Nationale Cyberstrategie (NCS)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat

Impressum

Herausgeber
Nationales Zentrum für Cybersicherheit (NCSC)
Schwarztorstrasse 59
CH-3003 Bern

info@ncsc.admin.ch
www.ncsc.admin.ch

Inhaltsverzeichnis

1 Einleitung

Die Cybersicherheit ist auf allen Ebenen ein entscheidendes Element geworden. Sie ist ein Schlüsselelement der Sicherheitspolitik, unabdingbare Voraussetzung für die Digitalisierung, zentraler Faktor des Datenschutzes, Chance für den Wirtschafts- und Forschungsstandort Schweiz sowie ein zunehmend wichtiges Element der Aussenpolitik. Sie betrifft aber nicht nur diese staatspolitischen Themen, sondern ist längst ein Faktor des täglichen Umgangs aller Bürgerinnen und Bürger mit digitalen Technologien geworden. Daraus ergibt sich, dass eine nationale Cybersicherheitsstrategie ein breites Spektrum an Themen und Massnahmen berücksichtigen muss. Zugleich muss der Anspruch einer Strategie sein, dieses breite Portfolio an Themen zu sortieren, zu gewichten und in Relation zueinander zu setzen. Als erster Schritt dazu werden in diesem einleitenden Kapitel die unterschiedlichen Bedrohungen beschrieben, welchen entgegengewirkt werden soll. Zweitens wird aufgezeigt, auf welcher Basis die Strategie aufbaut. Cybersicherheit ist kein neues Thema mehr, und in der Schweiz wurden bereits Grundlagenarbeiten geleistet. Es ist wichtig, auf diesen Arbeiten aufzubauen, sie aber gleichzeitig wo nötig zu hinterfragen und zu ergänzen. Drittens wird aufgezeigt, wo die Zuständigkeiten liegen. Beim Querschnittsthema der Cybersicherheit hat sich diese Frage immer wieder als eine der zentralen Herausforderungen erwiesen.

1.1 Die Cyberbedrohungslage

Als Cyberbedrohung wird in dieser Strategie ein Umstand bezeichnet, der das Potenzial hat, einen Cybervorfall zu verursachen. Ein Cybervorfall ist wiederum definiert als Ereignis, das bei der Nutzung von Informatik- und Kommunikationsmitteln (IKT) die Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt. Auf der Grundlage dieser Definitionen lässt sich ein breites Spektrum an möglichen Cyberbedrohungen ausmachen, welche im Folgenden beschrieben werden. Um geeignete Gegenmassnahmen zu identifizieren, ist zudem ein systematischer Überblick über jene Faktoren nötig, welche die Cyberbedrohungslage direkt beeinflussen.

1.1.1 Bedrohung durch Cyberangriffe

Unter Cyberangriffen werden Cybervorfälle verstanden, welche absichtlich herbeigeführt werden. Der Schutz vor solchen Bedrohungen steht im Zentrum der Massnahmen für die Cybersicherheit. Er ist deshalb so wichtig, weil die Bedrohung durch Cyberangriffe seit Jahren anhaltend hoch ist und die Abhängigkeit der Wirtschaft und Gesellschaft von funktionierenden IKT-Umgebungen weiter ansteigt. Zur Einschätzung der Lage und der möglichen Bewältigungsmechanismen ist es angesichts der Vielzahl von möglichen Cyberangriffen wichtig, zwischen verschiedenen Phänomenen zu unterscheiden. Unterscheidungskriterien sind der Zweck der Angriffe, die Akteure, welche hinter den Angriffen stehen, und der Kreis jener, welche angegriffen werden. Auf dieser Grundlage lassen sich fünf Arten von Cyberangriffen unterscheiden, wobei zu beachten ist, dass diese häufig in Kombination auftreten und zwischen ihnen Überschneidungen bestehen.

Cyberkriminalität: In Abgrenzung von den im Folgenden beschriebenen Bedrohungen, umfasst die Cyberkriminalität vor allem Vermögensdelikte. Cyberkriminalität umfasst die Gesamtheit aller strafbaren Handlungen und Unterlassungen im Cyberraum. Unterschieden wird zwischen «Cybercrime» und «digitalisierter Kriminalität». «Cybercrime» bezeichnet Straftaten die sich gegen das Internet, informationstechnische Systeme oder deren Daten richten und technische Ermittlungsarbeit auf Seiten der Strafverfolgungsbehörden erfordern. «Digitalisierte Kriminalität» bezeichnet Straftaten, die bisher überwiegend in der analogen Welt begangen worden sind. Aufgrund der zunehmenden Digitalisierung, werden klassische Delikte vermehrt mit Hilfe von Informationstechnik verübt.
Cyberkriminalität ist jene Bedrohung mit der höchsten Eintrittswahrscheinlichkeit. Da es nicht

das eigentliche Ziel der Angreifenden ist, das Funktionieren der Gesellschaft, Wirtschaft oder des Staates zu gefährden, beschränken sich die unmittelbaren Auswirkungen in der Regel auf die betroffenen Opfer. Cyberkriminelle nehmen jedoch hohe Kollateralschäden in Kauf oder nutzen die Möglichkeit solcher Auswirkungen, um von den Opfern höhere Summen zu erpressen. Aus diesem Grund bergen Angriffe durch Cyberkriminelle ein hohes Schadenspotenzial für die gesamte Gesellschaft und Wirtschaft.
Im Umfeld der Cyberkriminalität entstehen eigentliche Geschäftsfelder, in welchen organisierte Gruppen arbeitsteilig operieren. Aufgrund der grossen Konkurrenz ist der Innovationsdruck unter kriminellen Akteuren hoch, weshalb die Angreifer laufend neue Methoden entwickeln oder erwerben und sich zunehmend professionalisieren. Entsprechend muss weiterhin mit einer wachsenden Häufigkeit und Spezialisierung der kriminellen Aktivitäten im Cyberraum gerechnet werden.

Cyberspionage: Bei der Cyberspionage werden Cyberangriffe dafür eingesetzt, um für politische, militärische oder wirtschaftliche Zwecke unerlaubt an Informationen zu gelangen oder die Aktivitäten der Opfer zu beobachten. Oft versuchen die Angreifer dabei, nach dem erfolgreichen Eindringen in Netzwerke möglichst lange unentdeckt zu bleiben. Typisch für solche Aktivitäten sind komplexe und persistente Angriffe, sogenannte «Advanced Persistent Threats» (APTs). Cyberspionage wird oft von staatlichen, jedoch ebenso von halb- oder nichtstaatlichen Akteuren ausgeübt. Im Fokus der Angreifer stehen sowohl Unternehmen als auch staatliche, gesellschaftliche oder internationale Institutionen. Die Schweizer Wirtschaft ist eine der innovativsten der Welt, und viele internationale Konzerne haben ihren Hauptsitz oder wichtige Datenzentren hier. Zudem beherbergt die Schweiz viele internationale Organisationen und ist häufig Gastgeberin von internationalen Verhandlungen und Konferenzen. Dies macht die Schweiz zu einem attraktiven Ziel für Cyberspionage. Die Auswirkungen können ein sehr unterschiedliches Ausmass annehmen, je nach Art und Umfang der Daten, zu welchen sich die Angreifer Zugang verschaffen. Für stark von ihrer Innovationfähigkeit abhängige KMU können sie jedoch rasch ein existenzbedrohendes Ausmass annehmen. Die Auswirkungen sind meist nicht unmittelbar ersichtlich, da politische und wirtschaftliche Nachteile erst dann entstehen, wenn Angreifer ihr erlangtes Wissen nutzen. Zudem entstehen im Nachgang solcher Operationen oft Kollateralschäden, weil Cyberkriminelle die Angriffsvektoren zweitnutzen. Mit der Zunahme von geopolitischen Spannungen gewinnt auch die Cyberspionage weiter an Bedeutung. Die Bedrohung wird zusätzlich dadurch erhöht, dass Regierungen Einfluss auf Hersteller von IKT-Produkten ausüben. Dies erhöht die Wahrscheinlichkeit, dass Sicherheitslücken in Produkten bewusst offengelassen werden. Da die Lieferketten bei IKT-Produkten sehr komplex sind und die Schweiz in hohem Mass abhängig von ausländischen Herstellern ist, ist es eine grosse Herausforderung diese Bedrohung adäquat zu adressieren.

Cybersabotage: Cybersabotage bezeichnet die Tätigkeit, um mittels Cyberangriffe das zuverlässige und fehlerfreie Funktionieren der IKT zu manipulieren, stören oder zu zerstören, was je nach Art der Sabotage und des angegriffenen Ziels auch zu physischen Auswirkungen führen kann. Die Motivation für solche Angriffe kann sehr unterschiedlich sein. Sie können von Einzeltätern beispielsweise aus ideologischen Überzeugungen oder auf Grund persönlicher Frustration durchgeführt oder von staatlichen Akteuren zur Erreichung politischer oder militärischer Ziele eingesetzt werden. Ziel ist in jedem Fall eine Machtdemonstration und Einschüchterung, verbunden mit der Absicht, eine Organisation oder sogar die Gesellschaft zu destabilisieren.
Während auf internationaler Ebene verschiedene grössere Sabotageakte, unter anderem auf die Energieversorgung von Staaten, bekannt sind, fanden solche in der Schweiz bisher nicht statt. Die Eintrittswahrscheinlichkeit ist aber mit der Zunahme geopolitischer Spannungen auch für die Schweiz gestiegen. Die potenziellen Schäden sind dabei sehr gross.

Cybersubversion: Von Cybersubversion wird dann gesprochen, wenn staatliche, staatsnahe oder politisch motivierte Akteure Cyberangriffe gezielt dafür einsetzen, um das politische System eines anderen Staates zu unterminieren. Solche Angriffe zielen beispielsweise auf die Verfahren demokratischer Prozesse, die politischen Institutionen oder Organisationen von hohem öffentlichem Interesse. Die Angreifer versuchen so, das

Vertrauen in den Staat zu beeinträchtigen und kombinieren diese Angriffe oft mit Desinformationskampagnen.

Cyberoperationen in bewaffneten Konflikten: Der Einsatz von regulären und irregulären Mitteln in bewaffneten Konflikten ist heute verbreitete Praxis. Cyberoperationen sind dabei besonders geeignet, da sie kaum eindeutig zuzuordnen sind, vergleichsweise wenig kosten, über beliebig grosse Distanzen hinweg ohne physische Präsenz einsetzbar sind und es erlauben, Wirkung auch ohne direkten Bezug zu militärischen Operationen zu erzielen. Die beträchtlichen Investitionen vieler Staaten zum Schutz und zur aktiven Abwehr von Cyberbedrohungen unterstreichen die Bedeutung von Cybermitteln in bewaffneten Konflikten. Entsprechend ist zu erwarten, dass die Bedeutung von gezielten Cyberoperationen zu machtpolitischen Zwecken weiter zunehmen wird. Die Schweiz muss deshalb die Cyberabwehr sowie die Cyberdiplomatie zur Vorbeugung solcher Aktivitäten in die Vorbereitungen auf einen Konfliktfall miteinbeziehen.

1.1.2 Menschliches Fehlverhalten und technische Ausfälle

Neben den gezielten und vorsätzlichen Cyberangriffen können auch unbeabsichtigte Handlungen oder natur- und technikbedingte Ereignisse zu Cybervorfällen führen. Ausgelöst werden sie durch menschliches Fehlverhalten bei der Bereitstellung und Nutzung von IKT (z. B. unsachgemässe oder unachtsame Anwendung von IKT-Systemen, fehlerhafte Administration oder Konfiguration, Verlust von Datenträgern) oder durch technische Ausfälle, welche wiederum verschiedene Ursachen haben können (z. B. Überalterung der Infrastruktur oder Naturereignisse, Überbeanspruchung, Fehlkonstruktion, mangelhafte Wartung, unzureichende Energieversorgung). Ereignisse dieser Art kommen in unterschiedlicher Grössenordnung häufig vor und gehören zum Alltag der IKT-Abteilungen in Unternehmen und Behörden. Entsprechend sind die Auswirkungen dieser Fehler und Ausfälle in der Regel gut beherrschbar. Es ist aber wichtig festzuhalten, dass hinter vielen grossen Cybervorfällen nicht gezielte Angriffe, sondern eine Verkettung verschiedener Umstände wie menschliches Fehlverhalten oder technisches Versagen, verbunden mit einer unzureichenden Vorbereitung, stehen. Bei der Planung und Umsetzung von Schutzmassnahmen dürfen vorbeugende Massnahmen gegen solche Ereignisse darum nicht vernachlässigt werden. Cybervorfälle aufgrund von menschlichem Fehlverhalten oder technischen Ausfällen werden weiterhin häufig bleiben. Die zunehmende Komplexität durch die Vernetzung verschiedenster Bereiche macht es zudem schwierig, die Auswirkungen dieser unbeabsichtigten Ereignisse abzuschätzen und einzugrenzen. Die Schulung der Mitarbeitenden sowie generell eine gute Vorbereitung und vorsorgliche Planung für solche Vorfälle bleiben deshalb zentrale Elemente beim Schutz vor Cyberbedrohungen.

