
Umsetzungsplan der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022



Inhaltsverzeichnis

1	Einleitung	4
2	Organisation zur Umsetzung	5
2.1	Organisation des Bundes im Bereich Cyber-Risiken	5
2.2	Zusammenarbeit zwischen Bund, Kantonen, Wirtschaft und Hochschulen	6
2.2.1	Zusammenarbeit auf politisch-strategischer Stufe	7
2.2.2	Der Steuerungsausschuss NCS als Organ des gemeinsamen Projektmanagements	7
2.2.3	Direkte Kooperation auf operativer Stufe	7
3	Rechtliche Grundlagen	8
4	Strategisches Controlling und Reporting	8
5	Systematik des Umsetzungsplans	8
6	Roadmap für die Umsetzung	10
7	Umsetzungsplan	13
7.1	Kompetenzen- und Wissensaufbau	13
7.1.1	Früherkennung von Trends und Technologien und Wissensaufbau (M1)	13
7.1.2	Ausbau und Förderung von Forschungs- und Bildungskompetenz (M2)	15
7.1.3	Schaffung von günstigen Rahmenbedingungen für eine innovative IKT- Sicherheitswirtschaft in der Schweiz (M3)	18
7.2	Bedrohungslage	21
7.2.1	Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyber-Bedrohungslage (M4)	21
7.3	Resilienz-Management	24
7.3.1	Verbesserung der IKT-Resilienz der kritischen Infrastrukturen (M5)	24
7.3.2	Verbesserung der IKT-Resilienz in der Bundesverwaltung (M6)	26
7.3.3	Erfahrungsaustausch und Schaffung von Grundlagen zur Verbesserung der IKT- Resilienz in den Kantonen (M7)	29
7.4	Standardisierung / Regulierung	31
7.4.1	Evaluierung und Einführung von Minimalstandards (M8)	31
7.4.2	Prüfung einer Meldepflicht für Cyber-Vorfälle und Entscheid über Einführung (M9)	33
7.4.3	Globale Internet-Gouvernanz (M10)	34
7.4.4	Aufbau von Expertise bei den Fachämtern und Regulatoren (M11)	36
7.5	Vorfallbewältigung	38
7.5.1	Ausbau von MELANI als Public-Private-Partnership für die Betreiber kritischer Infrastrukturen (M12)	38
7.5.2	Aufbau von Dienstleistungen für alle Unternehmen (M13)	40
7.5.3	Zusammenarbeit des Bundes mit relevanten Stellen und Kompetenzzentren (M14)	42
7.5.4	Prozesse und Grundlagen der Vorfallbewältigung des Bundes (M15)	43
7.6	Krisenmanagement	45
7.6.1	Integration der zuständigen Fachstellen aus dem Bereich Cyber-Sicherheit in die Krisenstäbe des Bundes (M16)	45
7.6.2	Gemeinsame Übungen zum Krisenmanagement (M17)	46
7.7	Strafverfolgung	49
7.7.1	Fallübersicht Cyber-Kriminalität (M18)	49
7.7.2	Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung (M19)	51

7.7.3	Ausbildung (M20)	51
7.7.4	Zentralstelle Cyber-Kriminalität (M21)	52
7.8	Cyber-Defence.....	53
7.8.1	Ausbau der Fähigkeiten zur Informationsbeschaffung und Attribution (M22)	53
7.8.2	Fähigkeit zur Durchführung von aktiven Massnahmen im Cyber-Raum gemäss NDG und MG (M23).....	55
7.8.3	Gewährleistung Einsatzbereitschaft der Armee über alle Lagen im Cyber-Raum und Regelung ihrer subsidiären Rolle zur Unterstützung der zivilen Behörden (M24) ...	55
7.9	Aktive Positionierung der Schweiz in der internationalen Cyber-Sicherheitspolitik	58
7.9.1	Aktive Mitgestaltung und Teilnahme an Prozessen der Cyber-Aussensicherheitspolitik (M25).....	58
7.9.2	Internationale Kooperation zum Auf- und Ausbau von Kapazitäten im Bereich Cyber-Sicherheit (M26).....	61
7.9.3	Bilaterale politische Konsultationen und multilaterale Dialoge zu Cyber-Aussensicherheitspolitik (M27).....	63
7.10	Aussenwirkung und Sensibilisierung.....	65
7.10.1	Erstellung und Umsetzung eines Kommunikationskonzepts zur NCS (M28)	65
7.10.2	Sensibilisierung der Öffentlichkeit für Cyber-Risiken (Awareness) (M29)	66
	Abbildungsverzeichnis	68
	Abkürzungsverzeichnis	69
	Anhang Umsetzungsplan der Kantone	71

1 Einleitung

Am 18. April 2018 hat der Bundesrat die «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018 – 2022» verabschiedet. Die Strategie baut auf der ersten NCS für die Jahre 2012-2017 auf, entwickelt diese weiter und ergänzt sie mit weiteren Massnahmen. Sie trägt dadurch der deutlich intensivierten Bedrohungslage Rechnung. Die Strategie soll dazu beitragen, dass die Schweiz bei der Nutzung der Chancen der Digitalisierung angemessen vor Cyber-Risiken geschützt und ihnen gegenüber resilient ist. Aus dieser Vision abgeleitet, identifiziert die NCS sieben strategische Ziele, welche über 29 Massnahmen in insgesamt 10 Handlungsfeldern erreicht werden sollen. Abbildung 1 fasst die Inhalte der NCS zusammen:

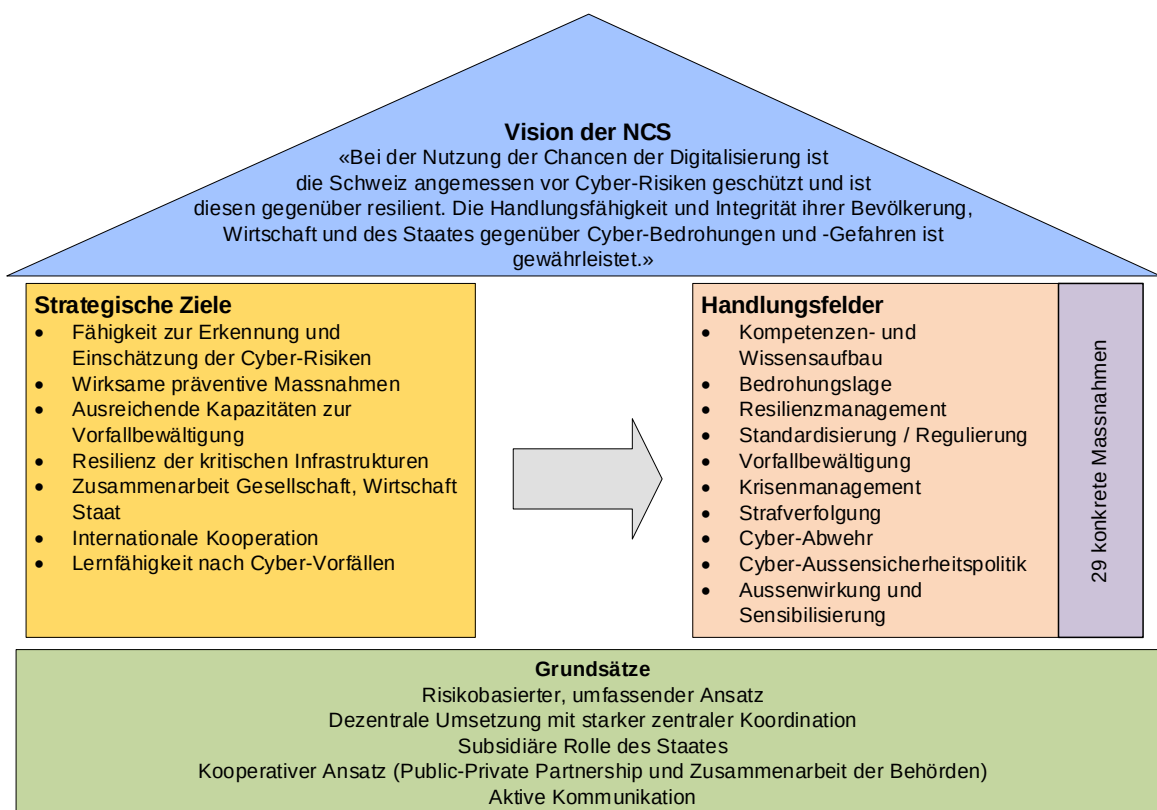


Abbildung 1 Inhalte der NCS

Der vorliegende Umsetzungsplan definiert für alle 29 Massnahmen der NCS konkrete Umsetzungsprojekte und legt die Verantwortlichkeiten, die zu erreichenden Leistungsziele und die Meilensteinplanung für diese Projekte fest.

Der Umsetzungsplan wurde gemeinsam unter Beteiligung der verantwortlichen Bundesstellen, der Kantone, der Wirtschaft und den Hochschulen Ende 2018 und Anfangs 2019 erarbeitet und gliedert sich nachfolgend anhand den NCS Handlungsfeldern. Durch die breite Beteiligung bei seiner Erarbeitung enthält der Umsetzungsplan nicht nur die geplanten Arbeiten der zuständigen Bundesstellen, sondern umfasst auch die wichtigsten Aktivitäten weiterer Akteure im Zusammenhang mit der NCS. Dadurch dient er sowohl als Grundlage für die Arbeitsplanung und das strategische Controlling zur Prüfung des Umsetzungsfortschritts, als auch als Instrument zur Koordination aller beteiligten Akteure.

Das vorliegende Dokument gibt den aktuellen Stand der Umsetzungsplanung wieder. Im dynamischen Umfeld der Cyber-Risiken müssen aber Anpassung jederzeit möglich sein. Die im folgenden Kapitel beschriebenen Gremien erhalten deshalb die Kompetenz, den Umsetzungsplan bei Bedarf anzupassen.

