Bericht zur Umsetzung der Nationalen Cyberstrategie (NCS) 2024

Steuerungsausschuss NCS

Mai 2025

Inhalt

1 Vorwort ... 3

2 Highlights der Umsetzung ... 4

3 Einleitung ... 8

3.1 Die Bedrohungslage ... 9
3.2 Der Steuerungsausschuss NCS begleitet die Umsetzung der NCS ... 11

4 Umsetzung der NCS 2024 ... 12

4.1 Strategisches Ziel 1: Selbstbefähigung ... 12
4.1.1 Stand der Umsetzung ... 12
4.1.2 Ausblick des Steuerungsausschuss NCS ... 15

4.2 Strategisches Ziel 2: Sichere und verfügbare digitale Dienstleistungen und Infrastruktur ... 16
4.2.1 Stand der Umsetzung ... 16
4.2.2 Ausblick des Steuerungsausschuss NCS ... 21

4.3 Strategisches Ziel 3: Wirksame Erkennung, Verhinderung, Bewältigung und Abwehr von Cyberangriffen ... 22
4.3.1 Stand der Umsetzung ... 22
4.3.2 Ausblick des Steuerungsausschuss NCS ... 25

4.4 Strategisches Ziel 4: Effektive Bekämpfung und Strafverfolgung der Cyberkriminalität ... 26
4.4.1 Stand der Umsetzung ... 26
4.4.2 Ausblick des Steuerungsausschuss NCS ... 28

4.5 Strategisches Ziel 5: Führende Rolle in der internationalen Zusammenarbeit 29
4.5.1 Stand der Umsetzung ... 29
4.5.2 Ausblick des Steuerungsausschuss NCS ... 32

5 Fokus des Steuerungsausschuss NCS 2025 ... 32

1 Vorwort

Seit der Veröffentlichung der aktuellen Nationalen Cyberstrategie (NCS) im April 2023 hat sich unsere Welt stark gewandelt.

Die Veränderungen der transatlantischen Beziehungen sowie die Entstehung öffentlich zugänglicher grosser Sprachmodelle sind nur die Spitze des Eisbergs der geopolitischen, technologischen und gesellschaftlichen Veränderungen in diesem Zeitraum. Diese Entwicklungen haben tiefgreifende Auswirkungen auf die globale Cyberbedrohungslandschaft und beeinflussen die Schweizer Wirtschaft und Gesellschaft sowohl kurzfristig als auch strategisch.

Als Antwort auf die aktuellen Herausforderungen im Cyberbereich hat die Schweiz bei der Umsetzung der NCS in den fünf strategischen Zielen konkrete Fortschritte erzielt. Der vorliegende Bericht zeigt erste Entwicklungen auf, ohne Anspruch auf eine vollständige Darstellung aller Massnahmen zu erheben.

Trotz der in diesem Dokument dargestellten Fortschritte bei der Umsetzung der NCS dürfen wir uns nicht in falscher Sicherheit wiegen.

Vielmehr erfordert das dynamische Feld der Cyberrisiken unsere kontinuierliche Wachsamkeit und proaktives Handeln, damit die Schweiz ihre vorteilhafte Position zur Nutzung der vielfältigen Chancen in der digitalen Welt erhalten und ausbauen kann. Die Strategie selbst unterliegt deshalb einem kontinuierlichen Evaluationsprozess, um sie angesichts der sich laufend verändernden globalen Rahmenbedingungen bei Bedarf anpassen zu können.

Cybersicherheit liegt nicht allein in der Verantwortung der Regierung oder einzelner Ressorts, sondern bedarf des gemeinsamen Engagements aller Beteiligten. Die erfolgreiche Umsetzung der NCS erfordert nachhaltige Anstrengungen, Unterstützung und finanzielle Mittel der Verwaltung und aller Partner in der Schweiz. Cybersicherheit ist eine gemeinsame Verantwortung und dieser Bericht ist ein Aufruf zum Handeln.

Im Namen des gesamten Steuerungsausschusses möchte ich allen, die an der Umsetzung der NCS mitwirken, herzlich danken!

Maya Bundt,
Präsidentin Steuerungsausschuss NCS

2 Highlights der Umsetzung

Strategisches Ziel 1: Selbstbefähigung

2024 wurden wichtige Grundlagen für die Stärkung von Bildung, Forschung und gesellschaftlicher Sensibilisierung im Bereich Cybersicherheit geschaffen:

Mit Massnahmen wie der S-U-P-E-R-Kampagne 2024 und dem European Cyber Security Month wurde gezielt die breite Öffentlichkeit sensibilisiert. Ergänzend dazu fanden für spezifische Zielgruppen (z.B. für Gemeinden), gesonderte Kampagnen statt.

Gezielte Aus- und Weiterbildungsprogramme wie Studienangebote, Seminare, Hackathons und Kurse wurden lanciert oder ausgeführt und förderten Talente im Bereich Cybersicherheit, um den zukünftigen Bedarf and Expertinnen und Experten zu sichern.

Forschungsergebnisse zu den Themen «Standardisierung», «Quantencomputer und Post-Quanten-Kryptografie», «Large Language Models in Cybersecurity», «Anti-Phishing-Bericht» und «Telefonbetrug im Cyberbereich» wurden publiziert. Sie bilden die Grundlage für strategische Resilienzentscheidungen, stärken das Fachwissen der Schweiz und sensibilisieren für technologische Trends.

Über die Plattform Cyber Security Hub (CSH) und regelmässige Produkte wie wöchentliche Berichte, Briefings, Informationen in sozialen Medien und den Halbjahresbericht wurde die kontinuierliche Verbreitung von Informationen über Cyberbedrohungen an Unternehmen, Behörden und die Öffentlichkeit sichergestellt. So konnten Schutzmassnahmen gezielter angepasst werden.

Durch eine verbesserte Organisation stärkt der Nachrichtendienst des Bundes seine Fähigkeiten im Bereich der Cyberbedrohungserkennung und -kommunikation und trägt damit zu einer fundierten Bedrohungslageeinschätzung sowie zur Stärkung der Cybersicherheit und Resilienz der Schweiz bei.

Strategisches Ziel 2: Sichere und verfügbare digitale Dienstleistungen und Infrastruktur

Die Schweiz setzt sich mit der NCS für sichere und widerstandsfähige digitale Dienste und Infrastrukturen ein. Die NCS fordert die Erkennung und Behebung von Schwachstellen, die Einhaltung von Cybersicherheitsstandards und eine bessere Koordination der Akteure, um die Cyberresilienz zu erhöhen. 2024 wurden zentrale Fortschritte erzielt, die digitale Dienste robuster gemacht, Anzahl von Schwachstellen systematisch reduziert und die Sicherheit von Verwaltung, Wirtschaft und Gesellschaft erhöht haben:

Das nationale Bug-Bounty-Programm führte zur Meldung von 371 Schwachstellen und zur Behebung von 45 kritischer Schwachstellen in Bundesinfrastrukturen.

Die neu aufgebauten Cyber Security Centres in den Sektoren Gesundheit und Bahn erleichtern den Informationsaustausch über Bedrohungen sowie die koordinierte Bewältigung von Cyberangriffen bis hin zu Krisensituationen und stärken die sektorspezifische Frühwarnung und Krisenreaktion.

Zur Stärkung der sektorübergreifenden Vernetzung und Handlungskompetenz unterstützte der Cyber Security Hub aktiv kritische Infrastrukturen, Unternehmen und Organisationen beim Austausch von Informationen. Die Zahl der registrierten Nutzer stieg von 1'000 (2023) auf 3'300 Ende 2024. Die Zahl der teilnehmenden Organisationen liegt bei 1'100.

Die Einführung der Meldepflicht für Cyberangriffe auf kritische Infrastrukturen zum 1. April 2025 legt die Grundlage für bessere Transparenz und Reaktionsfähigkeit bei Cybervorfällen in kritischen Sektoren und eine schweizweites Lageverständnis.

Zur Erhöhung der Cybersicherheit in digitalen Dienstleistungen wurden über 20'000 Phishing-Webseiten identifiziert, rund 1 Million Hinweise zu infizierten Geräten an Betreiber und Internetanbieter weitergeleitet und 8'116 Server identifiziert, die von Cyberkriminellen zur Steuerung von Malware-Infektionen genutzt wurden.

Um die Zusammenarbeit, den Wissensaustausch und den Transfer bewährter Praktiken zwischen Industrie, Hochschulen, Kantonen und Bundesstellen gezielt zu fördern, wurden unter anderem die Nationale Cybersicherheitskonferenz, die CYD Campus Konferenz und thematische Roundtables organisiert.

Strategisches Ziel 3: Wirksame Erkennung, Verhinderung, Bewältigung und Abwehr von Cyberangriffen

Die NCS legt den Schwerpunkt auf die frühzeitige Erkennung und Verhinderung von Cyberangriffen. Mit Massnahmen im Rahmen des Strategischen Ziels 3 soll die Bedrohungslage besser beurteilt werden können und robuste Reaktionen auf Vorfälle etabliert werden. 2024 wurden Grundlagen für den effektiveren Schutz vor Bedrohungen verbessert und die Reaktionsfähigkeit gestärkt:

Teilnahme und Durchführung internationaler (Cyber Europe Exercice für den Energiesektor) und nationaler (z.B. im Finanzsektor) Cyberübungen.
Die Koordination von Krisenübungen wurde verstärkt und ein wissenschaftlicher Beirat eingerichtet, der die Regierung in Fragen der Krisenvorsorge und -bewältigung berät.

Durch die Umsetzung der «Gesamtkonzeption Cyber» wurden die Cyberkapazitäten und -fähigkeiten der Armee weiterentwickelt.

Mit der Koordination eines Cyberlageverbundes konnten Cyberbedrohungen bei internationalen Veranstaltungen wie dem Weltwirtschaftsforums (WEF) und der hochrangige Konferenz zum Frieden in der Ukraine frühzeitig erkannt und bewältigt werden. Die gewonnenen Erkenntnisse werden 2025 weitergeführt, um die Cyberresilienz bei Grossveranstaltungen zu stärken.

Strategisches Ziel 4: Effektive Bekämpfung und Strafverfolgung der Cyberkriminalität

Mit den Massnahmen unter dem Strategischen Ziel 4 legt die NCS den Schwerpunkt auf verbesserte Ermittlungskapazitäten und Koordination zwischen den Justizbehörden, um Cyberkriminalität wirksam bekämpfen zu können.