1.1.3 Einflussfaktoren auf die Bedrohungslage

Technologische, politische und gesellschaftliche Entwicklungen haben grossen Einfluss auf die Bedrohungslage. Die Lage kann sich grundsätzlich jederzeit sehr rasch ändern. Dennoch ist es möglich, Einflussfaktoren zu identifizieren, welche mit hoher Wahrscheinlichkeit die künftige Entwicklung von Cyberbedrohungen beeinflussen werden. Es ist im strategischen Kontext wichtig, diese Einflussfaktoren zu beachten. Gleichzeitig muss auch stets bedacht werden, dass die Auflistung möglicher Einflussfaktoren keinesfalls abschliessend verstanden werden sollte und es zur kontinuierlichen Lagebeurteilung gehört, weitere mögliche Einflüsse frühzeitig zu erkennen und bereits identifizierte Faktoren stets neu zu beurteilen.
Die Entwicklung der Cyberbedrohungslage wird wesentlich durch geopolitische und technologische Innovationen geprägt. In Bezug auf die Geopolitik lässt sich vereinfachend feststellen, dass eine Zunahme von geopolitischen Spannungen eine Verschärfung der Cyberbedrohungslage zur Folge hat. Weil das Internet global Staaten, Unternehmen und Personen vernetzt, haben internationale Spannungen direkte Auswirkungen auf diese Interaktionen. Es ist dann zu erwarten, dass es vermehrt zu gegenseitigen Cyberangriffen in

allen der oben beschriebenen Ausprägungen kommt. Zugleich ist bei zunehmenden Spannungen zwischen Ländern, welche zu den wichtigsten Herstellern von Hard- und Software-Produkten zählen, auch mit gegenseitigen Blockaden zu rechnen. Dies erschwert die Beschaffung solcher Mittel und macht es umso wichtiger, dass die Leistungsbezüger bei Beschaffungen die Risiken sehr genau abwägen.
In Bezug auf technologische Entwicklungen ist festzuhalten, dass technische Innovationen die Lage sowohl verbessern als auch verschlechtern können und dies manchmal auch gleichzeitig tun. Neue Technologien helfen zwar oft, die Sicherheit zu verbessern, gleichzeitig führen sie zu neuen Abhängigkeiten, erhöhen die Komplexität oder führen gar direkt zu neuen Bedrohungen, indem Angreifer sie für sich nutzen. Für den Schutz vor Cyberbedrohungen ist es deshalb entscheidend, sich frühzeitig mit neuen technologischen Entwicklungen auseinanderzusetzen und mögliche Bedrohungen zu antizipieren.
In den kommenden Jahren werden dabei insbesondere die Entwicklungen bei den folgenden drei Grundlagetechnologien der Digitalisierung zu beachten sein:

- **Cloud-Computing:** Cloud-Computing ermöglicht neue Anwendungen und technologische Innovationen und kann die Cybersicherheit erhöhen, indem es beispielsweise für eine hohe Verfügbarkeit der Informationen sorgt. Gleichzeitig führt Cloud-Computing zu Risiken. Informationen mit hoher Bedeutung für die Schweiz können ausserhalb der Schweiz bearbeitet werden, was dazu führt, dass der rechtliche Schutz über den Zugriff und die Verwendung dieser Daten nicht mehr allein durch die Schweizer Gesetzgebung geregelt werden kann. Zudem kann Cloud-Computing potenziell zu einer hohen Abhängigkeit von einigen wenigen Anbietern führen. Diese Auswirkungen von Cloud-Computing können ohne geeignete Gegenmassnahmen die Cybersicherheit beeinträchtigen.
- **Internet of Things (IoT):** Die Vernetzung physischer Objekte (Things) über das Internet schreitet weiter rasant voran. Sie betrifft sowohl die Steuerung, Überwachung und Vernetzung von Systemen der Industrie (Operational Technology) als auch jene von Konsumgütern. In Bezug auf die Cyberbedrohungslage ist erstens die enorme Verbreitung von IoT von grosser Bedeutung. Die Verknüpfung tausender Geräte führt zu sehr komplexen Systemlandschaften und zu einer massiven Ausweitung der potenziellen Angriffsoberfläche. Zweitens vergrössert sich durch diese Vernetzung auch die Bedrohung durch Cybersabotage. Es wird einfacher, über Cyberangriffe direkte physische Auswirkungen zu erzielen. Drittens muss festgestellt werden, dass die Sicherheit bei IoT-Geräten häufig weder bei der Herstellung noch im weiteren Verlauf des Lebenszyklus der Geräte ausreichend berücksichtigt wird, um die Kosten tief zu halten. Dem wird auf nationaler und europäischer Ebene mit Bestimmungen für die Sicherheit von IoT-Geräten (z. B. mit der Verordnung des BAKOM über Fernmeldeanlagen) entgegengetreten.
- **Künstliche Intelligenz:** Die Verfügbarkeit von hoher Rechenleistung und Daten ermöglicht heute eine viel breitere Nutzung von künstlicher Intelligenz (KI). Durch teilweises oder gänzlich autonomes maschinelles Lernen sind Anwendungen der KI fähig, sehr komplexe Analysen in kurzer Zeit durchzuführen. Diese Möglichkeiten können genutzt werden, um Systeme besser zu schützen, umgekehrt können sie aber auch dazu verwendet werden, Angriffe effektiver und effizienter durchzuführen. Weil sich viele Organisationen bei Entscheidungen zunehmend auf die Analysen von KI-Anwendungen verlassen, sind auch Angriffe auf solche Anwendungen ein relevantes Bedrohungsszenario. Zudem können KI-Anwendungen auch ohne Fremdeinwirkung ein Sicherheitsrisiko darstellen, wenn eine fehlerhafte Anwendung eine Störung oder ein Datenleck verursacht.

Zusätzlich zu den Entwicklungen der Grundlagetechnologien der Digitalisierung gilt es, technologische Entwicklungen zu beachten, bei welchen sich noch keine breitflächige Anwendung abzeichnet, deren Nutzung aber einen direkten Einfluss auf die Cybersicherheit haben kann. Ein Beispiel für eine solche Technologie ist die Quantum-Technologie, welche

es ermöglicht, gewisse mathematische Probleme deutlich effizienter zu lösen als mit heutigen Computern. Die verbreiteten asymmetrischen Kryptologie-Verfahren könnten dadurch gebrochen werden und es ist nötig, Post-Quantum-Algorithmen zu entwickeln und einzusetzen. Solche Technologiesprünge gilt es deshalb bei der Umsetzung der Massnahmen der Strategie zu berücksichtigen.

1.2 Stand des Schutzes der Schweiz vor Cyberbedrohungen

Die vorliegende Strategie basiert auf den Arbeiten der ersten beiden Strategien zum Schutz der Schweiz vor Cyberrisiken, welche von 2012 bis 2017 und von 2018 bis 2022 umgesetzt wurden. Sie fügt sich zudem in den strategischen Kontext ein, welcher durch die Ausrichtung der Schweiz in der Digitalisierung und in der Sicherheitspolitik gegeben ist. Institutionell abgebildet ist der Stand des Schutzes vor Cyberbedrohungen in der Schweiz in der Organisation des Bundes und in den Organen, welche zur Förderung der Zusammenarbeit zwischen Bund, Kantonen, Wirtschaft und Hochschulen geschaffen wurden.

1.2.1 Die ersten beiden nationalen Cyberstrategien

Die ersten beiden NCS fokussierten auf den Auf- und Ausbau von Fähigkeiten, Strukturen und Prozessen. Die Umsetzung der Strategien hat die nötigen Grundlagen für eine kohärente Cybersicherheitspolitik der Schweiz geschaffen. Im Rahmen dieser Strategien wurden auch Grundsatzentscheide zu den Organisationsstrukturen der Cybersicherheitspolitik getroffen. Innerhalb des Bundes wurde mit dem Nationalen Zentrum für Cybersicherheit (NCSC) ein Kompetenzzentrum geschaffen, und für die Zusammenarbeit innerhalb der Bundesverwaltung und darüber hinaus mit den Kantonen, der Wirtschaft und den Hochschulen wurden die nötigen Gremien definiert. Mit den bisherigen Arbeiten wurde somit das nötige Fundament gelegt und die vorliegende Strategie kann nun inhaltliche Prioritäten der bereits bestehenden oder weiterführenden Arbeiten definieren.

1.2.2 Strategischer Kontext der Cyberstrategie

Verschiedene Strategien des Bundes legen Leitlinien fest, die für den Schutz vor Cyberbedrohungen massgeblich sind. Sie bilden den strategischen Kontext der vorliegenden Strategie:

- **Strategie Digitale Schweiz**: Die Strategie zeigt auf, wie die Schweiz die Chancen, die sich durch den digitalen Wandel für die Gesellschaft und die Wirtschaft ergeben, bestmöglich zum Wohl aller nutzen will. Sicherheit und Vertrauen ist einer von fünf Wirkungsbereichen der Strategie.
- **Nationale Strategie zum Schutz kritischer Infrastrukturen (SKI):** Die SKI-Strategie definiert den Begriff kritische Infrastrukturen und legt fest, welche Sektoren und Teilsektoren in der Schweiz als kritisch gelten. Sie enthält Massnahmen, die zum Ziel haben, die Resilienz der Schweiz im Hinblick auf kritische Infrastrukturen zu verbessern.
- **Bericht des Bundesrates über die Sicherheitspolitik der Schweiz:** Im sicherheitspolitischen Bericht definiert der Bundesrat die grundsätzliche strategische Ausrichtung der Sicherheitspolitik der Schweiz. Der Bericht und der Zusatzbericht von 2022 erläutern die Bedeutung der Cyberbedrohungen für die Sicherheitspolitik und definieren wichtige Begriffe im Zusammenhang mit der Thematik.
- **Gesamtkonzeption Cyber der Schweizer Armee:** Die Gesamtkonzeption Cyber zeigt die Herausforderungen im Cyber- und elektromagnetischen Raum (CER) sowie in der IKT auf und beschreibt, welche Fähigkeiten die Schweizer Armee bis Mitte der 2030er-Jahre entwickeln muss, um auch künftigen Bedrohungen begegnen zu können.

- **Strategie Digitalaussenpolitik:** Die Strategie definiert die Aktionsfelder der Digitalaussenpolitik der Schweiz. Im Bereich der Cybersicherheit engagiert sich die Schweiz für völkerrechtliche Normen im Cyberraum, für den Einbezug von privaten Akteuren in die Cybersicherheitspolitik und für vertrauensbildende Massnahmen. Sie bietet zudem die Guten Dienste auch in Bezug auf Fragen der Cybersicherheit an.

1.3 Organisation zum Schutz vor Cyberbedrohungen in der Schweiz

Cybersicherheit ist ein Querschnittsthema, das sich nicht einer einzelnen Behörde zuteilen lässt. Dies gilt umso mehr für die Schweiz, in welcher die Aufgabenzuteilung ohnehin durch den Föderalismus geprägt ist. Obwohl digitale Interaktionen kaum territorial zu verorten sind, bleibt das verfassungsmässige Prinzip der föderalen Zuständigkeit auch im Cyberraum bestehen. Auf dieser Grundlage haben Bund und Kantone ihre jeweiligen Cyberorganisationen entwickelt. Sowohl beim Bund als auch bei den Kantonen sind die Strukturen in den Grundzügen zwar festgelegt, es bleibt aber wichtig, dass diese laufend geprüft und wo nötig weiterentwickelt werden.
Neben der Aufgabenteilung zwischen den unterschiedlichen Staatsebenen ist der Aspekt der Zusammenarbeit zwischen öffentlichen und privaten Akteuren in der Cybersicherheit von entscheidender Bedeutung. Diese Zusammenarbeit ist verschiedenartig organisiert. Sie erfolgt über Organisationen, welche aus öffentlichen und privaten Akteuren zusammengesetzt sind, über den direkten Einbezug von Verbänden und Unternehmen in die Umsetzung von Massnahmen der NCS oder auch in der täglichen Kooperation und beim Erfahrungsaustausch zwischen privaten und öffentlichen Sicherheitsteams.
Im Folgenden sollen nicht alle für die Cybersicherheit relevanten Organisationen und Kooperationsformen aufgelistet, sondern die Grundzüge der Organisation von Bund und Kantonen dargestellt und die Mechanismen für die Steuerung der Umsetzung der Strategie aufgezeigt werden.

1.3.1 Organisation und Zuständigkeiten im Bund

Innerhalb des Bundes wird zwischen folgenden drei Aufgabenbereichen unterschieden:

- **Bereich Cybersicherheit:** Gesamtheit der Massnahmen, die der Prävention, der Bewältigung von Vorfällen und der Verbesserung der Resilienz gegenüber Cyberrisiken dienen und die internationale Zusammenarbeit zu diesem Zweck stärken.
- **Bereich Cyberdefence:** Gesamtheit der nachrichtendienstlichen und militärischen Massnahmen, die dem Schutz der für die Landesverteidigung kritischen Systeme, der Abwehr von Cyberangriffen, der Gewährleistung der Einsatzbereitschaft der Armee in allen Lagen und dem Aufbau von Kapazitäten und Fähigkeiten zur subsidiären Unterstützung ziviler Behörden dienen; dazu zählen auch aktive Massnahmen zur Erkennung von Bedrohungen, zur Identifikation von Angreifern und zur Störung und Unterbindung von Angriffen.
- **Bereich Cyberstrafverfolgung:** Gesamtheit aller Massnahmen der Polizei und der Staatsanwaltschaft von Bund und Kantonen zur Bekämpfung der Cyberkriminalität.

Zuständig für die Kernaufgaben im Bereich Cybersicherheit sowie für die Koordination mit allen weiteren beteiligten Stellen ist das NCSC. Der Bundesrat hat am 2. Dezember 2022 beschlossen, dieses in ein Bundesamt zu überführen. Die Aufgaben des Bundesamts sind ausschliesslich auf die zivile Cybersicherheit ausgelegt und damit klar abgegrenzt von den Aufgaben des Nachrichtendienstes und der Armee im Bereich der Cyberdefence. Das Bundesamt übernimmt auch keine Aufsichts- oder Regulierungsaufgaben von den Fachbehörden in den Sektoren. Diese bleiben für die Zulassung und laufende operative Aufsichtstätigkeiten der Industrie und konzessionierte Unternehmen bezüglich

sektorspezifischen Cyber-Security-Vorgaben zuständig. Das NCSC arbeitet direkt mit den Fachämtern zusammen und stellt ihnen Fachwissen zur Cybersicherheit zur Verfügung.
Der Bereich der Cyberstrafverfolgung liegt primär in der Zuständigkeit der Kantone. Seitens des Bundes sind das Bundesamt für Polizei (fedpol) und die Bundesanwaltschaft (BA) zuständig.
In den rechtlichen Grundlagen der Organisationen wird präzisiert, welche Kompetenzen die zuständigen Stellen haben. Gleichzeitig sorgen die Verwaltungseinheiten untereinander, im durch das Recht gesetzten Rahmen, über einen laufenden Informations- und Erfahrungsaustausch für eine optimale Abstimmung und die Nutzung von Synergien.

