Die Strategie Cyber VBS

kurz gefasst

März 2021

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Zusammenfassung der Strategie Cyber VBS

So schützt die Schweiz im Cyberraum

Der Bundesrat tritt den Cyberrisiken aktiv entgegen und ergreift die nötigen Massnahmen, um die Sicherheit des Landes gegenüber den Bedrohungen aus dem Cyberraum zu wahren.

Seit 2012 verfügt die Schweiz über eine **Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken** (NCS), um mit den Chancen und Herausforderungen im Cyberraum umzugehen. 2018 wurde die Strategie mit zusätzlichen Massnahmen erweitert und die Wichtigkeit der Zusammenarbeit zwischen dem Bund, den Kantonen, Partnern der Wirtschaft sowie den Hochschulen betont. Die Strategie berücksichtigt die zunehmende Digitalisierung und Vernetzung der Gesellschaft sowie der Verwaltung. Verantwortlicher auf Stufe Bund ist der Delegierte des Bundes für Cybersicherheit im Nationalen Zentrum für Cybersicherheit (National Cyber Security Centre – NCSC) innerhalb des Eidgenössischen Finanzdepartements (EFD).

*Unter **Cyberraum** versteht man einen mit IKT von Menschen erschaffenen, virtuellen Raum. Er dient der digitalen Vernetzung und Verarbeitung von Daten sowie der Erfassung und Steuerung von Systemen und Prozessen.*

*Die Massnahmen zum Schutz vor Cyberrisiken sind (gemäss Cyberrisikoverordnung, Art. 6) in folgende Bereiche unterteilt: Cybersicherheit, Cyberdefence und Cyberkriminalität. Im vorliegenden Text wurde, um die sprachliche Übereinstimmung zu garantieren, **Cyberdefence** als etablierter Begriff übernommen.*

Wer wird geschützt?

Einerseits zentral ist der Schutz der Bürgerinnen und Bürger vor Kriminalität im Cyberraum. Anderseits müssen die kritischen Infrastrukturen vor provozierten, gewollten und unfreiwilligen Störungen und Beeinträchtigungen geschützt werden, welche die Bevölkerung, Wirtschaft und Verwaltung treffen können. Bei grösseren Cyberangriffen, etwa durch böswillige Absichten eines Staates, wird auf die Cyberverteidigung, genannt **Cyberdefence**, zurückgegriffen. Sie umfasst verschiedene Mittel des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) und schützt die Schweiz, die Bevölkerung und deren Lebensgrundlagen vor Cyberbedrohungen. Auch bei grösseren, nicht böswillig verursachten Cyberstörungen kann die Cyberdefence unterstützend zum Einsatz kommen.

