

Bericht zur  
Umsetzung der Nationalen  
Cyberstrategie (NCS)  
2025





Vorwort . . . . .	2
Executive Summary . . . . .	4
Einleitung . . . . .	6
Kennzahlen zur Umsetzung der NCS. . . . .	7
<b>Strategisches Ziel 1:</b> Selbstbefähigung. . . . .	9
<b>Strategisches Ziel 2:</b> Sichere und verfügbare digitale Dienstleistungen und Infrastruktur . . . . .	12
<b>Strategisches Ziel 3:</b> Wirksame Erkennung, Verhinderung, Bewältigung und Abwehr von Cyberangriffen . . . . .	16
<b>Strategisches Ziel 4:</b> Effektive Bekämpfung und Strafverfolgung der Cyberkriminalität . . . . .	20
<b>Strategisches Ziel 5:</b> Führende Rolle in der internationalen Zusammenarbeit. . . . .	22
Kommentar des Steuerungsausschusses . . . . .	24
Exkurs: Künstliche Intelligenz (KI) im Fokus . . . . .	26
Anhänge . . . . .	30



## Vorwort

In einer Zeit, die von geopolitischer Unsicherheit und Konflikten geprägt ist und in der Sicherheit nicht mehr als selbstverständlich gilt, gewinnt die Nationale Cyberstrategie (NCS) an Bedeutung. Cybersicherheit ist eine Grundlage für den Wirtschaftsstandort Schweiz, für unseren Wohlstand und für unsere direkte Demokratie.

Sind wir mit den richtigen Massnahmen unterwegs, um diesen Herausforderungen zu begegnen? Wie steht es um die digitalen Abhängigkeiten der Schweizer Wirtschaft und Verwaltung? Welche Rolle spielen neue Technologien? Das sind zentrale Fragen, die wir uns im aktuellen Umfeld stellen müssen. Der Steuerungsausschuss hat deshalb begonnen, die Strategie entlang verschiedener Themenfelder zu überprüfen.

Im Bereich Cybersicherheit gehört es oft zum guten Ton, den Fokus auf Bedrohungen und Vorfälle zu legen – ein sicherer Weg, Aufmerksamkeit zu erzeugen. Von diesem Reflex möchte ich bewusst Abstand nehmen. Die Vision der NCS zielt nicht nur auf Verteidigung ab, sondern hat auch einen positiven Anspruch: «Die Schweiz nutzt die Chancen der Digitalisierung und mindert Cyberbedrohungen und deren Auswirkungen durch geeignete Schutzmassnahmen.»

Die Chancen der Digitalisierung zu nutzen, lässt sich auf zwei Arten verstehen. Erstens bedeutet es, dass Einwohnerinnen und Einwohner, Wirtschaft und Verwaltung die Digitalisierung nutzen, um besser, schneller und vielseitiger zu werden und damit Wohlstand sowie Entwicklung langfristig zu sichern.

Zweitens eröffnen sich Chancen, die über die Nutzung digitaler Technologien hinausgehen: Die Schweiz kann sich selbst zu einem bedeutenden Standort für Cybersicherheit im internationalen Kontext entwickeln. Wie wäre es, wenn die Schweiz künftig nicht nur für Schokolade und Käse, sondern auch für herausragende Leistungen im Bereich Cybersicherheit bekannt wäre?

### Was heisst das konkret?

Als kleiner, neutraler Staat mit einer langen diplomatischen Tradition, hoher Rechtssicherheit, Innovationskraft und hervorragend ausgebildeten Fachkräften in Cybersicherheit und Cyber Policy ist die Schweiz prädestiniert dafür,

- Organisationen, die für das Funktionieren und die Sicherheit des Internets zentral sind, einen sicheren und langfristigen Standort zu bieten,
- eine stärkere Rolle in der internationalen Cyberdiplomatie und (Cyber-)Mediation einzunehmen,
- und eine führende Nation in der Entwicklung von Technologien im Bereich Cybersicherheit zu werden.

Das bedeutet für mich, Chancen zu nutzen – im Kleinen wie im Grossen – und die Schweiz auf eine sichere und prosperierende Zukunft auszurichten.

Im hier vorliegenden Bericht erläutern wir die Fortschritte in der Umsetzung der NCS. Es gibt aber auch einige inhaltliche Neuerungen:

**Erstens** stellt der Steuerungsausschuss den einzelnen strategischen Zielen jeweils ein kurzes Zielbild voran, das das angestrebte Ambitionsniveau der Umsetzung beschreibt.

**Zweitens** werden ausgewählte Daten und Kennzahlen hervorgehoben, um die Umsetzung und Wirkung der NCS anschaulich zu illustrieren.

Und **drittens** ist ein eigenes Kapitel der Thematik der künstlichen Intelligenz gewidmet.

Der Bericht ist bewusst kompakt gehalten und soll dennoch die thematische Vielfalt der NCS abbilden. Vor diesem Hintergrund kann es stellenweise zu thematischen Wechseln ohne ausführliche Überleitungen kommen, da auf Verbindungselemente zugunsten einer prägnanten Darstellung bewusst verzichtet wurde.

Ich wünsche eine anregende Lektüre des Berichts zur Umsetzung der NCS 2025.

**Dr. Maya Bundt**

*Präsidentin des Steuerungsausschusses der Nationalen Cyberstrategie*

# Executive Summary

Die Umsetzung der NCS wurde im Jahr 2025 in einem von geopolitischer Unsicherheit, fortschreitender Digitalisierung und wachsenden digitalen Abhängigkeiten geprägten Umfeld substanziell weitergeführt. Der Bericht zeigt, dass in allen fünf strategischen Zielbereichen wesentliche Fortschritte erzielt werden konnten.

Im Bereich der Selbstbefähigung wurden 2025 weitere Initiativen umgesetzt. Der Cyber Defence Campus der armasuisse (CYD Campus) setzte sein Fellowship-Programm fort, förderte innovative, anwendungsnahe Lösungen im Rahmen der Cyber Startup Challenge und gewann mit einem Hackathon im Bereich Gebäudeautomation zusätzliche Erkenntnisse zur Stärkung der Cybersicherheit. Im Bereich der Aus- und Weiterbildung wurde gemeinsam mit FIRST ein Pilotprojekt mit Schulungstagen zum Thema Ransomware im Gesundheitssektor durchgeführt. Die Sensibilisierungsaktivitäten wurden mit dem Relaunch der S-U-P-E-R-Website und der Kampagne «Keine Ausreden – machen!» weiter ausgebaut; die Reichweite konnte gegenüber 2024 deutlich gesteigert werden. Ergänzend wurden Formate für junge Zielgruppen sowie Unterstützungsangebote für Gemeinden umgesetzt. Fortschritte wurden auch beim gemeinsamen Lageverständnis erzielt: An den zweiwöchentlichen Lagebesprechungen des Bundesamtes für Cybersicherheit (BACS) nahmen durchschnittlich 400 Fachleute aus kritischen Branchen teil. Die grösseren Schweizer CERTs tauschten sich zudem operativ nahezu täglich über Vorfälle aus und teilten Informationen zur gemeinsamen Abwehr von Angriffen.

Im Bereich der sicheren und verfügbaren digitalen Dienstleistungen und Infrastrukturen wurde mit der Inkraftsetzung der Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen per 1. April 2025 ein zentraler Meilenstein erreicht. Bis Ende Jahr wurden 222 Meldungen registriert. Gleichzeitig wurde die sektorspezifische Zusammenarbeit weiter ausgebaut, namentlich mit der Gründung des Rail-ISAC (Information Sharing and Analysis Center), dem Aufbau des Healthcare Cyber Security Center (Health-CSC) sowie der vertieften Zusammenarbeit mit dem Swiss Financial Sector Cyber Security Center (FS-CSC). Weitere Fortschritte wurden beim Schwachstellenmanagement erzielt: Der Bundesrat beschloss die Ausarbeitung einer Vorlage zur

Cyberresilienz digitaler Produkte; das BACS begleitete koordinierte Offenlegungen von Schwachstellen; das Nationale Testinstitut für Cybersicherheit (NTC) führte verschiedene technische Tests durch; und das Bug-Bounty-Programm der Bundesverwaltung führte erneut zu konkreten Sicherheitsverbesserungen. Zudem wurden mit CyberSeal, Cyber-Safe und der Entwicklung der Cybersicherheits- und Resilienzmethode (CSRM) zusätzliche Instrumente zur Stärkung des Selbstschutzes geschaffen. Auch die Zusammenarbeit zwischen Bund, Kantonen und Gemeinden wurde mit neuen Austausch- und Koordinationsgefässen weiterentwickelt.

Im Bereich der wirksamen Erkennung, Verhinderung, Bewältigung und Abwehr von Cyberangriffen wurden insbesondere die Vorfallbewältigung, die Frühwarnung, die Krisenvorsorge und der Fähigkeitsausbau weiter gestärkt. Beim BACS gingen 64 733 freiwillige Meldungen zu Cybervorfällen ein. Der Cyber Security Hub (CSH) wurde weiterentwickelt und mit über 1600 angeschlossenen Organisationen und rund 6000 Nutzerinnen und Nutzern als zentrale nationale Plattform gestärkt. Mit der Integrierten Übung 2025 sowie weiteren kantonalen und internationalen Übungen wurden Prozesse der Cyberkrisenbewältigung überprüft und weiterentwickelt. Parallel dazu hat der Nachrichtendienst des Bundes (NDB) im Rahmen der Arbeiten rund um die Revision des Nachrichtendienstgesetzes (NDG) rechtliche Grundlagen weiterentwickelt, die die Fähigkeiten zur Attribution stärken. Die Schweizer Armee trieb die Umsetzung der «Gesamtkonzeption Cyber» planmässig voran.



Beiratstreffen Digitale Schweiz 2025

Im Bereich der effektiven Bekämpfung und Strafverfolgung der Cyberkriminalität standen 2025 die Koordination, die Verbesserung gemeinsamer Grundlagen und die Weiterentwicklung bestehender Unterstützungsinstrumente im Vordergrund. Die Gremien CyberSTRAT und Cyber-CASE förderten den institutionellen und fachlichen Austausch. Zudem wurden die statistischen Grundlagen zur Erfassung von Cybercrime-Phänomenen weiterentwickelt, zusätzliche Ressourcen für die nationale Serienerkennung bereitgestellt und die Plattform [cybercrimepolice.ch](https://www.cybercrimepolice.ch) überarbeitet und national besser zugänglich gemacht. Auf politischer Ebene wurden Arbeiten zur Verbesserung des interkantonalen Datenaustauschs aufgenommen.

Auch im Bereich der internationalen Zusammenarbeit konnten 2025 wichtige Massnahmen weitergeführt werden. Mit der Geneva Cyber Week, der Global Conference on Cyber Capacity Building (GC3B) und der Global Digital Collaboration wurden hochrangige Veranstaltungen in Genf durchgeführt. Die Arbeiten am International Geneva Cybersecurity Center (IG-CSC) wurden weiter vorangetrieben. Eine Zusammenarbeit mit Quad9 ermöglicht den Betrieb eines DNS-Firewall für

die Mitglieder des CSC. Daneben wurde 2025 ein Pilotprojekt zur Deckung des Bedarfs an Data Hosting von in der Schweiz ansässigen humanitären Organisationen und Akteuren der Friedensförderung lanciert. Darüber hinaus setzte sich die Schweiz in multilateralen Prozessen, namentlich im Kontext der UNO-Cybercrime-Konvention, der OEWG, des Pall-Mall-Prozesses sowie bei der Umsetzung der vertrauensbildenden Massnahmen der OSZE, aktiv ein.

Insgesamt zeigt das Jahr 2025, dass die Umsetzung der NCS in allen strategischen Zielbereichen konkrete Fortschritte erzielt hat. Besonders hervorzuheben sind die Einführung der Meldepflicht, der Ausbau sektoraler Resilienzstrukturen, die Stärkung des nationalen Informationsaustauschs sowie die weitere Profilierung der Schweiz in der internationalen Cybersicherheit. Der Bericht enthält zudem ein eigenes Kapitel zur künstlichen Intelligenz, das KI-bezogene Umsetzungsinitiativen innerhalb der NCS sichtbar macht. Ebenfalls enthält er einen Kommentar des Steuerungsausschusses, der ausgewählte Entwicklungen einordnet und Hinweise für die strategische Weiterentwicklung der NCS gibt.

# Einleitung

Während sich die geopolitische Lage in den vergangenen Jahren stark verschlechtert hat, führten die weiterhin rasch voranschreitende digitale Transformation und wachsende globale Vernetzung<sup>1</sup> gleichzeitig dazu, dass unsere Abhängigkeit von Technologien weiter zunimmt. Als Folge davon steigt die Bedeutung der Bedrohung durch Cybervorfälle weiter an. Insbesondere im Hinblick auf die Zunahme hybrider Bedrohungen ist die Umsetzung einer kohärenten und wirkungsorientierten Nationalen Cyberstrategie (NCS) von grosser Bedeutung.

Dies kann nur gelingen, wenn diese Umsetzung durch alle relevanten Akteure aus Wirtschaft, Hochschulen, Gemeinden, Kantonen und Bund gemeinsam und aufeinander abgestimmt vorangetrieben wird. Um eine klare Governance und eine übergeordnete strategische Steuerung sicherzustellen, hat das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) im Juni 2024 den Steuerungsausschuss der NCS (StA NCS) eingesetzt. Er nimmt insbesondere folgende zentrale Aufgaben wahr:

- **Regelmässige Überprüfung und strategische Weiterentwicklung:** Er überprüft die NCS mindestens alle fünf Jahre, wirkt an deren Weiterentwicklung mit und erarbeitet zuhanden des Bundesrates Vorschläge zur Anpassung der Strategie.
- **Vorschlag zusätzlicher Massnahmen und Prioritäten:** Bei Bedarf unterbreitet er dem Bundesrat Vorschläge für zusätzliche Massnahmen. In Abstimmung mit den in der NCS genannten Umsetzungspartnern erarbeitet er zudem Vorschläge zur Priorisierung der Umsetzung der Strategie.
- **Jahresbericht:** Er erstattet jährlich Bericht über die Umsetzung der NCS an den Bundesrat, die Kantone sowie an die Öffentlichkeit.

