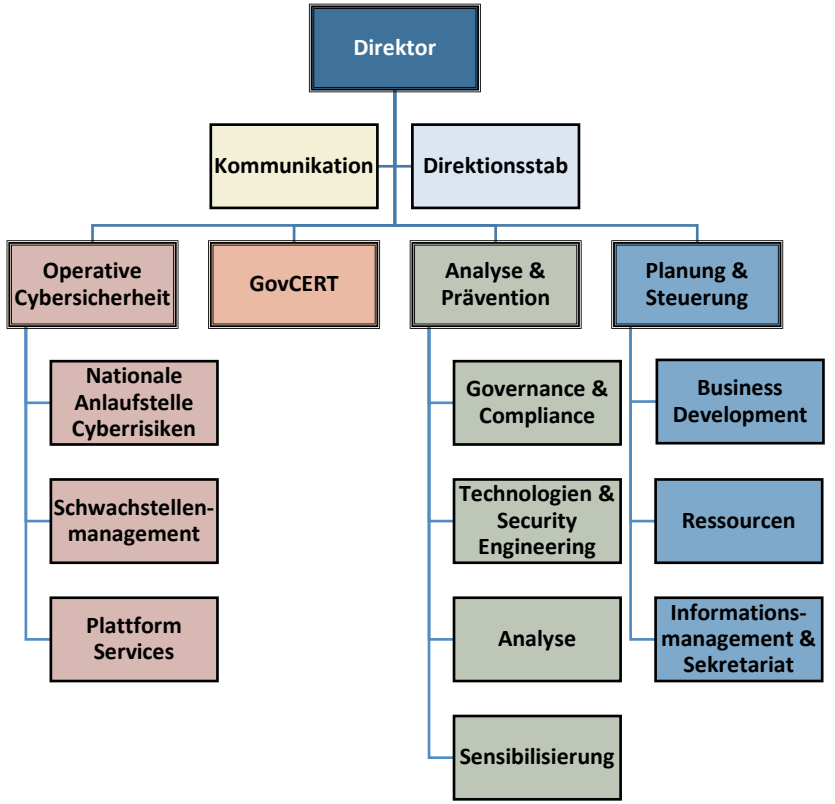
Nationale Cybersicherheitsstrategie

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS

Das Bundesamt für Cybersicherheit NCSC

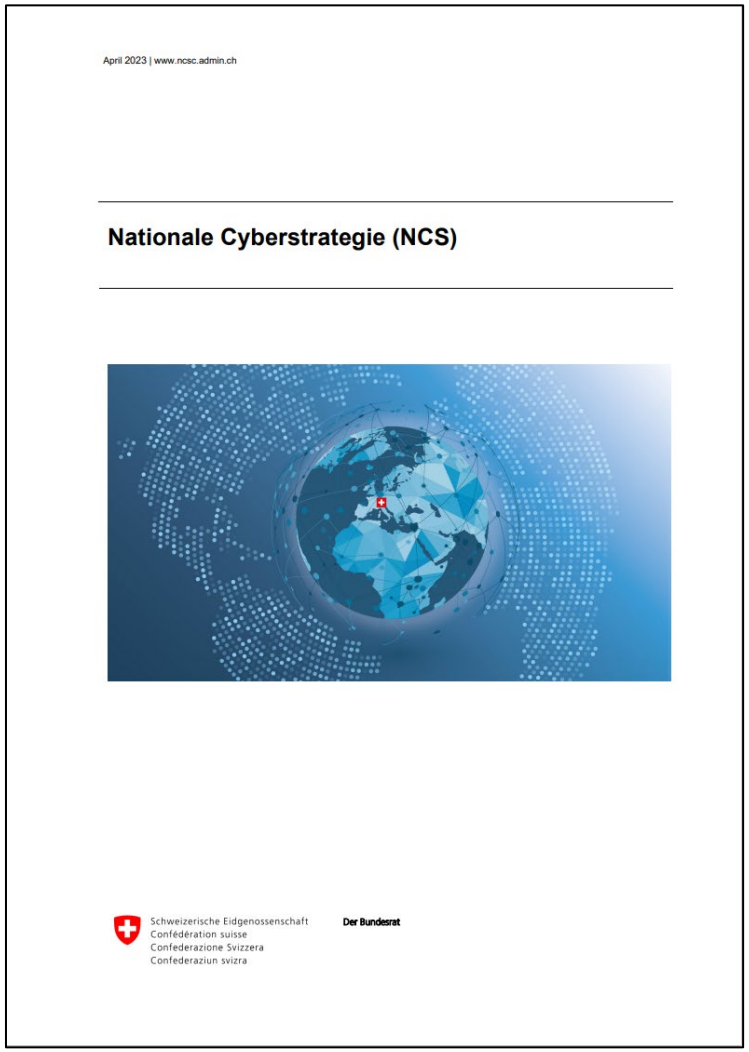
Das BACS verfügt über 67 Mitarbeitende und ein Budget von 16,1 Mio. CHF (2025)