1.3.2 Organisation und Zuständigkeiten bei den Kantonen

Die Kantone definieren ihre Organisation der Cybersicherheit selbständig und angepasst an ihren Bedarf. Sie können sich dabei an der «Empfehlung für die Umsetzung zur kantonalen Cyber-Organisation» orientieren, welche vom Sicherheitsverbund Schweiz (SVS) erarbeitet wurde und von der Kantonalen Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) 2020 verabschiedet wurde. Die empfohlene Organisationsstruktur beinhaltet die Ernennung einer Person für die Koordination der Aufgaben mit Bezug zur Cybersicherheit (Cyberkoordinator/in) und eines politischen Ausschusses auf der Stufe des Regierungsrates. Durch diese Strukturen kann gewährleistet werden, dass dem Querschnittscharakter der Cybersicherheit Rechnung getragen wird.
Die übergeordnete interkantonale Koordination zu Themen der Cybersicherheit findet über die KKJPD statt; dies schliesst jedoch nicht aus, dass sich andere Regierungskonferenzen im Rahmen ihrer Zuständigkeitsgebiete mit Cyberaspekten befassen. Die Zusammenarbeit mit dem Bund wird durch den SVS koordiniert und gefördert.

1.3.3 Gemeinsame Steuerung der NCS durch Bund, Kantone, Wirtschaft und Hochschulen

Der Bundesrat bestimmt einen Ausschuss, welcher die Umsetzung der NCS steuert, indem er die Umsetzungsarbeiten aller beteiligten Akteure koordiniert und deren Fortschritt erhebt und beurteilt. Der Steuerungsausschuss setzt sich aus Expertinnen und Experten der verschiedenen Gebiete der Cybersicherheit zusammen und soll die Anliegen der Kantone, der Wirtschaft, der Gesellschaft, der Hochschulen und des Bundes integrieren.
Für die Koordination der Arbeiten erstellt der Steuerungsausschuss in Abstimmung mit den zentralen Akteuren eine Umsetzungsplanung. Ziel dieser Planung ist es, die Prioritäten der beteiligten Akteure aufeinander abzustimmen, damit die Umsetzungsarbeiten aufeinander abgestimmt und zielgerichtet erfolgen.
Für die Beurteilung des Umsetzungsfortschritts definiert der Steuerungsausschuss Leistungsindikatoren zu den einzelnen Massnahmen. Diese sollen es ermöglichen festzustellen, ob die Ziele der Strategie durch die Umsetzung der Massnahmen in der nötigen Qualität erreicht werden.
Der Steuerungsausschuss informiert den Bundesrat und die Kantone regelmässig über den Umsetzungsstand der Strategie und über seine Beurteilung zur Qualität der Umsetzung. Dies erfolgt über das NCSC, welches als Geschäftsstelle des Steuerungsausschusses die Informationen des Steuerungsausschusses über das VBS dem Bundesrat und den Kantonen zur Kenntnis bringt. Auf dem gleichen Weg kann der Steuerungsausschuss dem Bundesrat und den Kantonen auch Ergänzungen, Änderungen oder Streichungen von Massnahmen oder die Ergänzung der Strategie mit weiteren Zielen oder Massnahmen vorschlagen.

2 Ausrichtung der NCS

2.1 Vision und strategische Ziele

2.1.1 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.»

2.1.2 Strategische Ziele

- **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.
- **Sichere digitale Dienstleistungen und Infrastrukturen:** 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.
- **Wirksame Erkennung, Verhinderung, Bewältigung und Abwehr von Cybervorfällen:** 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.
- **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.
- **Führende Rolle in der internationalen Zusammenarbeit:** 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.

2.2 Grundsätze

Die Vision und die strategischen Ziele geben vor, *was* die NCS erreichen will. Die Grundsätze definieren nun, *wie* dies geschehen soll.

- Die NCS geht von einem **risikobasierten, umfassenden Ansatz** aus, welcher zum Ziel hat, die Resilienz der Schweiz hinsichtlich Cyberbedrohungen zu verbessern. «Risikobasiert» impliziert, dass kein vollständiger Schutz vor Cyberbedrohungen möglich ist, diese aber so adressiert werden können, dass das verbleibende Risiko tragbar ist. In einem «umfassenden Ansatz» werden alle relevanten Verwundbarkeiten und Risiken berücksichtigt.

- Der Schutz der Schweiz vor Cyberbedrohungen ist eine **gemeinschaftliche Aufgabe von Gesellschaft, Wirtschaft und Staat.** Dabei sind die Verantwortungen und Zuständigkeiten klar definiert und werden von allen Beteiligten gelebt. Die NCS wird deshalb auf der Basis föderalistischer Prinzipien, dezentral und in gemeinsamer Verantwortung umgesetzt.
- Der NCS liegt ein Verständnis einer **subsidiären und partnerschaftlichen Rolle des Staates** zugrunde. Dies bedeutet, dass der Staat erst dann eingreift, wenn das Wohlergehen unserer Gesellschaft wesentlich bedroht ist und private Akteure nicht in der Lage oder nicht willens sind, das Problem selbständig zu lösen. Der Staat kann in diesem Fall unterstützend wirken, Anreize setzen oder regulativ eingreifen, wobei er die entsprechenden Massnahmen in engem Austausch mit den betroffenen Akteuren bestimmt und eine enge Zusammenarbeit mit diesen anstrebt.
- Die Umsetzung der NCS erfolgt transparent, soweit dies nicht zu einer Beeinträchtigung der Wirkung der Massnahmen führt. Erreicht wird dies über eine **aktive Kommunikation zur NCS** gegenüber Gesellschaft, Wirtschaft, Wissenschaft und Politik sowie über die direkte Einbindung der Schlüsselpartner aus Verwaltung, Gesellschaft und Privatwirtschaft.

2.3 Zielgruppen

Mit der NCS legen Bund und Kantone fest, welche Ziele sie in enger Zusammenarbeit mit der Wirtschaft, Wissenschaft und Gesellschaft umsetzen wollen. Die beabsichtigte Wirkung der NCS betrifft die ganze Schweiz. Explizit adressiert die NCS folgende Zielgruppen:

- **Bevölkerung:** Der Schutz der Bevölkerung ist Zweck aller Massnahmen der NCS. Direkt von Cybervorfällen betroffen ist die Bevölkerung vor allem bei Angriffen durch Cyberkriminelle oder wenn ihre persönlichen Daten von Cybervorfällen betroffen sind. Die NCS trägt dazu bei, die Bevölkerung vor solchen Bedrohungen zu sensibilisieren, zu warnen und ihr einen sicheren Umgang mit digitalen Technologien zu ermöglichen. Sie erhöht den Datenschutz, indem Verantwortliche und Betroffene die Kontrolle über die Personendaten behalten und der missbräuchliche Zugriff durch Dritte erschwert wird.
- **Wirtschaft:** Für die Wirtschaft ist ein sicheres Umfeld eine wichtige Grundlage und ein Standortfaktor. Cyberbedrohungen stellen alle Unternehmen, insbesondere KMU, vor grosse Herausforderungen. Die Umsetzung der NCS dient der Erhöhung der Sicherheit für die Unternehmen der Schweiz. Es wird definiert, welche Unterstützung die Unternehmen subsidiär zu den Angeboten des Marktes beim Umgang mit Cyberbedrohungen erhalten. Die Verantwortung für den Eigenschutz verbleibt dabei bei den Unternehmen selbst.
- **Kritische Infrastrukturen:** Kritische Infrastrukturen stellen die Verfügbarkeit von essenziellen Gütern und Dienstleistungen sicher. Ihr Funktionieren ist unabdingbar für die Bevölkerung und die Wirtschaft der Schweiz. Ihr Schutz hat hohe Priorität und steht bei allen Massnahmen der NCS im Fokus, wobei die unterschiedlichen Voraussetzungen in Bezug auf deren Risikoexposition berücksichtigt werden.
- **Behörden:** Bund, Kantone und Gemeinden sind verantwortlich für den Schutz ihrer Dienstleistungen. Sie müssen bei der Erfüllung ihres Auftrags eine hohe Verfügbarkeit aufweisen. Weiter behandeln Behörden aller Staatebenen sensitive Informationen und bieten zunehmend Dienstleistungen online an. Die Umsetzung der NCS ermöglicht eine Verbesserung der Resilienz von Behörden.
- **Internationale Organisationen und Nichtregierungsorganisationen:** Die Schweiz unterstützt die internationalen Organisationen beim Schutz vor Cyberbedrohungen und schafft sichere Rahmenbedingungen für die Tätigkeiten von internationalen Organisationen und Nichtregierungsorganisationen in Bezug auf die Cybersicherheit.

3 Massnahmen der NCS

Zur Erreichung der fünf strategischen Ziele werden die in diesem Kapitel beschriebenen Massnahmen umgesetzt. Die Massnahmen bauen auf den bisherigen Aktivitäten auf und spezifizieren, wie diese ausgebaut, weiterentwickelt und ergänzt werden müssen, um die strategischen Ziele zu erreichen. Es wird zudem aufgezeigt, welche Schwerpunkte bei der Umsetzung der Massnahmen gesetzt werden und welche Akteure dabei involviert sind. Die Auflistung der Schwerpunkte widerspiegelt dabei den Stand bei Erstellung der Strategie und wird durch den Steuerungsausschuss NCS laufend geprüft und bei Bedarf ergänzt.
Die Auflistung der Akteure ist nicht abschliessend zu verstehen, sondern soll dem Steuerungsausschuss aufzeigen, an welche Akteure er sich bei der Beurteilung und Weiterentwicklung der Massnahme wenden soll. Bei der Auflistung der zentralen Akteure der Bundesverwaltung werden die hauptverantwortlichen Verwaltungseinheiten jeweils zuerst genannt und kursiv hervorgehoben und die weiteren relevanten Akteure dann alphabetisch aufgelistet. Die Organisationen der Kantone, Hochschulen, Wirtschaft und Gesellschaft werden separat aufgeführt. Für alle Organisationen werden Kürzel verwendet, welche im Abkürzungsverzeichnis ausgeschrieben sind.
Vor der Umsetzung jeglicher Massnahmen ist zu prüfen, ob die erforderlichen Rechtsgrundlagen bestehen oder ob das Recht durch die jeweils zuständige Staatsebene angepasst werden muss. Dies gilt etwa in Bezug auf den Austausch von Daten, der insbesondere in Bezug auf Personendaten jeweils im anwendbaren Gesetzes- und Verordnungsrecht geregelt sein muss.

3.1 Massnahmen für das Ziel «Selbstbefähigung»

Um die Selbstbefähigung der Schweiz beim Schutz vor Cyberbedrohungen zu stärken, werden Massnahmen in den Bereichen Bildung, Forschung und Innovation, in der Sensibilisierung, bei der Beurteilung der Bedrohungslage und für den Ausbau der Fähigkeiten für die Analyse von Abhängigkeiten und Risiken ergriffen.

M1 Bildung, Forschung und Innovation in der Cybersicherheit

Übersicht Massnahme	
Beschreibung	Um sich vor Cyberbedrohungen zu schützen, braucht die Schweiz ausreichend fachspezifisches Personal. Zugleich muss gewährleistet sein, dass die Bevölkerung über die Grundkompetenzen für den Umgang mit digitalen Technologien und Dienstleistungen verfügt. Die entsprechenden Fähigkeiten sollen durch die bestehenden Bildungs- und Forschungsinstitutionen bereichsübergreifend aufgebaut, vermittelt und weiterentwickelt werden. Bildung, Forschung und Innovation braucht es aber nicht nur zur Stärkung des Schutzes vor Cyberbedrohungen, sie sollen vielmehr direkt zum Erfolg des Wirtschaftsstandorts Schweiz beitragen. Die Schweiz will ihre gute Ausgangslage als neutrales Land mit einem hohen Ausbildungsstandard und einem starken Innovationssystem nutzen, um zu den weltweit führenden Standorten für Dienstleistungen und Produkte im Bereich der Cybersicherheit zu gehören.

Ausgangslage und Handlungsbedarf	Die Schweiz verfügt über ein leistungsfähiges Netzwerk an Ausbildungs- und Forschungsinstitutionen. Es wurden in den letzten Jahren verschiedene Ausbildungsmöglichkeiten mit Bezug zu Cyberrisiken aufgebaut. Der hohe Bedarf der Wirtschaft an Fachleuten für Cybersicherheit kann jedoch noch nicht ausreichend gedeckt werden und die Vermittlung von Kompetenzen im Bereich Cybersicherheit findet noch nicht durchgehend über alle Ausbildungsstufen (obligatorische Schule, Sekundarstufe II und Tertiärstufe sowie Weiterbildung) statt. In der Schweiz hat sich in den letzten Jahren eine beachtliche Start-up-Szene im Bereich der Cybersicherheit entwickelt und verschiedene wichtige Akteure haben Niederlassungen in der Schweiz eröffnet. Ein Vergleich mit international führenden Regionen und mit der Innovationsfähigkeit der Schweiz in anderen Bereichen macht aber deutlich, dass die Rahmenbedingungen für Innovationen in der Cybersicherheit weiter verbessert werden müssen.
Schwerpunkte	- Bildung: Die Aus- und Weiterbildung zur Cybersicherheit soll auf allen Stufen gefördert werden. Während in der obligatorischen Schulzeit vor allem grundlegende Kompetenzen vermittelt werden sollen, braucht es für die Berufsbildung (Grundbildung und höhere Berufsbildung), die Hochschulbildung sowie die Weiterbildung gezielte, auf die Bedürfnisse des Arbeitsmarkts zugeschnittene Angebote. Bei der Förderung der Bildung zur Cybersicherheit werden die bewährten Instrumente der Schweizer Bildungspolitik genutzt. Die Lehrpersonen werden mit geeigneten Lehrmitteln und durch Fachspezialistinnen und Fachspezialisten bei der Vermittlung der Kompetenzen zur Cybersicherheit unterstützt und die Koordination unter den Bildungsinstitutionen wird gefördert. Für Fachpersonen (z. B. kritische Infrastrukturen) sollen verstärkt spezifische Trainings und Ausbildungsgänge in der Schweiz angeboten werden. - Forschung: Die Forschung zur Cybersicherheit wird über die bestehenden Mittel der Forschungspolitik gefördert. Der Einfluss der exzellenten Forschung der Schweiz auf Politik, Wirtschaft und Gesellschaft muss ausgebaut werden. Dazu ist eine verstärkte Koordination der Forschenden der verschiedenen Disziplinen der Cybersicherheit nötig, damit gemeinsame Empfehlungen erarbeitet und kommuniziert werden können. - Innovation: Ein ideales Umfeld für Innovationen entsteht durch die Vernetzung von Akteuren. Der Austausch zwischen Hochschulen, Unternehmen und Behörden soll weiter ausgebaut werden. Die zuständigen Bundesstellen fördern im Rahmen der rechtlichen Möglichkeiten den Einbezug von Expertinnen und Experten in die Cybersicherheit über die bereits existierenden Innovation Fellowships und ähnliche Programme.
Zentrale Akteure	- Bund: *CYD Campus, NCSC, SBFI* - Kantone: KKJPD, SPI, EDK, SHK - Hochschulen: Alle Schweizer Hochschulen, SSCC, swissuniversities, ETH-Rat - Wirtschaft / Gesellschaft: Berufsbildung Schweiz, IKT-Verbände, Innosuisse, SATW

