EBP

econcept
Forschung / Beratung / Evaluation

National Cyber Security Centre, NCSC

Wirksamkeitsüberprüfung «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018 bis 2022»

Schlussbericht
28. März 2022

Erarbeitet durch
econcept AG, Gerechtigkeitsgasse 20, CH-8002 Zürich
www.econcept.ch / + 41 44 286 75 75

EBP Schweiz AG, Mühlebachstrasse 11, 8032 Zürich
www.ebp.ch / +41 44 395 16 16

Autoren/innen
Benjamin Buser, Dr. sc. ETH, dipl. Geogr., Executive MBA HSG
Jasmin Gisiger, MA ETH UZH in Comparative and International Studies
Christof Egli, Dipl. Ing. ETH Zürich, CAS Datenschutz und Informationssicherheit

Inhalt

Abkürzungsverzeichnis

Abkürzung	Bedeutung
BABS	Bundesamt für Bevölkerungsschutz
BAKOM	Bundesamt für Kommunikation
BWL	Bundesamt für wirtschaftliche Landesversorgung
CYD	Cyber-Defence Campus
CyRV	Cyberrisikenverordnung
DTI	Digitale Transformation des Bundes
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDI	Eidgenössisches Departement des Inneren
EFD	Eidgenössischen Finanzdepartement
EPFL	Ecole Polytechnique Federal Lausanne
ETH Zürich	Eidgenössische Technische Hochschule Zürich
IKT-Lenkung	Lenkung der Informations- und Kommunikationstechnologie beim Bund -> wurde überführt in die Digitale Transformation DTI (siehe oben)
ISB	Informatiksteuerorgans des Bundes
IT	Informationstechnologie
KMU	Kleine und mittlere Unternehmen
MELANI	Melde- und Analysestelle Informationssicherung -> wurde überführt in das Nationale Zentrum für Cybersicherheit NCSC (siehe unten)
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
NCSC	Nationales Zentrum für Cybersicherheit
NDB	Nachrichtendienst des Bundes
NEDIK	Netzwerk digitale Ermittlungsunterstützung Internetkriminalität
NTC	Nationales Testinstitut für Cyber-Sicherheit
OECD	Organisation for Economic Co-operation and Development
SR	Systematische Rechtssammlung des Bundes
SDVN	Sicheres Datenverbundnetz
SSCC	Swiss Support Center for Cyber-Security
StA	Steuerungsausschuss
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
VBS	Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport

Zusammenfassung

Auftrag zur Wirksamkeitsüberprüfung

Die digitale Transformation der Schweiz bietet für Staat, Politik, Gesellschaft und Wirtschaft sowohl Chancen als auch Risiken. Mit der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) adressiert der Bundesrat seit 2012 entsprechende Bedrohungen. Mit der zweiten Umsetzungsperiode der NCS zwischen 2018 bis 2022 hat der Bundesrat auf erweiterte Bedrohungslagen reagiert und zusätzliche Massnahmen ergriffen, die sich an vier Zielgruppen richten. Der Bundesrat gibt darin sieben strategische Zielsetzungen vor, die sich an den Fähigkeiten zur Vor- und Nachsorge von Cyber-Vorfällen und der Zusammenarbeit staatlicher, ziviler und militärischer Akteure/innen ausrichten. Die Umsetzung erfolgt mittels zehn Handlungsfeldern und einem Umsetzungsplan, der Massnahmen mit konkreten Umsetzungsvorhaben festlegt.

Der Bundesrat hat das Nationale Zentrum für Cybersicherheit (NCSC) im Hinblick auf eine geplante Weiterentwicklung der NCS mit einer Wirksamkeitsüberprüfung der Strategie beauftragt. Die extern durchgeführte Wirksamkeitsüberprüfung beantwortet vier Fragen:

Gesamtbetrachtung / Zielerreichung: Erreicht die NCS 2018-2022 die strategischen Ziele?

Effizienz / Ressourcen: In welchem Verhältnis steht der Mitteleinsatz zu den erbrachten Leistungen?

Effektivität / Wirkungen: Inwiefern konnten die beabsichtigten Wirkungen erzielt werden?

Weiterentwicklung / Empfehlungen: Welche Empfehlungen lassen sich im Hinblick auf die Überarbeitung der Strategie für den zukünftigen Ressourceneinsatz ableiten?

Die Wirksamkeitsüberprüfung der NCS richtet sich an einem Wirkungsmodell aus, das Incomes, Input, Implementation, Output, Outcome und Impact beschreibt.

Zweckmässigkeit und Angemessenheit der NCS 2018-2022

Die Wirksamkeit der NCS hängt ab von der Konzeption, der Ausrichtung auf die Herausforderungen und der konkreten Umsetzung. Die Einschätzungen zur Konzeption der NCS beleuchten die Wirkungsebenen von Incomes (nationaler und internationaler Kontext), Inputs (Grundlagen, Ziele und Ressourcen) und Implementation (Strukturen und Prozesse) und lassen sich in sieben Aussagen zusammenfassen:

— Die NCS basiert bezüglich **Cyber-Bedrohung und Herausforderungen** auf aktuellen Grundlagen und ist auf die zentralen Herausforderungen und Entwicklungen zur Erhöhung der nationalen Cyber-Sicherheit ausgerichtet.

— Die **rechtlichen und strategischen Grundlagen** sind in der NCS inhaltlich adäquat berücksichtigt. Verbesserungspotenzial besteht bei der Abstimmung der NCS mit anderen Digitalisierungs- und Schutzstrategien des Bundes.

— Mit den **verfügbaren Ressourcen** nehmen die umsetzungsverantwortlichen Stellen ihren Kernaufgaben wahr. Die Effizienz des Mitteleinsatzes kann durch Anpassungen in der Zusammenarbeit zwischen den beteiligten Stellten erhöht werden. Zudem besteht ein zusätzlicher Bedarf nach personellen Kapazitäten zur NCS-Umsetzung.

— Die Netzwerkstruktur ist geeignet für die Umsetzung der NCS, in der Umsetzung müssen die Synergiepotenziale aus dem Netzwerk noch besser genutzt werden. Dies betrifft auch die Verbindung mit übergeordneten und verwandten Strategien. Die weiterentwickelte NCS-**Governance** unterstützt hierbei die **Zusammenarbeit**.

— Die Grundlagen, der erkannte Handlungsbedarf und die Herausforderungen sind angemessen in die **strategischen Ziele** der NCS eingeflossen. Teilweise kritisch einzuschätzen sind der Fokus auf die Bundesverwaltung und der fehlende Blick auf mögliche Chancen für ein «Cyber-Ökosystem» in der Schweiz.

— Mit den **vier Zielgruppen** richtet sich die NCS an ein breites Feld von Akteuren/innen. Innerhalb der Zielgruppen adressiert die NCS die verschiedenen Akteursgruppen unterschiedlich stark.

— **Handlungsfelder und Massnahmen** fügen sich gut in die Strategie ein. Der Umsetzungsplan ist ein geeignetes Schlüsselwerkzeug und die Handlungsfelder und Massnahmen decken die Herausforderungen in der erforderlichen Breite ab.

Leistungen und Wirkungen der Handlungsfelder

Die NCS soll ihre Wirkung durch die den zehn Handlungsfeldern zugewiesenen Massnahmen und Umsetzungsvorhaben erreichen. In der Wirksamkeitsüberprüfung werden die Handlungsfelder und Massnahmen bezüglich ihrer erzielten Leistungen (Outputs) und der angestrebten Wirkungen (Outcomes) beurteilt. Zu den Handlungsfeldern war es möglich, folgende Schlussfolgerungen zu ziehen.

— Mit der mehrheitlichen Realisierung der Umsetzungsvorhaben im Handlungsfeld **Kompetenzen- und Wissensaufbau** wurden die wesentlichen Leistungen erbracht; die gewünschten Strukturen wurden geschaffen und das Wissensnetzwerk wurde geknüpft. Outcomes werden erzielt, der Impact zeigt sich in den anderen Handlungsfeldern.

— Die realisierten Umsetzungsprojekte schafften im Handlungsfeld **Bedrohungslage** mit ihrem Outcome eine gute Basis, von der ausgehend die zuständigen Stellen Wirkung erzielen können. In der inhaltlichen Auswertung der Bedrohungslage sind weitere Fortschritte erwünscht. Als Herausforderung wird die angespannte Situation bezüglich verfügbarer Experten/innen betrachtet.

— Im Handlungsfeld **Resilienz-Management** wurden die Massnahmen, um die IKT-Resilienz kritischer Infrastrukturen und der Bundesverwaltung zu verbessern, deutlich

weiterentwickelt. Der Output wird als hoch eingestuft, das Problembewusstsein ist geschärft, aber die Wirkung auf die Zielgruppe fällt noch nicht zufriedenstellend aus.

— Zur Standardisierung wurden im Handlungsfeld **Standardisierung/Regulierung** Grundlagen erstellt, die aufgrund bislang geringer Verbreitung und hoher Freiwilligkeit zu wenig Anwendung finden. Durch die bearbeiteten Regulierungsvorhaben entstehen Rahmenbedingungen, welche die Verbreitung der Grundlagen begünstigten. Outcome und Impact werden aktuell als stark eingeschränkt beurteilt. Es bestehen jedoch gute Voraussetzungen zur künftigen Erhöhung der Wirkung.

— Im Handlungsfeld **Vorfallbewältigung** stärken die ausgebauten Fähigkeiten, Abläufe und Kapazitäten zur Vorfallbewältigung die Resilienz bei den Zielgruppen in unterschiedlichem Mass. Eine präventive Wirkung kann nicht festgestellt werden.

— Die Reaktions- und Interventionsfähigkeiten der Bundesverwaltung wurden im Handlungsfeld **Krisenmanagement** gestärkt, die durchgehende Handlungsfähigkeit von Behörden und Verwaltung durch Regelung von Verantwortlichkeiten und Trainings besser gesichert. Rasch intervenieren zu können bleibt eine komplexe Aufgabe.

— Im Handlungsfeld **Strafverfolgung** wird die Cyber-Strafverfolgung mit der Koordination und Stärkung der interkantonalen Zusammenarbeit effizienter und effektiver ausgestaltet. Technische, rechtliche, prozessuale und andere Unterschiede zwischen den föderal organisierten Strafverfolgungsbehörden und begrenzte personelle Kapazitäten hemmen derzeit mögliche Outcomes und Wirkungen. Die Massnahmen zur Kapazitätserhöhung befinden sich in der Umsetzung.

— Mit den realisierten Umsetzungsvorhaben wurden im Handlungsfeld **Cyber-Defence** die Fähigkeiten der Armee und des Nachrichtendienstes des Bundes sowie ihre Einsatzbereitschaft im Cyber-Raum klar gestärkt. Die «Strategie Cyber VBS» stärkt das Handlungsfeld zusätzlich mit weiteren Massnahmen. Ausstehend ist die Ausdehnung des Ausbildungsangebots zugunsten Dritter. Damit soll die Interoperabilität innerhalb bzw. die Wirkung im Sicherheitsverbund Schweiz gestärkt werden.

— Dem Handlungsfeld **Cyber-Aussen und -Sicherheitspolitik** fällt eine indirekte Wirkung zum Schutz der Zielgruppen zu. Schweizer Behörden und weitere zentrale Akteure/innen (bspw. im Rahmen des «Geneva Dialogue») wurden international in den Diskussionen zur Cyber-Governance positioniert.

— Die Aussenwirkung wurde durch verstärkte Kommunikation deutlich verbessert. Vor allem grosse sowie international operierende Unternehmen und Betreiber kritischer Infrastrukturen nehmen dies wahr. Bevölkerung und KMU werden durch das Handlungsfeld **Aussenwirkungen und Sensibilisierung** häufig noch zu wenig gut erreicht. Auch bei der Koordination der Kommunikationsaktivitäten der verschiedenen Akteure/innen besteht Handlungsbedarf. Der Impact entsteht indirekt.

Wirkungen auf die Zielgruppen

Die NCS hat den Anspruch, die Resilienz der vier Zielgruppen Verwaltung und Behörden, Betreiber kritischer Infrastrukturen, Bevölkerung sowie Wirtschaft gegenüber Cyber-Bedrohungen zu erhöhen, um deren Handlungsfähigkeit und Integrität zu gewährleisten. In der Wirksamkeitsüberprüfung wurde untersucht, inwiefern die NCS in diesen Zielgruppen Wirkung erzielt.

- Die Umsetzung der Strategie ist gut in der **Verwaltung und den Behörden** verankert. Handlungsfelder und Massnahmen bilden ein stimmiges Paket, da sich die Gliederung der Strategie und die vorgeschlagenen Massnahmen stark an der Verwaltungsstruktur orientieren. Die NCS führt zu einer verbesserten Zusammenarbeit zwischen Bund und Kantonen.
- Die Betreiber/innen **kritischer Infrastrukturen** sind gut sensibilisiert und eng in die Massnahmen bzw. Umsetzungsvorhaben eingebunden. Innerhalb der Branchen mit grossen Akteuren/innen ist ein enger Austausch und ein erhöhtes Engagement festzustellen. Bei kleinteilig strukturierten Branchen mit vielen unterschiedlichen Akteuren/innen hat dies bislang wenig stattgefunden, hier ist das Problembewusstsein weniger stark ausgeprägt. Die als Resultat der Strategie erbrachten Leistungen reichen derzeit nicht aus, um alle kritischen Infrastrukturbranchen angemessen zu schützen.
- Die Aufmerksamkeit der **Bevölkerung** für Sicherheit im Cyber-Raum ist in den vergangenen Jahren angestiegen; die NCS leistet bislang aber keine weitergehende Sensibilisierung und Cyber-Grundbildung der Bevölkerung. Die Massnahmen der NCS erreichen die Bevölkerung punktuell, die Breitenwirkung zur Sensibilisierung hinsichtlich Sicherheit im Cyber-Raum fehlt.
- In der Zielgruppe **Wirtschaft** schützen sich die grossen, internationalen Unternehmen angemessen gegen Cyber-Risiken. Die KMU hingegen verfügen über ein zu niedriges Bewusstsein für die Bedrohungen im Cyber-Raum und sind wenig geschützt. Mit der NCS gelingt es kaum, unternehmerische Aktivitäten hin zu einem verbesserten Schutz auszulösen.

Fazit zur Wirksamkeit der NCS

Bei der NCS 2018-2022 handelt es sich um eine kohärente Strategie. Ihr Umsetzungsplan unterstützt die strategischen Ziele. Die Umsetzung findet plangemäss statt und führt zu relevanten Outcomes, die grundsätzlich für die **strategische Zielerreichung** sorgen. Die Outcomes erreichen nicht alle Zielgruppen gleichermassen. Mit gezielten Eingriffen, wie etwa einer Wirkungsmessung und einer verstärkten strategischen Steuerung, können die Verantwortlichen die Effektivität der Umsetzung der NCS weiter erhöhen.

Die Verantwortlichen für die Umsetzung der NCS haben mit vorhandenen Ressourcen bislang ihren **Kernauftrag effizient erfüllt.** Die Ressourcenallokation könnte jedoch eine stärkere Ausrichtung an den Wirkungszielen erfahren. Zusätzliche personelle Ressourcen für die Restlaufzeit bis Ende 2022 sowie für verstetigte Aktivtäten erscheinen gerechtfertigt.

Durch die NCS lassen sich bislang insbesondere für kritische Infrastrukturen, nationale und kantonale Behörden und Institutionen sowie grosse Unternehmen Wirkungen erkennen. Ein empirischer Nachweis ist im Rahmen der noch laufenden NCS nicht möglich. Es liegen zudem klare Hinweise vor, dass die NCS KMU, Städte und Gemeinden sowie die Bevölkerung nicht im erforderlichen Umfang erreicht. Der Cyber-Schutz ist in diesen Zielgruppen noch nicht ausreichend.

Ausblick und Empfehlungen

Als Ergebnis der Wirksamkeitsüberprüfung sind Möglichkeiten zu nennen, wie sich die Ausgestaltung der NCS verbessern liesse, um Effizienz und Effektivität hin zu einem bestmöglichen Impact zu erhöhen.

— Die Vorteile eines **partizipativen Erarbeitungsprozesses** sind in der Weiterentwicklung der NCS für die Aktivitäten nach 2022 gezielt zu nutzen. Ein hierzu straff geführter und effizienter Prozess motiviert die verschiedenen Wissensträger/innen zur Mitarbeit.

— Die **Governance** der NCS soll gestärkt werden, indem der Steuerungsausschuss verkleinert wird, damit er seine Möglichkeiten zur strategischen Steuerung erhöhen kann. Zudem sind weitere Vernetzungsmöglichkeiten zu fördern. Es ist eine stärkere Einbindung von KMU und kommunaler Ebene in die Governance der NCS zu prüfen.

— Die **strategischen Ziele** sind auf allen Strategieebenen, inklusive in den Umsetzungsvorhaben, möglichst konkret und unabhängig zu formulieren, um eine bessere Fokussierung und wirksamere Bündelung von Aktivitäten und Ressourcen zu unterstützen. Eine mögliche Unterstützung hierzu liefert der SMART-Ansatz (spezifisch, messbar, akzeptiert, realistisch, terminiert).

— Die **Kommunikationsanstrengungen** sind zu verstärken, zu bündeln und zu koordinieren. Es ist zu prüfen, ob «Transfer und Kommunikation» als eine zusätzliche strategische Zielsetzung einzufügen ist.

— Die NCS entfaltet ihr Wirkung dann am besten, wenn die **Zielgruppen** passend adressiert und direkt in die Massnahmenplanung und -umsetzung eingebunden werden. Die Massnahmen der NCS sollen die Bedürfnisse der Zielgruppen möglichst direkt befriedigen. Zudem ist zu prüfen, ob die NCS gezielt «Brückenprojekte» über die drei Ebenen von Bund, Kantonen und Städte/Gemeinden hinweg schaffen soll.

— Der **Umsetzungsplan** hat sich als Schlüsselwerkzeug erwiesen, um rasch Aktivitäten aufnehmen und die strategischen Ziele verfolgen zu können. Die Ausgestaltung und die Abwicklung des Umsetzungsplans sollen mit zusätzlicher Flexibilität ausgestaltet werden, ggf. im Zusammenspiel mit zeitlich längeren Strategiezyklen. Zudem soll verstärkt auf eine Wirkungsmessung und das Controlling geachtet werden.

— Die **Massnahmen** weisen eine grosse Breite und Themenvielfalt auf. Hier ist eine andere Gliederung nach Art der Massnahme anzustreben («Sofortmassnahmen», «Best

Practices», «Regulierungsvorhaben», «Grundlagen-Querschnittsprojekte» und «Pilotprojekte»). Zudem sind die Themen «Supply-Chain-Risiken», «Bildung» und «Cyber-Ökosystem» zur Fokussierung von Chancen explizit aufzunehmen. Um die strategische Steuerung und Ressourcenallokation der NCS zu unterstützen, ist die Wirkungsmessung künftig in die Strategie- und Massnahmenplanung miteinzubeziehen.

— Die Kernaufträge aus der NCS sind mit den vorhandenen **Ressourcen** bislang zu erfüllen. Dennoch ergeben sich Ressourcenengpässe und es besteht der Wunsch nach gezielter personeller Verstärkung. Damit Ressourcen einfacher dort eingesetzt werden können, wo der Bedarf gross ist, sind die Planungs- und Budgetierungsprozesse kritisch zu hinterfragen. Zu prüfen ist etwa, ob Mittel oder Projektbudgets stärker durch die Kerngruppe Cyber oder den StA verwaltet werden sollten, damit Ressourcen einfacher zugeordnet werden können. Unbestritten bleibt der hohe Bedarf an weiteren Fachexperten/innen in allen Zielgruppen und auf allen Stufen. Der Pool an Fachexperten/innen ist durch gezielte Massnahmen in der Aus- und Weiterbildung zu vergrössern.

1 Auftrag zur Wirksamkeitsüberprüfung

1.1 Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018 bis 2022 (NCS 2018-2022)

Schutz im Cyber-Raum

Die digitale Transformation der Schweiz bietet für Staat, Politik, Gesellschaft und Wirtschaft sowohl Chancen als auch Risiken. Bereits heute werden Informations- und Kommunikationstechnologien und die weltweite digitale Vernetzung intensiv genutzt. Im Gleichschritt mit der Digitalisierung entwickeln sich die unrechtmässigen Aktivitäten im Cyber-Raum, welche die Integrität, Vertraulichkeit und Verfügbarkeit von IT-Systemen und Daten[1] gefährden. Wenn die Handlungsfähigkeit und Integrität von staatlichen und privaten Akteuren/innen gegenüber Cyber-Bedrohungen künftig gewährleistet werden sollen, sind gezielte Massnahmen zu deren Schutz zu ergreifen.

Strategie des Bundesrats

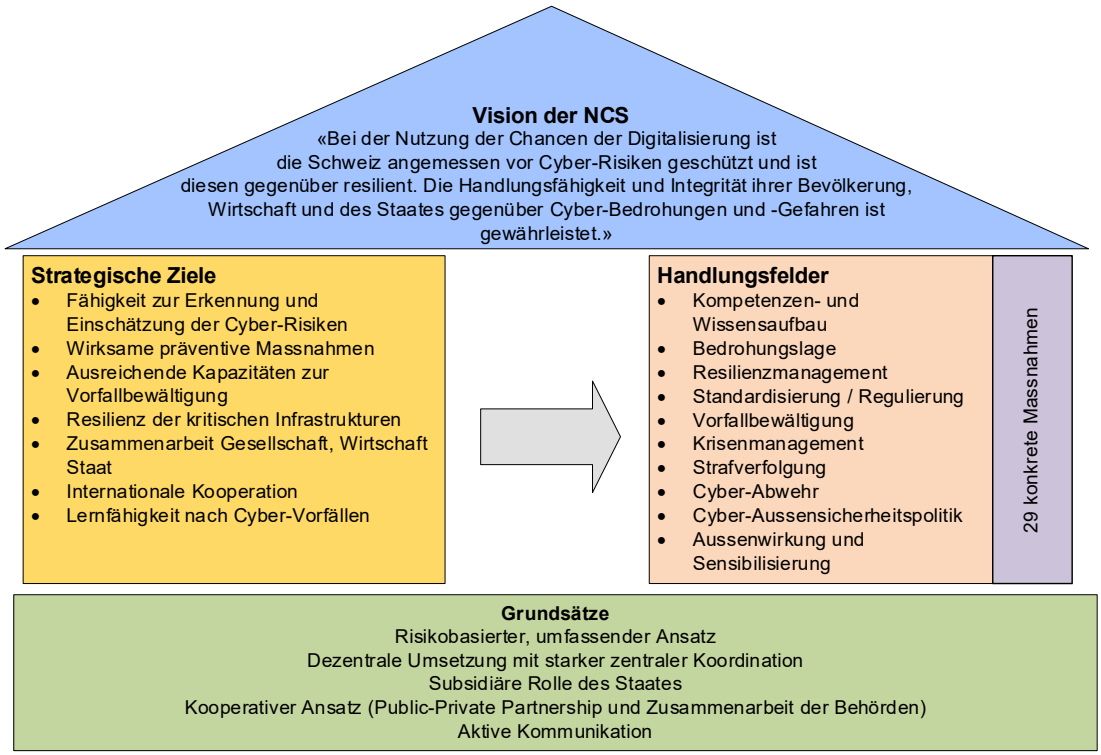
Mit der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken hat der Bundesrat entsprechende Bedrohungen adressiert (Bundesrat, 2018). In der laufenden, zweiten Umsetzungsperiode 2018 bis 2022 hat der Bundesrat auf erweiterte Bedrohungslagen reagiert und gegenüber der Vorperiode zusätzliche Massnahmen ergriffen.

Mit der NCS 2018-2022 wurde die Strategie auf Basis gemachter Erfahrungen und erreichter Massnahmenziele sowie unter Berücksichtigung aktueller und erwarteter Bedrohungslagen und Entwicklungen im Cyber-Raum neu verfasst. In den Strategieprozess wurden, unter Leitung der damaligen Melde- und Analysestelle Informationssicherung (MELANI) des Informatiksteuerorgans des Bundes (ISB), rund 50 staatliche und nicht-staatliche Organisationen miteinbezogen. Die Strategie wurde in einem mehrstufigen Prozess entwickelt und vom Bundesrat am 18. April 2018 beschlossen und in Kraft gesetzt. Der Bundesratsbeschluss sieht eine jährliche Berichterstattung zum Umsetzungsstand sowie eine Gesamtüberprüfung der Strategie bis Ende 2022 vor.

Die NCS 2018-2022 verfolgt die Vision, die Schweiz angemessen vor Cyber-Risiken zu schützen und die Resilienz der Schweiz gegenüber diesen Risiken zu erhöhen. Die Handlungsfähigkeit und Integrität der Bevölkerung, der Wirtschaft und des Staates gegenüber Cyber-Bedrohungen sollen jederzeit gewährleistet sein. Hierfür gibt der Bundesrat sieben strategische Ziele vor, die sich an den erforderlichen Fähigkeiten zur Vor- und Nachsorge von Cyber-Vorfällen und der erforderlichen Zusammenarbeit staatlicher, ziviler und militärischer Akteure/innen ausrichten (siehe Abbildung 1). Zahlreiche Bundesämter, die Kantone und die Wirtschaft sind in die Umsetzung der Strategie involviert.

[1] Sog. CIA-Triade: «Confidentiality», «Integrity» und «Availability».

