SCHWEIZER ARMEE

Kdo Cy · Cdmt Cy · Cdo Ci

Cyberbedrohungen verstehen - Sicherheit stärken

Diego Schmidlin — Lengnau BE, 13. November 2025

Bedrohungen, Sicherheitspolitisches Umfeld

Zeitenwende

- Die westlich geprägte regelbasierte Sicherheitsordnung gerät zunehmend unter Druck.
- Weltweit wird militärisch aufgerüstet. Die militärischen Potentiale nehmen zu.
- Das Sicherheitsumfeld der Schweiz bleibt auf lange Zeit hinaus volatil, unberechenbar und gefährlich.

Bedrohung: Ausrichtung auf militärische Potenziale

- Die Armee verfolgt eine bedrohungsorientierte Streitkräfteentwicklung.
- Bedrohungen entstehen, wenn sowohl militärisches Potenzial vorhanden ist als auch die Absicht besteht, dieses einzusetzen.
- Die strategische Bedrohungsanalyse erfolgt jeweils durch den Sicherheitspolitischen Bericht des Bundesrates.

Aktuelle Trends im Cyberspace

- Cyberspionage und Cyberkriminalität.
- Hacktivismus bei globalen Konflikten.
- Ransomware – doppelte Erpressung.
- Angriffe gestützt mit Künstlicher Intelligenz.
- Angriffe auf vernetzte Lieferketten.
- Quantum Computing.

Cyber Kriminelle

Hochrentable, serviceorientierte Industrie zur Gelderwirtschaftung

Ziele:

- Geschäftsmodell mit hohen Gewinnmargen;
- Erfolgreiche Lieferung an den Auftraggeber;
- Erpressung (Ransomware, DDoS), Identitätsdiebstahl, Kreditkartenbetrug;
- Geringes Risiko der Strafverfolgung.

Organisation:

- Gut organisierte Underground Economy;
- Aufgabenteilung: Auftraggeber – Händler – Akteur;
- Operieren international.

Mittel:

- Einfache Hacks, Zero Day Vulnerabilities;
- Malware Frameworks;
- Darknet, Crypto-Währungen, Moneymules.

Staatlich unterstützte Akteure

Strategischen Vorteil erzielen – politisch, wirtschaftlich, militärisch

Ziele:

- Geopolitische Position verbessern;
- Wirtschaftliche Position stärken;
- Sicherheits- und verteidigungspolitische Interessen durchsetzen;
- Machtposition einnehmen.

Organisation:

- Hervorragend organisiert und geführt;
- Minuziöse, langfristige Planung;
- Operieren auch Hybrid mit anderen Cyber Akteuren.

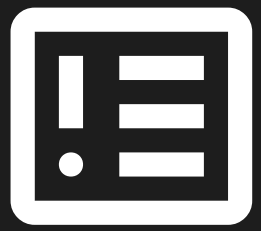
Mittel:

- Top Fähigkeiten, sehr viel Zeit und Geld;
- Auf Ziel zugeschnittene Angriffe;
- Unterstützung durch Nachrichtendienste.

Mögliche Folgen des Krieges für die Schweiz im Cyberbereich

Cyberangriffe und Hacktivismus

eher **wahrscheinlich**



Desinformationskampagnen

wahrscheinlich

Cyberspionage

Sehr **wahrscheinlich**

Anatomie einer Cyberattacke – Cyber Kill Chain

Recon
Informations-sammlung über Angriffsziel.

Weaponization
Ausnutzen einer Schwachstelle mit Schadsoftware.

Delivery
Ausbringen des Angriffspakets (E-Mail, USB-Stick, Webseite usw.).

Exploitation
Zielsystem über Schwachstelle infizieren.

Installation
Brückenkopf bilden, Hintertüren installieren.

