CANTON DU VALAIS
KANTON WALLIS

# Cybersicherheitsstrategie des Kantons Wallis

# *CyberStratVS*

24. Dezember 2024

**Frédéric Favre,** Staatsrat
Präsident der Arbeitsgruppe

***Gemeinsam in einem sicheren und resilienten Cyber-Wallis***

Die Sicherheit und der Wohlstand der Walliserinnen und Walliser sind dem Staatsrat ein zentrales Anliegen. Wie überall sonst, erlebt das Wallis eine tiefgreifende und rasche digitale Mutation, die für den Kanton und das gesamte sozioökonomische Gefüge eine mittlerweile entscheidende Dimension angenommen hat. Angesichts der Cyberherausforderungen wurden im Wallis bereits in den letzten Jahren zahlreiche Entscheidungen und Massnahmen getroffen, darunter das Gesetz über die Referenzdatenbanken und das Gesetz über die digitalen Dienste der Behörden. Zudem wurde im Jahr 2022 innerhalb der Kantonspolizei die Abteilung Cyberkriminalität geschaffen. Die mit der digitalen Mutation der Gesellschaft einhergehenden Risiken erfordern jedoch, dass das Wallis über eine Cybersicherheitsstrategie verfügt. Wie die jüngsten Cybervorfälle auf der ganzen Welt eindrücklich gezeigt haben, wird es nur mit einer kohärenten Gesamtpolitik gelingen, die Risiken von und im digitalen Raum besser zu beherrschen und zu verringern, um den vollen Nutzen aus den zahlreichen Fortschritten, die der digitale Raum bietet, zu ziehen.

Alle Akteure der Gesellschaft sind Cyberrisiken ausgesetzt. Es geht darum, diese rechtzeitig zu erkennen und sich dagegen zu wappnen. Cyberangriffe widerfahren nicht nur anderen und ihre Folgen können schwerwiegend sein. Wer auf einen Vorfall wartet, riskiert, dass die Auswirkungen mit voller Wucht eintreten. Im Wallis und in vielen Organisationen und Unternehmen werden Cyberrisiken bereits ernst genommen. Die Analyse zeigt jedoch, dass der allgemeine Reifegrad in Bezug auf die Cybersicherheit und die Kultur im Umgang mit Daten und deren Nutzung unzureichend ist. Eine Strategie und zusätzliche Massnahmen, die auf Antizipation ausgerichtet sind, sind dringend erforderlich. Der Staatsrat will damit die digitalen Risiken eindämmen und die Sicherheit und Resilienz von Behörden und wichtigen Akteuren gegenüber Cyberrisiken stärken.

Die Cybersicherheitsstrategie des Staatsrats richtet sich in erster Linie an Entscheidungsträger in der kantonalen Verwaltung, den Gemeinden, öffentlich-rechtlichen Institutionen und Betreiber kritischer Infrastrukturen, um ein kohärentes Kontinuum zwischen diesen Akteuren zu schaffen. Die Strategie schafft auch günstige Voraussetzungen dafür, damit Bürger und Unternehmen ihre eigene Verantwortung im Bereich der Cybersicherheit wahrnehmen.

Die Cybersicherheitsstrategie im Wallis wird ihre Wirkung erst im Laufe der Zeit entfalten. Der Staatsrat ist sich vollkommen bewusst, welche Anstrengungen und welchen Zeitaufwand es bedarf, damit sie sich als Reflex und Kultur bei jedem Einzelnen etablieren kann, genauso wie die Sicherheit im Strassenverkehr oder im Gesundheitsbereich. Daher beruht die Strategie auf einer kontinuierlichen Lageverfolgung und einer Steuerung, die es ermöglichen, gemeinsam mit allen Beteiligten die Wirksamkeit und Kohärenz der Walliser Strategie zu messen und allmählich zu verstärken.

**Frédéric Favre,** Staatsrat
Präsident der Arbeitsgruppe

# Die Strategie in Kürze

Die **Cybersicherheitsstrategie** des Kantons Wallis, kurz **CyberStratVS**, setzt die Vision des Staatsrats in konkrete Massnahmen um:

***Gemeinsam in einem sicheren und resilienten Cyber-Wallis***

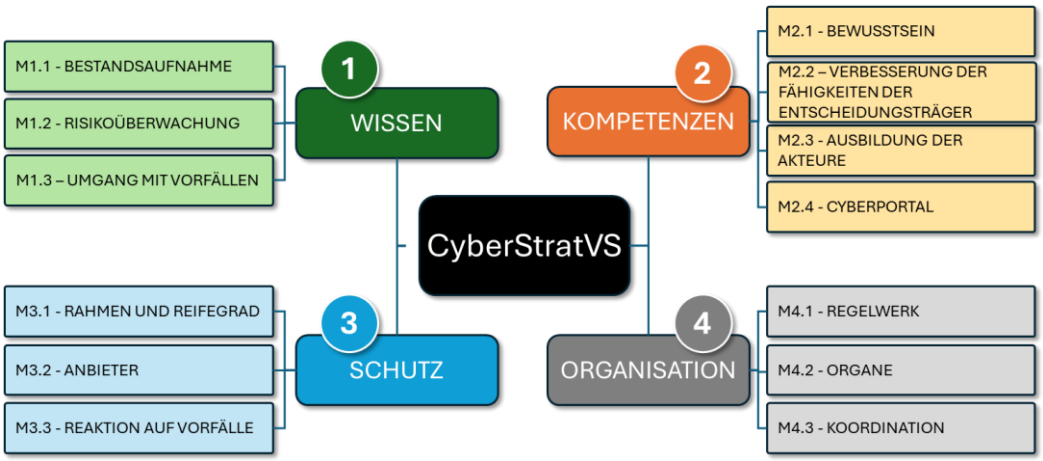
Die digitale Mutation erfordert ein schrittweises Vorgehen. Diese Strategie ist ein erster Schritt, um angesichts der Herausforderungen durch Cyberrisiken eine kohärente Politik zu etablieren und eine möglichst genaue Kenntnis des digitalen Ökosystems des Wallis zu erlangen, um die Relevanz und Effizienz seines Dispositivs schrittweise zu verbessern. Die CyberStrategieVS ist ein langfristiger Prozess, der agil bleiben muss, um sich kontinuierlich an die von Natur aus dynamischen und komplexen Herausforderungen anpassen zu können.

Die CyberStratVS auferlegt keine neuen Verpflichtungen. Sie unterstützt und begleitet - in erster Linie Entscheidungsträger, wobei sie für alle interessierten Kreise (im Folgenden: Stakeholder) zugänglich bleibt - **den Staat Wallis**, die **Gemeinden**, die **halbstaatlichen Institutionen** und die **Betreiber kritischer Infrastrukturen** bei der Umsetzung von Best Practices und in Übereinstimmung mit den gesetzlichen Anforderungen. Sie legt die Grundlage für die Zusammenarbeit zwischen den Beteiligten fest und lädt sie zum Informationsaustausch und zur gemeinsamen Nutzung von Mitteln und Massnahmen ein, wo immer dies möglich ist.

Um die Vision zu verwirklichen, wurden **vier Ziele** definiert:

1. Das Wallis verfügt über aktuelle **Kenntnisse** über den Vorbereitungsstand der Beteiligten;
2. Das Wallis verfügt über die notwendigen **Kompetenzen**, Fähigkeiten und Kooperationen, um das Vertrauen im Umgang mit Cyberrisiken zu stärken;
3. Das Wallis gewährleistet ein angemessenes Mass an **Schutz** und digitaler Resilienz (widerstandsfähige digitale Systeme);
4. Das Wallis verfügt über eine **Organisation,** in der die Verantwortlichkeiten und Kompetenzen der Beteiligten angesichts von Cyberbedrohungen festgelegt sind.

Diese Ziele werden in **13 Massnahmen** und **34 Aktionen** umgesetzt.




Um die Umsetzung von CyberStratVS zu gewährleisten, wurden zwei Schlüsselebenen definiert:

- Strategische Ebene: Die Oberaufsicht über CyberStratVS wird an die **Koordinationsgruppe Cybersicherheit VS** delegiert, die von einem **Cybersicherheitsbeirat** begleitet wird, der insbesondere Vertreter der verschiedenen Interessensgruppen umfasst.
- Operative Ebene: Mit der konkreten Umsetzung des CyberStratVS wird **die kantonale Stelle für Cybersicherheit VS** betraut, deren Aufgabe es ist, die CyberStratVS in enger Zusammenarbeit mit den ***Cyberrefe-renten*** **der Stakeholder** zu konkretisieren.

Um die Vollständigkeit der Massnahmen und Aktionen zu gewährleisten und sie mit dem vom Bund empfohlenen und in der Industrie üblichen Framework in Einklang zu bringen, stützt sich die CyberStratVS schliesslich auf die **sechs Säulen des NIST-Standards**[1]: Steuerung, Identifikation, Schutz, Detektion, Reaktion und Wiederherstellung.

[1] NIST Cybersecurity Framework 2.0 (National Institute of Standards and Technology) [https://www.nist.gov/system/files/documents/2022/10/03/NIST_CSF_update_Fact_Sheet.pdf].

# INHALTSVERZEICHNIS

# Geltungsbereich des Dokuments

## Ziel

Die Cybersicherheitsstrategie des Wallis zielt darauf ab, die Walliser Instanzen zu vereinen und zu koordinieren (das Wort "**gemeinsam**" in der Vision), damit für die immer stärker digitalisierte Walliser Gesellschaft (der Begriff "**Cyber-Wallis**" in der Vision) ein möglichst sicheres Lebens- und Arbeitsumfeld ("**sicher**", im Sinne von vertrauenswürdig und souverän) geschaffen wird, das sie im Falle eines Zwischenfalls in der Lage ist, weiter zu funktionieren und sich schnell zu erholen (der Begriff der "**Resilienz**" in der Vision).