Die Reichweite der Cybercrimepolice.ch Plattform wurde erweitert. Die Nationalisierung und Integration der Plattform in NEDIK ist in Planung, um eine einheitliche Warn- und Präventionsplattform bezüglich Cyberkriminalität für die gesamte Schweizer Bevölkerung und Polizeikorps zu schaffen.

Cyberwiki, die Wissensplattform rund um das Thema Cyberkriminalität für Polizeikorps, mit rund 890 Nutzern, wurde überprüft und aktualisiert. So konnte sichergestellt werden, dass Kenntnisse und Informationen zur Cyberlage und die sich ändernden Methoden der Cyberkriminalität stets auf dem neuesten Stand bleiben

Die kantonalen Justizbehörden und die Bundesanwaltschaft führten regelmässig Ausbildungsmodule zum Thema Internetkriminalität durch.

Strategisches Ziel 5: Führende Rolle in der internationalen Zusammenarbeit

Die Cybersicherheit ist ein wichtiges Thema in der Aussen- und Sicherheitspolitik. Die Strategie unterstreicht die Bedeutung der internationalen Zusammenarbeit, setzt sich ein für den Respekt des Völkerrechts, die Entwicklung globaler Cybersicherheitsnormen und nutzt die diplomatische Präsenz der Schweiz - insbesondere in Genf - um multilaterale Cyber-Diskussionen zu erleichtern.

Die Schweiz verstärkte partnerschaftliche Beziehungen mit Cybersicherheitsbehörden anderer Länder, einschliesslich bilateraler und multilateraler Gremien wie dem European GovCERT (EGC)- und dem International Watch and Warning Network (IWWN).

Internationale Initiativen wurden geleitet und unterstützt um kollektive/ internationale Widerstandsfähigkeit gegen Cyberherausforderungen zu entwickeln (z.B. Counter Ransomware Initiative[1], Pall Mall Process[2]; Vorsitz der OECD-Arbeitsgruppe «Security in Digital Economy»[3]).

Stärkung der Rolle Genfs in der globalen Cybersicherheit durch internationale Zusammenarbeit und Veranstaltungen, z.B. die Geneva Cyber Week (Mai 2025) und der Global Conference on Cyber Capacity Building (GC3B) (Mai 2025).

Durchführung bilateraler Cybersicherheitsdialoge (z. B. zu Themen wie Attribution, Multilaterale Prozesse etc.) mit elf Ländern (2023/24). Zusammenarbeit mit dem Centre for Humanitarian Dialogue zur Vermittlung bei digitalen Konflikten und zur Verhinderung von Eskalationen.

---

[1] *Counter Ransomware Initiative: eine vom Weissen Haus geleitete Initiative – mit 68 Mitgliedstaaten- die kollektive Widerstandsfähigkeit gegen Ransomware entwickelt und die Mitgliedstaaten bei Ransomware-Angriffen unterstützt* (About Us | International Counter Ransomware Initiative)

[2] *Pall Mall Prozess: im Februar 2024 von Frankreich und dem Vereinigten Königreich lancierten Initiative die darauf abzielt, die Verbreitung und den Missbrauch von kommerziellen Cyber Überwachungs- und Angriffstechnologien und Dienstleistungen durch die Erarbeitung von Leitprinzipien und politischen Optionen einzudämmen* (The Pall Mall Process declaration: tackling proliferation and irresponsible use of commercial cyber intrusion capabilities - GOV.UK))

[3] *OECD-Arbeitsgruppe «Security in Digital Economy» (SDE) – Die AG SDE der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) ist verantwortlich für politischen Analysen, praktischen Anleitungen und Empfehlungen im Umgang mit digitalen Sicherheitsrisiken für wirtschaftliche und soziale Aktivitäten und die Verbesserung der digitalen Sicherheit von Produkten und Dienstleistungen.*

3 Einleitung

Die Cybersicherheit ist ein wesentlicher Grundpfeiler der Sicherheit und wirtschaftlichen Stabilität der Schweiz, besonders in Zeiten zunehmender geopolitischer Spannungen und schnellen digitalen Wandels. Die Bedrohungen im Cyberraum werden komplexer, und sowohl die Häufigkeit als auch das Schadensausmass von Cybervorfällen steigen kontinuierlich.

Seit 2012 setzt die Schweiz kontinuierlich Nationale Cyberstrategien (NCS) um. Die aktuelle Strategie, verabschiedet im April 2023, entwirft eine zukunftsweisende Vision für die Cybersicherheit, die es der Schweiz ermöglicht, die Chancen und Potenziale der digitalisierten Welt optimal zu nutzen.

Die Vision «Die Schweiz nutzt die Chancen der Digitalisierung und mindert Cyberbedrohungen und deren Auswirkungen durch geeignete Schutzmassnahmen. Sie gehört zu den weltweit führenden Wissens-, Bildungs- und Innovationsstandorten in der Cybersicherheit. Die Handlungsfähigkeit und die Integrität ihrer Bevölkerung, ihrer Wirtschaft, ihrer Behörden und der in der Schweiz ansässigen internationalen Organisationen gegenüber Cyberbedrohungen sind gewährleistet» wird über fünf strategische Ziele und 17 daraus abgeleitete Massnahmen umgesetzt.

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

Dieser erste Bericht des Steuerungsausschusses NCS dokumentiert die Fortschritte seit der Verabschiedung der Strategie im April 2023 für das Jahr 2024. Die Erfolge wurden in Zusammenarbeit mit Vertretern aus Wirtschaft, Wissenschaft und Zivilgesellschaft erzielt. Der erste Abschnitt beleuchtet den strategischen Kontext 18 Monate nach Veröffentlichung der NCS. Der zweite Teil (Kapitel 4) fasst die Fortschritte unter den fünf strategischen Zielen detailliert zusammen.

3.1 Die Bedrohungslage

Seit der Publikation der Nationalen Cyberstrategie (NCS) hat sich die Bedrohungslage im Cyberraum erheblich verschärft. Zunehmende geopolitische Spannungen, technologische Innovationen und die fortschreitende Digitalisierung prägen die aktuelle Sicherheitslandschaft. Staatliche Akteure investieren systematisch in offensive Cyberfähigkeiten, während politisch motivierte Gruppierungen Cyberangriffe zur Durchsetzung strategischer und ideologischer Ziele einsetzen. Gleichzeitig wächst die Abhängigkeit von digitalen Infrastrukturen, was neue Angriffsmöglichkeiten eröffnet.

Bedrohungsakteure gehen mit stetig wachsender Raffinesse vor. Global nehmen Ransomware-Attacken, Datenschutzverletzungen und Angriffe auf Lieferketten sowohl in Häufigkeit als auch in Schadenspotenzial weiter zu. Diese Dynamik unterstreicht die Notwendigkeit einer umfassenden, widerstandsfähigen Cybersicherheitsarchitektur. Auch die Bedrohung für die Bevölkerung und insbesondere für kleine und mittlere Unternehmen (KMU) steigt. Vielen KMU und Privatpersonen fehlen die notwendigen Ressourcen oder das Fachwissen, um sich gegen komplexe Angriffe wirksam zu schützen. Dies erhöht das Risiko für die gesamte Wirtschaft.

Dies spiegelt sich in der Zahl der Cybervorfälle wider, die dem Bundesamt für Cybersicherheit (BACS)[4] gemeldet werden. Im Jahr 2024 gingen insgesamt 62'954 freiwillige Meldungen aus der Bevölkerung und von Unternehmen ein. Über die Plattform antiphishing.ch wurden 975’309 Meldungen über verdächtige Websites erfasst. Von diesen wurden über 20'000 Websites als Phishing-Seiten identifiziert. Fast 1 Million infizierte Geräte wie Smartphones, Computer oder IoT-Geräte wurden identifiziert und die jeweiligen Betreiber oder den zuständigen Internet-Provider gewarnt.

62’954
Freiwillige Meldungen zu Cybervorfällen

991’309
Meldungen zu mit Schadsoftware infizierten Geräten analysiert

975'309
Meldungen zu verdächtigen Webseiten, aus welchen über 20'000 Phishing Webseiten erhoben werden konnten.

8’116
Command and Control Systeme identifiziert, die von Attackern für die Steuerung von mit “Malware” infizierten Geräten genutzt wurde.

Weitere Informationen zur aktuellen Bedrohungslage werden für Firmen im Cybersecurity

[4] BACS Jahresbericht 2024

Hub (CSH), der nationalen Austauschplattform zum Vorbeugen vor und effizienten Behandlung von Cybervorfällen geteilt. Für die breite Öffentlichkeit sind auf der Website des BACS[5] und in den Halbjahresberichten[6] weiterführende Informationen verfügbar.

Die NCS verfolgt einen umfassenden Ansatz zur Stärkung der Resilienz auf allen Ebenen – von Individuen über Unternehmen bis hin zu Behörden. Dies umfasst die Sensibilisierung der Bevölkerung, gezielte Aus- und Weiterbildung, Investitionen in Forschung und Innovation so-wie die Bereitstellung klarer, sektorspezifischer Bedrohungs- und Lagebilder. Zudem setzt die NCS auf den gezielten Schutz und die Modernisierung kritischer Infrastrukturen sowie auf eine Stärkung der nationalen Vorfallsbewältigungs-Fähigkeiten. Im Bereich der Cyberkriminalitätsbekämpfung fordert die NCS den Aufbau spezialisierter Kapazitäten bei Strafverfolgungsbehörden sowie die enge Zusammenarbeit auf nationaler und internationaler Ebene. International engagiert sich die Schweiz aktiv für die Sicherheit im digitalen Raum, stärkt die Resilienz internationaler Organisationen und bringt sich in die Entwicklung verbindlicher Regeln für den Cyberraum ein.

Die Cybersicherheitslandschaft wird sich in den kommenden Jahren weiterhin dynamisch entwickeln:

- **Zunahme von Schwachstellen**: Mit der fortschreitenden Digitalisierung und zunehmender Systemkomplexität wird das Management von Sicherheitslücken immer anspruchsvoller
- **Systemische Risiken durch technologische Abhängigkeiten**: Digitale Monokulturen, z.B. Konzentration auf wenige Anbieter, bergen Risiken bei Ausfällen oder Angriffen. Die Förderung technologischer Vielfalt und die Reduktion einseitiger Abhängigkeiten gewinnen an strategischer Bedeutung.
- **Fragmentierung des Cyberraums**: Divergierende nationale Regulierungsansätze könnten die Fragmentierung des Cyberraums verstärken und die internationale Zusammenarbeit und Abstimmung internationaler Standards im Bereich der Cybersicherheit erschweren.
- **Des- und Fehlinformation und die damit verbundene Erosion des Vertrauens in digitale Inhalte**: Cybersicherheit muss künftig verstärkt auch die Integrität und Authentizität von Informationen schützen, nicht nur Verfügbarkeit und Vertraulichkeit.