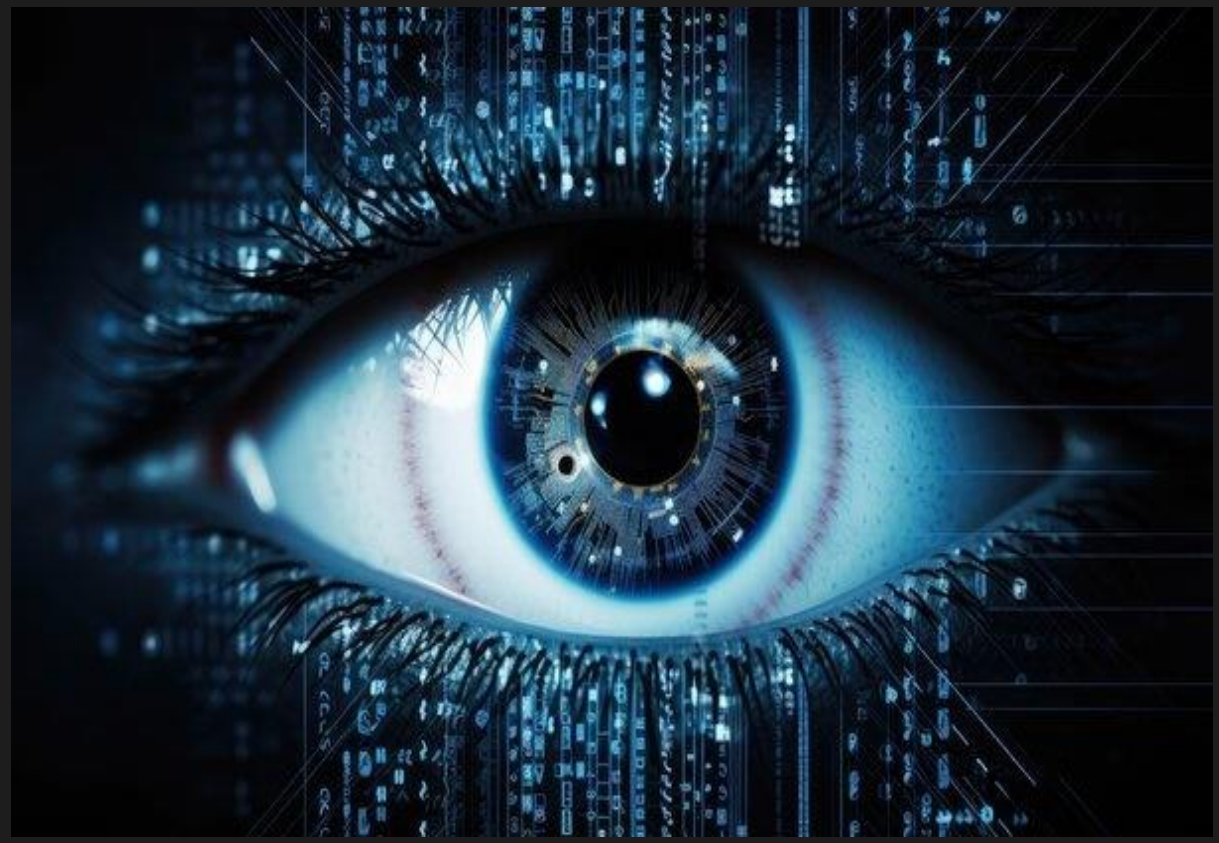
Command & Control
Fernzugriff einrichten. Kontrolle über Opfer.

Action
Angriffsziel erreichen (Stören, Exfiltrieren, Verschlüsseln).