## Zielpublikum

Der Umfang dieser Strategie umfasst folgende Stakeholder:

- **Staat Wallis**,
- **Gemeinden**,
- **staatsnahe und öffentlich-rechtliche Einrichtungen**
- **Betreiberinnen kritischer Infrastrukturen.** [2]

Diese Stellen müssen gewährleisten, dass die Daten und die Systeme, die diese Daten verarbeiten und für die sie verantwortlich und zuständig sind, gemäss den gesetzlichen Grundlagen sowie unter Beachtung der Aufgaben, Rollen und Kompetenzen aller Beteiligten geschützt und funktionsfähig sind. Die Strategie stellt ein Kontinuum mit den Anbietern von Dienstleistungen von nationaler Bedeutung, Dritten, der breiten Öffentlichkeit und der Wirtschaft her. Sie verhindert, dass Diskontinuitäten entstehen, von denen die Bedrohungsakteure profitieren können und stellt sicher, dass sich alle Stakeholder der Walliser Gesellschaft ihrer Risiken und Verantwortlichkeiten im Cyberraum bewusst sind.

## Entwicklung im Laufe der Zeit

Cyberrisiken, Dienstleistungen und Technologien entwickeln sich schnell weiter. Um sich kontinuierlich an die Veränderungen anzupassen, richtet der Staatsrat daher eine Struktur und Steuerung ein, deren Aufgabe es ist, die Umsetzung von CyberStratVS mit allen Beteiligten langfristig zu gewährleisten. Fortschritte werden **anhand von Leistungsindikatoren** gemessen und die erreichten Ergebnisse werden dazu beitragen, zu entscheiden, wann und wie Massnahmen angepasst / ergänzt werden müssen und wann die Strategie selbst eventuell überarbeitet werden muss.

[2] In Anlehnung an die Nationale Strategie zum Schutz Kritischer Infrastrukturen des Bundesamtes für Bevölkerungsschutz BABS [https://www.babs.admin.ch/de/nationale-strategie-zum-schutz-kritischer-infrastrukturen] beschränkt sich der Perimeter von CyberStratVS auf Infrastrukturen, die in der Verantwortung der Walliser Behörden liegen.

## Aufbau des Dokuments

Diese Cybersicherheitsstrategie besteht aus vier Kapiteln:

- Im ersten Teil **werden die Herausforderungen** dargelegt, die die Notwendigkeit einer kantonalen Cybersicherheitsstrategie begründen;
- der zweite Teil enthält **den Stand der Cybersicherheit** in der Schweiz und im Wallis, die Erwartungen, die von den während der Ausarbeitung des CyberStratVS konsultierten Instanzen geäussert wurden, sowie die Lehren aus den durchgeführten Übungen;
- der dritte Teil stellt **die Strategie** selbst vor, die Vision des Staatsrats, die Ziele und die Verteilung der Rollen und Verantwortlichkeiten unter den Stakeholdern;
- schliesslich wird im vierten Teil dargelegt**, wie die Strategie umgesetzt wird**.

Die konkreten Massnahmen sind in Anhang 1 aufgeführt, der somit an neue Situationen angepasst werden kann, ohne dass die Strategie selbst angepasst werden muss.

# 1. Die Herausforderungen der Digitalisierung

## 1.1. Gesellschaftlicher Wandel

In den letzten vier Jahrzehnten haben die Informations- und Kommunikationstechnologien (IKT) die Gesellschaft tiefgreifend verändert. Sie haben sich in drei grossen Phasen von einfachen Werkzeugen zum Motor des gesellschaftlichen Wandels entwickelt. Zunächst einmal haben die IKT die Optimierung von Arbeitsprozessen ermöglicht. Danach haben sie die Vernetzung von Objekten und Einheiten erleichtert. Heute ist die Abhängigkeit der Gesellschaft von den IKT und den Daten - ihrem Treibstoff - global und unumkehrbar.

Keine menschliche Aktivität - ob Gesundheit, Bildung, Energie, Verkehr oder öffentliche Sicherheit - kann mehr ohne diese technologische Ebene und ihre Dienste auskommen, während alle auf eine kritische Art und Weise auf einer möglichst sicheren Energieversorgung beruhen. Der Cyberraum lässt sich nicht auf IKT reduzieren. Deshalb sollte beispielsweise auch die folgende Vielzahl von Faktoren unter einem systemischen und nachhaltigen Ansatz berücksichtigt werden: Humanressourcen, Bildung (um eine solide Daten- und Nutzungskompetenz zu erreichen[3] ), Gesetze, Infrastruktur, natürliche Ressourcen und Finanzen.

## 1.2. Bedrohungen und Gefahren im digitalen Raum

Die Beherrschung des digitalen Umfelds ist eine entscheidende Herausforderung für die Gesellschaft, die einen flexiblen und gleichzeitig klar definierten Rahmen erfordert. Der Cyberraum stellt insbesondere aufgrund seiner Unbeständigkeit, der damit verbundenen Unsicherheiten und seiner Komplexität eine grosse Herausforderung dar. Einige dieser Dimensionen stellen bereits konkrete Risiken oder Bedrohungen dar, während andere zu solchen werden könnten, wenn sie nicht proaktiv gehandhabt werden. Entwicklungen frühzeitig zu erkennen und zu verstehen, um den Risiken vorzugreifen, ist daher zwingend erforderlich.

Mit ihrer Omnipräsenz und zunehmenden Komplexität weisen die IKT zahlreiche Schwachstellen auf, die häufig von böswilligen Akteuren ausgenutzt werden. Dies können Einzelpersonen, Organisationen oder Staaten sein. Während einige Schwachstellen zufällig auftreten, sind jedoch andere das Ergebnis von Entwicklungsfehlern, wie z. B. beim weltweiten IT-Ausfall von "Crowdstrike" am 19. Juli 2024, der durch ein fehlerhaftes Update verursacht wurde. Gewisse Schwachstellen werden auch absichtlich und ohne

[3] Datenkompetenz (oder "data literacy") umfasst die Fähigkeiten, Daten in ihrem jeweiligen Kontext kritisch und reflektiert zu sammeln, zu verwalten, zu bewerten und zu nutzen, wobei die Prinzipien der Datenethik und des Datenschutzes beachtet werden müssen - https://akademien-schweiz.ch/publications/data-literacy-charta-schweiz . Im digitalen Zeitalter, in dem Daten eine zentrale Rolle in Unternehmen, Regierungen und sogar im täglichen Leben spielen und ihre Vertraulichkeit, Integrität, Verfügbarkeit und Rückverfolgbarkeit ständig bedroht sind, ist Datenkompetenz eine Schlüsselkompetenz.

unser Wissen eingebaut, um Interessen zu verfolgen, die unseren eigenen zuwiderlaufen. Einige werden auch durch Fahrlässigkeit verursacht, ein Verhalten, das übrigens strafrechtlich relevant ist.

Mit den ersten Computersystemen tauchten bösartige Programme wie Viren auf. Sie führten zur Einführung von Sicherheitsmassnahmen zum Schutz der Geräte und Terminale. Später, mit der Hypervernetzung, wurde die Sicherheit immer wichtiger und erstreckte sich auf Netzwerke und Systeme. Das Datenzeitalter, gekoppelt mit einer Vielzahl von Abhängigkeiten, erfordert nun nicht mehr lediglich technische Massnahmen, sondern dass sich die Cybersicherheit auf strategischer Ebene etabliert und systemisch verwaltet wird. Neue Sicherheitspolitiken, die es ermöglichen, die gesellschaftlichen Herausforderungen der digitalen Mutation und ihrer Herausforderungen zu bewältigen, sind nunmehr die Norm.

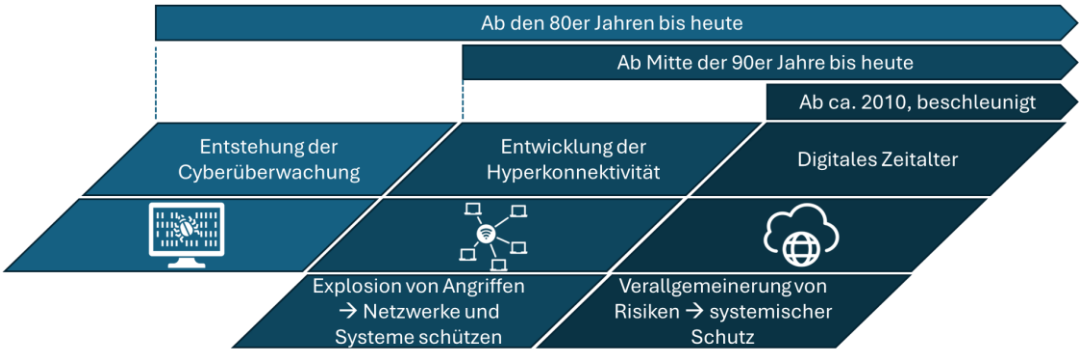



*Abbildung1 - Die Entwicklung des Cyberraums und der Natur der Cybersicherheit*

Die Bedrohungsakteure sind dieser Entwicklung gefolgt. Zunächst gab es **Hacker**, die von Spiel, Herausforderung und Aktivismus angetrieben wurden. Dann kamen die von Geldgier angezogenen **Cyberkriminellen** oder **Cyberpiraten** auf, böswillige Akteure, die den Wert von Daten, insbesondere von persönlichen Daten und die Möglichkeiten, sie zu nutzen, genau verstanden haben. Sie arbeiten in professionellen, international organisierten Banden, um sich zu bereichern und richten verheerende Schäden an.