Die NCS bietet eine solide Grundlage, um den aktuellen und zukünftigen Herausforderungen im Cyberraum zu begegnen. Sie ist zudem flexibel gestaltet und wird regelmässig überprüft, um auf neue technologische, gesellschaftliche und geopolitische Entwicklungen zu reagieren. Dadurch wird langfristig die digitale Souveränität, Resilienz und Innovationskraft der Schweiz gestärkt.

[5] Aktuelle Zahlen (https://www.ncsc.admin.ch/ncsc/de/home/aktuell/aktuelle-zahlen.html)

[6] Halbjahresbericht 2024/1 (https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2024-1.html)

3.2 Der Steuerungsausschuss NCS begleitet die Umsetzung der NCS

Der Steuerungsausschuss NCS wurde im Juni 2024 vom Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) eingesetzt. Die Wirksamkeitsüberprüfung der zweiten NCS (2022) zeigte die Notwendigkeit einer stärkeren strategischen Steuerung und Koordinierung. Daher wurde die Rolle des Steuerungsausschusses erweitert, um seine Unabhängigkeit, strategische Reichweite und Wirksamkeit zu verbessern. Er erfüllt folgende Kernfunktionen:

- **Regelmässige Überprüfung und Strategieentwicklung:** Er überprüft die NCS mindestens alle fünf Jahre, wirkt bei ihrer Weiterentwicklung mit und erarbeitet Anpassungsvorschläge zuhanden des Bundesrates.

- **Vorschlag von zusätzlichen Massnahmen und Prioritäten:** Er unterbreitet dem Bundesrat bei Bedarf Vorschläge für ergänzende Massnahmen. In Abstimmung mit den in der NCS genannten Umsetzungspartnern erarbeitet er Vorschläge zu den Prioritäten für die Umsetzung der NCS.

- **Jährliche Berichterstattung:** Er erstattet dem Bundesrat, den Kantonen und der Öffentlichkeit jährlich Bericht über die Umsetzung der NCS.

Das Bundesamt für Cybersicherheit (BACS) fungiert als Geschäftsstelle des Steuerungsausschusses und bringt Informationen und Einschätzungen des Steuerungsausschusses zuhanden des Bundesrates und der Kantone.

Dem Steuerungsausschuss NCS, unter dem Vorsitz von Dr. Maya Bundt, gehören Vertreter der Kantone, des Bundes, der Privatwirtschaft, der Zivilgesellschaft und der Wissenschaft an. Die Mitglieder wurden aufgrund ihrer strategischen Expertise in einem Themenbereich der Cybersicherheit bestimmt. Diese vielfältige Zusammensetzung gewährleistet unterschiedliche Sichtweisen und einen gesamtgesellschaftlichen Ansatz für die Cybersicherheit und die Umsetzung der NCS.

4 Umsetzung der NCS 2024

Die NCS bildet den Rahmen für alle laufenden Arbeiten zur Verbesserung der Cybersicherheit in der Schweiz. Sie gibt einen Überblick über die Hauptakteure, die die strategischen Vorhaben, Projekte und Programme umsetzen - einige davon wurden bereits eingeleitet, andere sind schon fortgeschritten. Die Umsetzung der NCS in den Kantonen schreitet ebenfalls voran. Ende 2024 hat die Fachgruppe Cybersicherheit ihre Arbeit aufgenommen, um den Informationsaustausch zwischen Bund, Kantonen und Gemeinden sicherzustellen und die Themen Selbstbefähigung, Resilienz und Vorfallmanagement zu unterstützen. Die Fachgruppe wird gemeinsam vom BACS und dem Sicherheitsverbund Schweiz (SVS) geleitet.

Der erste Umsetzungsbericht dokumentiert Fortschritte und benennt Handlungsfelder für zukünftigen Fokus. Die Informationen wurden vom NCS-Koordinationsteam im BACS durch bilaterale Gespräche und eine Umfrage erhoben. Der Bericht stellt eine Bestandsaufnahme dar; bestehende Lücken werden im Verlauf der Koordinierungsarbeit 2025 sukzessive identifiziert und bearbeitet. Das NCS-Koordinationsteam ergänzt das NCS-Portfolio fortlaufend mit neuen Vorhaben, die einen dreistufigen Bewertungsprozess durchlaufen. Bewertungsrahmen und Antragsformular werden im zweiten Quartal 2025 auf der Website des BACS[7] veröffentlicht.

4.1 Strategisches Ziel 1: Selbstbefähigung

4.1.1 Stand der Umsetzung

Sensibilisierungsmassnahmen erhöhen die nationale Resilienz

Die Fähigkeiten der Gesellschaft im Bereich der Cybersicherheit sind entscheidend für die nationale Resilienz. Die Sensibilisierung für Cyberbedrohungen ist ein wichtiger Aspekt der Selbstbefähigung. Landesweite Kampagnen, wie die Kampagne S-U-P-E-R[8] (2021 – 2024), klärten über Bedrohungen wie Phishing und Ransomware auf und vermittelten bewährte Praktiken. Im Jahr 2025 werden Organisationen aus Bund, Kantonen, Wirtschaft und Hochschulen auf diesen Kampagnen aufbauen, um die Bevölkerung weiter zu sensibilisieren. Der Beitrag der Schweiz zum European Cyber Security Month (ECSM) 2024 wird in der untenstehenden Fallstudie vorgestellt.

[7] BACS NCS Webseite – Information zu neuen Vorhaben (https://www.ncsc.admin.ch/ncsc/de/home/strategie/neue-ncs-vorhaben.html)

[8] Kampagne SUPER (S-U-P-E-R.ch)

Fallstudie - Das Bewusstsein für Cybersicherheit durch massgeschneiderte Ansätze schärfen.

Der European Cyber Security Month (ECSM) wird von der Agentur der Europäischen Union für Cybersicherheit (ENISA) in Zusammenarbeit mit den EU-Mitgliedstaaten organisiert. Im Jahr 2024 unterstützte das BACS den ECSM mit einer Kampagne zur Sensibilisierung für Social-Engineering-Angriffe mit Deepfake-Technologie.

Zusammen mit «Jugend und Medien» und «seniorweb.ch» entwickelte das BACS gezielte Inhalte für Jugendliche, Fachleute und Senioren. Die Kampagne umfasste ein kurzes Video über die Erstellung von Deepfake-Videos, ein Online-Meeting zur Diskussion des Themas, ein Erklärungsvideo für ältere Menschen und weitere Informationen auf der Website des BACS. Das Sensibilisierungsvideo wurde auf YouTube[9] in vier Sprachen veröffentlicht.

Für Branchen, die mit besonderen Herausforderungen im Bereich der Cybersicherheit konfrontiert sind, wurden sektorspezifische Leitlinien erstellt. Seminare, Workshops und gezielte Veröffentlichungen haben Unternehmen mit den Instrumenten und Kenntnissen ausgestattet, die sie benötigen, um robuste, auf ihre betrieblichen Gegebenheiten zugeschnittene Cybersicherheitsmassnahmen umzusetzen. Regelmässige «Brown-Bag-Lunches» mit Gemeinden wurden veranstaltet, um Empfehlungen zum Umgang mit Cyberbedrohungen abzugeben. Das BACS hat in Zusammenarbeit mit der Planzer Transport AG ein Pilotprojekt zur Cybersicherheit in der Lieferkette[10] durchgeführt. Die Ergebnisse des Projekts werden nicht nur der Logistik- und Transportbranche zugute-kommen, sondern ab 2025 auch KMUs der ganzen Schweiz.

Über die Plattform Cyber Security Hub (CSH) sowie durch regelmässige Produkte – darunter

[9] NCSC - National Cyber Security Centre Switzerland - YouTube

[10] Cybersicherheit in der Lieferkette (https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/lieferkette.html)

wöchentliche Berichte und Briefings, der Halbjahresbericht und wöchentliche Informationen auf sozialen Medien – wurde die kontinuierliche Verbreitung von Informationen über Cyberbedrohungen an Unternehmen, Behörden und die Öffentlichkeit sichergestellt.

Partnerschaften zwischen Hochschulen, Industrie und Behörden zur Stärkung der Innovation und der Pipeline an qualifizierten Fachkräften

Der Cyber-Defence Campus (CYD Campus) hat in Zusammenarbeit mit der École polytechnique fédérale de Lausanne (EPFL) im Jahr 2020 das CYD Fellowship Programm ins Leben gerufen, um Studierenden die Möglichkeit zu geben, sich mit Cyberabwehr zu befassen und das Fachwissen der Schweiz zu stärken. Seit seiner Einführung ist das Programm stetig gewachsen und konnte 2024 seine ersten Proof-of-Concept Fellows[11] sowie drei Postdoctoral, sechs Doctoral, und 12 Master Fellows aufweisen.

Besseres nationales Bedrohungsbild

Der Nachrichtendienst des Bundes (NDB) hat im Rahmen der laufenden Transformation seine Strukturen zur frühzeitigen Erkennung, Beurteilung und Verhinderung von Cyberbedrohungen und -angriffen optimiert. Das Hauptziel dieser Veränderungen war es, die Effizienz und Flexibilität des Dienstes zu steigern. Der NDB intensiviert kontinuierlich seine Zusammenarbeit mit anderen Behörden im Cyberbereich.