Strategiehaus der NCS 2018 bis 2022



Quelle: Bundesrat, 2018

Abbildung 1: Aufbau und Inhalte der NCS 2018-2022

In einem Umsetzungsplan zur Strategie werden zu allen Massnahmen konkrete Umsetzungsvorhaben definiert. Der Umsetzungsplan dient als Arbeitsplan und legt Verantwortlichkeiten und Meilensteine fest. Er kann durch den Steuerungsausschuss der NCS mit weiteren Umsetzungsvorhaben ergänzt werden, was zwischen 2019 und 2021 mehrfach gemacht wurde. Anhang A-5 enthält eine Übersicht zu Handlungsfeldern mit ihren Massnahmen und den geplanten Umsetzungsvorhaben.

Zielgruppen

Mit ihren Massnahmen richtet sich die NCS 2018-2022 an verschiedene Zielgruppen. Diese sind in vier Gruppen gegliedert.

Zielgruppe	Beschreibung
Kritische Infrastrukturen	Diese stellt die Hauptzielgruppe der Massnahmen dar, mit dem Ziel, die Verfügbarkeit essenzieller Güter und Dienstleistungen jederzeit sicherzustellen.
Behörden	Die Behörden von Bund, Kantonen und Gemeinden sind zuständig für Dienstleistungen, die in ihren Eigenschaften und den Anforderungen an eine erhöhte Resilienz den kritischen Infrastrukturen gleichzustellen sind.
Bevölkerung	Die NCS bezweckt den Schutz der Bevölkerung, die direkt vor Cyber-Kriminalität zu schützen ist. Für die Bevölkerung soll ein sicherer, informierter und vertrauensvoller Umgang mit IKT möglich sein.
Wirtschaft	Sicherheit im Cyber-Raum und stabile Versorgung mit Gütern und Dienstleistungen sind

Zielgruppe	Beschreibung
	zentral für die Integrität der Geschäftsprozesse. Hierfür sollen die Schweizer Unternehmen über bestmögliche Rahmenbedingungen und Sicherheit verfügen.

Tabelle 1: Zielgruppen der NCS 2018-2022

Fallweise werden die Zielgruppen in den Massnahmen weiter spezifiziert.

Zuständigkeiten

Zuständig für die Umsetzung der NCS 2018-2022 ist seit 2019 der Delegierte des Bundesrats für Cyber-Sicherheit. Er führt gleichzeitig das Nationale Zentrum für Cyber-Sicherheit (NCSC). Dieses ist dem Generalsekretariat des Eidgenössischen Finanzdepartements (EFD) angegliedert und bildet als Kompetenzzentrum des Bundes für die Cyber-Sicherheit die zentrale Anlaufstelle für Wirtschaft, Verwaltung, Bildungseinrichtungen und Behörden.

Die strategische Steuerung der NCS 2018-2022 nimmt der Delegierte des Bundesrats gemeinsam mit einem Steuerungsausschuss (StA) vor. Der StA mit rund 23 Mitgliedern bindet Verwaltungseinheiten aus allen Departementen, der Armee, der Kantone (über die zuständige Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren) sowie Vertreter/innen von Wirtschaften und Hochschulen in die kohärente Führung der NCS 2018-2022 mit ein. Der StA trifft sich vierteljährlich.

Die aktuelle Führungsstruktur hat sich in dieser Form seit 2018 entwickelt. Zuvor war das Informatiksteuerorgan des Bundes (ISB) für die NCS verantwortlich und die Melde- und Analysestelle Informationssicherheit (MELANI) setzte diese um. Die Zuständigkeiten sind seit Mai 2020 in der Verordnung über den Schutz vor Cyber-Risiken in der Bundesverwaltung (SR 120.73, Cyberrisikenverordnung, CyRV) geregelt.

1.2 Zielsetzungen und Fragestellungen der Wirksamkeitsüberprüfung

Der Bundesrat hat dem EFD den Auftrag erteilt, bis Ende 2022 die laufende NCS zu überprüfen und gegebenenfalls zu überarbeiten. Der Steuerungsausschuss NCS hat entschieden, die Wirksamkeit extern beurteilen zu lassen. Der Bericht zur Wirksamkeit soll die Basis sein für die weiteren Arbeiten. Die Wirksamkeitsüberprüfung soll deshalb neben einer Beurteilung der Wirksamkeit der NCS 2018-2022 Hinweise zur Anpassung und Optimierung der NCS im Rahmen der geplanten Überarbeitung und Weiterentwicklung geben.

Der vorliegende Bericht fasst die Ergebnisse der im Zeitraum Juli 2021 bis Januar 2022 vorgenommenen Wirksamkeitsüberprüfung zusammen. Diese richtet sich an vier übergeordneten Fragestellungen aus.

Gesamtbetrachtung / Zielerreichung: Inwiefern erreicht die NCS 2018-2022 die darin definierten strategischen Ziele? (Summativer Evaluationszweck)

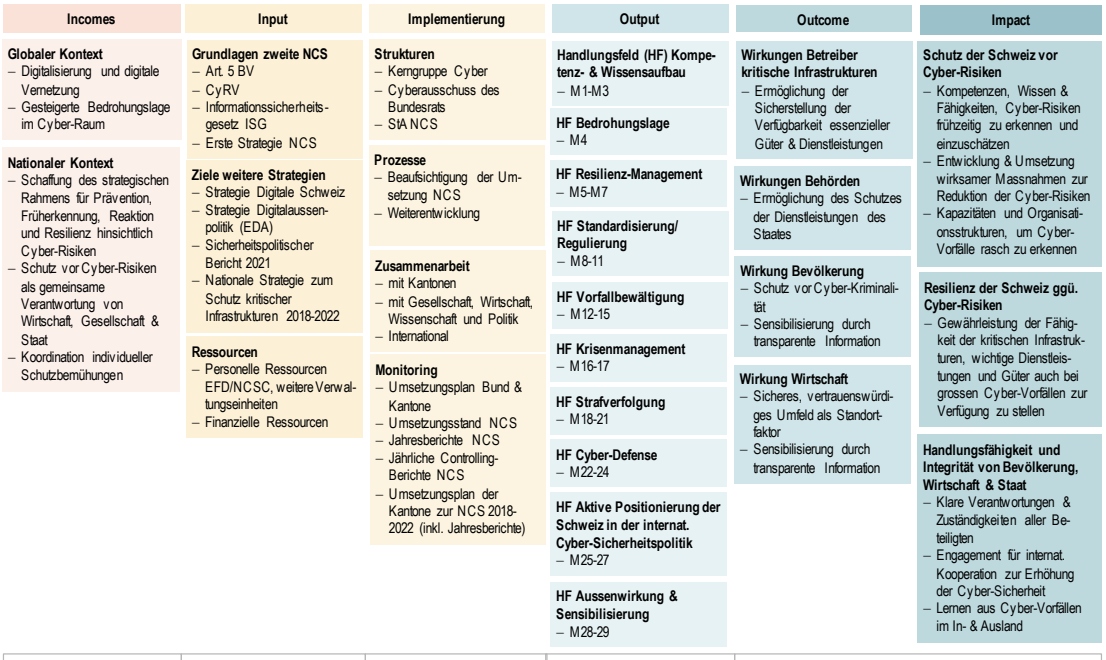
Effizienz / Ressourcen: In welchem Verhältnis steht der Mitteleinsatz zu den im Rahmen der Strategieumsetzung erbrachten Leistungen? (Summativer Evaluationszweck)

Effektivität / Wirkungen: Inwiefern konnten mit den erbrachten Leistungen die beabsichtigten Wirkungen erzielt werden? (Summativer Evaluationszweck)

Weiterentwicklung / Empfehlungen: Welche Empfehlungen lassen sich daraus für die Überarbeitung der Strategie einerseits und für den zukünftigen finanziellen und personellen Ressourceneinsatz andererseits ableiten? (Formativer Evaluationszweck)

Mit der NCS 2018-2022 wurde das dazugehörige Wirkungsmodell reflektiert und weiterentwickelt. Basierend auf der «Theory of Change» kann das Wirkungsmodell wie in Abbildung 2 dargestellt werden. Das Wirkungsmodell dient als umfassender Orientierungsrahmen für die Wirksamkeitsüberprüfung.

Wirkungsmodell



econcept und EBP, 2021

Abbildung 2: Wirkungsmodell NCS 2018-2022. Fokus der Wirksamkeitsüberprüfung bilden die Elemente Output, Outcome und Impact

Zum Wirkungsmodell sind folgende erläuternde Hinweise möglich:

— *Incomes*: Die Incomes umfassen den globalen und nationalen Kontext, in dem die NCS 2018-2022 entwickelt wurde. Sie ist geprägt durch die global wachsende digitale Vernetzung und die damit zusammenhängenden Chancen und Risiken mit dazugehörigen nationalen Schutzbemühungen.

— *Input*: Der Input umfasst die Ziele der NCS 2018-2022, die sich aus den rechtlichen Grundlagen, aus der ersten NCS sowie aus Zielen weiterer Strategien des Bundes ergeben. Zudem schliesst die Inputebene die Ressourcen mit ein, die seitens Bund zur Leistungserbringung im Rahmen der NCS 2018-2022 zur Verfügung stehen.

— *Implementation*: Die Implementation umfasst die Vollzugsstrukturen und -prozesse des Bundes in Zusammenarbeit mit den weiteren nationalen und internationalen Akteuren/innen. Auch umfasst sie das Monitoring anhand von Umsetzungsplänen und Jahresberichten.

— *Output*: Der Output umfasst die Leistungen des Vollzugs der NCS 2018-2022 aller beteiligter Akteure/innen, also die konkreten Aktivitäten und Projekte in den durch die Strategie 2018-2022 definierten Handlungsfeldern. Mittels 29 Massnahmen mit insgesamt 246 Meilensteinen sind die Outputs umfassend festgelegt (siehe Anhang A-5).

— *Outcome*: Die NCS 2018-2022 hat direkte kurz- bis mittelfristige Wirkungen auf ihre Zielgruppen, wie die Betreiber/innen kritischer Infrastrukturen, die Behörden, die Bevölkerung sowie die Wirtschaft (siehe Anhang A-5). Neben den intendierten Wirkungen sind nicht intendierte Wirkungen möglich.

— *Impact*: Der Impact umfasst die längerfristigen Wirkungen der NCS 2018-2022 auf übergeordneter, gesamtgesellschaftlicher Ebene. Auch auf dieser Ebene sind intendierte sowie nicht intendierte Wirkungen zu erwarten (siehe Anhang A-5).

Zu den vier übergeordneten Fragestellungen waren die nachfolgenden Detailfragen zu untersuchen (Tabelle 2).

	Fragestellung	Wirkungsebene
1	**Kontext**: Inwiefern berücksichtigt die NCS 2018-2022 die relevanten Herausforderungen und Entwicklungen auf nationaler und globaler Ebene sowie die gesetzlichen Vorgaben?	Incomes
2	**Grundlagen**: Inwiefern sind rechtliche, strategische und ggf. weitere Grundlagen in die Ziele der NCS 2018-2022 eingeflossen?	Input
3	**Ressourcen**: Inwiefern werden die für die Umsetzung der NCS 2018-2022 eingesetzten Ressourcen als adäquat eingeschätzt?[2]	Input
4	**Strukturen/Prozesse**: Inwiefern werden die Strukturen und Prozesse zur Implementierung der NCS 2018-2022 als effektiv eingeschätzt?	Implementierung
5	**Handlungsfelder**: Inwiefern sind die definierten Handlungsfelder geeignet, die anstehenden Herausforderungen im Umgang mit Cyber-Risiken anzugehen?	Output
6	**Massnahmen**: Inwiefern sind die einzelnen Massnahmen mit ihren Meilensteinen geeignet, um die Ziele der NCS 2018-2022 zu erreichen (z. B. Sind zusätzliche Massnahmen angezeigt? Gilt es, einzelne Massnahmen auszuweiten? Müssten ggf. auch Massnahmen abgebaut werden?)	Output
7	**Kohärenz**: Inwiefern sind Handlungsfelder und Massnahmen der NCS 2018-2022 kohärent?	Output
8	**Nutzen**: Inwiefern erreichen die Massnahmen der NCS die Zielgruppen im gewünschten Mass? (bspw. Nutzen die Zielgruppen die Massnahmen bzw. die etablierten Strukturen und Prozesse sowie die erarbeiteten Produkte, Dienstleistungen, Netzwerke, Methoden etc.?)	Output
9a	**Angestrebte Wirkungen Zielgruppen**: Inwiefern werden angestrebte Wirkungen der NCS 2018-2022 bei den vier explizit adressierten Zielgruppen (kritische Infrastrukturen, Behörden, Wirtschaft, Bevölkerung) erreicht? (bspw. mit Blick auf Befähigung der Akteure/innen, Resilienz etc.)	Outcome
9b	**Weitere Wirkungen Zielgruppen**: Gibt es auf Ebene der Zielgruppen darüber hinaus weitere, unbeabsichtigte Wirkungen? Wie sind diese einzuordnen?	Outcome
9c	**Wirkungen weitere Akteure/innen**: Inwiefern zeigen sich darüber hinaus bei weiteren Akteuren/innen (unbeabsichtigte) Wirkungen und wie sind diese einzustufen?	Outcome

2 Das NCSC plant für Herbst 2021 eine eigene quantitative Erhebung der Ressourcen je Massnahme.

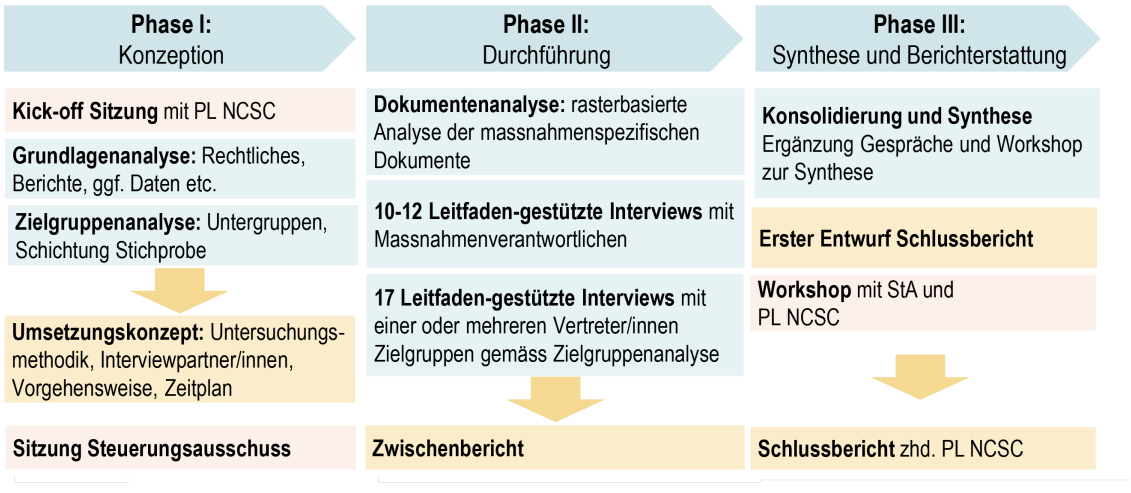
	Fragestellung	Wirkungsebene
10	**Gesamtgesellschaftliche Wirkungen**: Inwiefern werden die beabsichtigten Wirkungen der NCS 2018-2022 auf gesamtgesellschaftlicher Ebene erreicht? – Schutz der Schweiz vor Cyber-Risiken – Resilienz der Schweiz ggü. Cyber-Risiken Wahrung der Handlungsfähigkeit und Integrität von Bevölkerung, Wirtschaft und Staat: Gibt es darüber hinaus weitere, unbeabsichtigte Wirkungen? Wie sind diese einzuordnen?	Impact
11	**Empfehlungen**: Welche Empfehlungen und welches Optimierungspotenzial lassen sich daraus ableiten mit Blick auf... – die künftige NCS 2023-2027? – den künftigen personellen und finanziellen Ressourceneinsatz?	Alle Ebenen des Wirkungsmodells

Tabelle 2: Detailfragestellungen zur Wirksamkeitsüberprüfung NCS 2018-2022.

1.3 Vorgehen und Bericht

Für die Wirksamkeitsüberprüfung wurden verschiedene methodische Zugänge gewählt: Analyse von internen und/oder umsetzungsrelevanten Dokumenten, Analyse von nationaler und internationaler Literatur, Analyse von involvierten Akteuren/innen resp. Zielgruppen sowie leitfadengestützte Interviews (siehe Leitfäden in Anhang A-2) und Fokusgruppen sowohl mit Massnahmenverantwortlichen und -beteiligten der NCS 2018-2022 als auch mit Vertretern/innen der Zielgruppen (siehe Anhang A-3 und Anhang A-4). Dieses Vorgehen ermöglicht eine Beurteilung der NCS 2018-2022 sowohl aus der Innen- als auch aus der Aussenwahrnehmung. Die Untersuchung wurde in drei Phasen (siehe Abbildung 3) gegliedert, der NCS-Steuerungsausschuss wurde in Phase I und Phase II involviert.

Projektdesign in drei Phasen



econcept und EBP, 2021

Abbildung 3: Projektdesign zur Wirksamkeitsüberprüfung inkl. Methoden, Interaktion mit NCSC und Zeitplan. Phase I wird mit der Verabschiedung des Umsetzungskonzepts abgeschlossen.

Weitere Details zum Vorgehen finden sich in Anhang A-1. Die Bearbeitung erfolgte zwischen Juli 2021 und Januar 2022. Der vorliegende Bericht fasst die Ergebnisse der Wirksamkeitsüberprüfung wie folgt zusammen:

— Kapitel 2 nimmt eine übergeordnete Gesamtbeurteilung der NCS 2018-2022 vor und beantwortetet die Frage, ob und wie zweckmässig und angemessen die NCS 2018-2022 eingeschätzt wird, um den Schutz der Schweiz vor Cyber-Risiken zu erhöhen.

— In Kapitel 3 wird untersucht, welche Leistungen in den zehn Handlungsfeldern bislang erbracht wurden und welche Wirkungen im Sinne von Outcomes damit in Verbindungen gebracht werden.

— Mit Kapitel 4 wird auf die vier Zielgruppen fokussiert, um zu klären, ob und wie sich deren Integrität und Handlungsfähigkeit gegenüber Cyber-Bedrohungen erhöht hat.

— Kapitel 5 dient der Gesamtbeurteilung der Wirksamkeit, wozu die übergeordneten Untersuchungsfragen mit summativen Evaluationszweck (siehe Kapitel 1.2) beantwortet werden

— Im abschliessenden Kapitel 6 werden mit Blick auf die Fortschreibung der NCS Empfehlungen zur Erhöhung der Wirksamkeit hergeleitet (siehe auch vierte übergeordnete Fragestellung Kapitel 1.2)

Die vorliegende Wirksamkeitsbeurteilung widerspiegelt die durch ein systematisches, multimethodisches und multiperspektivisches Vorgehen gewonnene Einschätzung der Autoren/innen. Diese danken allen Beteiligten für die Bereitschaft und Offenheit zur Mitwirkung.

2 Zweckmässigkeit und Angemessenheit der NCS 2018-2022

Die Wirksamkeit der NCS 2018-2022 hängt einerseits von ihrer Konzeption und Ausrichtung auf die relevanten Herausforderungen ab. Anderseits ist es die Umsetzung der Strategie, welche die Wirksamkeit direkt beeinflusst. Nachfolgend werden die Einschätzungen zur Konzeption der NCS 2018-2022 dargelegt. Der Fokus liegt auf den Wirkungsebenen von Incomes (nationaler und internationaler Kontext), Input (Grundlagen, Ziele und Ressourcen) und Implementation (Strukturen und Prozesse). Die Handlungsfelder als Output der NCS sind hinsichtlich ihrer Eignung zur Zielerreichung beurteilt. Eine Wirkungsbeurteilung für die Handlungsfelder folgt in Kapitel 3.

Nachfolgend werden jeweils die Detailfragen vorangestellt, die mittels der Beurteilung aus Dokumentenanalyse sowie Interviews mit Massnahmenverantwortlichen und Vertreter/innen der Zielgruppen zu beantworten waren.

2.1 Cyber-Bedrohung und Herausforderungen

Kontext: Inwiefern berücksichtigt die NCS 2018-2022 die relevanten Herausforderungen und Entwicklungen auf nationaler und globaler Ebene sowie die gesetzlichen Vorgaben?

Die aktuelle Strategie greift einleitend die zentralen Bedrohungen resp. Cyber-Risiken für die Schweiz auf und identifiziert die Herausforderungen für die Widerstandskraft der Schweiz. So unterscheidet sie zwischen beabsichtigten unerlaubten Handlungen – sog. Cyber-Angriffe, zu denen Cyber-Kriminalität, Cyber-Spionage, Cyber-Sabotage und Terrorismus, Desinformation und Propaganda sowie Cyber in Konflikten gehören – und unabsichtlich herbeigeführten Ereignissen, namentlich menschliches Fehlverhalten (bspw. Kreditkartenbetrug, etc.) sowie technische Ausfälle.

Aus den identifizierten Bedrohungslagen und aus den Erfahrungen der NCS 2013-2017 wurde eine strategische Weiterentwicklung in fünf Bereichen angestossen. Die weiterentwickelte Strategie setzt die Schwerpunkte auf den Schutz vor Bedrohungen und auf eine resiliente Infrastruktur, um so handlungsfähig zu bleiben. Diese Schwerpunkte bedingen eine stärkere strategische Führung und eine Umsetzung mit einem ergänzten Massnahmenbündel, einen Ausbau der Kapazitäten und des Wissens, eine breitere Abstützung, indem mehr Zielgruppen adressiert wurden und eine Stärkung der Zusammenarbeit. Dabei liegt ein deutliches Gewicht auf der Stärkung der organisatorischen Strukturen.

Aus Sicht der Befragten wurden aus der ersten Strategie die richtigen Lehren gezogen und mit der NCS 2018-2022 ein angemessener Rahmen geschaffen, um mit den Cyber-Bedrohungen umgehen zu können. Aus dem strategischen Kontext mit dem sicherheitspolitischen Bericht 2016, der bundesrätlichen Strategie «Digitale Schweiz» und der nationalen Strategie zum Schutz der Kritischen Infrastrukturen wurde der richtige Handlungsbedarf

abgeleitet. Insbesondere die Ausdehnung auf weitere Zielgruppen und die Verstärkung der Zusammenarbeit wurde von den Befragten als positiv erwähnt.

Eine Studie der ETH Zürich (CSS, 2019) welche die NCS 2013-2017 und die NCS 2018-2022 einem internationalen Vergleich mit nationalen Cyber-Sicherheitsstrategien unterzog, stützt die obigen Einschätzungen. Die NCS richtet sich bislang an acht übergeordneten Herausforderungen aus, die sich international in verschiedenen Analysen zu Ausgangslagen und Strategien erkennen lassen.

Fazit: Die NCS 2018-2022 basiert auf aktuellen Grundlagen und ist auf die zentralen Herausforderungen und Entwicklungen zur Erhöhung der nationalen Cyber-Sicherheit ausgerichtet.

2.2 Institutioneller Kontext der Strategie

Grundlagen: Inwiefern sind rechtliche, strategische und ggf. weitere Grundlagen in die Ziele der NCS 2018-2022 eingeflossen?

Die NCS 2018-2022 baut auf den Vorarbeiten und den bisherigen Erkenntnissen der NCS 2012-2017 auf. Der Strategieprozess für die Jahre 2018-2022 hat diese bestehenden Grundlagen und Erfahrungen mit aktuellen Studien sowie Einschätzungen der beteiligten Akteure/innen nach Angaben der befragten Personen stringent und umfassend zusammengeführt. Die aktuellen Herausforderungen wurden nach allgemeiner Einschätzung gut erfasst (siehe Kapitel 2.1). Die damaligen rechtlichen Rahmenbedingungen wurden berücksichtigt sowie die laufenden Prozesse hin zur CyRV und zum Bundesgesetz über die Informationssicherheit beim Bund (SR 126, Informationssicherheitsgesetz, ISG) antizipiert.

Neben der NCS gibt es die Strategie «Digitale Schweiz»[3], die seit 2021 durch den geschaffenen Delegierten des Bundesrates für digitale Transformation und IKT-Lenkung in der Bundeskanzlei verantwortet wird (zuvor durch das Bundesamt für Kommunikation (BAKOM)). Das EDA hat eine «Strategie Digitalaussenpolitik 2021-2024»[4] und das VBS hat die «Strategie Cyber VBS 2021-2024»[5]. Mit Blick auf die Inhalte sind die drei Strategien als grösstenteils kohärent und ineinandergreifend zu beurteilen. So beabsichtigt bspw. das Handlungsfeld Cyber-Aussenpolitik der NCS die Verbindung von Cyber-Innen- und -Aussenpolitik. Befragte Personen weisen darauf hin, dass die Abstimmung der verschiedenen Strategien mit der NCS 2018-2022 Verbesserungspotenziale enthalte. Die strategischen Führungsgremien der Strategien werden hierzu zu wenig miteinander vernetzt.

Fazit: Die rechtlichen und strategischen Grundlagen sind in der NCS 2018-2022 adäquat berücksichtigt. Es bestehen jedoch institutionelle Inkongruenzen.

---

[3] https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/strategie-digitale-schweiz/digitale-schweiz.html, Zugriff vom 7. Januar 2022

[4] https://www.eda.admin.ch/dam/eda/de/documents/publications/SchweizerischeAussenpolitik/20201104-strategie-digitalaussenpolitik_DE.pdf, Zugriff vom 7. Januar 2022

[5] https://www.newsd.admin.ch/newsd/message/attachments/66200.pdf; Zugriff vom 22. Januar 2022.