Der StA NCS setzt sich aus Vertretungen der Kantone, des Bundes, der Wirtschaft, der Zivilgesellschaft sowie der Wissenschaft zusammen. Die Mitglieder wurden aufgrund ihrer fachlichen Expertise und ihres strategischen Know-hows in einem für die Cybersicherheit relevanten Bereich ausgewählt. Diese vielfältige Zusammensetzung gewährleistet die Berücksichtigung unterschiedlicher Perspektiven und ermöglicht einen ganzheitlichen Ansatz zur Cybersicherheit sowie zur Umsetzung der NCS auf gesamtgesellschaftlicher Ebene.

Das Bundesamt für Cybersicherheit (BACS) dient als Geschäftsstelle des StA NCS und koordiniert die Umsetzung der NCS.

Mit dem vorliegenden Jahresbericht informiert der StA NCS die Öffentlichkeit über den Stand der Umsetzung der NCS. Anhand der wichtigsten Kennzahlen und der Darstellung der zentralen Projekte kann nachvollzogen werden, welche Arbeiten im Jahr 2025 geleistet und welche Fortschritte erzielt wurden. Der Bericht schliesst an die im Umsetzungsbericht 2024<sup>2</sup> dargestellten Resultate an, ohne diese systematisch zu wiederholen.

<sup>1</sup> Parag Khanna: *Die Zukunft der Globalisierung und der multipolaren Welt*

<sup>2</sup> Bericht zur Umsetzung der Nationalen Cyberstrategie (NCS) 2024

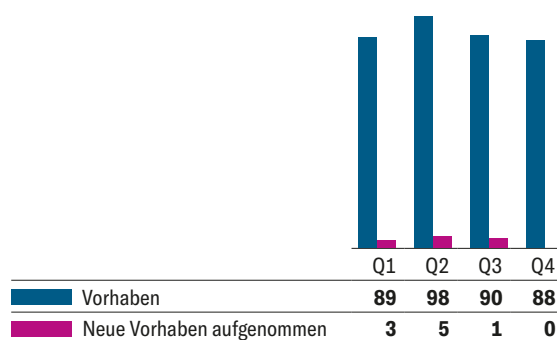
# Kennzahlen zur Umsetzung der NCS

## Meilensteine 2025



Meilensteine	Erreicht	in Umsetzung	neu terminiert	nicht umgesetzt	nicht berichtet
<b>Total</b>					
<b>Q1</b>	33	2	0	0	186
<b>Q2</b>	105	3	8	0	3
<b>Q3</b>	89	14	16	6	2
<b>Q4</b>	100	26	18	2	17

## Vorhaben 2025



**7**

Vom BACS publizierte  
Technologiebetrachtungen

**44**

CyberSeal-  
Zertifizierungen

**240**

Cyber-Safe zertifizierte  
Organisationen

**400**

Durchschnittliche Anzahl  
Teilnehmender an den Online-  
Bi-Weekly-Situation-Briefings

**525**

Meldungen von Schwachstellen  
durch ethische Hacker

**620**

Teilnehmende an der Global Conference  
on Cyber Capacity Building (GC3B)

**10 386**

Seitenaufrufe auf S-U-P-E-R.ch  
(24.4.25–31.5.25)

**17 468**

Identifizierte und gesperrte  
Command-and-Control-Systeme von Angreifern

**64 733**

Freiwillige Meldungen aus der Bevölkerung und von Unternehmen

**2 347 618**

Analysierte Meldungen zu mit Schadsoftware  
infizierten Geräten

Strategisches Ziel 1:

## Selbstbefähigung



*«Die Schweiz baut ihre Stellung als einer der weltweit führenden Wissens-, Bildungs- und Innovationsstandorte auch in der Cybersicherheit aus. Sie nutzt diese Fähigkeiten, um Cyberrisiken über die Lieferketten eigenständig zu beurteilen, technologische Entwicklungen zu antizipieren und agil darauf zu reagieren. Die Bevölkerung ist über Cyberrisiken informiert und gewinnt dadurch Vertrauen in die Nutzung digitaler Dienstleistungen.»<sup>3</sup>*

### Zielbild des StA NCS – Was wollen wir erreichen?

- **Kohärentes und leistungsfähiges Cybersicherheitsökosystem:** Die Schweiz positioniert sich als international anerkannter Forschungs- und Innovationsstandort und zählt zu den Referenzländern im Bereich der Cybersicherheit. Anwendungsorientierte Forschung unterstützt die Ausarbeitung von öffentlichen und privaten Massnahmen, Standards, regulatorischen Rahmenbedingungen und weiteren relevanten Bereichen.
- **Aus- und Weiterbildung:** Cybersicherheit wird in die Aus- und Weiterbildung auf allen Stufen (obligatorische Schule, allgemeinbildende Schulen, berufliche Grundbildung, höhere Berufsbildung, Hochschulen) integriert.
- **Information der Öffentlichkeit:** Sensibilisierungskampagnen sind koordiniert, zielgerichtet und werden im Nachgang auf ihre Wirksamkeit hin evaluiert.
- **Gemeinsames Lageverständnis:** Öffentliche und private Akteure teilen ihre Erkenntnisse zu Bedrohungen, Schwachstellen und Abhängigkeiten, um ein gemeinsames Lageverständnis zu ermöglichen. Sie verfügen über verlässliche Analysen zu aufkommenden und disruptiven Technologien und IKT-Produkten sowie über bedarfsgerechte Mechanismen für den Informationsaustausch.

### Wesentliche Fortschritte im Jahr 2025

Der Ausbau des Cyberökosystems wird wesentlich durch die Hochschulen und die bestehenden Strukturen der Innovationsförderung vorangetrieben. Im Rahmen der Umsetzung der NCS wurden auch 2025 gezielt ergänzende Fördermassnahmen umgesetzt. Der Cyber Defence Campus (CYD Campus) der armasuisse setzte sein Fellowship-Programm, mit welchem er gezielt Nachwuchstalente in der Cybersicherheit stärkt, fort. Über eine Cyber Startup Challenge fördert der CYD Campus zudem innovative, anwendungsnahe Lösungen und ermöglicht deren Weiterentwicklung in einem sicherheitsrelevanten Umfeld. Ergänzend dazu lieferte ein vom CYD Campus organisierter Hackathon im Bereich Gebäudeautomation wertvolle Erkenntnisse zu Systemen der Gebäudeautomation und -steuerung und trug zur Behebung identifizierter Sicherheitslücken bei.

Auch im Bereich der Aus- und Weiterbildung wurden über die NCS vor allem ergänzende Programme umgesetzt. Anfang 2025 wurde vom BACS gemeinsam mit FIRST (global Forum of Incident Response and Security Teams)<sup>4</sup> ein Pilotprojekt mit zwei Schulungstagen zum Thema Ransomware für den Gesundheitssektor initiiert und durchgeführt. Die positiven Rückmeldungen zeigen das bestehende Bedürfnis in den Sektoren und ermutigen diese, sich – beispielsweise über bestehende Cyber Security Centers (CSC) – aktiv einzubringen und geeignete Schulungsangebote zur weiteren Stärkung ihrer Resilienz zu nutzen.

<sup>3</sup> Nationale Cyberstrategie

<sup>4</sup> FIRST – Improving Security Together

# 400

**Durchschnittliche Anzahl Teilnehmende an den Online-Bi-Weekly-Situation-Briefings**

# 496

**Schweizer Forschungsinstitute sind jährlich seit 2020 an durchschnittlich 496 Publikationen zu Cybersicherheit beteiligt**

Die Umsetzung einzelner Initiativen zur Minderung des Fachkräftemangels verzögerte sich im Jahr 2025. Die Programme «Women in Cyber – Talent Academy»<sup>5</sup> und «Cyber4CH»<sup>6</sup> werden daher im Jahr 2026 wenn möglich weiterentwickelt.

Die Sensibilisierungsaktivitäten wurden fortgesetzt und weiter ausgebaut. Mit dem Relaunch der S-U-P-E-R-Website und dem neuen Kampagnenmotto «Keine Ausreden – machen!»<sup>7</sup> wurde die Bevölkerung verstärkt für Cybersicherheitsthemen sensibilisiert. Die Kampagne wurde schweizweit in Print- und Online-Medien, in sozialen Medien sowie an Bahnhöfen verbreitet und durch die Partner Schweizerische Kriminalprävention (SKP) – welche die Koordination des Projekts übernommen hat – sowie den Schweizerischen Versicherungsverband (SVV), die Post und die SBB unterstützt. Die Reichweite konnte gegenüber 2024 deutlich gesteigert werden. Zudem wurde eine Initiative im Rahmen des Cyber Security Month zusammen mit Netpathie<sup>8</sup> mit besonderem Fokus auf junge Zielgruppen

gestartet. Parallel dazu konnten in diesem Rahmen über 550 Teilnehmende an einem «Brown Bag Lunch»<sup>9</sup> teilnehmen. Ergänzt wurden diese Aktivitäten durch spezifische Massnahmen für Schweizer Gemeinden. Ihnen stellte das BACS in Zusammenarbeit mit weiteren Partnern ein Notfallkonzept<sup>10</sup> zur Verfügung. Dieses wird durch Erklärvideos sowie Vorlagen ergänzt, um eine möglichst einfache Umsetzung zu gewährleisten.

Die Thematik der Cybersicherheit wurde zudem durch öffentlichkeitswirksame Veranstaltungen, wie beispielsweise die Global Cyber Conference<sup>11</sup>, die Swiss Cyber Storm, die Nationale Cybersicherheitskonferenz oder die Swiss Cyber Security Days verstärkt in den öffentlichen Diskurs eingebracht. Darüber hinaus war das Thema Cybersicherheit im Jahr 2025 auch Teil der Jugendsession<sup>12</sup>.

5 SANS Talent Academy – [Women in Cyber Switzerland](#)

6 Cyber 4 CH – [Cyber4ch](#)

7 «Keine Ausreden – machen!» – Start der nationalen Sensibilisierungskampagne für Cybersicherheit 2025

8 [Netpathie](#) – Sicherheit im Netz, respektvolle Kommunikation, mentale Gesundheit. Kinder und Internet, Eltern, Fachpersonen und Unternehmungen.

9 «Schützen Sie Ihre Daten online, um nicht Opfer von Phishing zu werden» – [BrownBagLunch ECSM 2025](#) – YouTube

10 Das [Notfallkonzept](#) als Schlüssel zur Cyberresilienz

11 Die Konferenz brachte 320 Teilnehmende aus 30 Ländern zusammen, davon 85% auf Führungsebene (C-Level und Senior Executives). Sie umfasste 60 Referierende, 90 Sessions sowie 10 strategische Partner und ermöglichte einen hochrangigen Austausch zu Cyberresilienz und internationaler Zusammenarbeit.

12 [Jugendsession 2025](#)



NCSK 2025, Sebastien Jaquier (ILCE), Beatrice Kübli (SKP)

Schliesslich konnten im Bereich des gemeinsamen Lageverständnisses wichtige Fortschritte erzielt werden. An den zweiwöchentlichen Lagebesprechungen des BACS nehmen durchschnittlich 400 Fachleute aus allen kritischen Branchen teil und tauschen sich über aktuelle Cyberbedrohungen und mögliche Gegenmassnahmen aus. Auf operativer Ebene tauschen sich die grösseren Schweizer CERTs (CH-CERTs) fast täglich über Vorfälle aus und teilen relevante Informationen, um gemeinsam Angriffe abzuwehren.

**Strategisches Ziel 2:**

# Sichere und verfügbare digitale Dienstleistungen und Infrastruktur



*«Die Schweiz setzt flächendeckend Massnahmen zur Stärkung der Cyberresilienz um. Bund und Kantone schaffen die nötigen Rahmenbedingungen dafür, dass ein hohes Schutzniveau gewährleistet ist, sichere digitale Infrastrukturen, Produkte und Dienstleistungen eingesetzt werden und die Risikobereitschaft bewusst gesteuert wird.»<sup>13</sup>*

## Zielbild des StA NCS – Was wollen wir erreichen?

- **Resilienz der kritischen Infrastrukturen:** Jeder Teilsektor der kritischen Infrastrukturen verfügt über ein Resilienzmanagement, welches die prioritären Handlungsfelder sowie die notwendigen Massnahmen zur Reduktion der cyberbezogenen Risiken festlegt und dessen Umsetzung regelmässig überprüft wird. Die beteiligten Akteure einschliesslich der KMUs und der Gemeinden sind mit den relevanten Normen vertraut und setzen diese um.
- **Umsetzung der Meldepflicht:** Die im Rahmen der Einführung der Meldepflicht gewonnenen Erkenntnisse können künftig dazu beitragen, aus den gemachten Erfahrungen zu lernen und gegebenenfalls Überlegungen zu einer Weiterentwicklung des regulatorischen Rahmens zur Stärkung der Resilienz des Landes anzustellen.
- **Schwachstellenmanagement:** In der Schweiz entwickelte Software, digitale Komponenten und IKT-Produkte erfüllen angemessene Sicherheitsanforderungen, die auf einem risikobasierten Ansatz beruhen. Ein systematisches Schwachstellenmanagement stellt ein hohes Sicherheits- und Resilienzniveau der kritischen Infrastrukturen sowie der Bundesverwaltung sicher. Dieses umfasst die Identifikation, Behandlung, Prävention sowie die verantwortungsvolle Offenlegung von Schwachstellen.
- **Zusammenarbeit der Behörden:** Die Zusammenarbeit, der Informationsaustausch und die gegenseitige Unterstützung zwischen Bund, Kantonen und Gemeinden auf einem klaren Governance-Modell und stützen sich auf ein Netzwerk zuständiger Stellen.

<sup>13</sup> Nationale Cyberstrategie



NCSK 2025, Bundesrat Martin Pfister

### Wesentliche Fortschritte im Jahr 2025

Ein zentraler Meilenstein in der Umsetzung der NCS wurde am 1. April 2025 mit der Inkraftsetzung der Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen erreicht. Die Betreiberinnen von kritischen Infrastrukturen werden damit verpflichtet, dem BACS Cyberangriffe innerhalb von 24 Stunden nach deren Entdeckung zu melden. Das standardisierte Meldeformular auf dem Cyber Security Hub (CSH) des BACS ermöglicht einen effizienten, harmonisierten Meldeprozess und stärkt den Informationsaustausch – ein entscheidender Faktor zur Bewältigung der rasch zunehmenden Cyberbedrohungen. Die Schweiz orientiert sich dabei an internationalen Standards wie der EU-NIS-Richtlinie. Seit der Einführung der Meldepflicht im April 2025 wurden bis Ende Jahr 222 Meldungen registriert.