Trends und Entwicklungen im Bereich der Cybersicherheit

Die NCS fokussiert unter anderem auf die Erforschung der Risiken und Chancen neuer Technologien und Methoden für die Cybersicherheit. Das BACS hat durch Analysen verschiedener Technologien, die sich auf die Cybersicherheit auswirken, durchgeführt, darunter «Post-Quantum-Kryptographie», «Quantencomputer» und «Zero Trust». Die Ergebnisse sind auf der BACS-Website[12] abrufbar. Zusätzlich erarbeitet das BACS momentan eine strukturierte Methodik zur Stärkung der Cybersicherheit, die sich am National Institute of Standards and Technology (NIST) Cyber Security Framework orientiert aber an die Bedürfnisse und Rahmenbedingungen der Schweiz angepasst ist. Die erarbeitet Methodik soll in Zukunft den IKT-Minimalstandard[13] ersetzen

Der CYD-Campus hat Forschungsartikeln und Studien zu verschiedenen neuen Technologien und Methoden publiziert[14]. Zudem wurde die Technology Market Monitoring (TMM 2.0) Plattform so weiterentwickelt, dass diese nun auch Patentdaten nutzt, um für die Cybersicherheit relevante technologische Trends zu identifizieren. Weiter wurden das Technologiemonitoring im Bereich der Quantentechnologien intensiviert. Der Einbeziehung von Quantensicherheitsrisiken stellt sicher, dass entsprechende Bedrohungen, insbesondere deren praktische Relevanz, frühzeitig erkannt werden. Eine Studie über generative KI-Risiken hat

---

[11] *Bei einem Proof of Concept (PoC) wird ein Prototyp eines Produkts oder einer Dienstleistung für die Cyberverteidigung auf der Grundlage eines Konzepts oder einer Idee (z.B. aus einer Masterarbeit oder einem Doktorat) validiert und auf seine Machbarkeit hin überprüft.*

[12] BACS-Berichte (https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte.html) und Technologiebetrachtungen (https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/technologiebetrachtung.html

[13] Empfehlungen IKT-Minimalstandards (https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/ikt-minimalstandards.html)

[14] CYD-Campus Publikationen: Large Language Models in Cybersecurity: Threats, Exposure and Mitigation | SpringerLink; Trends in Data Protection and Encryption Technologies | SpringerLink

die Auswirkungen grosser Sprachmodelle auf die Cybersicherheit analysiert und ihren potenziellen Missbrauch für Deepfakes, Desinformation und Betrug aufgezeigt. Ausführlichere Informationen zu diesen und weiteren Initiativen finden sich im CYD Campus Jahresbericht[15].

Um Trends, Risiken und Abhängigkeiten frühzeitig zu verstehen, untersucht das Nationale Testinstitut für Cybersicherheit (NTC) digitale Technologien und Entwicklungen. So hat das NTC potenzielle Risiken im Zusammenhang mit Systemabhängigkeiten Europas[16] und die Apps Temu[17] und TikTok[18] (in Absprache mit dem BACS) untersucht und konkrete Handlungsempfehlungen abgegeben.

Gemeinsam bilden diese Arbeiten die Grundlage für strategische Resilienzentscheidungen, stärken das Fachwissen der Schweiz und sensibilisieren für technologische Trends

4.1.2 Ausblick des Steuerungsausschuss NCS

Für die Widerstandsfähigkeit der Schweiz im Bereich der Cybersicherheit ist es entscheidend, dass Einzelpersonen, Unternehmen und öffentliche Einrichtungen über die notwendigen Fähigkeiten und Kenntnisse verfügen. Trotz wichtiger Initiativen im vergangenen Jahr muss weiter investiert werden.

Partnerschaften zwischen Wissenschaft, Industrie und Regierung sind unerlässlich, um qualifizierte Fachkräfte zu sichern. Die Schweiz muss als globales Innovations-zentrum für Cybersicherheit positioniert werden und Forschungsergebnisse für Politik und Regulierung nutzen.

Bedrohungsinformationen müssen leicht zugänglich und für Entscheidungsträger im öffentlichen und privaten Sektor nutzbar sein. Die Schweiz kann sich als welt-weit führend in der Cybersicherheitsausbildung und -innovation etablieren, durch öffentlich-private Partnerschaften und die Förderung von Start-ups und Scale-ups.

Die Überwachung technologischer Risiken hat sich verbessert, aber Abhängigkeiten und Schwachstellen müssen weiter systematisch identifiziert werden. Geopolitische Spannungen verschärfen die Risiken technologischer Abhängigkeiten. Ein ausgewogener Ansatz zur Förderung inländischer Innovation und Diversifizierung der Technologieanbieter ist notwendig, um systemische Risiken zu mindern und die digitale Widerstandsfähigkeit langfristig zu gewährleisten.

[15] CYD Campus Jahresbericht (https://www.cydcampus.admin.ch/en/annual-report)

[16] NTC-Bericht «Der Systemabhängigkeit entkommen – Für eine resiliente digitale Zukunft Europas» (https://www.ntc.swiss/hubfs/20241216-kurzbericht-systemabhaengigkeiten-ntc-de.pdf)

[17] NTC-Bericht «Technische Sicherheitsanalyse Mobile App «Temu» (https://www.ntc.swiss/hubfs/temu-sicherheitsanalyse-ntc-de.pdf)

[18] NTC-Bericht «Technische Sicherheitsanalyse Mobile App «TikTok» (ntc-security-analysis-tiktok-v1-0-de.pdf)

4.2 Strategisches Ziel 2: Sichere und verfügbare digitale Dienstleistungen und Infrastruktur

Mit der NCS setzt sich die Schweiz dafür ein, dass digitale Dienste und Infrastrukturen sicher und widerstandsfähig bleiben. Die Strategie fordert die Erkennung und Behebung von Schwachstellen, die Einhaltung von Cybersicherheitsstandards und eine bessere Koordination zwischen Bund, Kantonen und Privatsektor, um die allgemeine Cyberresilienz zu erhöhen.

Im November 2024 nahmen Mitglieder des Steuerungsausschusses an einer Sitzung des Beirats Digitale Schweiz teil[19], um die Bedeutung der Cybersicherheit zu diskutieren. Diese Sitzungen und der anhaltende Fokus auf Cybersicherheit unterstreichen das Engagement der Schweiz, die Herausforderungen der Digitalisierung im Cyberbereich anzugehen.

4.2.1 Stand der Umsetzung

Identifizierung und Adressierung von Schwachstellen

Das Bug-Bounty-Programm des BACS reduzierte Schwachstellen und erhöht die Cyberresilienz in der Bundesverwaltung. Schwachstellen in IT-Systemen gehören zu den häufigsten Eingriffswegen für Cyberangriffe. In der **Bundesverwaltung** wird seit 2022 ein Bug-Bounty-Programm umgesetzt. Im Jahr 2024 gingen insgesamt 371 Schwachstellenmeldungen von ethischen Hackern ein. Davon wurden 239 nach technischer Analyse als gültig eingestuft. Zwölf Prozent der gültigen Schwachstellen, insgesamt 45 Meldungen, wurden als «kritisch» eingestuft und deshalb innerhalb der Bundesverwaltung mit höchster Priorität behandelt und

[19] Medienmitteilung «Beirat Digitale Schweiz: Cybersicherheit wichtige Basis für die Digitalisierung» (news.admin.ch/de/nsb?id=103074)

unverzüglich behoben.

Angesichts des zunehmenden Einsatzes von Open-Source-Software (OSS) Produkten ist deren Cybersicherheit ein zunehmend wichtiges Thema. 2024 startete das BACS in Zusammenarbeit mit dem NTC ein Pilotprojekt zur Prüfung von zwei häufig verwendete OSS-Produkte. Diese Initiative zielt darauf ab, die Transparenz und Sicherheit von OSS zu erhöhen, Angriffs-flächen zu reduzieren und die Cyberresilienz zu stärken. Sie unterstützt auch die internationale OSS-Entwicklergemeinschaft und trägt zur globalen Cybersicherheit bei.
Im Jahr 2024 hat das NTC zusätzlich Cybersicherheitsanalysen von drei der meistgenutzten Klinikinformationssysteme (KIS) mehrerer Schweizer Spitälern[20] und der Ladeinfrastruktur für Elektromobilität[21] durchgeführt. Den Herstellern wurden schwerwiegende Schwachstellen gemeldet, welche behoben werden konnten.

Der CYD-Campus verstärkte seine Aktivitäten im Bereich der Identifikation technischer Schwachstellen in durch armasuisse beschafften Systemen sowie weiteren kritischen Systemen (z.B. E-ID) und Infrastrukturen (z.B. Weltraum und Mobilität). Zusammen mit Partnern aus Behörden, der Akademie und Industrie publizierte er im Jahr 2024 verschiedene Beiträge zu Schwachstellen in kritischen Systemen (z.B. dem für das Funktionieren des Internets zentralen Domain-Name System) und zur Verbesserung und Effizienzsteigerung der Tools und Methoden zum Finden und Analysieren von Schwachstellen (z.B. das BlueToolkit[22] zur Prüfung von Geräten mit Bluetooth Schnittstelle; Morion[23]). Ebenfalls im Fokus standen Methoden und Tools zur Erkennung von Risiken und Schwachstellen bei KI-Modellen und Systemen. Hier wurde mittels der Startup Challenges innovative Lösungen gesucht. Die Siegerlösung wird 2025 in einem Proof-of-Concept beim Bund erprobt. Um die Zusammenarbeit und Fähigkeiten bei der Schwachstellenidentifikation zu stärken, führt der CYD-Campus jährlich Hackathons mit Teilnehmenden aus Verwaltung, Wissenschaft und Industrie durch. Technologiebereiche mit Nachholbedarf stehen dabei im Fokus. Weitere Informationen finden sich im CYD Campus Jahresbericht[24].

Ab Januar 2025 verstärkt das Bundesamt für Kommunikation (BAKOM) mit der Abteilung «Marktzugang und Cybersicherheit» sein Engagement im Bereich der Cybersicherheit. Die Abteilung wird ab August 2025 dafür zuständig sein internetfähige Funkanlagen (z.B. Smartphones, Smartwatches, Fitnesstracker, Spielzeuge oder Babyfone) auf Cybersicherheit zu prüfen. Diese Anforderungen sind in der Verordnung des BAKOM über Fernmeldeanlagen festgelegt.