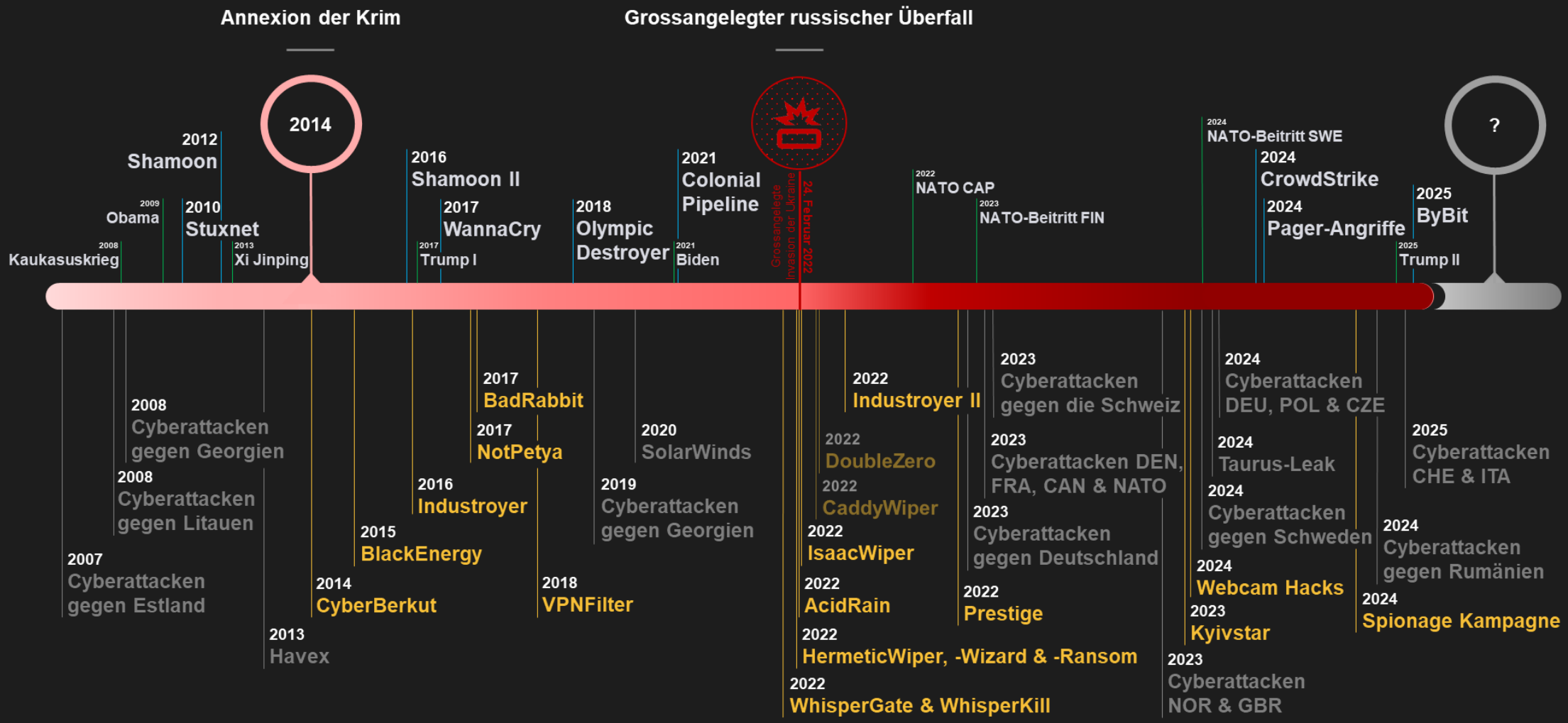
Konkrete Beispiele

Vorfälle:

- RUAG 2016 – Militärische Geheimnisse
- Xplain 2023 – Sensitive Daten
- Apple 2024 – Warnung vor Spyware-Angriffen



