SCHWEIZER ARMEE

SPIK 2025 – Cybersicherheit der Schweizer Armee neu gestalten

Diego Schmidlin — Bern, 26. März 2025

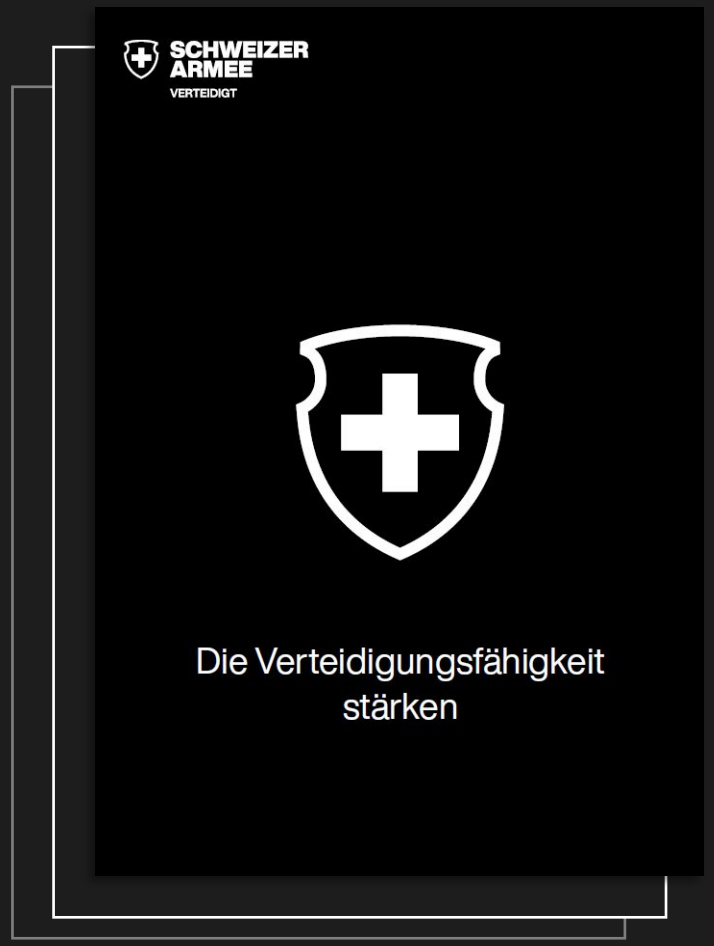
Zeitenwende

- 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.

Aktuelle Trends im Cyberspace

- Cyberspionage und Internetkriminalität.
- Hacktivismus bei globalen Konflikten.
- Ransomware – doppelte Erpressung.
- Angriffe gestützt mit Künstlicher Intelligenz.
- Angriffe auf vernetzte Lieferketten.
- Ausnutzung der Schwachstellen bei IoT/OT.
- Quantum Computing.

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.

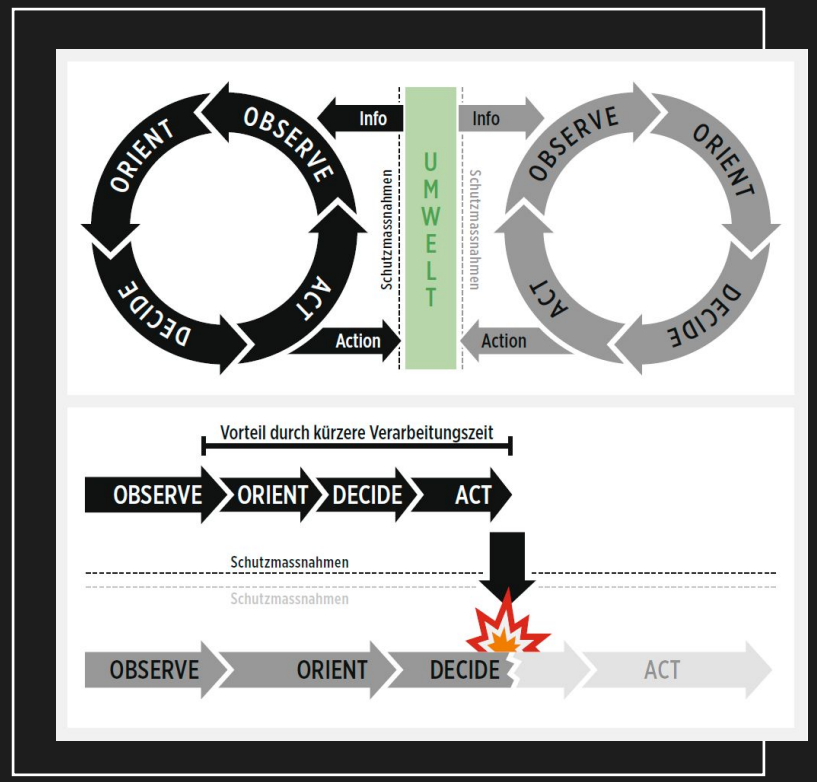
Mit Aktionen im Cyber- und im elektromagnetischen Raum die gegnerische Führungsfähigkeit beeinträchtigen.»