Verschiedenen Schätzungen zufolge kostet diese Geissel der Gesellschaft bereits mehr als vier Prozentpunkte des BIP, Tendenz steigend. Nur ein geringer Teil dieser Straftaten (ca. 15%) wird den Strafverfolgungsbehörden zur Kenntnis gebracht, während diese nur etwa 15% dieser Straftaten bearbeiten können. Die dritte Kategorie sind **Cybersoldaten**, die im Nachrichtendienst, im politischen Bereich (z.B., um demokratische Prozesse zu beeinflussen) oder auch auf militärischer Ebene aktiv sind, wie man im Rahmen von Kriegen, insbesondere zwischen Russland und der Ukraine sowie im Nahen Osten, beobachten kann.

Der Cyberraum ist somit ein eigenständiger Konfliktraum, in dem die Kriegsparteien die gegnerischen Mittel stören, ausspionieren und zerstören. Die jüngsten Fälle verdeutlichen im Übrigen, wie wichtig es ist, dass das Wallis im Bereich der Cybersicherheit einen **systemischen** Ansatz und die **Beherrschung der Lieferketten** verfolgt.

Für die Verantwortlichen für Cybersicherheit im Kanton spielt die Unterscheidung zwischen den Akteuren und ihren Absichten - kriminell, Spionage, Sabotage, Subversion oder militärische Zwecke - keine Rolle. **Ihre Aufgabe ist es, tagtäglich dafür zu sorgen, dass die Daten und Prozesse, von denen die Bevölkerung und die Wirtschaft abhängen, in Bezug auf Vertraulichkeit, Integrität, Verfügbarkeit und Rückverfolgbarkeit bestmöglich geschützt sind.**[4]

## 1.3. Menschlicher Faktor

Trotz der rasanten technologischen Fortschritte der letzten Jahre steht der Mensch weiterhin im Mittelpunkt des Cyber-Ökosystems, insbesondere als bevorzugtes Ziel böswilliger Akteure, die sich seine technischen und psychologischen Schwächen zunutze machen. So geht ein erheblicher Teil der Angriffe auf immer neue Tricks (Social Engineering) zurück. Die rasche technologische Entwicklung erfordert daher eine ständige Anpassung der Fähigkeiten von Personen und Organisationen.

Die Weiterbildung, die nur wenige Unternehmen und Institutionen allein gewährleisten können, ist somit eine zentrale Investition, um zu verhindern, dass es aufgrund von Unterschieden in Bezug auf Alter (in der Schweiz sind bereits fast 20% der Bevölkerung über 65 Jahre alt), Ausbildung, Herkunft, Kultur usw. zum Ausklinken und zu Gräben in und zwischen den Bevölkerungsgruppen kommt. Dieser Aspekt ist umso wichtiger, als er vor dem Hintergrund eines zunehmenden Mangels an IKT-Fachkräften betrachtet werden muss - einer Entwicklung, die die Fähigkeit öffentlicher wie privater Einrichtungen, ihren Betrieb, ihre Sicherheit und sogar ihre Projekte und Entwicklungen zu gewährleisten, immer stärker belastet.

Nutzer, Entscheidungsträger, Techniker und viele andere Akteure spielen eine grundlegende Rolle bei der Cybersicherheit, die sowohl im beruflichen als auch im privaten Bereich eine gemeinsame Verantwortung darstellt. Wie die öffentliche Gesundheit, die nicht nur von Ärztinnen und Ärzten und Spitälern abhängt oder die Verkehrssicherheit, die nicht nur von der Polizei kontrolliert wird, liegt die **Cybersicherheit** nicht in der alleinigen Verantwortung von Informatikerinnen und Informatiker. Sie **betrifft die gesamte Gesellschaft**.

[4] Diese vier Prinzipien sind grundlegend für die Festlegung einer wirksamen umfassenden Sicherheitsstrategie und werden häufig bei der Bewertung und Gestaltung von Massnahmen zum Schutz von Informationssystemen herangezogen. Vertraulichkeit: Sicherstellen, dass nur befugte Personen Zugang zu Informationen haben. Integrität: Sicherstellen, dass die Informationen nicht unbefugt verändert oder modifiziert werden. Verfügbarkeit: Sicherstellen, dass die Informationen den berechtigten Nutzern zur Verfügung stehen, wenn sie sie benötigen. Rückverfolgbarkeit: Gewährleistung der Fähigkeit, den Ursprung einer Information und aller Aktionen, denen sie unterzogen wurden, zu identifizieren, um insbesondere die Authentizität der Informationen zu gewährleisten.

## 1.4. Stand der Cyberkriminalität im Wallis

Was die Daten zur digitalen Kriminalität betrifft, verfolgt die Kantonspolizei 33 Tatvorgehen und 29 Straftaten nach Strafgesetzbuch, die in fünf grosse Bereiche unterteilt sind: Cyberwirtschaftskriminalität (Phishing, Hacking, Betrug, Denial of Service usw.), Cybersexualdelikte, Cyber-Rufschädigung und unlauteres Verhalten, Darknet (illegaler Handel), andere (insbesondere Datenlecks). Im Jahr 2023 verzeichnete die Polizei 1'126 Fälle, was im Vergleich zu 2022 einen Anstieg von +113% bei der Datenentnahme, +117% beim unberechtigten Zugang zu einem Computersystem und +88% bei der betrügerischen Nutzung eines Computers bedeutet. Phishing-Fälle stiegen um 81% und Fälle von Ransomware um 60%. Es ist wichtig, daran zu erinnern, dass sich diese Zahlen nur auf Straftaten beziehen, die den Strafverfolgungsbehörden gemeldet werden

Diese beunruhigenden Zahlen sind sogar noch höher als die des Bundesamts für Cybersicherheit (BACS), das in seinem Halbjahresbericht vom Mai 2024[5] von einem Anstieg der gemeldeten Cybervorfälle in der Schweiz um 43% Jahr 2023 (49'380) im Vergleich zu 2022 (34'527) berichtet. Um den Ernst der Lage zu erfassen, muss man nochmals berücksichtigen, dass diese Zahlen[6] lediglich 15% der tatsächlichen Fälle darstellen. Die effektive Zahl für das Wallis hätte somit im Jahr 2023 fast 7'500 Fälle betragen, was 20 Cybervorfällen pro Tag entspricht, mit weit unterschätzten wirtschaftlichen und persönlichen Folgen.

## 1.5. Perspektiven

Die IKT nehmen mittlerweile eine zentrale Rolle in der Gesellschaft ein. Wie bereits Ende 2022 mit generativen KI-Tools wie ChatGPT von OpenAI, Copilot von Microsoft oder Gemini von Google festgestellt wurde, entstehen immer mehr disruptive Technologien. Dieser Trend wird sich tendenziell beschleunigen, insbesondere in Bereichen wie vernetzte Objekte, künstliche Intelligenz, Quantencomputer[7] und Raumfahrttechnologien.

[5] https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2024/ncsc-hjb-2023-2.html

[6] https://www.fedpol.admin.ch/fedpol/de/home/aktuell/mm.msg-id-101469.html

[7] Quantencomputing ist eine aufstrebende Technologie, die sich die Prinzipien der Quantenmechanik zunutze macht und komplexe Berechnungen unendlich viel schneller als herkömmliche Computer durchführen kann. Mit dieser Technologie werden Bedrohungsakteure in naher Zukunft in der Lage sein, alle Standardverschlüsselungsarten, die die Vertraulichkeit von Daten und Kommunikation schützen, zu durchbrechen.

Dieser Fortschritt bringt wiederum neue Risiken mit sich, die ständig überwacht und bewertet werden müssen und die durch geopolitische Spannungen noch verschärft werden. Die grösste Herausforderung für jede Organisation, insbesondere mit begrenzten Mitteln, besteht darin, diese Umwälzungen und ihre Auswirkungen rechtzeitig zu erkennen und vorbeugende oder korrigierende Massnahmen zu ergreifen, um die damit verbundenen Risiken zu verringern. Antizipation ist daher mehr denn je und auf sämtlichen Ebenen ein Schlüsselfaktor. Zu diesem Zweck muss eine Auslegeordnung aller relevanten Bereiche wie Gesellschaft, Recht, Finanzen, Demografie, Umwelt und Energie erstellt und auf dem neuesten Stand gehalten werden.

# 2. Stand der Cybersicherheit in der Schweiz

## 2.1. Bund

### 2.1.1. Vision und strategische Ziele

Die Bekämpfung von Cyberrisiken ist eine neuere Entwicklung, die 1997 im Zuge der Strategischen Führungsübung zum Thema "Verwundbarkeit unserer Informationsgesellschaft" entstand. Im Jahr 2003 wurde die Melde- und Analysestelle Informationssicherung (MELANI) gegründet und 2012 erhielt die Schweiz ihre erste Nationale Strategie zum Schutz vor Cyberrisiken NCS, die 2023 von der derzeit gültigen Nationalen ***Cyberstrategie*** NCS[8] abgelöst wurde:

"*Die Schweiz nutzt die Chancen der Digitalisierung und mindert Cyberbedrohungen und deren Auswirkungen durch geeignete Schutzmassnahmen. Sie gehört zu den weltweit führenden Wissens-, Bildungs- und Innovationsstandorten in der Cybersicherheit. Die Handlungsfähigkeit und die Integrität ihrer Bevölkerung, ihrer Wirtschaft, ihrer Behörden und der in der Schweiz ansässigen internationalen Organisationen gegenüber Cyberbedrohungen sind gewährleistet.*"

### 2.1.2. Nationales Dispositiv

Das vom Bundesamt für Cybersicherheit BACS koordinierte nationale Dispositiv basiert auf 3 Aktionsbereichen[9] (Abbildung 2):

- **Cybersicherheit:** Umfasst sämtliche Massnahmen zur Verhinderung und Bewältigung von Vorfällen, zur Verbesserung der Resilienz gegenüber Cyberrisiken und zur Entwicklung der Zusammenarbeit.
- **Cyberdefence:** Umfasst sämtliche Massnahmen der Nachrichtendienste und der Armee zum Schutz kritischer Systeme, von denen die Landesverteidigung abhängt, zur Abwehr von Cyberangriffen, zur Sicherstellung der Einsatzbereitschaft der Armee in allen Situationen, die den Cyberraum betreffen und zur Entwicklung ihrer Fähigkeiten und Kompetenzen, um die zivilen Behörden subsidiär unterstützen zu können; dieser Bereich umfasst Massnahmen zur Identifikation von Bedrohungen und zur Behinderung von Angreifern.