M2 Sensibilisierung

Übersicht Massnahme	
Beschreibung	Damit die Schweizer Bevölkerung elektronische und digitale Produkte und Dienstleistungen risikobewusst nutzen kann, braucht es Sensibilisierungsmassnahmen. Ziel ist es, flächendeckend ein hohes Bewusstsein für die Cybersicherheit zu schaffen und Instrumente bereit zu stellen, die den eigenverantwortlichen Umgang mit digitalen Technologien und Dienstleistungen fördern. Dazu gehört auch das datenschutzrechtliche Ziel, dass Einzelpersonen die Kontrolle über ihre persönlichen Daten behalten und Unternehmen und Organisationen ihre Datenbearbeitungsmethoden transparent machen. Insgesamt soll über die Sensibilisierung die Resilienz der Gesellschaft gegenüber Cyberrisiken gestärkt werden.
Ausgangslage und Handlungsbedarf	Die Sensibilisierung für die Cybersicherheit steht in zahlreichen Schweizer Institutionen, Unternehmen und Organisationen auf der Agenda, immer mit dem Ziel, Unternehmen und Private widerstandsfähig gegen Cyberrisiken zu machen. Es braucht jedoch eine verstärkte Koordination und Bündelung der laufenden und geplanten Anstrengungen, denn es gilt, möglichst zielgruppengerecht und nach Betroffenheit zu sensibilisieren. Aus diesem Grund müssen die Zielgruppen definiert und der Bedarf an Massnahmen dort erhoben werden, wo die grösste Nähe zu den Zielgruppen besteht. Die Botschaften müssen unter den Absendern abgestimmt werden, um durch eine abgeglichene Kommunikation das Verständnis der Empfänger für die zuweilen komplexe Materie zu fördern. Viele Kompetenzen zur Ansprache bestimmter Zielgruppen existieren bereits. Aus diesem Grund sollen bestehende Gremien und Organisationen sowie ihre Kanäle zur Vermittlung der Massnahmen wie bis anhin weiter genutzt werden (z. B. über Veranstaltungen und Fachzeitschriften von Verbänden, Interessensgruppen, Dachorganisationen).
Schwerpunkte	- Bedarfserhebung: Der Sensibilisierungs- und Präventionsbedarf in den unterschiedlichen Bereichen wird kontinuierlich geprüft. Als Grundlage dafür dienen aktuelle Vorfälle, die Entwicklung der Bedrohungslage sowie die Einschätzungen der Behörden, Unternehmen und Wirtschaftsverbände zum Sensibilisierungsbedarf in ihren Bereichen. - Übersicht und Koordination: Die in der Sensibilisierung tätigen Akteure sind bekannt und der Austausch unter ihnen wird gezielt gefördert. - Messung: Die Aufwände und Wirkungen der Sensibilisierungsmassnahmen werden erhoben, um ihren Erfolg zu ermitteln und sie optimieren zu können.
Zentrale Akteure	- Bund: *NCSC,* BABS, BAKOM, BAV, BAZL, BFE, BSV, BWL, EDÖB, NDB - Kantone: Gemeinden und Städte, kantonale Kompetenzzentren für Cybersicherheit, Kantonale Polizeikorps, KKJPD, SKP - Wirtschaft / Gesellschaft: Alle interessierten Branchen- und Wirtschaftsverbände, Vereine, NGO und Einzelfirmen werden wo sinnvoll in die Kampagnen einbezogen.

M3 Bedrohungslage

Übersicht Massnahme	
Beschreibung	Für die Beurteilung der Bedrohungslage muss festgestellt werden, welche Akteure welche Angriffsvektoren und Schwachstellen ausnutzen oder ausnutzen könnten. Dabei wird auch eine Gewichtung der Bedrohungen vorgenommen. Daraus resultiert dann eine Einschätzung zur Bedrohungslage, auf deren Grundlage Wirtschaft, Gesellschaft und Verwaltung ihre risikominimierenden Massnahmen möglichst kosteneffizient und zielgerichtet identifizieren und umsetzen können. Die Bedrohungslage soll somit nicht nur grundlegende und breitenwirksame, sondern auch geschäfts- und prozessspezifische Bedrohungen aufzeigen.
Ausgangslage und Handlungsbedarf	Die Schweiz verfügt bereits über periodisch nachgeführte, taktische, operative und strategische Darstellungen der Bedrohungslage im Cyberbereich. Diese speisen sich aus der Beobachtung von Bedrohungsakteuren und deren tatsächlichen und potenziellen Möglichkeiten sowie aus Informationen zu den durch Cybervorfälle verursachten Schäden oder Ausfälle. Aufgrund der zunehmenden Digitalisierung von Prozessen in verschiedenen Wirtschaftssektoren steigt der Bedarf nach spezifischen, auf diese Sektoren ausgerichtete Einschätzungen zur Bedrohungslage. Diesem Bedarf soll über eine adressatengerechte Aufarbeitung der bedrohungsrelevanten Information entgegengekommen werden. Bedrohungsrelevante Informationen sollen Unternehmen und übrigen Organisationen bedarfsgerecht vermittelt werden.
Schwerpunkte	- Weiterentwicklung der Lageverfolgung mit Fokus auf die Akteure, von denen eine Bedrohung für die Schweiz auf taktischer, operativer und strategischer Ebene ausgeht. - Weiterentwicklung der Einschätzung und Aufbereitung lagerelevanter Informationen. Stufengerechte Zurverfügungstellung für Wirtschaft, Gesellschaft und Verwaltung. - Unterstützung des Aufbaus von sektorspezifischen Informationsaustausch- und Analysezentren (ISACs) sowie Etablierung einer engen Zusammenarbeit zur Beurteilung der spezifischen Bedrohungslagen.
Zentrale Akteure	- Bund: *NDB*, NCSC - Kantone: Kantonale Polizeikorps, kantonale Kompetenzzentren für die Cybersicherheit, Informatikämter, NEDIK - Wirtschaft / Gesellschaft: CERTs/SOCs der Wirtschaft, ISACs, Sicherheitsdienstleister, SWITCH

M4 Analyse von Trends, Risiken und Abhängigkeiten

Übersicht Massnahme	
Beschreibung	Für die Schweiz ist es von grosser Bedeutung zu verstehen, wie gross die Abhängigkeit von digitalen Technologien ist, wie sie sich entwickelt und welche Risiken sie mit sich bringt. Weil sich digitale Technologien dynamisch entwickeln, ist dabei wichtig, neue Entwicklungen frühzeitig zu erkennen und deren Auswirkungen auf die Sicherheit zu verstehen. Dies soll dazu beitragen, die Schweiz als Wirtschaftsstandort zu stärken; als Standort, an dem sichere digitale Technologien und Dienstleistungen angewendet und selber entwickelt werden. Ein weiterer Analysebedarf entsteht dadurch, dass digitale Schlüsseltechnologien heute mehrheitlich im Ausland hergestellt werden. Es ist für die Schweiz wichtig zu verstehen, welche Abhängigkeiten von diesen Herstellern bestehen und welche Risiken damit verbunden sind. Die Schweiz muss Entscheidungen über den Einsatz von digitalen Technologien und Dienstleistungen treffen können, welche auf eigenständigen, unabhängigen Analysen und Einschätzungen beruhen.
Ausgangslage und Handlungsbedarf	Das Technologiemonitoring in Bezug auf die Cybersicherheit wird durch den Cyber Defence Campus in enger Zusammenarbeit mit den Hochschulen und der Wirtschaft durchgeführt. Die Schweizerischen Akademien der Wissenschaften haben den Auftrag, Chancen und Risiken von neuen Technologien zu beurteilen. Deutlich weniger weit ist die Schweiz bei der systematischen Analyse der Abhängigkeiten und Risiken mit Bezug zu IKT-Produkten. Mit dem Nationalen Testinstitut für Cybersicherheit (NTC) ist ein Zentrum im Aufbau, welches die Kapazitäten erhalten soll, IKT-Produkte vertieft auf ihre Angriffsoberfläche hin zu untersuchen. Dieses ergänzt und verstärkt die heute beim CYD Campus vorhandenen Fähigkeiten und die vermehrt auch bei privaten Sicherheitsdienstleistern aufgebauten Fähigkeiten. Solche Fähigkeiten sind eine Voraussetzung für eine unabhängige Einschätzung der Sicherheit von Produkten, welche zum Beispiel bei kritischen Infrastrukturen eingesetzt werden. Ebenfalls weiteres Potenzial besteht in der systematischen Auswertung von Vorfällen. Solche können dazu beitragen, besser zu verstehen, wer von welchen Angriffen betroffen ist und wie solche in Zukunft verhindert werden könnten. Dazu braucht es einen etablierten Informationsaustausch zwischen Behörden, Sicherheitsdienstleistern und Hochschulen und die Bereitschaft betroffener Unternehmen, transparent über Vorfälle und deren Auswirkungen zu informieren.

Schwerpunkte	- Monitoring von neuen Technologien: Der CYD Campus antizipiert zusammen mit den Hochschulen die technologischen Cyberentwicklungen und stellt die Erkenntnisse dieses Monitorings den relevanten Akteuren zur Verfügung. - Ausbau von Kompetenzen für die Untersuchung von Cybervorfällen: Die Ursachen und Abläufe von Cybervorfällen sollen genauer untersucht und Erkenntnisse aus diesen Untersuchungen systematisch aufbereitet und charakterisiert werden. Zu diesem Zweck wird der Datenaustausch zwischen Behörden, Versicherern und Sicherheitsdienstleistern im Rahmen der rechtlichen Möglichkeiten gefördert. Die Untersuchungen sind für Betroffene freiwillig und sollen helfen, aus Cybervorfällen zu lernen. - Für die Prüfung von IKT-Produkten und digitalen Netzwerken wird auf Testzentren in der Schweiz wie das Nationale Testinstitut für Cybersicherheit NTC oder auf Anbieter von Schwachstellenanalysen und Penetrationstests verwiesen. Mit dem Ausbau des NTC für Cybersicherheit werden so in Zusammenarbeit mit den Hochschulen und der Privatwirtschaft sowie internationalen Partnern die Fähigkeiten und Prüfkapazitäten in der Schweiz für die unabhängige Analyse von Risiken in IKT-Produkten gestärkt. Der CYD Campus stärkt seine Fähigkeiten für solche Analysen bei der Beschaffungsvorbereitung und Beschaffung von sicherheitskritischen IKT-Produkten für den Bund ebenfalls weiter. - Der Ausbau des Nationalen Testzentrums für Cybersicherheit wird vorangetrieben. In Zusammenarbeit mit den Hochschulen und der Privatwirtschaft werden so Fähigkeiten für die unabhängige Analyse von Risiken in IKT-Produkten geschaffen. - Abhängigkeiten: Es wird analysiert, welche Abhängigkeiten von welchen Produkten und welchen Zulieferern in der Schweiz wie ausgeprägt sind. Unternehmen, Hochschulen und Behörden legen dabei gemeinsam fest, wie diese Analysen durchgeführt und laufend aktualisiert werden können. - Monitoring von KI-Anwendungen in kritischen Infrastrukturen: Um die Fähigkeiten dieser Anwendungen und deren Auswirkungen auf die Gesellschaft besser zu verstehen, soll ihr Einsatz im Auftrag von Bund und Kantonen regelmässig überprüft werden. - Stärkung des Austausches zwischen den Forschungsstellen: Der bestehende Austausch im Rahmen des CYD Campus, den Hochschulen und der SATW wird weiter ausgebaut und untereinander koordiniert.
Zentrale Akteure	- Bund: *CYD Campus, NCSC*, DTI, NDB, - Hochschulen: SSCC - Wirtschaft / Gesellschaft: NTC, SATW, Sicherheitsdienstleister

3.2 Massnahmen für das Ziel «Sichere und verfügbare digitale Dienstleistungen und Infrastruktur»

Um die Sicherheit von digitalen Dienstleistungen und Infrastrukturen zu gewährleisten, sind Massnahmen auf verschiedenen Ebenen nötig. Wichtig ist, dass Verwundbarkeiten in den Dienstleistungen und Infrastrukturen frühzeitig erkannt und behoben werden und neue Dienstleistungen und Infrastrukturen so entwickelt werden, dass sie von Anfang an möglichst wenig Schwachstellen aufweisen. Neben der Erkennung und Behebung von Schwachstellen ist das Resilienzmanagement von entscheidender Bedeutung. Basierend auf Risiko- und Verwundbarkeitsanalysen muss festgelegt werden, welche technischen und organisatorischen Massnahmen umgesetzt werden um die Resilienz der Dienstleistungen und Infrastrukturen zu erhöhen. Dazu gehört es auch zu prüfen, in welchen Bereichen über Standards oder Regulierungen Vorgaben gemacht werden müssen. Schliesslich gilt es für die Behörden, ihre eigenen Dienstleistungen gegenüber Cyberbedrohungen zu schützen.