Hauptaufgabe des BACS ist es, die Schweiz im Cyberraum sicherer zu machen. Hierzu sensibilisiert und warnt es die Öffentlichkeit vor Cyberbedrohungen und Cyberangriffen. Das BACS nimmt Meldungen zu Cybervorfällen entgegen und unterstützt insbesondere Betreiberinnen von kritischen Infrastrukturen bei der Bewältigung. Es erstellt technische Analysen zur Bewertung und Abwehr von Cybervorfällen und Cyberbedrohungen sowie zur Identifikation und Behebung von Schwachstellen beim Schutz der Schweiz vor Cyberbedrohungen.



NCS ab 2023

- Grundsatzentscheid des Cyber-Ausschusses des BR: die Strategie wird nicht mehr befristet
- Anpassungen werden nach Bedarf gemacht
- Review alle fünf Jahre



https://www.ncsc.admin.ch/ncsc/de/home/strategie/cyberstrategie-ncs.html

Vorgehen zur Strategieentwicklung

Grob-konzept

- Grundstruktur
- Vision und strategische Ziele

Workshops

- Identifikation der Massnahmen für die Ziele
- Einbezug der Wirtschaft, Hochschulen und Kantone

Konsul-tation

- Breite Konsultation der interessierten Stellen (insbes. Kantone)
- Konsultation der betroffenen Ämter

Beschluss

- 5. April 2023: Beschluss durch den Bundesrat
- 13. April 2023: Beschluss durch die Kantone (KKJPD)

Nationale Cyberstrategie (NCS)

	5 strategische Ziele	17 Massnahmen
	Selbstbefähigung	M1: Bildung, Forschung und Innovation in der Cybersicherheit M2: Sensibilisierung M3: Bedrohungslage M4: Analyse von Trends, Risiken und Abhängigkeiten
	Sichere und verfügbare digitale Dienstleistungen und Infrastruktur	M5: Schwachstellen erkennen und verhindern M6: Resilienz, Standardisierung und Regulierung M7: Ausbau der Zusammenarbeit zwischen den Behörden
	Wirksame Erkennung, Verhinderung, Bewältigung und Abwehr von Cyberangriffen	M8: Vorfallmanagement M9: Attribution M10: Krisenmanagement M11: Cyberdefence
	Effektive Bekämpfung und Strafverfolgung der Cyberkriminalität	M12: Ausbau der Zusammenarbeit der Strafverfolgungsbehörden M13: Fallübersicht M14: Ausbildung der Strafverfolgungsbehörden
	Führende Rolle in der internationalen Zusammenarbeit	M15: Stärkung des digitalen internationalen Genfs M16: Internationale Regeln im Cyberraum M17: Bilaterale Zusammenarbeit zu strategischen Partnern und internationalen Kompetenzzentren

Ableitung auf Stufe Organisation - BACS

1 Cyberbedrohungen verständlich machen

Das BACS macht die komplexen Zusammenhänge, die zu Cyberbedrohungen führen, zielgruppen-gerecht verständlich. Damit ermöglicht es einen fundierten Dialog zwischen Politik, Wirtschaft und Gesellschaft über Cybersicherheit und befähigt alle, ihre individuelle Verantwortung so wahr-zunehmen, dass die systemischen Risiken sinken.