Die Meldepflicht ist aber nicht die einzige Massnahme, welche die Cybersicherheit von kritischen Infrastrukturen stärkt. 2025 haben die Betreiberinnen kritischer Infrastrukturen ihre Zusammenarbeit stark ausgebaut. Im April 2025 wurde das Rail-ISAC<sup>14</sup>, ein Cyber Security Center für den Bahnsektor, offiziell gegründet. Ebenfalls 2025 wurde das Healthcare-CSC<sup>15</sup> der Spitäler offiziell ins Leben gerufen und verfügte per Ende Jahr über 33 Mitglieder. Es leistet einen wesentlichen Beitrag zur Stärkung der Resilienz im Gesundheitswesen. Das Cyber Security Center des Finanz- und Versicherungssektors (FS-CSC) und das BACS intensivierten im Jahr 2025 ihre Zusammenarbeit<sup>16</sup> und verstärkten ihre Aktivitäten zur Erhöhung der sektoralen Resilienz.

<sup>14</sup> Rail ISAC Sicherheitsorganisation | SBB

<sup>15</sup> Home - H-CSC

<sup>16</sup> Kooperation für mehr Cybersicherheit im Finanzsektor: BACS und Swiss FS-CSC intensivieren Zusammenarbeit

# 222

**Registrierte meldepflichtige Meldungen**  
(April–Dezember 2025)

# 251

**Teilnehmende an der NCSK**

Die Sicherheit von kritischen Infrastrukturen hängt aber nicht nur von eigenen Sicherheitsdispositionen ab, sondern auch direkt von der Verfügbarkeit von sicheren digitalen Produkten. Der Bundesrat hat am 20. August 2025 beschlossen, dass er eine Vorlage zur Cyberresilienz ausarbeiten will, welche Vorgaben für die Sicherheit digitaler Produkte definiert.<sup>17</sup> Bereits heute werden im Rahmen der NCS verschiedene Massnahmen zur Verbesserung des Schwachstellenmanagements umgesetzt. Das BACS betreute 33 koordinierte Offenlegungen von gemeldeten Schwachstellen und das Nationale Testinstitut für Cybersicherheit (NTC) führte eine Reihe von Tests an Open-Source-Software, Photovoltaikanlagen, Klinikinformationssystemen sowie IT-Peripheriegeräten durch. Aus den Erkenntnissen der durchgeführten Tests wurden entsprechende Handlungsempfehlungen formuliert. Innerhalb der Bundesverwaltung führt das BACS das Bug-Bounty-Programm weiter. Im Jahr 2025 gingen beim BACS insgesamt 525 Meldungen zu möglichen Schwachstellen ein. Nach Analyse und Prüfung wurden 328 Meldungen als gültig anerkannt und führten zu Massnahmen zur Behebung oder zur Verbesserung der Sicherheit in der Bundesverwaltung.

Eine stärkere Cybersicherheit ist nicht nur bei kritischen Infrastrukturen wichtig. Es braucht zusätzlich Instrumente, welche alle Organisationen dabei unterstützen, die Cybersicherheit zu verbessern. Eine Möglichkeit dazu ist die freiwillige Selbstprüfung zur Erlangung von Gütesiegeln und Labels. Im Rahmen der NCS sind zwei Projekte dazu entstanden.

Das CyberSeal ist ein Schweizer Gütesiegel, das IT-Dienstleistern bescheinigt, angemessene technische und organisatorische Massnahmen zum Schutz vor Cyberrisiken umzusetzen. Ende 2025 verfügten 44 Organisationen über eine CyberSeal-Zertifizierung; im Jahr 2025 wurden 16 neue Audits durchgeführt.

Ergänzend dazu unterstützt das schweizerische Label Cyber-Safe KMU und Gemeinden in der Schweiz durch Sensibilisierung bei der Umsetzung grundlegender Cybersicherheitsmassnahmen, überprüft die effektive Umsetzung bewährter Praktiken, führt regelmässige Vulnerability-Scans durch und organisiert Sensibilisierungskampagnen zu Phishing. Bis Ende 2025 wurden rund 240 Organisationen mit dem Label ausgezeichnet (2024: 180), während sich etwa 215 Organisationen im Zertifizierungsprozess befanden (2024: 200). Diese Entwicklung unterstreicht die zunehmende Bedeutung des Cyber-Safe Labels für die Cybersicherheit von KMU und Gemeinden in der Schweiz. Parallel dazu wurde die Überarbeitung der Anforderungen des Cyber-Safe Labels initiiert und durch eine Expertengruppe mit Vertreterinnen und Vertretern aus Wissenschaft, Behörden, KMU sowie Gemeinden vorangetrieben. Nicht zuletzt wurde im dritten Jahr in Folge das Cyber-Safe Label in Partnerschaft mit dem Programm Trust4SMEs der Trust Valley, einer Initiative der Stiftung EPFL Innovation Park mit Unterstützung des Kantons Waadt, weitergeführt. Im Rahmen dieser Zusammenarbeit wurde ein Einführungsworkshop zu Cyberrisiken durchgeführt, alle teilnehmenden KMU nutzten das Cyber-Safe-Risikobewertungstool, und rund die Hälfte von ihnen absolvierte ein Audit im Hinblick auf das Cyber-Safe Label.

<sup>17</sup> [Der Bundesrat will die Cyberresilienz von digitalen Produkten stärken](#)

# 328

## «Bug-Bounty»-Schwachstellenmeldungen führten zu Massnahmen zur Behebung oder zur Verbesserung der Sicherheit in der Bundesverwaltung

Als weitere Möglichkeit zur Stärkung des Selbstschutzes entwickelte das BACS eine Methode zur Stärkung der Cybersicherheit und Resilienz (CSRM),<sup>18</sup> die Organisationen und Unternehmen zur Förderung ihrer entsprechenden Fähigkeiten einsetzen können. Diese wurde zur breiten Konsultation öffentlich geteilt und wird in enger Zusammenarbeit mit Partnern und Fachpersonen getestet und weiterentwickelt.

Die Zusammenarbeit zwischen Behörden zur Umsetzung der NCS wurden ebenfalls ausgebaut. Im Jahr 2025 wurden mehrere Strukturen etabliert oder konzipiert: Der «Round Table zur Nationalen Cyberstrategie» ermöglicht einen raschen Informationsaustausch auf Direktionsebene der relevanten Ämter. Die «Fachgruppe Cybersicherheit» fördert den Austausch bewährter Praktiken und die Zusammenarbeit zwischen kommunaler, kantonaler und eidgenössischer Ebene. Zudem wurden in Zusammenarbeit mit den Umsetzungspartnern die «Umsetzungsforen» ins Leben gerufen, welche die Akteure der NCS-Umsetzung zusammenführt. Die Nationale Cybersicherheitskonferenz, welche das Thema «Cyberresilienz: Regulierung oder Selbstverantwortung?» thematisierte, versammelte im September 2025 über 250 Teilnehmende in Bern.

Darüber hinaus wurden zahlreiche (inter-)kantonale Initiativen zur Stärkung der Resilienz und der gemeinsamen Verantwortung in der Schweiz umgesetzt. Ein Beispiel ist die Umsetzung der «Vereinbarung Cybersicherheit Kanton-Gemeinden» durch den Kanton Waadt. Diese 2024 lancierte Initiative stärkt die

Cybersicherheit auf Gemeindeebene durch Massnahmen zur verbesserten Krisenbewältigung und Reaktion bei Cybervorfällen, zur Erhöhung der Cyberresilienz sowie zur Verbesserung der Cyberprävention.<sup>19</sup>

Im Rahmen des Projekts «Sicherheitskultur» des Kantons Zürich wurden zudem 11 000 Mitarbeitende mittels einer Simulationsplattform für das Thema Phishing sensibilisiert.

Ebenfalls auf kantonaler Ebene hat der Kanton Zug eine Cybersicherheitsinitiative lanciert. Dabei ist das Kernelement der Aufbau eines Kompetenzzentrums für Cybersicherheit, das unter anderem die Sensibilisierung der Bevölkerung, die Unterstützung von KMU sowie die Vernetzung öffentlicher und privater Akteure umfasst.<sup>20</sup>

In ähnlicher Weise veröffentlichte der Kanton Wallis am 24. Dezember 2024 die Strategie «CyberStratVS», die den kantonalen Referenzrahmen im Bereich der Cybersicherheit bildet.<sup>21</sup>

<sup>18</sup> [Cybersicherheits- und Resilienzmethode \(CSRM\)](#) (PDF, 742 kB, 24.11.2025)

<sup>19</sup> [Convention cybersécurité Canton-Communes | État de Vaud](#)

<sup>20</sup> [Der Regierungsrat stellt seine Cybersicherheitsinitiative vor](#)

<sup>21</sup> [Stratégie cybersécurité du canton du Valais](#)

## Strategisches Ziel 3:

# Wirksame Erkennung, Verhinderung, Bewältigung und Abwehr von Cyberangriffen



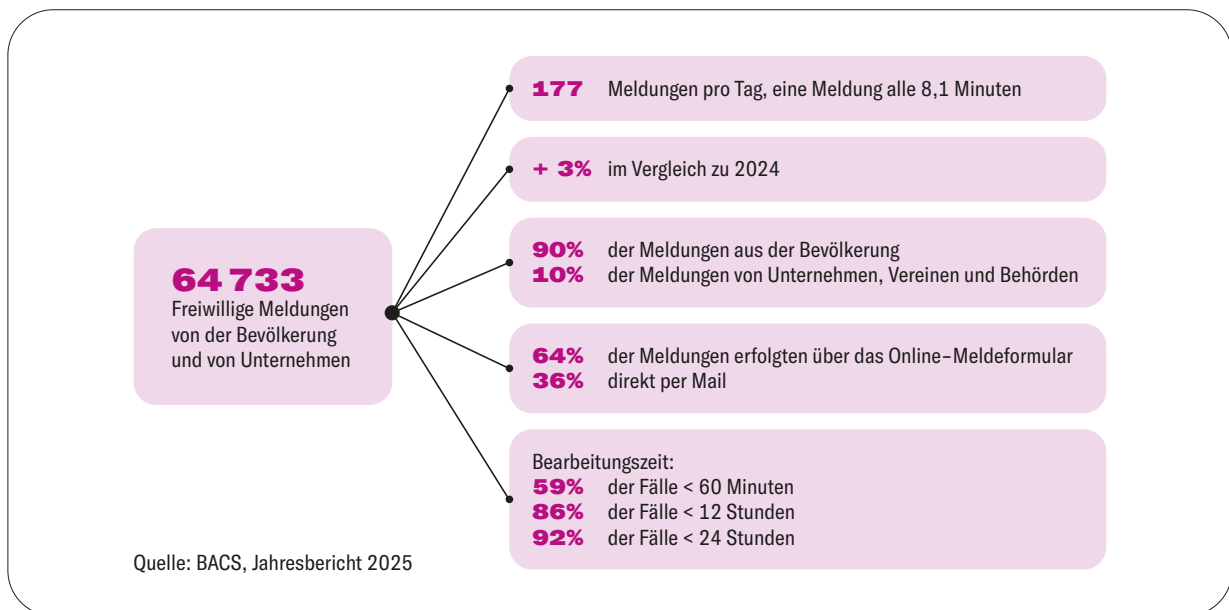
*«Die Schweiz verfügt in allen Lagen über die nötigen Kapazitäten und Organisationsstrukturen, um Cyberbedrohungen und -vorfälle rasch zu erkennen und deren Schäden zu minimieren. Vorfälle werden auch dann bewältigt, wenn sie über längere Zeit andauern und verschiedene Bereiche gleichzeitig betreffen.»<sup>22</sup>*

## Zielbild des StA NCS –

### Was wollen wir erreichen?

- **Ausbau der Fähigkeiten zur Vorfallbewältigung:** Die Schweiz strebt an, ihre Fähigkeit zur wirksamen Bewältigung von Cybervorfällen und Krisen mit Bezug zur Cybersicherheit zu stärken. Dies erfolgt auf der Grundlage geeigneter Einsatz- und Interventionspläne in sämtlichen kritischen Infrastrukturen sowie durch einen strukturierten Austausch von Informationen und Erkenntnissen aus Vorfällen. Die verschiedenen relevanten Sektoren verfügen über verlässliche Austauschmechanismen, die eine kontinuierliche Stärkung der Resilienz auf nationaler Ebene ermöglichen.
- **Ausbau der Fähigkeiten zur Attribution:** Mit dem Ziel, sicherheitspolitisch relevante Cybervorfälle mit Bezug zur Schweiz frühzeitig erkennen und einordnen zu können, setzt der Nachrichtendienst des Bundes (NDB) einen Prozess um, der sich an seinen strategischen Prioritäten orientiert und im Einklang mit seinem Mandat steht. Die Fähigkeiten des NDB zur Attribution werden weiterentwickelt, damit der NDB die Täterschaft bei sicherheitspolitisch relevanten Cybervorfällen wirksamer identifizieren kann. Dadurch schafft der NDB die Grundlagen, um gegebenenfalls den Prozess zur politischen Attribution anzustossen.
- **Krisenbewältigung und Krisenübungen:** Krisen mit Bezug zur Cybersicherheit sind klar definiert und es besteht ein Konzept zur Krisenbewältigung, das auf klaren Governance-Grundsätzen sowie auf eindeutig geregelten Rollen und Verantwortlichkeiten im Sinne des Subsidiaritätsprinzips beruht. Cyberübungen werden auf sektoraler und intersektoraler Ebene durchgeführt; die Übungen des Bundes werden durch eine nationale Stelle koordiniert, die zugleich als Anlaufstelle für Partner, Wirtschaft und Öffentlichkeit dient. Darüber hinaus beteiligt sich die Schweiz an internationalen Übungen zur Stärkung ihrer Einbindung und ihrer Fähigkeiten. Die Schweizer Armee verfügt ebenfalls über die erforderlichen Fähigkeiten, um sich selbst zu schützen. Diese werden entlang der beauftragten Option 3 der «Gesamtkonzeption Cyber» kontinuierlich weiter ausgebaut.