2.3 Ressourcen

Ressourcen: Inwiefern werden die für die Umsetzung der NCS 2018-2022 eingesetzten Ressourcen als adäquat eingeschätzt?

Die ETH Zürich stellte 2019 in einer internationalen Vergleichsstudie zusammenfassend fest, dass die politischen Akteure/innen in anderen Staaten bereit sind, bei einer strategischen Herangehensweise zur nationalen Cyber-Sicherheit umfassend Ressourcen bereitzustellen (CSS, 2019). Die Ausgaben der Schweiz seien hierfür im Vergleich eher niedrig.

Die personellen Ressourcen der NCS wurden seit 2018 verschiedentlich erhöht. Das NCSC hat im Herbst 2021 eine aktualisierte Ressourcen- und Bedarfserhebung 2021 bei den an der NCS beteiligten Ämtern vorgenommen (NCSC, 2021c). Demnach äussert eine Mehrheit der Ämter einen Bedarf, die mit der Massnahmenumsetzung der NCS 2018-2022 verbundenen personellen Kapazitäten auszubauen.

Im Zuge der Wirksamkeitsüberprüfung wurde durch die massnahmenverantwortlichen Personen präzisiert, dass bislang die zentralen Elemente und Kernaufgaben der 29 Massnahmen mit den verfügbaren personellen Ressourcen erfüllt werden konnten. Der Bedarf für zusätzliche personelle Ressourcen wurde wie folgt begründet:

- *Doppelbelastungen*: Zahlreiche Projekte werden durch Personen geführt, die gleichzeitig eine Linienfunktion in ihrer Organisation zu erfüllen haben. Daraus entstehen eine Ressourcenkonkurrenz und eine Doppelbelastung, die in vielen Fällen als Überlast empfunden wird. Mit der Bereitstellung zusätzlicher Ressourcen gehe es um das Erfüllen laufender Aufgaben in Linienfunktionen.
- *Unbesetzte Stellen*: Verschiedene Verwaltungseinheiten weisen unbesetzte Stellen auf. Ursache hierfür seien Vorhalteentscheidungen durch Amtsdirektionen sowie Schwierigkeiten, Personen mit den notwendigen Fähigkeiten zur Stellenbesetzung zu finden.
- *Weiterbildungsbedarf*: Die hohe Entwicklungsdynamik im Cyber-Raum erfordere eine intensive Weiterbildungsaktivität. Dies wiederum beschneide die einsetzbaren Kapazitäten. Eine Erhöhung der Ressourcen würde die durchgehende Handlungsfähigkeit bei gleichzeitig hoher Weiterbildungsaktivität sicherstellen.
- *Aufgabenwachstum*: Die NCS 2018-2022 umfasst Massnahmen zum Aufbau operationeller Aktivitäten (bspw. Fallübersicht u. Ä.). Eine Zunahme von Cyber-Angriffen führe zu einem laufenden Wachstum in der operationellen Abwicklung, sodass zusätzliche Ressourcen als erforderlich angesehen werden. Für stark operationelle Massnahmen sei eine Verstetigung anzustreben, weshalb die Ressourcen langfristig benötigt werden.

Verschiedene Interviewpartner/innen waren der Meinung, dass mit den vorhandenen Ressourcen in der Governance und den Umsetzungsprozessen mehr Wirkung hätte erzielt werden können. Die NCS habe eine starke Orientierung an Zielsetzungen und Wirkungen der NCS gefördert, ohne permanent die Allokation der Ressourcen zu hinterfragen. Dennoch könnten die Ressourcen noch stärker geteilt werden, insbesondere über die drei Be-

reiche von Cyber-Strafverfolgung, Cyber-Sicherheit und Cyber-Defence hinweg. Verschiedene Akteure/innen regen hierzu seit längerem einen mit ausreichenden personellen Ressourcen ausgestatteten gemeinsamen Experten/innenpool an, der die bereichsübergreifende Zusammenarbeit stark prägen soll. Rechtsstaatliche Prinzipien und hiermit verbunden Rechtsgrundlagen, die gezielte Abgrenzungen zwischen den Bereichen vorsehen, sollen jedoch jederzeit gewahrt werden.

Fazit: Mit den bislang verfügbaren Ressourcen können die Kernaufgaben zur Umsetzung der Massnahmen der NCS 2018-2022 wahrgenommen werden. Die Effizienz des Mitteleinsatzes könnte durch eine bereichsübergreifende Intensivierung und/oder Anpassung der Zusammenarbeit (bspw. mittels Experten/innenpool) erhöht werden. Darüber hinaus besteht ein begründeter Bedarf, um die personellen Kapazitäten zur NCS-Umsetzung zu erhöhen.

2.4 Governance und Zusammenarbeit

Strukturen/Prozesse: Inwiefern werden die Strukturen und Prozesse zur Implementierung der NCS 2018-2022 als effektiv eingeschätzt?

Die Umsetzung der NCS basiert auf einem dezentralen Ansatz, wonach verschiedene an der NCS beteiligte Bundesämter ihnen zugewiesene Umsetzungsvorhaben direkt umsetzen (siehe Bundesrat, 2018). Dabei unterstützt das NCSC die Koordination zwischen den Bundesämtern und übernimmt auch selbst die Verantwortung für Umsetzungsvorhaben. Die NCS versteht den dezentralen Steuerungs- und Umsetzungsansatz als eine Netzwerkstruktur. Diese Struktur ist geprägt durch eine gemeinsame Koordinationsstelle sowie wenig formale Abstimmungen zwischen den Bereichen «Cyber-Defence», «Cyber-Security» und «Cyber-Strafverfolgung» und wenig formale Abstimmungen zwischen den verschiedenen Handlungsfeldern.

Die Befragten schätzen diese Netzwerkstruktur durchgehend als zweckmässig ein. Zum einen habe diese bei Einführung der NCS 2018-2022 eine rasche Aufnahme der Aktivitäten und die Integration bereits vorhandener Kompetenzen durch etablierte Strukturen ermöglicht. Zum anderen sichere die Netzwerkstruktur laufend eine hohe Agilität und Reaktionsfähigkeit, wobei zusätzliche Akteure/innen rasch und gleichwertig integriert werden können. Die Zusammenarbeit im Netzwerk wird als vertrauensvoll, effizient und lösungsorientiert geschildert. Dies gilt sowohl auf operativer Ebene zur Umsetzung von Massnahmen als auch auf Ebene der strategischen Führung. Die gegebenen Rahmenbedingungen und inhaltlichen Stossrichtungen durch die NCS unterstützen dies. Diese Feststellung untermauern vereinzelte Aussagen, wonach sich der Prozess der Strategieentwicklung zur NCS 2018-2022 wegen des grossen inhaltlichen Freiheitsgrades und der vielen Beteiligten als arbeitsintensiv erwiesen hat.

Die potenziellen inhaltlichen Synergien des Netzwerkes würden allerdings kaum vollständig genutzt. Als Ursache hierfür wird eine Vernetzung gesehen, die primär innerhalb der drei übergeordneten Bereiche «Cyber-Defence», «Cyber-Security» und «Strafverfolgung

und Cyber-Kriminalität» der Bundesverwaltung vorgenommen werde. Eine laterale, über diese drei Bereiche resp. über alle Handlungsfelder greifende Vernetzung werde zu wenig intensiv vorgenommen. Als Beispiele entsprechender Synergieverluste werden Gefährdungsanalysen, Resilienzmassnahmen und Ausbildungen genannt, die nicht vollständig abgestimmt zwischen «Defence» und «Security» sowie zwischen zivilen Behörden und militärischen Elementen erfolgen. Allerdings weisen gewisse Akteure/innen darauf hin, dass die vollständige Abstimmung zwischen «Defence» und «Security» aufgrund rechtstaatlicher Vorbehalte und konkreter Gesetze nicht erfolgen dürfe. Dies betreffe bspw. den Informationsaustausch zu ermittelten Schwachstellen. Gemeinsamer Kompetenzaufbau hingegen sei erwünscht. Ein Beispiel dafür ist die Ausbildung zum Cyber Security Specialist mit eidgenössischem Fachausweis (EFA), mit der gleichzeitig für die Armee und für zivile Organisationen ein wichtiges Angebot entstanden ist.

Für die noch stärkere bereichsübergreifende Vernetzung fehle es, zusätzlich zum Steuerungsausschuss, an Gelegenheiten, welche die Vernetzung und die direkte Ansprache anderer Akteure/innen ermöglichten.

Die Governance zur NCS 2018-2022 hat mit der neuen Position des Delegierten des Bundesrates für Cyber-Sicherheit und mit dem Aufbau des Nationalen Zentrums für Cyber-Sicherheit NCSC eine zusätzliche Institutionalisierung erhalten. Diese auf die Governance bezogenen Massnahmen sowie die Zusammenarbeit mit den Mitarbeitenden des NCSC werden durchgehend als positiv beurteilt.

Die NCS 2018-2022 habe die Grundlage zur Konsolidierung verschiedener Aktivitäten im Nationalen Zentrum für Cyber-Sicherheit gelegt. Das NCSC wiederum wirke positiv auf die Strategie, indem es die strategische Führung verstärkt und die Reaktionsfähigkeit erhöht habe. Das Zentrum mit seinen regelmässigen Publikationen sowie der Delegierte geben nach Meinung der meisten befragten massnahmenverantwortlichen Personen der NCS eine Sichtbarkeit mit Wiedererkennung. Diese lasse sich an einer verstärkten Berichterstattung in den Medien über Cyber-Risiken inkl. Referenzierung auf den Delegierten und die Stellen des Bundes (insb. NCSC) feststellen. Die fachlichen und strategischen Fähigkeiten, kombiniert mit einer integrativen Persönlichkeit, werden von den Interviewten häufig als wesentliche Eigenschaften des Delegierten des Bundes für Cybersicherheit herausgehoben.

Als zu wenig effizient und effektiv hinsichtlich Governance und Prozessen haben vereinzelte Befragte die Verbindung der NCS mit den weiteren Digital-, Cyber- und Schutzstrategien innerhalb der Bundesverwaltung eingeschätzt. Einerseits seien nicht alle relevanten Verwaltungseinheiten aus übergeordneter strategischer Ebene in die «Kerngruppe Cyber» eingebunden. Anderseits berücksichtige die Governance der NCS operative Tätigkeiten über die beteiligten Verwaltungseinheiten hinweg zu wenig.

Fazit: Die Netzwerkstruktur wird als vorteilhaft für die Umsetzung der NCS 2018-2022 angesehen. In der operationellen Umsetzung werden die Vorteile nicht vollständig realisiert,

wobei die seit 2018 vorgenommene Weiterentwicklung der NCS-Governance als zweckmässig hierfür eingeschätzt wird. Die strukturelle und prozessuale Verbindung mit übergeordneten und verwandten Strategien wird als verbesserungswürdig beurteilt.

2.5 Strategische Zielsetzungen

Grundlagen: Inwiefern sind rechtliche, strategische und ggf. weitere Grundlagen in die Ziele der NCS 2018-2022 eingeflossen?

Die befragten Interviewpartner/innen sind der Meinung, dass der Erarbeitungsprozess wesentlich dazu beigetragen hat, die beteiligten Wissensträger/innen früh zu vernetzen und die Zusammenarbeit zu stärken. Das gemeinsame Engagement wurde ausdrücklich begrüsst. Diese frühe Einbindung der Stakeholder in die Strategieentwicklung empfiehlt die European Union Agency for Network and Information Security in ihrem Practice Guide (ENISA, 2016). Die identifizierten Ziele der Strategie gelten aus damaliger Sicht als richtig. Die Zielsetzungen basieren auf dem relevanten Wissen aller Beteiligten und einem Konsens unter diesen. Damit haben sie auch die Zustimmung geben, sich für das Erreichen der Zielsetzung einzusetzen.

Die sieben übergeordneten strategischen Ziele und die Grundsätze des Handelns definieren aus Sicht der Gesprächspartner/innen ausreichend genau, was zur Erfüllung der NCS-Vision notwendig ist, damit die Schweiz angemessen vor Cyber-Risiken geschützt ist und die Handlungsfähigkeit und Integrität von Bevölkerung, Wirtschaft und Staat gegenüber Cyber-Bedrohungen gewährleistet bleiben. Ebenfalls positiv erwähnt wurde die Dreiteilung in Security, Strafverfolgung und Defence. Dies wird als sinnvoll erachtet. Als wichtig für die Akzeptanz der Zielsetzungen wurde der breite Ansatz eingeschätzt, der auch Kantone und weitere Institutionen mit einbindet. Einige Interviewpartner/innen beurteilen diesen föderalen bzw. dezentralen Ansatzes auch kritisch, weil er eine schnelle Wirkungsentfaltung im Alltag erschwere.

Verschiedentlich wurde angemerkt, dass die Strategie nach wie vor stark auf den Bund bzw. die Bundesverwaltung ausgerichtet sei. Mit der Umsetzungsplanung der Kantone konnten gemäss Interviewten hier zusätzliche Schwerpunkte gesetzt werden. Die Anliegen der Kantone sollten in Zukunft noch stärker einfliessen können.

Punktuell wurde darauf hingewiesen, dass die in der Strategie unter «Vision» aufgeführten Chancen der Digitalisierung keine Entsprechung in den strategischen Zielen finden würden. Es wären hierzu keine spezifischen Massnahmen festgelegt worden. Die strategischen Ziele fokussieren ausschliesslich auf den Umgang mit Cyber-Risiken. Dieser Einschätzung stehen einzelne Meinungen gegenüber, die dezidiert auf den Schutz- und Risikocharakter der NCS als Hauptzweck hinweisen. Die entsprechenden Chancen eines hohen Cyber-Schutzes der Schweiz mit hoher Handlungsfähigkeit und Integrität gegenüber Cyber-Bedrohungen seien andernorts, bspw. in der bundesrätlichen Strategie «Digitale Schweiz» (Schweizerische Eidgenossenschaft, 2020a), aufzunehmen.

Fazit: Die Grundlagen, der erkannte Handlungsbedarf und die Herausforderungen sind angemessen in die Ziele der NCS 2018-2022 eingeflossen. Teilweise kritisch eingeschätzt werden der starke Fokus auf die Bundesverwaltung und der fehlende Blick auf mögliche Chancen.

2.6 Zielgruppen

Grundlagen: Inwiefern sind rechtliche, strategische und ggf. weitere Grundlagen in die Ziele der NCS 2018-2022 eingeflossen?

Nutzen: Inwiefern erreichen die Massnahmen der NCS die Zielgruppen im gewünschten Mass?

Die Ausrichtung an Zielgruppen stellt eine wichtige Grundlage zur wirksamen Ausgestaltung der NCS 2018-2022 dar (siehe auch «Outcome» Wirkungsmodell, Kapitel 1.2). Die NCS 2018-2022 nimmt mit den vier Zielgruppen von kritischen Infrastrukturen, Behörden, Bevölkerung und Wirtschaft eine stark aggregierte Einteilung vor. Diese Aggregation mit der Möglichkeit zur weiteren Aufteilung im Zuge der Umsetzung von Massnahmen betrachten die Massnahmenverantwortlichen grundsätzlich als angemessen. Die Schwierigkeit der NCS 2018-2022 sei vielmehr, dass ihre Massnahmen die vier Zielgruppen nicht gleichermassen adressierten und hierdurch nicht alle Zielgruppen im gewünschten Mass erreicht werden können.

Die Unterschiede in der Ansprache der Zielgruppen werden u. a. mit fehlenden gesetzlichen Grundlagen erklärt. Demnach hat der Bund primär sich selbst von Cyber-Risiken zu schützen.[6] Die Massnahmen zum Schutz kritischer Infrastrukturen stützen sich in der NCS auf bestehende Rechtsgrundlagen der beteiligten Stellen (z. B. NDB, BABS, BWL, BAKOM). Zusätzlich wurde während der Umsetzung der NCS das Informationssicherheitsgesetz (ISG) durch das Parlament verabschiedet, das den Bund explizit beauftragt Betreiber/innen kritischer Infrastrukturen bei der Cyber-Sicherheit zu unterstützen.

Für Aktivitäten zum Schutz der Bevölkerung oder beispielsweise von KMU bestehen keine ausreichenden Rechtsgrundlagen.

Der starke Fokus auf die Zielgruppe «kritische Infrastruktur», wird mit Blick auf die Wirkungsziele der NCS durchgehend als richtig angesehen. Schwierigkeiten ergeben sich aus der konkreten Abgrenzung, welche Akteure/innen unter diese Zielgruppe fallen. Probleme sehen Befragte darin, dass das Bewusstsein für Lieferkettenrisiken im Zusammenhang mit Bestandteilen oder auch Dienstleistungen für kritische Infrastrukturen mangelhaft sei und durch die NCS nicht konsequent angesprochen werde. Gleiches gelte auf kommunaler Ebene für den Infrastrukturbetrieb durch Städte und Gemeinden.

Eine weitere Unsicherheit innerhalb der NCS ergab sich anfänglich aus der unterschiedlichen Sichtweise, wie das Bundesamt für Bevölkerungsschutz (BABS), das Bundesamt für

6 CyRV

wirtschaftliche Landesversorgung (BWL) und sektorspezifische Fachämter kritische Infrastruktur betrachten und Anforderungen an diese formulieren. Mit der Übertragung der koordinativen Gesamtverantwortung für das Resilienzmanagement an das BABS konnte eine einheitliche Analyse mit einem konsolidierten Gefährdungsbild sichergestellt werden. Das BWL übernahm im Gegenzug die Gesamtverantwortung zur Ausarbeitung von Minimalstandards für den Schutz kritischer Infrastrukturen. Für einzelne Befragte besteht der Bedarf für eine abschliessende und durch die gesamte Bundesverwaltung zu verwendende Definition kritischer Infrastrukturen weiterhin.

Bezüglich der Zielgruppe «Behörden» erkennen sowohl massnahmenverantwortliche Personen als auch Vertreter/innen von Zielgruppen zu Beginn der NCS 2018-2022 eine Lücke bei der Ansprache der Gemeinden. Mit dem später aufgegriffenen Umsetzungsvorhaben für ein Cyber-Sicherheitslabel für Gemeinden und KMU (Cyber-Safe) wurde versucht, diese Lücke zu schliessen. Die Zusammenarbeit zwischen Bund und Gemeinden sei im geltenden Subsidiaritätsprinzip wenig etabliert, sodass sowohl beim Bund als auch bei den Gemeinden wenig Sensibilisierung bezüglich möglicher Angebote und Zusammenarbeit vorhanden sei. Die Zusammenarbeit mit den Kantonen habe sich in der NCS 2018-2022 hingegen stark entwickelt. Die Kantone vermögen keine flächendeckende Verbindung mit den Gemeinden zu schaffen.

Verschiedentlich wurde darauf hingewiesen, dass die NCS innerhalb des Bundes nicht alle wichtigen Akteure/innen gleichermassen einbinde. So würden beispielsweise wichtige Ämter des Departements Umwelt, Verkehr, Energie und Kommunikation (UVEK) nicht adäquat berücksichtigt. Das Bundesamt für Zivilluftfahrt (BAZL), das Bundesamt für Verkehr (BAV), das Bundesamt für Strassen (ASTRA) und das Bundesamt für Energie (BFE) sind jeweils verantwortlich für kritische Infrastrukturen, nehmen jedoch keinen Einsitz in die Gremien der NCS. Für die Umsetzung ihrer Aufgaben im Kontext der NCS haben diese Bundesämter teilweise selbstständig zusätzliche, explizit auf diese Aufgabe ausgerichtete, Stellen geschaffen.

Die Ansprache der Zielgruppe «Wirtschaft» beurteilt eine Mehrheit der Befragten als wenig ausgeglichen. Die Wirtschaft lasse sich demnach in folgende Untergruppen unterteilen, die sich in Strukturen und Herausforderungen, aktuellem Schutzstandard vor Cyber-Risiken sowie Regulierungen unterscheiden:

- *Betreiber/innen kritischer Infrastruktur*: Diese werden als eigene Zielgruppe der NCS 2018-2022 berücksichtigt, wobei die Unternehmen relevante Unterschiede in ihrer Grösse und dem Umfang ihrer Tätigkeiten aufweisen.
- *International tätige Unternehmen*: International tätige Unternehmen verwenden häufig erhebliche Ressourcen zur Sicherstellung der Integrität der Geschäftsprozesse und zur Erfüllung verschiedener nationaler Regulierungen für Datensicherheit und Datenschutz. Dies gilt auch für internationale Unternehmen, die mit Niederlassungen in der Schweiz aktiv sind. Die international tätigen Unternehmen erreichen ihre Cyber-Sicherheit autonom und es kommen nur wenige dieser Unternehmen regelmässig in Berührung mit der

NCS. Das NCSC hat hierzu in den vergangenen Jahren seine sog. geschlossenen Kundenkreise ausgeweitet und dabei vermehrt KMU eingebunden.

– *Kleine und mittlere Unternehmen*: Sowohl massnahmenverantwortliche Personen und Vertreter/innen der Wirtschaft sehen in den vielen KMU eine Cyber-Sicherheitslücke. Dabei bestehe insbesondere ein Problem der «Awareness», womit diese Zielgruppe zu wenig in der NCS 2018-2022 berücksichtigt werde.

Die Bevölkerung wird von vielen Akteuren/innen als schwächstes Glied in der Wirkungskette zum Schutz von Cyber-Risiken betrachtet. Gleichzeitig spräche die NCS 2018-2022 die Bevölkerung am wenigsten direkt an. Zur Bedeutung der Bevölkerung nehmen die Befragten differenzierte Einschätzungen danach vor, ob es um die Reduktion von Cyber-Risiken und Schäden in den privaten Haushalten geht oder um die arbeitende Bevölkerung, die über ein minimales Mass an Sensibilisierung und Grundwissen zur Cyber-Sicherheit zwecks beruflicher Tätigkeit verfügen soll.

Fazit: Mit den vier Zielgruppen richtet sich die NCS 2018-2022 an einem umfassenden Spektrum relevanter Akteure/innen aus. Innerhalb der Zielgruppen weist die NCS starke Unterschiede und Lücken betreffend konkrete Massnahmen für die unterschiedlichen Teilsegmenten innerhalb der Zielgruppen auf.

2.7 Handlungsfelder und Massnahmen im Strategiegefüge

Kohärenz: Inwiefern sind Handlungsfelder und Massnahmen der NCS 2018-2022 kohärent?

Um die strategischen Ziele zu erreichen, definiert die NCS 2018-2022 zehn Handlungsfelder, die diverse Teilaspekte der Cyber-Risiken adressieren. In diesen Handlungsfeldern finden sich insgesamt 29 Massnahmen.

Der Aufbau der NCS 2018-2022 wird von allen Gesprächspartnern/innen als geeignet und in sich kohärent wahrgenommen. Umfang, Gliederung und Tiefgang seien angemessen und ermöglichten einen schnellen und guten Überblick wie die Schweiz mit Cyber-Risiken umgehe.

In den Handlungsfeldern werden geeignete Stossrichtungen gesehen zum Erreichen der sieben strategischen Zielsetzungen. Das breite Spektrum von zehn Handlungsfelder sei für die NCS 2018-2022 bei aktuellem Maturitätsgrad der Schweiz hinsichtlich Cyber-Risiken angemessen. Es schaffe die Voraussetzung für die Einbindung vieler Zielgruppen und Herausforderungen, berge aber auch die Gefahr des Verzettelns. Bei zunehmender Maturität sei, nach Einschätzung mehrerer Befragten, eine stärkere Fokussierung zu prüfen. Die Handlungsfelder dienen in der NCS 2018-2022 primär zur Strukturierung der Herangehensweise. Für die Interviewpartner/innen bildet der Umsetzungsplan zur Strategie das Schlüsselwerkzeug. Der Umsetzungsplan knüpfe an die Handlungsfelder der Strategie an. Gleichzeitig widerspiegle er die Breite der Verwaltung und der involvierten Zielgruppen, was zu einer starken organisatorischen Prägung führe. Die hierarchische Unterteilung in

Handlungsfeld --> Massnahme --> Umsetzungsprojekt wird zudem als zu komplex und zu starr wahrgenommen. Aus Sicht einiger Interviewpartner/innen hat das eine mangelnde inhaltliche Quervernetzung zur Folge und Synergiepotenziale werden nicht ausgeschöpft. Zudem wurde darauf hingewiesen, dass die Handlungsfelder und Massnahmen stark auf die Bundesverwaltung ausgerichtet seien. Einige Gesprächspartner/innen weisen darüber hinaus darauf hin, dass noch kein befriedigender Ansatz vorhanden sei, wie die Wirksamkeit der Massnahmen zu beurteilen oder zu kontrollieren sei.

Wenig konkrete Ansätze zur Wirkungsmessung führen dazu, dass das Controlling der Massnahmen stark formal und wenig inhaltlich wahrgenommen wird. Hier wünscht man sich eine flexiblere Gliederung, die eine stärkere Differenzierung nach der Art der Massnahme erlaube, wie etwa eine Sofortmassnahme, ein Projekt oder eine neue laufende Aufgabe.

Fazit: Handlungsfelder und Massnahmen fügen sich gut in die Strategie ein. Der Aufbau der Strategie wird insgesamt als angemessen eingeschätzt und der Umsetzungsplan als geeignetes Schlüsselwerkzeug wahrgenommen. Die Handlungsfelder und Massnahmen decken die Herausforderungen in der ganzen Breite ab und lassen sich nachvollziehbar aus den Zielen der Strategie ableiten.