M5 Schwachstellen erkennen und verhindern

Übersicht Massnahme	
Beschreibung	Der Einsatz von digitalen Technologien führt zu Prozessautomatisierungen und Vernetzungen. Daraus entstehen komplexe Systeme, die potenziell eine grosse Angriffsfläche aufweisen. Diese Komplexität in Kombination mit dem oft hohen Kosten- und Zeitdruck bei der Entwicklung und Anwendung solcher Technologien erhöhen das Risiko von Schwachstellen in den Systemen. Für die Cybersicherheit ist es von essenzieller Bedeutung, dass die Entstehung solcher Schwachstellen wo immer möglich verhindert wird und bestehende Schwachstellen rechtzeitig erkannt und rasch behoben werden. Wichtig ist, dass Schwachstellen erst dann veröffentlicht werden, wenn Gegenmassnahmen identifiziert und umgesetzt wurden («Coordinated Vulnerability Disclosure»), da die Veröffentlichung sonst die Angreifenden stärkt.
Ausgangslage und Handlungsbedarf	In der Schweiz ist viel Fachwissen vorhanden, um Schwachstellen zu identifizieren und Ursachen zu analysieren. Das Potenzial wird aber noch zu wenig genutzt. Es bestehen für Sicherheitsforschende zu wenige Anreize, Schwachstellen zu suchen und zu melden, und es fehlt an einer nationalen Koordination bei der Schwachstellenanalyse. Wichtig ist zudem eine enge Zusammenarbeit mit Fachstellen anderer Länder und internationaler Organisationen. Voraussetzung für ein effektiveres Schwachstellenmanagement ist die Schaffung von Rechtsgrundlagen für die Untersuchung, Meldung und die Veröffentlichung von Schwachstellen. Schliesslich ist darauf hinzuwirken, dass Sicherheitslücken zügig kommuniziert und auch geschlossen werden. Zu viele Unternehmen und Organisationen bleiben verwundbar, weil sie Schwachstellen nicht beheben, obwohl für diese längst Lösungen (Patches) vorhanden wären.

Schwerpunkte	- Ethisches Hacking institutionalisieren: Bug-Bounty- und Public-Trust-Programme werden durchgeführt. Das ethische Hacking wird gefördert, indem die Rechtssicherheit für ethische Hacker verbessert wird. - Coordinated Vulnerability Disclosure: Um Sicherheit und Vertrauen durch Transparenz zu schaffen, wird ein koordiniertes Vorgehen bei der Entdeckung von Schwachstellen gefördert. Dazu werden, Richtlinien definiert und verbreitet und Anreize für das Melden von Schwachstellen geschaffen - Schwachstellenkommunikation zentralisieren: Das NCSC wird als zentrale Drehscheibe für die Koordination und Publikation von Meldungen zu Schwachstellen positioniert und verbreitet Informationen und Warnungen zu neuen Schwachstellen sowie zu technischen und organisatorischen Lösungen für deren Behebung. - Automatisierte Schwachstellenerkennung: Es werden Lösungen zur automatisierten Schwachstellenerkennung und Behebung entwickelt und eingesetzt. - Software-Ökosystem: Die sichere Software-Entwicklung (insbesondere im Bereich der Open Source Software) wird durch die Zusammenarbeit mit Organisationen und Initiativen in diesem Bereich unterstützt. Ziel ist die Schaffung von Anreizen für eine frühzeitige Berücksichtigung der Sicherheit bei der Entwicklung von Software. Bei der Entwicklung von IKT-Komponenten sollen formal verifizierbare Sicherheitseigenschaften definiert werden. - Cybersicherheit bei drahtlosen, mit dem Internet verbundenen Geräten: die Anforderungen der revidierten Verordnung über Fernmeldeanlagen müssen durch eine effektive Marktüberwachung durchgesetzt werden.
Zentrale Akteure	- Bund: *BAKOM, CYD Campus, NCSC* - Kantone: Informatikämter, Kantonale Kompetenzzentren für die Cybersicherheit, - Hochschulen: Forschungsinstitute zur IKT-Sicherheit - Wirtschaft / Gesellschaft: Allianz Digitale Sicherheit Schweiz, NTC, Sicherheitsfirmen

M6 Resilienz, Standardisierung und Regulierung

Übersicht Massnahme	
Beschreibung	Um sich vor Cyberbedrohungen zu schützen, bestehen eine Vielzahl von technischen und organisatorischen Massnahmen. Nach wie vor gilt, dass der Grossteil von Cybervorfällen durch eine konsequente Umsetzung grundlegender Massnahmen (Grundschutz) verhindert werden könnte. Grundlage für die Entscheide über die richtigen Massnahmen sind fundierte Analysen über die Risikoexposition gegenüber Cyberbedrohungen. Wenn verstanden wird, wie sich diese Risiken in den einzelnen Sektoren manifestieren, können Massnahmen zur Verbesserung der Resilienz festgelegt werden. Die Massnahmen orientieren sich dabei an internationalen Standards. Diese sind ein wichtiges Instrument zur Umsetzung von Schutzmassnahmen. Die Einhaltung von Standards kann über verschiedene Wege gefördert werden. Neben der Möglichkeit, Standards über regulative Massnahmen für verbindlich zu erklären, sollen vor allem Anreize zu ihrer Umsetzung geschaffen werden. Ein starker Anreiz kann dabei durch Transparenz gesetzt werden, indem über Labels ausgewiesen wird, wer welche Standards einhält. Durch diese Transparenz führen Investitionen in die Cybersicherheit in mehr Vertrauen bei den Kunden.

Ausgangslage und Handlungsbedarf	Risiko- und Verwundbarkeitsanalysen der kritischen Sektoren waren bereits Bestandteil der ersten beiden Cyberstrategien. Die vorhandenen Einschätzungen und die identifizierten Resilienzmassnahmen müssen für alle kritischen Sektoren regelmässig überprüft und angepasst werden. Es bestehen auch bereits gut etablierte, internationale Standards zur Cybersicherheit, die auch in der Schweiz angewendet werden. Das BWL hat in Zusammenarbeit mit der Wirtschaft und den Fachämtern einen IKT-Minimalstandard erarbeitet und daraus Branchenstandards abgeleitet. Verbindlich vorgeschrieben ist die Einhaltung dieser Standards meist nicht. Das neue Datenschutzgesetz, welches im September 2023 in Kraft tritt, führt jedoch Mindestanforderungen an die Datensicherheit bei der Bearbeitung von Personendaten ein. Zusätzlich wird in verschiedenen Sektoren geprüft, welche Standards für welche Organisationen verbindlich eingeführt werden sollen. Neben den branchenspezifischen Standards sind auch technologiespezifische Standards wichtig. Sicherheitsstandards für die Anwendung von Cloud-Computing oder für IoT spielen eine wichtige Rolle bei der Gewährleistung der Sicherheit bei neuen technologischen Anwendungen. Die Schweiz hat mit der Verordnung des BAKOM über Fernmeldeanlagen bereits Vorgaben zur Sicherheit von drahtlosen, mit dem Internet verbundenen Geräte erlassen. Sie prüft nun, welche Vorgaben im Bereich des Cloud-Computings nötig sind. Der Bedarf an der Prüfung und Erarbeitung von rechtlichen Grundlagen beschränkt sich jedoch nicht auf die Frage, ob Standards verbindlich eingeführt werden sollen. Ein Beispiel dafür ist die bereits verabschiedete Vorlage zur Einführung einer Meldepflicht bei Cyberangriffen. Es muss laufend geprüft werden, wo ein allfälliger weiterer Bedarf für Rechtsgrundlagen besteht.
Schwerpunkte	- Die bestehenden Risiko- und Verwundbarkeitsanalysen in den kritischen Teilsektoren werden bedarfsgerecht durch das BABS und die zuständigen Fachämter aktualisiert. Die identifizierten Risiken werden als Teil eines Resilienzmanagements mit geeigneten Handlungsfeldern und Massnahmen zur Verbesserung der Resilienz adressiert. Die Umsetzung der Massnahmen wird regelmässig geprüft und der Austausch über Risiken, Verwundbarkeiten und Resilienzmassnahmen zwischen Bund, Kantonen gefördert - Die Verbreitung der Einhaltung von Standards wird gefördert. Insbesondere soll die Anwendung von Standards bei KMU und Gemeinden gestärkt werden, indem einfache Hilfsmittel zur Verfügung gestellt werden. Bei öffentlichen Beschaffungen ist zudem die Einhaltung von IKT-Sicherheitsstandards zu verlangen und zu überprüfen. - Förderung der Verbreitung der bestehenden Labels: In der Schweiz wurden erfolgreich Labels für die Cybersicherheit eingeführt. Wichtig ist, dass diese Labels untereinander national und international koordiniert werden. Die Anwendung der bestehenden Labels soll deshalb mittels Erfahrungsaustausches zwischen den Labels unterstützt werden. - Es wird geprüft, ob und wie die Verantwortung der Unternehmen für den eigenen Schutz vor Cybervorfällen über rechtliche Vorgaben gestärkt werden kann. Dabei sollen wirksame Regelungen statt detaillierter operativer Vorgaben angestrebt werden. Regelungen müssen zudem sektorübergreifend abgeglichen werden, um Disparitäten zwischen allfälligen Vorgaben möglichst gering zu halten. - Die Notwendigkeit von sektorspezifischen Regulierungen wird geprüft und wo nötig werden entsprechende Vorlagen ausgearbeitet. - Die Pflicht zur Meldung von Cyberangriffen auf kritische Infrastrukturen ist bereits in Prüfung. Bei einem Beschluss wird die Umsetzung in enger Zusammenarbeit mit den Betroffenen angegangen.

Zentrale Akteure	- Bund: *BABS, BAKOM, BAV, BAZL, BFE, NCSC,* BWL, EDÖB, - Kantone: Kantonale Kompetenzzentren für Cybersicherheit - Hochschulen: SSCC - Wirtschaft / Gesellschaft: cyber-safe.ch, ITSec4KMU, Normungsorganisationen, NTC, Sicherheitsdienstleister, Verbände der betroffenen Wirtschaftssektoren, Versicherungen

M7 Ausbau der Zusammenarbeit zwischen den Behörden

Übersicht Massnahme	
Beschreibung	Die Cybersicherheit ist für Behörden auf allen Staatsebenen zu einer zentralen Herausforderung geworden. Digitale Behördendienstleistungen müssen eine hohe Sicherheit aufweisen. Während Angriffe zum Zweck der Spionage seit Jahren zu den relevanten Cyberbedrohungen gehören, haben in jüngerer Zeit auch Angriffe von Kriminellen auf Behörden zugenommen. Diese erpressen beispielsweise Behörden mit der Verschlüsselung und der Veröffentlichung von Behördendaten. Dieser Herausforderung muss auf allen Staatsebenen entgegengetreten werden.
Ausgangslage und Handlungsbedarf	Die eigene Cybersicherheit liegt in der Verantwortung der jeweiligen Behörde. Das Informationssicherheitsgesetz (ISG) legt den Rahmen und die Verfahren für die Sicherheitsmassnahmen im Bund fest und hat für die Kantone dann Gültigkeit, wenn diese auf die Informatikmittel des Bundes zugreifen oder klassifizierte Informationen des Bundes bearbeiten. Es ist eine grosse Herausforderung, die Cybersicherheit in allen föderalen Strukturen sicherzustellen. Da es an Fachpersonal und oft auch an finanziellen Ressourcen fehlt, ist die Zusammenarbeit zwischen Behörden aller Stufen wichtig. Die nötigen Gefässe für die Kooperation bestehen, es bleibt aber noch viel Potenzial für eine stärkere operative Zusammenarbeit. Zu klären ist dabei, wie stark der Bund in welchen Fällen die Kantone, Städte und Gemeinden unterstützen kann.
Schwerpunkte	- Umsetzung des Informationssicherheitsgesetzes innerhalb der Bundesverwaltung. - Förderung des Informationsaustausches zur Cybersicherheit innerhalb der Bundesverwaltung, insbesondere zwischen dem NCSC und den Fachämtern. - Stärkung der Zusammenarbeit zwischen Bund und Kantonen. - Klärung der Unterstützung des Bundes zu Gunsten der Kantone, Städte und der Gemeinden. - Klärung der Unterstützung der Kantone für ihre Gemeinden. - Förderung des Austausches mit internationalen Behörden.
Zentrale Akteure	- Bund und Kantone: *SVS,* DTI, DVS, kantonale Kompetenzzentren für die Cybersicherheit, Armee, kommunale Organisationen (z. B. Gemeindeverband, Städteverband), NCSC

3.3 Massnahmen für das Ziel «Wirksame Erkennung, Verhinderung, Bewältigung und Abwehr von Cyberangriffen»

Die effektive Erkennung, Verhinderung, Bewältigung und Abwehr von Cyberangriffen sind Schlüsselfaktoren der Cybersicherheit. Um geeignete Schutzmassnahmen zu bestimmen, muss klar sein, gegen welche Bedrohungen sie wirken müssen. Kommt es dennoch zu einem Vorfall, braucht es geeignete Werkzeuge, Daten und Prozesse für die Vorfallbewältigung. Anschliessend geht es darum, die Urheber des Angriffs möglichst genau zu identifizieren (Attribution). Dies hilft wiederum, die Bedrohungslage genauer einzuschätzen und hilft, künftige Angriffe zu verhindern. Haben Cybervorfälle Auswirkungen auf die Funktionsfähigkeit von kritischen Infrastrukturen oder auf die Sicherheit der Schweiz, wird ein Krisenmanagement nötig. Damit dieses funktioniert, muss es regelmässig geübt werden.
Schliesslich beschränken sich die Möglichkeiten zur Abwehr von Cyberangriffen nicht auf Massnahmen zum Schutz der eigenen Systeme. Es ist wichtig, dass technische Daten über Angreifer, ihre Infrastrukturen und ihren Modi Operandi gesammelt und möglichen Betroffenen zur Verfügung gestellt werden. Möglich sind auch aktive Massnahmen zur Erkennung von Bedrohungen, zur Identifikation von Angreifern und zur Störung und Unterbindung von Angriffen.