2 Organisation zur Umsetzung

Der Erfolg der Umsetzung der NCS hängt stark davon ab, dass die heute bereits vorhandenen Ressourcen optimal eingesetzt und gut aufeinander abgestimmt weiter ausgebaut werden können. Die im vorliegenden Umsetzungsplan beschriebenen Aufgaben sind verbindliche Vorgaben für die Bundesämter. Diese sind jedoch bei der Umsetzung der Vorgaben auf Grund der Komplexität der Aufgaben, der beschränkten Ressourcen und den rechtlichen Einschränkungen in Bezug auf die Zuständigkeit auf die Mitwirkung Dritter angewiesen. Die Organisation der Arbeiten muss diesem Umstand gerecht werden. Im Folgenden wird deshalb zunächst beschrieben, wie sich der Bund im Bereich Cyber-Risiken organisiert hat, dann wird darauf eingegangen, wie die Zusammenarbeit zwischen Bund, Kantonen, Wirtschaft und Hochschulen bei der Umsetzung der NCS ausgestaltet sein soll und schliesslich wird die Organisation des Controllings und der Berichterstattung beschrieben.

2.1 Organisation des Bundes im Bereich Cyber-Risiken

Innerhalb der Bundesverwaltung werden in Bezug auf Cyber-Risiken drei Bereiche unterschieden:

- **Cyber-Sicherheit:** Gesamtheit der Massnahmen, welche die Prävention, die Bewältigung von Vorfällen und die Verbesserung der Resilienz gegenüber Cyber-Risiken zum Ziel haben und die internationale Zusammenarbeit zu diesem Zweck stärken. Der Bund ergreift die nötigen Massnahmen zur Erhöhung der eigenen Cyber-Sicherheit und trägt unter Berücksichtigung des Grundsatzes der Subsidiarität zur Verbesserung der Cyber-Sicherheit der Wirtschaft und Gesellschaft bei, wobei die zentrale Bedeutung der kritischen Infrastrukturen entsprechend gewichtet wird. Zu den Massnahmen zählt ebenfalls die Förderung der internationalen Zusammenarbeit im Bereich Cyber-Sicherheit.
- **Cyber-Defence:** Gesamtheit der zivilen nachrichtendienstlichen und militärischen Massnahmen, die der Verteidigung kritischer Systeme, der Abwehr von Angriffen im Cyber-Raum, der Gewährleistung der Einsatzbereitschaft der Armee in allen Lagen und dem Aufbau von Kapazitäten und Fähigkeiten zur subsidiären Unterstützung ziviler Behörden dienen. Der Bereich schliesst insbesondere aktive Massnahmen zur Erkennung von Bedrohungen, zur Identifikation von Angreifern und zur Störung und Unterbindung von Angriffen mit ein.
- **Cyber-Strafverfolgung:** alle Massnahmen der Polizei und der Staatsanwaltschaft von Bund und Kantonen im Kampf gegen die Cyber-Kriminalität.

Am 30. Januar 2019 hat der Bundesrat ausgehend von dieser Aufgabenteilung die übergeordnete Organisation des Bundes im Bereich Cyber-Risiken definiert. Die wesentlichen Elemente dieser Organisation mit Bezug auf die Umsetzung der NCS sind in Abbildung 2 veranschaulicht.

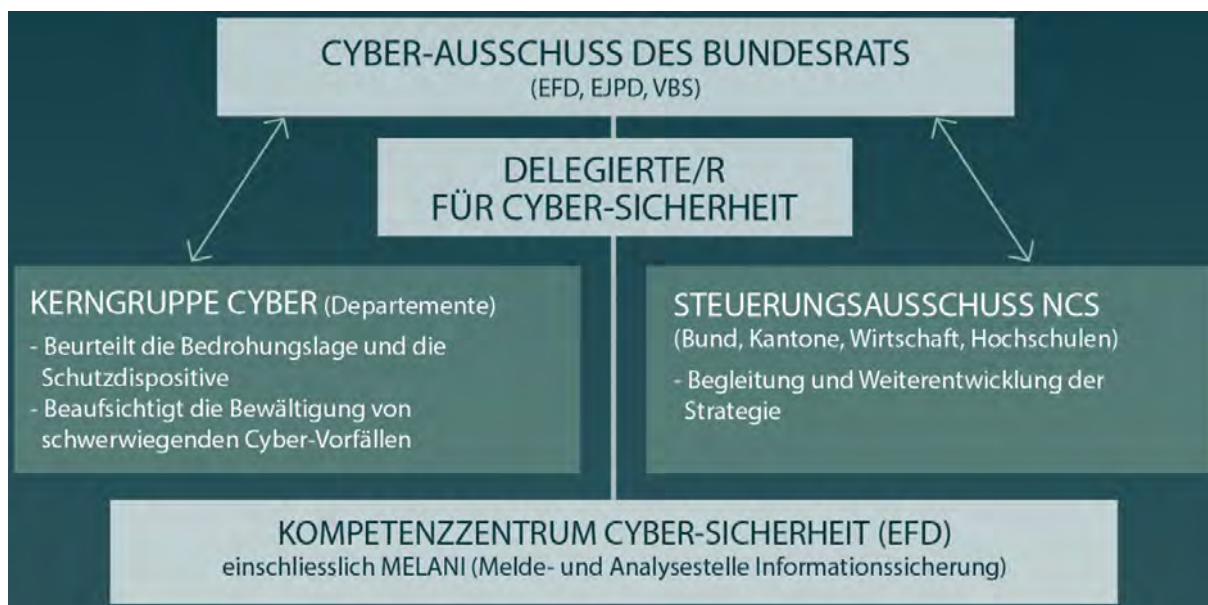


Abbildung 2 Organisation des Bundes im Bereich Cyber-Risiken

Mit Bezug auf die NCS ist die Aufgabenteilung zwischen diesen neu geschaffenen Gremien und Funktionen wie folgt definiert:

- Der **Cyber-Ausschuss des Bundesrats** durch die **Vorstehenden der Departemente EFD, EJPD und VBS** hat die Aufgabe, die Umsetzung der NCS zu beaufsichtigen.
- Das **Kompetenzzentrum des Bundes für die Cyber-Sicherheit im EFD** ist die nationale Anlaufstelle für alle Fragen mit Bezug zur Cyber-Sicherheit und übernimmt mit seiner Geschäftsstelle die Koordination der NCS-Umsetzung.
- Der/die **Delegierte/r für Cyber-Sicherheit** übernimmt die strategische Leitung der Cyber-Sicherheit im Bund, leitet die vom Bund eingesetzten Gremien und vertritt den Bund in weiteren Gremien.
- Die **Kerngruppe Cyber** stärkt die Koordination zwischen den drei Bereichen Sicherheit, Defence und Strafverfolgung, sorgt für eine gemeinsame Beurteilung der Bedrohungslage und beaufsichtigt die Bewältigung von schwerwiegenden und departementsübergreifenden Vorfällen durch die Bundesstellen.
- Der **Steuerungsausschuss NCS (StA NCS)** stellt die koordinierte und zielgerichtete Umsetzung der NCS-Massnahmen sicher und erarbeitet Vorschläge zur Weiterentwicklung der NCS.

2.2 Zusammenarbeit zwischen Bund, Kantonen, Wirtschaft und Hochschulen

Die Zusammenarbeit zwischen Bund, Kantonen, Wirtschaft und Hochschulen muss auf allen Stufen sichergestellt sein. Dies verlangt auf strategisch-politischer Ebene gut aufeinander abgestimmte Entscheide und einen regelmässigen, direkten Austausch. Ebenso wichtig ist ein gemeinsames Projektmanagement resp. Projektportfoliomanagement zur Umsetzung der NCS durch alle beteiligten Stellen und schliesslich benötigt es einen regelmässigen Austausch auf operativer Stufe.

2.2.1 Zusammenarbeit auf politisch-strategischer Stufe

Die Zusammenarbeit auf politisch-strategischer Stufe ist insbesondere für die Aufgabenverteilung zwischen Kantonen und Bund von zentraler Bedeutung. Es ist für die Umsetzung der NCS entscheidend, dass Klarheit darüber herrscht, welche Staatsebene welche Aufgabe übernimmt. Der Cyber-Ausschuss des Bundesrats tauscht sich zur Erörterung solcher Fragen regelmässig mit den massgeblichen Konferenzen der Kantonsregierungen, insbesondere mit der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und –direktoren, (KKJPD) und in den Bereichen Militär und Zivilschutz mit der Regierungskonferenz Militär, Zivilschutz und Feuerwehr (RK MZF) aus. Die Politische Plattform des Sicherheitsverbundes Schweiz (SVS) bietet ausserdem die Möglichkeit, die mit Cyber im Zusammenhang stehenden Themen weiter zu vertiefen.

Dem/der Delegierten für Cyber-Sicherheit kommt bei der Zusammenarbeit auf politisch-strategischer Ebene ebenfalls eine zentrale Rolle zu. Er/sie ist die zentrale Ansprechperson des Bundes für Fragen zur Cyber-Sicherheit, nimmt politische Anliegen auf und legt diese dem Cyber-Ausschuss des Bundesrates vor.

2.2.2 Der Steuerungsausschuss NCS als Organ des gemeinsamen Projektmanagements

Weil die NCS als Gesamtprojekt aber von allen Beteiligten gemeinsam getragen werden soll, verlangt es neben dieser direkten Zusammenarbeit auch ein Gremium zur gemeinsamen Entscheidungsfindung. Diese Funktion übernimmt der StA NCS, in welchem Vertretungen der wichtigsten Umsetzungspartner Einsitz erhalten sollen. Der StA NCS stellt die koordinierte, zielgerichtete Umsetzung der NCS-Massnahmen unter Einbezug aller beteiligten Akteure sicher, prüft regelmässig den Stand der Umsetzung, entwickelt bei Bedarf Sondermassnahmen, nimmt Priorisierungen vor, sorgt für die Berichterstattung zur NCS gegenüber der Politik und der Öffentlichkeit und arbeitet an der Weiterentwicklung der NCS. Er setzt sich aus nachfolgenden Vertretungen zusammen:

- Vertretungen der für NCS-Massnahmen beteiligten Bundesstellen;¹
- Vertretungen der Kantone und der Koordinationsgremien zwischen Bund und Kantonen durch das Generalsekretariat der Kantonalen Konferenz der Justiz- und Polizeidirektorinnen und –direktoren (KKJPD), den Sicherheitsverbund Schweiz (SVS) und das Cyberboard der Strafvollzugsbehörden;
- Vertretungen der Wirtschaft (zwei Vertretungen aus verschiedenen Wirtschaftszweigen mit Relevanz für die NCS);
- Vertretungen der Hochschulen (zwei Vertretungen).