[20] NTC-Bericht «Cybersicherheit von Klinikinformationssystemen» (250123-ntc-summarischer-bericht-kis-de.pdf)

[21] NTC-Bericht «Sicherheitsanalyse öffentliche Ladeinfrastruktur für Elektromobilität» (ntc-security-analysis-e-mobility-charging-de.pdf)

[22] https://github.com/sgxgsx/BlueToolkit

[23] https://github.com/cyber-defence-campus/morion

[24] CYD-Campus Jahresbericht (https://www.cydcampus.admin.ch/en/annual-report)

Verbesserung der Cyberresilienz von Gemeinden und Kleinen und Mittleren Unternehmen (KMUs)

Das 2018 gegründete Cyber-Safe-Label hat sich weiterentwickelt, um zur Verbesserung der Cybersicherheit in Schweizer Gemeinden und KMUs beizutragen. Das Label schafft ein Anreizsystem für mehr Cybersicherheit, zum Beispiel durch Partnerschaften mit Versicherern und reduzierte Prämien für zertifizierte Unternehmen. 2023 wurden die Bewertungsanforderungen unter Beteiligung zahlreicher Stakeholder und KMU-Vertreter überprüft und aktualisiert. Zu den Entwicklungen im kommenden Berichtszeitraum gehören die Expansion in der deutschsprachigen Schweiz, neue Partnerschaften und die Steigerung des Bekanntheitsgrades. Die nächste Überprüfung der Anforderungen ist für 2025 geplant. Aktuell haben rund 350 Organisationen (Gemeinden und KMUs) sich mit dem Label Cyber-Safe engagiert.

Das CyberSeal-Label zeichnet IT-Dienstleister aus, die mit geeigneten technischen und organisatorischen Massnahmen ihren Kunden ein angemessenes Schutzniveau vor Cyberrisiken garantieren. Die CyberSeal Audit Anforderungen werden jährlich überprüft und mit neuen Bedrohungslage abgeglichen. Das Gütesiegel unterstützt KMUs bei der Suche nach geeigneten externen IT-Dienstleistern und leistet einen Beitrag zur Erhöhung der Cyber-Resilienz der Schweizer KMUs. Seit der Gründung des CyberSeal-Labels (2021) hat sich das Vorhaben vom Pilotprojekt zu einem etablierten Qualitätsstandard entwickelt: Insgesamt 57 IT-Dienstleister wurden bis heute erfolgreich zertifiziert. Das Label, das gemeinsam mit dem BACS entwickelt wurde, wird aktiv für die Zusammenarbeit mit IT-Providern empfohlen und stärkt durch transparente Prozesse sowie strenge Standards das Vertrauen in die Schweizer IT-Dienstleistungsbranche nachhaltig.

Cyberresilienz kritischer Infrastrukturen

Die Cybersicherheit von kritischen Infrastrukturen ist eine Priorität der NCS und wird in enger Abstimmung mit der nationalen Strategie vom Bundesamt für Bevölkerungsschutz (BABS) zum Schutz kritischer Infrastrukturen[25] koordiniert. Die 27 Sektoren der kritischen Infrastrukturen werden periodisch überprüft, um festzustellen, ob Schwachstellen und Risiken bestehen, die zu schwerwiegenden Störungen und Ausfällen führen könnten, und ob zusätzliche Massnahmen zur Verbesserung der Widerstandsfähigkeit erforderlich sind. Diese Massnahme wird vom BABS koordiniert und durch die Fachämter durchgeführt und soll sicherstellen, dass die einzelnen Bereiche der kritischen Infrastrukturen (Stromversorgung, Telekommunikation, Strassenverkehr usw.) über eine angemessene Resilienz verfügen. Die Methodik der Resilienzüberprüfung wurde 2024 überarbeitet und wird in den kommenden Jahren in den 27 Sektoren angewendet. Aktualisierungen und weitere Informationen können auf der BABS-Website[26] abgerufen werden

Der Cyber Security Hub (CSH) des BACS unterstützte kritische Infrastrukturen, Unternehmen und Organisationen, indem er eine Plattform für den Austausch von Informationen über Cyberbedrohungen und -massnahmen bietet. Die Zahl der teilnehmenden Organisationen liegt nun bei 1'100. Die Zahl der registrierten Nutzer stieg von 1’000 (2023) auf 3’300 Ende 2024 (*pro Organisation können mehrere Nutzerinnen und Nutzer registriert werden*).

[25] Nationale Strategie zum Schutz kritischer Infrastrukturen (https://www.babs.admin.ch/de/nationale-strategie-zum-schutz-kritischer-infrastrukturen)

[26] Die kritischen Infrastrukturen (https://www.babs.admin.ch/de/die-kritischen-infrastrukturen)

Die Meldepflicht für Cyberangriffe auf kritische Infrastrukturen tritt ab 1. April 2025 in Kraft. Betreiber kritischer Infrastrukturen müssen Cyberangriffe innerhalb von 24 Stunden nach Entdeckung an den BACS melden und haben dann 14 Tage Zeit, ihre Meldung zu vervollständigen. Auf dem CSH steht ihnen ein entsprechendes Meldeformular zur Verfügung. Die Meldepflicht legt die Grundlage für bessere Transparenz und Reaktionsfähigkeit bei Cybervorfällen in kritischen Sektoren und eine schweizweites Lageverständnis.

Fallstudie: Vertiefung der sektorspezifischen Cyberresilienz durch Cybersicherheitszentren (Cyber Security Centres)

Um die sektorspezifische Widerstandsfähigkeit zu stärken, unterstützt das BACS die Entwicklung von Cyber Security Centres (CSCs). Diese sektorspezifische Zentren für präventive Cybersicherheitsmassnahmen arbeiten in Partnerschaft mit dem BACS und berücksichtigen die Anforderungen der sektoralen Akteure.

Zu den etablierten CSCs gehören der FS-CSC[27] mit dem Finanzsektor und dem Verband der Schweizer Industrie für Cyber-Sicherheit («Swiss Industry Cyber-Security Association» SWICYBA), ein Zusammenschluss von rund einem Dutzend Industrieunternehmen. Beide CSCs erweitern ihre Dienstleistungen für ihre Sektoren.

Das Rail-ISAC ((Information Sharing and Analysis Center) und der Healthcare-CSC befinden sich in der Umsetzungsphase:

- Das Rail-ISAC stellt seinen Mitgliedern sektorspezifische Cyber Threat Intelligence, Analysekapazitäten sowie Unterstützung bei Sicherheitsvorfällen zur Verfügung. Ein besonderer Schwerpunkt liegt auf dem Schutz der Operational-Technology-Umgebungen im Bahnsektor. Damit unterstützt das Rail-ISAC seine Mitglieder dabei, ihre Infrastrukturen sicherer und widerstandsfähiger gegenüber Cyberangriffen zu gestalten, Bedrohungen frühzeitig zu erkennen und im Ernstfall schneller und gezielter reagieren zu können.
- Das Projekt «Healthcare Cyber Security Centre (H-CSC)» wurde 2024 lanciert und zielt darauf ab, einen Verein zu gründen, der die Synergien und die Zusammenarbeit im Bereich der Cybersicherheit für Schweizer Spitäler stärkt, Fachwissen bündelt und sie bei Cybervorfällen unterstützt. Nach Abschluss des Pilotprojektes (Februar 2025), wird der H-CSC voraussichtlich im Sommer 2025 formell gegründet. Nach seiner Gründung wird sich das H-CSC in zwei Phasen ausweiten: (1) Integration von Mitgliedern aus allen Universitäts- und Kantonsspitälern und (2) Öffnung des H-CSC für alle Spitäler in der Schweiz mit einem Leistungsauftrag. Weitere Informationen sind auf der Website des H-CSC abrufbar.[28]

Im Eidgenössischen Departement für auswärtige Angelegenheiten (EDA), Abteilung Digitales, ist der Aufbau des Internationalen Genf CSC (IG-CSC) in Planung. Das CSC soll proaktive und reaktive Unterstützung für internationale und humanitäre Organisationen in der Schweiz bieten. Ein Proof-of-Concept wurde entwickelt und wird in Abhängigkeit von den Ressourcen umgesetzt werden. Diese Initiative trägt auch zum strategischen Ziel 5 bei.

[27] Cyber-Sicherheitszentrum des Schweizer Finanzsektors (https://fscsc.ch/)

[28] Zentrum für Cybersicherheit im Gesundheitswesen (https://h-csc.ch/)

Zusammenarbeit fördern - Gezielter Wissensaustausch, Transfer bewährter Praktiken und die Zusammenarbeit zwischen Industrie, Hochschulen, Kantonen und Bundesstellen.

In Zusammenarbeit mit dem SVS veranstaltete das BACS die jährliche **Nationale Cybersicherheitskonferenz** die den Austausch zwischen Bund, Kantonen, Gemeinden, Wirtschaft und Gesellschaft fördert. Im Jahr 2024 fokussierte sich die Konferenz auf das Thema «Geopolitik und operationelle Sicherheit» und zog über 280 Teilnehmende an. 93% der Teilnehmenden bewerteten die Veranstaltung als gut oder ausgezeichnet. Die Nationale Cybersicherheitskonferenz 2025 findet am 25. September statt.

Cyber Defence Campus Konferenz 2024

Die Veranstaltung im Zeichen wegweisender Cybertechnologien fand in Bern statt. Über 300 Teilnehmende aus Verwaltung, Industrie und Wissenschaft tauschten sich über Quantum Computing, Next-Generation-Netze und KI aus. Keynotes, Vorträge und ein Panel machten die Konferenz zu einem Treffpunkt für die Community. Eingebettet in die Konferenz war auch die Prämierung des Gewinners der Cyber Startup Challenge, bei der im Jahr 2024 Lösungen zum Thema Sicherheit von künstlicher Intelligenz gesucht wurden.

4.2.2 Ausblick des Steuerungsausschuss NCS

Seit der Veröffentlichung der NCS wurden grundlegende Fortschritte erzielt. Es bleibt jedoch von höchster Priorität, dass alle IT-Systeme des Bundes und kritischen Infrastrukturen über ein voll funktionsfähiges Schwachstellenmanagementprogramm verfügen, das proaktive Schwachstellenerkennung und schnelle Reaktionsmechanismen umfasst.

Das Bug-Bounty-Programm hat sich als wirksames Instrument erwiesen, um sicherheitsrelevante Schwachstellen in der IT des Bundes frühzeitig zu erkennen und gezielt zu beheben. Solche Programme – ob Bug-Bounty-Formate oder vergleichbarer Ansätze – leisten einen wichtigen Beitrag zur Stärkung der Cybersicherheit des Bundes. Angesichts der dynamischen Bedrohungslage im digitalen Raum ist ein kontinuierlicher Mechanismus zur Schwachstellenidentifikation unerlässlich. Der Ausschuss betont daher die Notwendigkeit eines solchen Programmes als festen Bestandteil der Sicherheitsarchitektur des Bundes.