22 Nationale Cyberstrategie



### Wesentliche Fortschritte im Jahr 2025

Kernelemente der Vorfallbewältigung bleiben der aktive Informationsaustausch und die Frühwarnung zu Cybervorfällen. Dieser konnte 2025 weiter gestärkt werden. Beim BACS gingen 64 733 freiwillige Meldungen zu Cybervorfällen ein. Diese ermöglichen es, Entwicklungen und neue Gefahren im Internet frühzeitig zu erkennen und entsprechende Warnungen zu veröffentlichen. Der Grossteil der Meldungen betraf Betrugsfälle (35 968, 55,6%) und Phishing (12 280, 19,0%),

gefolgt von Hacking (743, 1,15%) und Schadsoftware (275, 0,42%), darunter 104 Fälle von Ransomware (0,16%). Zudem wurden Datenabflüsse (37, 0,06%) sowie DDoS-Angriffe (35, 0,05%) gemeldet. Seit Mitte September 2025 kann das BACS in Zusammenarbeit mit dem Bundesamt für Bevölkerungsschutz (BABS) Cyberwarnungen auch über Alertswiss publizieren und stellt damit einen zusätzlichen Kanal zur raschen Information der Bevölkerung bei schwerwiegenden Cyberbedrohungen bereit.



Neben den öffentlichen Warnungen, betreibt das BACS mit dem Cyber Security Hub (CSH) eine Plattform für den Informationsaustausch, welche sich an Betreiberinnen kritischer Infrastrukturen und Fachpersonen wendet. Im Jahr 2025 wurde der CSH gezielt weiterentwickelt und u. a. um das Meldesystem für Angriffs-Meldungen gemäss Informationssicherheitsgesetz (ISG) erweitert. Mit über 1600 angeschlossenen Organisationen und rund 6000 Nutzerinnen und Nutzern etabliert sich der CSH als zentrale nationale Plattform zur Stärkung der Cyberresilienz.

Im Zusammenhang mit der Attribution lag der Fokus des NDB 2025 auf der Revision des Nachrichtendienstgesetzes (NDG). Der NDB prüft und ergänzt die rechtlichen Grundlagen für die Bearbeitung von sicherheitspolitisch bedeutsamen Vorgängen im Cyberraum. Ein Ziel ist, dass der NDB solche Aktivitäten wirksamer aufklären und damit attribuieren kann. Die Vernehmlassung wird voraussichtlich im Sommer 2026 starten. Gleichzeitig hat der NDB auch technische und organisatorische Rahmenbedingungen geschaffen, um die Fähigkeiten bei der Aufklärung und Attribution von sicherheitspolitisch bedeutsamen Vorgängen im Cyberraum weiter zu stärken.

Im Bereich Krisenbewältigung und Krisenübungen stand 2025 die Integrierte Übung 2025 (IU 25) im Zentrum, welche unter der gemeinsamen Leitung von Bund und Kantonen (Co-Übungsleitung) im November erfolgreich durchgeführt wurde. Cyberangriffe waren ein wichtiger Bestandteil der grossangelegten, nationalen Übung. Dies erlaubte es, Prozesse der Cyberkrisenbewältigung zu testen und fortlaufend zu verbessern. Die Auswertung der Übung erfolgt unter der Verantwortung der Co-Übungsleitung. Die Bundeskanzlei (BK) wird dem Bundesrat einen Antrag zur Umsetzung von Empfehlungen aus dem Übungsbericht unterbreiten.

Zusätzlich fanden kantonale Übungen in Neuenburg und Genf statt und das Kommando Cyber war zusammen mit Vertreterinnen und Vertretern vom BACS und BABS an internationalen Cyber-Defence Übungen wie «Locked Shields» und «Cyber Coalition 25» beteiligt.

Zusätzlich hat die BK zusammen mit Verwaltung und Wissenschaft den Cluster «Cybersicherheit» aufgebaut. Ziel des Clusters ist, im Krisenfall Expertinnen und Experten schneller identifizieren zu können, Vertrauen zwischen Verwaltung und Wissenschaft aufzubauen sowie den Austausch im Sinne der Krisenanti-



Cyberübung «Locked Shields» 2022

pation zu fördern. Der Cluster «Cybersicherheit» hat im September 2025 gemeinsam mit dem BACS einen Workshop organisiert, um zu erörtern, nach welchen Kriterien bei umfassenden Cyberangriffen auf die Schweiz die Arbeiten des BACS priorisiert werden könnten.

Auch 2025 lag die Cybersicherheit bei Grossveranstaltung in der Schweiz im Fokus. Durch die enge Zusammenarbeit des BACS GovCERT, des Bundes sowie der kantonalen Behörden konnte die Cybersicherheit beim World Economic Forum (WEF), dem Eurovision Song Contest (ESC) oder der UEFA Women's Euro sichergestellt werden.

Die Schweizer Armee hat die Umsetzung der «Gesamtkonzeption Cyber»<sup>23</sup> planmässig vorangetrieben. Substanzielle Fortschritte konnten insbesondere in den Fähigkeitsbereichen «Führung und Vernetzung» sowie «Wirkung im Cyber- und elektromagnetischen Raum» erzielt werden. Dazu wurde ein adaptives und iteratives Vorgehen gewählt, das sich an den Nutzerbe-

dürfnissen orientiert. Dies ermöglicht eine anwendernah und agile Weiterentwicklung durch die enge Abstimmung zwischen Entwicklung, Sicherheit und Betrieb. Dieses Vorgehen unterscheidet sich deutlich von einem rein projektorientierten Ansatz. Das Kommando Cyber konnte auf der Neuen Digitalisierungsplattform (NDP) bereits erste Funktionalitäten erfolgreich testen. Diese werden Mitte 2026 im Rahmen einer Übung (EOS 26) des Kommandos Spezialkräfte erprobt. Dabei werden erstmals einsatzkritische IKT-Leistungen über die NDP bezogen. Dieser Schritt ist ein wichtiger Meilenstein zur Prüfung des Umsetzungsfortschritts der «Gesamtkonzeption Cyber».

23 Gesamtkonzeption Cyber

## Strategisches Ziel 4:

# Effektive Bekämpfung und Strafverfolgung der Cyberkriminalität



«Die Schweiz baut ihre Fähigkeiten aus, Verursacher von Cyberangriffen zu identifizieren, strafrechtlich im Verbund zu verfolgen und im Rahmen der gesetzlichen Möglichkeiten zu verurteilen.»<sup>24</sup>

## Zielbild des StA NCS – Was wollen wir erreichen?

- **Schaffung von Rechtsgrundlagen für die Bekämpfung von Cyberkriminalität:** Die Schweiz strebt an, die Bekämpfung der Cyberkriminalität koordiniert zu stärken, indem alle Kantone über die erforderlichen und harmonisierten rechtlichen Grundlagen verfügen. Gemeinsame Strukturen, einschliesslich einheitlicher Daten- und Verfahrensstandards, ermöglichen eine engere Zusammenarbeit der Strafverfolgungsbehörden auf nationaler und internationaler Ebene sowie den Aufbau spezialisierter Kompetenzzentren.
- **Fallübersicht:** Eine umfassende Gesamtübersicht über die Fälle – einschliesslich Ereignisse, Meldesituationen und gerichtlicher Nachverfolgung – steht der Strafverfolgung in Echtzeit zur Verfügung und unterstützt ein kohärentes und wirksames Vorgehen.
- Sämtliche Strafverfolgungsbehörden, einschliesslich der Gerichte, haben Zugang zu aktuellen und **bedarfsgerechten Weiterbildungsangeboten**, die der fortlaufenden Entwicklung der Formen der Cyberkriminalität Rechnung tragen und eine kontinuierliche Kompetenzentwicklung gewährleisten.

## Wesentliche Fortschritte im Jahr 2025

Die jährlichen Sitzungen von Cyber-STRAT, an denen die Direktorinnen und Direktoren der wichtigsten in der Bekämpfung der Cyberkriminalität engagierten Institutionen teilnehmen, ermöglichten den Austausch sowie die Erörterung strategischer und politischer Fragestellungen in diesem Bereich. Parallel dazu fanden insgesamt drei Treffen von Cyber-CASE statt. Cyber-CASE ist in erster Linie als Netzwerk spezialisierter Staatsanwältinnen und Staatsanwälte im Bereich der Cyberkriminalität auf kantonaler und eidgenössischer Ebene ausgestaltet. In das Netzwerk eingebunden sind auch das Netzwerk Digitale Ermittlungsunterstützung Internetkriminalität (NEDIK) sowie das BACS. Die Treffen dienten insbesondere dem Austausch von Erfahrungen und bewährten Praktiken. Im Rahmen von Cyber-CASE wurde 2025 eine Arbeitsgruppe «Ransomware» geschaffen, um wichtige Informationen zu Verfahren der kantonalen Staatsanwaltschaften und der Bundesanwaltschaft (BA) auszutauschen sowie die Koordination zu stärken.<sup>25</sup>

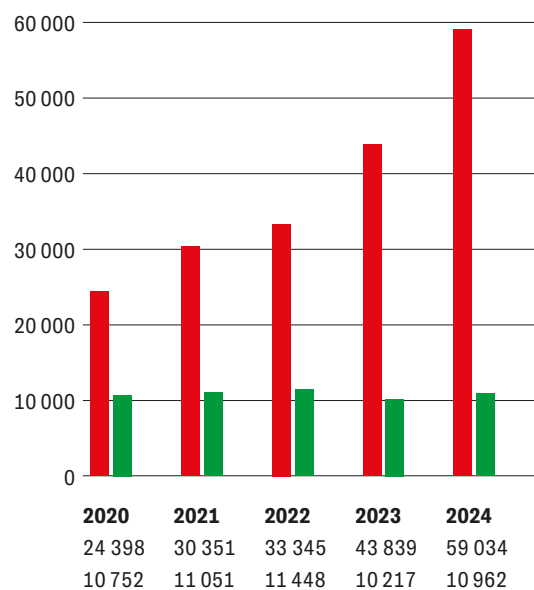
<sup>25</sup> Darüber hinaus führt die BA in Zusammenarbeit mit zahlreichen Staaten mehrere Strafverfahren durch, insbesondere in Ransomware-Fällen, unter der Koordination der Agenturen EUROPOL und EUROJUST (Cyberkriminalität: Hackergruppe AKIRA intensiviert ihre Aktivitäten).

## Die Entwicklung von Cyberstraftaten und der Aufklärungsrate

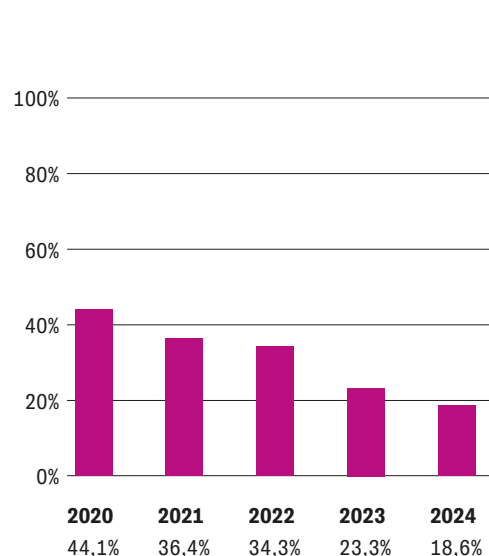
(2020-2024)

### Total digitale Kriminilität

■ Anzahl Straftaten  
■ Anzahl aufgeklärte Straftaten



■ Aufklärungsrate in %



NEDIK führte innerhalb der kantonalen Polizeikorps eine Umfrage über die Bekämpfung der virtuellen Pädokriminalität durch und arbeitet derzeit an der Entwicklung entsprechender Massnahmen. Ausserdem wurden die Cybercrime-Phänomene der polizeilichen Kriminalstatistik (PKS) und die dazugehörigen Factsheets für die Polizeikorps in Zusammenarbeit mit dem Bundesamt für Statistik (BFS) per 01.01.2026 aktualisiert, um bessere statistische Erhebungen zu ermöglichen. Zudem wurden zusätzliche Ressourcen für die nationale Serienerkennung sowie für den Betrieb der Plattform [cybercrimepolice.ch](https://cybercrimepolice.ch) bereitgestellt. Das Design der Plattform wurde überarbeitet und wird seit 2025 ebenfalls auf Französisch zur Verfügung gestellt, um eine nationale Nutzung zu erleichtern. Zudem konnte die Zusammenarbeit mit der nationalen Anlaufstelle des BACS weiter verstärkt werden. Auf der politischen Ebene fordert die Motion 23.4311<sup>26</sup> der Sicherheits-

politischen Kommission des Nationalrates die Schaffung einer Verfassungsgrundlage, welche es dem Bund ermöglicht, im Bundesgesetz über die polizeilichen Informationssysteme des Bundes (BPI) den Datenaustausch zwischen den Kantonen zu regeln. Ziel ist es, den polizeilichen Informationsaustausch zu verbessern und die vorhandenen Daten effizienter zu nutzen. Die Arbeiten zur Schaffung dieser Verfassungsgrundlage sowie zur Teilrevision des BPI wurden aufgenommen.

Über die Frage des Datenaustauschs hinaus befasste sich der Bundesrat auch mit operativen Massnahmen zur Bekämpfung konkreter Bedrohungen im digitalen Raum. Im Bericht «Abschaltung von betrügerischen Websites. Nationale Koordination bei Internetbetrug»<sup>27</sup> in Beantwortung des Postulats 22.3457 zeigt der Bundesrat auf, welche Massnahmen zur Bekämpfung von Internetbetrug heute möglich sind und wie diese ausgebaut werden könnten.