Geleitet wird der StA NCS durch den/die Delegierte/n des Bundes für Cyber-Sicherheit. Das Sekretariat des Gremiums übernimmt die Geschäftsstelle Cyber-Sicherheit des/der Delegierten.

2.2.3 Direkte Kooperation auf operativer Stufe

Die Kooperation bei der Umsetzung von Massnahmen durch die jeweils operativ tätigen Einheiten ist die direkteste Form der Zusammenarbeit. Sie orientiert sich an den in diesem Umsetzungsplan festgehaltenen Zuständigkeiten und Beteiligungen, kann jedoch flexibel angepasst und ausgeweitet werden. Zentrale Anlaufstelle des Bundes für alle im Bereich Cyber-Risiken engagierten Stellen ist das Kompetenzzentrum Cyber-Sicherheit unter der strategischen Leitung des/der Delegierten für Cyber-Sicherheit.

¹ Jedes Departement und die BK verfügen über mindestens eine Vertretung

3 Rechtliche Grundlagen

Das Recht gibt gemäss Art. 5 der Bundesverfassung die Grundlage und die Schranke des staatlichen Handelns vor. Die im Umsetzungsplan beschriebenen Tätigkeiten der Behörden müssen deshalb auf rechtlichen Grundlagen basieren. Die im Umsetzungsplan aufgeführten Verwaltungseinheiten verfügen – falls nicht ausdrücklich auf fehlende Rechtsgrundlagen hingewiesen wird – über die für die vorgesehenen Massnahmen nötigen rechtlichen Kompetenzen. Sie übernehmen im Rahmen ihrer in den vorhandenen Rechtsgrundlagen definierten Tätigkeiten Aufgaben im Bereich der NCS. Diese Aufgaben sind nicht materiell neu, sondern finden in Bezug auf Cyber-Risiken ein neues Anwendungsfeld. Es liegt in ihrer Verantwortung der zuständigen Stellen, bei der Umsetzung den NCS nicht über die bestehenden rechtlichen Kompetenzen hinauszugehen.

Rechtssetzungsbedarf besteht hingegen bei den Aufgaben des Cyber-Kompetenzzentrums, da sich diese neu geschaffene Verwaltungseinheit nicht auf bestehende Grundlagen stützen kann und Aufgaben übernimmt, für welche noch keine rechtliche Basis vorhanden ist. Es wird in den Beschreibungen der Massnahmen jeweils explizit darauf hingewiesen, wo es nötig ist, rechtliche Grundlagen zu schaffen.

4 Strategisches Controlling und Reporting

Mit Hilfe eines strategischen Controllings prüft der StA NCS regelmässig den Stand der Umsetzung und entwickelt bei Abweichungen der für die Zielsetzung massgeblichen Einflussfaktoren Anpassungsstrategien oder Planänderungen. Zudem schafft die Berichterstattung des strategischen Controllings Transparenz für alle Beteiligten.

Das Controlling beinhaltet eine Begutachtung der erreichten Meilensteine in den einzelnen Projekten sowie eine Bewertung der weiteren Planung hinsichtlich Inhalte, Terminen und Ressourcen durch die Geschäftsstelle des Kompetenzzentrums Cyber-Sicherheit. Diese legt den Stand der Umsetzungsmassnahmen halbjährlich mittels eines Kurzberichts dem StA NCS vor, welcher diesen verabschiedet und ihn dem Cyber-Ausschuss des Bundesrates zur Kenntnisnahme unterbreitet. Der StA NCS erstattet dem Bundesrat jährlich Bericht über die Umsetzung der NCS. Spätestens bis 2022 wird eine Wirksamkeitsüberprüfung der NCS durchgeführt, welche Aufschluss über den weiteren Handlungsbedarf geben soll.

5 Systematik des Umsetzungsplans

Der Umsetzungsplan definiert die Umsetzungsprojekte aller 29 Massnahmen. Er ist analog zur NCS strukturiert und gruppiert die Massnahmen pro Handlungsfeld in zehn Unterkapitel. Daraus ergibt sich die in Abbildung 3 dargestellte Systematik des Umsetzungsplans.

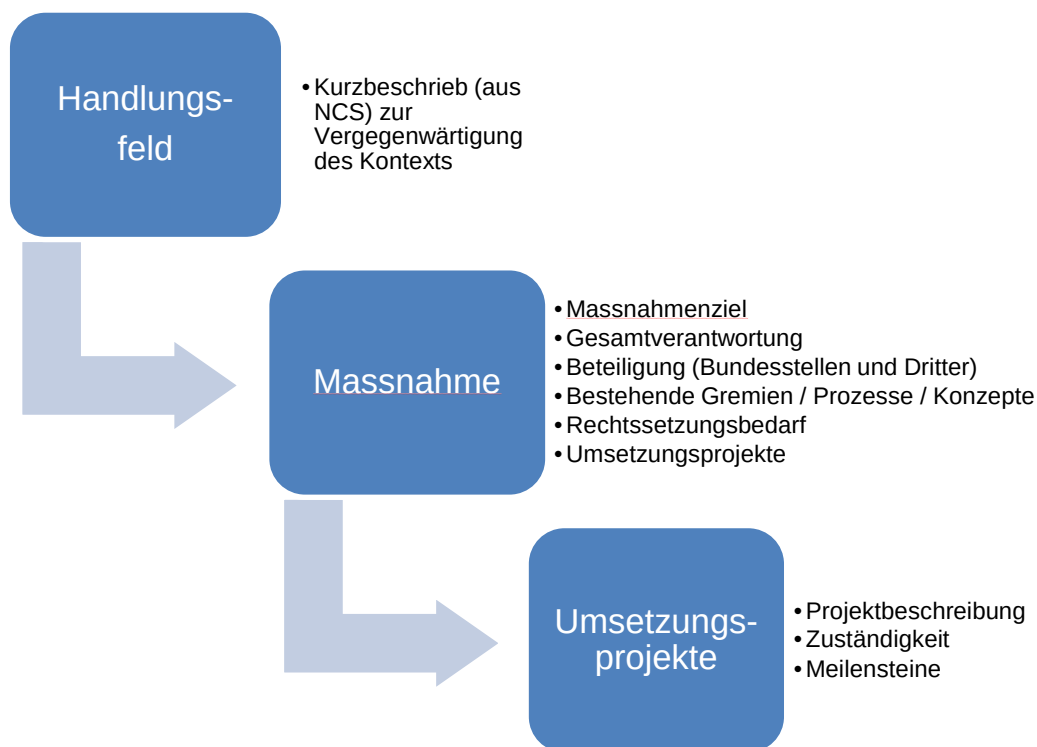


Abbildung 3 Systematik des Umsetzungsplans

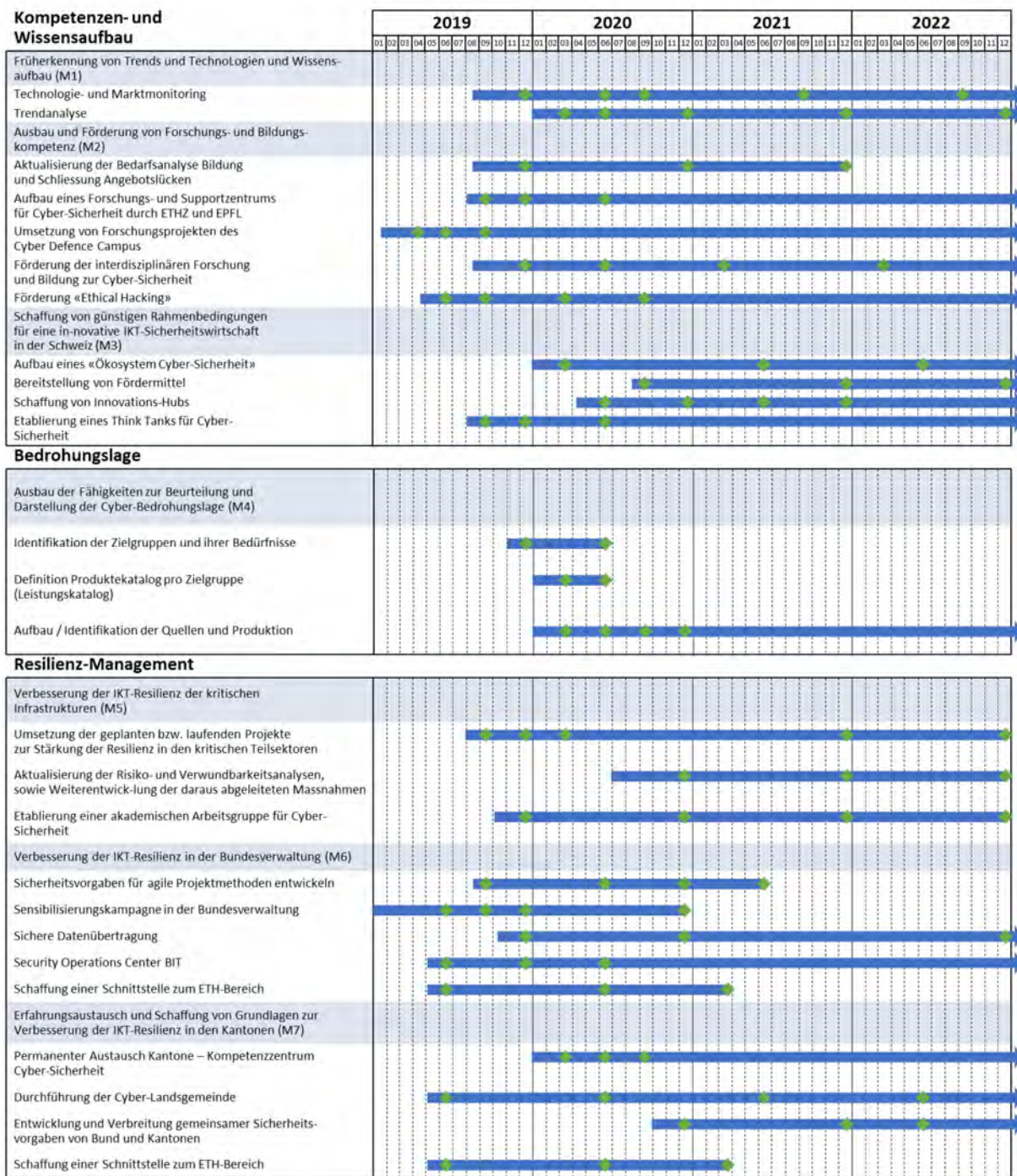
Jedes Handlungsfeld wird zunächst kurz eingeführt, um den Kontext der Umsetzungsprojekte nochmals zu vergegenwärtigen. Ergänzt wird die Einführung zum Handlungsfeld mit dem für das Handlungsfeld relevanten Auszug aus der Roadmap zur Umsetzung. Für jede Massnahme wird eingangs in einer Übersichtstabelle präsentiert, in welcher folgende Punkte beschrieben sind:

- Massnahmenziele: direkt abgeleitet aus der NCS wird aufgezeigt, was konkret mit der Massnahme erreicht werden soll
- Gesamtverantwortung für die Massnahme: jene Stelle(n) welche für die Umsetzung der gesamten Massnahme zuständig ist und gegenüber dem Steuerungsausschuss NCS über den Umsetzungsstand Rechenschaft ablegt.
- Beteiligung Bundesstellen / Dritter: Organisationen der Bundesverwaltung oder externer Stellen, welche sich im Rahmen des Umsetzungsplans verpflichtet haben, an der Umsetzung der Massnahme mitzuarbeiten. Die Auflistung hat keinen ausschliessenden Charakter, weitere Stellen können sich jederzeit an der Umsetzung von Massnahmen beteiligten.
- Bestehende Gremien / Prozesse / Konzepte: Darstellung der für die Massnahme relevanten, bereits vorhandenen Grundlage als Beschreibung des Ist-Zustandes.
- Rechtssetzungsbedarf: Falls für die Umsetzung der Massnahme rechtliche Grundlagen neu geschaffen oder bestehende Grundlagen angepasst werden müssen, wird dies als Rechtssetzungsbedarf ausgewiesen (vgl. Kapitel 3).
- Umsetzungsprojekte der Massnahme: Übersicht zu den definierten Umsetzungsprojekten.

Anschliessend werden die Umsetzungsprojekte erläutert. Zuerst werden die Inhalte des Projekts kurz erläutert, anschliessend die Zuständigkeit definiert und schliesslich die für die Roadmap relevanten Meilensteine aufgelistet.

6 Roadmap für die Umsetzung

In nachfolgender Roadmap werden pro Handlungsfeld der NCS sämtliche Massnahmen aufgelistet und deren Umsetzungsprojekte mit den entsprechenden Laufzeiten visualisiert.



[illegible]

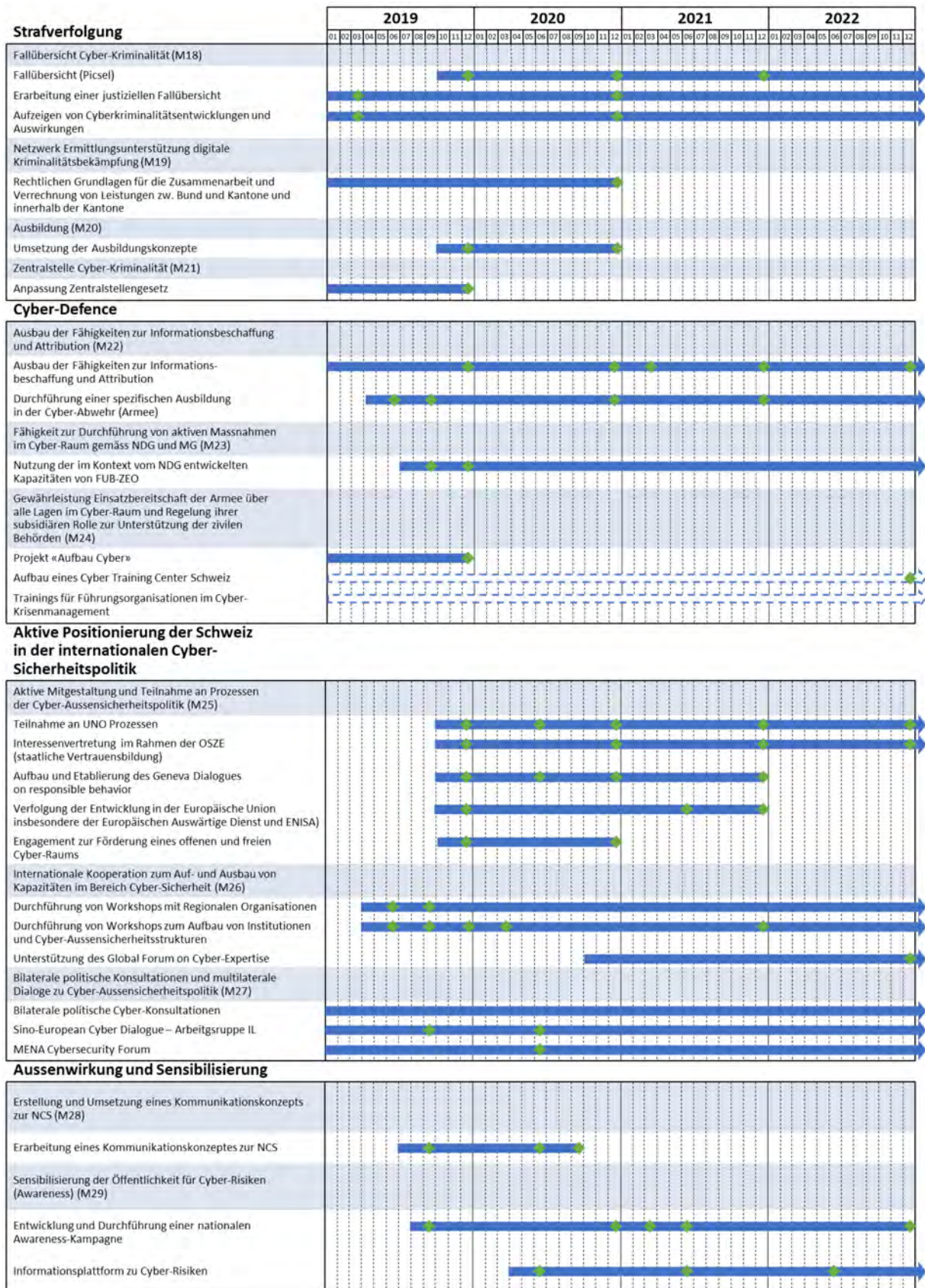


Abbildung 4 Roadmap Übersicht

7 Umsetzungsplan

7.1 Kompetenzen- und Wissensaufbau

Die möglichst frühe Erkennung und die richtige Einschätzung von Cyber-Risiken sind Voraussetzung dafür, dass diese Risiken gemindert werden können. Die entsprechenden Fähigkeiten sollen durch die bestehenden Bildungs- und Forschungsinstitutionen bereichsübergreifend aufgebaut, vermittelt und weiterentwickelt werden. Die Schweiz verfügt über ein leistungsfähiges Netzwerk an Ausbildungs- und Forschungsinstitutionen auf den verschiedenen Stufen. Der Bildungs- und Forschungsplatz Schweiz soll dem Bereich Cyber-Risiken das angemessene Gewicht verleihen und Gesellschaft, Wirtschaft und Behörden mit den notwendigen Kompetenzen und Forschungserkenntnissen versorgen. Die Grundlage für die Erreichung dieser Ziele wird durch Forschung im Bereich der Cyber-Sicherheit geschaffen.

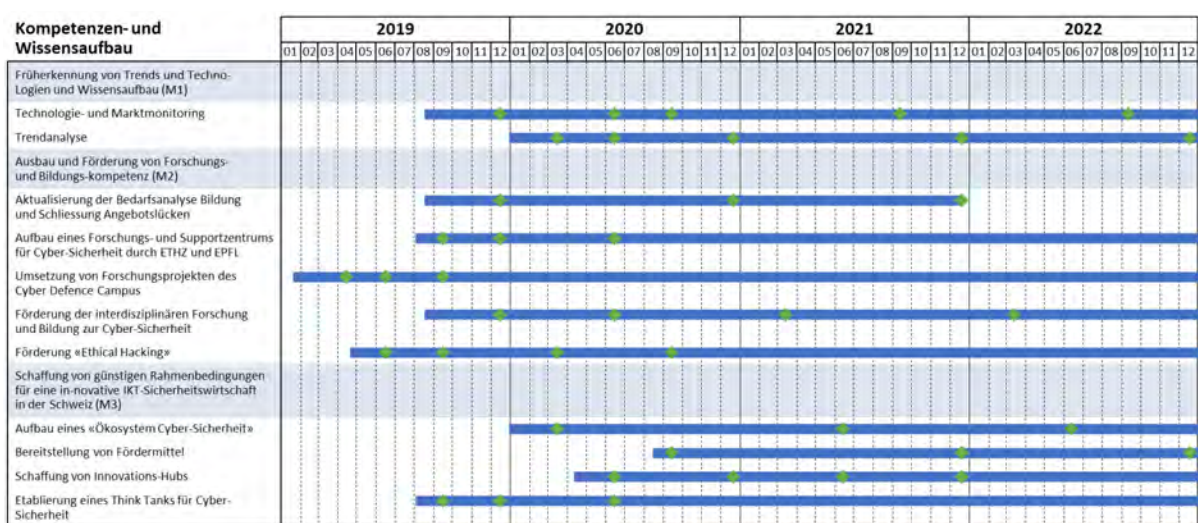


Abbildung 5 Roadmap Kompetenzen- und Wissensaufbau

7.1.1 Früherkennung von Trends und Technologien und Wissensaufbau (M1)

Übersicht Massnahme	
Massnahmenziel	Trends und Technologien im Bereich IKT sowie sich daraus ergebende Chancen und Risiken werden frühzeitig identifiziert und den Akteuren aus Wissenschaft, Politik und Gesellschaft kommuniziert.
Gesamtverantwortung für Massnahme	armasuisse W+T
Beteiligung Bundstellen	Kompetenzzentrum Cyber-Sicherheit, SBFI
Beteiligung Dritter	Hochschulen, SATW (Trendanalyse)
Bestehende Gremien / Prozesse / Konzepte	Cyber Defence Campus der armasuisse W+T: Antizipationsplattform zum Monitoring und Früherkennung von Cyber-Technologien