Auswirkungen im Cyberraum – Ukraine

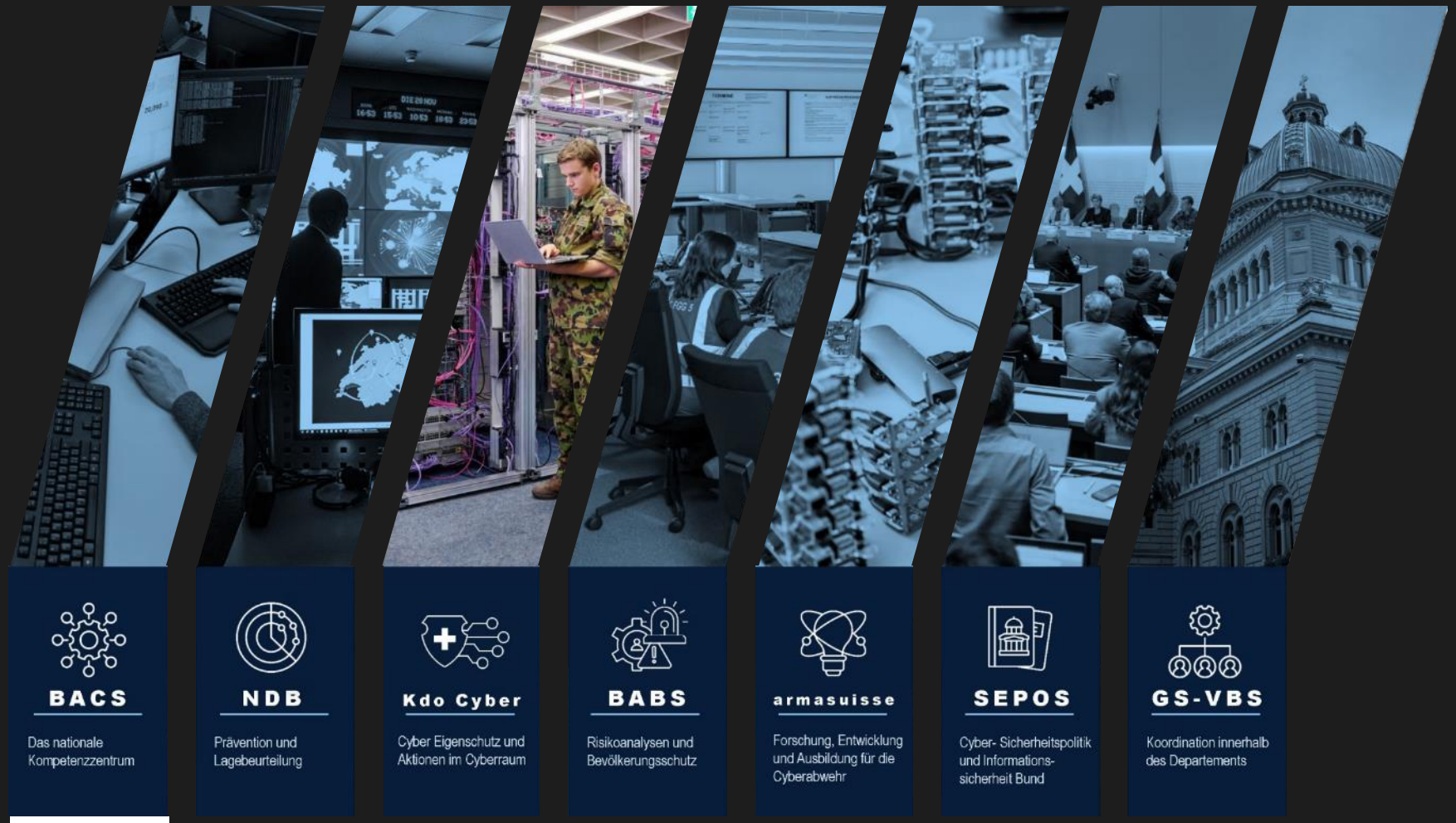


Föderale Zuständigkeiten

Strategischer Kontext der Nationalen Cyberstrategie NCS

- Strategie Digitale Schweiz.
- Nationale Strategie zum Schutz kritischer Infrastrukturen (SKI).
- Bericht des Bundesrates über die Sicherheitspolitik der Schweiz.
- Gesamtkonzeption Cyber der Schweizer Armee.
- Strategie Digitalaussenpolitik.

Cyber Bereiche VBS



Quelle: https://www.vbs.admin.ch/de/cybersicherheit

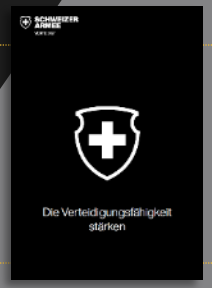
Strategische Ziele der Armee

Nationale Cyberstrategie (NCS)

Departement-übergreifender Cyber-Ansatz

Strategie Cyber VBS

Cyber-Zuständigkeiten innerhalb des VBS



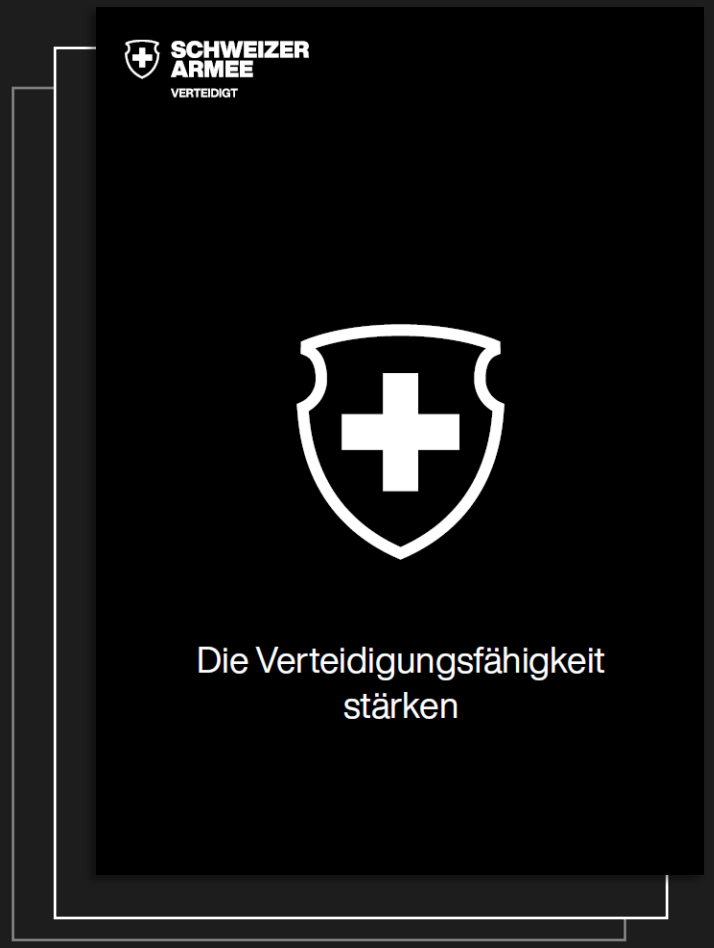
Zielbild und Strategie für den Aufwuchs:
Die Verteidigungsfähigkeit stärken