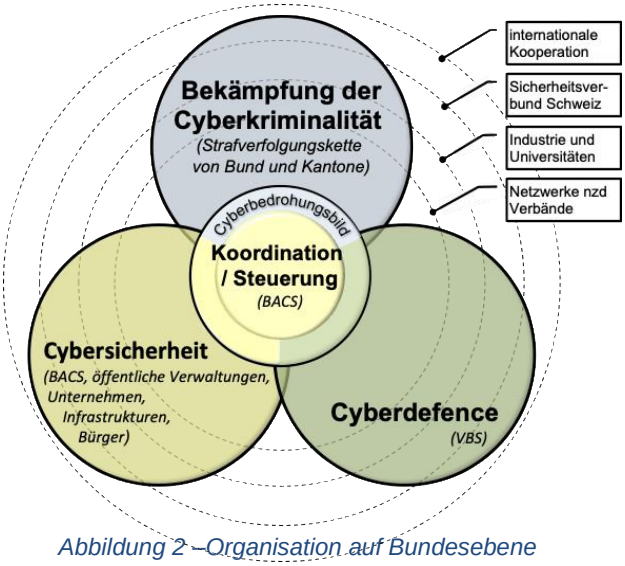



*Abbildung 2 – Organisation auf Bundesebene*

[8] https://www.ncsc.admin.ch/ncsc/de/home/strategie/cyberstrategie-ncs.html
[9] https://www.fedlex.admin.ch/eli/cc/2020/416/de

- **Strafrechtliche Verfolgung von Cyberkriminalität:** Umfasst alle Massnahmen der strafrechtlichen Verfolgung des Bundes und der Kantone zur Bekämpfung der Cyberkriminalität.

Wie oben dargestellt, kann dieses System nicht ohne unterstützende Netzwerke funktionieren, insbesondere dem Sicherheitsverbund Schweiz SVS, internationale Kooperationen, Industrie, akademische Kreise sowie Verbands- und Berufsorganisationen.

### 2.1.3. Wichtigste Akteure[10]

Zur Bekämpfung von Cyberrisiken verfügt die Schweiz innerhalb des Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) über die folgenden **Hauptinstanzen**:

- *Generalsekretariat des VBS* (strategische Steuerung, Koordination und politische Beratung),
- *Staatssekretariat für Sicherheitspolitik* (Antizipation und Entwicklungen in der Sicherheitspolitik, Informationssicherheit und Sicherheitskontrollen in Bezug auf Personen und Unternehmen),
- *Nachrichtendienst des Bundes* (Beobachtung der Lage in Bezug auf Cyberbedrohungen, Reaktion bei Cyberangriffen auf kritische Infrastrukturen, Bekämpfung von Cyberspionage),
- *Kommando Cyber (*Leistungen im Cyberraum und im elektromagnetischen Raum zugunsten der Armee und subsidiäre Unterstützung zugunsten der Partner des Sicherheitsverbunds Schweiz),
- *Bundesamt für Rüstung* / armasuisse (Aufbau von wissenschaftlich-technischem Wissen zugunsten der Armee und des VBS, insbesondere mit dem *Cyberdefence Campus*),
- *Bundesamt für Bevölkerungsschutz* (Einbezug des Cyberbereichs in die Nationale Risikoanalyse von Katastrophen und Notlagen und die Nationale Strategie zum Schutz von Kritischen Infrastrukturen),
- *Bundesamt für Cybersicherheit* (Kompetenzzentrum des Bundes für den Umgang mit Cyberbedrohungen und erste Anlaufstelle für Unternehmen, Verwaltung, Bildungseinrichtungen und die Bevölkerung).

Zu den **weiteren nationalen Schlüsselakteuren** gehören ausserdem:

- *Sicherheitsverbund Schweiz SVS* (Koordination der Kantone im Bereich Cyber), insbesondere im Rahmen der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren, die unter anderem die Schweizerische Kriminalprävention leitet.

[10] https://www.parlament.ch/centers/eparl/curia/2022/20223368/Bericht%20BR%20D.pdf

- *Bundesanwaltschaft*, die das *Netzwerk digitale Ermittlungsunterstützung Internetkriminalität NEDIK*, das nationale Netzwerk zur Unterstützung von Ermittlungen im Kampf gegen Computerkriminalität im Auftrag der Konferenz der Kantonalen Polizeikommandantinnen und Polizeikommandanten der Schweiz (KKPKS) ins Leben gerufen hat.

### *2.1.4.* Wichtigste bundesstaatliche Rechtsgrundlagen

Im Bereich **Recht** berücksichtigt die vorliegende Strategie insbesondere die folgenden Gesetzestexte:

- **Informationssicherheitsgesetz** (ISG[11]): Dieses Gesetz legt neu insbesondere den Betreiberinnen kritischer Infrastrukturen eine Meldepflicht für Cybervorfälle und die damit verbundenen Fristen auf.
- **Datenschutzgesetz** (DSG[12]): Dieses Gesetz harmonisiert die Praktiken auf nationaler Ebene und stellt die rechtliche Kompatibilität der Schweiz mit der Datenschutz-Grundverordnung DSGVO der Europäischen Union her.
- **Nachrichtendienstgesetz** (NDG[13]): Neben den gleichnamigen Aufgaben definiert dieses Gesetz insbesondere die operative Intervention des Nachrichtendienstes des Bundes bei Cyberangriffen auf kritische Infrastrukturen.

## 2.2. Aktivitäten in den Kantonen

Die erste Version der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) konzentrierte sich auf Massnahmen auf Bundesebene. Bei der Überarbeitung 2018 wurden den Kantonen im Anhang vier Ziele zugewiesen ▸Verbesserung der Kompetenzen innerhalb der Kantonsverwaltungen, ▸Teilnahme am Wissensaustausch über Cyberbedrohungen, ▸Stärkung der IT-Resilienz und ▸Beitrag zur Schaffung einer gemeinsamen Basis für den Erfahrungsaustausch.

Die neue NCS wurde von den Kantonen anlässlich der Plenarversammlung der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren vom 13. April 2023 validiert. Sie ist nun auf kantonaler Ebene vollumfänglich anwendbar. Die Heterogenität zwischen den Kantonen ist noch gross, aber die Kantone stellen sich allmählich auf die Bekämpfung ein. Mehrere Kantone verfügen nun über eine Cybersicherheitsstrategie oder Arbeitsgruppen, um die wichtigsten Akteure zu koordinieren. Zudem sind verschiedene Gesetzesentwürfe zur Informations- und Cybersicherheit in Arbeit.

Die ***Conférence latine des directeurs du numérique*** *(CLDN)* hat im Mai 2023 eine gemeinsame Vision zum Thema digitale Souveränität[14] veröffentlicht, die insbesondere technische (Zweckmässigkeit einer souveränen

[11] https://www.fedlex.admin.ch/eli/oc/2022/232/de

[12] https://www.fedlex.admin.ch/eli/oc/2022/491/de

[13] https://www.fedlex.admin.ch/eli/oc/2017/494/de

[14] https://cldn.ch/les-cantons-latins-veulent-renforcer-leur-action-concertee-pour-la-souverainete-numerique/

Cloud), rechtliche und sozioökonomische (Definition der digitalen Souveränität) sowie ethische Aspekte umfasst. So definiert die CLDN digitale Souveränität als "*die Fähigkeit der Verwaltung, ihre strategische Autonomie zu wahren, d.h. materielle und immaterielle Güter und digitale Dienste, die sich auf Wirtschaft, Gesellschaft und Demokratie auswirken, selbstständig nutzen und kontrollieren zu können*".

## 2.3. Lage im Wallis

### 2.3.1. Kanton

Achtgrösster Schweizer Kanton nach Einwohnerzahl, drittgrösster Kanton nach Fläche, zwölfgrösster Kanton nach BIP, zweisprachig, mit einer anspruchsvollen Topografie - vom Genfersee bis zu den höchsten Alpengipfeln, einer diversifizierten Wirtschaft - von der Berglandwirtschaft über den Tourismus und die Industrie bis hin zur Hochtechnologie, nationaler Pfeiler der Energiewirtschaft mit 28% der nationalen Wasserkraftproduktion..., das Wallis ist ein komplexer Kanton. Mehr als andere ist er auch mit klimatischen Unwägbarkeiten und deren Auswirkungen auf kritische Infrastrukturen konfrontiert, wie bei den Unwettern im Jahr 2024.

Cyberbedrohungen sind seit mehreren Jahren Gegenstand zahlreicher Massnahmen, die auf kantonaler Ebene ergriffen werden. Bereits 2019 erkannte das Kantonale Risikoobservatorium (KRO) die Bedeutung von Cyberrisiken und am 11. Dezember 2024 verabschiedete der Staatsrat die neue kantonale Strategie zum Schutz kritischer Infrastrukturen (SKI.VS).