Rechtssetzungsbedarf	Das Kompetenzzentrum Cyber-Sicherheit soll die Aufgabe erhalten, für den zivilen Bereich Analysen zu Trends und Technologien durchzuführen oder in Auftrag zu geben und darüber auch der Öffentlichkeit Bericht zu erstatten.
Umsetzungsprojekte der Massnahme	1. Technologie- und Marktmonitoring: Aufbau eines Monitorings von technologischen Entwicklungen 2. Trendanalyse: Bewertung von technologischen Entwicklungen, Berichterstattung

Umsetzungsprojekte

1. Technologie- und Marktmonitoring	
Projektbeschreibung	Aufbau eines automatisierten Technologie-Radars, welcher bestehende Datenbanken, Websites und Verzeichnisse nutzt, um Trends und Technologien frühzeitig zu erkennen und deren Bedeutung für die Schweiz abzuschätzen.
Zuständigkeit	armasuisse W+T
Meilensteine	 Q4/2019: Leistungen des Cyber Defence Campus der armasuisse W+T für das Monitoring zuhanden des Kompetenzzentrums Cyber-Sicherheit sind festgelegt Q2/2020: Aufnahme des Betriebs des Monitorings Q3/2020: Erste Auswertung zu Monitoring liegt vor Q3/2021: Zweite Auswertung zu Monitoring liegt vor Q3/2022: Dritte Auswertung zu Monitoring liegt vor
2. Trendanalyse	
Projektbeschreibung	Basierend auf den Auswertungen des Technologie- und Marktmonitorings werden qualitative Auswertungen erstellt und die Bedeutung der identifizierten Trends und Technologien für die Schweiz in Bezug auf Cyber-Sicherheit analysiert.
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit
Meilensteine	 Q1/2020: Konzept für Zielpublikum, Inhalte, Verbreitung der Berichte ist erstellt Q2/2020: Aufträge für Auswertung sind erteilt Q4/2020: Erster Bericht publiziert Q4/2021: Zweiter Bericht publiziert Q4/2022: Dritter Bericht publiziert

7.1.2 Ausbau und Förderung von Forschungs- und Bildungskompetenz (M2)

Übersicht Massnahme	
Massnahmenziel	Es wird im Austausch zwischen Wirtschaft, den Hochschulen, Bund und Kantonen analysiert, welcher Bedarf in Bezug auf die Kompetenzbildung zu Cyber-Risiken besteht. Dabei wird insbesondere geprüft, wie das Thema Cyber-Risiken, unter Berücksichtigung der Hochschulautonomie, verstärkt in bestehende Ausbildungsgänge integriert werden kann und wie Talente im Bereich «Ethical Hacking» gefördert werden können. Die für das Verständnis von Cyber-Risiken nötige Grundlagen- und angewandte Forschung werden gestärkt und es werden Möglichkeiten aufgezeigt, wie die interdisziplinäre Forschung gezielt gefördert werden kann. Über den Cyber Defence Campus (CYD-Campus) entwickelt das VBS Kompetenzen und Wissen im Bereich Cyber Defence.
Verantwortung für Massnahme	Kompetenzzentrum Cyber-Sicherheit (für den Bereich Cyber Sicherheit) und armasuisse W+T mit dem CYD Campus (für den Bereich der Cyber-Defence)
Beteiligung Bundesstellen	SBFI
Beteiligung Dritter	Hochschulen, ICT-Berufsbildung Schweiz, SATW (Erarbeitung Forschungsübersichten, Identifizierung von Forschungslücken), Universität Zürich; Bankenvertreter (Bedarfsanalyse).
Bestehende Gremien / Prozesse / Konzepte	• Bericht: «Forschung zu Cyber-Risiken in der Schweiz: Expertenbericht 2017 zur Identifikation der wichtigsten Forschungsthemen» • Forschungsprogramm des Cyber Defence Campus • Aktionsplan Digitalisierung im BFI-Bereich in den Jahren 2019 und 2020 • Bedarfsanalyse: «Kompetenzbildungsangebote im Umgang mit Cyber-Risiken» (2015) • Zusammenarbeit Bund, Wirtschaft zur Schaffung neuer Abschlüsse der Berufsbildung im Rahmen von ICT-Berufsbildung Schweiz. • Canvas-Projekt (EU H2020) unter der Leitung der Universität Zürich zu rechtlichen und ethischen Fragen im Bereich Cyber-Sicherheit • Swiss Cyber Storm mit «European Cybersecurity Challenge»
Umsetzungsprojekte der Massnahme	1. Aktualisierung der Bedarfsanalyse Bildung und Schliessung Angebotslücken 2. Aufbau eines Forschungs- und Supportzentrums für Cyber-Sicherheit durch EPFL und ETHZ: Zusammenarbeit mit übrigen Hochschulen 3. Umsetzung von Forschungsprojekten des Cyber Defence Campus 4. Förderung der interdisziplinären Forschung und Bildung zur Cyber-Sicherheit 5. Förderung «Ethical Hacking»

Umsetzungsprojekte

1. Aktualisierung der Bedarfsanalyse Bildung und Schliessung Angebotslücken	
Projektbeschreibung	Die Bedarfsanalyse zur zielgruppengerechten Schaffung von Bildungsangeboten wird aktualisiert. Basierend auf der Analyse werden vorhandene Angebote in existierenden Bildungsstrukturen identifiziert und Angebotslücken mit bedarfsge-rechten Massnahmen aufgezeigt.
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit in Zusammenarbeit mit Verbänden (bspw. ICT-Berufsbildung Schweiz), EPFL
Meilensteine	 Q4/2019: Bedarfsanalyse erstellt und Zielgruppen sind definiert Q4/2020: Übersicht der bestehenden Bildungsangebote ist erstellt Q4/2021: Angebotslücken sind identifiziert und Möglich-keiten diese zu schliessen sind aufgezeigt Q4/2021 Durchführung von Trainingsmassnahmen auf Schweizer Ebene

2. Aufbau eines gemeinsamen Forschungs- und Supportzentrums für Cyber-Sicherheit durch ETHZ und EPFL	
Projektbeschreibung	Schaffung eines gemeinsamen Forschungs- und Support-zentrums für Cyber-Sicherheit der ETHZ und der EPFL. Das Forschungszentrum soll eng mit den relevanten Stellen des Bundes (insbesondere mit dem Kompetenzzentrum Cyber-Sicherheit) und der Kantone zusammenarbeiten und zur An-laufstelle für die Verwaltung zum ETH-Bereich für Fragen zur Cyber-Sicherheit werden. Sie soll auch zur Vernetzung der Forschung beitragen und den Wissenstransfer in die Wirt-schaft stärken.
Zuständigkeit	EPFL und ETHZ
Meilensteine	 Q3/2019: Konzept für das Forschungs- und Supportzent-rum ist erstellt Q4/2019: Fragen der Finanzierung und Lokalität ist sind geklärt Q2/2020: Forschungszentrum nimmt Betrieb auf, mit schrittweisen Ausbau in der Jahren 2021-2022

3. Umsetzung von Forschungsprojekten des Cyber Defence Campus	
Projektbeschreibung	Der Cyber Defence Campus setzt ein eigenes Forschungs-programm für Forschungsprojekte mit Relevanz für die Cyber Defence um. Er arbeitet dabei direkt mit der ETHZ und der E-PFL zusammen und etabliert eigene Forschungsstandorte an diesen Hochschulen.
Zuständigkeit und einge-setzte Ressourcen	armasuisse W+T
Meilensteine	 Q1/2019: Standort Thun nimmt Betrieb auf Q2/2019: Standort EPFL nimmt Betrieb auf Q3/2019: Standort ETHZ nimmt Betrieb auf

4. Förderung der interdisziplinären Forschung und Bildung zur Cyber-Sicherheit	
Projektbeschreibung	Der Austausch zwischen den verschiedenen Forschungsrichtungen im Bereich Cyber-Risiken wird gefördert. Es wird ein informelles Netzwerk von Forschenden aufgebaut, welches zu besserem gegenseitigem Verständnis und zu gemeinsamen Forschungsprojekten führen soll.
Zuständigkeit	armasuisse W+T und Kompetenzzentrum Cyber-Sicherheit in Zusammenarbeit mit SATW (Vernetzung Forschende, Sensibilisierung)
Meilensteine	 Q4/2019: Wichtigste Forschungsinstitute der Schweizer Hochschulen im Bereich Cyber-Risiken sind identifiziert Q2/2020: Bedarfsabklärung unter den identifizierten Instituten Q1/2021: Form und Inhalte des regelmässigen Austausches unter den Beteiligten sind definiert Q1/2022: Austausch findet statt

5. Förderung «Ethical Hacking»	
Projektbeschreibung	Durch die Unterstützung und Förderung verschiedener bereits etablierter Anlässe im Themenbereich «Ethical Hacking» soll der Wissensaufbau und -austausch in diesem Themengebiet gestärkt werden sowie das Netzwerk ausgebaut werden. Die Durchführung eines Swiss Hacking Contest ermöglicht es, dass sich die Teilnehmer in einem Wettbewerb messen können und das Thema «Ethical Hacking» einem breiten Publikum präsentiert werden kann. Zudem werden damit junge Talente in diesem Bereich identifiziert sowie gefördert.
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit
Meilensteine	 Q2/2019: Etablierte Anlässe im Bereich «Ethical Hacking» sind identifiziert Q3/2019: Förderinstrumente sind ausgestaltet; Finanzmittel, wenn nötig beantragt Q1/2020: Fördermittel stehen zur Verfügung Q3/2020: Durchführung Swiss Hacking Contest