Zielbild und Strategie für den Aufwuchs: Die Verteidigungsfähigkeit stärken

Paradigmenwechsel
Vorbereitung auf einen erfolgreichen Cyberangriff

- Sie sind das Ziel!
- Silent Warefare: Wirkung aus dem Cyberspace auf Gesellschaft und Wirtschaft.
- Cyber in militärischen Operationen – Der Multi-Domain-Ansatz.
- Resilienz statt reines Risikomanagement.

Gesamtkonzeption Cyber – Fähigkeiten der Armee



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.

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

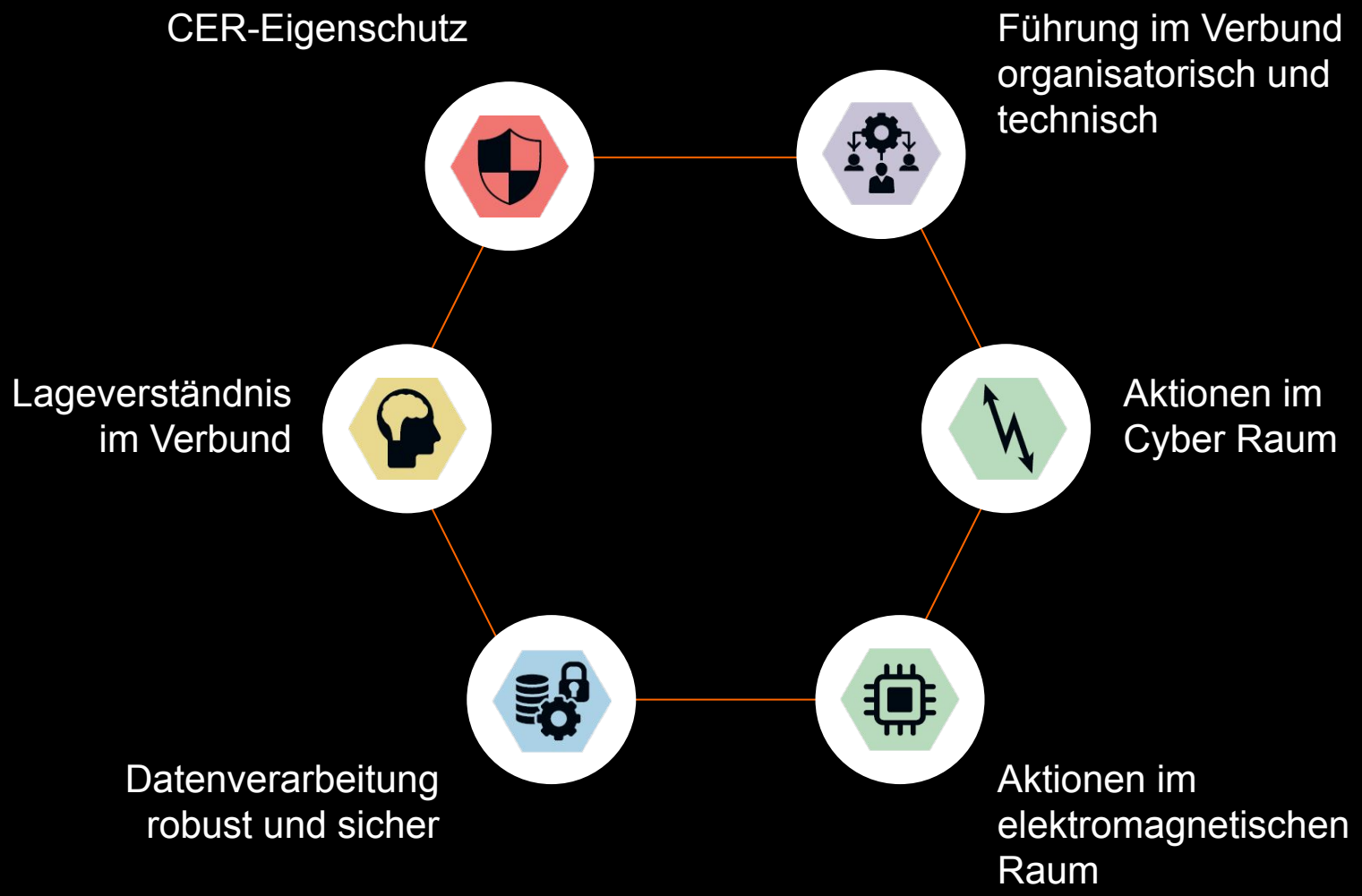
Cybersicherheit der Schweizer Armee neu gestalten