2 Mittel zur Verhinderung von Cyber-angriffen zur Verfügung stellen

Das BACS reduziert die Angriffsfläche von Schweizer Personen und Organisationen im Cyberraum.
Es warnt vor Angriffen und stellt Informationen sowie gegebenenfalls technische Instrumente zur Verfügung, die deren Verhinderung erleichtern.

3 Schäden aus Cybervorfällen reduzieren

Das BACS hilft Betroffenen von Cybervorfällen, Schäden zu reduzieren und das Risiko einzugrenzen, dass Vorfälle sich auf weitere Opfer ausweiten.

4 Sicherheit von digitalen Produkten und Dienstleistungen erhöhen

Das BACS fördert ökonomische Modelle und schafft Anreize für Hersteller, sichere und erschwingliche Produkte und Dienstleistungen anzubieten. Es fördert die Tranparenz für Nutzer, sodass sie informierte Entscheide über die Cybersicherheit von Produkten und Dienstleistungen treffen können.

NCS Umsetzung

- Der Steuerungsausschuss NCS wird neu gewählt und trägt die Verantwortung für die Umsetzung.
- Zusammensetzung: Expertinnen und Experten aus Kantonen, Wirtschaft, Hochschulen und Bund. Keine direkte Vertretung der Massnahmenverantwortlichen.
- Der Steuerungsausschuss erarbeitet zusammen mit den Umsetzungsverantwortlichen eine Planung (Roadmap) für die Massnahmen.
- Der Steuerungsausschuss kontrolliert die Umsetzung und beschliesst wenn nötig zusätzliche oder ergänzende Massnahmen.

Der Steuerungsausschuss

- 2012 – 2017: Alle an der NCS-Umsetzung beteiligten Verwaltungseinheiten des Bundes ➔ bundesinternes Koordinationsgremium
- 2018 – 2022: Ergänzung mit Vertretungen der Kantone, Wirtschaft, Hochschulen ➔ nationales Koordinationsgremium
- 2024: Paritätische Zusammensetzung zwischen verwaltungsexternen und verwaltungsinternen Vertretungen ➔ Steuerungsgremium

---

- Rechtliche Grundlagen über neue Cybersicherheitsverordnung (CSV)

Aufgaben StA NCS

- Überprüft die NCS mindestens alle fünf Jahre, wirkt bei ihrer Weiterentwicklung mit und erarbeitet bei Bedarf Anpassungsvorschläge.
- Erarbeitet in Absprache mit den in der NCS aufgeführten Akteuren Vorschläge für die Prioritäten und Zeitpläne für die Umsetzung der Massnahmen der NCS.
- Beurteilt laufend die Umsetzung der Massnahmen und informiert den Bundesrat und die Kantone über Verzögerungen.
- Unterbreitet dem Bundesrat bei Bedarf Vorschläge für ergänzende Massnahmen.
- Erstattet dem Bundesrat, den Kantonen und der Öffentlichkeit jährlich Bericht über die Umsetzung der NCS.