7.1.3 Schaffung von günstigen Rahmenbedingungen für eine innovative IKT-Sicherheitswirtschaft in der Schweiz (M3)

Übersicht Massnahme	
Massnahmenziel	Die Schweiz soll ein attraktiver Standort für Unternehmen im Bereich der IKT-Sicherheit sein. Über einen verstärkten Austausch zwischen Wirtschaft und Forschung soll ein günstiges Umfeld für Innovationen und Start-ups geschaffen werden.
Verantwortung für Massnahme	Kompetenzzentrum Cyber-Sicherheit
Beteiligung Bundesstellen	armasuisse W+T, Innosuisse
Beteiligung Dritter	Hochschulen, Wirtschaftsverbände, ICTswitzerland
Bestehende Gremien / Prozesse / Konzepte	• Kompetenznetzwerk des Cyber Defence Campus • Förderinstrumente der Innosuisse • Bestehende Innovationszentren
Rechtsetzungsbedarf	Es ist zu klären, welche Aufgaben der Bund beim Aufbau eines «Ökosystems Cyber-Sicherheit» auf der Basis der vorhandenen Rechtsgrundlagen übernehmen kann oder ob Rechtsetzungsbedarf besteht.
Umsetzungsprojekte der Massnahme	1. Aufbau eines «Ökosystem Cyber-Sicherheit» 2. Bereitstellung von Fördermitteln 3. Schaffung von Innovation-Hubs 4. Etablierung eines Think Tanks für Cyber-Sicherheit

Umsetzungsprojekte

1. Aufbau eines «Ökosystem Cyber-Sicherheit»	
Projektbeschreibung	Das Kompetenzzentrum Cyber-Sicherheit etabliert sich als Vermittlungsstelle zwischen Wirtschaft, Hochschulen, Behörden und bestehenden Innovationszentren mit dem Ziel, ein innovatives Ökosystem für Cyber-Sicherheit in der Schweiz zu fördern. Es arbeitet zu diesem Zweck mit dem Kompetenznetzwerk des Cyber Defence Campus der armasuisse W+T zusammen, welches den Kompetenzpol für die Zusammenarbeit zwischen Hochschulen und Wirtschaft im Bereich der Cyber Defence bildet.
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit gemeinsam mit dem Cyber Defence Campus der armasuisse W+T und ICTswitzerland
Meilensteine	 Q1/2020: Gemeinsame Planung des Kompetenzzentrums und des Cyber Defence Campus zu den Massnahmen für Austausch mit Wirtschaft und Hochschulen liegt vor Q2/2021: Erste Massnahmen zur Förderung des Austausches sind durchgeführt. Q2/2022: Anlaufstelle hat sich etabliert

2. Fördermittel	
Projektbeschreibung	Es werden Fördermittel für Innovationsprojekte von Hochschulen, Verbände und Unternehmen im Bereich Cyber-Sicherheit identifiziert und ausgewiesen. Es wird geprüft, über welche Förderinstrumente (z.B. nationale thematische Netzwerke, F&E Innovationsprojekte; eigenes Förderprogramm) die Innovation im Bereich Cyber-Sicherheit am effektivsten gefördert werden kann.
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit gemeinsam mit Innosuisse
Meilensteine	 Q3/2020: Analyse zu den Möglichkeiten der Förderung ist abgeschlossen, Instrumente sind definiert Q4/2021: Förderinstrumente sind ausgestaltet Q4/2022: Förderinstrumente stehen zur Verfügung

3. Aufbau von Innovationszentren	
Projektbeschreibung	Es wird geprüft, wie rund um das Kompetenzzentrum Cyber-Sicherheit ein Cyber-Hub (inklusive des Forschungszentrums der ETH, Einbezug Ökosystem Cyber Sicherheit und Campus Cyber Defence sowie Forschungsnetzwerk) aufgebaut werden kann. Als Teil des Netzwerks wird Innovation im Bereich Cyber-Sicherheit an bestehenden oder neu geschaffenen regionalen Innovationszentren gezielt gefördert.
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit
Meilensteine	 Q2/2020: Vorschlag für Aufbau und Finanzierung eines nationalen Cyber-Hubs ist erarbeitet Q4/2020: Beschluss über Aufbau eines nationalen Cyber-Hubs Q2/2021: Konzept für Aufbau von regionalen Cyber-Innovationszentren an verschiedenen Standorten sind erstellt Q4/2021: Finanzierung der regionalen Cyber-Innovationszentren ist sichergestellt

4. Etablierung eines Think Tanks für Cyber-Sicherheit	
Projektbeschreibung	Das gemeinsame Forschungs- und Supportzentrum der beiden ETHs wird Analyse- und Antizipationskapazitäten zu Cybersicherheitsthemen bereitstellen. Dank ihrer Technologie- und Governance-Kompetenz kann sie die Schweiz bei der Schaffung günstiger Rahmenbedingungen für Technologieunternehmen unterstützen.
Zuständigkeit und eingesetzte Ressourcen	EPFL und ETHZ

Meilensteine	 Q3/2019: Konzept für das Forschungs- und Supportzentrum ist erstellt Q4/2019: Fragen der Finanzierung und Lokalität ist sind geklärt Q2/2020: Forschungszentrum mit Think Tank nimmt Betrieb auf, mit schrittweisen Ausbau in der Jahren 2021-2022
--------------	--

7.2 Bedrohungslage

Ein Überblick über die aktuelle Bedrohungslage ist ein zentrales Element zum Schutz vor Cyber-Risiken. Er ist die Grundlage für die Wahl und Priorisierung von präventiven und reaktiven Massnahmen und unabdingbar, um bei Vorfällen und in Krisenlagen die richtigen Entscheidungen zu treffen. Zum Schutz der Schweiz vor Cyber-Risiken bleibt die Schweiz darauf angewiesen, über ein gesamtheitliches Cyber-Lagebild zu verfügen. Die bereits vorhandenen Fähigkeiten müssen angesichts der intensivierten Bedrohungslage ausgebaut und der Informationsaustausch mit der Wirtschaft und den Kantonen weiter gestärkt werden. Erkenntnisse über die Bedrohungslage sollen zudem nicht mehr nur den Behörden und Betreibern kritischer Infrastrukturen zur Verfügung gestellt, sondern in geeigneter Form auch weiteren Schweizer Unternehmen und der Bevölkerung zugänglich gemacht werden.

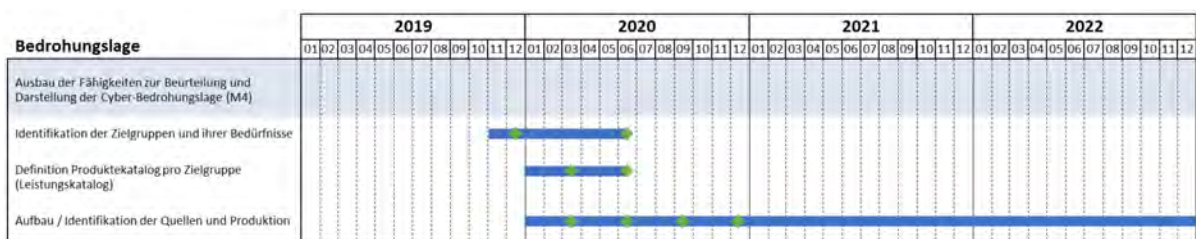


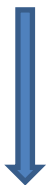
Abbildung 6 Roadmap Bedrohungslage

7.2.1 Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyber-Bedrohungslage (M4)

Übersicht Massnahme	
Massnahmenziel	Zum Schutz der Schweiz vor Cyber-Risiken verfügt die Schweiz über ein gesamtheitliches Cyber-Lagebild. - Die Bedrohungslage wird adressatengerecht aufbereitet und umfasst Abnehmer im technisch-operativen bis zum strategisch-politischen Bereich. - Die systematische und nachhaltige Aufarbeitung und Erfassung von Cyber-Vorfällen ist durch einen Ausbau der vorhandenen Kapazitäten gewährleistet. - Die Systematisierung des OSINT im Cyberbereich ist vollzogen und liefert die benötigte, vollständige Informationsbasis aus öffentlich zugänglichen Quellen. - Bei der Einschätzung von relevanten Bedrohungen werden die Lageeinschätzungen der Strafverfolgung, der Cybersicherheitsexperten, der Armee und des Nachrichtendienstes einbezogen. Der Informationsaustausch mit der Wirtschaft und den Kantonen wird weiter gestärkt. Erkenntnisse über die Bedrohungslage werden nicht nur den Behörden und Betreibern kritischer Infrastrukturen zur Verfügung gestellt, sondern in geeigneter Form auch Schweizer Unternehmen und der Bevölkerung zur Verfügung gestellt.
Verantwortung für Massnahme	NDB (OIC MELANI)
Beteiligung Bundesstellen	fedpol, BA, Kompetenzzentrum Cyber-Sicherheit (GovCert), FUB (MilCERT, CYD), NDB (Cyber NDB, BLZ)

Beteiligung Dritter	Kantone (insbesondere über Cyberboard), Partner aus der Wirtschaft (MELANI GK, SCE), Wissenschaft (Hochschulen) und der Kantone
Bestehende Gremien / Prozesse / Konzepte	- Die Prozesse zur Erstellung der Bedrohungslage, der organisatorischen Abläufe, des Führungsrhythmus sowie der Verantwortlichkeiten zwischen MELANI- ISB/GovCERT, MELANI-OIC und Cyber NDB sind im Rahmen der NCS 1 erfasst, wo nötig ergänzt, getestet und implementiert worden. - Zusammenarbeit mit nationalen und internationalen Partnern.
Umsetzungsprojekte der Massnahme	- Identifikation der Zielgruppen und ihrer Bedürfnisse - Definition Produktkatalog pro Zielgruppe - Identifikation/Aufbau der Quellen und Produktion

Umsetzungsprojekte

1. Identifikation der Zielgruppen und ihrer Bedürfnisse	
Projektbeschreibung	Identifikation bereits abgebildeter Bedürfnisse (Lagebilder vorhanden) und Definition von Zielgruppen. Analyse derer Bedürfnisse bezüglich Inhalte und Vermittlungsart (Aktualität, kurz- und langfristig, operativ oder strategisch) zur Cyber-Bedrohungslage
Zuständigkeit	NDB (OIC MELANI) in Zusammenarbeit mit Vertreter aus Wirtschaft, Gesellschaft, Kanton, Bund (Strafverfolgung, Armee, BWL/BABS)
Meilensteine	 Q4/2019: Identifikation erweiterter Zielgruppen und deren Bedürfnisse liegen vor Q2/2020: Kommunikationskanäle für die jeweiligen Zielgruppen identifiziert (Nationale Anlaufstelle, Alertswiss, Lageradar, Quarterlies, KGCYS-Bulletins usw.)