Fähigkeitsentwicklung Armee

Gesamtkonzeption Cyber

Fähigkeitsentwicklung Cyber

Strategische Ziele im Cyberraum

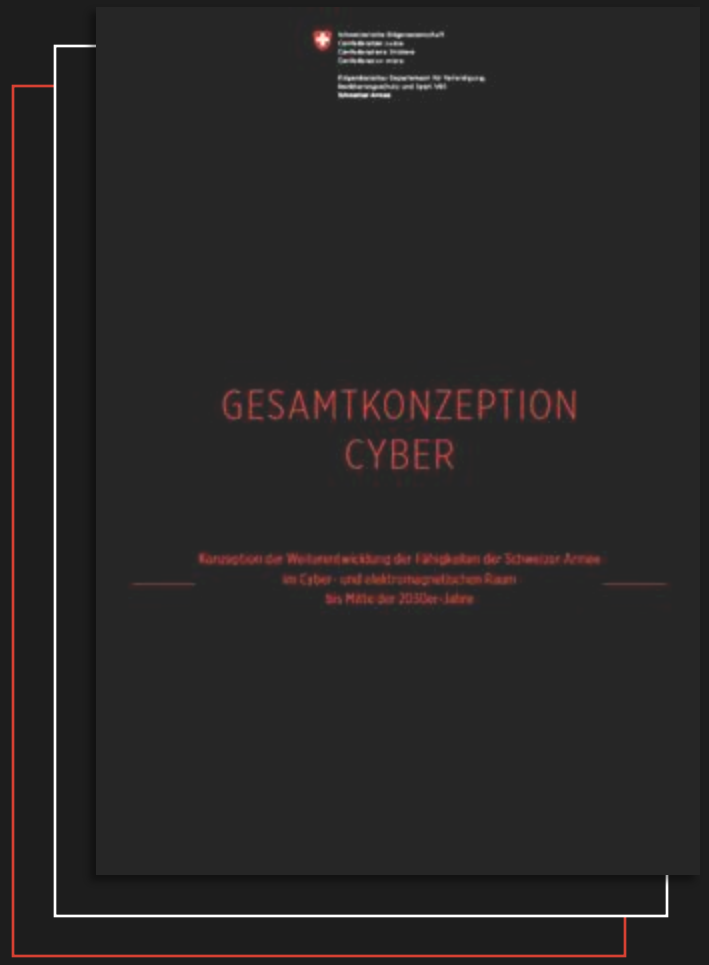


«Wissens- und Entscheidvorsprung über alle Lagen und in allen Wirkungsräumen sicherstellen.

Resilienz der Systeme und die Abwehr von Cyberangriffen auf militärische oder zivile Infrastrukturen gewährleisten.

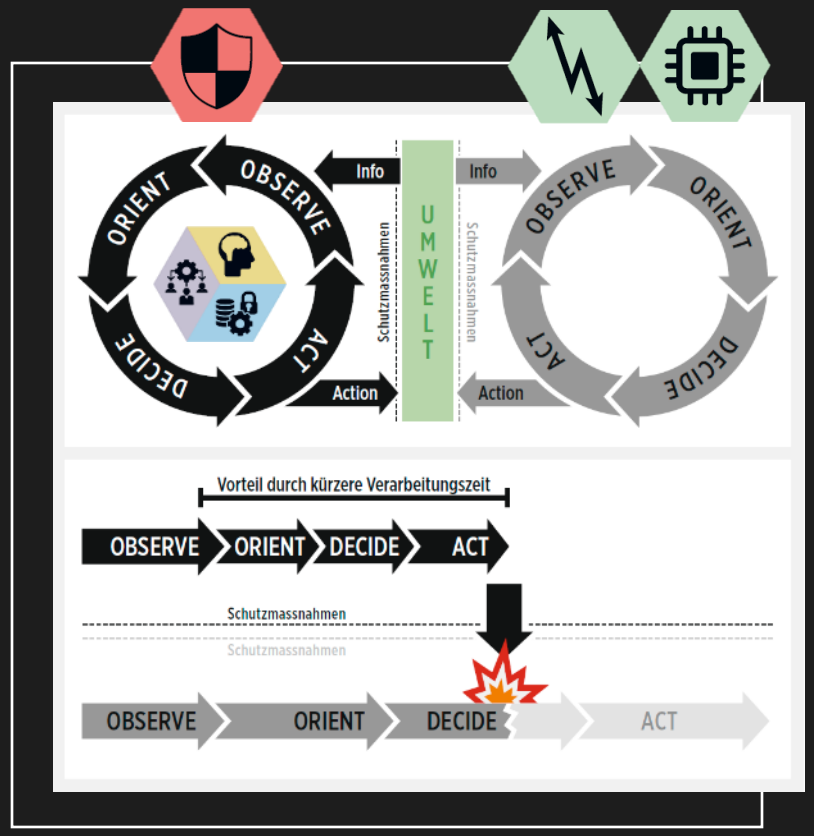
Mit Aktionen im Cyber- und im elektromagnetischen Raum die gegnerische Führungsfähigkeit beeinträchtigen.»