3 Leistungen und Wirkungen der Handlungsfelder

Die NCS 2018-2022 ist darauf ausgelegt, ihre Wirkung durch die den zehn Handlungsfeldern zugewiesenen Massnahmen zu erreichen. Die Handlungsfelder und Massnahmen sind in ihrer Gesamtheit und mit Blick auf die Strategie auf der Outputebene zu finden. Hingegen lassen sich die Handlungsfelder mit ihren Massnahmen in durch sie zu erzielende erzielte Leistungen (Outputs) und angestrebte Wirkungen (Outcomes) ausdifferenzieren. Die nachstehenden Ausführungen beziehen sich auf Output- und Outcome-Ebene der Handlungsfelder und Massnahmen und nehmen eine bilanzierende Gesamtbetrachtung für die Handlungsfelder vor. Für die einzelnen Handlungsfelder werden jeweils folgende Fragen beantwortet:

Handlungsfelder: Inwiefern sind die definierten Handlungsfelder geeignet, die anstehenden Herausforderungen im Umgang mit Cyber-Risiken anzugehen?

Massnahmen: Inwiefern sind die einzelnen Massnahmen mit ihren Meilensteinen dazu geeignet, die Ziele der NCS 2018-2022 zu erreichen (z. B. sind zusätzliche Massnahmen angezeigt? Gilt es einzelne Massnahmen auszuweiten? Müssten ggf. auch Massnahmen abgebaut werden?)

3.1 Kompetenzen- und Wissensaufbau

Nr.	Massnahme	Umsetzungsvorhaben	Status
1	Früherkennung von Trends und Technologien und Wissensaufbau	Technologiemonitoring	umgesetzt
		Trendanalyse	umgesetzt
2	Ausbau und Förderung von Forschungs- und Bildungskompetenz	Bedarfsanalyse zu Bildungsangeboten	umgesetzt
		Forschungs- und Supportzentrum der beiden ETH	umgesetzt
		Cyber Defence Campus	umgesetzt
		Interdisziplinäre Forschung und Bildung zur Cybersicherheit	umgesetzt
		Förderung «Ethical Hacking»	umgesetzt
		Durchführung Pilot Bug Bounty Programm	umgesetzt
3	Schaffung von günstigen Rahmenbedingungen für eine innovative IKT-Sicherheitswirtschaft in der Schweiz	Aufbau von Innovationszentren	sistiert
		Think Tank Cyber-Sicherheit	umgesetzt

Tabelle 3: Massnahmen und Meilensteine inkl. Umsetzungsstand im Handlungsfeld «Kompetenzen- und Wissensaufbau». Quelle: Bundesrat, 2021

Massnahmen und Ziel: Das Handlungsfeld «Kompetenzen- und Wissensaufbau» umfasst die Massnahmen M1 bis M3, die gute Voraussetzungen und Bedingungen schaffen sollen für darauf aufbauende Aktivitäten.

Beurteilung der Leistungen: In allen Massnahmen wurden wichtige Umsetzungsvorhaben realisiert, in zwei Massnahmen Umsetzungsvorhaben sistiert. Im Handlungsfeld

«Kompetenzen- und Wissensaufbau» konnten die wesentlichen Leistungen erbracht («Outputs») und mit dem SSCC die gewünschte Vernetzung zwischen den Hochschulen, der Verwaltung, der Industrie und der Zivilgesellschaft etabliert werden. Auch zwischen der ETH und dem VBS wurde die Zusammenarbeit verstärkt, vor allem im Bereich der Cyber-Sicherheits-Ausbildung. Mehrere konkrete Projekte und Umsetzungsvorhaben in anderen Handlungsfeldern wurden bzw. werden bearbeitet («Outcome»).

Beurteilung der Wirkungen: Die Interviewpartner/innen weisen auf die hohe Bedeutung des Handlungsfeldes hin, mit dessen Outcome die Voraussetzungen geschaffen werden, um mit Cyber-Risiken angemessen umzugehen. Als wichtige Outcomes werden der Bericht des Cyber-Defence Campus (CYD) der armasuisse zur technologischen Entwicklung sowie die Konferenzen des CYD gemeinsam mit Hochschulen genannt; ebenso die Workshops des Swiss Support Center for Cyber-Security (SSCC), der gemeinsamen Initiative der EPFL Lausanne und der ETH Zürich sowie die Übersicht über die Bildungsangebote an den Hochschulen. Die Wirkung des Handlungsfeldes wird als indirekt spürbar bezeichnet. Diese Wahrnehmung deckt sich mit einer Untersuchung der Universität Oxford, die den sog. «Framework for Professional Training» in einer Maturitätsskala von eins bis fünf überdurchschnittlich hoch mit 4.5 einschätzt (University of Oxford, 2020, siehe auch Anhang A-5).

Fazit: Mit der mehrheitlichen Realisierung der Umsetzungsvorhaben im Handlungsfeld wurden die wesentlichen Leistungen erbracht; die gewünschten Strukturen wurden geschaffen und das Wissensnetzwerk wurde geknüpft. Outcomes werden erzielt, der Impact zeigt sich in den anderen Handlungsfeldern.

3.2 Bedrohungslage

Nr.	Massnahme	Umsetzungsvorhaben	Status
4	Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyberbedrohungslage	Identifikation der Zielgruppen und ihrer Bedürfnisse	umgesetzt
		Definition Produktekatalog pro Zielgruppe (Leistungskatalog)	umgesetzt
		Aufbau benötigter Quellen und Produktionsressourcen:	umgesetzt

Tabelle 4: Massnahmen und Meilensteine inkl. Umsetzungsstand im Handlungsfeld «Bedrohungslage». Quelle: Bundesrat, 2021

Massnahme und Ziel: Im Handlungsfeld «Bedrohungslage» findet sich die Massnahme M4, deren Ziel es ist, durch einen möglichst umfassenden Überblick zur Bedrohungslage eine wirksame, auf effektive Bedrohungen ausgerichtete, Prävention zu unterstützen.

Beurteilung der Leistungen: Die Massnahme ist weitgehend umgesetzt. Es wurden aus Sicht der Interviewpartner/innen die richtigen Umsetzungsprojekte realisiert. Diese seien gut dazu geeignet, Bund und weitere «Kunden/innen» zielgruppengerecht zu informieren.

Beurteilung der Wirkungen: Hier wurde insbesondere auf das Lageradar hingewiesen, das regelmässig und systematisch zur Information des Cyberausschusses des Bundesrats und der Kerngruppe Cyber über die Bedrohungslage erarbeitet wird. Ebenfalls positiv hervorgehoben wurden die Information der Öffentlichkeit über aktuelle Bedrohungen durch das NCSC sowie die Präventions- und Sensibilisierungsprogramme des Nachrichtendienstes des Bundes.

In den Interviews wiesen die Massnahmenverantwortlichen auf spezifische Anforderungen in Bezug auf die Bedrohungslage hin: Die hochdynamische Veränderung der Bedrohungslage stellt eine grosse Herausforderung für die fachliche Breite des Personals dar. Die Herausforderung bestehe darin, den entsprechenden Input als Voraussetzung zur Wirksamkeit leisten zu können. Neben der Bewältigung der geplanten operativen Arbeiten müssen ausreichend Kapazität vorhanden sein für eine schnelle Reaktion auf neue Situationen und für kontinuierliche Weiterbildung. In Zukunft müsse hier der Fokus noch stärker auf gut ausgebildeten Experten/innen liegen. Dies sei eine grosse Herausforderung, währenddessen die infrastrukturellen Aspekte zum Ausbau von Kapazitäten und Fähigkeiten sich bereits erfolgreich im Ausbau befinden.

Fazit: Die realisierten Umsetzungsprojekte schafften mit ihrem Outcome eine gute Basis, damit die zuständigen Stellen (v. a. der NDB und NCSC) Wirkung erzielen können. In der inhaltlichen Auswertung der Bedrohungslage sind weitere Fortschritte erwünscht. Als Herausforderung wird die angespannte Situation bezüglich verfügbarer Experten/innen betrachtet.

3.3 Resilienz-Management

Nr.	Massnahme	Umsetzungsvorhaben	Status
5	Verbesserung der IKT-Resilienz der kritischen Infrastrukturen (BABS in Zusammenarbeit mit den Fachämtern in regulierten Sektoren)	Umsetzung der geplanten bzw. laufenden Projekte zur Stärkung der Resilienz in den kritischen Teilsektoren	umgesetzt
		Etablierung einer akademischen Arbeitsgruppe für Cybersicherheit	umgesetzt
6	Verbesserung der IKT-Resilienz der Bundesverwaltung [7]	Sicherheitsvorgaben für agile Projektmethoden entwickeln	umgesetzt
		Sensibilisierungskampagne in der Bundesverwaltung	umgesetzt
		Sichere Datenübertragung (SCION)	umgesetzt
		Security Operations Center (SOC) BIT	umgesetzt
		Schaffung einer Schnittstelle zum ETH-Bereich	umgesetzt
7		Permanenter Austausch Kantone	sistiert
		Durchführung der Cyber-Landsgemeinde	umgesetzt

7 Der Bundesrat hat bereits 2015 den Auftrag zum Aufbau eines Sicheren Datenverbundnetz Schweiz (SDVN) gegeben (Bundesrat, 2015). Das entsprechende Projekt ist kein Umsetzungsvorhaben der NCS, wird jedoch eng verzahnt mit Massnahme Nr. 6 der NCS 2018 bis 2022.

Nr.	Massnahme	Umsetzungsvorhaben	Status
	Erfahrungsaustausch und Schaffung von Grundlagen zur Verbesserung der IKT-Resilienz in den Kantonen	Schaffung Schnittstelle ETH zu Kantonen	umgesetzt

Tabelle 5: Massnahmen und Meilensteine inkl. Umsetzungsstand im Handlungsfeld «Resilienz-Management». Quelle: Bundesrat, 2021

Massnahmen und Ziele: Kritische Infrastrukturen und Behörden müssen Massnahmen umsetzen, die bei möglichen Vorfällen die Schäden eindämmen und Ausfallszeiten minimieren. Die Massnahmen M5 bis M7 dienen der Identifikation und Umsetzung geeigneter Aktivitäten zur Erhöhung der Resilienz.

Beurteilung der Leistungen: Die Massnahmen sind in der Umsetzung gut fortgeschritten. Mit ihrem Fokus auf die Stärkung der Resilienz der kritischen Infrastrukturen, den Vorgaben für die Bundesverwaltung und dem Austausch unter den Kantonen konnten wichtige Fortschritte erzielt werden. Insbesondere bei der Massnahme M7 spielt das Engagement der Kantone eine grosse Rolle, die mit einem eigenen Umsetzungsplan die Cyber-Sicherheit zusätzlich stärken. Als wichtige Outputs wurde die Aktualisierung der Risiko- und Verwundbarkeitsanalysen in verschiedenen Sektoren genannt, die Stärkung der Resilienz der Bundesverwaltung durch die Cyberrisikenverordnung (CyRV) sowie die Durchführung der Cyber-Landsgemeinde und der Aufbau des Nationalen Testzentrums für Cybersicherheit in Zug. Punktuell wurde betont, dass das Handlungsfeld Resilienz-Management im nächsten Strategiezyklus unbedingt weiterzuführen sei.

Beurteilung der Wirkungen: Aus den Interviews mit den Massnahmenverantwortlichen zeigt sich, dass die gewählten Massnahmen als zweckmässig und richtig erachtet werden und dass sie weiterzuverfolgen sind. Bei den kritischen Infrastrukturen führen die Massnahmen zu Aktivitäten («Outcome»), die den Schutz vor Cyber-Risiken unterstützen; aktuell sind 27 verschiedene Teilsektoren gemäss bundesrätlicher Strategie zum Schutz kritischer Infrastrukturen (SKI-Strategie, Bundesrat, 2017) abgedeckt. Der schon in der Strategie NCS 2012-2017 gewählte risikobasierte Ansatz erwähnte die European Union Agency for Network and Information Security in ihrem Practice Guide als beispielhaft (ENISA, 2016). Nach Einschätzung der Universität Oxford ist die Schweiz in der Umsetzung derzeit noch auf einem Maturitätsgrad von drei («Established Stage») von fünf («Dynamic Stage») angelangt (University of Oxford, 2020). Während ein hoher Wissensstand und taugliche Strategien vorliegen, fehle es noch an den Kapazitäten, Wissen und Schutzstrategien flächendeckend rasch umzusetzen.

Der verfolgte Ansatz, der stark auf Eigenverantwortung der Betreiber/innen setzt, kommt allerdings an Grenzen, weil er den Akteuren/innen viel Handlungsspielraum lässt und diese selbst über den Umfang der Aktivitäten im Sinne des Outcomes entscheiden können.

Wünschenswert wäre aus Sicht der meisten Befragten eine höhere Verbindlichkeit, wie zum Beispiel Vorgaben innerhalb einer Branche oder verstärkte regulatorische Ansätze (siehe auch nachfolgendes Kapitel 3.4). Zu gleichen Schlüssen kommt ein externer Review zur Cyber-Sicherheit aus dem Jahr 2020 (University of Oxford, 2020). Eine Studie der ETH

Zürich (CSS, 2016) regt diesbezüglich an, sich mit anderen Modellen auseinanderzusetzen. Einige Stimmen betonen den hohen Stellenwert der Eigenverantwortung und betrachten ein «Mehr» an Regulierung skeptisch. Zudem ist zu beachten, dass die kritischen Teilsektoren unterschiedlich stark reguliert werden.

Fazit: Die Massnahmen der IKT-Resilienz wurden sowohl für die kritischen Infrastrukturen als auch für die Bundesverwaltung deutlich weiterentwickelt. Der Output wird als hoch eingestuft, das Problembewusstsein ist geschärft, aber die Wirkung auf die Zielgruppe fällt noch nicht zufriedenstellend aus. Es können bislang keine Mindeststandards durchgesetzt werden.

3.4 Standardisierung/Regulierung

Nr.	Massnahme	Umsetzungsvorhaben	Status
8	Evaluierung und Einführung von Minimalstandards	Entwicklung und Umsetzung von Minimalstandards für die IKT-Resilienz Entwicklung und Etablierung von Hilfsmitteln für KMU	umgesetzt
		Label Cyber-Safe für Gemeinden	umgesetzt
		Label für IT-Dienstleister	umgesetzt
9	Prüfung einer Meldepflicht für Cybervorfälle und Entscheid über Einführung	Studie über Grundmodelle von Meldepflichten	umgesetzt
		Grundsatzdiskussion mit Wirtschaft und Behörden	umgesetzt
10	Globale Internet-Gouvernanz	Treffen des hochrangigen Panels des UN-Generalsekretärs	umgesetzt
		Multistakeholder-Austauschplattformen zur Koordination auf nationaler Ebene	umgesetzt
11	Aufbau von Expertise zu Fragen der Standardisierung in Bezug auf Cybersicherheit	Stärkung von Standardisierungsvorhaben durch die Unterstützung der Hochschulen	umgesetzt
		Beitrag der Schweiz zur Verankerung des Themas Cybersicherheit in der internationalen Finanzpolitik	umgesetzt

Tabelle 6: Massnahmen und Meilensteine inkl. Umsetzungsstand im Handlungsfeld «Standardisierung/Regulierung». Quelle: Bundesrat, 2021

Massnahmen und Ziele: Die Massnahmen M8 bis M11 zur Standardisierung und Regulierung der NCS 2018-2022 fokussieren auf die Schaffung von Grundlagen, welche die Standardisierung und Regulierung unterstützen. Es wurden drei Labels entwickelt zur Cyber-Sicherheit von Gemeinden und KMU (Cyber-Safe), für IT-Dienstleister (Cyberseal) und für Technologieunternehmen (Digital Trust). Zur Regulierung wurde das Regulierungsvorhaben abgeschlossen, das bestimmte «Funkgeräte» wie Mobiltelefone, Tablets und andere Geräte, die über das Internet kommunizieren können und Anwendungen für das sog. Internet der Dinge aufweisen, ab 2022 bestimmten Anforderungen betreffend Cyber-Sicherheit unterstehen. Diese neuen Bestimmungen sollen einen Beitrag zu einem erhöhten

Schutz der Telekommunikationsnetze, zum verbesserten Schutz der Privatsphäre der Verbraucher/innen und zu einer Risikoreduktion für finanziellen Betrug leisten. Ferner wurden die Vernehmlassungsvorlagen zur Meldepflicht und zur Fernmeldeverordnung ausgearbeitet sowie das ISG durch die eidgenössischen Räte verabschiedet.

Beurteilung der Leistungen: Die Massnahmen wurden bislang nach Plan umgesetzt. In allen vier Massnahmen wurden die Umsetzungsvorhaben, welche die fachlichen Grundlagen aufbereiten und Vorschläge zur Ausgestaltung machen, durch die involvierten Ämter umgesetzt. Es wurde darauf hingewiesen, dass neben den Umsetzungsvorhaben technische Erkenntnisse der Hochschulen verschiedentlich direkt in Standards einfliessen (z. B. Beseitigen von Schwachstellen in der 5G-Technologie).

Die befragten Akteure/innen verweisen auf die anspruchsvolle Durchsetzung der Standards. Ursachen hierfür sind:

— *Freiwilligkeit*: Für weite Teile von Wirtschaft, Bevölkerung und Behörden basieren Massnahmen zum erhöhten Schutz von Cyber-Risiken auf Freiwilligkeit. Best Practices sind als Angebote und Teil von unterstützenden Rahmenbedingungen zu betrachten. Ein weitergehender Durchgriff zur Forcierung von Standards bestehe primär für kritische Infrastrukturen.

— *Gesetzgebungsprozess*: Die NCS 2018-2022 ist eine inhaltbezogene Strategie des Bundesrats. Sie kann lediglich gesetzgeberische Prozesse anregen und inhaltlich unterstützen. Ob solche und wie solche geführt werden sollen, unterliegt den politischen Entscheidungsträger/innen.

— *Vernetzung und dezentrale Strukturen*: Einheitliche Standards und Governance-Anforderungen können in den dezentral vernetzten Strukturen des Internets nicht einseitig durchgesetzt werden. Eine Vielzahl von Akteuren/innen (staatlich, halbstaatlich wie auch privat) müssen entsprechende Bemühungen unterstützen. Mit inhaltlich fundierten Vorschlägen und Diskussionsbeiträgen kann die Schweiz in internationalen Gremien hierzu Einfluss nehmen.

Die befragten Personen kommen zusammenfassend zum Schluss, dass die Massnahmenoutputs die erforderlichen Grundlagen zur Unterstützung von Standardisierung und künftig von möglicher Regulierung bereitgestellt haben. Eine Umsetzung und Verbreitung habe im Rahmen der NCS 2018-2022 und den im NCS-Netzwerk zusammengeschlossenen Akteuren/innen nicht massgeblich forciert werden können.

Beurteilung der Wirkungen: Die von den ausgeführten Umsetzungsvorhaben ausgehenden Wirkungen werden derzeit noch als gering beurteilt. Als «indirekte» Massnahme sei ein Angebot geschaffen worden, das durch die Zielgruppe als Nachfrage aufzunehmen sei. Mit den erzielten Fortschritten in den Regulierungen wird angenommen, dass diese Nachfrage forciert und die künftige Wirkung erhöht werden kann.

Die potenzielle Wirkung der erarbeiteten Standards werde darüber hinaus dadurch geschwächt, dass den Unternehmen verschiedene Standards von unterschiedlichen Akteuren/innen und Institutionen zur Auswahl stehen. Hier sei zu prüfen, ob im nächsten Strategiezyklus anstelle von selbst entwickelten Standards verstärkt auf international etablierte Standards und Frameworks zurückgegriffen werden könne.

Fazit: Zur Standardisierung wurden Grundlagen erstellt, die aufgrund bislang geringer Verbreitung und hoher Freiwilligkeit zu wenig Anwendung finden. Durch die bearbeiteten Regulierungsvorhaben entstehen Rahmenbedingungen, welche die Verbreitung der Grundlagen begünstigten. Outcome und Impact werden aktuell als stark eingeschränkt beurteilt, es sind jedoch gute Voraussetzungen gegeben zur künftigen Erhöhung der Wirkungen.

3.5 Vorfallbewältigung

Nr.	Massnahme	Umsetzungsvorhaben	Status
12	Ausbau von MELANI als Public-Private-Partnership für die Betreiberinnen kritischer Infrastrukturen	Gezielte Erweiterung des geschlossenen Kundenkreises	umgesetzt
		Entwicklung und Erweiterung von Dienstleistungen und Produkten	umgesetzt
		Ausbau der bestehenden Austauschplattform	umgesetzt
13	Aufbau von Dienstleistungen für alle Unternehmen	Schaffung einer nationalen Anlaufstelle Cyber	umgesetzt
		Zeitnahe Information im Ereignisfall über die Alertswiss-App	umgesetzt
14	Zusammenarbeit des Bundes mit relevanten Stellen und Kompetenzzentren	Übersicht über bestehende operative SOCs und CERTs inkl. Ansprechpartner/innen	umgesetzt
		Informationsaustausch mit CERTs und SOCs	umgesetzt
15	Prozesse und Grundlagen der Vorfallbewältigung des Bundes	Erarbeitung Cyberverordnung zur Cybersicherheit	umgesetzt
		Erstellung eines Sicherheitsvorfallbewältigungsprozesses für die Bundesverwaltung	umgesetzt

Tabelle 7: Massnahmen und Meilensteine inkl. Umsetzungsstand im Handlungsfeld «Vorfallbewältigung». Quelle: Bundesrat, 2021

Massnahmen und Ziele: Die vier Massnahmen M12 bis M15 zur Vorfallbewältigung sollen die rechtlichen, organisatorischen prozessualen und inhaltlichen Voraussetzungen schaffen, um Cybervorfälle schnell und wirksam bewältigen zu können.

Beurteilung der Leistungen: Die Umsetzungsvorhaben der vier Massnahmen sind praktisch vollständig realisiert worden; die Outputs der Umsetzungsvorhaben liegen vor. Die Interviewpartner/innen haben dabei insbesondere auf das NCSC als Anlaufstelle hingewiesen und auf die CyRV, welche die Kompetenzen zur Vorfallbewältigung innerhalb der Bundesverwaltung regelt. Das NCSC hat dabei im Jahr 2021 über 21'400 Meldungen zu Cyber-Vorfällen erhalten und geprüft (www.ncsc.admin.ch, Zugriff vom 31.01.2022). Die

sog. geschlossenen Kundenkreise wurden weiter ausgebaut, die Anlaufstelle als Privat-Public-Partnership hierdurch gestärkt.

Beurteilung der Wirkungen: In der Beurteilung der Wirkungen wird eine Unterscheidung vorgenommen betreffend Einzelfallbetrachtung und Gesamtwirkung zum Schutz vor Cyber-Risiken.

In der Einzelfallbetrachtung werden die zur Vorfallbewältigung aufgebauten Strukturen, Kompetenzen und Abläufe von den hierzu befragten Personen als wirksam eingeschätzt. Das NCSC verfügt über die erforderlichen Fähigkeiten und Strukturen, die deren Reaktionsfähigkeit sicherstellen. Zudem wird der Prozess der Vorfallbewältigung aufgrund der bearbeiteten Ereignisse laufend überprüft und wo nötig angepasst. Die gesetzlichen Rahmenbedingungen zur Vorfallbewältigung innerhalb der Bundesverwaltung sind durch die CyRV geklärt, während die Handlungsspielräume des NCSC für den zivilen Bereich mit der in Vernehmlassung befindlichen Vorlage zur Meldepflicht erweitert werden sollen. Die Armee hat parallel dazu einsatzbereite Kapazitäten zur Vorfallbewältigung im militärischen Bereich aufgebaut. Es resultieren als Outcome einsatzbereite Strukturen und Prozesse, die als dazu geeignet beurteilt werden, die Handlungsfähigkeit und Integrität von Behörden, Wirtschaft, kritischer Infrastruktur und Bevölkerung sicherzustellen.

Für die Bundesverwaltung wurde seit 2018 der Ablauf zur Vorfallbewältigung geklärt und mit der Cyberrisikenverordnung (CyRV) die Zuständigkeiten festgelegt. Die Führung zur Vorfallbewältigung wurde dem NCSC zugewiesen, was durch die Beteiligten als wichtiger Schritt zu einer agilen und wirksamen Vorfallbewältigung beurteilt wird. Seit Festlegung sind keine gravierenden Vorfälle aufgetreten. Die direkten Erfahrungen betreffend Zweckmässigkeit und unmittelbarer Wirksamkeit des definierten Vorgehens fehlen somit.

Eine effiziente Vorfallbewältigung kann eine präventive Wirkung entfalten und potenzielle Angriffe verhindern. Eine entsprechende Wirkung stellen die befragten Akteure/innen nicht fest; die Meldungen an das NCSC über Angriffe im Cyber-Raum steigen weiter stark an.

Fazit: Die ausgebauten Fähigkeiten, Abläufe und Kapazitäten zur Vorfallbewältigung stärken potenziell die Resilienz bei der Zielgruppe, jedoch in unterschiedlichem Masse. Eine präventive Wirkung ist hingegen nicht festzustellen.