eraneos

Adrian Marti, Partner, Eraneos

Bedarf Cyber Fähigkeiten

Die Gesamtkonzeption Cyber ermöglicht den Schutz der IKT-Infrastruktur der Schweizer Armee vor Bedrohungen aus dem Cyber- und elektromagnetischen Raum



eraneos

Sicherheitsstrategie Kdo Cy

7 Handlungsfelder

41 Elemente

- → Steuerung, IKT-Sec Architektur, Risiko Mgmt
- → Wissensmanagement, Awareness
- → Partner, Leistungsbezüger
- → Schutzbedarf, IT Service Continuity
- → Schutzobjekte, Schwachstellen, Incident Mgmt
- → Objekte, Anlagen, Geräte, Versorgung
- → Gesundheit, Personensicherheit

eraneos

Umsetzung Sicherheitsstrategie

Ausgangslage

→ Sicherheitsstrategie

→ Beurteilung Maturität Cybersicherheit

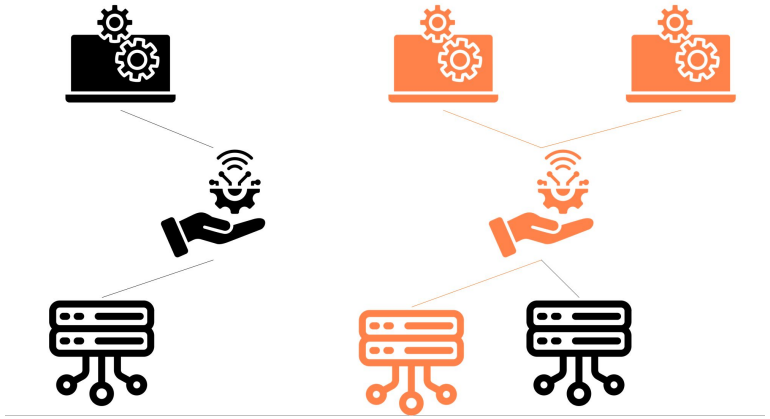
Beitrag zur Zielerreichung

Welche Massnahmen sind prioritär umzusetzen

5 Massnahmen entscheidend

61 Massnahmen total

Verknüpfung IKT Asset – End User Anwendung

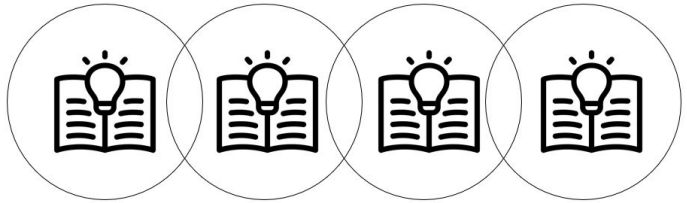


Dashboards zur risikobasierten Führung

Auf operativer, taktischer und strategischer Ebene

Fachführung

Erschliessung von Expertenwissen



Ausblick

→ Umsetzung Massnahmen
  – organisatorisch
  – technisch

→ Regelmässige Überprüfung

→ Iterative Verfeinerung

eraneos

Ihr Kontakt

- **Adrian Marti**
  Eraneos Switzerland AG

Head Cyber Security Public Clients
Andreasstrasse 11, CH-8005 Zürich
+41 58 411 97 67
adrian.marti@eraneos.com