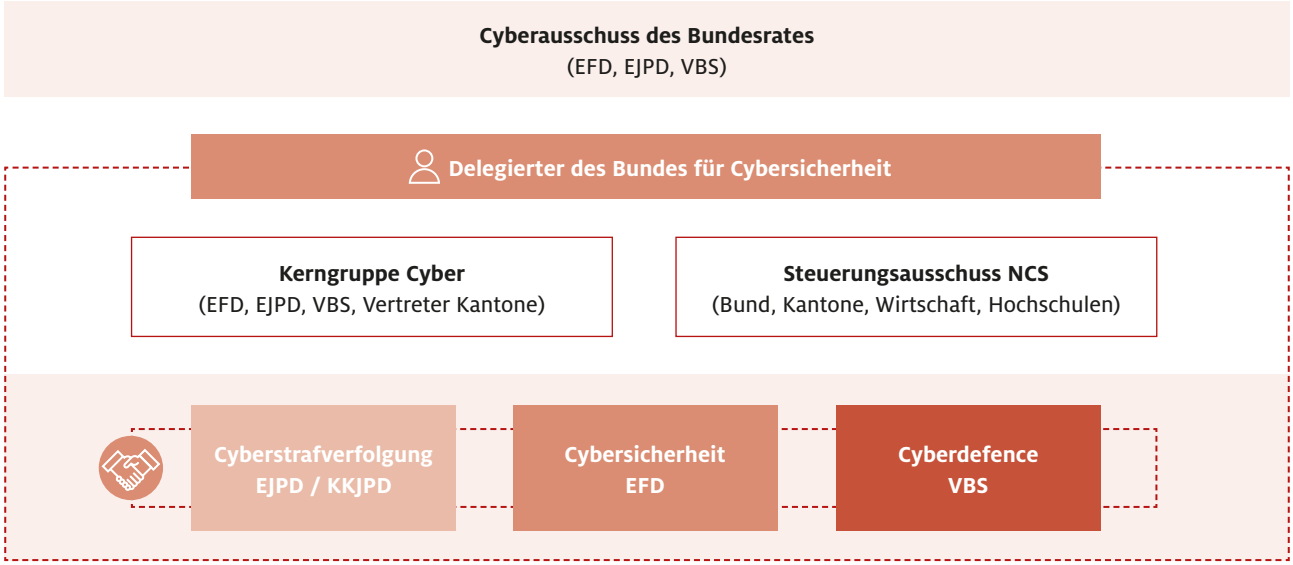


Abbildung 1 – Verantwortlichkeiten für Cybersicherheit in der Bundesverwaltung

So schützt das VBS im Cyberraum: strategisch, im Verbund, permanent

Bisher: von 2017 bis 2020

Der **Aktionsplan Cyberdefence VBS (APCD)** aus dem Jahr 2017 definierte als Teil der NCS spezifisch die Aufgaben, Kompetenzen und Prozesse der Verwaltungseinheiten des VBS im Umgang mit Cyberdefence. Die darin festgelegten Massnahmen wurden bis Ende 2020 weitestgehend umgesetzt.

Das VBS hat mit der **Koordination von Kompetenzen und Kapazitäten** an Effektivität gewonnen. Die Zusammenarbeit zwischen den Departementen konnte verbessert werden. Das VBS arbeitet mit den **Kantonen, der Wirtschaft und den Hochschulen** zusammen sowie bei Bedarf mit internationalen Partnern. Das VBS verfügt heute über Fähigkeiten, um hochstehenden Schutz und Verteidigungsleistungen im Cyberraum zu erbringen und kann auf ein zuverlässiges Netzwerk im In- und Ausland zurückgreifen.

Heute: von 2021 bis 2024

Die **Strategie Cyber VBS** baut auf den Erkenntnissen des Aktionsplans Cyberdefence auf. Sie stellt sicher, dass das VBS und seine Verwaltungseinheiten gezielt und ganzheitlich auf die sich ständig ändernden Anforderungen ausgerichtet sind.

Die **Strategie Cyber VBS** reflektiert in einem ersten Schritt die Bedrohungslage, die Herausforderungen und Trends im Cyberraum weltweit.[1] Es werden Entwicklungen beschrieben, die in nächster Zeit in den Bereichen Technologie, Politik, Wirtschaft und Personal erwartet werden.

So werden zum Beispiel böswillige Handlungen vermehrt automatisiert und gestützt auf künstliche Intelligenz ausgeführt. Unzureichende Sicherheitskonfigurationen von Systemen verschiedener Generationen (Legacy Systems) werden systematisch ausgenutzt. Der Missbrauch des Cyberraums für Manipulation dürfte mit der wachsenden Bedeutung von sozialen Medien und der starken digitalen Vernetzung weiter zunehmen.

1 Siehe Jahresbericht Nachrichtendienst des Bundes NDB: «Sicherheit Schweiz 2020»

Die Strategie Cyber VBS präsentiert eine **IST-Analyse**. Diese zeigt auf, wie die Aufgaben und Massnahmen aus dem APCD, dem Vorgänger der Strategie, bis heute umgesetzt werden. Dazu gehören beispielsweise die Weiterentwicklung des Cyberlehrgangs der Rekrutenschule sowie der Cyberdefence-Campus der armasuisse. Ebenso beteiligt sich die Schweiz weiterhin an internationalen Cyberübungen.

Der Abgleich der Bedrohungen, Herausforderungen und Trends mit dem IST-Zustand ermöglichen es, künftiges Entwicklungspotenzial zu identifizieren. Die daraus gewonnenen Erkenntnisse dienen als Ausgangspunkt für die Formulierung der Ziele der Strategie Cyber VBS. Diese hält fest, wer im VBS welche Aufgaben wahrnimmt und wahrnehmen wird. Die Strategie Cyber VBS konzentriert sich auf den Bereich Cyberdefence. Die übergeordnete **Nationale Strategie NCS** und weitere Referenzdokumente decken weitere Aspekte der Cybersicherheit ab.