Ab 2022 wurden die Massnahmen des Kantons im Bereich der Cybersicherheit intensiviert und zunehmend besser koordiniert. Die Gemeinden wurden zu ihren Bedürfnissen und Erwartungen befragt. Subsidiäre forensische Unterstützung im Falle eines Vorfalls wurde vom Kanton eingeführt, ebenso wie Schwachstellentests. Verschiedene Informationsmaterialien wurden an die Gemeinden versandt und mehrere Übungen durchgeführt (CyberREG23, CyberVS24). Der Kanton unterstützte zudem konkrete Lösungen wie die Erlangung von Labels für die Cybersicherheit oder die Sensibilisierungsplattform elearningcyber.ch. Die Notwendigkeit, diese Massnahmen zu harmonisieren und zu verstärken, hat ab 2023 die Arbeitsgruppe Cybersicherheit VS unter dem Vorsitz des Vorstehers des Departements für Sicherheit, Institutionen und Sport (DSIS) dazu veranlasst, die vorliegende Strategie für den gesamten Kanton zu erstellen.

Was die gesetzlichen Grundlagen betrifft, so verfügt das Wallis bereits über mehrere Gesetze, die direkt oder indirekt mit der Cybersicherheit in Verbindung stehen:

- **Gesetz über die Information der Öffentlichkeit, den Datenschutz und die Archivierung** (GIDA[15]): Dieses Gesetz umfasst Bestimmun-

[15] https://lex.vs.ch/app/de/texts_of_law/170.2

gen über die Information der Öffentlichkeit und den Zugang zu amtlichen Dokumenten (Transparenz), den Schutz von Personendaten und die Archivierung amtlicher Dokumente.

- **Gesetz über digitale Dienste der Behörden** (GDDB[16]): Dieses Gesetz schafft die Rahmenbedingungen für die Entwicklung, den Betrieb, die Nutzung und die Finanzierung der Digitalen Verwaltung und Behördenleistungen.
- **Gesetz über den Bevölkerungsschutz und die Bewältigung von besonderen und ausserordentlichen Lagen** (GBBAL[17] ): Dieses Gesetz regelt die Koordination der Bewältigung und des Schutzes der Bevölkerung in besonderen und ausserordentlichen Lagen, die Organisation der Vorbereitungsmassnahmen und den schrittweisen Übergang zwischen ordentlichen und kritischen Lagen.

### 2.3.2. Gemeinden

Die Befragung der Gemeinden im Jahr 2022 - mit einer soliden Beteiligung von 66% - ergab, dass nur 13% dieser über einen IT-Verantwortlichen verfügten. 55% fühlten sich wenig oder schlecht auf Cyberangriffe vorbereitet, während 80% eine Unterstützung durch den Kanton wünschten, insbesondere bei Cyberangriffen. Die jüngsten Arbeiten zeigten einen Bedarf an Mindeststandards, an Unterstützung in den Beziehungen zu Anbietern, bei Versicherungsfragen, Penetrationstests, Ausbildung und der Finanzierung dieser Massnahmen. Um den Stand der Dinge zu präzisieren und bei der Formulierung der CyberStratVS-Massnahmen zu helfen, wurde den Gemeinden im September 2024 ein nach dem NIST-Standard artikulierter Fragebogen zugestellt. Die Rücklaufquote von über 65% verdeutlicht erneut, wie besorgt die Gemeinden über die Cybersicherheit sind:

- Im Hinblick auf die **Identifikation** und Verwaltung von Computern und Daten wurden einige Fragen nur zu 20%, andere zu 90% positiv beantwortet. Darüber hinaus zeigt sich, dass die Gemeinden ihren Anbietern oft einfach vertrauen. An dieser Stelle ist es wichtig daran zu erinnern, dass die Gemeinden auch im Falle einer Delegation an Dritte für die Daten und die Systeme, auf denen sie gehostet werden, verantwortlich bleiben.
- Auch bei den bewährten Verfahren in Bezug auf **Datenschutz**, Datenzugriff, Personalschulung oder technische Sicherheitslösungen ist die Situation ebenfalls uneinheitlich; manchmal bejahen 30% der Gemeinden diese Frage, manchmal 90%.
- Bei den Fragen, ob die Gemeinden in der Lage sind, ihre Infrastruktur zu überwachen und Vorfälle zu **erkennen**, schwankt die Spanne zwischen 60 und 75%. Darüber hinaus sind lediglich 20% der Gemeinden der Meinung, dass sie auf das Krisenmanagement vorbereitet sind.

[16] https://lex.vs.ch/app/de/texts_of_law/170.8
[17] https://lex.vs.ch/app/de/texts_of_law/501.1 .

- Bei Fragen zur **Reaktion** auf Vorfälle schätzen die Gemeinden ihre Bereitschaft auf 30 bis 40%. Die Delegation an Anbieter gilt häufig als positive Antwort.
- 40% der Gemeinden sind der Ansicht, dass sie für die **Wiederherstellung** nach einem Vorfall gewappnet sind, aber nur 15% verfügen über ein Verfahren zur Analyse nach einem Vorfall, was ebenfalls auf eine Lücke im Krisenmanagement hindeutet.
- In Bezug auf die **Steuerung** geben nur 40% der Gemeinden an, über eine Richtlinie zur Cybersicherheit und definierte Rollen zu verfügen.

Diese vielfältigen und insgesamt unbefriedigenden Ergebnisse zum **Reifegrad bezüglich Cybersicherheit (Cybersecurity maturity)** der Gemeinden zeigen, welche Anstrengungen unternommen werden müssen, um sie auf einen zufriedenstellenden Zielwert zu bringen. Es ist jedoch anzumerken, dass die Gemeinden, die ein Cybersicherheits-Label anstreben, grundsätzlich im Vergleich zu anderen einen höheren Vorbereitungsstand aufweisen.

In den Workshops und bilateralen Gesprächen bestätigten die Vertreter der Gemeinden den geringen Reifegrad bezüglich Cybersicherheit, der in den Fragebögen aufgezeigt wurde. Diese - häufig nicht spezialisierten und auf Milizbasis tätigen - Verantwortlichen berichteten einhellig, dass sie sich **allein gelassen fühlen** angesichts der Herausforderungen und der Komplexität der digitalen Mutation und der damit verbundenen Risiken.

### 2.3.3. Öffentlich-rechtliche Einrichtungen und kantonale kritische Infrastrukturen

Im Wallis gibt es zahlreiche öffentlich-rechtliche Institutionen sowie kritische Infrastrukturen, die vielen Einschränkungen unterworfen sind. Die Vertreter, die an der Ausarbeitung des CyberStratVS mitgewirkt haben, stellen fest, dass der Rahmen im Bereich der Cybersicherheit unzureichend ist. Die Feststellungen und Bedürfnisse sind mit denen der Gemeinden vergleichbar, d.h. mit Cybersicherheitsbeauftragten, die angeben, sich allein gelassen zu fühlen. Sie stellen fest, dass nur ein Bruchteil der Dachorganisationen Leitlinien herausgibt, die je nach Bedeutung der betroffenen kritischen Infrastrukturen zwingend oder empfehlenswert sind.

Anhand der gesammelten Aussagen lässt sich feststellen, dass sich der Reifegrad bezüglich Cybersicherheit dieser Institutionen und Infrastrukturen nicht von demjenigen der Gemeinden unterscheidet. Für diese Akteure ist es eine Herausforderung, komplexe Cybersicherheitskriterien zu implementieren und aufrechtzuerhalten. Da die meisten von ihnen wichtige personenbezogene Daten verwalten, sind eine besondere Aufmerksamkeit und Unterstützung dringend erwünscht.

### 2.3.4. Zusammenfassung der Bedürfnisse

Die Stabsübungen (siehe 2.3.1) haben die Identifikation wichtiger Verbesserungspunkte erlaubt, insbesondere:

- **Kommunikation** (reaktiv und proaktiv), da die Digitalisierung diesen Bereich stark verändert, das Tempo von Krisen beschleunigt und das Verhalten der Öffentlichkeit verändert hat;
- die Notwendigkeit einer umfassenden **Auslegeordnung**;
- eine effektive **Zusammenarbeit** der Akteure
- und **den** kontinuierlichen **Austausch** von Informationen zwischen den Ansprechpartnern sowie deren Verwaltung, um sicherzustellen, dass alle relevanten Informationen ermittelt und genutzt werden.

Die Workshops und der Austausch mit Vertretern von Gemeinden, Institutionen und kritischen Infrastrukturen haben ihrerseits die folgenden Bedürfnisse und Erwartungen hervorgehoben:

- **Steuerung** - CyberStratVS muss die Rollen und Verantwortlichkeiten der privaten und öffentlichen Stakeholder klären. Klare Ansprechpersonen und Kontaktstellen werden gefordert, ebenso wie eine umfassende Auslegeordnung der relevanten Punkte und Akteure. Eine Mehrheit ist der Ansicht, dass die Gemeindeautonomie im Bereich der Cybersicherheit relativiert werden muss und dass zur Sicherstellung der konkreten Umsetzung der Massnahmen verschiedene Instrumente (Verfahren, Gesetz, Audits usw.) erforderlich sind, wie beispielsweise die neuen Verpflichtungen der Energieversorger oder im Bereich der Staatsfinanzen.
- **Information** - Die Stakeholder halten es für notwendig, eine kantonale Kultur der Cybersicherheit zu etablieren. Sie äussern einen Bedarf an Unterstützung, um die Cybersicherheit für verschiedene Zielgruppen, insbesondere Entscheidungsträger, zugänglich zu machen. Der Wissensaustausch ist von höchster Bedeutung und sollte durch eine kantonale Überwachung begleitet werden. Es wird erwartet, dass eine einzige kantonale Anlaufstelle eingerichtet wird, um der Verzettelung entgegenzuwirken.
- **Ausbildung** - Die Teilnehmenden der Workshops waren sich einig, dass der Einzelne wichtig ist und daher Ausbildungsbedarf besteht. Besonders hervorgehoben wurde der Bedarf an Fähigkeiten im Bereich Krisenmanagement.
- **Ressourcen** - Die Stakeholder berichten von grossen Schwierigkeiten, was die Ressourcen betrifft. Zu den Prioritäten gehören die Bündelung der Kräfte, Harmonisierung, Zusammenarbeit und die Nutzung von Synergien, um diese Probleme zu bewältigen. Die Rolle des Kantons ist zentral und alle halten es für entscheidend, dass er eine stärkere Rolle übernimmt. Darüber hinaus sollte geprüft werden, ob es sinnvoll ist, den Zugang zu bestimmten Leistungen zu erleichtern, etwa im Bereich des Security Operations Center (SOC) oder der Beschaffungspolitik.
- **Rahmen** - Es wurde die klare Erwartung geäussert, dass ein Richtlinien-Katalog erstellt werden sollte. Die Teilnehmenden wiesen jedoch auf die Gefahr einer Erhöhung der Komplexität und des Risikos hin, dass mit jeder Verantwortlichkeitsstufe die Anzahl der Vorschriften zunimmt. Sie betonten auch die Zeit, die sie für ihren Aufwuchs benötigen.