Zielbild und Strategie für den Aufwuchs: Die Verteidigungsfähigkeit stärken



Gesamtkonzeption Cyber

Fähigkeiten der Armee im CER und in der IKT



CER Eigenschutz
Die Truppenverbände, Systeme, Infrastrukturen, Informationen und Netze im CER von Einwirkungen eines gegnerischen Akteurs schützen.

Operationelle Fähigkeiten der Digitalisierung

Lageverständnis im Verbund
Risiken und Bedrohungen identifizieren, den Kontext verstehen und Chancen erkennen – und bei Zusammenarbeit kohärent einschätzen.

Datenverarbeitung robust und sicher
Die Verarbeitung und Verteilung von Daten auftragsbezogen und lagegerecht erstellen.

Führung im Verbund organisatorisch und technisch
Die Führung lagegerecht über alle Stufen und Wirkungsräume sowie im Verbund mit Partnern organisatorisch und technisch sicherstellen.

Aktionen im elektromagnetischen Raum
Aktionen im Em Rm führen.

Aktionen im Cyberraum
Aktionen im Cy Rm führen.

Das Kommando Cyber der Schweizer Armee

Führungsteam

Chef
Kommando Cyber

Divisionär
Simon Müller

Stv. Chef
Kommando Cyber /
Chef Langfristige
Entwicklung

Jean-Claude Brossard

Stabchef
Kommando Cyber

Oberst i Gst
Michail Genitsch

Chef Cyber &
Elektromagnetische
Sicherheit & Abwehr

Diego Schmidlin

Chef Cyber &
Elektromagnetische
Aktionen

Oberst i Gst
Robert Flück

Chef Einsatz IKT

Luca Antoniolli

Kdt FU Br 41

Brigadier
Martino Ghilardi

Chef einsatzkritische
Infrastrukturen &
Luftwaffensysteme

Linus Felder

Kdt Komp Zen FFS

Oberst i Gst
Alexandre Molles

per Q3/25
Pilotphase

Unser Auftrag

Das Kommando Cyber …

- verantwortet die Leistungserbringung im Cyber- und elektromagnetischen Raum (CER). Dies in den Bereichen der Aktionsführung und der einsatzkritischen IKT;
- stellt die Bereitschaft sicher und beurteilt die Machbarkeit in den Operationssphären CER;
- schützt die einsatzkritische IKT-Infrastruktur der Armee im CER;

… zugunsten der Schweizer Armee und ihrer Partner im Sicherheitsverbund Schweiz.