*Unter **Bedrohungslage** versteht man böswillige Handlungen durch staatliche und nichtstaatliche Akteure, sei es, um sich zu bereichern oder politische Interessen durchzusetzen. Dazu kann Spionage, Sabotage oder gezielte Desinformation / Destabilisierung eingesetzt werden.*

***Herausforderungen:** Gemeint sind die technologischen Entwicklungen, Abhängigkeiten und die Machtpolitik. Dazu gehört auch die Knappheit der natürlichen Ressourcen – Insbesondere seltene Erden oder die Stromversorgung – sowie der Ausbildungsbedarf und die Engpässe bei den Fachkräften.*

***Resilienz:** die Fähigkeit eines Systems, einer Organisation oder einer Gesellschaft, Störungen zu widerstehen und die Funktionsfähigkeit möglichst zu erhalten, respektive rasch wieder zu erlangen.*

Strategie Cyber VBS

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.

Die 6 strategischen Ziele

Die Steuerung der Umsetzung der *Strategie Cyber VBS* erfolgt im Rahmen der Konferenz «Cyberdefence VBS» unter der Leitung des Generalsekretärs VBS. Das VBS will folgende Ziele realisieren:

1. **Das VBS kennt die Herausforderungen und Entwicklungen im Cyberraum.** Es versteht die sich daraus ergebenden Bedrohungen, Chancen und Risiken und passt sich laufend an, um diese zu bewältigen.
2. **Das VBS ist fähig, Bedrohungen und Angriffen vorzubeugen**, welche Schaden anrichten, nationale Auswirkungen haben oder nationale Interessen gefährden.[2] Das VBS kann rechtzeitig und in allen Situationen Bedrohungen und Angriffe frühzeitig erkennen, stören oder verhindern.
3. **Das VBS bietet Aus- und Weiterbildungen** für die zivilen und militärischen Mitarbeitenden sowie für die Angehörigen der Miliz an, um diese auf Cyberherausforderungen vorzubereiten.
4. Das VBS **minimiert** die **Anfälligkeit für Cyberrisiken** und ist resistent. Im Ereignisfall oder in der Krise stellt es möglichst rasch die grundlegenden Funktionen wieder her, kann seine Aufgaben erfüllen und ist resilient.
5. Das VBS hält Hardware, Software und Netzwerke auf dem aktuellen technischen Stand. Es sorgt für den zuverlässigen Betrieb und dafür, dass immer das nötige Material vorhanden ist. Das VBS ist möglichst unabhängig von Dienstleistern und Lieferanten und erhöht somit seine **Autonomie**.
6. Das VBS positioniert sich im Bereich Cyberdefence als **Vorreiter und Vorbild** und als **attraktiver Arbeitgeber**.

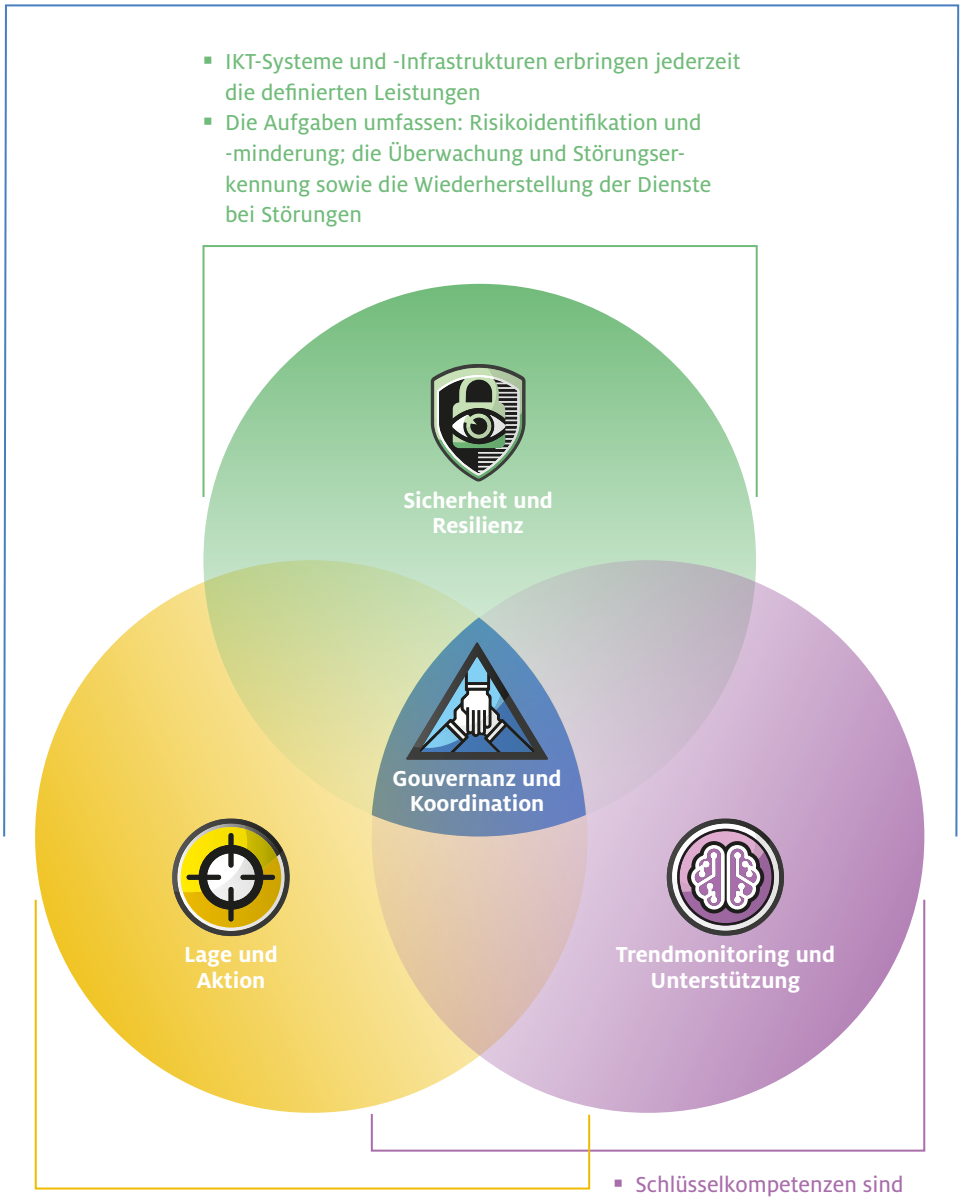
Resistenz: *wenn viele Schutzmassnahmen und möglichst wenig Schwachstellen vorhanden sind und der Schutz lange gewährleisten werden kann.*