M8 Vorfallmanagement

Übersicht Massnahme	
Beschreibung	Da es keinen vollständigen Schutz gegen Cybervorfälle gibt, gehört der Aufbau und Betrieb einer Organisation zur Bewältigung von Vorfällen zu den Kernaufgaben in der Cybersicherheit. Zur Vorfallbewältigung gehört es, diese so früh wie möglich zu erkennen, die richtigen Gegenmassnahmen zu identifizieren und umzusetzen sowie die Vorfälle zu analysieren, um daraus Erkenntnisse für die Verbesserung der Prävention abzuleiten. Für die Bewältigung dieser Aufgabe braucht es Fachkompetenzen, Analyseinstrumente, eine gut funktionierende Organisation mit klar definierten Entscheidungskompetenzen und eine intensive Zusammenarbeit zwischen allen relevanten Stellen. Entscheidend ist der Informationsaustausch zwischen vertrauenswürdigen Partnern über Vorfälle und mögliche Gegenmassnahmen, da Vorfälle oft verschiedene Stellen gleichzeitig betreffen und deshalb schneller und effektiver bewältigt werden können, wenn alle betroffenen Stellen relevante Informationen austauschen.

Ausgangslage und Handlungsbedarf	Für die Bewältigung von Cybervorfällen haben viele Organisationen – aber noch längst nicht alle kritischen Infrastrukturen – in der Schweiz spezialisierte Teams aufgebaut oder beauftragt. Diese Teams haben unterschiedliche Bezeichnungen (z. B. Security Operations Centers, Computer Emergency Response Teams, Computer Security Incident Response Teams) und jeweils auf ihren Aufgabenbereich ausgerichtete Kompetenzen. Auch viele Kantone und der Bund verfügen über solche Teams. Die Vorfallbewältigung erfolgt in erster Linie über diese Einheiten. Der Bund unterstützt subsidiär die Teams der Kantone, der Gemeinden und Städte sowie der Betreiberinnen kritischer Infrastrukturen und ihrer Sicherheitsdienstleister durch das NCSC bei der technischen Analyse der Vorfälle und unterstützt den Informationsaustausch zwischen ihnen. Auch die breite Öffentlichkeit kann dem NCSC Cybervorfälle und Cyberbedrohungen melden und erhält bei Bedarf erste fachliche Einschätzungen und Empfehlungen zum weiteren Vorgehen. Diese Meldungen sind wichtig für die Einschätzung der Cyberbedrohungen. Diese Leistungen durch den Bund beruhen bisher nicht auf einer gesetzlichen Grundlage. Auch der rechtliche Rahmen des Informationsaustausches muss geregelt werden. Die Vorschläge für die nötigen rechtlichen Anpassungen wurden erarbeitet, sind aber noch nicht beschlossen. Eine Herausforderung bei der Vorfallbewältigung besteht in der Skalierung. Treten mehrere Grossereignisse gleichzeitig ein, sind die bestehenden Ressourcen rasch ausgeschöpft. Es muss geprüft werden, wie die Kapazitäten über die Einbindung von Fachleuten im Bedarfsfall rasch erhöht werden können.
Schwerpunkte	- Ausbau der Fähigkeiten der kritischen Infrastrukturen zur Erkennung und Bewältigung von Cybervorfällen durch den Aufbau und die Schaffung und die gemeinsame Nutzung von SOCs. - Ausbau der Meldungen von Cybervorfällen: Es sollen möglichst viele Cybervorfälle gemeldet werden, damit ein gutes Bild der aktuellen Bedrohungslage entsteht. - Informationsaustausch: Die bestehende Plattform des NCSC für den Informationsaustausch zwischen Betreiberinnen kritischer Infrastrukturen wird überarbeitet und ausgebaut, mit dem Ziel, diesen zu vereinfachen und stufenweise auch breiteren Kreisen zugänglich zu machen. - Kapazitätserweiterung durch Zusammenarbeit: Weitere Intensivierung der operativen Zusammenarbeit und Verbesserung der Abstimmung zwischen dem GovCERT, SWITCH-CERT und weiteren Sicherheitsteams. Es wird darüber hinaus geprüft, wie und wann freiwillige Expertenpools die Vorfallbewältigung unterstützen können. Bestehende Organisationen werden dabei berücksichtigt. - Stärkung der Zusammenarbeit mit den Fachämtern: Damit die zuständigen Fachämter die Bedrohungen in ihrem Sektor abschätzen können, werden sie durch das NCSC über Vorfälle in ihrem Sektor informiert. Davon ausgenommen sind Informationen, welche Rückschlüsse auf Betroffene geben, sofern letztere nicht mit einer Information der Fachämter einverstanden sind.
Zentrale Akteure	- Bund: *NCSC*, BAKOM, BAV, BAZL, BFE, BIT, MilCERT - Kantone: Kantonale CERTs, CSIRTs, SOCs (oder ähnliche Organisationen), Meldestellen der Kantonspolizeien - Wirtschaft / Gesellschaft: CERTs, CSIRTs, SOCs (oder ähnliche Organisationen) von Unternehmen und Organisationen, SWITCH

M9 Attribution

Übersicht Massnahme	
Beschreibung	Attribution bedeutet die möglichst genaue Identifikation der Urheberschaft von Angriffen. Sie spielt eine wichtige Rolle bei der Wahl der Mittel für das weitere Vorgehen. Die Schweizer Behörden müssen in der Lage sein, gegen unser Land gerichtete, sicherheitspolitisch relevante Cyberangriffe zu attribuieren. Dabei kann es sich um Cyberangriffe auf Schweizer Ziele oder auch den Missbrauch von Schweizer Infrastruktur für Angriffe im Ausland handeln. Die Attribution bildet die Grundlage zur Formulierung von politischen und rechtlichen Handlungsoptionen.
Ausgangslage und Handlungsbedarf	Um die Urheber eines Cyberangriffs zur Verantwortung ziehen zu können, müssen sie zuerst identifiziert werden. Dies ist eine grosse Herausforderung im Cyberraum, da die Urheber nicht physisch am Ort des Angriffs sind. Die Identifizierung gelingt nur, wenn Angriffe rechtzeitig erkannt werden und ihr technischer, operationeller und strategischer Kontext analysiert werden kann. Die Attribution von Cyberangriffen ist eine Aufgabe des Nachrichtendienstes des Bundes (NDB). Damit er sie erfüllen kann, braucht er Erkenntnisse aus eigenen Recherchen, ist aber auch auf die Zusammenarbeit mit anderen Stellen des Bundes und den Austausch mit Partnerdiensten angewiesen. Diese gilt es zu regeln. Die Attribution von Cyberangriffen ist für die politischen Verantwortungsträger wichtig, um die Bedrohungslage einschätzen zu können. Dazu gehört die Einschätzung, ob eine Handlung völkerrechtlich attribuiert werden kann und welche Reaktionsmöglichkeiten völkerrechtlich erlaubt sind. Sie ist zudem die Voraussetzung für Entscheidungen über technische, politische oder strafrechtliche Massnahmen.
Schwerpunkte	- Prüfung und Ergänzung der rechtlichen Grundlagen für die Analyse von Cyberangriffen auf die Schweiz. - Zusammenarbeit zwischen NDB und weiteren Stellen. - Ausbau der Fähigkeiten des NDB zur Analyse von sicherheitspolitisch relevanten Cyberangriffen. - Definition der strategischen Prioritäten: Es muss festgelegt werden, welche Angriffe vertieft analysiert werden.
Zentrale Akteure	- Bund: *NDB,* EDA, fedpol, NCSC GS-VBS - Kantone: Kantonale Polizeikorps, NEDIK

M10 Krisenmanagement

Übersicht Massnahme	
Beschreibung	Cybervorfälle können gravierende Konsequenzen haben und so weit eskalieren, dass ein Krisenmanagement auf nationaler Ebene nötig wird. Entscheidend für die Bewältigung von Krisen sind ein aktuelles, einheitliches und umfassendes Lagebild, die Definition von effizienten Prozessen zur Entscheidungsfindung und die Festlegung einer Kommunikationsstrategie. Die entsprechenden Fähigkeiten und Strukturen müssen regelmässig geübt, überprüft und angepasst werden.
Ausgangslage und Handlungsbedarf	Die bereichsübergreifende Zusammenarbeit ist im Krisenfall entscheidend. Das NCSC muss fähig sein, die Zusammenarbeit mit allen Partnern im Krisenfall rasch zu etablieren. Es verfügt zu diesem Zweck über Kontakte zu den relevanten Organisationen innerhalb und ausserhalb der Bundesverwaltung. Zusätzlich wurde das NCSC in die Krisenstäbe des Bundes integriert. Es muss auch bei allfälligen Weiterentwicklungen oder Umgestaltungen des Krisenmanagements im Bund sichergestellt werden, dass die Cybersicherheit direkt in die Strukturen des Krisenmanagements einbezogen wird. Die Zusammenarbeit zwischen den zentralen Akteuren aus Bund, Kantonen und Wirtschaft unter Zeitdruck zur Bewältigung einer Krise ist anspruchsvoll. Damit sie funktioniert, braucht es regelmässige Übungen. Die Schweiz beteiligt sich heute an internationalen Übungen, und es wurden national einzelne sektorspezifische Übungen durchgeführt. Es fehlt jedoch ein übergreifendes Konzept zur Planung und Implementierung von Krisenübungen im Bereich der Cybersicherheit. Diese Planung muss erstellt und in die Gesamtplanung von Krisenübungen eingebracht werden.
Schwerpunkte	- Konzeptionierung und Umsetzung von sektorspezifischen (z. B. Energieversorgung, Wasserversorgung, Gesundheitsversorgung) und sektorübergreifenden Cyberübungen. Die Planung und Konzeptionierung muss dabei in Koordination mit der Gesamtplanung von Krisenübungen erfolgen. - Integration von Aspekten der Cybersicherheit in alle geplanten Krisenübungen. - Klärung der Grundlagen in Abstimmung mit den übergeordneten Arbeiten zur Organisation des Krisenmanagements: Welche Kriterien definieren eine Krise mit Bezug zur Cybersicherheit? Welche Strukturen sind für die politische Beurteilung und für die Einleitung von Massnahmen des Krisenmanagements zuständig? - Sicherstellung der Vertretung der Cybersicherheit im Dispositiv der Krisenbewältigung (auf Stufe Bund und auf Stufe Kantone). - Klärung der (subsidiären) Unterstützung zur Krisenbewältigung im Verbund, inklusive der dabei zu verwendenden Kommunikationsmittel.
Zentrale Akteure	- Bund: *BK, BABS, NCSC*, Armee, BAKOM, BAV, BAZL, BFE, BWL, EDA, GS-VBS, SVS - Kantone: Kantonale Führungsorganisationen, kantonale Kompetenzzentren für die Cybersicherheit. - Wirtschaft / Gesellschaft: Betreiberinnen kritischer Infrastrukturen, Hersteller/Anbieter kritischer Software, Sektororganisationen (wie z. B. Swiss FS-CSC, SWITCH-CERT)

M11 Cyberdefence

Übersicht Massnahme	
Beschreibung	Die Handlungsfreiheit und Integrität des Staats, der Wirtschaft und der Bevölkerung muss im Cyberraum geschützt und im Konfliktfall verteidigt werden. Zur Cyberdefence gehört die Gesamtheit der nachrichtendienstlichen und militärischen Massnahmen zu folgenden Zwecken: dem Schutz der für die Landesverteidigung kritischen Systeme, der Abwehr von Cyberangriffen, der Gewährleistung der Einsatzbereitschaft der Schweizer Armee in allen Lagen und dem Aufbau von Kapazitäten und Fähigkeiten zur subsidiären Unterstützung ziviler Behörden. Dazu zählen, unter anderem, aktive Massnahmen zur Erkennung von Bedrohungen, zur Identifikation von Angreifern und zur Störung und Unterbindung von Angriffen.
Ausgangslage und Handlungsbedarf	Der Nachrichtendienst des Bundes (NDB) und die Schweizer Armee haben ihre Fähigkeiten für ihre Aufgaben im Bereich der Cyberdefence ausgebaut. Die «Gesamtkonzeption Cyber» beschreibt, welche Fähigkeiten die Schweizer Armee bis Mitte der 2030er-Jahre entwickeln muss, um Bedrohungen im und aus dem Cyber- und elektromagnetischen Raum begegnen zu können. Mit dem Nachrichtendienstgesetz (NDG) und dem revidierten Militärgesetz (MG) verfügt der Bund über die notwendigen Rechtsgrundlagen für aktive Gegenmassnahmen im Rahmen der Cyberdefence. Die Entwicklung von Cyberangriffen über die letzten Jahre und ihre wachsende Komplexität bindet jedoch zunehmend Ressourcen über längere Zeiträume. Handlungsbedarf besteht deshalb weiterhin im Ausbau der Fähigkeiten und bei der Koordination mit den zuständigen Stellen zur Einhaltung des Völkerrechts.
Schwerpunkte	- Ausbau der zentralen Fähigkeiten auf Stufe Armee. Dazu gehören CER-Eigenschutz, Antizipation und Autonomie sowie die Grundbefähigung in Datascience. - Aufbau von dezentralen Fähigkeiten. Dies beinhaltet zum Beispiel die robuste und sichere Datenverarbeitung innerhalb von Bataillonen und Kompanien. Ein weiteres Schwergewicht bildet der Resilienzausbau der einsatzrelevanten Kerninfrastruktur im CER-Eigenschutz. Zudem wird die Organisation der Verbände angepasst. - Reifung der politischen Fallbearbeitung für sicherheitspolitisch relevante Cyberkampagnen. - Verstärkte Integration der Fähigkeiten der Schweiz, um eine direkte Schutzwirkung für Schweizer Stakeholder zu erzielen. - Erweiterung der Grundfähigkeiten für Aktionen im Cyberraum des NDB und der Armee.
Zentrale Akteure	- Bund: *Armee,* CYD Campus, GS-VBS, NDB - Kantone: Kantonale Führungsorganisationen

3.4 Massnahmen für das Ziel «Effektive Bekämpfung und Strafverfolgung der Cyberkriminalität»

Die über das Internet verfügbare digitale Infrastruktur eröffnet potenziellen Straftätern und Straftäterinnen neuartige Möglichkeiten mit grossem Schadenspotenzial für Gesellschaft und Wirtschaft. Cyberkriminalität überschreitet territoriale Grenzen, und dies in einem hochdynamischen Prozess mit kurzen Innovationszyklen. Je stärker die digitale Vernetzung ist, desto grösser wird die Gefahr, dass Cybervorfälle zwar in der virtuellen Welt beginnen, aber ihre schädigende Wirkung in der realen Welt entfalten.
Vor dem Hintergrund dieser Entwicklung ist es wichtig, gesamtschweizerisch und in Zusammenarbeit mit internationalen Partnern die Interoperabilität und Reaktionsfähigkeit weiter zu verbessern sowie die fachlichen, technischen und personellen Kompetenzen wirksam aufeinander abzustimmen, ohne dabei die Befugnisse zwischen den verschiedenen Behörden und Staatsebenen zu verschieben.