Die Einführung von Cybersicherheitsvorschriften, einschliesslich der Meldepflicht für Cybervorfälle in kritischen Infrastrukturen, stellt einen wichtigen Schritt dar. Entscheidend ist jedoch, dass deren Umsetzung kontinuierlich evaluiert wird, um sicherzustellen, dass sie tatsächlich zu einer spürbaren Erhöhung der Resilienz in allen betroffenen Sektoren führt.

Die Entwicklung sektorspezifischer Cyber Security Centres (CSCs) markiert einen bedeutenden Fortschritt für die Cyberresilienz kritischer Infrastrukturen. Erfolgreiche Initiativen im Finanz-, Industrie-, Bahn- und Gesundheitssektor zeigen, dass CSCs gezielt auf branchenspezifische Risiken eingehen und den Austausch sowie die Reaktionsfähigkeit stärken.

Die Zusammenarbeit im öffentlichen Sektor hat sich verbessert, jedoch müssen die Governance-Modelle weiter formalisiert werden, um eine nahtlose Kooperation zwischen Bund, Kantonen und Gemeinden zu gewährleisten.

4.3 Strategisches Ziel 3: Wirksame Erkennung, Verhinderung, Bewältigung und Abwehr von Cyberangriffen

Die NCS legt den Schwerpunkt auf die frühzeitige Erkennung und Verhinderung von Cyberangriffen. Mit Massnahmen im Rahmen des Strategischen Ziels 3 soll die Bedrohungslage besser beurteilt werden können und robuste Reaktionen auf Vorfälle etabliert werden. Durch die systematische Analyse von Cybervorfällen wird eine kontinuierliche Verbesserung sichergestellt.

4.3.1 Stand der Umsetzung

Angepasste Organisationsstrukturen der Cybersicherheit

Um die Organisationsstrukturen der Cybersicherheit in der Schweiz zu stärken, haben am 1. Januar 2024 die beiden neuen Verwaltungseinheiten im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS), das Staatssekretariat für Sicherheitspolitik (SEPOS) und das BACS, ihre Tätigkeit aufgenommen:

- **SEPOS** ist das Kompetenzzentrum des Bundes für Sicherheitspolitik und Informationssicherheit in der Verwaltung. Es beobachtet sicherheitspolitische Entwicklungen und bereitet strategische Handlungsoptionen für politische Entscheidungsträger vor.
- Das **BACS** koordiniert die Umsetzung der NCS. Als Kompetenzzentrum des Bundes für Cybersicherheit ist es erste Anlaufstelle für die Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen. Ausserdem koordiniert das BACS die Arbeiten des Bundes im Cyberbereich.
- Im Bereich der Cyberdefence wurde das **Kommando Cyber** eingerichtet (Dezember 2023). Es ist für die Bereitstellung von Diensten im Cyber- und elektromagnetischen Bereich zuständig und sorgt so dafür, dass Daten schnell und effizient ausgetauscht werden können.

Vorbereitung auf Cyberangriffe durch Cyberübungen

Die NCS unterstreicht die Bedeutung der Vorbereitung durch regelmässige Cyberübungen, um die Reaktionsfähigkeit zu testen. Der Bericht des Bundesrates[29] zu Cybersicherheitsübungen in der Bundesverwaltung und der Armee in Beantwortung des Postulats 22.4081[30] umfasst drei strategische Ziele: Stärkung der internen Koordination und Zusammenarbeit, Standardisierung der Vor- und Nachbereitung von Übungen und Institutionalisierung der Zusammenarbeit auf Bundes- und internationaler Ebene. Das BACS wird eine zentrale Koordinationsrolle übernehmen und die Zusammenarbeit in der Bundesverwaltung vorantreiben, um sicherzustellen, dass Cybersicherheitsoperationen in Krisenmanagementübungen integriert werden und die Zusammenarbeit verstärkt wird.

[29] Cyberübungen in der Bundesverwalttung und der Armee (https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/dokumentation/berichte/Bericht_Cyberuebungen_in_der_Bundesverwaltung_und_der_Armee.pdf.download.pdf/Bericht_Cyberuebungen_in_der_Bundesverwaltung_und_der_Armee.pdf)

[30] Postulat Übergeordnete Cyber-Teststrategie im VBS (22.4081 | Übergeordnete Cyber-Teststrategie im VBS | Geschäft | Das Schweizer Parlament)

Im Jahr 2024 hat das BACS an internationalen (z.B. Cyber Europe Exercice für den Energiesektor) und nationalen (z.B. im Finanzsektor) Cyberübungen teilgenommen. Um die Kantone und kritischen Infrastrukturen in diesem Bereich in Zukunft besser zu unterstützen, hat der Kanton Wallis unter Einbezug des BABS und des BACS eine Krisenübung durchgeführt, bei welcher das Szenario eines Cyberangriffs auf Behörden des Kantons durchgespielt wurde. Die daraus gewonnenen Erkenntnisse tragen dazu bei, die Planung und Durchführung von zukünftigen Krisenübungen mit Betreiberinnen kritischer Infrastrukturen zu verbessern.

Der Bundesrat will sicherstellen, dass das BACS bei grossen oder systemischen Cybervorfällen schneller und effizienter von der Armee (Kommando Cyber) unterstützt werden kann. Im September 2024 wurde das VBS beauftragt, die Rechtsgrundlage für diese Unterstützung zu prüfen. Dieser Entscheid stützt sich auf den Bericht[31] der Sicherheitspolitischen Kommission des Nationalrates zur Subsidiarität und Internetsicherheit. Dies ermöglicht dem BACS und dem Kommando Cyber schnelle und effiziente Zusammenarbeit mit klaren Rollen und Verantwortlichkeiten.

Im Rahmen des Pilotprojekts «Cyber Training @ CYD Campus» wurde zudem im Mai 2024 eine Krisensimulation mit 20 Personen aus kritischen Infrastrukturen, Polizeieinheiten, kantonalen und Bundesbehörden sowie deren Dienstleister durchgeführt. Während der Simulation wurden die Teilnehmenden mit einem fiktiven Szenario, wo ein Energieversorgungsunternehmen der Stadt Zürich eine Cyber-Krise bewältigen muss, konfrontiert. Die Teilnehmenden konnten wertvolle Erfahrungen sammeln und erhielten wichtige Erkenntnisse darüber, wie sie ihre internen Prozesse verbessern können. Die positive Resonanz und die Lessons Learned betonen die Bedeutung solcher Übungen für die Stärkung der Cybersicherheitsfähigkeiten in Industrie und kritischen Infrastrukturen.

Attribution

Im Rahmen der laufenden Revision des Nachrichtendienstgesetzes werden die Verfahren zur Erhebung von cyberspezifischen Daten überprüft. Der Nachrichtendienst des Bundes arbeitet eng mit nationalen und internationalen Partnern zusammen, um die Täterschaft bei Angriffen staatlicher Cyberakteure zu identifizieren (Attribution). Die Transformation hat es dem Nachrichtendienst des Bundes ermöglicht, seine Prioritäten zu schärfen und Prozesse zur Prioritätensetzung zu verbessern.

Cyberdefence

An dieser Stelle ist anzumerken, dass die Massnahme «**Cyberdefence**» in die NCS integriert ist, aber unter der Federführung des Kommando Cyber umgesetzt wird und strategisch in das «Gesamtkonzeption Cyber» eingebettet ist. Über die Fortschritte innerhalb des Kommando Cyber, die für die Umsetzung der NCS relevant sind, wird separat berichtet.

Der CYD-Campus hat durch die Veröffentlichung verschiedener Forschungsmanuskripte und -bücher, in denen Trends und Auswirkungen aufgezeigt werden (wie in Strategisches Ziel 1 hervorgehoben), zur Umsetzung der Massnahme «Cyberdefence» beigetragen. Sie

[31] Bericht des Bundesrates «VBS. Subsidiarität und Cybersicherheit» (https://www.newsd.admin.ch/newsd/message/attachments/89721.pdf)

sollen Forschern, politischen Entscheidungsträgern, Cybersicherheitsspezialisten und Branchenführern, die sich in der sich rasch entwickelnden Cyberverteidigungslandschaft zurechtfinden müssen, als Ressource dienen. Der CYD-Campus fokussierte dabei insbesondere auf Megatrends wie die zunehmende Automatisierung von Angriff und Verteidigung mittels künstlicher Intelligenz und analysierte neue Ansätze und Innovationen zur Stärkung der Verteidigungsfähigkeit der Schweiz z.B. im Rahmen von Cyberübungen wie Locked Shields. Ausführlichere Informationen zu diesen und weiteren Aktivitäten des CYD-Campus finden sich im Jahresbericht[32].

Cybersicherheit bei internationalen Veranstaltungen

2024 stand die Schweiz im Mittelpunkt einer Reihe internationaler Veranstaltungen, wie zum Beispiel das jährliche Treffen des Weltwirtschaftsforums (WEF) und die hochrangige Konferenz zum Frieden in der Ukraine im Juni. Wenn solche wichtigen internationalen Veranstaltungen stattfinden, kann die Wahrscheinlichkeit steigen, dass Cyberakteure sie als Plattform für Cyberangriffe nutzen oder dass die Teilnehmenden und ihre Organisationen zum Ziel genommen werden. Das BACS spielte bei diesen Ereignissen eine koordinierende Rolle und verwaltete zusammen mit Partnern aus dem öffentlichen und privaten Sektor ein Cyberlage-Netzwerk und Lagezentrum. Diese enge Zusammenarbeit ermöglichte die frühzeitige Erkennung und Bewältigung potenzieller Cyberbedrohungen. Die wichtigsten Erkenntnisse aus diesen Ereignissen wurden öffentlich zugänglich gemacht[33] und werden nun im Jahr 2025 weitergeführt, um die Cyberresilienz bei Grossveranstaltungen wie dem Jahrestreffen des WEF 2025, dem Eurovision Song Contest und der UEFA-Frauen-Europameisterschaft zu gewährleisten.