2 Vorsorgliche Massnahmen sind u. a. in den Bereichen Technologie, Prozesse sowie Personal zu treffen.

Cyberdefence VBS: vier Hauptbereiche

Die Strategie Cyber VBS unterteilt die zu treffenden Massnahmen in vier Themenbereiche. Diese umfassen: Lage und Aktion; Sicherheit und Resilienz; Trendmonitoring und Unterstützung. Die Gouvernanz und Koordination bildet das vierte, verbindende Element. Jeder Departementsbereich unterteilt auch seine eigenen Aktionen in diese Themenbereiche.

- Voraussetzungen schaffen für die Entwicklung und Nutzung aller notwendigen Ressourcen
- Den Fortschritt der Umsetzung überwachen und die Zusammenarbeit mit den Beteiligten koordinieren



- Alles ist vorhanden für die Antizipation, frühzeitige Erkennung, Verhinderung und Attribution von Cyberangriffen, die sicherheitspolitisch relevant sind
- Die Lage darstellen und Bedrohungen beurteilen
- Für die nachrichtendienstliche Informationsbeschaffung sorgen und Cyberoperationen durchführen

- Schlüsselkompetenzen sind vorhanden für den Aufbau der technischen, fachlichen und personellen Mittel
- Der Wissensaufbau und -transfer erfolgt in Zusammenarbeit mit den Hochschulen und der Industrie

Kernbereiche und Aufgaben des VBS

Gouvernanz und Koordination
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.

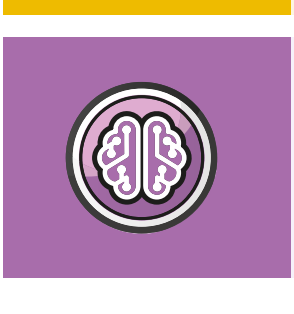
Beispiel: *Organisationsentwicklung: Die Departementsbereiche erstellen eine Analyse der Herausforderungen im Cyberraum sowie eine Übersicht für die jeweiligen Stufen; wo nötig, erfolgen zeitgerechte Entscheidungen und Weiterentwicklungen aufgrund der Analysen.*

Sicherheit und Resilienz
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.

Beispiel: *Massnahmen entwickeln zur Wiederherstellung von Systemen nach einem Vorfall.*

Lage und Aktion
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).

Beispiel: *Defensive Cybergegenmassnahmen bei einem Angriff durchführen können.*



Trendmonitoring und Unterstützung
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.