M12 Ausbau der Zusammenarbeit der Strafverfolgungsbehörden

Übersicht Massnahme	
Beschreibung	Die Zusammenarbeit bei der Strafverfolgung von Cyberkriminellen zwischen Bund und Kantonen sowie zwischen den Kantonen soll weiter ausgebaut werden. Sie ist entscheidend für eine effiziente und effektive Strafverfolgung. Sie erfolgt bereits heute im Rahmen der rechtlichen Möglichkeiten, insbesondere über das Netzwerk digitale Ermittlungsunterstützung Internetkriminalität (NEDIK), muss aber gefestigt und weiterentwickelt werden. Dazu gehört auch zu prüfen, welche Anpassungen der rechtlichen Grundlagen dafür nötig sind. Die Zusammenarbeit kann durch verschiedene zusätzliche Massnahmen gestärkt werden. Wenn gemeinsame Vorgehensweisen definiert und Prozesse standardisiert werden, ist bereits eine Grundlage für eine einfachere Kooperation gelegt. Bei schwierig zu beschaffenden Fachkompetenzen (z. B. im Bereich digitale Forensik) kann ein direkter Austausch zwischen Fachpersonen oder gar eine regionale Bündelung der Kompetenzen sehr hilfreich sein, auch bezüglich eines koordinierten Aus- und Weitebildungsangebots. Die für die Strafverfolgung entscheidende internationale Zusammenarbeit soll weiter gestärkt werden. Im Fokus steht insbesondere die Kooperation mit EUROPOL.
Ausgangslage und Handlungsbedarf	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. Im Rahmen des Cyberboards soll der Cyber-CASE den Informations- und Wissensaustausch unter spezialisierten Fachpersonen der Staatsanwaltschaften und der Ermittlungsbehörden im Rahmen von drei bis vier jährlichen Tagungen ermöglichen. Das Cyberboard soll weiter gestärkt werden. Die Zusammenarbeit zwischen den Kantonspolizeien wird über NEDIK und über das regionale Cyber Competence Center (RC3) gestärkt. Über NEDIK erfolgt eine regelmässige Abstimmung zu strategischen und operativen Themen. Dank diesen Gremien besteht bereits eine gute Zusammenarbeit, welche weiter ausgebaut werden soll. Diese kann nun gezielt in jenen Bereichen gefördert werden, in welchen der grösste Nutzen erzielt wird. Die örtlichen Zuständigkeitsregeln der Strafprozessordnung erschweren die Strafverfolgung der Cyberkriminalität. Die Schaffung rechtlicher Grundlagen zum nationalen Datenaustausch muss deshalb vordringlich geprüft werden.
Schwerpunkte	- Stärkung der bestehenden Zusammenarbeit: durch die Standardisierung von Prozessen sowie Schnittstellen und Förderung des Erfahrungsaustausches. - Bündelung von Fachkompetenzen (z. B. zu IT-Forensik) und von sicherheitsrelevanten Beschaffungen. - Koordination bei der Zusammenarbeit mit nationalen und internationalen Akteuren, vor allem im Bereich der Beweissicherung sowie der Rechtshilfen. - Prüfung der Rechtsgrundlagen für die Zusammenarbeit und Schaffung neuer Rechtsgrundlagen bei Bedarf.
Zentrale Akteure	- Bund: *BA*, *fedpol*, BJ, - Kantone: kantonale Polizeikorps, KKJPD, KKPKS, Staatsanwaltschaften, SSK - Gemeinsame Gremien: Cyberboard, NEDIK, SKK

M13 Fallübersicht

Übersicht Massnahme	
Beschreibung	Eine Übersicht über Ereignisse ist eine wichtige Voraussetzung für die Einschätzung der Bedrohungslage. Sie ist auch für die Strafverfolgung von grosser Bedeutung. Eine Fallübersicht dient der Steigerung der Effizienz, der Qualität und der Aufklärungsquote bei interkantonalen oder internationalen Fallkomplexen Zu unterscheiden sind drei Stufen der Fallübersicht: Ereignisse (z. B. gemeldete Vorfälle), eingegangene Anzeigen und die justizielle Fallübersicht über die laufenden Verfahren. Eine vollständige Übersicht ist dann erreicht, wenn sich die Daten der verschiedenen Stufen in Echtzeit miteinander korrelieren und auswerten lassen.
Ausgangslage und Handlungsbedarf	Mit der Etablierung der Nationalen Anlaufstelle Cyberrisiken für Cyberbedrohungen im NCSC und den Meldestellen bei Kantonspolizeien (z. B. cybercrimepolice.ch) ist es gelungen, deutlich mehr Informationen über Cybervorfälle aus Bevölkerung und Wirtschaft zu erhalten. Das Bundesamt für Statistik veröffentlicht zudem jährlich Kennzahlen zur Entwicklung er digitalen Kriminalität. Zwischen den Justiz- und Strafverfolgungsbehörden werden die vorhandenen Daten im Rahmen der rechtlichen Möglichkeiten bereits heute ausgetauscht. Für die systematische und strukturierte Erfassung von Fällen steht mit PICSEL (Plateforme d'Information de la Criminalité Sérielle En Ligne) ein Instrument zur Verfügung, welches es erlaubt, Serien festzustellen und neue Phänomene und Modi Operandi zu identifizieren. PICSEL ist bereits im Einsatz und wird durch das Kompetenzzentrum Polizei-Technik und -Informatik (PTI) weiterentwickelt. Es sind aber noch nicht alle Kantone daran beteiligt. Grund dafür ist eine fehlende gemeinsame und einheitliche Rechtsgrundlage, die es PICSEL erlauben würde, in der gesamten Schweiz Anwendung zu finden. Es muss geklärt werden, wie eine Rechtsgrundlage für eine Plattform für den Informationsaustausch geschaffen werden kann. NEDIK erstellt monatlich eine Übersicht über das aktuelle Geschehen im Bereich der Cybersicherheit, und die Meldestelle des NCSC veröffentlicht wöchentlich die Fallzahlen der gemeldeten Vorfälle, aufgeschlüsselt nach Phänomenen. In der polizeilichen Kriminalstatistik werden zudem jährlich die Fallzahlen nach Phänomen aufgelistet. Der Austausch und die Aufbereitung der Fallstatistiken finden aber noch nicht umfassend und strategisch gesteuert statt, weshalb noch keine nationale Gesamtschau besteht.
Schwerpunkte	- Lagebild zu Cybervorfällen, gegliedert nach Ereignissen: Die nationale Anlaufstelle des NCSC erfasst die eingegangenen Vorfälle. Sie tauscht sich mit den Anlaufstellen der Polizeibehörden aus. - Die rechtlichen Rahmenbedingungen für den Informationsaustausch zwischen der Anlaufstelle und den Strafverfolgungsbehörden sind zu klären. - Fallübersicht zu den eingegangenen Anzeigen und zu laufenden polizeilichen und justiziellen Verfahren: Es werden rechtliche und technische Voraussetzungen geschaffen, damit eine zentrale Erfassung der eingegangenen Strafanzeigen zu Cybervorfällen und zu den laufenden Verfahren möglich wird.
Zentrale Akteure	- Bund: *BA, fedpol,* NCSC - Kantone: Kantonale Polizeikorps und Staatsanwaltschaften, KKJPD, NEDIK, SSK, PTI

M14 Ausbildung der Strafverfolgungsbehörden

Übersicht Massnahme	
Beschreibung	Die Cyberkriminalität umfasst sehr unterschiedliche Delikte, welche mit ständig wechselnden Methoden verübt werden und welche oft nicht einfach ab- und eingrenzbar sind. Dies macht den Umgang mit Cyberdelikten für Strafverfolgungsbehörden anspruchsvoll. Es muss auf allen Stufen der Strafverfolgung sichergestellt sein, dass das für die jeweiligen Aufgaben nötige Wissen über Cyberkriminalität vorhanden ist.
Ausgangslage und Handlungsbedarf	Die Grundausbildung zur Cyberkriminalität findet in den Polizeischulen und am Schweizerischen Polizei-Institut (SPI) statt. In der Westschweiz besteht zusätzlich das Angebot der «Ecole romande de la magistrature pénale (ERMP)» des «Institut de lutte contre la criminalité économique (ILCE)». Neben diesen spezifischen Ausbildungen sind auch zahlreiche Ausbildungsangebote der Universitäten und Fachhochschulen für Mitarbeitende der Strafverfolgungsbehörden relevant. Auch für Staatsanwältinnen und -anwälte, Richterinnen und Richter sowie Gerichtsschreiberinnen und -schreiber bestehen bereits Ausbildungsangebote. Im Auftrag der Konferenz der Kantonalen Polizeikommandanten der Schweiz (KKPKS) wurde mit cyberpie.ch eine Übersichtsplattform zu den relevanten Ausbildungsmöglichkeiten geschaffen. Zudem organisiert NEDIK jährlich mehrere Ausbildungen für Spezialistinnen und Spezialisten nach aktuellen Bedürfnissen und stellt mit CyberWiki eine nationale Wissensplattform zur Verfügung. Die SKP stellt den Kantonspolizeien fallspezifische Broschüren zur Verfügung mit Informationen zu den einzelnen Phänomenen und stärkt so die Ausbildung der Polizeimitarbeitenden. Aufbauend auf diesen vorhandenen Möglichkeiten, gilt es, die Ausbildung der Justiz- und Strafverfolgungsbehörden weiter zu fördern. Zusätzlich ist der Erfahrungsaustausch zwischen Strafverfolgungsbehörden, aber auch jener zwischen diesen Strafverfolgungsbehörden und der Privatwirtschaft weiter zu stärken, weil auch dadurch sehr viel Wissen vermittelt werden kann. Das Schweizerische Polizei-Institut sollte hierzu eine zentrale Rolle in der Koordination übernehmen können.
Schwer-punkte	- Weiterentwicklung der Ausbildungsangebote: Es wird laufend geprüft, ob die vorhandenen Angebote den Bedürfnissen entsprechen. Bei zusätzlichem Bedarf wird geklärt, wie neue Angebote geschaffen werden können. - Erfahrungsaustausch: über Praktika, Expertenpools oder Onlineplattformen wird der Wissensaustausch zwischen Strafverfolgungsbehörden gefördert.
Zentrale Akteure	- Bund: *BA, fedpol,* NCSC - Kantone: Kantonale Polizeikorps, KKPKS, NEDIK, Staatsanwaltschaften, SSK, SPI, ASR-SVM - Wirtschaft / Gesellschaft: SPI, Hochschulen

3.5 Massnahmen für das Ziel «Führende Rolle in der internationalen Zusammenarbeit»

Cybersicherheit ist ein wichtiges Thema der Aussenpolitik. Cyberangriffe werden von staatlichen Akteuren zunehmend zur Machtprojektion und für die Erreichung politischer Ziele, nachrichtendienstliche Vorhaben sowie militärische Zwecke genutzt. Zusätzlich zum Einsatz von Cybermitteln in konventionellen, bewaffneten Konflikten werden Auseinandersetzungen vermehrt auch im digitalen Raum von staatlichen und nicht-staatlichen Akteuren ausgetragen. Entsprechend ist die internationale Zusammenarbeit sowohl auf diplomatischer als auch auf technisch-operativer Ebene und im Bereich der koordinierten Aus- und Weiterbildung zur Reduktion von Cyberrisiken unabdingbar.
Die Wahrung der aussen- und sicherheitspolitischen Interessen der Schweiz muss auch im Cyberraum sichergestellt werden. Die Schweiz engagiert sich daher sowohl auf diplomatischer als auch auf technisch-operativer Ebene wie auch im Bereich der Aus- und Weiterbildung für die Stärkung der internationalen Kooperation zur Minimierung von Cyberrisiken.