3.6 Krisenmanagement

Nr.	Massnahme	Umsetzungsvorhaben	Status
16	Integration der zuständigen Fachstellen aus dem Bereich Cyber-Sicherheit in die Krisenstäbe des Bundes	Erweiterung Cyber-Glossar	umgesetzt
17	Gemeinsame Übungen zum Krisenmanagement	Schaffung von Grundlagen für Krisenübungen mit Cyberaspekten	umgesetzt
		Durchführung von sektorspezifischen Übungen	umgesetzt
		Einbringen von Cyber-Aspekten in übergreifende Krisenübungen	umgesetzt

Tabelle 8: Massnahmen und Meilensteine inkl. Umsetzungsstand im Handlungsfeld «Krisenmanagement». Quelle: Bundesrat, 2021

Massnahmen und Ziele: Mit den Massnahmen M16 und M17 entwickelt der Bund seine eigenen Fähigkeiten zum Krisenmanagement weiter und trainiert diese. Entsprechendes Wissen und Trainingsmöglichkeiten teilt er insbesondere mit der Zielgruppe der kritischen Infrastruktur.

Beurteilung der Leistungen: Das im Rahmen der Massnahmen M16 und M17 geplante Krisenmanagement wurde entwickelt. Abläufe zur Bildung und Arbeitsweise von Krisenstäben sind definiert, sodass eine operationelle Tätigkeit rasch aufgenommen werden kann. Es haben Krisenübungen gemeinsam mit der Finanzbranchen und im Gesundheitswesen stattgefunden. Der Delegierte des Bundes für Cybersicherheit wurde in den Bundesstab Bevölkerungsschutz (BSTB) integriert.

Beurteilung der Wirkungen: Die Beteiligten gehen davon aus, dass rasche Reaktionszeiten und ausreichender Interventionsdauer («Outcome») die Resilienz der Bundesverwaltung stärken. Die Handlungsfähigkeit durch tendenziell kürzere Ausfallzeiten bei Ereignissen wird als gestärkt betrachtet.

In der Regel sei klar, wie Angriffsziele ermittelt und Angriffe geplant würden. Nach jeder Krise finde ein Debriefing statt und es werde angestrebt, dass die «lessons learnt» in die Prozesse und Strukturen einflössen. Ob und wie weit das eine präventive Wirkung auslöse, können die befragten Personen nicht klar einschätzen. Die Handlungsfähigkeit von Krisenstäben werde gezielt geschult und mit Übungen getestet. Die langfristigen Wirkungen der Übungen in den bisherigen Formen werden allerdings als unklar beschrieben.

Fazit: Reaktions- und Interventionsfähigkeiten der Bundesverwaltung wurden gestärkt, die durchgehende Handlungsfähigkeit von Behörden und Verwaltung durch Regelung von Verantwortlichkeiten und Trainings besser gesichert. Die Komplexität zur raschen Intervention bleibt hoch. Die Wirkungen der Massnahmen werden sich im Rahmen künftiger Ereignisse zeigen.

3.7 Strafverfolgung

Nr.	Massnahme	Umsetzungsvorhaben	Status
18	Fallübersicht Cyber-Kriminalität (fedpol und KKPKS mit NEDIK)	Fallübersicht Cyber-Kriminalität (PICSEL)	Testphase läuft
		Erarbeitung einer justiziellen Fallübersicht	umgesetzt
		Aufzeigen von Entwicklungen, Szenarien und Auswirkungen	umgesetzt
19	Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung (fedpol als Teil der KKPKS)	Rechtliche Grundlagen für die Zusammenarbeit und Verrechnung von Leistungen zw. Bund und Kantonen und unter Kantonen	umgesetzt
20	Ausbildung (KKPKS inkl. fedpol, SSK inkl. BA)	Umsetzung der Ausbildungskonzepte	umgesetzt
21	Zentralstelle Cyber-Kriminalität (fedpol)	Keine Meilensteine bis Q2 2021	

Tabelle 9: Massnahmen und Meilensteine inkl. Umsetzungsstand im Handlungsfeld «Strafverfolgung». Quelle: Bundesrat, 2021

Massnahmen und Ziele: In der Cyber-Strafverfolgung verfügt der Bund über einen Auftrag zur Unterstützung der interkantonalen Zusammenarbeit als auch über direkte Strafverfolgungskompetenzen. Das Bundesgericht hat diese Strafverfolgungskompetenzen gegenüber den Kantonen bereits mehrfach bestätigt, u. a. im Kampf gegen das organisierte Verbrechen und schwere Wirtschaftskriminalität, die den Cyber-Raum nutzen. Die Bekämpfung findet gemeinsam mit den Kantonen statt mittels des sog. Cyber-Board (Cyber-STRAT und Cyber-CASE). Seit 2018 hat eine Intensivierung des Informations- und Wissensaustausches stattgefunden, in dessen Zentrum das Netzwerk digitale Ermittlungsunterstützung Internetkriminalität (NEDIK) steht. In dieses müssen 26 autonome kantonale Organisationen mit ihren eigenen Abläufen, IT-Systemen, Vorleistungen zur Bekämpfung von Cyber-Kriminalität etc. integriert werden. Das Bundesamt für Polizei (fedpol) leistet mit den Massnahmen M18 bis M21 Grundlagenarbeit, fördert die Ausbildung und unterstützt die Koordination.

Beurteilung der Leistungen: Die Massnahmen M18 bis M21 schreiten insgesamt nach Plan voran und die operationelle Umsetzung wird schrittweise mit den Kantonen aufgebaut. Die Fallübersicht PICSEL befindet sich in einer Testphase. Mit NEDIK steht ein Netzwerk zur Ermittlungsunterstützung zur Verfügung und ein Ausbildungsgang wurde konzipiert. Die Vernetzung der Kantone ist hier gut etabliert, ihre Beiträge für NEDIK fallen aber unterschiedlich aus. Sämtliche Massnahmen betreffend Strafverfolgung sind noch nicht vollständig abgeschlossen. So stelle ein nach wie vor unvollständiges Lagebild (Umsetzungsvorhaben Fallübersicht «PICSEL») eine hohe Herausforderung dar. Zuletzt wurden mit Blick auf die Aktivitäten im Jahr 2022 Projektanpassungen diskutiert, die Entscheide dazu stehen noch aus.

Beurteilung der Wirkungen: Insbesondere mit NEDIK sei ein bedeutsamer Fortschritt in der schweizweit koordinierten Bekämpfung von Cyber-Kriminalität realisiert worden. Für NEDIK als auch die weiteren abgeschlossenen Umsetzungsvorhaben sei die Zeitdauer seit Abschluss zu kurz, dass deren Outcome festzustellen und Wirkungen nachzuweisen seien.

Die befragten Akteure/innen betonen allesamt die hohe Wichtigkeit eines umfassenden und aktuellen polizeilichen Lagebilds. Die Massnahmen der NCS seien dabei präventiv angelegt und primär polizeilich geprägt. Es fehle der NCS daher bislang an einer justiziellen Dimension. So weisen auch die befragten «Nutzervertreter» der Kantone auf verschiedene Hürden in Organisationsfragen, kantonalen Rechtsgrundlagen sowie Aufteilung zwischen Ermittlungs- und Strafverfolgungsbehörden hin. Diese seien für eine volle Nutzung der geschaffenen Möglichkeiten zu überwinden.

Bezogen auf die rechtliche Klärung sehen befragte Akteure/innen das Erfordernis für den Gesetzgeber, sich bezüglich Cyber-Kriminalität von der Hardware stärker zu lösen. Die «CIA-Triade» [8] sei im Kontext von dezentralen und ortsunabhängigen Speichermedien mit Echtzeitverbindungen anzuwenden. Bei Strafverfolgungsbehörden seien verschiedene Ansätze hierzu wie «Durchgriffsprinzip» (Rechtsfortentwicklung) zur Sicherstellung/Beweiserhebung am Ort der Verfügbarkeit und ein «Swiss CLOUD-Act» (Rechtsdurchsetzung), die sämtlichen international tätigen Unternehmen mit Niederlassung in der Schweiz zur Datenherausgabe nach Schweizer Recht verpflichten würde. In den eidgenössischen Räten wurden in Vergangenheit entsprechende Vorstösse eingereicht.

Fazit: Mit der Koordination und Stärkung der interkantonalen Zusammenarbeit in der Cyber-Strafverfolgung kann diese effizienter und effektiver mit präventiver Ausrichtung ausgestaltet werden. Technische, rechtliche, prozessuale und andere Unterschiede zwischen den föderal organisierten Strafverfolgungsbehörden und begrenzte Kapazitäten hemmen derzeit mögliche Outcomes und Wirkungen. Die Massnahmen zur Kapazitätserhöhung laufen. Es bestehen überdies justizielle Defizite in der prozessualen Umsetzung der Cyber-Strafverfolgung.

3.8 Cyber-Defence

Nr.	Massnahme	Umsetzungsvorhaben	Status
22	Ausbau der Fähigkeiten zur Informationsbeschaffung und Attribution	Fähigkeiten zur Informationsbeschaffung und Attribution	umgesetzt
		Durchführung einer spezifischen Ausbildung in der Cyberabwehr (Armee)	umgesetzt
23	Fähigkeit zur Durchführung von aktiven Massnahmen im Cyber-Raum gemäss NDG und MG	Nutzung der im Kontext vom NDG entwickelten Kapazitäten von FUB-ZEO	umgesetzt
24	Gewährleistung Einsatzbereitschaft der Armee über alle Lagen im Cyber-Raum und Regelung ihrer subsidiären Rolle zur Unterstützung der zivilen Behörden	Projektabschluss «Aufbau Cyber»	umgesetzt

Tabelle 10: Massnahmen und Meilensteine inkl. Umsetzungsstand im Handlungsfeld «Cyber-Defence». Quelle: Bundesrat, 2021

Massnahmen und Ziele: Art. 6b der Cyberrisikenverordnung definiert Cyber-Defence als die «Gesamtheit der nachrichtendienstlichen und militärischen Massnahmen, die dem

[8] CIA-Triade: «Confidentiality», «Integrity» und «Availability»

Schutz der für die Landesverteidigung kritischen Systeme, der Abwehr von Cyber-Angriffen, der Gewährleistung der Einsatzbereitschaft der Armee in allen Lagen und dem Aufbau von Kapazitäten und Fähigkeiten zur subsidiären Unterstützung ziviler Behörden dienen; dazu zählen aktive Massnahmen zur Erkennung von Bedrohungen, zur Identifikation von Angreifern und zur Störung und Unterbindung von Angriffen». Mit den drei Massnahmen M22, M23 und M24 wird das umfassende Aufgabenfeld der Cyber-Defence mit dem Aufbau der erforderlichen Fähigkeiten und personellen Kapazitäten unterstützt.

Beurteilung der Leistungen: Die Massnahmen M22 und M23 wurden vollständig sowie die Massnahme M24 weitgehend umgesetzt. Als wichtige Schritte werden der Entscheid des Bundesrates zur Weiterentwicklung der Führungsunterstützungsbasis (FUB) der Armee in ein Kommando Cyber sowie die neue Strategie Cyber VBS 2021-2024 (VBS, 2021), die die Basis legt für die Ausrichtung des Departementes im Bereich Cyber-Defence genannt. Die Armee verfügt über die Fähigkeit zur Durchführung von aktiven Massnahmen im Cyber-Raum. Ihre Einsatzbereitschaft im Cyber-Raum ist über alle Lagen gewährleistet. Ebenso ist die Cyber-Ausbildung für die Angehörigen der Armee umgesetzt; der Aufbau des Cyber Training Centers mit einem Ausbildungsangebot, das Dritten offenstehen wird, verzögert sich bis ca. 2026.

Beurteilung der Wirkungen: Mit den im Handlungsfeld erbrachten Outputs wird aus Sicht der Interviewpartner/innen eine klare Wirkung erzielt und das Thema Cyber-Defence werde klar als einer der drei Pfeiler der Strategie wahrgenommen. Der NDB und die Armee konnten in der beurteilten Strategieperiode eine deutliche Entwicklung durchlaufen und eigene Fähigkeiten deutlich ausbauen. Sie haben die Grundlagen geschaffen, die erforderlichen Outcomes künftig erbringen zu können.

Fazit: Mit den realisierten Umsetzungsprojekten wurden die Fähigkeiten der Armee und des Nachrichtendienstes des Bundes sowie ihre Einsatzbereitschaft im Cyber-Raum klar gestärkt. Die Strategie Cyber VBS stärkt dies zusätzlich mit weiteren Massnahmen. Ausstehend ist die Ausdehnung des Ausbildungsangebots zugunsten Dritter. Damit soll die Interoperabilität bzw. die Wirkung im Sicherheitsverbund gestärkt werden.

3.9 Cyber- Aussen- und -Sicherheitspolitik

Nr.	Massnahme	Umsetzungsvorhaben	Status
25	Aktive Mitgestaltung und Teilnahme an Prozessen der Cyber-Aussensicherheitspolitik	Teilnahme an UNO-Prozessen	umgesetzt
		Interessenvertretung im Rahmen der OSZE (staatliche Vertrauensbildung)	umgesetzt
		Aufbau und Etablierung des Geneva Dialogue on Responsible Behavioral Cyberspace	umgesetzt
		Verfolgung der Entwicklungen in der Europäischen Union (insbesondere im Europäischen Auswärtigen Dienst und ENISA)	umgesetzt
		Engagement zur Förderung eines offenen und freien Cyber-Raums	umgesetzt

Nr.	Massnahme	Umsetzungsvorhaben	Status
26	Internationale Kooperation zum Auf- und Ausbau von Kapazitäten im Bereich Cyber-Sicherheit	Durchführung von Workshops mit regionalen Organisationen	umgesetzt
		Workshops zum Aufbau von Institutionen und Cyberaussensicherheitsstrukturen	umgesetzt
27	Bilaterale politische Konsultationen und multilaterale Dialoge zu Cyber-Aussensicherheitspolitik	Sino-European Cyber Dialogue (SECD)	umgesetzt
		MENA Cyber-Security Forum	umgesetzt

Tabelle 11: Massnahmen und Meilensteine inkl. Umsetzungsstand im Handlungsfeld «Cyber-Sicherheitspolitik». Quelle: Bundesrat, 2021

Massnahmen und Ziele: Die Massnahmen zur Cyber-Aussen- und -Sicherheitspolitik (M25, M26 und M27) beabsichtigen eine aktive Positionierung der Schweiz in der internationalen Cyber-Sicherheitspolitik. Sie sind Teil der Aussenpolitik und nicht darauf angelegt, unmittelbare Wirkungen auf die Zielgruppen zu entfalten.

Beurteilung der Leistungen: Die Massnahmenverantwortlichen haben seit 2018 verschiedene Anpassungen an den Massnahmen vorgenommen mit dem Ziel einer Fokussierung auf Massnahmen, die einen Beitrag zur Strategie erkennen lassen. Dieser Beitrag bestehe darin, dass eine Brücke zwischen internationalen Akteuren/innen und der Schweiz gebildet werden solle. Im Rahmen der Massnahmen M26 und M27 wurde ein Dialog aufgebaut resp. befindet sich im Aufbau mit Schweden, der Niederlanden, Österreich, Grossbritannien, Japan, USA, Israel, China sowie multilateral mit der ASEAN. Workshops zum Capacity Building wurden in Zusammenarbeit mit der ständigen Mission Kenias bei den Vereinten Nation (UN) und weiteren afrikanische Staaten und Organisationen durchgeführt (Quelle: Zusammenstellung EDA vom 26.01.2022).

Beurteilung der Wirkungen: Bezüglich des Outcomes habe sich gezeigt, dass Diskussionsbeiträge für multilaterale Gremien mehr Beachtung gefunden haben als der bilaterale Austausch zwischen Staaten. Dabei habe sich die OECD, entgegen der ursprünglichen Wahrnehmung, als eine geeignete Arbeits- und Wirkungsebene erwiesen. Ab dem 1. Januar 2022 wird zudem der Delegierte des Bundesrats der OECD-Arbeitsgruppe «Security in Digital Economy» vorsitzen. Einen relevanten Beitrag habe die NCS 2018-2022 zur Schaffung des «Geneva Dialogue» für verantwortungsvolles Verhalten im Cyber-Raum[9] geleistet.

In einer aktuellen Bevölkerungsumfrage (SOTOMO, 2022) äussern sich 56 % der Befragten dahingehend, dass der Bund die Interessen der Schweiz zur multilateralen Regulierung im Cyber-Raum gut vertreten könne.

Durch die aktive und strategische Beteiligung der Schweiz in einem internationalen Dialog würden die internationalen Kontakte aus den anwendungsorientieren Handlungsfeldern (insb. betreffend Bedrohungslage, Strafverfolgung und Cyber-Defence) flankiert und die Basis zur Zusammenarbeit zusätzlich gestärkt. Dieser Outcome unterstützt andere Handlungsfelder darin, deren Outcomes hin zu den angestrebten Impacts zu realisieren.

[9] www.genevadialogue.ch, Zugriff vom 10. Januar 2022

Fazit: Der Cyber-Aussen und -Sicherheitspolitik fällt eine indirekte Wirkung zum Schutz der Zielgruppen zu. Schweizer Behörden und weitere zentrale Akteure/innen (im Rahmen des «Geneva Dialogue») wurden in einem unterstützenden Sinn der NCS 2018-2022 international in den Diskussionen zur Cyber-Governance positioniert.

3.10 Aussenwirkungen und Sensibilisierung

Nr.	Massnahme	Umsetzungsvorhaben	Status
28	Erstellung und Umsetzung eines Kommunikationskonzepts zur NCS	Erarbeitung eines Kommunikationskonzeptes zur NCS	umgesetzt
29	Sensibilisierung der Öffentlichkeit für Cyber-Risiken	Entwicklung und Durchführung einer nationalen Awareness-Kampagne	umgesetzt
		Informationsplattform zu Cyberrisiken	umgesetzt

Tabelle 12: Massnahmen und Meilensteine inkl. Umsetzungsstand im Handlungsfeld «Aussenwirkungen». Quelle: Bundesrat, 2021

Massnahmen und Ziele: Die zwei Massnahmen M28 und M29 bilden das Handlungsfeld «Aussenwirkung und Sensibilisierung». Sie richten sich nach aussen an die Bevölkerung und die Wirtschaft und dienen zum einen der Information über die Strategie und deren Umsetzung und zum anderen der Information über aktuelle Entwicklungen und Vorfälle.

Beurteilung der Leistungen: Auf Basis des Kommunikationskonzepts und diversen Umsetzungsvorhaben haben seit 2018 verschiedene Awareness-Kampagnen innerhalb und ausserhalb der Bundesverwaltung stattgefunden, auch in Zusammenarbeit mit der Schweizerischen Kriminalprävention (SKP). Parallel dazu wurde die Website mit den Informationen zuhanden der Bevölkerung, der Unternehmen, der Spezialisten und der Behörden genannt sowie die Halbjahresberichte, die «End-of-Week Reports», ausgebaut.

Die Umsetzungsprojekte der beiden Massnahmen wurden zu grossen Teilen realisiert. Aufgrund der verfügbaren Ressourcen mussten zur Kommunikation wenige Schwerpunkte gebildet werden. Mit Hilfe der kommunikativen Schwerpunkte aus der NCS- Umsetzung sucht der Bund nicht nur den direkten Kontakt mit den Zielgruppen, er arbeitet mit verschiedenen Partnern zusammen und nutzt bereits bestehende Gefässe und Plattformen von Dritten. Aus den durchgeführten Umsetzungsvorhaben ergeben sich Ideen und Konzepte zur Weiterführung und anhaltenden Sensibilisierung, hierfür fehlte es bislang an Ressourcen.

Beurteilung der Wirkungen: Die Befragten konstatieren als Outcome eine deutlich verbesserte Aussenwirkung und führen das auf die laufenden kommunikativen Aktivitäten des NCSC, auf die von Partnern unterstützten Awareness-Kampagnen und Umfragen sowie auf die spezifische Kommunikation über ausgewählte Projekte zurück. Auswertungen anhand von sog. Werbeanzeigeäquivalenten und Zugriffen, Verweildauern und Absprungraten weisen auf eine nationale Reichweite und eine gute Ansprache verschiedener Teilsegmente der Zielgruppen hin. Die schweren Vorfälle in den letzten Monaten haben geholfen, das Augenmerk der Zielgruppen auf das Thema zu lenken.

Nach wie vor Handlungsbedarf verortet man bei der Bevölkerung und den KMU. Hemmend wirke hier die passive Haltung bei Teilen der Zielgruppen, die sich erst im Ereignisfall mit den Themen auseinandersetzen.

Punktuell sieht man Handlungsbedarf bei der Information über die Zuständigkeiten; teilweise herrsche in der Bundesverwaltung und im Parlament Unklarheit darüber, welche Gremien für welche Aufgaben zuständig seien, etwa in der Abgrenzung zwischen dem NCSC und dem Bereich Digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei.

Hingewiesen wurde auf die mannigfaltigen Aktivitäten verschiedener Kommunikationsstellen der Bundesverwaltung ausserhalb der NCSC, die ebenfalls das Thema Schutz vor Cyber-Risiken zum Inhalt haben, aber oft nicht mit dem NCSC abgesprochen sind. Hier soll eine bessere Koordination angestrebt werden, um Outcome und letztlich gewünschte Wirkung bei den Zielgruppen zu verstärken.

Fazit: Die Aussenwirkung wurde durch die klar verstärkte Kommunikation deutlich verbessert, was vor allem bei der Wirtschaft und bei den kritischen Infrastrukturen wahrgenommen wird. Bevölkerung und KMU werden noch zu wenig gut erreicht. Auch bei der Koordination der Kommunikationsaktivitäten der verschiedenen Akteure/innen besteht Handlungsbedarf. Der Impact aus dem Handlungsfeld entsteht indirekt.

4 Wirkungen auf die Zielgruppen

Die NCS 2018-2022 folgt der Vision, die Resilienz von Bevölkerung, Wirtschaft und Staat gegenüber Cyber-Bedrohungen zu erhöhen, um deren Handlungsfähigkeit und Integrität zu gewährleisten. Im Rahmen der Wirksamkeitsüberprüfung wurde untersucht, ob und wie bei diesen Zielgruppen entsprechende Wirkungen festzustellen sind. Die nachstehenden Darlegungen und Beurteilungen finden sich insbesondere auf der Outcome-Ebene der Strategie.

Konkret wurden die nachfolgenden Fragen analysiert:

Nutzen: Inwiefern erreichen die Massnahmen der NCS die Zielgruppen im gewünschten Mass (bspw. nutzen die Zielgruppen die Massnahmen bzw. die etablierten Strukturen und Prozesse sowie die erarbeiteten Produkte, Dienstleistungen, Netzwerke, Methoden)?

Angestrebte Wirkungen Zielgruppen: Inwiefern werden angestrebte Wirkungen der NCS 2018-2022 wie bspw. die Befähigung der Akteure/innen oder die Stärkung der Resilienz bei den vier explizit adressierten Zielgruppen (kritische Infrastrukturen, Behörden, Wirtschaft, Bevölkerung) erreicht?

Wirkungen weitere Akteure/innen: Inwiefern zeigen sich darüber hinaus bei weiteren Akteuren/innen Wirkungen und wie sind diese einzustufen?

4.1 Behörden

Entwicklung und Umsetzung der Strategie sind aus Sicht der befragten Personen gut in der Verwaltung und den Behörden verankert. Handlungsfelder und Massnahmen bildeten ein stimmiges Paket, was aber nicht überraschend sei, da sich die Gliederung und die Massnahmen stark an der Verwaltungsstruktur orientiere. Ebenfalls hervorgehoben wird die dank der NCS verbesserte Zusammenarbeit zwischen Bund und Kantonen.

Überall dort, wo die Akteure/innen bzw. Zielgruppen eng in die NCS eingebunden seien, wird eine gute Wirkung konstatiert, das trifft für die Behörden im Besonderen zu. Hier leiste die Strategie wesentliche Sensibilisierung. Wo Aufgaben klar zugeordnet werden, zeige die Strategie ebenfalls Wirkung. Wo sie lediglich sensibilisiere, löse sie allenfalls kurzfristige Wirkung aus.

Es wurde darauf hingewiesen, dass die nationale Strategie von anderen Behörden etwa in den Kantonen aufgegriffen wurde und dort eigene Projekte zum Umgang mit Cyber-Risiken ausgelöst wurden. Offen sei diesbezüglich die Situation der Städte und grossen Gemeinden, hier wird ein Handlungsbedarf vermutet. Diesen Handlungsbedarf, der durch Medienberichte in den vergangenen Monaten sichtbar wurde, nimmt auch die Bevölkerung wahr. Befragt nach der Cyber-Sicherheit von Verwaltung und kritischer Infrastruktur, schätzen lediglich 28 % der befragten Personen die Sicherheit als ausreichend ein (Sotomo, 2022).

Auch in Bezug auf die Behörden wurde die Bedeutung der horizontalen Vernetzung betont. Diese wird als noch zu wenig stark eingeschätzt; Personen, die sich in verschiedenen Bereichen mit denselben Themen auseinandersetzen, sollen sich besser vernetzen können.

Fazit: Die Bundes- und Kantonsbehörden sind gut in die Strategie und die Umsetzungsprojekte eingebunden. Der Output trägt zur Sensibilisierung bei. Bei klaren Zuständigkeiten und Verantwortlichkeiten erzeugt sie Wirkung.

4.2 Kritische Infrastruktur

Mehrheitlich sind die Interviewpartner/innen der Meinung, dass bei den kritischen Infrastrukturen die Sensibilisierung weiter vertieft werden konnte. Die Betreiber/innen kritischer Infrastrukturen sind branchenspezifisch umfassend eingebunden über das Projekt Schutz Kritischer Infrastrukturen (SKI) beim Bundesamt für Bevölkerungsschutz sowie über die entsprechenden Massnahmen der Kantone gemäss deren Umsetzungsplan zur NCS, den der Sicherheitsverbund Schweiz (SVS) erarbeitete.