2. Definition Produktkatalog pro Zielgruppe (Leistungskatalog)	
Projektbeschreibung	Format, Frequenz und Inhalte der Produkte für die verschiedenen Zielgruppen sind definiert. In diesem Kontext ist ebenfalls die Abgrenzung der Aufgabe zwischen Bund und der Wirtschaft (Anbieter von kommerziellen Diensten im Bereich Bedrohungslage) gemäss Subsidiaritätsprinzip vorzunehmen.
Zuständigkeit	NDB (OIC MELANI) in Zusammenarbeit mit Vertreter aus Wirtschaft, Gesellschaft, Kantone (Strafverfolgung) und Bund (Strafverfolgung, Armee, BWL/BABS)
Meilensteine	 Q1/2020: Aufgabenbereich zw. Bund und Wirtschaft geklärt Q2/2020: Leistungskatalog per Zielgruppe definiert

3. Aufbau benötigter Quellen und Produktionsressourcen	
Projektbeschreibung	Identifikation zusätzlich benötigter Quellen zur Erstellung der definierten Leistungen und Aufbau der zusätzlich benötigten Netzwerke zur Wirtschaft und zu internationalen Stellen. Schaffung von analytischen Ressourcen zur Verifizierung, Priorisierung und Einschätzung der vorhandenen Informationen; Technische Unterstützung zur Strukturierung und Auswertung des Informationsaufkommens.
Zuständigkeit	NDB (OIC MELANI) in Zusammenarbeit mit dem Kompetenzzentrum Cyber-Sicherheit
Meilensteine	 Q1/2020: Liste zusätzlich benötigter Quellen erstellt Q2/2020: Ressourcen zur Intensivierung internationaler Beziehungen geschätzt und alloziert Q2/2020: Konzept zur Systematisierung der internen Beschaffung erstellt Q3/2020: Projekt zum Aufbau der technischen Unterstützung vorhanden Q4/2020: Ressourcen zum Aufbau von Quellen, Systematisierung Beschaffung und Produktion geschätzt und alloziert

7.3 Resilienz-Management

Massnahmen zur Reduktion von IKT-Verwundbarkeiten kritischer Infrastrukturen sind von grosser Bedeutung für den Schutz der Schweiz vor Cyber-Risiken. Sie beziehen sich nicht nur auf eine Stärkung der Abwehr, sondern schliessen Massnahmen zur Eindämmung von Schäden und zur Verringerung der Ausfallszeiten bei Vorfällen ein. Die Umsetzung der Massnahmen zur Verbesserung der IKT-Resilienz erfolgt durch die jeweiligen Organisationen und Unternehmen. Der Bund übernimmt eine aktive Rolle bei der Definition von Massnahmen zur Verbesserung der IKT-Resilienz in den kritischen Teilsektoren und überwacht auch deren Umsetzung. Bund und Kantone sind selber zuständig für die Umsetzung der Massnahmen zum Schutz der eigenen kritischen IKT-Infrastrukturen.

Die identifizierten Massnahmen zur Verbesserung der IKT-Resilienz in den kritischen Teilsektoren und in den Verwaltungen sollen umgesetzt, aufeinander abgestimmt und basierend auf periodisch zu aktualisierenden Risiko- und Verwundbarkeitsanalysen weiterentwickelt werden.

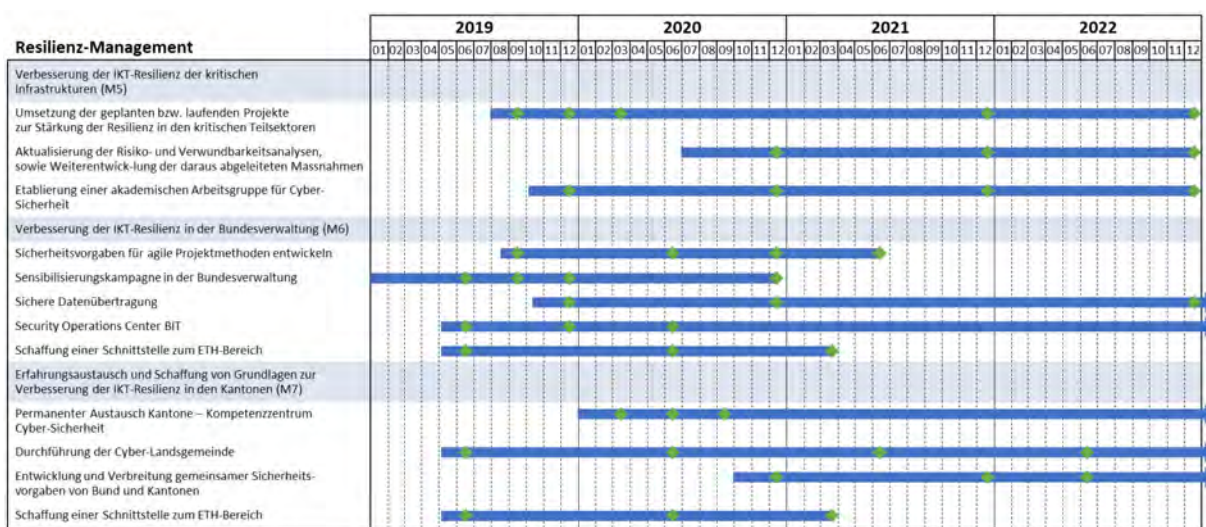


Abbildung 7 Roadmap Resilienz-Management

7.3.1 Verbesserung der IKT-Resilienz der kritischen Infrastrukturen (M5)

Übersicht Massnahme	
Massnahmenziel	Im Fokus steht die Umsetzung von Massnahmen zur Verbesserung der IKT-Resilienz der kritischen Teilsektoren unter Einbezug der relevanten Regulierungsbehörden und Fachämter. Grundlage dafür sind die vorhandenen Risiko- und Verwundbarkeitsanalysen und die daraus abgeleiteten Massnahmenvorschläge. Neben der Umsetzung der identifizierten Massnahmen müssen die Analysen und die Massnahmen regelmässig aktualisiert und wo nötig an neue Erkenntnisse und Entwicklungen angepasst werden.
Verantwortung für Massnahme	BABS in Zusammenarbeit mit den Fachämtern in regulierten Sektoren
Beteiligung	Fachämter (BAKOM, BAG, BAV, BAZL, BFE), BWL, Kompetenzzentrum Cyber-Sicherheit
Beteiligung Dritter	Regulatoren, Branchenverbände, KI-Betreiber

Bestehende Gremien / Prozesse / Konzepte	• Risiko- und Verwundbarkeitsanalysen der kritischen Teilsektoren aus der NCS 2012 – 2017 • Umsetzung der «Nationale Strategie zum Schutz kritischer Infrastrukturen 2018 – 2022» • (Aktualisierung) nationale Risikoanalyse Katastrophen und Notlagen Schweiz 2015 • Zusammenarbeit zwischen Wirtschaft und Behörden im Rahmen der Landesversorgung • Sektor spezifische Vorgaben
Umsetzungsprojekte der Massnahme	1. Umsetzung der geplanten bzw. laufenden Projekte zur Stärkung der Resilienz in den kritischen Teilsektoren 2. Aktualisierung der Risiko- und Verwundbarkeitsanalysen 3. Etablierung einer akademischen Arbeitsgruppe für Cyber-Sicherheit

Umsetzungsprojekte

1. Umsetzung der geplanten bzw. laufenden Projekte zur Stärkung der Resilienz in den kritischen Teilsektoren	
Projektbeschreibung	Umsetzung der im Rahmen der NCS 2012 – 2017 geplanten und in den Massnahmenberichten beschriebenen Massnahmen in den kritischen Teilsektoren.
Zuständigkeit	Koordination, Begleitung und Unterstützung der Arbeiten durch das BABS, in regulierten Sektoren in enger Zusammenarbeit mit den Fachämtern. Die Umsetzung der Massnahmen erfolgt durch Wirtschaftsverbände, Fachämter und Unternehmen.
Meilensteine	 Q3/2019 Bestandesaufnahme der umgesetzten und noch nicht umgesetzten Vorhaben aus den Massnahmenberichten erstellt Q4/2019 Verantwortlichkeiten für die Umsetzung sind geklärt Q1/2020 Roadmap/Planung der laufenden und anstehenden Massnahmen erarbeitet Q4/2021 Abstimmung und Information mit den involvierten Umsetzungsverantwortlichen zum Stand und weiterer Massnahmenumsetzung erfolgt Q4/2022 Übersicht, Standbericht umgesetzter Massnahmen ist erstellt

2. Aktualisierung der Risiko- und Verwundbarkeitsanalysen, sowie Weiterentwicklung der daraus abgeleiteten Massnahmen	
Projektbeschreibung	Periodische Aktualisierung sowie Weiterentwicklung der spezifischen Resilienzarbeiten, Risiko- und Verwundbarkeitsanalysen inkl. Massnahmenvorschläge in den definierten kritischen Teilsektoren (Branchen)