26 [23.4311](#) | Schaffung einer Verfassungsgrundlage für eine Bundesregelung des nationalen polizeilichen Datenaustausches | Geschäft | Das Schweizer Parlament

27 [Bundesrat will gegen betrügerische Webseiten vorgehen](#)

Strategisches Ziel 5:

## Führende Rolle in der internationalen Zusammenarbeit



Global Conference on Cyber Capacity Building (GC3B)

*«Die Schweiz setzt sich auf operativer und strategischer Ebene für einen offenen, freien und sicheren Cyberraum und für die umfassende Anerkennung, Einhaltung und Durchsetzung des Völkerrechts im digitalen Raum ein. Das internationale Genf wird als führender Standort für Debatten zur Cybersicherheit genutzt. Die Schweiz kann bei Differenzen mit Bezug zu Cyberoperationen als Vermittlerin auftreten.»<sup>28</sup>*

### Zielbild des StA NCS – Was wollen wir erreichen?

- **Stärkung der internationalen digitalen Sicherheit:** Die Schweiz strebt an, die internationale digitale Sicherheit zu stärken, indem sie den Schutz internationaler Organisationen (IO) und Nichtregierungsorganisationen (NGO) unterstützt, insbesondere durch den Zugang zu

verbesserten Mechanismen der Cybersicherheit und des Informationsaustauschs.

- **Förderung des internationalen Genfs:** Genf positioniert sich als anerkannter Standort für internationale Diskussionen zu Digitalisierung und Technologien und festigt damit die Rolle der Schweiz als zentraler Akteur in der globalen digitalen Governance.
- **Offenes, freies und sicheres Internet:** Die Schweiz setzt sich für ein offenes, freies und sicheres Internet sowie für die Achtung des Völkerrechts im digitalen Raum ein. Sie beteiligt sich an den relevantesten internationalen Gremien und Kompetenzzentren – insbesondere an jenen, die wirksam zur Reduktion von Cyberbedrohungen beitragen – und stärkt damit ihr Engagement sowie ihren Einfluss in der internationalen Zusammenarbeit im Bereich der Cybersicherheit.

### Wesentliche Fortschritte im Jahr 2025

Auch 2025 gelang es, hochrangige Anlässe zur Cybersicherheit in Genf durchzuführen. Die Geneva Cyber Week<sup>29</sup> fand erstmals vom 12. bis 15. Mai 2025 statt. Sie bietet der globalen Cybersicherheits-Community die Möglichkeit, in Genf zusammenzukommen und eine engere Verbindung zu den in Genf ansässigen Organisationen sowie zum Wissens- und Erfahrungsschatz der Geneva Digital Community herzustellen, um ein regelmässiges Engagement zwischen den verschiedenen Akteuren zu fördern. Die Global Conference on Cyber Capacity Building (GC3B)<sup>30</sup> brachte über 620 Teilnehmende aus mehr als 100 Staaten zusammen. Der Fokus der Konferenz lag auf der sicheren Nutzung neuer digitaler Technologien in der Entwicklungszusammenarbeit, insbesondere im globalen Süden. Die Veranstaltung wurde vom Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) ausgerichtet und vom Global Forum on Cyber Expertise (GFCE) organisiert. Ebenfalls fand 2025 die Global Digital Collaboration (GDC), unter der Federführung des Bundesamtes für Justiz (BJ) mit mehr als 1500 Teilnehmenden statt. Die GDC hat die Förderung und den Schutz globaler digitaler Allmenden, welche für den Cyberraum unerlässlich sind unter Einbezug staatlicher und privater Akteure zum Ziel.

Eine Massnahme für die Förderung von Genf als Standort für internationale Organisationen besteht auch darin, diese bei ihrer Cybersicherheit zu unterstützen. Unter der Leitung des EDA wurden die Arbeiten am International Geneva Cyber Security Center (IG-CSC) im Jahr 2025 weiter vorangetrieben. Eine Zusammenarbeit mit Quad9 ermöglicht den Betrieb einer DNS-Firewall für die Mitglieder des CSC. Ein Pilotprojekt zur Deckung des Bedarfs an Data Hosting von in der Schweiz ansässigen humanitären Organisationen und Akteuren der Friedensförderung wurde 2025 lanciert und wird 2026 weiterentwickelt.

Ebenfalls wurde im Herbst 2025 unter Federführung des EDA informelle Verhandlungen zu den Verfahrensregeln der künftigen Vertragsstaatenkonferenz der UNO-Cybercrime-Konvention aufgenommen. Die Schweiz setzte sich dabei aktiv für umfassende Beteiligungsmöglichkeiten nichtstaatlicher Akteure sowie für einen breiten Zugang auch für Nichtvertragsstaaten und die Respektierung der Menschenrechte bei der Umsetzung der Konvention ein.

#### Global Conference on Cyber Capacity Building: (GC3B)

mehr als  
**100**

**Staaten**

über  
**620**

**Teilnehmende**

Generell setzte die Schweiz ihr aktives Engagement in internationalen Gremien fort. Sie brachte ihre Empfehlungen in den Schlussbericht der Open-ended Working Group (OEWG 2021–2025) ein und beteiligte sich weiterhin an den Arbeitsgruppen des Pall-Mall-Prozesses zur Cyberproliferation. Im Rahmen ihrer Zusammenarbeit innerhalb der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), deren Vorsitz die Schweiz 2026 übernimmt, bringt sich die Schweiz im Kontext ihrer Mitwirkung in der Troika der Organisation aktiv ein. Ein besonderer Fokus liegt dabei auf der Umsetzung der vertrauensbildenden Massnahmen der OSZE. Damit fördert sie den Dialog und die Zusammenarbeit zwischen den Teilnehmerstaaten und stärkt Transparenz und Vertrauen in der euro-atlantischen Sicherheit.

Zudem setzte die Schweiz die bilaterale Zusammenarbeit mit zahlreichen strategischen Partnern weltweit fort, unter anderem im Rahmen der Counter Ransomware Initiative (CRI).<sup>31</sup> Darüber hinaus pflegt das GovCERT des BACS enge Beziehungen zu seinen europäischen und internationalen Partnern, insbesondere zu FIRST, CERT-EU, Europol EC3 sowie dem IWWN.

29 [Geneva Cyber Week](#) | DCAF – Geneva Centre for Security Sector Governance

30 [GC3B](#) | Global Conference on Cyber Capacity Building

31 [Home](#) | International Counter Ransomware Initiative

# Kommentar des Steuerungsausschusses

Die eingeleiteten Anstrengungen zur Stärkung der Cybersicherheit im Bildungsbereich werden anerkannt und geschätzt. Gleichwohl ist das Thema Cybersicherheit bislang noch nicht auf allen Ebenen des Bildungssystems systematisch verankert. Vor diesem Hintergrund könnte der Positionierung der Cybersicherheit als übergreifende Querschnittskompetenz – von der Grundbildung über die tertiäre Bildung bis hin zur Berufsbildung und Weiterbildung – künftig verstärkt Beachtung geschenkt werden.

Über die Bildungsdimension hinaus leisten die Cyber Security Centers (CSC) einen zentralen Beitrag zur Stärkung der sektoralen Resilienz. Im Jahr 2025 sind CSCs in den Bereichen Gesundheit, Finanz- und Versicherungswesen, Bahnsektor sowie im Umfeld des Internationalen Genfs operativ tätig. Eine schrittweise Ausweitung von CSCs auf weitere Sektoren, insbesondere dort, wo kritische Infrastrukturen betroffen sind, erscheint sinnvoll und könnte den Aufbau zahlreicher zusätzlicher Zentren erforderlich machen.

Damit solche strukturellen Massnahmen gezielt weiterentwickelt werden können, braucht es eine verlässliche und transparente Datengrundlage. Forschung zur Cybersicherheit ist deshalb ein wesentlicher Faktor für eine wirksame Umsetzung der NCS. Zusätzliche Initiativen zur Verbesserung der Datenqualität und -zugänglichkeit würden evidenzbasierte Entscheidungsprozesse und eine gezieltere strategische Priorisierung unterstützen. In diesem Zusammenhang kommt auch der Stärkung des Technologietransfers von der Forschung und spezialisierten Unternehmen in die Praxis und Politik besondere Bedeutung zu.

Darauf aufbauend stellen Initiativen zur Festigung der Position der Schweiz im Bereich der Cybertechnologien und der Innovation einen wichtigen Hebel dar und sollten unter Nutzung der bestehenden Stärken in Forschung, Wirtschaft und Innovationsökosystem weiterverfolgt werden.

Neben strukturellen und innovationspolitischen Aspekten bleibt auch eine verstärkte Zusammenarbeit zwischen Bund, Kantonen und Gemeinden, aufbauend auf bestehenden Strukturen und Initiativen, zentral. Die Zusammenarbeit kann zur Erhöhung der Kohärenz und Wirksamkeit der Umsetzung beitragen. Klarere Rahmenbedingungen und gezielte Orientierungshilfen (wie z. B. das Notfallkonzept<sup>32</sup>) würden insbesondere kleinere Organisationen und Gemeinden dabei unterstützen, regulatorische Komplexität zu reduzieren und sich auf die relevantesten Prioritäten im Bereich der Cybersicherheit zu konzentrieren. Im Bereich der Strafverfolgung von Cyberkriminalität erscheint es zudem wünschenswert, rascher zu rechtlichen Grundlagen zu gelangen, die eine gesamtschweizerische Übersicht über die Fälle ermöglichen; die bereits eingeleiteten Bemühungen zur Stärkung der interkantonalen Zusammenarbeit werden dabei begrüsst und könnten bei Bedarf durch Impulse auf Bundesebene ergänzt werden.

---

32 [Das Notfallkonzept als Schlüssel zur Cyberresilienz](#)



Beiratstreffen Digitale Schweiz 2025

Gleichzeitig bleibt das Engagement der Schweiz in internationalen Rahmenwerken zur Bekämpfung der Cyberkriminalität, insbesondere im Kontext der Budapester Konvention, der Cybercrime-Konvention sowie laufender multilateraler Prozesse, ein zentraler Faktor für die Stärkung der internationalen Zusammenarbeit. In diesem Sinne ermutigt die Schweiz ihre Partner, das Internationale Genf als Plattform für Dialog, Kooperation und gemeinsames Handeln zu nutzen, damit Digitalisierung und Technologien zur Stärkung der Sicherheit beitragen und dem Gemeinwohl dienen.

Für die strategische Weiterentwicklung insgesamt ist schliesslich eine klare Steuerungslogik entscheidend. Die Festlegung klarer Ambitionsniveaus trägt dazu bei, die angestrebte Vision zu präzisieren, während der Einsatz von Leistungsindikatoren (KPI) die Messung von Fortschritten und der Wirkung der umgesetzten Massnahmen ermöglicht. Die Weiterführung dieser Arbeiten bildet eine wichtige Grundlage zur Stärkung der Steuerung der nationalen Cybersicherheit und zur gezielten Identifikation von Lücken.

Schliesslich wird eine kontinuierliche Auseinandersetzung mit Umfang und Tiefe der Strategie in enger Zusammenarbeit mit sämtlichen relevanten Anspruchsgruppen begrüsst. Zu diesem Zweck ist in den kommenden Monaten ein vertiefter und partizipativer Prozess vorgesehen, um die strategische Überprüfung im Jahr 2028 vorzubereiten.<sup>33</sup>

<sup>33</sup> Der Steuerungsausschuss wird sich prioritär mit folgenden Themen befassen:

- Künstliche Intelligenz und Cybersicherheit
- Digitale Souveränität im Kontext der Cyberresilienz der Schweiz
- Authentizität von Daten (Datenintegrität im Kontext von Desinformation)
- Risikoteilung in der Wirtschaft sowie geopolitische Auswirkungen und internationale Zusammenarbeit im Bereich der Cybersicherheit

## Exkurs: Künstliche Intelligenz (KI) im Fokus

Die rasante technologische Entwicklung im Bereich der Künstlichen Intelligenz (KI) beeinflusst zunehmend die Cyberbedrohungslage sowie die Fähigkeiten zur Verteidigung digitaler Infrastrukturen. Die NCS verfolgt bei der Definition ihrer strategischen Ziele und Massnahmen einen technologieneutralen Ansatz. Sie versteht sich als ein offener und flexibler Ordnungsrahmen, der es ermöglicht, neue technologische Entwicklungen dynamisch und adaptiv in die Umsetzung zu integrieren.

Um den technologischen Entwicklungen im Bereich der KI angemessen Rechnung zu tragen und deren Einfluss auf die Umsetzung der NCS fundiert beurteilen zu können, wird im Bericht des Bundesrates in Erfüllung des Postulats 23.3861 Andrey vom 15. Juni 2023<sup>34</sup> festgehalten, dass der jährliche Bericht des Steuerungsausschusses NCS zur Umsetzung der NCS ein eigenes Kapitel enthalten soll, welches die Umsetzungsinitiativen mit Bezug zur KI explizit hervorhebt.

Im Rahmen der NCS zeigt sich, dass KI als Querschnittstechnologie zunehmend Einfluss auf alle strategischen Ziele hat. Trotz des technologieneutralen Ansatzes der NCS entstehen in sämtlichen Zielbereichen Projekte mit direktem oder indirektem KI-Bezug. Die nachfolgende Zusammenfassung ordnet die wichtigsten KI-bezogenen Umsetzungsinitiativen der NCS für das Jahr 2025 ein. Sie bietet jedoch nicht eine Übersicht aller KI-bezogenen Projekte des Bundes, diese wird durch das Kompetenznetzwerk für künstliche Intelligenz (KI-Netzwerk) erstellt und regelmässig aktualisiert.<sup>35</sup> Zudem will der Bundesrat die KI-Strategie der Bundesverwaltung mit einem Umsetzungsplan gezielt vorantreiben und die bundesweite Koordination stärken.<sup>36</sup> Zur Koordinationsstärkung wechselt die KI-Netzwerk-Anlaufstelle per 1. Februar 2026 zur BK-DTI und die Zusammenarbeit wird entlang von sieben Themenfeldern organisiert – darunter «Cyber- und Informationssicherheit sowie Datenschutz» als eigenes Themenfeld.