Der Schutz vor Cyber-Risiken werde von den Betreibern/innen kritischer Infrastrukturen gegenüber früher deutlich ernster genommen. Innerhalb der Branchen mit grossen Akteuren/innen sei man zusammengerückt und tausche sich enger aus, es wird ein hohes Engagement wahrgenommen. Bei kleinteilig strukturierten Branchen mit vielen unterschiedlichen Akteuren/innen habe das bis jetzt weniger stattgefunden, hier sei das Problembewusstsein weniger stark ausgeprägt.

Den Eindruck eines unterschiedlichen und teilweise zu geringen Problembewusstseins unterstreichen verschiedene Studien, Analysen und Umfragen. So wird in einer Studie des Bundesamtes für Energie dem schweizerischen Stromversorgungssektor ein tiefer Maturitätsgrad bezüglich Umsetzung von empfohlenen Massnahmen zugeschrieben (BFE, 2021). Das NCSC setzte sich im Halbjahresbericht 2020/2 mit den Gefährdungen für das Gesundheitswesen auseinander und empfahl verschiedene zusätzlichen Schutzmassnahmen zur Umsetzung (NCSC, 2021a). Und eine Befragung von 1'254 Personen aus der Deutschschweiz im Herbst 2021 (Sotomo, 2022) ergab, dass 72 % der Befragten die kritische Infrastruktur und die Behörden in der Schweiz als nicht ausreichend geschützt gegenüber Cyber-Risiken ansehen.

Einen Zielkonflikt nehmen die Befragten wahr zwischen dem angestrebten eigenverantwortlichen Handeln der Betreiber/innen kritischer Infrastrukturen und der fehlenden Verbindlichkeit beim Umsetzen von Schutzmassnahmen. Hier werde das Potenzial der Wirkung noch nicht ausgeschöpft. Zu prüfen seien andere Wege, wie die Umsetzung der Massnahmen gefördert werden könne. Genannt wird eine verstärkte Regulierung, wobei diese von einem Vorsorgeprinzip über eine Revisionspflicht (ähnlich zur Buchführung) bis hin zum Einhalten eines gesetzlichen Mindeststandard reichen können. Ein weiterer Ansatz besteht in intensivierten Analysen von gefährlichen Ereignissen, deren Ursachen und tieferliegenden Gründen mit dem Ziel, künftige Gefahrensituationen und Ereignisse zu ver-

hindern. Die aktuelle Vernehmlassung zur Einführung einer Meldepflicht bei Cyber-Angriffen für Betreiberinnen und Betreiber von kritischen Infrastrukturen zeigt einen möglichen Ansatz auf.

Fazit: Die Betreiber/innen kritischer Infrastrukturen sind sensibilisiert und eng in die Massnahmen bzw. Umsetzungsprojekte eingebunden; es sind aber klare Unterschiede zwischen den Sektoren erkennbar. Die aus der Strategie erbrachten Leistungen reichen noch nicht aus, sämtliche kritischen Infrastrukturen angemessen zu schützen.

4.3 Bevölkerung

Viele Befragte erkennen eine erhöhte «Awareness» der Bevölkerung für Cyber-Sicherheit. So gehen Einschätzungen durch die massnahmenverantwortlichen Personen davon aus, dass Sensibilisierungskampagnen und Öffentlichkeitsarbeit innerhalb der NCS und durch das NCSC eine den Mitteln angemessene Reichweite entfalten konnten. Eine empirische Evidenz hierfür als auch für die Beiträge parallellaufender Initiativen und Kampagnen zur Sensibilisierung[10] fehle jedoch.

Die Meldungen aus der Bevölkerung an das NCSC steigen laufend (2021 insgesamt über 21'400 Meldungen), wobei der Zusammenhang einer wachsenden Zahl von Angriffen und erhöhter Sensibilisierung zur Beurteilung und Meldung eines Ereignisses unklar sei. Das NCSC diene der Bevölkerung teilweise zur Orientierung, wodurch eine Sensibilisierung entstehe, die bestimmte Kreise der Bevölkerung erreiche. Dabei sei zu berücksichtigen, dass unterschiedliche Bevölkerungsgruppen nicht nur über unterschiedliche digitale Kompetenzen verfügen, sondern die IKT-Instrumente auch unterschiedlich Nutzen (siehe bspw. Universität Zürich, 2020). In der Vorfallbewältigung sei das NCSC hingegen nur teilweise auf die Bevölkerung ausgerichtet.

Was die NCS bislang nicht leiste resp. nicht leisten könne, sei eine Sensibilisierung und «Cyber-Grundbildung», die bei Jugendlichen zu erfolgen habe. Darin sehen insbesondere befragte Vertreter/innen der Wirtschaft den grössten und langfristigen Hebel zum Schutz der Bevölkerung vor Cyber-Risiken. Die Möglichkeiten der NCS hierzu werden jedoch auch als begrenzt betrachtet, zumal das Bildungswesen grundsätzlich im Verantwortungsbereich der Kantone liegt.

Die gemäss verschiedenen Aussagen mangelhafte «Cyber-Grundbildung» fällt zusammen mit einer insgesamt als zu niedrig wahrgenommenen digitalen Kompetenz (Sotomo, 2022). Dabei gehen in einer Bevölkerungsumfrage 60 % der Befragten davon aus, dass die Entwicklung der digitalen Kompetenz im Bildungswesen zu langsam erfolge.

Fazit: Die Massnahmen der NCS 2018-2022 erreichen nur sehr punktuell die Bevölkerung, die Breitenwirkung zur Sensibilisierung ist bislang nicht eingetreten.

[10] Es besteht kein Überblick über entsprechende Initiativen und Kampagnen Dritter.

4.4 Wirtschaft

In den geführten Gesprächen zum Schutz der Wirtschaft bestand Einigkeit, dass grosse, internationale Unternehmen sich besser gegen Cyber-Risiken schützen. Diese bringen punktuell ihre Fähigkeiten und Erfahrungen in die NCS ein. Die KMU als grösster Teil der Schweizer Wirtschaft seien hingegen zu wenig geschützt und hätten ein zu niedriges Bewusstsein für die Bedrohungen im Cyber-Raum. Die Anstrengungen zur Erhöhung des Schutzes halten nach Einschätzungen von Experten/innen nicht Schritt mit der Zunahme der Cyber-Angriffe. Dabei stünden zwei Schwachstellen im Vordergrund:

— *Angriffsziel*: Unternehmen stuften sich als «uninteressante» Angriffsziele ein.

— *Bewusstsein für Daten*: Das Bewusstsein für Daten fokussiere stark auf den Datenschutz, während dessen Verfügbarkeit und die Integrität von Daten (und Geschäftsprozessen) vernachlässigt würden.

Aktuelle Befragungen bei den Unternehmen bestätigen, dass diese gegenüber Cyber-Angriffen häufig nicht ausreichend geschützt sind (gfs-Zürich, 2021). So ist der Anteil angegriffener Unternehmen mit erheblichem Aufwand zur Schadensbehebung von 25 % im Jahr 2020 per Ende 2021 auf 33 % angestiegen (gfs-Zürich, 2021). Eine Zunahme der Angriffe verzeichnet auch das NCSC. Betroffen sind vermehrt bekannte, international agierende Unternehmen (NCSC, 2021b). Hochgerechnet wurden in der Schweiz bereits rund 55'000 Unternehmen aus dem Cyber-Raum mit gravierenden Folgen angegriffen.

Die Befragung durch gfs-Zürich (2021) weist zudem einen starken Zusammenhang zwischen der Unternehmensgrösse und dem Bewusstsein für Cyber-Risiken auf. Auch die Bevölkerung schätzt die digitale Kompetenz in den Unternehmen sehr unterschiedlich ein (Sotomo, 2022). So schätzten in einer aktuellen Befragung 78 % die digitale Kompetenz grosser Unternehmen als hoch ein. Betreffend die KMU stimmten hingegen nur 45 % der Befragten zu, dass deren digitale Kompetenz hoch sei. Mit Bezug auf die Cyber-Sicherheit erwarten 87 % der Befragten, dass die staatlichen Anstrengungen zum Schutz der Unternehmen vor Cyber-Angriffen erhöht werden.

Zu beobachten sei, dass die Unternehmen derzeit stark in ihren technischen Schutz investierten, die pandemiebedingten Anforderungen für das Arbeiten von zu Hause habe diese Entwicklung beschleunigt. Es treten aber weiterhin organisatorische Mängel auf. So nehmen bspw. die Fälle des sog. «CEO-Betrugs» weiter stark zu. Die Massnahmen der NCS 2018-2022 seien zu wenig wirksam, um eine umfassende Verbesserung der Schutzaktivitäten bei den KMU auszulösen. Zwar habe die NCS 2018-2022 durch verschiedene Massnahmen (bspw. Handlungsfeld «Kompetenzen- und Wissensaufbau», Handlungsfeld «Standardisierung/Regulierung», Handlungsfeld «Aussenwirkungen und Sensibilisierung») gute Grundlagen geschaffen. Es fehle jedoch an Massnahmen und Möglichkeiten (finanziell, organisatorisch, regulatorisch etc.), um eine umfassende Verbreitung und Anwendung von entwickelten Grundlagen und Best Practices voranzutreiben.

Als eine sehr wirksame Massnahme zur Einbindung von Unternehmen wird deren Aufnahme in den geschlossenen Kundenkreis des NCSC gesehen. Dabei sei als Outcome

von einer Multiplikatorwirkung der eingebundenen Unternehmen auszugehen. In Verbindung mit der Publizität bei schweren Vorfällen bei bekannten Unternehmen wird hiermit eine hohe Erwartung an die Sensibilisierungswirkungen geknüpft. Das NCSC würde in diesem Zusammenhang zunehmend in den Medien erwähnt, verstärkt durch die seit 2019 bestehende Funktion des Delegierten des Bundes für Cybersicherheit.

Fazit: Die Wirtschaft konnte im Rahmen der NCS 2018-2022 ihren Schutz gegenüber Cyber-Risiken nicht ausreichend verbessern. Insbesondere bei den KMU gelingt es der NCS kaum, über ihre Outputs Aktivitäten hin zu verbessertem Schutz auszulösen.

5 Fazit zur Wirksamkeit der NCS

Die folgenden Erläuterungen geben Antwort auf die übergeordneten Fragestellungen der Wirksamkeitsüberprüfung (summativer Evaluationszweck).

5.1 Strategische Zielerreichung

Fragestellung: Inwiefern erreicht die NCS 2018-2022 die darin definierten strategischen Ziele?

Das Erreichen der Vision der NCS 2018-2022 soll über die konsequente Verfolgung von sieben strategischen Zielsetzungen erfolgen (siehe Abbildung 1). Mittels Handlungsfeldern und den diesen zugewiesenen Massnahmen mit ihren Umsetzungsvorhaben unterstützt die NCS 2018-2022 diese Zielsetzungen als Beitrag zum Erreichen der Vision wie folgt:

- Die NCS 2018-2022 bildet einen konsistenten Rahmen, der auf die Zielerreichung ausgerichtet ist. Zielsetzungen und Strategieaufbau bilden ein logisches, an institutionellen und thematischen Gegebenheiten ausgerichtetes, Gefüge. Dieses richtet sich konsequent am Wirkungspotenzial aus.
- Die Umsetzung der NCS 2018-2022 ist zu beachtlichen Teilen bereits erfolgt, sämtliche Massnahmen haben vor Ablauf der Strategielaufzeit relevante Outcomes erzeugt. Die Zeitspanne zwischen Massnahmenumsetzung mit deren Outcomes und dem erwarteten Impact auf den Cyber-Schutz ist zu kurz für belastbare resp. messbare Beobachtungen.
- Die angestrebten Outcomes auf Massnahmenebene werden grundsätzlich als geeignet zur Zielerreichung beurteiltet. Sie richten sich aber nicht gleichermassen an allen Zielgruppen aus. Es bestehen einerseits deutliche Unterschiede hinsichtlich ihres Beitrags zur Zielerreichung zwischen den Zielgruppen als auch innerhalb der Zielgruppen. Andererseits erschwert die Heterogenität in den Zielgruppen die strategische Zielerreichung durch die NCS 2018-2022.
- Es lassen sich für die NCS 2018-2022 Defizite in der strategischen Steuerung, der Umsetzungsplanung und den verfügbaren Ressourcen feststellen. Diese wirken hemmend auf die Wirkungspotenziale. Eine wenig ausgeprägte Wirkungsmessung auf Ebene Handlungsfeld und Massnahmen erschwert die Reaktionsfähigkeit und damit die Anpassungen von Massnahmen zur laufenden Maximierung von Wirkungen.
- Die hohe Dynamik der Cyber-Bedrohung (insb. starke Zunahme der Angriffe) gefährdet die strategische Zielerreichung, sofern es mit den Massnahmen der NCS nicht gelingt, den Schutz der Schweiz angemessen und mit der Fähigkeit zur dynamischen Anpassung zu erhöhen.

Fazit: Die NCS 2018-2022 stellt eine kohärente Strategie mit einem Umsetzungsplan dar, der die strategischen Zielsetzungen unterstützt. Die Umsetzung findet plangemäss statt

und führt zu relevanten Outcomes, die jedoch nicht alle Zielgruppen gleichermassen erreichen. Mit gezielten Eingriffen (u. a. Wirkungsmessung und strategische Steuerung) kann die Effektivität der Umsetzung der NCS weiter erhöht werden.

5.2 Wirkungen

Frage: Inwiefern konnten mit den erbrachten Leistungen die beabsichtigten Wirkungen erzielt werden?

Die Wirkungen der NCS 2018-2022 als langfristiger Impact auf Gesellschaft und Wirtschaft in der Schweiz lassen sich bislang kaum messen oder anderweitig empirisch nachweisen. Die konsolidierte Einschätzung aus Gesprächen mit massnahmenverantwortlichen Personen, Vertreter/innen der Zielgruppen sowie aktuelle Studien lassen sich zu folgenden Einschätzungen zusammenfassen:

- Die bislang grössten Wirkungen dürfen für die kritischen Infrastrukturen, die nationalen Behörden und Institutionen sowie für die kantonalen Behörden und Hochschulen angenommen werden. Wirtschaft und Bevölkerung werden bislang wenig bis fast gar nicht durch Massnahmen-Outcomes erreicht.
- Innerhalb der Wirtschaft zeigen sich starke Unterschiede aufgrund von Tätigkeitsspektrum und Unternehmensgrösse. Während Betreiber/innen kritischer Infrastrukturen und grosse und international operierende Unternehmen ihren Cyber-Schutz erhöhen konnten, gelten die KMU weiterhin als mehrheitlich zu wenig geschützt.
- Als zu wenig geschützt werden die Städte und Gemeinden betrachtet. Die Massnahmen der NCS 2018-2022 erreichen diese kaum. Die in die NCS eingebundenen kantonalen Institutionen vermögen keinen wirksamen Transfer der Outputs aus den Massnahmen hin zu Städten und Gemeinden sicherstellen.
- Für die Zielgruppe der Bevölkerung lassen sich keine direkten Wirkungen zur Erhöhung des Cyberschutzes aufgrund der NCS 2018-2022 erkennen. Die durchgeführten Massnahmen sprechen die Bevölkerung kaum direkt an.
- Generell verfügt die NCS 2018-2022 über zu wenig Kanäle und Kapazitäten, um die Outcomes der Massnahmen den Zielgruppen bekannt zu machen und sie zu Aktivitäten hin zu einem erhöhten Cyber-Schutzniveau zu bewegen. Die erbrachten Leistungen aus den umgesetzten Massnahmen werden in der Wirkungsentfaltung hierdurch gebremst.

Fazit: Durch die NCS 2018-2022 lassen sich bislang insbesondere für kritische Infrastrukturen, nationale und kantonale Behörden und Institutionen sowie grosse Unternehmen Wirkung annehmen. Ein empirischer Nachweis ist im Rahmen der noch laufenden NCS 2018-2022 nicht möglich. Es liegen zudem klare Hinweise vor, dass KMU, Städte und Gemeinden sowie die Bevölkerung nicht in substanziellem Ausmass durch die Massnahmen zur Umsetzung der NCS erreicht und im Ausbau des Cyber-Schutzes unterstützt werden.

5.3 Effizienz

Frage: In welchem Verhältnis steht der Mitteleinsatz zu den im Rahmen der Strategieumsetzung erbrachten Leistungen?

Der Mitteleinsatz für die NCS 2018-2022 ist im internationalen Vergleich niedrig. Bezogen auf die Leistungserfüllung lassen sich folgende Erkenntnisse festhalten:

- Die eingesetzten Ressourcen waren ausreichend, um die nach Umsetzungsplan bis zum Untersuchungszeitpunkt (Herbst 2021) geplanten Massnahmen-Outcomes im Kernauftrag zu erzeugen. Diese Outcomes bilden die Voraussetzungen für die Wirkungspotenziale der NCS 2018-2022.
- Die Allokationseffizienz des Mitteleinsatzes wird kritisch beurteilt vor dem Hintergrund, dass
  - die hohe Anzahl an Massnahmen und Umsetzungsvorhaben die Fokussierung der Mittel anspruchsvoll gestaltete;
  - fallweise Ressourcenkonkurrenz zwischen Projekttätigkeit und operativen Aktivitäten festgestellt wurden. Daraus kann sich eine Gefährdung von Handlungsfähigkeit und Integrität gegenüber Cyber-Bedrohungen in laufenden Vollzugsaufgaben ergeben;
  - der Transfer von erzeugten Leistungen zu den Zielgruppen aufgrund fehlender Ressourcen zu wenig sichergestellt werden konnte.
- Die für die Restlaufzeit der NCS 2018-2022 zusätzlich beantragten personellen Ressourcen werden als gerechtfertigt und notwendig für eine hohe Qualität der Auftragserfüllung (in Projekttätigkeit und operativer Aktivität) betrachtet. Der genaue Umfang der Ressourcenaufstockung erfordert weitere Abklärungen. Eine Unterscheidung nach Projektaktivitäten und verstetigten Aktivitäten (bspw. laufende Fallübersicht) ist angezeigt.

Fazit: Die NCS 2018-2022 hat mit den vorhandenen Ressourcen bislang ihren Kernauftrag erfüllt. Die Ressourcenallokation könnte jedoch eine stärkere Ausrichtung an den Wirkungszielen erfahren. Zusätzliche personelle Ressourcen für die Restlaufzeit sowie für verstetigte Aktivtäten erscheinen als gerechtfertigt.

6 Ausblick und Empfehlungen

Der Cyber-Raum ist geprägt von einer hohen Dynamik. Cyber-Sicherheit ist dementsprechend als eine dynamische Entwicklung zu sehen. Sie ist darauf ausgelegt, jederzeit unter den jeweiligen Rahmenbedingungen, technologischen Möglichkeiten, organisatorischen Vorgaben und relevanten Bedrohungslage die Handlungsfähigkeit und Integrität von Unternehmen, Organisationen sowie öffentlichen und privaten Haushalten zu sichern. Die Erhöhung des Schutzes vor Cyber-Risiken wird eine auch nach 2022 weiterzuführende Aufgabe sein. Mit Blick auf nachfolgende Strategiezyklen der NCS (bspw. 2023-2027) wurde folgende übergeordnete Frage untersucht (formativer Evaluationszweck):

Frage: Welche Empfehlungen lassen sich aus der Wirksamkeitsüberprüfung für die Überarbeitung der Strategie einerseits und für den zukünftigen finanziellen und personellen Ressourceneinsatz anderseits ableiten?

Die Wirksamkeitsüberprüfung weist auf verschiedene kritische Erfolgsfaktoren inhaltlichen und organisatorischen Ursprungs hin. Kritische Erfolgsfaktoren können dabei als Gegebenheiten verstanden werden, die in einer bestimmten Ausprägung für das Erreichen der Gesamtzielsetzung der NCS 2018-2022 von zentraler Bedeutung sind. Ist diese Ausprägung nicht gegeben oder gar gegenteilig ausgestaltet, so entstehen Defizite, welche die Wirksamkeit der NCS massgeblich behindern (in Anlehnung an: Gabler Wirtschaftslexikon, www.wirtschaftslexikon.gabler.de, Zugriff vom 22. Januar 2022).

Aufgrund von identifizierten kritischen Erfolgsfaktoren lassen sich Empfehlungen ableiten, wie sich die angemessene Ausgestaltung der NCS verbessern und hierdurch Effizienz und Effektivität hin zu einem bestmöglichen Impact erhöht werden könnten. Die Empfehlungen gliedern sich entlang des Aufbaus der aktuellen NCS.

6.1 Prozess und Akzeptanz

Ein wesentlicher Erfolgsfaktor für die NCS 2018-2022 liegt in deren Erarbeitungsprozess. Dieser hat strukturiert und unter Einbezug einer Vielzahl von Akteuren/innen stattgefunden. Diese Herangehensweise

- sichert eine breite Berücksichtigung von Grundlagen, zielgruppenspezifischen Herausforderungen und Fähigkeiten
- erhöht die Akzeptanz von Massnahmen, da diese gemeinsam entwickelt wurden
- schafft eine Basis zur Mitwirkung in der Umsetzung, wobei von Beginn an die hierfür erforderliche Zusammenarbeit etabliert wurde
- bildet ein Netzwerk, das zur Verbreitung von Outputs hin zu Aktivitäten in den Zielgruppen mit den intendierten Wirkungen führte.

Der Erarbeitungsprozess zur NCS 2018-2022 hat als grundlegende «Neuentwicklung» der Strategie ein Zeichen gesetzt. Nach dem Start der NCS 2012-2017 wurden die ersten Erfahrungen gezielt genutzt, um für den zweiten Strategiezyklus die strategische Herangehensweise und die Einbindung vieler Akteure/innen zu stärken.

Empfehlung: Die Vorteile eines partizipativen Erarbeitungsprozesses sind in der Weiterentwicklung der NCS gezielt zu nutzen. Ein hierzu straff geführter und effizienter Prozess motiviert die verschiedenen Wissensträger/innen zur Mitarbeit.

6.2 Governance

Die Governance der NCS in einer Netzwerkstruktur mit einem Steuerungsausschuss wird zur Abwicklung der NCS als vorteilhaft angesehen. Die Schaffung des NCSC hat zudem die operativen Kapazitäten zur Koordination sowie die operative Abwicklung von Querschnittsthemen gestärkt. Als zu wenig wirksam schätzen zahlreiche Beteiligte den StA ein. Aufgrund der Grösse, seiner Organisation und fehlender Gesamteinblicke der einzelnen Mitglieder sei dieser bislang kaum in der Lage, strategisch zu steuern. Die Kapazitäten des StA werden primär für ein Massnahmencontrolling eingesetzt. Übergeordnete Diskussionen mit strategischen Inhalten werden wenig umfassend geführt.

In den Gesprächen wurde mehrmals auf die Notwendigkeit einer Verkleinerung und Fokussierung des StA hingewiesen. Die Möglichkeit zum Austausch aller an der NCS-Umsetzung beteiligter Personen solle formell und informell in anderen Gremien und Gefässen stattfinden. Dabei ist am Prinzip der Selbstorganisation festzuhalten.

Empfehlung: Der Steuerungsausschuss ist in seinem Aufbau (insbesondere Verkleinerung) und seinen Funktionen und Aufgaben zu reorganisieren, um seine Möglichkeiten zur strategischen Steuerung zu erhöhen. Zudem sind weitere Vernetzungsmöglichkeiten zu fördern.

Die Analyse der Wirkungen auf die Zielgruppen hat gezeigt, dass innerhalb der Zielgruppen relevante Unterschiede bestehen, wie diese erreicht werden. Schwierigkeiten zeigen sich insbesondere bei KMU, kommunalen Behörden und der Bevölkerung. Die direkten Zugänge des Bundes zu diesen sind stark eingeschränkt, sodass nur eingeschränkte aktuelle Informationen zu Herausforderungen und Bedürfnissen vorliegen. Auf operativer Ebene werden zur Verbesserung der Zusammenarbeit und des Transfers «Brückenprojekte» empfohlen. Bedeutung und Wirksamkeit entsprechender Projekte lassen sich ggf. steigern, wenn Interessensgruppierungen von KMU und kommunale Behörden und Verwaltung stärker in die strategische Ebene der NCS eingebunden werden.

Empfehlung: Die stärkere Einbindung von KMU und kommunaler Ebene in die Governance der NCS soll geprüft werden.

6.3 Strategische Ziele

Die Wirksamkeitsüberprüfung zeigt, dass die strategischen Zielsetzungen der NCS insgesamt zweckmässig und angemessen sind. Diese betten sich ein in einen klassischen Strukturaufbau von Vision und Zielsetzungen sowie Handlungsfeldern zur Zielerreichung. Ergänzend entstand ein Umsetzungsplan, der die Massnahmen mit Umsetzungsvorhaben konkretisiert.

Punktuell wurde angeregt, die Vision der NCS explizit auf einen weiter entfernten Zeithorizont als die bisherigen Strategiezyklen auszurichten. Damit werde auch eine geeignete Orientierungshilfe für längerfristige Vorhaben geschaffen. Etliche Umsetzungsvorhaben in den aktuellen Massnahmen liessen sich nämlich kaum innerhalb nur eines Strategiezyklus wirksam realisieren.