Ein Konsens bestand darin, dass Labels gefördert werden sollten und viele waren der Ansicht, dass ein spezielles Gesetz die Umsetzung der Massnahmen erleichtern würde.

# 3. Strategie

## 3.1. Vision

***Gemeinsam in einem sicheren und resilienten Cyber-Wallis***

**Der Staatsrat hat sich zum Ziel gesetzt…**

Die folgenden Handlungsgrundsätze - die Handlungsdoktrin - kennzeichnen die Walliser Strategie:

- **Antizipieren** - In einem hochdynamischen Bereich ist Geschwindigkeit entscheidend. Auf der Grundlage einer fundierten Kenntnis der Gegebenheiten gilt es, Herausforderungen und Risiken so früh wie möglich zu erkennen, um nicht unvorbereitet getroffen zu werden.
- **Begleiten** - Es geht darum, eine Linie vorzugeben, günstige Bedingungen zu schaffen und nur dann besondere Massnahmen vorzuschreiben, wenn das allgemeine Interesse auf dem Spiel steht und der Mehrwert erwiesen ist.
- **Zusammenarbeiten** - In einem Bereich, in dem niemand über das absolute Wissen oder alle Handlungsmöglichkeiten verfügt, geht es darum, einen gemeinsamen Ansatz, Erfahrungsaustausch und Subsidiarität zu bevorzugen, um zu tragbaren Kosten einen hohen Reifegrad bezüglich Cybersicherheit zu erreichen und aufrechtzuerhalten.

## 3.2. Ziele

Aus der Situationsanalyse und der Vision wurden **vier Ziele** abgeleitet. Sie werden von Absichten begleitet, die den angestrebten Endzustand oder die angestrebte Wirkung darlegen.

| Ziel | Absicht / angestrebter Endzustand |
|---|---|
| 1. Das Wallis verfügt über aktuelle Kenntnisse zum Vorbereitungsstand der Stakeholder. | Es geht darum:<br>▪ Über ein dynamisches (aktuelles) Inventar der Stakeholder, ihren Vorbereitungsstand und ihrer gegenseitigen Abhängigkeiten zu verfügen.<br>▪ Risiken (Bedrohungen und Gefahren) sowie deren Auswirkungen auf die Beteiligten kontinuierlich zu bewerten.<br>▪ Herausforderungen im Zusammenhang mit der digitalen mutationion zu verstehen und in der Lage zu sein, diese zu antizipieren.<br>▪ Über Kenntnisse zu Vorfällen zu verfügen, die Stakeholder betroffen haben, mit dem Ziel eine kontinuierliche Verbesserung zu erreichen. |
| 2. Das Wallis verfügt über die | Es geht darum: |

| Ziel | Absicht / angestrebter Endzustand |
|---|---|
| Kompetenzen, Fähigkeiten und Kooperationen, die angesichts von Cyberrisiken notwendig sind, um die Selbstbefähigung zu stärken. | ▪ Die Fähigkeit von Entscheidungsträgern zu entwickeln, die Herausforderungen und Risiken des Cyberbereichs zu integrieren und zu beherrschen.<br>▪ Alle Mitarbeitenden von Stakeholdern mit den wesentlichen Kenntnissen über die Herausforderungen und Risiken der Digitalisierung und der Datenkompetenz auszustatten.<br>▪ Über kompetente Fachkräfte zu verfügen, die sich den Herausforderungen und Risiken der Digitalisierung stellen.<br>▪ Ein kollaboratives Umfeld zu schaffen, das die Stakeholder bei der Bewältigung der Herausforderungen und Risiken der Digitalisierung unterstützt. |
| 3. Das Wallis gewährleistet ein angemessenes Niveau an digitalem Schutz und digitaler Resilienz. | Es geht darum:<br>▪ Sicherzustellen, dass die Beteiligten sowie ihre Partner und Anbieter über ein Schutzniveau (technisch, organisatorisch, prozessual) verfügen, das dem Stand der Technik entspricht.<br>▪ In der Lage zu sein, Vorfälle oder versuchte Angriffe auf die digitale Infrastruktur von Stakeholdern frühzeitig zu erkennen.<br>▪ In der Lage zu sein, Cyberkrisen flexibel (*skalierbar*) zu begegnen.<br>▪ Die Kontinuität der wesentlichen Leistungen der Stakeholder zu gewährleisten. |
| 4. Das Wallis verfügt über eine Organisation, die die Verantwortlichkeiten und Kompetenzen der Beteiligten im Hinblick auf Cyberbedrohungen definiert. | Es geht darum:<br>▪ Im Rahmen der Grundsätze der Subsidiarität und der guten Zusammenarbeit über eine kantonale Steuerung zu verfügen, in der klare Rollen und Verantwortlichkeiten festgelegt sind, die eine Koordination der Beteiligten untereinander ermöglicht.<br>▪ Über einen formellen Rahmen zu verfügen, der die Grundsätze und Massnahmen zur Gewährleistung eines angemessenen Niveaus der Cybersicherheit auf kantonaler Ebene legitimiert.<br>▪ Über eine kontinuierliche Bestandsaufnahme zu verfügen, die es ermöglicht, die Umsetzung der Strategie und ihrer Massnahmen einzuschätzen. |

## 3.3. Massnahmen

In den Augen des Staatsrats hat die Konkretisierung von CyberStratVS hohe Priorität, damit sie zum gewünschten Effekt führt: das Wallis zu einem Kanton zu machen, der angesichts der zahlreichen Cyberherausforderungen so sicher wie möglich ist.

Die Strategie gibt die Richtung für mehrere Jahre vor. Sie verschafft den Stakeholdern einen Überblick über die Sicherheit im Kanton. Sie ermöglicht es ihnen, auf ihrer Ebene und im Rahmen ihrer Verantwortlichkeiten rechtzeitig alle nützlichen Massnahmen zu ergreifen, um das allgemeine Niveau des Reifegrads bezüglich Cybersicherheit zu erhöhen. Sie stützt sich auf den "Management by Objectives"-Ansatz in der vom Staatsrat für das Gemeinwohl vorgezeichneten Richtung.

Die aus der Vision und den Zielen abgeleiteten Handlungen haben eine kürzere "Lebensdauer". Sie müssen in kürzeren Abständen ergänzt und korrigiert werden können, ohne dass dies zu einer Änderung der Strategie führt. Sie bestehen aus **13 Massnahmen,** die in **34** messbare **Aktionen** unterteilt sind (*siehe* Anhang 1). Sie werden Gegenstand eines Monitorings und einer regelmässigen Evaluation sein, die sich nach den erreichten Ergebnissen und der Entwicklung der Technologien und Herausforderungen richtet.

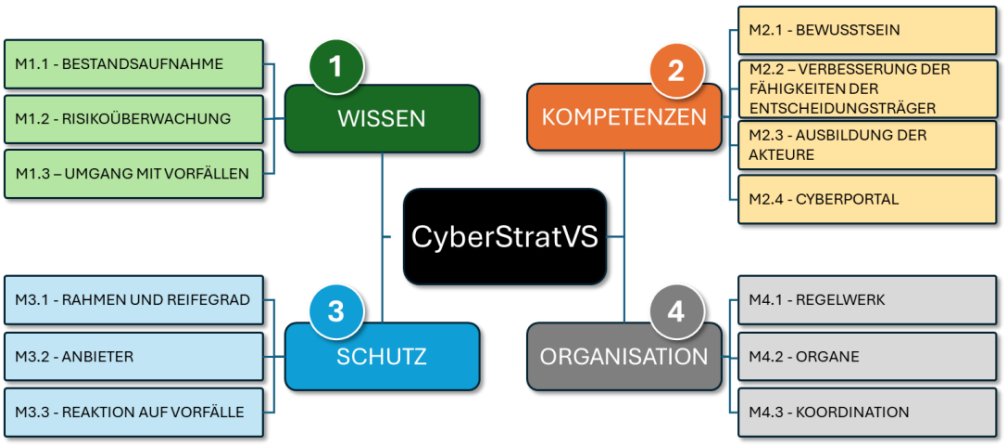



*Abbildung 3 – Massnahmen der CyberStratVS*

## 3.4. Rollen und Verantwortlichkeiten

Die allgemeine Organisation und die Beziehungen der Stakeholder im Rahmen von CyberStratVS werden im Folgenden beschrieben und veranschaulicht.