<sup>34</sup> Bericht

<sup>35</sup> Kompetenznetzwerk für künstliche Intelligenz

<sup>36</sup> Bund plant gezielte Massnahmen für den Einsatz von KI in der Bundesverwaltung und stärkt Koordination

### Forschung zur Bedeutung von KI in der Cybersicherheit

Im Jahr 2025 veröffentlichte der CYD Campus eine technologiebezogene Analyse zu den Chancen und Risiken von KI-generierten Bildern für militärische Kräfte.<sup>37</sup> Die Studie zeigt auf, dass Fortschritte in generativer KI, insbesondere bei der Erzeugung fotorealistischer Bilder, das heutige Informationsumfeld vor neue Herausforderungen stellen, indem sie sowohl neue taktische Möglichkeiten als auch potenzielle Bedrohungen eröffnen.

KI-generierte Bilder können nicht nur für Ausbildungs-, Trainings- und Simulationszwecke eingesetzt werden, sondern insbesondere auch zur Desinformation, Täuschung und Manipulation im Informationsraum genutzt werden. Der Bericht schliesst mit Empfehlungen, wie Streitkräfte und cyberverteidigungsnahe Einheiten besser auf diese Entwicklungen vorbereitet werden können, etwa durch Erkennungsmethoden, Ausbildung der Analytinnen und Analysten sowie Sensibilisierung der Einheiten für die Identifikation synthetischer Medieninhalte.

<sup>37</sup> Threats and Opportunities in AI-generated Images for Armed Forces.pdf

Parallel dazu adressieren verschiedene Vorhaben die Erhöhung der Sicherheit von KI-Systemen selbst, darunter forensische Analysen von Diffusionsmodellen für die Bildgenerierung, die Charakterisierung und Abschwächung von Angriffen auf Large Language Models (LLMs), die Analyse und Verbesserung der Robustheit von Foundation Models sowie die Entwicklung dezentraler, vertrauenswürdiger und ressourceneffizienter KI-Systeme.

Zur Unterstützung der Bedrohungsanalyse wurden Projekte zur Anomalieerkennung in dynamischen Netzwerken sowie zur Rückverfolgbarkeit von Datenlecks mittels robuster, bildstabiler Wasserzeichen vorangetrieben. Weitere Projekte untersuchen Anwendungsfälle von Large Language Models, unter anderem zur Analyse von Halluzinationen in Retrieval-Augmented-Generation-Systemen, zur Identifikation und Nutzung von LLMs in verschiedenen Use Cases sowie zu ihrem Einsatz im parlamentarischen Kontext. Ergänzend dazu wurden Projekte zur Intelligenzsteigerung von Edge-Geräten weitergeführt, etwa im Bereich frühzeitiger Warnsysteme auf Basis biomedizinischer Daten, der Lokalisierung von Funksignalen sowie der luftgestützten Verarbeitung von Sensordaten.

### **Sensibilisierung zu Cyberbedrohungen durch KI**

Das BACS informiert kontinuierlich über aktuelle Trends und neue Bedrohungen im Bereich der Cybersicherheit. Grundlage bilden freiwillige Meldungen aus Bevölkerung und Wirtschaft. Dabei wurde insbesondere ein zunehmender Missbrauch von künstlicher Intelligenz für Betrugszwecke festgestellt. Zudem zeigt das BACS auf, wie solche Bedrohungen frühzeitig erkannt werden können, und gibt konkrete Empfehlungen zum Schutz und zum angemessenen Umgang mit entsprechenden Vorfällen. Ergänzend zu diesen Warnhinweisen führt das BACS gemeinsam mit seinen Partnern Sensibilisierungsmassnahmen im Rahmen von Kampagnen durch. Der Einsatz von KI in Cyberangriffen stand im Zentrum der BACS-Kampagne im Rahmen des European Cyber Security Month (ECSM). Dabei produzierte das BACS ein kurzes Video, das aufzeigt, wie einfach Cyberkriminelle mithilfe von KI manipulierte Deepfake-Videos erstellen können.

### **Regulierung der Cybersicherheit von KI**

Im Kontext der Regulierung der KI ist eingehend zu prüfen, ob und in welcher Form cybersicherheitsrelevante Aspekte, unter Berücksichtigung der einschlägigen internationalen Normen und Standards, notwendig sind. Eine interdepartementale Arbeitsgruppe des Bundes hat eine Auslegeordnung zur Regulierung von KI<sup>38</sup> veröffentlicht, welche den Handlungsbedarf sowie mögliche regulatorische Ansätze aufzeigt. Die Auslegeordnung definiert drei übergeordnete Ziele, die durch eine Schweizer Regulierung im Bereich KI erreicht werden sollen: die Stärkung des Innovationsstandorts Schweiz, die Wahrung des Grundrechtsschutzes, einschliesslich der Wirtschaftsfreiheit, sowie die Stärkung des Vertrauens der Bevölkerung in KI.

Am 12. Februar 2025 hat der Bundesrat entschieden, die KI-Konvention des Europarats zu ratifizieren. Damit soll die KI so reguliert werden, dass ihr Potential für den Wirtschafts- und Innovationsstandort Schweiz nutzbar gemacht wird. Gleichzeitig sollen Risiken für die Gesellschaft möglichst klein bleiben. Die KI-Konvention des Europarats wird ins Schweizer Recht übernommen. In ihren Geltungsbereich fallen in erster Linie staatliche Akteure. Geprüft werden sektorbezogene Gesetzesanpassungen, die sich auf zentrale, grundrechtsrelevante Bereiche, wie beispielsweise den Datenschutz beschränken. Neben der Gesetzgebung werden auch rechtlich nicht verbindliche Massnahmen zur Umsetzung der Konvention erarbeitet. Zu diesen können Selbstdeklarationsvereinbarungen oder Branchenlösungen gehören.

### **KI in der Abwehr von Cyberangriffen und bei der Entdeckung von Schwachstellen**

KI wird zum Monitoring von Cyberangriffen und zur Erkennung von Schwachstellen eingesetzt. Die zuständigen Fachteams des Bundes wenden solche Möglichkeiten an und tauschen sich dazu auch mit Expertinnen und Experten der Privatwirtschaft aus.

<sup>38</sup> [Auslegeordnung zur Regulierung von künstlicher Intelligenz](#)

### **Internationale Zusammenarbeit**

In Zusammenarbeit mit der ETH sowie internationalen Partnern hat das EDA die Initiative ICAIN (International Computation and AI Network) lanciert. Ziel dieser Initiative ist es, die Entwicklung und den Einsatz von transparenten, sicheren und verantwortungsvollen KI-Systemen zu fördern. Im Zentrum steht dabei der Aufbau allgemein zugänglicher KI-Infrastrukturen, die die internationale Zusammenarbeit stärken und zur Etablierung ethischer Standards beitragen sollen. ICAIN hat im Jahr 2025 die Lancierung weiterer Pilotprojekte vorangetrieben. Am 27. März 2025 unterzeichnete Bundesrat Albert Rösti in Strassburg im Namen der Schweiz die Rahmenkonvention des Europarates über Künstliche Intelligenz, Menschenrechte, Demokratie und Rechtsstaatlichkeit. Mit dieser Unterzeichnung bekräftigt die Schweiz ihr Engagement für einen verantwortungsvollen Einsatz von KI-Technologien, der mit den Grundrechten im Einklang steht.

### **Ausblick: KI als Thema der NCS**

Die bisherige Bewertung zeigt, dass sich der technologie neutrale und prozessorientierte Ansatz der NCS bewährt hat. Die bestehenden Strukturen erlauben es, neue technologische Entwicklungen flexibel zu integrieren. KI-relevante Fragestellungen werden über alle fünf strategischen Ziele hinweg adressiert.

Gemäss seinem Mandat überprüft der StA NCS die NCS mindestens alle fünf Jahre, wirkt an ihrer Weiterentwicklung mit und erarbeitet Anpassungsvorschläge zuhanden des Bundesrates. Der StA NCS hat die Arbeiten zur regulären Überprüfung und Weiterentwicklung der NCS bereits gestartet und die zentralen Themenfelder zur Überprüfung bestimmt, wobei KI als einer der prioritären Bereiche analysiert wird. Auf Basis der laufenden Arbeiten wird der StA NCS dem Bundesrat Vorschläge vorlegen, ob die bestehende Integration von KI in die Ziele und Massnahmen der NCS weiterhin zweckmässig ist oder ob KI als eigenständiges Themenfeld in der Strategie verankert werden soll.





# Anhänge

## Selbstbefähigung

n°	Name des Vorhabens	Beschreibung
<b>M1: Bildung, Forschung und Innovation in der Cybersicherheit</b>		
1.1	Übersicht der Schweizer Bildungsangebote im Cyberbereich	Auflistung aller Ausbildungen auf Stufe Hochschulen. Die Liste ist seit 2022 nicht mehr aktualisiert. (Eine Überarbeitung ist in 2026 geplant).
1.2	Forschungsnetzwerk	Bessere Vernetzung der Forschenden im Bereich Cybersicherheit Das Sicherheitsforschungs- und Unterstützungszentrum der Schweizerischen Eidgenössischen Technischen Hochschulen (EPFL Lausanne und ETH Zürich) unterstützt die Bundesbehörden und die Schweizer Industrie dabei, aktuelle und zukünftige Herausforderungen im Bereich der Cybersicherheit zu bewältigen.
1.3	Women in Cyber – Talent Academy	Ziel der Initiative ist es, dem Fachkräftemangel im Cyberbereich zu begegnen, indem Frauen als Quereinsteigerinnen eine Ausbildungsmöglichkeit erhalten. Die Initiative ist noch nicht lanciert.
1.4	Cyber4CH	Ziel der Initiative ist es, dem Fachkräftemangel im Cyberbereich zu begegnen, indem Quereinsteiger/innen eine Ausbildungsmöglichkeit erhalten. Die Initiative ist noch nicht lanciert.
1.5	Pilot Ransomware Training Critical infrastructure mit FIRST	Pilotprojekt: Durchführung von zwei Präsenztrainings zum Thema Ransomware für Betreiber kritischer Infrastrukturen im Gesundheitssektor im Jahr 2025.
1.6	Global Cyber Conference	Ziel ist, Cybersicherheitsexperten, Regierungsdelegationen und Vertreter der Wirtschaft aus aller Welt zu vernetzen, um Best Practices auszutauschen und gemeinsam Lösungen für aktuelle und zukünftige Herausforderungen im Bereich Cybersicherheit zu erarbeiten.
1.7	CyArc	Analyseplattform zur Mitigation von systemischen Cyberrisiken
1.8	Cyber Security research – CYD Campus	Ziel der Forschungsprojekte im Bereich Cybersicherheit ist es, technologische Expertise zur Identifikation, Bewertung und Reduktion von Risiken im digitalen Raum zu entwickeln und sicherzustellen.
1.9	Cyber Security Fellowship Programme and training – CYD Campus	Ziel des Projekts ist, verschiedene Organisationen von nationaler Bedeutung als Community zusammenzubringen und ihnen ein fundiertes Cyber Training-Angebot zur Verfügung stellen zu können.
1.10	Cyber Data Technologies – CYD Campus	Die Bestrebungen des CYD Campus für einen sichereren digitalen Raum basieren auf Datentechnologien und – im weiteren Sinne – auf Künstlicher Intelligenz (KI).
1.11	Cybersicherheit bei der Jugendsession 2025	Im Rahmen einer Zusammenarbeit mit dem SAJV beteiligt sich die NCS an der Jugendsession zum Thema Cybersicherheit, mit dem Ziel, das Bewusstsein junger Menschen für diese Thematik zu stärken.
<b>M2: Sensibilisierung</b>		
2.1	Sensibilisierung KMU	Gezielte Stärkung der Prävention und des Cyberwissens bei KMU
2.2	Sektorspezifische Sensibilisierung	Gezielt auf bestimmte Sektoren ausgerichtete Sensibilisierungsaktivitäten im Bereich Cybersicherheit.
2.3	SUPER – Nationale Sensibilisierungskampagne Bevölkerung	Sensibilisierung der Schweizer Bevölkerung über Cyberbedrohungen und Vermittlung von Schutzmassnahmen, die jeder Einzelne in Eigenverantwortung treffen kann.
2.4	European Cyber Security Month ECSM	Beteiligung an der europäischen Cybersicherheitskampagne
2.5	Nationale Sensibilisierungskampagne 2025	Die Cyberkampagne 2025 spricht zwei Hauptzielgruppen an: Privatpersonen (breite Schweizer Bevölkerung) und KMU.
2.6	Sensibilisierung Cybersicherheit bei den Schweizer Gemeinden	Gezielte Stärkung der Prävention und des Cyberwissens bei Gemeinden. Austausch der Gemeinden untereinander gefördert.

Verantwortlich	Kontakt	URL
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	<a href="https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/bildungsangebote.html">https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/bildungsangebote.html</a>
Swiss Support Center for Cybersecurity	<a href="https://sscc.ethz.ch/people.html">https://sscc.ethz.ch/people.html</a>	<a href="https://sscc.ethz.ch/">https://sscc.ethz.ch/</a>
Women in Cyber	info@women-in-cyber.ch	<a href="https://women-in-cyber.ch/sans-talent-academy/">https://women-in-cyber.ch/sans-talent-academy/</a>
Cyber4CH (Ict Berufsbildung CH, Post, Swisscom)	Ernst «Aschi» Hegg aschi@ict-berufsbildung.ch	
FIRST	ncs@ncsc.admin.ch	<a href="https://www.first.org/blog/20241220-FIRST-Ransomware-Training">https://www.first.org/blog/20241220-FIRST-Ransomware-Training</a>
Swiss Cyber Institute GmbH	conference@swisscyberinstitute.com	<a href="https://globalcyberconference.com/">https://globalcyberconference.com/</a>
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	
CYD Campus	cydcampus@armasuisse.ch	<a href="https://www.cydcampus.admin.ch/de">https://www.cydcampus.admin.ch/de</a>
CYD Campus	cydcampus@armasuisse.ch	<a href="https://www.cydcampus.admin.ch/de">https://www.cydcampus.admin.ch/de</a>
CYD Campus	cydcampus@armasuisse.ch	<a href="https://www.cydcampus.admin.ch/de">https://www.cydcampus.admin.ch/de</a>
SAJV/ CSAJ (Jugendsession)	admin@jugendsession.ch	<a href="https://jugendsession.ch/">https://jugendsession.ch/</a>
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	<a href="https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen.html">https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen.html</a>
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	<a href="https://www.s-u-p-e-r.ch/de/">https://www.s-u-p-e-r.ch/de/</a>
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	<a href="https://cybersecuritymonth.eu/countries/switzerland">https://cybersecuritymonth.eu/countries/switzerland</a>
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	<a href="https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2025/kampagne-super-25-1.html">https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2025/kampagne-super-25-1.html</a>
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	<a href="https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-behoerden.html">https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-behoerden.html</a>

## Selbstbefähigung

n°	Name des Vorhabens	Beschreibung
2.7	Anlaufstelle - BACS Sensibilisierung	Die Anlaufstelle publiziert jeden Dienstag auf der Webseite des BACS einen aktuellen Fall, um betreffend aktuelle Betrugs- und Angriffsvarianten zu sensibilisieren.
2.8	Kanton ZH - Sicherheitskultur Projekt	Der Kanton setzt auf eine kontinuierliche Phishing-Sensibilisierung, ergänzt durch ein breit gefächertes, derzeit freiwilliges Schulungsangebot mit grosser Reichweite innerhalb der kantonalen Verwaltung.