Die Analyse der Wirksamkeit zeigt, dass in der Umsetzung der strategischen Zielsetzungen nicht gleichermassen fokussiert wird. So weisen die Massnahmen teilweise wenig konkrete Zielsetzungen auf und können nur in einem Gesamtkontext eingeordnet werden. Eine unabhängige Durchführung wird teilweise nicht als möglich angesehen. Unklare Zielsetzungen wirken sich ungünstig auf die Fokussierung in den Massnahmen aus (Verzettelung, unklare Zielgruppen etc.) und erschweren die Messung und Beurteilung der erreichten Wirkungen. Eine mögliche Herangehensweise zur präzisen Zielformulierung und Wirkungsmessung liefert der SMART-Ansatz (spezifisch, messbar, akzeptiert, realistisch, terminiert).

Zur wirksamen Bündelung von Aktivitäten und Ressourcen werden einfache und verständliche Zielsetzungen auf jeder Ebene als wichtig angesehen. Für die NCS 2018-2022 trifft dies nicht vollumfänglich zu. Während die Vision und die strategischen Zielsetzungen als konkret eingeschätzt werden, werden die Zielsetzungen für verschiedene Projekte von den Beteiligten als zu wenig konkret beschrieben.

Empfehlung: Der Zielsetzungen sind auf allen Strategieebenen inkl. in den Umsetzungsvorhaben möglichst konkret und unabhängig zu formulieren.

Eine Schwäche der NCS 2018-2022 wurde im Transfer der Outputs hin zu den Zielgruppen festgestellt. Zwar wurde im Rahmen der NCS 2018-2022 ein Kommunikationskonzept erarbeitet und die deutlich erhöhten Kommunikationsleistungen schufen eine höhere und messbare Sichtbarkeit des Themas und des NCSC bei den Zielgruppen und in der Öffentlichkeit.

Dennoch sind viele Interviewpartner/innen der Meinung, dass die Kommunikationsanstrengungen zu verstärken seien. Die Sichtbarkeit sei weiter zu erhöhen, der Auftritt dürfe noch prägnanter und prominenter werden. Hierzu wurde auf Kampagnen aus dem Gesundheitsbereich als mögliche Muster verwiesen. Geplante Aktivitäten und erreichte Meilensteine sollen noch besser «verkauft» werden und besondere Projekte beziehungsweise Erfolge dürften durchaus ein angemessenes mediales Echo finden. Zudem wurde angeregt, die Kommunikationsaktivitäten der verschiedenen Bundesstellen zum Thema Umgang mit Cy-

ber-Risiken stärker zu bündeln und zu koordinieren. Ebenso sollten «key player» als Multiplikatoren mitwirken, insbesondere die Wirtschaft. Der Fokus der verstärkten Kommunikationsanstrengungen sollte sich auf die Zielgruppe Bevölkerung richten. Dazu sind durchaus griffige Botschaften zu verwenden, wie das etwa in SUVA-Kampagnen oder in der Informationskampagne des Bundes zum Coronavirus stattfindet.

Empfehlung: Die Kommunikationsanstrengungen sind zu verstärken, zu bündeln und zu koordinieren. Hierzu soll geprüft werden, ob «Transfer und Kommunikation» als eine zusätzliche strategische Zielsetzung einzufügen ist.

6.4 Zielgruppen

Die NCS kann nur Wirkung entfalten, wenn die Zielgruppen passend adressiert werden. Erst die Aktivitäten der Zielgruppen führen dazu, dass der Schutz der Schweiz gegenüber Cyber-Risiken erhöht wird (siehe Wirkungsmodell Abbildung 2). Hierzu ist es wichtig, dass die Zielgruppen in ihren Herausforderungen differenziert erfasst und möglichst viele Akteure/innen direkt durch die Massnahmen angesprochen werden.

Die Massnahmen entfalten dort ihre grösste Wirkung, wo Vertreter/innen der Zielgruppen direkt in die Massnahmenplanung und -umsetzung eingebunden sind. Die NCS 2018-2022 hat wenige Zielgruppen von hoher strategischer Bedeutung direkt mittels Vertreter/innen eingebunden. Wo Zielgruppen lediglich Nutzniesser/innen oder Betroffene der Massnahmen waren, wurden die Wirkungen tendenziell als ungenügend eingeschätzt (bspw. Zielgruppe «Bevölkerung», teilweise auch «Wirtschaft»).

Empfehlung: Die Massnahmen der NCS sollen die Bedürfnisse der Zielgruppen möglichst direkt befriedigen. Die Zielgruppen sollen in geeigneter Form (siehe insb. «Bevölkerung») in die Umsetzungsvorhaben eingebunden werden.

In der Ausgestaltung und Herangehensweise für die konkreten Massnahmen gilt es die Ebenen Bund, Kantonen und Städten/Gemeinden zu verbinden. So habe beispielsweise die Einführung eines kantonalen Umsetzungsplans der Kantone durch den Sicherheitsverbund Schweiz (SVS), der auch die Entwicklung eines E-Learning-Moduls zur Sensibilisierung von kantonalen Angestellten für Cyber-Risiken vorsieht, die Realisierung und Verbreitung der Umsetzungsprojekte positiv unterstützt.

Empfehlung: Es ist zu prüfen, ob die NCS gezielt «Brückenprojekte» über die drei Staatsebenen hinweg schaffen soll.

6.5 Umsetzungsplan

Der Umsetzungsplan, der zeitgleich mit der NCS 2018-2022 erstellt wurde, hat sich als ein wichtiger Faktor erwiesen, um rasch Aktivitäten aufnehmen und die strategischen Zielsetzungen verfolgen zu können. Der Plan wird verschiedentlich als zu starr angesehen. Dies

geht einher mit Einschätzungen, wonach die Strategie zur Vision der NCS über einen längeren Zeitraum als vier Jahre Gültigkeit haben sollte und zur Umsetzung ein rollierender Umsetzungsplan eingesetzt werden könnte. Ein in seiner Flexibilität erweiterter Umsetzungsplan wird teilweise als attraktiver zur Mitwirkung angesehen.

Empfehlung: Ausgestaltung und Abwicklung des Umsetzungsplans sollen mit zusätzlicher Flexibilität ausgestaltet werden, ggf. im Zusammenspiel mit zeitlich längeren Strategiezyklen.

Die Einführung eines flexibleren resp. rollierenden Umsetzungsplanes ist mit einer Stärkung von Wirkungsmessung und Controlling (siehe nachfolgende Empfehlung Kapitel 6.6 und strategischer Steuerung (siehe Empfehlung Kapitel 6.2) zu verbinden.

6.6 Massnahmen und Wirkungsmessung

Die 29 Massnahmen widerspiegeln die Vielfalt von Herausforderungen und umfassen daher eine enorme Breite und Themenvielfalt. Die hohe Anzahl der Massnahmen kann auch so verstanden werden, dass mit der NCS ein Sammelsurium von Massnahmen geschaffen wurde.

Eine zusätzliche Strukturierung mittels Typisierung der Massnahmen, bspw. nach Schlüsselmassnahmen und flankierenden Massnahmen, würde Schwerpunkte unterstreichen und das beabsichtigte Zusammenspiel hervorheben. Mögliche Arten sind bspw. «Sofortmassnahmen», «Best Practices», «Regulierungsvorhaben», «Grundlagen-Querschnittsprojekte» und «Pilotprojekte». Ferner ist zu berücksichtigen, dass relevante Unterschiede zwischenzeitlich begrenzten Projekten und Projekten, die dem Aufbau einer operationellen Tätigkeit inkl. Verstetigung vorsehen, bestehen. Darüber hinaus könnte für die Schlüsselmassnahmen ein sogenanntes Ambitionslevel definiert werden und die flankierenden Massnahmen könnten dahingehend beurteilt werden, wie sie die Schlüsselmassnahmen unterstützen.

Empfehlung: Die Massnahmen mit ihren Umsetzungsvorhaben sollen künftig unterschieden werden nach Kriterien wie Art der Massnahme und Zielsetzung, Fristigkeit und Ambitionslevel.

Mehrere Interviewpartner/innen wiesen auf weitere Themen und Fragestellungen hin, die im nächsten Strategiezyklus mittels Massnahmen gezielt aufzugreifen seien:

— *Supply-Chain-Risiken betrachten*: Die Schweiz weist eine ausgeprägte Abhängigkeit von global geprägten Lieferketten auf. Just-in-time-Produktionen, komplexe Lieferbeziehungen und minimierte Lagerbestände machen die Wertschöpfungskette anfällig für Störungen, Ausfälle oder Angriffe. Die systematische Auseinandersetzung mit Supply-Chain-Risiken soll als eigenes Thema aufgegriffen werden oder sie ist als weiterer Einflussfaktor bei den bestehenden Massnahmen zu betrachten. Dabei sind auch die Verbindung mit den aussenpolitischen Bemühungen und dem multilateralen Dialog zu berücksichtigen, um der globalen Dimension von Lieferketten gerecht zu werden.

— *Bildung stärken*: Verschiedentlich wurde betont, dass die Befähigung aller Beteiligten in allen Zielgruppen, mit Cyberrisiken angemessen umgehen zu können, einer der Schlüsselfaktoren sei. Das Thema Bildung und Weiterbildung soll daher im nächsten Strategiezyklus noch stärker als bisher betrachtet werden.

— *Cyber-Ökosystem Schweiz*: Cyber-Risiken stellen eine weltweite Herausforderung dar, der mit technischen und organisatorischen Massnahmen zu begegnen ist. Eine Volkswirtschaft, die als gut geschützt gilt und hohe Integrität und Handlungsfähigkeit gegenüber Cyber-Vorfällen ausweist, verfügt im globalen Standortwettbewerb über Wettbewerbsvorteile. Darüber hinaus ergeben sich aus dem systematischen Wissensaufbau in einem reifen Cyber-Ökosystem neue Marktchancen für den Export von Technologien und wissensintensiven Dienstleistungen. Die thematische Einbindung eines Cyber-Ökosystems in die NCS bildet die Chancen ab, die sich aus der NCS ergeben.

Empfehlung: Die NCS soll in den Massnahmen zusätzliche Themen aufgreifen. Als prioritär angesehen werden die Themen Supply-Chain-Risiken, Bildung und Cyber-Ökosystem zur Fokussierung von Chancen.

Die Massnahmen der NCS 2018-2022 verfügen über keine systematische Wirkungsmessung. Die strategische Steuerung stützt sich bislang auf ein Umsetzungsmonitoring ab. Eine Wirkungsmessung wird dadurch erschwert, dass Massnahmen teilweise über wenig konkrete Zielsetzungen verfügen und bislang das Festsetzen von Ambitionszielen unterlassen wurde. Hierfür gibt es nachvollziehbare Gründe. Verschiedene Beteiligte weisen auf die hohe Bedeutung messebarer Zielsetzungen und laufender Wirkungsmessung als Erfolgsfaktor hin. Die Wirkungsmessung unterstützt die strategische Steuerung und Ressourcenallokation der NCS. Wirkungsmessungen für alle Einzelmassnahmen erlauben eine laufende Einschätzung der Gesamtwirksamkeit.

Im Rahmen der Cyber-Strategie des VBS werden Überlegungen zur Wirkungsmessung durch bspw. Maturitätsgrade angestellt; ein entsprechender Ansatz wurde im Cyber-Security Capacity Review für die Schweiz angewendet (University of Oxford, 2020). Diese etablierten wissenschaftlichen Ansätze können für ein internationales Benchmarking genutzt werden.

Empfehlung: Die Wirkungsmessung ist künftig fix in die Strategie- und Massnahmenplanung miteinzubeziehen. In der Konzeption der Wirkungsmessung sind die Vorteile eines partizipativen Erarbeitungsprozesses sowie Erfahrungen aus «benachbarten» Strategien der beteiligten Departemente und dem NCS-Umsetzungsplan der Kanton gezielt zu nutzen.

6.7 Ressourcen

Kapitel 2.3 (Ressourcen) und Kapitel 5.3 (Effizienz) zeigen, dass die für die Umsetzung der NCS 2018-2022 eingesetzten Ressourcen adäquat sind. Die Kernaufträge aus der NCS 2018-2022 können mit den vorhandenen Ressourcen bislang erfüllt werden.

Dennoch ergeben sich Ressourcenengpässe und es taucht der Wunsch nach gezielter personeller Verstärkung auf. Damit sich eine solche Verstärkung kurzfristig realisieren liesse, müssen verschiedene Rahmenbedingungen anders ausgestaltet werden. Zum einen muss klar sein, welches Ziel beziehungsweise welches Ambitionslevel erreicht werden soll. Hier sollen klarer messbare Ziele definiert werden, die bei Bedarf mit Kennzahlen versehen werden, um die Leistung von Aktivitäten zu ermitteln («key performance indicators»). Daraus lässt sich klarer ableiten, welche Kompetenzen und Qualifikationen gefordert sind, um das Ziel zu erreichen.

Zum anderen soll es möglich sein, Ressourcen einfacher als heute dort einzusetzen, wo der Bedarf gross ist. Die mehrjährigen Planungszyklen und die dezentral verwalteten Budgets erschweren eine flexible und schnelle Zuordnung der Ressourcen. Hier sind die Planungs- und Budgetierungsprozesse der Bundesverwaltung im Kontext der Netzwerkstruktur der NCS kritisch zu hinterfragen. Zu prüfen ist etwa, ob wesentliche Mittel oder Projektbudgets stärker durch die Kerngruppe Cyber oder den StA verwaltet werden sollten.

Empfehlung: Ziele und Ambitionslevels sind durchgängig messbar zu formulieren, um erforderliche Ressourcen genauer bezeichnen zu können. Projektbudgets sind stärker durch die Kerngruppe Cyber oder den Steuerungsausschuss zu verwalten, damit Ressourcen einfacher zugeordnet werden können.

Unbestritten bleibt der hohe Bedarf an weiteren Fachexpertinnen und -experten in allen Zielgruppen und auf allen Stufen. Die hohe Dynamik im Cyber-Raum bedingt eine laufende Weiterbildung. Auch im nächsten Strategiezyklus muss deshalb ein klarer Fokus auf das Thema Aus- und Weiterbildung und das sog. Capacity Building gelegt werden.

Empfehlung: Der Pool an Fachexperten/innen ist durch gezielte Massnahmen in der Aus- und Weiterbildung zu vergrössern.

Anhang

A-1 Details zum Vorgehen

Dokumentenanalyse und Interviews Massnahmenverantwortliche

Nr.	Methode/Arbeitsschritt	Zeitraum	Details	Generierte Information/Erkenntnisse
1	Dokumentenanalysen	Sep-Nov 2021	Fragerasterbasiertes Vorgehen Gruppierung Dokumente in Strategieentwicklung, Umsetzungsplanung und Ressourcenplanung Vertiefte Analyse der massnahmenspezifischen Dokumente	Vorbereitung der Kurzinterviews mit MNV Operationalisierung Outputs, Outcomes und Impact je Meilenstein Hinweise zu Fragestellungen auf allen Wirkungsebenen
Geschäftsstelle NCSC	*Umsetzungscontrolling durch Geschäftsstelle*	*Sep-Okt 2021*	*Erhebung und Auswertung gemäss Ablauf zum Quartalscontrolling z.H. StA*	*Laufendes Umsetzungscontrolling*
	Ressourcenerhebung durch Geschäftsstelle	*Sep-Nov 2021*	*Erhebung der beantragten, gesprochenen und eingesetzten Ressourcen* *Schriftliche Befragung durch Geschäftsstelle NCSC*	*Übersicht eingesetzte Ressourcen nach Massnahmen*
2	Leitfaden-gestützte Interviews	Sep-Okt 2021	Erstkontakt mit den MNV gemäss Absprache mit StA Aufgleisung der Termine und ggf. Zustellung spezifischer Dokumente 10-12 telefonische/videogestützte Interviews (max. 1 h) entlang Leitfaden mit den MNV Gesprächsprotokoll zu internen Zwecken (keine Herausgabe an NCSC)	Wahrgenommene Wirkungen der NCS aus der Innenperspektive Fördernde/hemmende Faktoren für Wirkungen Herausforderung Umsetzung der Massnahmen Klärung allfällige Angaben im Rahmen Umsetzungscontrolling
3	*Zwischenbericht*	*Bis Mitte Nov 2021*	– *Verarbeitung der Innen- sowie Aussenwahrnehmung durch die Auftragnehmerinnen für den Zwischenbericht*	*Zwischenergebnisse für Auftragnehmer* *Entwurf möglicher Workshopthemen*
4	Feedback NCSC und StA	*Ende Nov 2021*	– Bericht an StA – Konsolidierungen Rückmeldungen durch Geschäftsstelle NCSC – Besprechung mit econcept/EBP	Validierung Zwischenergebnisse Hinweise auf Vertiefungen/Zusatzabklärungen

Interviews/Fokusgruppen Vertreter/innen Zielgruppen

Nr.	Methode	Zeitraum	Details	Erwartete Information/Erkenntnisse
1	Zielgruppenanalyse	Aug 2021	Definition der Zielgruppe Akteursanalyse nach Einfluss/Beeinflussung Auswahl Akteure/innen (siehe weiter unten)	Auswahl geeigneter Akteure/innen mit Einblick Aussenwahrnehmung aus versch. Perspektiven
2	StA (Präsentation/Klärungsfragen)	14.9.2021	Erstkontakt mit StA Erläuterung/Diskussion/Spiegelung Zielgruppenanalyse und Auswahl Interviewpartner/innen Klärung Unterstützung Kontaktnahme durch StA	Akzeptanz des Projekts Finale Auswahl Vertreter/innen Zielgruppen Kontaktpersonen Zielgruppen
3	Leitfaden-gestützte Interviews	Sep-Nov 2021	Begleitschreiben NCSC (Entwurf durch econcept/EBP) Erstkontakt mit den Gesprächspartnern/innen je nach Person/Stelle durch NCSC oder econcept/EBP Kontakt Terminvereinbarung durch econcept/EBP Versand Interviewleitfaden, angepasst nach Akteur/in Durchführung/Protokollierung Interview (ca. 45', Telefon/online) Gesprächsprotokoll zu internen Zwecken (keine Herausgabe an NCSC)	Wahrgenommene Wirkungen der NCS aus der Aussenperspektive Fördernde/hemmende Faktoren für Wirkungen Herausforderung Verbindung Massnahmen NCS mit eigenen Aktivitäten
4	Fokusgruppe Kommission Cyber Digitalswitzerland	Nov. 2021	Planung gemeinsam mit Digitalswitzerland Diskussionsleitfaden Durchführung (2 h, Videokonferenz) Gesprächsprotokoll zu internen Zwecken (keine Herausgabe an NCSC)	Wahrgenommene Wirkungen der NCS aus der Aussenperspektive Fördernde/hemmende Faktoren für Wirkungen Herausforderung Verbindung Massnahmen NCS mit eigenen Aktivitäten
5	*Zwischenbericht*	*Bis Mitte Nov 2021*	*Verarbeitung der Innen- sowie Aussenwahrnehmung durch die Auftragnehmerinnen für den Zwischenbericht*	*Zwischenergebnisse für Auftragnehmer* *Entwurf möglicher Workshopthemen*
6	Feedback NCSC und StA	*Ende Nov 2021*	– Bericht an StA – Konsolidierungen Rückmeldungen durch Geschäftsstelle NCSC Besprechung mit econcept/EBP	Validierung Zwischenergebnisse Hinweise auf Vertiefungen/Zusatzabklärungen

A-2 Interviewleitfäden

Interviewleitfaden massnahmenverantwortliche Personen

Einstieg

Funktion: Bitte erläutern Sie uns zum Einstieg kurz Ihre Funktion und Ihre Verantwortlichkeiten mit Blick auf die Umsetzung der NCS 2018-2020.

Gesamteinschätzung

Strategie und Grundlagen: Inwiefern erachten Sie die NCS 2018-2022 insgesamt als geeignet, um die Schweiz angemessen vor Cyber-Risiken zu schützen? Wurden relevante Grundlagen ausreichend berücksichtigt? Gibt es Ihrer Ansicht nach Lücken, welche es künftig zu schliessen gilt?

Massnahmen generell: Inwiefern erachten Sie die 29 Massnahmen in der Gesamtheit als geeignet, um die Ziele der Strategie zu erreichen?

Wirkungen bei den Zielgruppen: Erreicht die NCS 2018-2022 aus Ihrer Sicht die anvisierten Wirkungen bei den Zielgruppen? Weshalb ja/nein?

Weitere Wirkungen: Zeigen sich mit der NCS 2018-2022 Ihrer Ansicht nach weitere (nicht beabsichtigte) Wirkungen?

Umsetzung der NCS 2018-2022

Massnahme(n) in Ihrer Verantwortung: Wie sind aus Ihrer Sicht die folgenden Aspekte im Hinblick auf das Ziel des Schutzes der Schweiz vor Cyber-Risiken zu beurteilen – bzw. inwiefern eignet/eignen sie sich, dieses Ziel zu erreichen:

Umsetzungsprojekte im Rahmen der Massnahmen (vgl. Umsetzungsplanung)?

Ambitionsniveau (Sollzustand 2022) mit Blick auf die Massnahmen?

Ressourcen: Wie beurteilen Sie die zur Verfügung stehenden Ressourcen – für die Umsetzung Ihrer Massnahme(n) sowie ggf. darüber hinaus?

Strukturen und Prozesse: Inwiefern erachten Sie vorhandene Strukturen und/oder Prozesse als effektiv und effizient hinsichtlich:

der Umsetzung Ihrer Massnahme(n)?

der Zusammenarbeit innerhalb Ihrer Stelle/Abteilung

der Zusammenarbeit innerhalb des Steuerungsausschusses/mit dem NCSC

ggf. weiterer Themen

Optimierungspotenziale

Optimierungspotenziale: Wo identifizieren Sie ggf. (weitere) Optimierungspotenziale hinsichtlich:

Strategie NCS 2018-2022 (z. B. Ziele)

Handlungsfelder (z. B. gegenseitige Kohärenz)

Massnahmen (z. B. Eignung)

Umsetzungsprojekte (z. B. zusätzliche Projekte)

Meilensteine

Ggf. Weiteres

Abschluss

Und überdies: Haben Sie weitere Bemerkungen, die Sie uns an dieser Stelle mitgeben möchten?

Vielen Dank für das Gespräch!

Interviewleitfaden Vertreter/innen Zielgruppen

Einstieg

1 **Funktion**: Bitte erläutern Sie uns zum Einstieg kurz Ihre Verantwortlichkeiten bzgl. Cyber-Sicherheit in Ihrer Organisation/Unternehmung/Stelle.

2 **Risiko und Verwundbarkeit**: Wie schätzen Sie die folgenden Aspekte ein:

2.1 Risiko durch Cyber-Bedrohungen für Ihre Organisation/Unternehmung/Stelle [*nur Vertreter/innen Kritische Infrastruktur/Wirtschaft:* sowie Ihre Branche/Sektor] und

2.2 deren Verwundbarkeit durch Cyber-Angriffe

Wie hat sich Ihre Einschätzung über die Risiken und die Verwundbarkeit seit 2018 verändert?

Risiken, Verwundbarkeit, Strategie

3 **NCS 2018-2022**: Welche Auswirkungen bzw. welchen Einfluss hat die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018-2022 auf Ihre Organisation/Unternehmung/Stelle [*nur Vertreter/innen Kritische Infrastruktur/Wirtschaft:* sowie Ihre Branche/Sektor]? Nutzen Sie die Strategie als Arbeitsinstrument – und weshalb ja/nein?

4 **Anforderungen**: Welche Anforderungen hat eine Strategie zum Schutz der Schweiz vor Cyber-Risiken vor dem Hintergrund spezifischer Risiken und Verwundbarkeiten zu berücksichtigen? Welche Aspekte sollen Ihrer Meinung nach geregelt werden, welche nicht?

5 **Beurteilung NCS 2018-2022**: Wie beurteilen Sie vor diesem Hintergrund die NCS 2018-2022 ganz generell?

6 **Beurteilung Handlungsfelder und Massnahmen**: Und wie beurteilen Sie die darin identifizierten Handlungsfelder und Massnahmen zum Schutz der Schweiz vor Cyber-Risiken? [*nur Vertreter/innen Kritische Infrastruktur/Wirtschaft:* Inwiefern tragen sie aus Ihrer Sicht zum Schutz Ihrer Branche/Ihres Sektors bei?]

Umsetzung der Strategie

7 **Wirkungen der NCS 2018-2022**: Haben sich im Zusammenhang mit der Strategie 2018-2022 konkrete Veränderungen für Ihre Organisation/Unternehmung/Stelle [*nur Vertreter/innen Kritische Infrastruktur/Wirtschaft:* sowie Ihre Branche/Sektor] ergeben? Wenn ja, welche sind dies?

8 **Einflussfaktoren (Treiber + Bremser)**: Welche Sachverhalte oder Rahmenbedingungen unterstützen Ihrer Meinung nach die Wirkung der NCS 2018-2022? Und welche hindern sie?

9 **Optimierungspotenziale**: Ergeben sich daraus konkrete Bedürfnisse nach Verbesserungen bzw. sehen Sie Optimierungspotenzial mit Blick auf die Strategie selbst, auf Prozesse oder Strukturen? Wenn ja, welche sind dies?

Abschluss

10 **Erwartungen**: Welche Erwartungen haben Sie an eine Strategie zum Schutz der Schweiz vor Cyber-Risiken ganz generell? Welche Erwartungen an die verantwortlichen Stellen haben Sie?

11 **Und überdies**: Haben Sie weitere Bemerkungen, die Sie uns an dieser Stelle mitgeben möchten?