Beispiel: *Forschung, Entwicklung und Innovation: technisch, fachlich und personell up to date sein.*

Handlungsgrundsätze

Die Stärkung der Cybersicherheit der Schweiz ist eine Priorität des VBS. Für die Umsetzung der Strategie wurden deshalb folgende Handlungsgrundsätze formuliert:

Subsidiarität: Die im VBS vorhandenen Cyberkompetenzen können eingesetzt werden, um zivile Akteure bei möglichen Ereignissen zu unterstützen, wenn die gesetzlichen Vorgaben gegeben sind. Dafür muss laufend die Zusammenarbeit geübt und gestärkt werden, zum Beispiel durch Wissenstransfer und Übungen.

Institutionelle Zusammenarbeit: Das VBS bringt seine Mittel in die Zusammenarbeit mit den anderen sicherheitspolitischen Partnern in der Schweiz ein. Die Zusammenarbeit erfolgt mit Kantonen, Gemeinden, Partnern aus der Wirtschaft, der Gesellschaft, der Wissenschaft und internationalen Partnern. Sie ist in der Cyberrisikenverordnung des Bundes geregelt (CyRV).[3] Der Delegierte für Cybersicherheit des Bundes koordiniert die folgenden drei Bereiche: Cybersicherheit, Cyberstrafverfolgung und Cyberdefence (gemäss der Nationalen Cyberstrategie NCS).

Internationale Zusammenarbeit: Diese erfolgt bilateral und multilateral mit anderen Bundesstellen (Eidgenössisches Departement für auswärtige Angelegenheiten, Eidgenössisches Finanzdepartement, Eidgenössisches Justiz- und Polizeidepartement) und dient vor allem der Antizipation und Früherkennung von Bedrohungen und Herausforderungen im Cyberraum.

Aufgeschlossenheit / Offenheit: Das VBS unterstützt weitere Partner mit seinen Kompetenzen.

Kommando Cyber der Armee: Gemäss Auftrag des Bundesrats soll die heutige Führungsunterstützungsbasis der Armee (FUB) auf Anfang 2024 in ein Kommando Cyber weiterentwickelt werden; die Einsatzfähigkeit der Armee im Cyberraum soll kontinuierlich verbessert werden.

Die Strategie Cyber VBS dient dem bestmöglichen Schutz der Schweiz im Cyberraum. Dieser Schutz wird mit den Verbundspartnern gemeinsam wahrgenommen und dient der Minimierung der Verletzlichkeit der Schweiz im Cyberraum.

Durch die kontinuierliche Zusammenarbeit der VBS-internen und auch externen Partner im Alltag können Ereignis- oder Krisenfälle effizienter bewältigt werden. Die verschiedenen Prozesse sind eingeübt, die Aufgaben bekannt und das Netzwerk eingespielt. Somit garantiert die Strategie VBS durch die konkrete Massnahmenplanung nicht nur deren professionelle Umsetzung, sondern stärkt auch die gemeinsame Vorbereitung auf den Ernstfall und dessen Bewältigung im Cyber-Verbund.

---

3 SR 120.73 – Verordnung vom 27. Mai 2020 über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) (admin.ch)

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS
Generalsekretariat GS-VBS
Digitalisierung und Cybersicherheit VBS (DCS VBS)
Maulbeerstrasse 9, 3003 Bern

Premedia
Zentrum elektronische Medien ZEM
80.256.01 d 03.2021

Wichtigste Punkte der Strategie Cyber VBS

- Das VBS ist permanent fähig, verschiedene Bedrohungen, Ereignisse und Krisen im Cyberraum zu bewältigen oder Unterstützung zu leisten.
- Alle Akteure mit cyberrelevanten Aufgaben im VBS koordinieren sich aktiv im Rahmen der Strategie Cyber VBS.
- Die verantwortlichen Partner im VBS arbeiten zusammen, um Risiken und Chancen jetzt und in Zukunft zu identifizieren und bereit zu sein, diese gemeinsam zu bewältigen.
- Das VBS richtet seine Entwicklung fachlich, materiell, prozessual, wie auch personell auf die Cybersicherherausforderungen aus. Ein Schwergewicht bildet hier die Aus- und Weiterbildung aller VBS-Mitarbeitenden sowie dem Militär (Berufs- und Milizpersonal).
- Die Cyberverantwortlichen im VBS arbeiten mit Partnern zusammen. Diese sind die Kantone und Gemeinden, die Forschung und Privatwirtschaft, und auch das internationale Umfeld. Das VBS arbeitet eng mit dem Nationalen Zentrum für Cybersicherheit zusammen.