Mission Statement

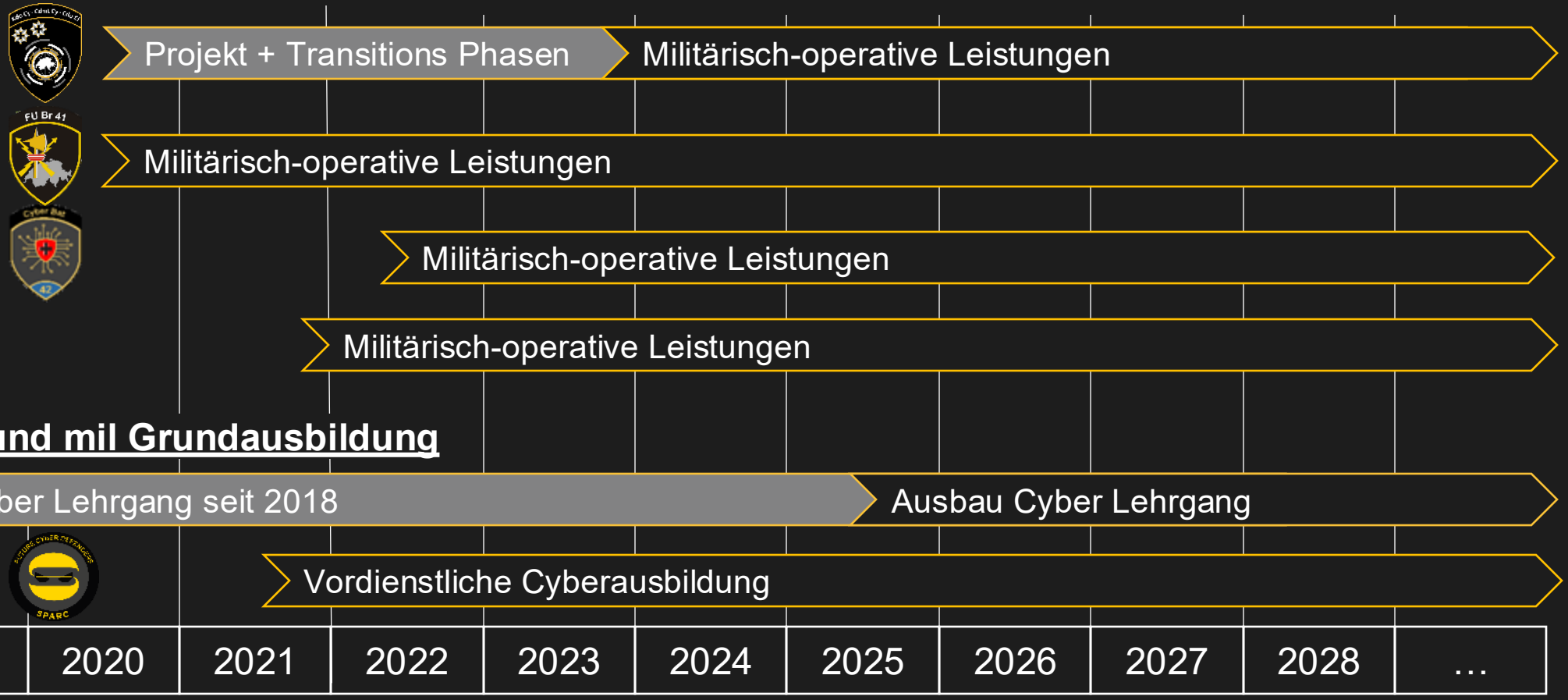
Wir ermöglichen der Armee in allen Lagen den notwendigen **Wissens-** und **Entscheidvorsprung**.

Wir vereinigen **Innovation**, **Technologie**, **Knowhow** und **Begeisterung** für die Auftragserfüllung in einem schlagkräftigen Kommando Cyber der Schweizer Armee.

Wir erbringen die erwarteten und geforderten Leistungen für die Armee, den SVS und Partner immer **präzise**, **auf den Punkt**, **abgestimmt**, **robust** und **sicher**.

Aufbau Kommando Cyber

Berufsorganisation und Miliz



Cyber-Lehrgang der Armee

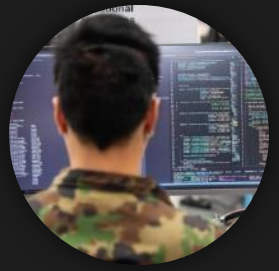
Ausbildungsprogramm

2-stufiges Selektionsverfahren

Sechs Wochen Grundausbildung (260 Stunden): allgemeine und technische Grundlagen

Führungsausbildung

Unteroffiziersschule (UOS) der Armee (90 Stunden)



Fachausbildung

Spezifische Ausbildung (300 Stunden) in einem von drei Bereichen: Computer Network Operations (CNO), Cyber Fusion Center (CFC) oder Cyber Defence (CYD)

Einsatz und Übungen

Praktische Anwendung (ca. 150 Stunden) unter anderem bei Partner (bspw. Swisscom, Post oder kantonale Polizeikorps)

6 WOCHEN

34 WOCHEN

SPARC

Kostenloses Programm für Schweizerinnen und Schweizer ab 16 Jahren, die sich für Cybersicherheit interessieren.