Vielen Dank für das Gespräch!

A-3 Übersicht MNV-Gespräche

Nr.	Vorname	Name	Organisation	1	2	3	4	5	6	7	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
1	Philipp	Kronig	NDB				X																	X	X						
2	Stefan	Brem	BABS					X																							
	Giorgio	Ravioli	BABS																												
3	André	Duvillard	VBS							X																					
4	Daniel	Caduff	BWL					X																							
	Christophe	Hauert	Cybersafe																												
5	René	Dönni Kuoni	BAKOM									X																			
	Nicolas	Rollier	BAKOM																												
6	Yanis	Callandret	Fedpol																	X	X	X	X								
	Céline	Aubry	BKP/Fedpol																												
7	Roger	Michlig	VBS																							X					
8	Jonas	Grätz	EDA																								X	X	X		
	Daniel	Seiler	EFD																												
9	Claudio	Stricker	KKJPD							X											X	X	X								
10	Robert	Flück	Kdo Cyber																						X	X					
11	Patrick	Schaller	ETHZ		X	X		X	X	X		X	X											X							
	Imad	Aad	EPFL		X	X		X	X	X		X	X											X							
12	Martin	Leuthold	SWITCH													X															
13	Pascal	Lamia	NCSC																												
	Manuel	Sutter	NCSC			X				X	X		X	X	X	X	X	X	X											X	
	Marco	Willisch	NCSC																												
14	Dominique	Trachsel	NCSC						X																						X
15	Monica	Ratté	NCSC							X																					

Tabelle 13: Übersicht über die geführten Gespräche Massnahmenverantwortliche (*noch zu führen)

A-4 Übersicht Gespräche Zielgruppen

Nr.	Vorname	Name	Organisation	Status
1	Christoph	Niederberger	Gemeindeverband	geführt
2	Erich	Herzog	economiesuisse	geführt
	Andreas W.	Kälin	Digitalswitzerland	geführt
	Christian	Grasser	Schweizerischer Verband der Telekommunikation, ASUT	geführt
	Thomas	Holderegger	UBS	geführt
	Raphael	Reischuk	Zülke	geführt
2	Markus	Trutmann	Spitalverband H+	geführt
	Stefan	Trachsel	Koordinierter Sanitätsdienst KSD	geführt
4	Andy	Fluetsch	UPC/Salt	geführt
5	Roger	Schneeberger	KKJPD	geführt
6	Patric	Graber	ETH Rat	geführt
8	Philippe	Vuilleumier	Swisscom	geführt
10	Serdar	Cünal Rütsche	Kapo Zürich	geführt
	Stefan	Walder	Staatsanwaltschaft Kanton Zürich	geführt
11	Bertrand	Schnetz	Kripo JU	geführt
12	Gunthard	Niederbäumer	Schweizerischer Versicherungsverband	geführt
	Maya	Bundt	SwissRE	geführt
13	Nicole	Wettstein	SATW	geführt
	Umberto	Annino	Präsident Advisory Board Cyber-Security	geführt
14	Christophe	Hauert	Cyber-Safe	mit MNV geführt
15	Olivier	Crochat	C4DT	mit MNV geführt
	Imad	Aad		
16	Alain	Gut	IBM, Präsident Swiss Cyber Experts	geführt

Tabelle 14: Liste Organisationen Vertreter/innen Zielgruppen

A-5 Outputs gemäss Meilensteinen

HF	Massnahme	Umsetzungsvorhaben (Output)	Outcome
Kompetenz- und Wissensaufbau	M1: Früherkennung von Trends und Technologien und Wissensaufbau	Aufbau eines Technologie- und Marktmonitorings Bewertung von technologischen Entwicklungen und Berichterstattung im Rahmen einer Trendanalyse	– Frühzeitige Identifikation Trends und Technologien im Bereich IKT – Frühzeitige Identifikation von darauf resultierenden Chancen und Risiken – Kommunikation an Akteure aus Wissenschaft, Politik, Gesellschaft
	M2: Ausbau und Förderung von Forschungs- und Bildungskompetenzen	Aktualisierung der Bedarfsanalyse Bildung und Schliessung von Angebotslücken Aufbau eines gemeinsamen Forschungs- und Supportzentrums für Cyber-Sicherheit durch ETHZ und EPFL Umsetzung von Forschungsprojekten des Cyber Defence Campus Förderung der interdisziplinären Forschung und Bildung zu Cyber-Sicherheit durch Aufbau eines informellen Netzwerks Förderung «Ethical Hacking» durch Unterstützung etablierter Anlässe	– Analyse des Bedarfs bzgl. Kompetenzbildung zu Cyber-Risiken – Prüfung der Integration des Themas Cyber-Risiken in Ausbildungsgänge an Hochschulen und der Förderung von Talenten im Bereich «Ethical Hacking» – Stärkung der Grundlagen- und angewandten Forschung – Aufzeigen von Möglichkeiten der Förderung interdisziplinärer Forschung – Entwicklung von Kompetenzen und Wissen im Bereich Cyber Defence beim VBS durch CYD-Campus
	M3: Schaffung von günstigen Rahmenbedingungen für eine innovative IKT-Sicherheitswirtschaft in der Schweiz	Aufbau eines «Ökosystem Cyber-Sicherheit» durch Kompetenzzentrum Cyber-Sicherheit Bereitstellung von Fördermitteln für Innovationsprojekte Schaffung von Innovation-Hubs Etablierung eines Think Tanks für Cyber-Sicherheit	– Förderung der Schweiz als attraktiver Standort für Unternehmen im Bereich der IKT-Sicherheit – Stärkung des Austausches zwischen Wirtschaft und Forschung – Schaffen eines günstigen Umfelds für Innovationen und Start-Ups
Bedrohungslage	M4: Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyber-Bedrohungslage	Identifikation der Zielgruppen und ihrer Bedürfnisse zur Cyber-Bedrohungslage Definition Produktekatalog pro Zielgruppe Identifikation/Aufbau der Quellen und Produktion	– Bereitstellen eines gesamtheitlichen Cyber-Lagebilds inkl. Darstellung und Aufarbeitung der Bedrohungslage an Behörden, Betreiber kritischer Infrastrukturen, Unternehmen und Bevölkerung – Aufbau der Kapazitäten, um Cyber-Vorfälle systematisch und nachhaltig zu erfassen – Vollzug der Systematisierung des OSINT, welcher als Informationsbasis dient – Stärkung des Informationsaustausches mit Strafverfolgung, Cybersicherheitsexperten, Armee, Nachrichtendienst, Wirtschaft und Kantonen
Resilienz-Management	M5: Verbesserung der IKT-Resilienz der kritischen Infrastrukturen	Umsetzung der geplanten bzw. laufenden Projekte zur Stärkung der Resilienz in den kritischen Teilsektoren Aktualisierung der Risiko- und Verwundbarkeitsanalysen Etablierung einer akademischen Arbeitsgruppe für Cyber-Sicherheit	– Umsetzung von Massnahmen zur Verbesserung der IKT-Resilienz der kritischen Teilsektoren unter Einbezug der relevanten Regulierungsbehörden und Fachämter – Regelmässige Aktualisierung der Analysen und Massnahmen
	M6: Verbesserung der IKT-Resilienz in der Bundesverwaltung	Sicherheitsvorgaben für agile Projektmethoden entwickeln Sensibilisierungskampagne in der Bundesverwaltung	– Verbesserung der Resilienz der IKT in der Bundesverwaltung

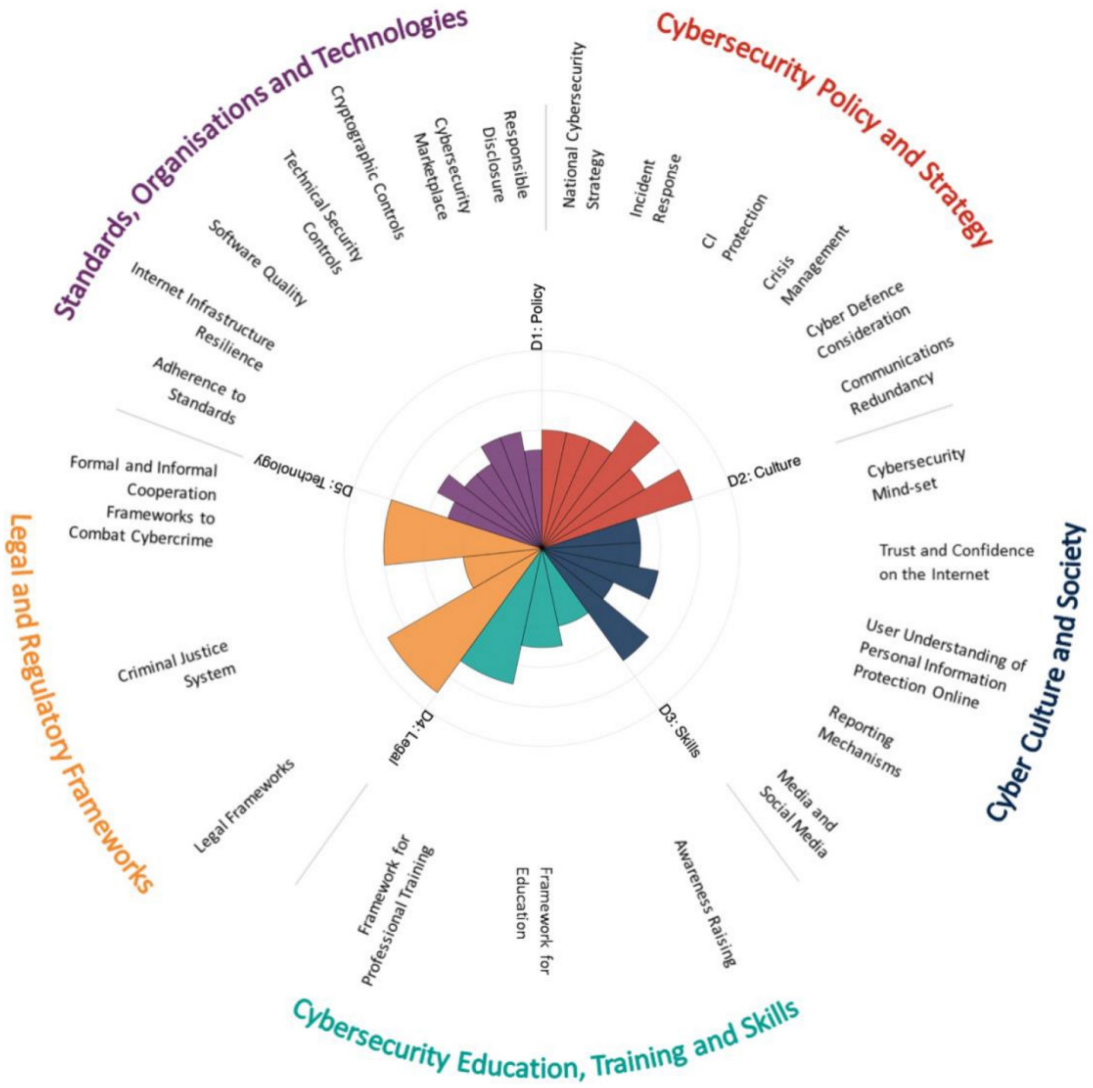
HF	Massnahme	Umsetzungsvorhaben (Output)	Outcome
		Sichere Datenübertragung durch neue Technologien: Testbetrieb SCION Security Operations Center BIT Schaffung einer Schnittstelle zum ETH-Bereich	
	M7: Erfahrungsaustausch und Schaffung von Grundlagen zur Verbesserung der IKT-Resilienz in den Kantonen	Permanenter Austausch Kantone – Kompetenzzentrum Cyber-Sicherheit Jährliche Durchführung der Cyber Landsgemeinde Entwicklung und Verbreitung gemeinsamer Sicherheitsvorgaben von Bund und Kantonen Schaffung einer Schnittstelle zum ETH-Bereich	– Schaffung eines Behördennetzwerkes, um Erfahrungen auszutauschen und gemeinsame Grundlagen für die Stärkung der IKT-Resilienz in den Kantonen zu schaffen – Gegenseitige Unterstützung und ein koordiniertes Vorgehen der Behörden aus Bund und Kantonen.
Standardisierung / Regulierung	M8: Evaluierung und Einführung von Minimalstandards	Entwicklung und Umsetzung von Minimalstandards zur Verbesserung der IKT-Resilienz Entwicklung und Etablierung von Hilfsmitteln für KMU	– Erarbeitung und Einführung überprüfbarer IKT-Minimalstandards – Prüfung, für welche Organisationen und Tätigkeiten die Standards verbindlich sein sollen
	M9: Prüfung einer Meldepflicht für Cyber-Vorfälle und Entscheid über Einführung	Studie über Grundmodelle von Meldepflichten Grundsatzdiskussion mit Wirtschaft und Behörden	– Prüfung einer Meldepflicht für Cyber-Vorfälle und Entscheid über Einführung
	M10: Globale Internet-Gouvernanz	Hochrangiges Panel des UNO-Generalsekretärs zur digitalen Kooperation Multistakeholder-Austauschplattformen zur Koordination auf nationaler Ebene	– Einsatz eines internationalen Regelwerks zur Nutzung und Weiterentwicklung des Internets, welches mit den Schweizer Vorstellungen von Freiheit, Demokratie und (Eigen-)Verantwortung, Grundversorgung, Chancengleichheit, Sicherheit, Menschenrechten und Rechtsstaatlichkeit vereinbar ist
	M11: Aufbau von Expertise bei den Fachämtern und Regulatoren	Schaffung eines überdepartementalen Expertenpools Cyber-Sicherheit zur Unterstützung der Fachämter Stärkung von Standardisierungsvorhaben durch die Unterstützung der Hochschulen Beitrag der Schweiz zur Verankerung des Themas Cyber-Sicherheit in der internationalen Finanzpolitik	– Stärkung der Cyber-Sicherheit – Aufbau eines Expertenpools zur Erarbeitung von gezielten Massnahmen, inkl. regulatorischer Eingriffe
Vorfallbewältigung	M12: Ausbau von MELANI als Public-Private-Partnership für die Betreiber kritischer Infrastrukturen	Gezielte Erweiterung des geschlossenen Kundenkreises Entwicklung und Erweiterung von Dienstleistungen und Produkten Ausbau der bestehenden Austauschplattform	– Ausbau von MELANI (Plattform von Informationsaustausch) – Einbezug aller Sektoren in den Informationsaustausch – Sicherstellung der bisherigen Qualitäten und klare Definition des Zugangs
	M13: Aufbau von Dienstleistungen für alle Unternehmen	Schaffung einer nationalen Anlaufstelle für Cyber-Risiken Publikation von «Best Practices» zur Vorfallbewältigung und technischen Einschätzungen Zeitnahe Information im Ereignisfall → Alertswiss-App	– Unterstützung der Schweizer Wirtschaft durch MELANI – Erweiterung der Zielgruppe für MELANI – Entwicklung eines Dienstleistungsangebots im Bereich Prävention und Vorfallbewältigung
	M14: Zusammenarbeit des Bundes mit relevanten Stellen und Kompetenzzentren	Übersicht über bestehende operative SOCs inkl. Ansprechpartner/innen Informationsaustausch mit CERTs und SOCs	– Stärkung der Zusammenarbeit und des Austausches zu MELANI zwischen den relevanten Stellen in Bund und Kantonen

HF	Massnahme	Umsetzungsvorhaben (Output)	Outcome
	M15: Prozesse und Grundlagen der Vorfallbewältigung des Bundes	Erarbeitung einer Verordnung zur Cyber-Sicherheit Erstellung eines Sicherheitsvorfallbewältigungsprozesses für die Bundesverwaltung	– Standardisierung der Vorfallbewältigung innerhalb der Bundesverwaltung
Krisenmanagement	M16: Integration der zuständigen Fachstellen aus dem Bereich Cyber-Sicherheit in die Krisenstäbe des Bundes	Definition der Rolle des Kompetenzzentrum Cyber-Sicherheit in den Krisenstäben des Bundes Erweiterung Cyber Glossar	– Nutzung der bestehenden Krisenstäbe bei der Bewältigung von Cyber-Krisen – Aufbau von branchenspezifischen Krisenorganisationen bei Cyber-Krisen in der Wirtschaft – Vernetzung der zuständigen Fachstellen aus dem Bereich Cyber-Sicherheit mit den Stäben
	M17: Gemeinsame Übungen zum Krisenmanagement	Schaffung von Grundlagen für Krisenübungen mit Cyber-Aspekten Durchführung von sektorspezifischen Übungen Einbringen von Cyber-Aspekten in übergreifende Krisen-Übungen	– Testen des Krisenmanagements – Optimierung der Führungsabläufe und -prozesse
Strafverfolgung	M18: Fallübersicht Cyber-Kriminalität	Zusammenfassung der kantonalen polizeilichen Daten in einer Fallübersicht (PICSEL) Erarbeitung einer justiziellen Fallübersicht Aufzeigen von Cyberkriminalitätsentwicklungen und Auswirkungen	– Prüfung und Konzipierung der technischen Rahmenbedingungen für die Erarbeitung einer nationalen Fallübersicht Cyber-Kriminalität
	M19: Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung	Rechtlichen Grundlagen für die Zusammenarbeit und Verrechnung von Leistungen zw. Bund und Kantone und innerhalb der Kantone	– Erarbeitung der Rahmenbedingungen für die polizeiliche Zusammenarbeit und Koordination zwischen den kantonalen und nationalen Cyber-Kompetenzzentren im NEDIK
	M20: Ausbildung	Umsetzung der Ausbildungskonzepte	– Nachhaltiger Aufbau der erforderlichen Kompetenzen in der Strafverfolgung
	M21: Zentralstelle Cyber-Kriminalität	Anpassung Zentralstellengesetz	– Schaffung einer Zentralstelle Cyber-Kriminalität und der notwendigen Grundlagen für die Zusammenarbeit mit den Kantonen bei der Bekämpfung der Cyber-Kriminalität
Cyber-Defence	M22: Ausbau der Fähigkeiten zur Informationsbeschaffung und Attribution	Ausbau der Fähigkeiten zur Informationsbeschaffung und Attribution Durchführung einer spezifischen Ausbildung in der Cyber-abwehr (Armee)	– Frühzeitige Erkennung von neuen Angriffsmuster durch den NDB – Weiterentwicklung des Spezialwissens und der Fähigkeiten des NDB zur Informationsbeschaffung – Durchführung vertiefter Akteurs- und Umfeldanalysen – Nutzung und Entwicklung technischer Hilfsmittel – Systematische Aufarbeitung von erkannten Cyber-Angriffen
	M23: Fähigkeit zur Durchführung von aktiven Massnahmen im Cyber-Raum gemäss NDG und MG	Nutzung der im Kontext vom NDG entwickelten Kapazitäten von FUB-ZEO	– Aufbau von genügend qualitativen und quantitativen Kompetenzen und Kapazitäten, um Angriffe auf kritische Infrastrukturen zu stören, zu verhindern oder zu verlangsamen

HF	Massnahme	Umsetzungsvorhaben (Output)	Outcome
	M24: Gewährleistung Einsatzbereitschaft der Armee über alle Lagen im Cyber-Raum und Regelung ihrer subsidiären Rolle zur Unterstützung der zivilen Behörden	Projekt «Aufbau Cyber»: Befähigung der Armee, ihre Leistungen im Cyberraum zu erbringen Aufbau eines Cyber Training Center Schweiz Trainings für Führungsorganisationen im Cyber- Krisenmanagement	– Bewältigung der in Anzahl, Intensität und Komplexität zunehmenden Formen der Cyber-Bedrohung – Umsetzung der Cyber-Aspekte des Nachrichtendienstgesetzes und des Militärgesetzes – Unterstützung der Betreiber kritischer Infrastrukturen, die Opfer von Cyber-Angriffen wurden
Aktive Positionierung der Schweiz in der internationalen Cyber-Sicherheitspolitik	M25: Aktive Mitgestaltung und Teilnahme an Prozessen der Cyber-Aussensicherheitspolitik	Teilnahme an UNO-Prozessen für die internationale Cybersicherheit Interessenvertretung im Rahmen der OSZE (staatliche Vertrauensbildung) Etablierung des Geneva Dialogues on responsible behavior Verfolgung der Entwicklungen in der Europäischen Union (insbesondere der Europäische Auswärtige Dienst und ENISA) Engagement zur Förderung eines offenen und freien Cyber-Raums	– Weiterentwicklung und Umsetzung von staatlichen und nichtstaatlichen Verhaltensnormen im Cyber-Raum – Anerkennung des Völkerrechts und den Schutz der Menschenrechte im Cyber-Raum – Schaffung von staatlichem Vertrauen im Cyber-Raum – Durchsetzung der Exportkontrollregime mit Blick auf Überwachungstechnologien
	M26: Internationale Kooperation zum Auf- und Ausbau von Kapazitäten im Bereich Cyber-Sicherheit	Durchführung von Workshops mit regionalen Organisationen Durchführung von Workshops zum Aufbau von Institutionen und Cyber-Aussensicherheitsstrukturen Unterstützung des Global Forum on Cyber-Expertise	– Austausch mit internationalen staatlichen und nichtstaatlichen Stellen zum Auf- und Ausbau von nationalen Fähigkeiten im Bereich Cyber-Risiken – Auf- und Ausbau von Cyber-Fähigkeiten in Drittstaaten – Verbesserung der globalen Cyber-Sicherheit
	M27: Bilaterale politische Konsultationen und multilaterale Dialoge zu Cyber-Aussensicherheitspolitik	Bilaterale politische Cyber-Konsultationen zu Cyber-Aussensicherheitspolitik Sino European Cyber Dialogue – IL Arbeitsgruppe: Vertrauensbildung MENA Dialogue: Diskussionsrahmen für Staaten der MENA-Region	– Durchführung von Konsultationen zu Cyber-Sicherheit – Mitgestaltung von multilateralen Dialogen
Aussenwirkung und Sensibilisierung	M28: Erstellung und Umsetzung eines Kommunikationskonzepts zur NCS	Erarbeitung eines Kommunikationskonzeptes zur NCS	– Erstellung und Umsetzung eines Kommunikationskonzepts zur NCS – Festhalten von Kommunikationsleitlinien, Zuständigkeiten und Prozesse
	M29: Sensibilisierung der Öffentlichkeit für Cyber-Risiken (Awareness)	Entwicklung und Durchführung einer nationalen Awareness-Kampagne Informationsplattform zu Cyber-Risiken geführt durch die nationale Anlaufstelle	– Sensibilisierung der Öffentlichkeit für Cyber-Risiken – Verstärkung der Kommunikation zu Cyber-Risiken

Tabelle 15: Outputs und Outcomes pro Massnahme. HF = Handlungsfeld. Quelle: Umsetzungsplan NCS 2018-2022.

A-7 Maturitätsgrade Cyber-Security Capacity Switzerland



Quelle: University of Oxford, 2020

Abbildung 4: Maturitätsgrade Cyber-Security Capacity Switzerland

Literatur

Bundesamt für Energie (2021), Cyber-Sicherheit und Cyber Resilienz für die Schweizer Stromversorgung. Bericht, 28 Juni 2021. Bern

Bundesrat (2015): Sicheres Datenverbundnetz (SDVN). Medienmitteilung vom 20. Mai 2015. Bern.

Bundesrat (2017): Nationale Strategie zum Schutz kritischer Infrastrukturen 2018-2022 (SKI-Strategie). Bern.

Bundesrat (2018): Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018-2022. Bern.

Bundesrat (2021): Bericht zum Umsetzungsstand der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018-2022. Stand zweites Quartal 2021. Bern.

Center for Security Studies (CSS) ETH Zürich (2019: Nationale Cyber-Sicherheitsstrategien im Vergleich -Herausforderungen für die Schweiz. Zürich.

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS (2021): Strategie Cyber VBS. Bern.

European Union Agency for Network and Information Security ENISA (November 2016), NCSS Good Practice Guide, Designing and Implementing National Cyber Security Strategies, Attiki, Greece

gfs-Zürich (2021): Auswirkungen der Corona-Krise auf die Digitalisierung und Cyber-Sicherheit in Schweizer KMU. Befragung von Geschäftsführenden kleiner Unternehmen in der Schweiz. Studie im Auftrag von: Digitalswitzerland, et al., Zürich.

Nationalen Zentrums für Cyber-Sicherheit NCSC (2021c): Ergebnisse der Ressourcenerhebung zur Umsetzung der NCS 2021. Interne Auswertung. Bern.

Nationales Zentrum für Cyber-Sicherheit NCSC (2021a): Halbjahresbericht 2020/2. Bern.

Nationales Zentrum für Cyber-Sicherheit NCSC (2021b): Halbjahresbericht 2021/1. Bern.

Schweizerische Eidgenossenschaft (2020a): Strategie Digital Schweiz. Bern.

Schweizerische Eidgenossenschaft (2020b): Strategie Digitalaussenpolitik 2021-2024. Bern.

Sotomo (2022): Digitaler Staat in der Schweiz. Studie im Auftrag der Swico, Zürich.

Universität Zürich, Zentrum für Gerontologie (2020): Digitale Senioren 2020. Nutzung von Informations- und Kommunikationstechnologien durch Personen ab 65

Jahren in der Schweiz. Studie im Auftrag von Pro Senectute Schweiz, Zürich.

University of Oxford (2020): Cyber-Security Capacity Review. Switzerland. June 2020. Study at the invitation of the Swiss Federal Department of Foreign Affairs and the Swiss Federal Department of Finance, Oxford.