information Center
SVS	Sicherheitsverbund Schweiz
VE-VBS	Verwaltungseinheit des VBS

Liste der Abbildungen

Liste der Tabellen