[32]CYD-Campus Jahresberichte (https://www.cydcampus.admin.ch/de/jahresberichte)

[33] BACS Bericht «Massnahmen zur Cyberresilienz im Kontext von Grossveranstaltungen und internationalen Konferenzen» (https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/aktuell/im-fokus/2024/Massnahmen-Grossanlaesse_internat-Veranstaltungen-DE.pdf.download.pdf/Massnahmen-Grossanlaesse_internat-Veranstaltungen-DE.pdf)

4.3.2 Ausblick des Steuerungsausschuss NCS

Die Fähigkeit, Cyberangriffe in Echtzeit zu erkennen, zu verhindern und darauf zu reagieren, ist für die nationale Sicherheit und die wirtschaftliche Stabilität von entscheidender Bedeutung. Die Schweiz hat 2024 zentrale Voraussetzungen für ein stärker integriertes System zur Erkennung und Bewältigung von Cybervorfällen geschaffen. Die rasche Zunahme des Austauschs von Bedrohungsdaten zwischen den Betreiberinnen kritischer Infrastrukturen ist eine positive Entwicklung.

Dennoch bleibt die dynamische Natur der Cyberbedrohungslandschaft eine grosse Herausforderung. Besonders neue Schwachstellen und geopolitische Risiken verlangen eine noch stärkere Bereitschaft und Anpassungsfähigkeit. Auch wenn die Mechanismen zur Bedrohungserkennung erheblich verbessert wurden, muss sichergestellt werden, dass alle Betreiber kritischer Infrastrukturen über umfassende und robuste Pläne für die Reaktion auf Vorfälle verfügen.

Die Entwicklung operativer Strukturen für die Cybersicherheit und die politischen Überlegungen zu Zuständigkeiten und Handlungsprinzipien bei Cyberangriffen sind noch in Arbeit. Diese Strukturen sollen im Krisenfall effektiv und effizient sein. Eine gut funktionierende Struktur kann nicht nur die nationale Widerstandsfähigkeit stärken, sondern erhöht auch das Vertrauen in die staatliche Handlungsfähigkeit bei schweren Cybervorfällen.

Die Einbindung kritischer Infrastrukturen, der Austausch von Erfahrungen aus realen Vorfällen und der Aufbau vertrauensvoller Kooperationen mit internationalen Partnern sind weiterhin zentrale Prioritäten. Der Steuerungsausschuss wird die Entwicklungen beobachten und regelmässig prüfen, ob die aktuellen Instrumente und Prozesse den zukünftigen Anforderungen entsprechen.

Mit der Umsetzung der «Gesamtkonzeption Cyber» wurden im Bereich Cyberdefence Fortschritte erzielt. Es bleibt jedoch entscheidend, dass die Schweizer Armee ihre Fähigkeiten im Bereich der Cyberverteidigung kontinuierlich verstärkt und sicherstellt, dass alle in der «Gesamtkonzeption Cyber» festgelegten Ziele erreicht werden.

4.4 Strategisches Ziel 4: Effektive Bekämpfung und Strafverfolgung der Cyberkriminalität

Cyberkriminalität entwickelt sich schnell, überschreitet Grenzen und nutzt digitale Infrastrukturen für maximalen Gewinn mit minimalem Aufwand. Die Bekämpfung erfordert enge Zusammenarbeit zwischen nationalen und internationalen Strafverfolgungsbehörden. Die NCS fokussiert auf verbesserte Ermittlungskapazitäten, bessere Koordination der Justizbehörden und Anpassung des rechtlichen Rahmens, um neue Formen der Cyberkriminalität effektiv zu bekämpfen. Effizientere Strafverfolgungsprozesse bleiben zentral.

Der 2024 Bericht[34] des Bundesrates in Beantwortung des Postulats 22.3145 Silberschmidt[35] zeigt zwei zentrale Herausforderungen zur Verbesserung der Bekämpfung der Internetkriminalität auf: einerseits die fehlende gesetzliche Grundlage für den automatisierten Austausch polizeilicher Informationen zwischen den Kantonen und mit der Bundesverwaltung und andererseits offene Fragen im Zusammenhang mit der internationalen Rechtshilfe in Strafsachen. Die Empfehlungen des Berichts spiegeln sich in der NCS und in den Zielen dieses strategischen Ziels wider.

4.4.1 Stand der Umsetzung

Verstärkte Zusammenarbeit auf nationaler und internationaler Ebene

Die Schweiz engagiert sich in der internationalen Polizeizusammenarbeit. Das Bundesamt für Polizei (Fedpol) ist die Kontakt- und Koordinationsstelle für die internationale Polizeizusammenarbeit. Es unterstützt die Herstellung von Kontakten zwischen den kantonalen Polizei- und Strafverfolgungsbehörden und ihren ausländischen Partnern.

Die Zusammenarbeit wurde durch die Koordinationsplattform Cyber-CASE verstärkt. Zwei Arbeitsgruppen zu Ransomware und Online-Anlagebetrug wurden mit kantonalen Staatsanwälten eingerichtet, um Lösungen, Empfehlungen und Richtlinien zu erarbeiten und die Verfahrenskoordination zu verbessern.

Cyber-CASE hat die Schnittstelle zwischen kantonalen Staatsanwälten und internationalen Akteuren wie dem European Judicial Cybercrime Network (EJCN) und Eurojust verbessert. Dadurch konnten nationale ad-hoc-Ermittlungen durchgeführt und Ergebnisse an internationale Partnerbehörden weitergeleitet werden. Der Austausch mit dem Privatsektor wurde intensiviert, indem Strafverfolgungsanliegen zwischen den Kantonen koordiniert und mit Vertretern von Kryptobörsen, Finanzintermediären, Anbietern von Finanztechnologie und Cybersicherheitslösungen sowie Kommunikations-dienstleistern diskutiert wurden.

[34] Bericht des Bundesrates «Wie fit sind die Kantone in der Cyber-Strafverfolgung?» (https://www.parlament.ch/centers/eparl/_layouts/15/DocIdRedir.aspx?ID=MAUWFQFXFMCR-2-55715)

[35] Postulat «Wie fit sind die Kantone in der Cyber-Strafverfolgung?» (22.3145 | Wie fit sind die Kantone in der Cyber-Strafverfolgung? | Geschäft | Das Schweizer Parlament)

Die Generalversammlung der Vereinten Nationen hat die erste globale UN-Konvention gegen Cyberkriminalität verabschiedet, um die internationale Zusammenarbeit im Kampf gegen digitale Bedrohungen zu stärken. Die Konvention tritt in Kraft, sobald sie in vierzig UNO-Mitgliedstaaten ratifiziert wurde. Das nationale Verfahren für die mögliche Unterzeichnung und Ratifizierung durch die Schweiz folgt 2025.

Strafverfolgung und Internetkriminalität

Das Netzwerk zur Unterstützung der Ermittlungen im Bereich der digitalen Kriminalität (NEDIK) vereint die Schweizer Polizeikräfte zur gemeinsamen Bekämpfung der Digital- und Cyberkriminalität. NEDIK widmet sich der Verbesserung des Informationsaustauschs, der Wissensparität und der Vernetzung von Strafverfolgungsexperten, um die sich entwickelnden Herausforderungen der Cyberkriminalität zu bewältigen. Dies wird durch die etablierten Operational Cyber Meetings (OCM) operationalisiert. Die OCM finden alle zwei Wochen statt. Im Jahr 2024 nahmen durchschnittlich 20 Kantone an jedem OCM teil. Im Jahr 2024 veröffentlicht NEDIK einen nationalen monatlichen Fallbericht, in dem es einen Überblick über aktuelle Phänomene, neue Modi Operandi, relevante Fälle und Massnahmen gibt und über die aktuelle Situation der Digital- und Cyberkriminalität in der Schweiz informiert.

Die Präventionsseite Cybercrimepolice.ch hat sich als wichtige Warn-Plattform im Kampf gegen Cyberkriminalität weiter etabliert. Die Nationalisierung und Integration von Cybercrimepolice.ch in NEDIK ist geplant, um eine einheitliche Warn- und Präventionsplattform für die gesamte Schweizer Bevölkerung und Polizeikorps zu ermöglichen.

Die nationale Wissensplattform Cyberwiki ist für Angehörige aller Polizeikorps, die mit Cyberkriminalität zu tun haben, zugänglich und bietet eine Wissensplattform rund um das Thema Cyberkriminalität. Mit rund 890 registrierten Nutzern hat die Plattform an Bedarf und Relevanz gewonnen. Um sicherzustellen, dass die Informationen auf der Plattform relevant, korrekt und zugänglich sind, wurde ihr Inhalt 2024 überprüft und aktualisiert.

4.4.2 Ausblick des Steuerungsausschuss NCS

Die Cyberkriminalität wächst weiter und stellt die Schweiz vor zunehmende Heraus-forderungen. Um dieser Entwicklung gerecht zu werden, müssen rechtliche und operative Rahmenbedingungen angepasst und weiterentwickelt werden. Trotz Fortschritten bei der Zusammenarbeit zwischen Bundes- und kantonalen Behörden so-wie der Stärkung internationaler Partnerschaften bestehen weiterhin Lücken bei der Bekämpfung komplexer Cyberkriminalität.

Eine zentrale Herausforderung ist das Fehlen einer einheitlichen Echtzeit-Fallübersicht, die Daten zu Vorfällen, Strafverfolgungsmassnahmen und Gerichtsverfahren effizient verknüpft. Diese Lücke ist eine vorrangige Aufgabe der NCS und essenziell für eine verbesserte Verfolgung von Cyberkriminalität. Zudem bleibt die internationale Zusammenarbeit aufgrund unterschiedlicher rechtlicher Rahmenbedingungen und der Schwierigkeiten bei der grenzüberschreitenden Sammlung digitaler Beweise ein ungelöstes Problem.

Die zukünftige Arbeit muss sich daher verstärkt auf die Umsetzung dieses strategischen Ziels konzentrieren. Besondere Aufmerksamkeit sollte der Verbesserung der Datenstandardisierung zwischen den Kantonen, der Stärkung forensischer Fähigkeiten sowie der Sicherstellung eines breiten Zugangs für Strafverfolgungsbehörden zu spezialisierten Schulungen gelten.

Nur durch eine enge, koordinierte Zusammenarbeit und kontinuierliche Investitionen in die richtigen Werkzeuge und Fachkenntnisse wird es möglich sein, der zunehmenden Bedrohung durch Cyberkriminalität wirksam zu begegnen.

4.5 Strategisches Ziel 5: Führende Rolle in der internationalen Zusammenarbeit

Die Cybersicherheit ist angesichts der Cyberbedrohungslage und geopolitischer Spannungen zu einem wichtigen aussenpolitischen Thema geworden. Internationale Zusammenarbeit ist unerlässlich, um Cyberrisiken zu verringern und die aussen- und sicherheitspolitischen Interessen der Schweiz zu schützen. Die Schweiz will ihre Position als wichtiger Akteur in der globalen Cybersicherheitsdiplomatie stärken. Die NCS unterstreicht die Bedeutung der internationalen Zusammenarbeit, Respekt des Völkerrechts und die Entwicklung globaler Cybersicherheitsnormen. Die diplomatische Präsenz der Schweiz, insbesondere in Genf, wird genutzt, um multilaterale Cyberdiskussionen zu erleichtern.