- Der Staatsrat delegiert die Oberaufsicht über CyberStratVS an die **Koordinationsgruppe Cybersicherheit** (KG Cysec) und somit die Nachfolgerin der Arbeitsgruppe, die die Leitung bisher innehatte. Bei Bedarf kann diese Gruppe einen **Cybersicherheitsbeirat** einrichten, dem unter anderem Vertreter der Stakeholder angehören.
- Die Umsetzung von CyberStratVS wird der **kantonalen Stelle für Cybersicherheit VS** (*vgl.* Massnahme M4.2b) anvertraut. Über dessen genaue Struktur und Bezeichnung entscheidet der Staatsrat zu einem späteren Zeitpunkt. Dieses arbeitet bei der Umsetzung von CyberStratVS eng mit der KG Cysec zusammen, insbesondere bei Vorschlägen zur Weiterentwicklung und Überarbeitung entsprechend den erreichten Ergebnissen und der sich ändernden Situation und Cyberrisiken.
- Im Falle eines Vorfalls, der einen der Stakeholder betrifft, bleibt die betroffene Einheit in jedem Fall für ihren Perimeter verantwortlich. Wenn sich die zur Verfügung stehenden Mittel und die ihrer Anbieter als unzureichend erweisen, können die Spezialisten der kantonalen Verwaltung, sofern sie verfügbar sind und über die erforderlichen Kompetenzen verfügen, ausschliesslich subsidiär Hilfe leisten. Wenn die Krise mehrere Einheiten betrifft oder eine kantonale Dimension annimmt, sorgt das **Kantonale Führungsorgan** (KFO) für die Koordination auf kantonaler Ebene gemäss dem kantonalen Bevölkerungsschutzgesetz.

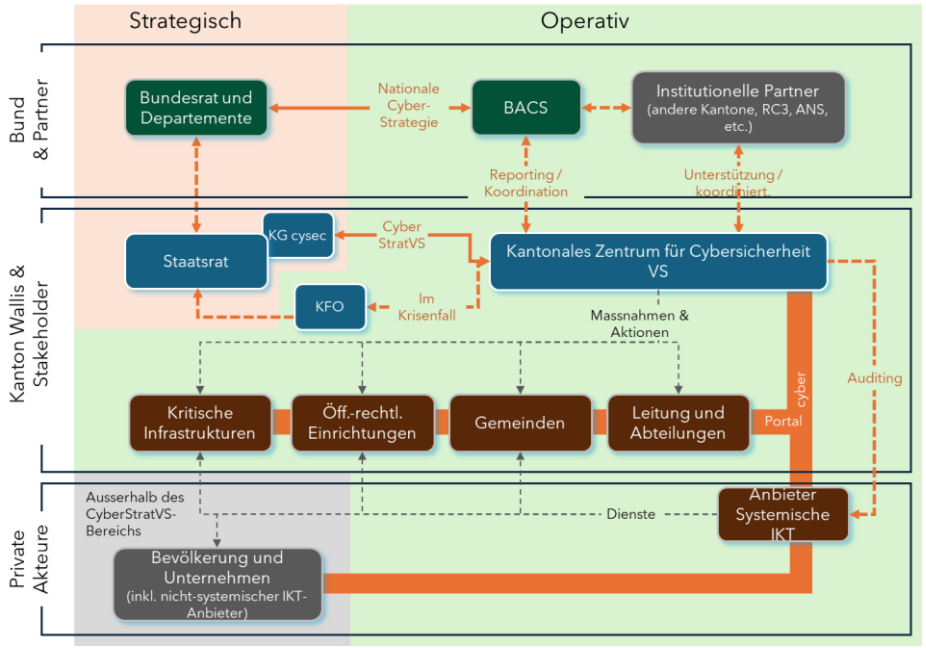



*Abbildung 4 - Rollen und Verantwortlichkeiten im Bereich Cybersicherheit im Wallis*

# 4. Umsetzung

## 4.1. Erfolgsmessung (Schlüsselkennzahlen KPI)

Gemessen werden folgende Leistungsindikatoren (KPI[18] ), **ausgedrückt in % der Anzahl Stakeholder**[19]. Die detaillierte Evaluation wird von der kantonalen Stelle für Cybersicherheit VS festgelegt und durchgeführt.

a. Ernennung von **Cyber-Ansprechpersonen.**
b. Beurteilung des **Reifegrads bezüglich Cybersicherheit** (Ziel: 2.6 von 4 nach den IKT-Minimalstandards).[20]
c. Teilnahme an einem **Label**.
d. Teilnahme der Mitarbeitenden am **Sensibilisierungsprogramm**.
e. Teilnahme der leitenden Organe an **Cyber-Veranstaltungen für Entscheidungsträger**.
f. Anschluss an einen **SOC-Dienst**.
g. Einhaltung der **Leistungsvereinbarungen**.
h. Einbeziehung von Cyberrisiken in die **Risikomatrix**.
i. Vorbereitung auf das **Krisenmanagement.**
j. Durchführung regelmässiger **Audits** bei systemrelevanten Anbietern.

[18] Key Performance Indicator

[19] Auf der Grundlage der Bestandsaufnahme gemäss Massnahme M1.1a

[20] https://www.bwl.admin.ch/de/ikt-minimalstandards .

## 4.2. Ressourcen

Die Konkretisierung der CyberStratVS hängt stark von den Kompetenzen und den zugewiesenen Ressourcen ab. Die KG cysec legt der Regierung auf Vorschlag der kantonalen Stelle für Cybersicherheit VS jährlich ein Budget und eine Roadmap vor, die der Cyberrisikosituation und dem Fortschritt der Arbeiten an CyberStratVS angepasst sind (siehe Ziff. 4.3).

Die folgende Tabelle zeigt die minimalen **jährlichen** Ressourcen auf, zu deren Aufwendung die Stakeholder eingeladen sind, um ihren Vorbereitungszustand zu erhöhen.

| | Kanton Wallis | Gemeinden | staatsnahe / öffentlich-rechtliche Institutionen | Betreiberinnen von kritischen Infrastrukturen |
|---|---|---|---|---|
| **Personal** | ▪ Bestehende Einheiten KDI (Zelle Cybersicherheit), Kantonspolizei (Cybersektion) und andere Einheiten (ComSec usw.).<br>▪ Beiträge des DZSM (u. a. Zivilschutz).<br>Zusätzlich<br>▪ KG Cysec (ca. 4 Sitzungen à 2h / Jahr für Mitglieder).<br>▪ Kantonale Stelle Cysec VS (2 VZÄ). | ▪ Cyberreferent (Aufwand von ca. 5% Pensum für einen Angestellten oder Outsourcing, d.h. ca. 1 Tag/Monat).[21] | ▪ Cyberreferent (ca. 5% Pensum für Cyber-Sicherheitsbeauftragte, d.h. ca. 1 Tag/Monat). | ▪ Cyberreferent (ca. 5% Pensum für Cyber-Sicherheitsbeauftragte, d.h. ca. 1 Tag/Monat). |
| **Budget** | ▪ Materialien und Schulungs- und Sensibilisierungsveranstaltungen (100 KCHF).<br>▪ Prüfungen und Beratungen (70 KCHF).<br>▪ Verschiedene Hilfen und Labeling (50 KCHF).<br>▪ CSIRT-Kapazität (gemäss späterem Konzept - zusätzlicher Betrag) | ▪ SOC-Dienst (gemäss einer noch festzulegenden Strategie).<br>▪ Mindestanforderungen und Labeling (nach Marktpreis). | ▪ SOC-Dienst (gemäss einer noch festzulegenden Strategie).<br>▪ Mindestanforderungen und Labeling (nach Marktpreis). | ▪ SOC-Dienst (nach Marktpreisen)<br>▪ Mindestanforderungen und Labeling (nach Marktpreis). |

[21] Hierbei handelt es sich um einen geschätzten Zeitaufwand im Zusammenhang mit der Rolle der Cyber-Ansprechpartner und der damit verbundenen Koordination. Diese Zeit beinhaltet keinesfalls das gesamte Sicherheitsmanagement der Gemeinde, Institution oder der Betreiberin kritischer Infrastrukturen.

## 4.3. Allgemeiner Fahrplan

Die zur Konkretisierung der von CyberStratVS vorgesehenen Massnahmen und Aktionen sind alle wichtig, aber unterschiedlich dringlich. Der in Anhang 1 dargestellte Fahrplan dient als Ausgangspunkt für jede Massnahme und wird jährlich entsprechend dem Stand der Arbeiten überprüft.

Aus Gründen der Effizienz und Transparenz wird für jede Massnahme eine separate Planung erstellt, die wie folgt gegliedert ist: **Priorität** (Begründung der Wichtigkeit und Priorität), **Produkt** (Definition des Zwecks und der angestrebten Wirkung), **Qualität** (Definition des Anspruchsniveaus), **Absicht** (Definition des "Wie", der Idee, wie das Ziel erreicht werden soll), **Zeit** (Definition des Startpunkts und der Dauer), **Ressourcen** (Angabe der finanziellen und personellen Kosten).