M15 Stärkung des digitalen internationalen Genfs

Übersicht Massnahme	
Beschreibung	Der Bundesrat hat sich zum Ziel gesetzt, die Schweiz und namentlich das internationale Genf als führenden Standort der Digitalisierungs- und Technologiedebatten zu positionieren. Dazu gehört, dass die Schweiz den hier ansässigen internationalen Organisationen und internationalen Nichtregierungsorganisationen möglichst gute Rahmenbedingungen bieten kann. Da viele dieser Organisationen politisch exponiert sind, werden sie häufig Ziel von Cyberangriffen. Die Schweiz muss daher prüfen, wie sie die Rahmenbedingungen dafür verbessern kann, damit sich diese Organisationen vor Cyberdrohungen schützen können.
Ausgangslage und Handlungsbedarf	Die Organisationen des internationalen Genfs sehen sich zunehmend mit Bedrohungen im digitalen Raum konfrontiert. Will die Schweiz ein attraktiver Standort für internationale Organisationen und Nichtregierungsorganisationen bleiben, muss geprüft werden, wie für diese auch im digitalen Raum gute Rahmenbedingungen geschaffen werden können. Weiter sollen in der Schweiz ansässige internationale Organisationen und NGOs bei der Prävention unterstützt werden. Der Bund beteiligt sich mit der Bereitstellung von Fachwissen am Aufbau eines «Information Sharing and Analysis Centre» (ISAC) für solche Organisationen. Er trägt dadurch zum gegenseitigen Erfahrungsaustausch zwischen diesen Organisationen bei und nimmt daran teil.
Schwerpunkte	- Aufbau eines ISACs für das internationale Genf: Der Informations- und Erfahrungsaustausch zwischen internationalen Organisationen wird über den Aufbau eines ISACs gefördert. - Es sollen attraktive Rahmenbedingungen für digitale Dienstleistungen zuhanden internationaler Organisation und NGOs geprüft und geschaffen werden.
Zentrale Akteure	- Bund: *EDA,* BAKOM, GS-VBS NCSC, NDB - Wirtschaft / Gesellschaft: internationale Organisationen, NGO

M16 Internationale Regeln im Cyberraum

Übersicht Massnahme	
Beschreibung	Die Schweiz engagiert sich aktiv für ein offenes, freies und sicheres Internet. Sie setzt sich ein für die umfassende Anerkennung, Einhaltung und Durchsetzung des Völkerrechts im digitalen Raum und klärt die konkrete Anwendung der bestehenden Regeln im Austausch mit anderen Staaten. Sie hilft zudem mit, Rahmenbedingungen zu schaffen, welche die internationale Bekämpfung von Cyberkriminalität erleichtern. Die Schweiz verfolgt diese Ziele sowohl in internationalen Gremien, wie der UNO, OSZE oder OECD, in internationalen Fachgremien sowie auf bilateraler Ebene.
Ausgangslage und Handlungsbedarf	Seit 2004 verhandelt die Staatengemeinschaft im Rahmen von UNO-Arbeitsgruppen über die Anwendung des Völkerrechts im Cyberraum. Die Schweiz ist seit Beginn an diesen Diskussionen beteiligt und setzt sich mit gleichgesinnten Staaten für ein offenes, freies und sicheres Internet und die umfassende Anerkennung, Einhaltung und Durchsetzung des Völkerrechts ein. Die Schweiz befürwortet dabei einen inklusiven Multi-Stakeholder-Ansatz. Auf einer konkreteren Ebene sind die Herausforderungen bei der Bekämpfung von Internetkriminalität grösser geworden. Hier besteht ein Bedarf zur besseren internationalen Zusammenarbeit von Strafverfolgungsbehörden. Als besondere Herausforderung zeichnet sich Cloud-Computing ab, bei dem Daten vermehrt auf fremdem Territorium von Unternehmen aus Drittstaaten bearbeitet werden. Hier will die Schweiz mit bilateralen Abkommen mehr Rechtssicherheit schaffen.
Schwerpunkte	- Aktive Teilnahme an UNO-Prozessen: Die Schweiz beteiligt sich an den relevanten Prozessen, insbesondere der Open Ended Working Group (OEWG), und den Verhandlungen zu einer UNO Cybercrime-Konvention. - Aktive Beteiligung der Schweiz an der Weiterentwicklung und der Umsetzung des Übereinkommens über die Cyberkriminalität («Budapest Konvention») des Europarats. - Aktive Teilnahme bei der Umsetzung der vertrauensbildenden Massnahmen der OSZE. - Die Schweiz führt bilaterale Gespräche zur Thematisierung zwischenstaatlicher Fragestellungen und Anliegen und schliesst Abkommen mit strategisch wichtigen Partnern.
Zentrale Akteure	- Bund: *EDA,* Armee, BAV, BAKOM, BAZL, BFE, BJ, GS-VBS, NCSC

M17 Bilaterale Zusammenarbeit zu strategischen Partnern und internationalen Kompetenzzentren

Übersicht Massnahme	
Beschreibung	Die Schweiz ergreift Massnahmen, um die operative Zusammenarbeit mit internationalen Partnern zu stärken, zu koordinieren und gezielt auszubauen. In Anbetracht der internationalen Dimension der Cybersicherheit ist eine gezielte Zusammenarbeit mit internationalen Partnern, Kompetenzzentren und führenden Fachorganisationen mitentscheidend für die erfolgreiche Umsetzung aller Massnahmen zum Schutz vor Cyberbedrohungen.
Ausgangslage und Handlungsbedarf	Die Schweiz ist in einem globalen Internet auf die Zusammenarbeit mit anderen Staaten angewiesen. Erfahrungsgemäss sind solche Aktivitäten nur nachhaltig, wenn sie breit und auf gemeinsamen Interessen abgestützt sind. Im Rahmen verschiedener Aktivitäten pflegt die Schweiz bilaterale Beziehungen zu strategischen Partnern. Besonders wichtig ist die internationale Zusammenarbeit bei der Strafverfolgung. Ohne gegenseitige Unterstützung zwischen verschiedenen Staaten können die global agierenden Täter nicht effektiv verfolgt werden. Die Schweiz tauscht sich deshalb auf operativer und strategischer Ebene in den entsprechenden Fachgremien aber auch direkt mit anderen Staaten zu diesen Themen aus. Neben der staatlichen Zusammenarbeit ist auch die Kooperation mit privaten internationalen Initiativen und technischen Kompetenzzentren für Cybersicherheit sehr wichtig. Eine solche Zusammenarbeit auf hohem Vertrauensniveau kann einen relevanten Beitrag zu einem besseren Verständnis der relevanten Bedrohungslage und deren Entwicklung und zum effektiveren Schutz von Gesellschaft, Wirtschaft und Verwaltung leisten. Dazu braucht es langjährige Zusammenarbeit auf höchstem Vertrauensniveau und einen gezielten Auf- und Ausbau der internationalen Beziehungsnetze relevanter Akteure in der Schweiz.
Schwerpunkte	- Die bestehenden Cyberdialoge mit Partnerstaaten werden weitergeführt und Cyberdialoge mit weiteren Staaten werden angestrebt. - Die Schweiz prüft im Austausch mit Partnerstaaten, wie die Rahmenbedingungen der Strafverfolgung der Cyberkriminalität über bilaterale Staatsverträge verbessert werden können. - Die Schweiz engagiert sich gemeinsam mit ausländischen Partnern in operativen Programmen, wie beispielsweise der CounterRansomware-Initiative. - Es werden bilaterale Abkommen zur gegenseitigen Unterstützung bei der Bekämpfung von Cyberkriminalität angestrebt. - Falls sich die Möglichkeit ergibt, wird eine Zusammenarbeit mit dem Europäischen Kompetenzzentrums für Cybersicherheit (ECCC) angestrebt. - Aktive Mitwirkung in relevanten Organisationen, welche diese technisch-operative Zusammenarbeit ermöglichen und fördern wie z. B. FIRST, TF-CSIRT, NatCSIRT (nationale CERT). - Ausbau der Zusammenarbeit in internationalen Arbeitsgruppen zu technischen Fragestellungen (z. B. OT-Security, Phishing, usw.).
Zentrale Akteure	- Bund: *EDA,* BAV, BAKOM, BAZL, BFE, fedpol, GS-VBS, NCSC, NDB - Wirtschaft / Gesellschaft: Fachverbände, CERTs, Sicherheitsdienstleister

4 Umsetzung der Strategie

Die Umsetzung der Strategie wird durch den Steuerungsausschuss der NCS koordiniert. Dieser verantwortet die Erstellung eines Umsetzungsplans. Die Planung wird in direkter Absprache mit den zentralen Akteuren der einzelnen Massnahmen erstellt. Diese sind die Ansprechstellen des Ausschusses für die Umsetzung der betreffenden Massnahmen und legen ihm dar, welchen Beitrag sie bis wann leisten können. Sie erteilen ihm zudem Auskunft über den Stand der Aktivitäten. Können sie ihnen zugeteilte Massnahmen nicht umsetzen, ist dies auszuweisen. Der Steuerungsausschuss beurteilt dann die Konsequenzen, welche sich daraus für die Ziele der Strategie ergeben und informiert nötigenfalls über seine Geschäftsstelle, welche durch das NCSC gestellt wird, den Bundesrat und die Kantone über diese Auswirkungen.
Die Finanzierung der Umsetzungsarbeiten erfolgt grundsätzlich durch die zentralen Akteure selbst. Die Akteure des Bundes setzen dafür die Ressourcen ein, welche ihnen zur Umsetzung der ersten beiden Cyberstrategien zugesprochen wurden. Die Kantone und die Organisationen der Wirtschaft und der Gesellschaft weisen gegenüber dem Steuerungsausschuss aus, welche Beiträge zur Umsetzung der Massnahmen sie mit eigenen Mitteln umsetzen können. Das NCSC unterstützt die zentralen Akteure bei der Umsetzung. Es stellt dazu einen Expertenpool zur Verfügung. Zentrale Akteure der Bundesverwaltung können für die Umsetzung der NCS beim NCSC Unterstützung durch den Expertenpool beantragen.
Übersteigt der Ressourcenbedarf einer Massnahme die vorhandenen Mittel der beteiligten Akteure und lässt sich dieser Bedarf nicht anderweitig decken, ist dies ebenfalls gegenüber dem Steuerungsausschuss auszuweisen.
Die Überprüfung der Umsetzung verantwortet der Steuerungsausschuss. Als dessen operative Geschäftsstelle erhebt und dokumentiert das NCSC regelmässig den Umsetzungsstand bei allen Massnahmen.
Nach fünf Jahren werden die Strategie selbst und ihre Umsetzung geprüft. Auf der Basis der Ergebnisse dieser Überprüfung entscheidet der Steuerungsausschuss, ob er bei den Kantonen und beim Bund eine vollständige Überarbeitung der Strategie beantragt oder einzelne Ergänzungen und Änderungen vornimmt, um die Strategie weiterzuführen.

5 Abkürzungsverzeichnis

BA	Bundesanwaltschaft
BABS	Bundesamt für Bevölkerungsschutz
BFE	Bundesamt für Energie
BAKOM	Bundesamt für Kommunikation
BAV	Bundesamt für Verkehr
BJ	Bundesamt für Justiz
BWL	Bundesamt für wirtschaftliche Landesversorgung
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CYD Campus	Cyberdefence Campus der armasuisse (Wissenschaft und Technologie)
DTI	Bereich Digitale Transformation und IKT-Lenkung der Bundeskanzlei
DVS	Digitale Verwaltung Schweiz
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDK	Konferenz der kantonalen Erziehungsdirektorinnen und -direktoren
EDÖB	Eidgenössischer Daten
EFD	Eidgenössisches Finanzdepartement
EU	Europäische Union
EUROPOL	Europäische Polizeiamt
Fedpol	Bundesamt für Polizei
GK Cyber	Gesamtkonzeption Cyber
IKT	Informations- und Kommunikationstechnologien
IoT	Internet of Things
ISG	Informationssicherheitsgesetz
IT	Informationstechnologien
Kdo Cyber	Kommando Cyber
KKJPD	Konferenz der Kantonalen Justiz und Polizeidirektoren und –direktorinnen
KKPKS	Konferenz der kantonalen Polizeikommandanten der Schweiz
KMU	Kleine- und Mittlere Unternehmen
MG	Militärgesetz
NCS	Nationale Cyberstrategie
NCSC	Nationales Zentrum für Cybersicherheit
NDB	Nachrichtendienst des Bundes
NDG	Nachrichtendienstgesetz
NEDIK	Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung
NTC	Nationales Testzentrum für Cybersicherheit
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OEWG	Open Ended Working Group
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
PTI	Polizeitechnik und -informatik Schweiz
SATW	Schweizerische Akademie der Technischen Wissenschaften
SBFI	Staatsekretariat für Bildung Forschung und Innovation
SOC	Security Operations Centers
SHK	Schweizerische Hochschulkonferenz
SKP	Schweizerische Kriminalprävention
SSCC	Swiss Support Center for Cybersecurity
SVS	Sicherheitsverbund Schweiz
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport

6 Glossar

Cyberangriff	Cybervorfall, der absichtlich ausgelöst wurde.
Cyberkriminalität	Cyberkriminalität umfasst die Gesamtheit aller strafbaren Handlungen und Unterlassungen im Cyberraum. Unterschieden wird zwischen «Cybercrime» und «digitalisierter Kriminalität». «Cybercrime» bezeichnet Straftaten die sich gegen das Internet, informationstechnische Systeme oder deren Daten richten und technische Ermittlungsarbeit auf Seiten der Strafverfolgungsbehörden erfordern. «Digitalisierte Kriminalität» bezeichnet Straftaten, die bisher überwiegend in der analogen Welt begangen worden sind. Aufgrund der zunehmenden Digitalisierung, werden diese klassischen Delikte vermehrt mit Hilfe von Informationstechnik verübt.
Cyberraum	Gesamtheit der Informations- und Kommunikationsinfrastrukturen (Hard- und Software), die untereinander Daten austauschen, diese erfassen, speichern, verarbeiten oder in (physische) Aktionen umwandeln, und der dadurch ermöglichten Interaktionen zwischen Personen, Organisationen und Staaten.
Cybersabotage	Tätigkeit, um im Cyberraum das zuverlässige und fehlerfreie Funktionieren von Informations- und Kommunikationsinfrastrukturen zu stören oder zu zerstören; dies kann je nach Art der Sabotage auch zu physischen Auswirkungen führen.
Cyberspionage	Tätigkeit, um im Cyberraum für politische, militärische oder wirtschaftliche Zwecke unerlaubt an geschützte Informationen zu gelangen.
Cybervorfall	Ereignis bei der Nutzung von Informatikmitteln, das dazu führt, dass die Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist.
Kritische Infrastrukturen	Prozesse, Systeme und Einrichtungen, die essenziell für das Funktionieren der Wirtschaft bzw. das Wohlergehen der Bevölkerung sind.
Resilienz	Die Fähigkeit eines Systems, einer Organisation oder einer Gesellschaft, intern oder extern verursachten Störungen zu widerstehen und das ordnungsgemässe Funktionieren zu erhalten oder dieses möglichst rasch und vollständig wiederzuerlangen.
Cybersicherheit	Anzustrebender Zustand, bei dem die Datenbearbeitung, insbesondere der Datenaustausch zwischen Personen und Organisationen, über Informations- und Kommunikationsinfrastrukturen wie beabsichtigt funktioniert.
Informations-sicherheit	Informationssicherheit ist die Unversehrtheit der Authentizität, Vertraulichkeit, Integrität und Verfügbarkeit eines informations- und kommunikationstechnischen Systems und der darin verarbeiteten und gespeicherten Daten.
Cyberbedrohung	Jeder Umstand oder jedes Ereignis mit dem Potenzial, einen Cybervorfall zu ermöglichen.