4.5.1 Stand der Umsetzung

Verstärkung der grenzüberschreitenden Zusammenarbeit im Bereich der Cybersicherheit

Die partnerschaftliche Zusammenarbeit mit Cybersicherheitsbehörden anderer Länder wurde weiter aufgebaut, um den Austausch von Bedrohungsdaten und technischem Fachwissen ermöglichen. Die technischen und operativen Abteilungen des BACS unterhalten auch bilaterale Beziehungen oder sind Teil multilateraler Gremien, z. B. der European GovCERT (EGC)-Gruppe und des International Watch and Warning Network (IWWN), das Cybersicherheitsbehörden aus 16 Ländern umfasst.

2024 fand in Washington DC das vierte jährliche Gipfeltreffen der International Counter Ransomware Initiative (CRI) statt. Diese vom Weissen Haus geleitete Initiative umfasst inzwischen 68 Mitgliedstaaten, darunter auch die Schweiz. Die Initiative zielt darauf ab, die kollektive Widerstandsfähigkeit gegen Ransomware zu entwickeln und die Mitgliedstaaten bei Ransomware-Angriffen zu unterstützen. Zur Unterstützung des Gipfels erarbeitete das BACS einen internationalen Überblick und bewährte Praktiken zu Meldepflichten bei Ransomware-Vorfällen sowie einen Vorschlag für die standardisierte Erfassung relevanter Informationen. 2024 haben die Mitglieder der CRI einen Leitfaden für Organisationen, die von Ransomware betroffen sind, herausgegeben. Der Leitfaden kann auf der Seite der Britischen Behörden abgerufen werden.[36]

Die Schweiz hat zahlreiche relevante Initiativen zur Bewältigung internationaler Cyber-Herausforderungen unterstützt, darunter auch die gemeinsame Erklärung[37] über die Bekämpfung der Verbreitung und des Missbrauchs von kommerzieller Spyware. Die Unterzeichner verpflichteten sich, strenge Sicherheitsvorkehrungen zu treffen, um sicherzustellen, dass der Einsatz kommerzieller Spyware durch Regierungen mit den Menschenrechten, der Rechtsstaatlichkeit und den bürgerlichen Freiheiten vereinbar ist. Das Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) beteiligt sich auch an dem im Februar 2024 von

[36] CRI-Leitfaden für Organisationen bei Ransomware-Vorfällen - GOV.UK (https://www.gov.uk/government/publications/cri-guidance-for-organisations-during-ransomware-incidents/cri-guidance-for-organisations-during-ransomware-incidents#fn:1)

[37] Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware - United States Department of State

Frankreich und dem Vereinigten Königreich lancierten Pall-Mall-Prozess[38], der darauf abzielt, die Verbreitung und den Missbrauch von Cyber Überwachungs- und Angriffstechnologien und Dienstleistungen durch die Erarbeitung von Leitprinzipien[39] und politischen Optionen einzudämmen.

Das BAKOM engagiert sich in Genf für digitale Governance, insbesondere im Rahmen des Global Digital Compact, der im September 2024 als Teil des UN Pact for the Future[40] verabschiedet wurde.

Genf als globaler Cyber-Hub

Mit der Umsetzung der NCS will die Schweiz die Rolle Genfs in der globalen Cybersicherheit weiter stärken. In Genf arbeiten internationale und nichtstaatliche Organisationen, wissenschaftliche und akademische Akteure, die Zivilgesellschaft und der Privatsektor zusammen, um Lösungen für die globalen Herausforderungen zu finden, vor denen unsere Gesellschaften stehen. Aus diesem Grund wird oft auf das Konzept des internationalen Genf verwiesen.

Die Global Conference on Cyber Capacity Building (GC3B) findet im Mai 2025 in Genf statt. Der strategische Fokus der Konferenz liegt auf der Verbindung zwischen Cybersicherheit und internationaler Zusammenarbeit für eine nachhaltige digitale Entwicklung. Die vom EDA in Zusammenarbeit mit dem Global Forum on Cyber Expertise (GFCE[41]) durchgeführte Konferenz trägt zur Stärkung des internationalen Genf bei und zielt darauf ab, breite politische Unterstützung für das Thema zu gewinnen. Zeitgleich wird die erste Geneva Cyber Week (GCW) stattfinden, um das Genfer Know-How in den Bereichen internationale Zusammenarbeit, multilaterale Diplomatie und Cybersicherheit zu nutzen und die Position Genfs als wichtiger Knotenpunkt im globalen Cybersicherheitsökosystem zu stärken.

Im Bereich des Kapazitätsaufbaus trägt das BAKOM aktiv und koordinierend bei, um internationale Prozesse und Diskussionsplattformen zur digitalen Governance in Genf anzusiedeln und bestehende Institutionen zu unterstützen. Ziel ist es, den Standort Genf optimal zu nutzen und die Zusammenarbeit zwischen öffentlichen und privaten Akteuren zu verbessern, um mehr Vertrauen in die globalisierte digitale Gesellschaft zu schaffen.

Der 2018 durch das EDA ins Leben gerufene Geneva Dialogue über verantwortungsvolles Verhalten im Cyberraum bildet die Rollen und Verantwortlichkeiten nichtstaatlicher Akteure für die Umsetzung der vereinbarten Cybernormen ab und trägt so zu Cyber-Stabilität und -Sicherheit bei. Die Resultate des Dialoges sind im Geneva Manual[42] dokumentiert und können auf der Website des Geneva Dialogues[43] abgerufen werden.

Cyber-Diplomatie

Das EDA vertritt die Positionen und Interessen der Schweiz in multilateralen Gremien wie

[38] The Pall Mall Process: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities - GOV.UK

[39] Schweizerische Versicherungsverband (SVV) deutsche Übersetzung des Letfadens für «Ransomware-Vorfälle: Leitfaden für Unternehmen» (https://www.svv.ch/de/themen/digitalisierung/ransomware-vorfaelle-leitfaden-fuer-unternehmen)

[40] Pact for the Future - United Nations Summit of the Future | United Nations

[41] GFCE - platform for international cooperation on cyber capacity

[42] GENEVA MANUAL – On Responsible Behaviour in Cyberspace – Geneva Dialogue

[43] Webseite des Geneva Dialogue (https://genevadialogue.ch/about/)

den Vereinten Nationen (z.B.Open-ended Working Group Cybersecurity der Vereinten Nationen (UN OEWG), Ad Hoc Komitee zur Erarbeitung der UN-Konvention über Cyberkriminalität (AHC-Cybercrime)) oder der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE). Es beteiligt sich aktiv an Diskussionen über Cyberbedrohungen, Völkerrecht im Cyberraum, freiwillige Normen, vertrauensbildende Massnahmen und Kapazitätsaufbau.

Das EDA leitete im Rahmen der UN OEWG die Schweizer Delegation, welche eine Schlüsselrolle bei der Förderung von Diskussionen über das Völkerrecht, und speziell das humanitäre Völkerrecht, im Cyberspace spielt. Gemeinsam mit Kanada hat die Schweiz unter anderem ein Arbeitspapier zum Völkerrecht vorgelegt und die Einrichtung einer Regionen-übergreifenden Gruppe zum humanitären Völkerrecht initiiert

In Zusammenarbeit mit dem Centre for Humanitarian Dialogue (HD[44]) engagiert sich das EDA in der **Cyber-Mediation** zur Bewältigung digitaler Konflikte. Diese Initiative konzentriert sich auf die Vermittlung bei offensiven Cyberoperationen gegen kritische Infrastrukturen und die Schaffung von Kommunikationskanälen, um eine Eskalation zu verhindern.

[44] Webseite des Centre for Humanitarian Dialogue (https://hdcentre.org/)

4.5.2 Ausblick des Steuerungsausschuss NCS

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

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

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

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

5 Fokus des Steuerungsausschuss NCS 2025

Die Sicherstellung messbarer Fortschritte bei der Umsetzung der NCS hat für den NCS-Steuerungsausschuss hohe Priorität. 2025 sollen die Bemühungen auf fünf Schlüsselaktivitäten konzentriert werden. Darüber hinaus wird jährlicher ein Bericht zur Umsetzung der NCS veröffentlicht, um Transparenz zu gewährleisten und die Fortschritte sowie Herausforderungen im Umsetzungsvorhaben darzulegen.

Einbeziehung von Interessengruppen

Messbarkeit der Fortschritte

Strategische Aufsicht & Beratung

Strategische Überprüfung

Benchmarking

Einbeziehung von Interessengruppen: Die Zusammenarbeit mit der öffentlichen Verwaltung, der Industrie, der Wissenschaft und der Zivilgesellschaft ist unerlässlich, um die Herausforderungen bei der Umsetzung zu bewerten. Durch die Umsetzung einer neuen NCS-Governance wird Dialog gefördert und Feedback aktiv eingeholt, um die strategischen Arbeiten auf eine breite Basis zu stellen.

Messbarkeit der Fortschritte: Die Umsetzung der Strategie soll durch die Einführung strategischer Ambitionen und messbarer Leistungsindikatoren unterstützt werden.

Strategische Aufsicht und Beratung: Die Fortschritte bei der Umsetzung der NCS werden regelmässig bewertet und die Prioritäten in der Umsetzung in Abstimmung mit der aktuellen Strategie beurteilt. Etwaige Lücken in der Umsetzung können so identifiziert werden, und Massnahmen zur Anpassung können ergriffen werden.

Strategische Überprüfung: Die NCS muss regelmässig überprüft werden, um sicher-zustellen, dass sie im sich rasch entwickelnden Umfeld die richtigen Akzente zum Wohl der Schweiz setzt. Dieser Prozess ist keine Neuentwicklung, sondern eine Überprüfung und wird im Sommer 2025 gestartet

Benchmarking: Internationale Ansätze zur Implementierung Nationaler Cybersicherheitsstrategien werden analysiert und mit der Schweiz verglichen, so dass die NCS wettbewerbsfähig und innovativ bleibt und gegebenenfalls von anderen lernen kann.