Junge Talente für das Thema Cyber in der Armee begeistern – Vorkenntnisse nicht erforderlich

Individuelle und selbstorganisierte Lernpfade, online und auf Englisch

Austausch innerhalb der Community

Einmalige Gelegenheit, erste Schritte in der Welt der Cybersicherheit zu machen

Facts & Figures

> 700
Mitarbeitende im Kdo Cy

ca. 400
betreute Standorte Fhr Netz Schweiz

11’500
Milizangehörige in der FU Br 41

3
Rechenzentren in Betrieb/Planung

Cyber + EM Sicherheit und Abwehr (CESA)

Auftrag von CESA

Gesamtverantwortung für den CER-Eigenschutz

Schützt und verteidigt Truppenkörper, Infrastrukturen, Informationen, IT-Systeme/Services und Computernetzwerke im CER vor Einwirkungen eines gegnerischen Akteurs

Gliedert sich in vier Sektionen:

- Aktionen CESA
- Special Security Systems
- Chief Security Office
- Cyber Fusion Center

Cyber und Elektromagnetische Sicherheit und Abwehr (CESA)

Diego Schmidlin

Einsatzverfahren CESA – Resilienz

NDB, MND/DPSA
Partner

Cy + Em
OSINT

BACS
govCERT
Partner

CNO
CYD Campus
Supplyer/Industrie

Cy + Em + Phys
Bedrohungen

Actor Intel
Threat Intel
Adversary TTPs

Detektion und
Abwehr von Cyber
Angriffen

Threat
detection

Exploits
Vulnerabilities

Cy + Em + Phys
Schwachstellen

Regelwerk

Gesetze
Policies
Anforderungen
Security Architektur

Info-/IKT-Assets
(Schutzobjekte)

Services/Systeme

	Identify Risks	Assess Risks	Mitigate/Control Risks	
	Strategische Gefahrenanalyse	Strategische Risiken	Strategische Massnahmen-Entwicklung	Strat
	Umsetzung und Kontrolle in der Fähigkeitsentwicklung (Portfolio/HR/FIN)			
	Operative Gefahrenanalyse	Operative Risiken	Operative Massnahmen	Op
	ISMS / Information Security Management System ISO/IEC 27001			
	Taktische Gefahrenanalyse	Taktische Risiken	Taktische Massnahmen	Takt
	Umsetzung und Kontrolle im DevSecOps			

Elemente des Cyber Schutzes – Schweizer Armee

Cyber Analyse: Bedrohungsanalyse, Cyber Threat Intelligence (TTP, IoC);

Vulnerability Management: Schwachstellenanalyse, Penetration Tests, Bug Bounty;

Incident Management: CER-Vorfälle priorisieren, bewerten und bewältigen;

Cyber Operations Center: APP/LV CESA, Teillagebild CER-Eigenschutz;

Informations Sicherheits Management: Vorgaben, Compliance, ISMS;

Awareness/Ausbildung: E-Learning, Sicherheits-Ausbildung/-Zertifikate, Übungen;

Security Operations Center: SIEM, Threat Detection/Response;

Computer Emergency Response Team: Threat Hunting, E-Forensik;

Lauschabwehr: Detektion von Abhöreinrichtungen, Schutz vor Em Wirkung und Abstrahlung.

Vorbereitung auf einen erfolgreichen Cyberangriff

- Seine Kronjuwelen kennen und schützen;
- Community Bildung – Branchenspezifisch;
- Fachliche Vernetzung;
- Eigene ausgeprägte Cyberfähigkeiten / Managed Cyber Security Services;
- Krisen-/Notfallpläne.

Tips für den Cyberschutz

- **Starke Passwörter:** Nutzen Sie für jeden Dienst ein individuelles und starkes Passwort. Ein Passwort-Manager kann dabei helfen.
- **Zwei-Faktor-Authentifizierung (2FA):** Aktivieren Sie 2FA, wo immer möglich.
- **Software-Updates:** Installieren Sie Updates für Betriebssysteme und Programme umgehend.
- **Datenschutz-Tools:** Nutzen Sie beim Web-Surfen Werbe- und Tracker-Blocker
- **Vorsicht bei E-Mails:** Seien Sie bei Links und Anhängen in E-Mails besonders vorsichtig und klicken Sie nicht unbedacht darauf.
- **Datensicherungen:** Sichern Sie Ihre wichtigen Daten regelmäßig und bewahren Sie eine Sicherung offline auf.
- **Kontobewegungen prüfen:** Überwachen Sie regelmäßig Ihre Bank- und Kreditkartenumsätze auf ungewöhnliche Abbuchungen.
- **Datenschutz-Check:** Überprüfen Sie mit Diensten wie dem Identity Leak Checker, ob Ihre E-Mail-Adresse in Datenlecks aufgetaucht ist.

Wertvoller Link: S-U-P-E-R.ch

SCHWEIZER ARMEE

VERTEIDIGT

Diego Schmidlin
Schweizer Armee – Kdo Cyber
Chef Cyber + Elektromagnetische Sicherheit und Abwehr
Stauffacherstrasse 65, CH-3003 Bern
+41 58 483 61 95
diego.schmidlin@vtg.admin.ch