### M3 Bedrohungslage

3.2	Informationen zur Bedrohungslage	Stufengerechte Zurverfügungstellung von Informationen über die Bedrohungslage für Wirtschaft, Gesellschaft und Verwaltung.
3.3	Anlaufstelle - BACS - Lagebild	Bearbeitung von Meldungen aus der Bevölkerung und von KMUs. Meldungen aus der Bevölkerung und von KMU tragen wesentlich zum Lagebild bei. So lassen sich aktuelle Bedrohungen schnell erkennen.
3.6	Einzelberichte Situation	Einzelberichte sind kurze, thematisch fokussierte Artikel. Sie dienen dazu, spezifische Fragestellungen oder Einzelthemen gezielt und punktuell zu behandeln.
3.7	Parlamentslage	Vor den Sessionen der eidgenössischen Räte wird die aktuelle Cyberbedrohungslage geeignet dargestellt. Die bereitgestellten Informationen werden von den Parlamentsdiensten in ihre Dokumentation übernommen und den Parlamentsdiensten sowie den Präsidi (Rats-PräsidentInnen) des National- und Ständerats zugestellt.
3.8	Kanton ZH - Bedrohungslage Radar	ZH Bedrohungslage auf kantonalem Intranet veröffentlicht. Wird regelmässig in Zusammenarbeit mit KAPO ZH überarbeitet.

### M4: Analyse von Trends, Risiken und Abhängigkeiten

4.1	Post-Incident Analysen	Analyse der technischen, organisatorischen und personellen Gründe und Auswirkungen von Cyber-vorfällen
4.2	Monitoring und Trendanalysen	Technische Entwicklungen beobachten und Auswirkungen auf Cybersicherheit abschätzen
4.3	Technologiebetrachtung	Die Technologiebetrachtungen bereiten den technologischen Fortschritt in kompakter und verständlicher Form für Wirtschaft, Bund und Kantone auf. Sie fördern das Verständnis für die kontinuierliche Entwicklung der Informationstechnologie und unterstützen Sicherheitsverantwortliche bei strategischen Entscheidungen zur Ausrichtung der IT-Infrastruktur.
4.4	Threat Assessments	Cyber-Bedrohungen und -Akteure werden analysiert, entlang verschiedener Dimensionen bewertet und die gewonnenen Erkenntnisse bedarfsgerecht in den Analyseplattformen aufbereitet. Die daraus resultierenden Threat Assessments dienen als Grundlage für Analyseprodukte sowie für weiterführende Tätigkeiten in der Lagebeurteilung und Risikobewertung.
4.5	Technologiemarktüberwachungsplattform	Geleitet durch den CYD Campus, mit Fokus auf Trendanalysen und Fachpublikationen.
4.6	Kanton ZH - SOC Austausch	Kantonaler Austausch der SOC's des Flughafens ZH, KAPO ZH, Aargau, NCSC

## Sichere und verfügbare digitale Dienstleistungen und Infrastruktur

n°	Name des Vorhabens	Beschreibung
<b>M5: Schwachstellen erkennen und verhindern</b>		
5.1	Bug Bounty Programm	Früherkennung von Schwachstellen in der IT des Bundes: Bug-Bounty-Programme ergänzen bestehende Sicherheitsmassnahmen, indem sie in Zusammenarbeit mit ethischen Hackern dazu beitragen, potenzielle Schwachstellen in IT-Systemen und -Anwendungen frühzeitig zu identifizieren, zu dokumentieren und zu beheben.
5.3	Koordinierte Veröffentlichung von Schwachstellen (coordinated vulnerability disclosure)	Etablierung und Förderung des Coordinated Vulnerability Disclosure (CVD) Ansatzes zur präventiven Erkennung und Verhinderungen von Schwachstellen und Erhöhung der Cyberresilienz der Bundesverwaltung und der Schweiz vor Cyberangriffen.

Verantwortlich	Kontakt	URL
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	<a href="https://www.ncsc.admin.ch/ncsc/de/home/aktuell/aktuelle-vorfaelle.html">https://www.ncsc.admin.ch/ncsc/de/home/aktuell/aktuelle-vorfaelle.html</a>
Kanton ZH	sicher@zh.ch	<a href="https://www.zh.ch/de/politik-staat/kanton/kantonale-verwaltung/cybersicherheit.html">https://www.zh.ch/de/politik-staat/kanton/kantonale-verwaltung/cybersicherheit.html</a>
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	<a href="https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte/fachberichte/ddos-bericht-6-2023.html">https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte/fachberichte/ddos-bericht-6-2023.html</a>
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	<a href="https://www.ncsc.admin.ch/ncsc/de/home/aktuell/aktuelle-zahlen.html">https://www.ncsc.admin.ch/ncsc/de/home/aktuell/aktuelle-zahlen.html</a>
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	
Kanton ZH	sicher@zh.ch	
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	
CYD Campus	cydcampus@armasuisse.ch	<a href="https://www.cydcampus.admin.ch/de/technologie-monitoring">https://www.cydcampus.admin.ch/de/technologie-monitoring</a>
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	<a href="https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/technologiebe-trachtung.html">https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/technologiebe-trachtung.html</a>
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	
CYD Campus	cydcampus@armasuisse.ch	
Kanton ZH	sicher@zh.ch	
Verantwortlich	Kontakt	URL
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	<a href="https://www.bugbounty.ch/ncsc">https://www.bugbounty.ch/ncsc</a>
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	<a href="https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden.html">https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden.html</a>

## Sichere und verfügbare digitale Dienstleistungen und Infrastruktur

n°	Name des Vorhabens	Beschreibung
5.4	Cyber Resilience Act für die Schweiz	Prüfen wie der CRA in der Schweiz umgesetzt werden kann.
5.5	Nationales Testinstitut für Cybersicherheit NTC	Erhöhung der Testkapazitäten der Schweiz für digitale Produkte.
5.7	Umsetzung Fernmeldegesetz / Verordnung	Das BAKOM verfolgt die Normierungsarbeiten im Cyberbereich, insbesondere jene im Zusammenhang mit dem Mandat der Europäischen Kommission an die europäischen Normungsorganisationen zur Unterstützung des Cyber Resilience Act (CRA).
5.8	Kanton ZH – Bug Bounty Programm	Seit 2025 befindet sich ein Bug-Bounty-Programm im Aufbau. Erste Tests erfolgten im Umfeld von ZH Web, derzeit laufen Gespräche mit der Stadt Zürich als möglichem Umsetzungspartner.
5.9	Kanton ZH – Security Rating Service	Ein Pilotprojekt wurde mit verschiedenen Stakeholdern durchgeführt.
<b>M6: Resilienz, Standardisierung und Regulierung</b>		
6.1	Swiss FS-CSC	Der Verein Swiss FS-CSC zielt im Rahmen einer Public-Private Partnership darauf ab, die Widerstandsfähigkeit des Finanzsektors gegen Cyberrisiken zu verbessern und eine Partnerschaft zwischen Finanzinstituten und Behörden in strategischen und operativen Fragen zu pflegen. Der Verein wurde am 5. April 2022 in Zürich gegründet und hat inzwischen über 170 Mitglieder, darunter Banken, Rück- /Versicherungen, die Schweizerische Nationalbank (SNB), SIX, Wertpapierhäuser, Finanzdienstleister, Asset Manager, Liechtensteinische Finanzinstitute und Branchenverbände. Die Eidgenössische Finanzmarktaufsicht FINMA, das Bundesamt für Cybersicherheit (BACS) und das Staatssekretariat für internationale Finanzfragen (SIF) unterstützen den Verein als Affiliates und wirken in seinen wichtigen Gremien mit.
6.2	SWICYBA – Swiss Industry Cybersecurity Association	Cyber Security Center im Bereich der Schweizer Industrie
6.3	Rail ISAC (Information Sharing and Analysis Center)	Information Sharing and Analysis Center im Bereich des Bahnmobilitätssektors
6.4	Health CSC	Cyber Security Center im Bereich des Gesundheitssektors. Mit dem Projekt H-CSC wird eine nationale Cyberorganisation geschaffen, die Synergien und die Zusammenarbeit im Bereich Cybersicherheit für Schweizer Spitäler stärkt, sie bei Cybervorfällen unterstützt und deren Fachkenntnisse bündelt.
6.5	NCSC – Markant Cyber Conference Lebensmittelbranche 2025	Ziel ist es, den Informationsaustausch innerhalb der Schweizer Lebensmittelversorgungskette zu fördern. Die Veranstaltung wird zudem bestehende Sensibilisierungskampagnen sowie das Konzept der Cyber Security Center (CSC) vorstellen, mit dem Ziel, das Interesse an der Einrichtung eines dedizierten CSC für den Sektor der Lebensmittelversorgungskette zu evaluieren.
6.6	Entwicklung von Grundlagen, Methoden und Hilfsmittel für die Erreichung von Cyberresilienz von Behörden und Unternehmen	Weiterentwicklung und Umsetzungsinstrumente für den NIST-Standard
6.7	Meldepflicht für Cyberangriffe auf kritische Infrastrukturen	Der Bundesrat hat die Meldepflicht für Cyberangriffe auf kritische Infrastrukturen per 1. April 2025 in Kraft gesetzt. Die Betreiberinnen von kritischen Infrastrukturen werden verpflichtet, dem BACS Cyberangriffe innerhalb von 24 Stunden nach deren Entdeckung zu melden. Die Meldepflicht wird im Informationssicherheitsgesetz (ISG) sowie in der Cybersicherheitsverordnung (CSV) geregelt.
6.8	Cyber-Safe – Label	Cyber-Safe.ch ist ein Schweizer Label zur Cybersicherheit, das speziell für kleine und mittlere Unternehmen (KMU) sowie öffentliche Institutionen wie Gemeinden entwickelt wurde.
6.9	Resilienzüberprüfungen (Risiko- und Verwundbarkeitsanalysen) in den Teilsektoren	Kritische Infrastrukturen sollen regelmässig daraufhin überprüft werden, ob Verwundbarkeiten und Risiken bestehen, die zu erheblichen Störungen oder Ausfällen führen könnten, und ob zusätzliche Massnahmen zur Stärkung der Resilienz erforderlich sind.
6.12	Cyberkrisen Bewältigung in Finanzzentren: ein internationaler Vergleich	Durchführen eines Internationalen Vergleichs, wie andere Finanzzentren strukturiert sind, um systemische Cyberkrisen zu bewältigen.
6.13	CyberSeal – Label	Das CyberSeal bestätigt, dass ein IT-Dienstleister geeignete technische und organisatorische Massnahmen umsetzt, um seine Kunden einen angemessenen Schutz vor Cyberrisiken zu gewährleisten. Das CyberSeal leistet einen Beitrag zur Erhöhung der Cyberresilienz der Schweizer KMU.
6.14	Cyber Community Management	Cyber Community Management ist die koordinierte Zusammenarbeit, Unterstützung und Wissensvermittlung zwischen dem BACS und Stakeholdern zur Stärkung der gemeinsamen Cyberresilienz.

Verantwortlich	Kontakt	URL
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	
Nationales Testinstitut für Cybersicherheit NTC	<a href="https://www.ntc.swiss/kontakt">https://www.ntc.swiss/kontakt</a>	<a href="https://www.ntc.swiss">https://www.ntc.swiss</a>
Bundesamt für Kommunikation (BAKOM)	info@bakom.admin.ch	<a href="https://www.bakom.admin.ch/de">https://www.bakom.admin.ch/de</a>
Kanton ZH	sicher@zh.ch	
Kanton ZH	sicher@zh.ch	
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	Swiss Financial Sector Cyber Security Centre FS-CSC <a href="https://fscsc.ch/">https://fscsc.ch/</a>
Bundesamt für Cybersicherheit (BACS)	info@swicyba.ch	
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	"Healthcare Cyber Security Centre H-CSC <a href="https://www.h-csc.ch/de/home/">https://www.h-csc.ch/de/home/</a> "
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	<a href="https://www.ncsc.admin.ch/ncsc/de/home/meldepflicht.html">https://www.ncsc.admin.ch/ncsc/de/home/meldepflicht.html</a>
Verband Schweizer Cybersecurity Label	info@cyber-safe.ch	cyber-safe.ch
Bundesamt für Bevölkerungsschutz (BABS)	info@babs.admin.ch	Bundesamt für Bevölkerungsschutz (BABS) <a href="https://www.babs.admin.ch/de">https://www.babs.admin.ch/de</a>
FS-CSC/ Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	
Allianz Digitale Sicherheit Schweiz ADSS	<a href="https://www.digitalsecurityswitzerland.ch/de/kontakt">https://www.digitalsecurityswitzerland.ch/de/kontakt</a>	Allianz Digitale Sicherheit Schweiz <a href="https://www.digitalsecurityswitzerland.ch/de/cyberseal">https://www.digitalsecurityswitzerland.ch/de/cyberseal</a>
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	

## Sichere und verfügbare digitale Dienstleistungen und Infrastruktur

n°	Name des Vorhabens	Beschreibung
<b>M7: Ausbau der Zusammenarbeit zwischen den Behörden</b>		
7.1	Umsetzung Informationssicherheitsgesetz	Umsetzung der Vorgaben für die Bundesverwaltung, Koordination mit den Kantonen.
7.2	Nationale Cybersicherheitskonferenz (NCSK)	Jährliche Konferenz zum Austausch zwischen Behörden und kritischen Infrastrukturen über die NCS und Cybersicherheit.
7.3	Fachgruppe Cybersicherheit	Die Fachgruppe Cybersicherheit hat zum Ziel, Schwachstellen in den Bereichen Selbstbefähigung, Resilienz und Vorfallmanagement in der Schweiz zu erkennen und zu beheben. Sie entwickelt dafür Mindeststandards sowie einheitliche Lösungen und «Best Practices», damit Bund, Kantone und Gemeinden bei gemeinsamen Herausforderungen im Bereich Cybersicherheit koordiniert und wirksam handeln können.
7.5	Gremium «Round Table Cyber»	Austauschgremium auf Direktionsebene, das einen schnellen und effizienten Informationsfluss ermöglicht.
7.6	Stärkung der Beziehungen mit internationalen Behörden	Förderung des regelmässigen Austauschs und der Vertiefung internationaler Beziehungen.
7.8	Cyber by Events	Sicherstellung des durchgängigen Einbezugs der Cyberkomponente bei den Beteiligten während Events von nationaler, politischer oder strategischer Bedeutung.
7.9	Harmonisierung Cybersicherheit in den Kantonen und Fachämtern	Das BACS unterstützt mit fachlichem Wissen und gibt Feedback zu Richtlinien und Empfehlungen. Als Nebeneffekt können wir Sicherheitsvorgaben über die Kantone hinweg harmonisieren und aktiv für ein gemeinsames Verständnis sorgen.
7.10	Cyber Security Vocabulary Exchange «Glossar»	Austausch von Begriffen und Informationen, um die TERMDAT-Datenbank zu harmonisieren und dadurch die Gesamtqualität cyberbezogener Übersetzungen innerhalb der Verwaltung zu verbessern.