Der Steuerungsausschuss- ein diverses Gremium

Gäste:

- Florian Schütz
- Manuel Suter
- Administrative Unterstützung

Zusätzliche Gäste je nach Thema

Umsetzungsmonitoring

Bericht zur Umsetzung der Nationalen Cyberstrategie

Steuerungsausschuss NCS

Mai 2025

4.5 Strategisches Ziel 5: Führende Rolle len Zusammenarbeit

Die Cybersicherheit ist angesichts der Cyberbedrohungslag gen zu einem wichtigen aussenpolitischen Thema geworder beit ist unerlässlich, um Cyberrisiken zu verringern und die a schen Interessen der Schweiz zu schützen. Die Schweiz wil teur in der globalen Cybersicherheitsdiplomatie stärken. Die tung der internationalen Zusammenarbeit, Respekt des Völk globaler Cybersicherheitsnormen. Die diplomatische Präsen Genf, wird genutzt, um multilaterale Cyberdiskussionen zu e

4.5.1 Stand der Umsetzung

Verstärkung der grenzüberschreitenden Zusammer bersicherheit

Die partnerschaftliche Zusammenarbeit mit Cybersicherheits wurde weiter aufgebaut, um den Austausch von Bedrohungs wissen ermöglichen. Die technischen und operativen Abteilu auch bilaterale Beziehungen oder sind Teil multilateraler Gr GovCERT (EGC)-Gruppe und des International Watch and Cybersicherheitsbehörden aus 16 Ländern umfasst.

2024 fand in Washington DC das vierte jährliche Gipfeltreffe Ransomware Initiative (CRI) statt. Diese vom Weissen Haus zwischen 68 Mitgliedstaaten, darunter auch die Schweiz. Di kollektive Widerstandsfähigkeit gegen Ransomware zu entw bei Ransomware-Angriffen zu unterstützen. Zur Unterstützu BACS einen internationalen Überblick und bewährte Praktik Ransomware-Vorfällen sowie einen Vorschlag für die standa Informationen. 2024 haben die Mitglieder der CRI einen Leit von Ransomware betroffen sind, herausgegeben. Der Leitfa schen Behörden abgerufen werden.[36]

4.5.2 Ausblick des Steuerungsausschuss NCS

Als neutrale Nation mit starkem Engagement für internationale Zusammenarbeit, insbesondere durch Genfs Rolle als Zentrum für multilaterale Gespräche, ist die Schweiz gut positioniert, eine führende Rolle in der Cybersicherheit zu spielen. Der Schwerpunkt liegt auf der Entwicklung und Stärkung internationaler Partnerschaften, um sich als Vermittlerin in der globalen Governance der Cybersicherheit zu etablieren. Initiativen wie die Digital Geneva Initiative und der Geneva Dialoge fördern die Cyberdiplomatie auf der globalen Agenda.

Durch breitere politische Strategien und die Umsetzung der NCS will die Schweiz optimale Bedingungen für internationale Organisationen und NGOs schaffen, auch im Hinblick auf Cyber-Angriffe. Initiativen wie das internationales Genf Cyber-Sicherheitszentrum (IG-CSC) bieten proaktive und reaktive Unterstützung und steigern den Wert der Schweiz als Standort für internationale Organisationen und humanitäre Organisationen.

Die Herausforderung besteht darin, nationale und internationale Interessen in Ein-klang zu bringen und Vertrauen zwischen den Beteiligten zu fördern. Cybersicherheit ist zunehmend mit geopolitischen Spannungen verwoben, und die Schweiz muss diese komplexen Zusammenhänge bewältigen. Der internationale Rechts-rahmen für Cyber-Normen und Durchsetzungsmechanismen entwickelt sich weiter, und die Schweiz sollte die Diskussionen aktiv mitgestalten.

Zukünftig wird es entscheidend sein die bilateralen Partnerschaften im Bereich Cybersicherheit weiter auszubauen, sich weiter in den Prozessen internationaler Organisationen und Initiativen zu engagieren, sich für die Einhaltung und Durchsetzung des Völkerrechts einzusetzen, und das verantwortungsvolles Staatenverhalten im Cyberraum weiter zu fördern. Durch einen proaktiven und strategischen Ansatz kann die Schweiz ihre Rolle als globale Führungsmacht in der Cybersicherheitsdiplomatie und -Governance festigen.

Fragen