# Anhang 1 - Massnahmen und Aktionen

*Legende*

- *Prioritätsgrad der Massnahmen: ❶= jetzt ❷= später ❸ = zum Schluss.*
- *Zuständigkeit für die Umsetzung der Massnahmen: VS: Kanton Wallis (Kantonales Zentrum für Cybersicherheit VS gemäss Massnahme M4.2b); alle: alle Stakeholder.*
- *Sofern nicht ausdrücklich angegeben, sind die Massnahmen in einem dynamischen und langfristigen Ansatz zu verstehen (z.B. bedeutet "erstellen" auch "nachhaltig nutzen").*

| | |
|---|---|
| 1. WISSEN | **M1.1 - BESTANDSAUFNAHME**<br>a) Stakeholder-Inventar erstellen [❶ / VS]<br>b) Cyberreferenten bei allen festlegen [❶ / alle].<br>c) Inventar der im Wallis tätigen IT-Anbieter und -Experten erstellen [❷ / VS].<br>d) Einschätzung des Reifegrads bezüglich Cybersicherheit der einzelnen Stakeholder erstellen [❸ / VS].<br>e) Inventar der gegenseitigen Abhängigkeiten erstellen [❸ / VS]. |
| | **M1.2 - RISIKOÜBERWACHUNG**<br>a) Eine Überwachung von Cyberrisiken durchführen [❶ / VS].<br>b) Kantonales Management für Cyberrisiken etablieren [❷ / VS]. |
| | **M1.3 – UMGANG MIT VORFÄLLEN**<br>a) Sicherstellen, dass die kantonale Stelle für Cybersicherheit VS (siehe M4.2b) über jeden bedeutenden Cybervorfall, der einen Stakeholder betrifft, informiert wird [❶ / VS].<br>b) Alle signifikanten Vorfälle analysieren und den Stakeholdern ggf. Empfehlungen abgeben [❷ / VS]. |
| 2. KOMPETENZEN | **M2.1 - SENSIBILISIERUNG**<br>a) Interessensgruppen [❶ / VS] Sensibilisierungsunterlagen zur Verfügung stellen, damit sie mit diesem ihre Mitarbeitenden für Cyberrisiken sensibilisieren können [❷ / alle].<br>b) *Für Cyber-Ansprechpersonen* Veranstaltungen zur Sensibilisierung anbieten. [❷ / VS]. |
| | **M2.2 - VERBESSERUNG DER FÄHIGKEITEN VON ENTSCHEIDUNGSTRÄGERN**<br>a) Den Mitgliedern der Gemeindeexekutiven in jeder Legislaturperiode einen Cyber-Informationsworkshop anbieten [❶ / VS].<br>b) Führungskräften der Stakeholder regelmässige Informationsveranstaltungen anbieten [❶ / VS]. |
| | **M2.3 - AUSBILDUNG DER AKTEURE** |

| | |
|---|---|
| | a) Schulung des Personals der verschiedenen Führungsgremien / Krisenstäbe der Stakeholder in den Verfahren und im Umgang mit einem Cybervorfall [❷ / alle].<br>b) Für *Cyber-Ansprechpartner* der Stakeholder spezifische Schulungen anbieten [❷ / VS].<br>c) Unterstützung der Führungsorgane / Krisenstäbe der Stakeholder bei der Integration des Themas Cyber in Übungen [❸ / VS]. |
| | **M2.4 - CYBERPORTAL**<br>Den Stakeholdern folgende Inhalte zur Verfügung stellen (nicht abschliessende und sich entwickelnde Liste) [❶ / VS]<br>• CyberStratVS und ihre Umsetzung;<br>• alle Informationen, Unterlagen und Angebote zur Sensibilisierung / Schulung zum Thema Cyberrisiken;<br>• alle Informationen über die für die Cybersicherheit zuständigen Stellen und die Verfahren im Falle eines Vorfalls;<br>• alle Informationen über die Mindestkriterien, die von den Stakeholdern in Bezug auf die Cybersicherheit erreicht werden müssen;<br>• alle hilfreichen Dokumentationen zu gesetzlichen Grundlagen, Normen, Labels sowie zu Instrumenten zur Selbstbewertung. |
| 3. SCHUTZ | **M3.1 - RAHMEN UND REIFEGRAD**<br>a) Regelmässige Selbstbewertung der Cyber-Maturität durch die Stakeholder [❶ / alle].<br>b) Umsetzung der empfohlenen Mindestmassnahmen (siehe M4.1) durch die Stakeholder [❷ / alle].<br>c) Erlangung eines Labels durch die Beteiligten (gemäss Empfehlung des Kantons oder gleichwertig) [❸ / alle]. |
| | **M3.2 - ANBIETER**<br>a) Festlegung von Mindestanforderungen für im Wallis tätige Dienstleister als Entscheidungshilfe für Stakeholder bei der Vergabe von Aufträgen [❶ / alle].<br>b) Den Stakeholder Musterverträge / Teile von Musterverträgen für IKT-Leistungen zur Verfügung stellen [❶ / alle].<br>a) IT-Anbieter mit systemischer Bedeutung regelmässigen Prüfungen unterziehen [❷ / VS]. |
| | **M3.3 - REAKTION AUF VORFÄLLE** |

| | |
|---|---|
| | a) Kantonale SOC- und CSIRT-Strategie erstellen [❶ / VS].<br>b) Alle Stakeholder an einen SOC anschliessen [❸ / alle].<br>c) Aufbau einer CSIRT-Einsatzfähigkeit (Technik, Recht, Führung usw.) im Falle eines Cybervorfalls [❸ / alle]. |
| 4. ORGANISATION | **M4.1 - REGELWERK**<br>a) Mindestanforderungen an die Cybersicherheit für Stakeholder entsprechend ihrer Wichtigkeit festlegen [❶ / VS].<br>b) Beurteilen, ob es sinnvoll wäre, über ein kantonales Gesetz für die Cybersicherheit zu verfügen [❷ / VS].<br>c) Entwicklung klarer Subsidiaritätsregeln [❷ / VS]. |
| | **M4.2 - ORGANE**<br>a) Schaffung der Koordinationsgruppe für Cybersicherheit [❶ / VS].<br>b) Einrichten einer kantonalen Stelle für Cybersicherheit VS [❶ / VS]. |
| | **M4.3 - KOORDINATION**<br>a) Überwachung der Umsetzung der Massnahmen der Cyber-StratVS [❶ / VS].<br>b) Sicherstellung der Koordination der Aktionen des Kantons Wallis mit dem Bund und den Nachbarkantonen [❶ / VS].<br>c) Den Stakeholdern bei sich bietenden Gelegenheiten die gemeinsame Nutzung von Mitteln oder die Bildung von Einkaufsgemeinschaften für IKT-Güter und -Dienstleistungen im Bereich der Cybersicherheit vorschlagen [❷ / VS]. |


Diese Planung hängt von den Mitteln ab, die für die Umsetzung der Strategie bewilligt werden und kann daher zeitlich nach hinten verschoben werden.

# Anhang 2 - NIST-Architektur

Um die Ziele und Absichten von CyberStratVS zu konkretisieren, müssen sie in Form von Massnahmen umgesetzt werden. Diese müssen streng und überprüfbar nach einem allen Akteuren bekannten und angewandten Schema geordnet werden. Hierfür dient das NIST-Framework, das die folgenden sechs Schlüsselbereiche umfasst


NIST Cybersecurity Framework

**Identify** - Jede Einheit muss über eine umfassende Kartierung ihres Cyberraums / ihrer IKT-Strukturen und ihrer Umgebung verfügen, um ihre Risiken zu verstehen und somit zu definieren, was und mit welcher Priorität geschützt werden muss.

**Protect** - Hierbei handelt es sich um die Gesamtheit aller technischen und nichttechnischen Massnahmen (Organisationen, Prozesse usw.) nach dem Stand der Technik und in einem angemessenen Verhältnis zu den ermittelten Risiken.

**Detect** - Hier geht es darum, wachsam zu bleiben, Massnahmen auf ihre Wirksamkeit hin zu testen, Anomalien zu erkennen und zu melden usw. und schliesslich darum, bei Vorfällen so vorzeitig wie möglich handeln zu können.

**Respond** - Sobald eine Anomalie / ein Cybervorfall oder ein Cyberangriff aufgedeckt wurde, muss sichergestellt werden, dass jede Einheit, die involviert sein muss, so schnell und effektiv wie möglich eingreift, um die Situation unter Kontrolle zu bringen, ihre Ausweitung zu verhindern und ihre Folgen zu minimieren.

**Recover** - Ziel dieser Phase ist es, so schnell wie möglich zu einer sogenannten "normalen" Situation zurückzukehren und aus der Krise zu lernen, damit die gleichen Ursachen nicht mehr die gleichen Wirkungen verursachen können.

**Govern** - Diese Säule der Cybersicherheit ist das Bindeglied der ersten fünf Säulen. Sie legt vor allem die zu erreichenden Ziele und Wirkungen, die dafür vorgesehenen Ressourcen und die Verantwortlichkeiten fest. Ausserdem soll sie ein Gesamtbild der Situation in allen Bereichen vermitteln, die die Situation des Ökosystems, das Gegenstand der Strategie ist, beeinflussen. Dies geht über die reine Informationstechnologie hinaus und umfasst alle relevanten Bereiche (Energie, Personal, Recht, Politik, Lieferketten, Umwelt usw.).

# Anhang 3 - Abkürzungen

| | |
|---|---|
| CLDN | Conférence latine des directeurs du numérique |
| CSIRT | Cyber Security Incident Response Team |
| NCS | Nationale Cyberstrategie |
| CyberStratVS | Cyberstrategie des Kantons Wallis |
| KG cysec | Koordinationsgruppe für Cybersicherheit |
| KPI | Key Performance Indicator (Leistungsindikator) |
| GIDA | Gesetz über die Information der Öffentlichkeit, den Datenschutz und die Archivierung |
| DSG | Bundesgesetz über den Datenschutz |
| GBBAL | Gesetz über den Bevölkerungsschutz und die Bewältigung von besonderen und ausserordentlichen Lagen |
| NDG | Bundesgesetz über den Nachrichtendienst |
| ISG | Bundesgesetz über die Informationssicherheit beim Bund |
| GDDB | Gesetz über die digitalen Dienste der Behörden |
| NEDIK | Netzwerk digitale Ermittlungsunterstützung Internetkriminalität |
| NIST | National Institute for Standards and Technology |
| BACS | Bundesamt für Cybersicherheit |
| KFO | Kantonales Führungsorgan |
| KRO | Kantonales Risikoobservatorium des Kantons Wallis |
| SOC | Security Operations Center |
| IKT | Informations- und Kommunikationstechnik |