## Wirksame Erkennung, Verhinderung, Bewältigung und Abwehr von Cyberangriffen

n°	Name des Vorhabens	Beschreibung
<b>M8: Vorfallmanagement</b>		
8.1	Ausbau des Cyber Security Hub (CSH) zur zentralen Informations- und Kommunikationsplattform	Der Cyber Security Hub (CSH) ist ein wichtiges Informationssystem des Bundesamtes für Cybersicherheit. Er dient als Instrument für den Austausch und das Management von Informationen über Cyberbedrohungen, Cybervorfälle und Cybersicherheitspraktiken.
8.2	Meldestelle / Anlaufstelle	Entgegennahme und Analyse von Meldungen aus der breiten Öffentlichkeit
8.3	Incident management development	Verstärkte Koordination bei grossen Cybervorfällen durch das BACS
<b>M9 Attribution</b>		
9.1	Attribution von Cyberangriffen	Technische und nachrichtendienstliche Analysen zur Identifikation der Täterschaft
9.2	Politische Attribution von Cyberangriffen	Prozess zur Entscheidung darüber, ob öffentlich über die Attribution kommuniziert wird. Prozess betreffend politische Attribution von Cybervorfällen in 2022 finalisiert. Wird von EDA überarbeitet. Vorhaben läuft seit 2024, wird in 2025 finalisiert.
<b>M10: Krisenmanagement</b>		
10.1	Krisenübungen Koordination	Das BACS stellt die Integration von Cyberübungen in die Koordination der Krisenübungen in der Bundesverwaltung sicher und ermöglicht eine verstärkte Zusammenarbeit der betroffenen Fachstellen.
10.3	Einbezug der Wissenschaft in Krisenmanagement	Bildung von Clustern für die Beratung der Bundesverwaltung im Krisenmanagement
10.4	Krisenorganisation in der Bundesverwaltung	Diese Massnahme fördert eine ganzheitliche Herangehensweise an die Krisenbewältigung und stellt sicher, dass alle erforderlichen Interessengruppen angemessen vertreten sind.



## Wirksame Erkennung, Verhinderung, Bewältigung und Abwehr von Cyberangriffen

n°	Name des Vorhabens	Beschreibung
<b>M11 Cyberdefence</b>		
11.1	Ausbau Kommando Cyber	Ausbau der zentralen Fähigkeiten und Aufbau von dezentralen Fähigkeiten auf Stufe Armee und bei der Koordination mit den zuständigen Stellen.
11.2	Subsidiäre Unterstützung bei Cyberangriffen	Klärung der Frage, wer wen bei Cyberangriffen unterstützt.
11.3	CYD Campus – research and events	Der Campus leitet Forschungsarbeiten und schlägt verschiedene Veranstaltungen und Workshops vor, um das Wissen und die Fähigkeiten der Schweizer Cyberabwehr zu verbessern.

## Effektive Bekämpfung und Strafverfolgung der Cyberkriminalität

n°	Name der Initiative	Beschreibung
<b>M12: Ausbau der Zusammenarbeit der Strafverfolgungsbehörden</b>		
12.1	NEDIK – Netzwerk digitale Ermittlungsunterstützung Internetkriminalität	Das NEDIK (Netzwerk digitale Ermittlungsunterstützung Internetkriminalität) ist ein nationales Netzwerk zur Unterstützung der Ermittlungen im Kampf gegen die Computerkriminalität. Es ist insbesondere für den Wissensaustausch zwischen den Kantonen zuständig.
12.2	Cyberboard	Mit dem Cyberboard besteht eine Koordinations- und Kooperationsplattform zur Bekämpfung der Cyberkriminalität, auf welcher alle wichtigen Akteure vertreten sind. Diese koordiniert die Fallbearbeitung, verschafft den Strafverfolgungsbehörden eine Austauschmöglichkeit über die in der Schweiz bekannten Modi Operandi, typische Fälle und Fallkonstellationen, erkennt Querbezüge und prüft und initiiert bei Bedarf Massnahmen zur Verbesserung bestehender Prozesse.
12.3	Unterstützung der Strafverfolgung durch BACS	Regelmässiger Austausch und kontinuierliche Verbesserung der Zusammenarbeit zwischen BACS, fedpol, den kantonalen Polizeikörpern und der Bundesanwaltschaft.
12.4	Cybercrimepolice.ch	Cybercrimepolice informiert unabhängig und aktuell über Internetbetrug und gibt Tipps zum Schutz. Täglich werden Warnmeldungen für die Bevölkerung zu aktuellen und neuen Cyberbedrohungen veröffentlicht.
<b>M13: Fallübersicht</b>		
13.1	PICSEL (Einführung Plattform für nationale Fallübersicht)	PICSEL (Einführung Plattform für nationale Fallübersicht) ist eine Plattform, die der systematischen Erfassung und Analyse von Fällen dient. Sie ermöglicht die Zentralisierung von Informationen, die Erkennung von Ereignisreihen sowie die Identifizierung neuer Phänomene und Vorgehensweisen.
13.2	Schaffung von Rechtsgrundlagen für den Datenaustausch	Gesamtschweizerische Übersicht zu den Fällen der Strafverfolgung
13.3	End of Week Anlaufstelle BACS	Der effiziente Austausch zwischen dem BACS und der Strafverfolgungsbehörden ist eines der wichtigsten Vorhaben der Anlaufstelle.
<b>M14: Ausbildung der Strafverfolgungsbehörden</b>		
14.1	Cyberspezifische Ausbildung von Strafverfolgungsbehörden	Integration von Cyberausbildung in bestehende Lehrgänge

## Führende Rolle in der internationalen Zusammenarbeit

n°	Name der Initiative	Beschreibung
<b>M15: Stärkung des digitalen internationalen Genfs</b>		
15.1	Aufbau des International Geneva Cyber Security Centres	Cyber Security Center im Bereich der internationalen Organisationen in Genf

Verantwortlich	Kontakt	URL
Armee	gfs.cy@vtg.admin.ch	<a href="https://www.vbs.admin.ch/de/projekt-kommando-cyber">https://www.vbs.admin.ch/de/projekt-kommando-cyber</a>
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	
CYD Campus	cydcampus@ar.admin.ch	<a href="https://www.cydcampus.admin.ch/de">https://www.cydcampus.admin.ch/de</a>

Verantwortlich	Kontakt	URL
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	
Bundesanwaltschaft (BA)	cyber-case@ba.admin.ch	
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	
NEDIK	feedback@cybercrimepolice.ch	<a href="https://cybercrimepolice.ch/de">https://cybercrimepolice.ch/de</a>

fedpol		
Eidgenössisches Justiz- und Polizeidepartement EJPD		<a href="https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?Affairid=20234311">https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?Affairid=20234311</a>
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	

KKPKS		
-------	--	--

Verantwortlich	Kontakt	URL
Eidgenössisches Departement für auswärtige Angelegenheiten (EDA)	ncs@ncsc.admin.ch	

### Führende Rolle in der internationalen Zusammenarbeit

n°	Name der Initiative	Beschreibung
15.2	Global Conference on Cyber Capacity Building (GC3B)	Der strategische Fokus der Konferenz liegt auf der Verknüpfung zwischen Cybersicherheit und internationaler Zusammenarbeit für eine nachhaltige digitale Entwicklung. Gastgeber sind die DEZA und die AIS. Die Konferenz trägt dazu bei, das internationale Genf zu stärken und bezweckt, eine breite politische Unterstützung für die Thematik zu generieren. Mit der GC3B wird ebenfalls die in Zukunft jährlich stattfindende «Geneva Cyber Week» lanciert.
15.3	Geneva Cyber Week	Die Geneva Cyber Week (GCW) nutzt das Genfer Know-how in den Bereichen internationale Zusammenarbeit, multilaterale Diplomatie und Cybersicherheit. Dadurch wird die Position Genfs als wichtiger Knotenpunkt im globalen Cybersicherheitsökosystem gestärkt.
15.4	Geneva Dialogue on Responsible Behaviour in Cyberspace und Geneva Manual	Der Geneva Dialogue erforscht in einem breit abgestützten Multistakeholder-Prozess die Rollen und Verantwortlichkeiten nichtstaatlicher Akteure bei der Umsetzung des UN-Frameworks und dokumentiert die Ergebnisse im Geneva Manual.
15.5	Swiss neutral Data Solutions	Pilotprojekt: In dieser ersten Phase sollen die Bedürfnisse einiger in der Schweiz ansässiger humanitärer und friedensfördernder Organisationen im Bereich des Datenhostings in der Schweiz erfasst und adressiert werden.

#### M16: Internationale Regeln im Cyberraum

16.1	Engagement der Schweiz in der OECD	Stärkung der Cybersicherheit auf internationaler Ebene
16.2	Engagement der Schweiz in der UNO	Stärkung der Cybersicherheit auf internationaler Ebene
16.3	Konvention des Europarats zur Cyberkriminalität (Budapest Konvention)	Stärkung der Cybersicherheit auf internationaler Ebene
16.4	Pall Mall Prozess über Cyberproliferation	Stärkung der Cybersicherheit auf internationaler Ebene
16.5	Vertrauensbildende Massnahmen der OSZE	Stärkung der Cybersicherheit auf internationaler Ebene.

#### M17: Bilaterale Zusammenarbeit zu strategischen Partnern und internationalen Kompetenzzentren

17.1	Bilaterale Dialoge zur Cybersicherheit	Stärkung der Kontakte zu ausgewählten Partnerstaaten
17.2	Counter Ransomware Initiative	Die Schweiz engagiert sich gemeinsam mit ausländischen Partnern in den Arbeitsgruppen der CounterRansomware-Initiative.
17.3	Digital Nodes	Die Abteilung Digitalisierung arbeitet mit ausgewählten Aussenstellen des EDAs zusammen, welche für digitale Themen relevant sind.
17.4	ASEAN Japanese Cyber Capacity Building Center	
17.5	China-European Cyber Dialogue	
17.6	Cyber Mediation – Projekt mit dem Centre for Humanitarian Dialogue (HD)	
17.7	GovCERT international partners exchange	

Verantwortlich	Kontakt	URL
Eidgenössisches Departement für auswärtige Angelegenheiten (EDA)	contact@gc3b.org	<a href="https://gc3b.org/">https://gc3b.org/</a>
Eidgenössisches Departement für auswärtige Angelegenheiten (EDA)	ncs@ncsc.admin.ch	
Eidgenössisches Departement für auswärtige Angelegenheiten (EDA)	genevdialogue@diplomacy.edu	<a href="https://genevdialogue.ch/geneva-manual/">https://genevdialogue.ch/geneva-manual/</a>
Eidgenössisches Departement für auswärtige Angelegenheiten (EDA)	ncs@ncsc.admin.ch	
Bundesamt für Cybersicherheit (BACS)	paris.ocde@eda.admin.ch	<a href="https://www.oecd.org/en/countries/switzerland.html">https://www.oecd.org/en/countries/switzerland.html</a>
Eidgenössisches Departement für auswärtige Angelegenheiten (EDA)	sts.uno@eda.admin.ch	<a href="https://www.eda.admin.ch/eda/de/home/aussenpolitik/internationale-organisationen/vereinte-nationen.html">https://www.eda.admin.ch/eda/de/home/aussenpolitik/internationale-organisationen/vereinte-nationen.html</a>
Eidgenössisches Departement für auswärtige Angelegenheiten (EDA)	ncs@ncsc.admin.ch	
Eidgenössisches Departement für auswärtige Angelegenheiten (EDA)	ncs@ncsc.admin.ch	
Eidgenössisches Departement für auswärtige Angelegenheiten (EDA)	ncs@ncsc.admin.ch	
Eidgenössisches Departement für auswärtige Angelegenheiten (EDA)	ncs@ncsc.admin.ch	
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	
Eidgenössisches Departement für auswärtige Angelegenheiten (EDA)	ncs@ncsc.admin.ch	
Eidgenössisches Departement für auswärtige Angelegenheiten (EDA)	ncs@ncsc.admin.ch	
Eidgenössisches Departement für auswärtige Angelegenheiten (EDA)	ncs@ncsc.admin.ch	
Eidgenössisches Departement für auswärtige Angelegenheiten (EDA)	ncs@ncsc.admin.ch	
Eidgenössisches Departement für auswärtige Angelegenheiten (EDA)	ncs@ncsc.admin.ch	
Bundesamt für Cybersicherheit (BACS)	ncs@ncsc.admin.ch	