Zuständigkeit und eingesetzte Ressourcen	BABS in Zusammenarbeit mit BWL und den zuständigen Fachämtern, Wirtschaftsverbänden und Unternehmen/Organisationen der kritischen Teilsektoren
Meilensteine	 Q4/2020 Erstes Drittel der Risiko- und Verwundbarkeitsanalysen ist überprüft und entsprechend aktualisiert, die zugehörigen Massnahmen sind geprüft und bei Bedarf weiterentwickelt Q4/2021 Zweites Drittel der Risiko- und Verwundbarkeitsanalysen ist überprüft und entsprechend aktualisiert, die zugehörigen Massnahmen sind geprüft und bei Bedarf weiterentwickelt Q4/2022 Drittes Drittel der Risiko- und Verwundbarkeitsanalysen ist überprüft und entsprechend aktualisiert, die zugehörigen Massnahmen sind geprüft und bei Bedarf weiterentwickelt

3. Etablierung einer akademischen Arbeitsgruppe für Cyber-Sicherheit

Projektbeschreibung	Etablierung einer akademischen Arbeitsgruppe zur Cybersicherheit von kritischen Infrastrukturen, die sich auf die Untersuchung langfristiger Risiken durch neue Technologien konzentriert.
Zuständigkeit	EPFL und ETHZ
Meilensteine	 Q4/2019 Bestandsaufnahme von Projekten und aktiven Gruppen Q4/2020 Institutionalisieren der Arbeitsgruppe Q4/2021 Koordination und Risikoanalyse Q4/2022 Bericht über Massnahmen und Umsetzung

7.3.2 Verbesserung der IKT-Resilienz in der Bundesverwaltung (M6)

Übersicht Massnahme	
Massnahmenziel	Die Verbesserung der Resilienz der IKT in der Bundesverwaltung erfolgt über die Umsetzung und Aktualisierung der bestehenden Vorgaben und Konzepte im Rahmen eines Informationssicherheitsmanagements, über die Sensibilisierung von Mitarbeitenden der Bundesverwaltung und über technische Massnahmen zur sicheren Datenübertragung.
Verantwortung für Massnahme	Kompetenzzentrum Cyber-Sicherheit
Beteiligung	IT-Leistungserbringer des Bundes, Informatik- und Informationssicherheitsbeauftragte der Departemente, Informations- und Objektsicherheit (IOS), Risikomanagement Bund
Bestehende Gremien / Prozesse / Konzepte	Ausschuss Informatiksicherheit des Bundes

Umsetzungsprojekte der Massnahme	1. Sicherheitsvorgaben für agile Projektmethoden entwickeln 2. Sensibilisierungskampagne in der Bundesverwaltung 3. Sichere Datenübertragung durch neue Technologien: Testbetrieb SCION2 4. Security Operations Center BIT 5. Schaffung einer Schnittstelle zum ETH-Bereich
----------------------------------	---

Umsetzungsprojekte

1. Sicherheitsvorgaben für agile Projektmethoden entwickeln	
Projektbeschreibung	Projektmethoden (z. B. HERMES) werden mit Sicherheitsaspekten (Security by Design) erweitert. Dazu wird geprüft, wie bestehende Sicherheitsvorgaben angepasst werden können, damit sie bei agilen Projektmethoden rechtzeitig berücksichtigt werden.
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit in Abstimmung mit HERMES Fachgruppe von eCH
Meilensteine	 Q3/2019: Bestehenden sicherheitsrelevanten Aufgaben und Ergebnisse in Projektmethoden analysiert Q2/2020: Zusätzliche Aufgaben und Ergebnisse sowie Ergänzungen bestehender Teile identifiziert und beschrieben Q4/2020: Vernehmlassung der geplanten sicherheitsrelevanten Änderungen in der Fachgruppe durchgeführt Q2/2021: Änderungen am Projektstandard vorgenommen
2. Sensibilisierungskampagne in der Bundesverwaltung	
Projektbeschreibung	Konzeption und Durchführung einer adressatengerechten Sensibilisierungskampagne IKT-Sicherheit in der Bundesverwaltung
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit
Meilensteine	 Q4/2018: Grobkonzept Sensibilisierungskampagne IKT-Sicherheit in der Bundesverwaltung «SIB 19» erstellt Q2/2019: Start der Sensibilisierungskampagne IKT-Sicherheit in der Bundesverwaltung «SIB» Q3/2019: Abstimmung mit aktiven Akteuren zur konzeptionellen Ausdehnung zu einer nationalen Kampagne durchgeführt (siehe M29 «Sensibilisierung der Öffentlichkeit für Cyber-Risiken») Q4/2019: Erstellung eines weiteren Massnahmenplans für die Jahre 2021/2022 Q4/2020: Berichterstattung über die Durchführung sowie Wirksamkeit der «SIB»

² Scalability, Control, and Isolation on Next-Generation Networks

3. Sichere Datenübertragung	
Projektbeschreibung	Mit SCION ³ wurde an der ETH Zürich eine hochsichere Technologie für Kommunikationsnetzwerke entwickelt. Basierend auf dieser werden Pilotprojekte aufgebaut und betrieben. Die Ergebnisse der Pilotphase werden in einem Evaluationsbericht dokumentiert. Erkenntnisse daraus sollen ebenfalls in die Bereitstellung einer resilienten Infrastruktur für kritische Aufgaben mit einfließen (M5 und M7).
Zuständigkeit	ETHZ, BIT in Abstimmung mit den anderen LEs (insb. FUB)
Meilensteine	 Q4/2019: Absichtserklärung interessierter Bedarfsträger und Pilotanwendern Q4/2020: Aufbau und Inbetriebnahme der Pilotanwendungen umgesetzt Q4/2022: Evaluationsbericht des Pilotbetriebes erstellt

4. Security Operations Center BIT	
Projektbeschreibung	Die Effizienz in der Bearbeitung von IKT-Sicherheitsvorfällen soll durch den Aufbau und die Operationalisierung eines Security Operations Centers (SOC) im BIT gesteigert werden. Repetitive Aufgaben sollen auf weniger teure Stellenprofile verschoben werden. Damit entsteht eine «1st Line of Defense». Das Monitoring sicherheitsrelevanter Ereignisse auf den Systemen wird ausgebaut und die Behandlung von definierten Standard-Vorfällen wird in das SOC verschoben. Dieses wird auch für die Bearbeitung von sicherheitsrelevanten Change-Anträgen (z.B. Firewall-Öffnungen) zuständig sein. Mit diesen Massnahmen werden zudem die Prozesse zur Vorfallbearbeitung und das System-Monitoring weiter optimiert und die Spezialisten des CSIRT BIT können vermehrt für Analysen eingesetzt werden.
Zuständigkeit	BIT
Meilensteine	 Q2/2019: Konzept und Umsetzungsplan Q4/2019: Umsetzung abgeschlossen Q2/2020: Operationelle Reife erreicht

5. Schaffung einer Schnittstelle zum ETH-Bereich	
Projektbeschreibung	Das gemeinsame Forschungs- und Unterstützungszentrum der beiden ETHs bietet eine ideale einheitliche Schnittstelle, um die Interaktionen der Kantone mit den Universitäten im Bereich der Cyber-Sicherheit zu koordinieren und das Handeln von Bund und Kantonen im Hinblick auf die jüngsten disruptiven Entwicklungen zu überwachen und anzupassen.
Zuständigkeit	EPFL und ETHZ

³ SCION <https://www.scion-architecture.net/>

Meilensteine	 Q2/2019: Koordination mit der Delegiertenstelle des Bundesrates für Cyber-Risiken Q2/2020: Durchführung konkreter Massnahmen Q1/2021: Gemeinsame Koordination
--------------	--

7.3.3 Erfahrungsaustausch und Schaffung von Grundlagen zur Verbesserung der IKT-Resilienz in den Kantonen (M7)

Übersicht Massnahme	
Massnahmenziel	Es wird ein Behördennetzwerk geschaffen (oder bestehende Netzwerke genutzt) um Erfahrungen auszutauschen und gemeinsame Grundlagen für die Stärkung der IKT-Resilienz in den Kantonen zu schaffen. Ziel ist die gegenseitige Unterstützung und ein koordiniertes Vorgehen der Behörden aus Bund und Kantonen.
Verantwortung für Massnahme	Kompetenzzentrum Cyber-Sicherheit, SVS
Beteiligung	Schweizerische Informatikkonferenz (SIK), Schweizerische Staatsschreiberkonferenz (SSK), Konferenz der kantonalen Polizeidirektoren (KKPKS) und weitere Fachkonferenzen der Kantone
Bestehende Gremien / Prozesse / Konzepte	• Cyber-Landsgemeinde des SVS (Konferenz für die Kantone zur Cyber-Sicherheit) -> Operative Plattform des SVS) • Fachgruppe zur Cyber-Sicherheit des SVS • Schulungsmaterial der KKPKS zu Cyber
Umsetzungsprojekte der Massnahme	1. Permanenter Austausch Kantone – Kompetenzzentrum Cyber-Sicherheit 2. Jährliche Durchführung der Cyber Landsgemeinde 3. Entwicklung und Verbreitung gemeinsamer Sicherheitsvorgaben von Bund und Kantonen 4. Schaffung einer Schnittstelle zum ETH-Bereich

Umsetzungsprojekte

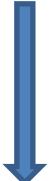
1. Permanenter Austausch Kantone – Kompetenzzentrum Cyber-Sicherheit	
Projektbeschreibung	Schaffung einer Arbeitsplatzmöglichkeit für Kantonsmitarbeitende im Kompetenzzentrum Cyber-Sicherheit, zum Austausch von Informationen sowie Erfahrungen im Kampf gegen die Cyber-Bedrohungen «Know-how-Transfer»
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit

Meilensteine	 Q1/2020 Anforderungskklärung der Arbeitsplatzausstattung (Anforderungskatalog) durchgeführt Q2/2020 Initialisierung sowie Beantragung der Büroinfrastruktur ist erfolgt Q3/2020 Identifikation sowie Definition der Kommunikationsart und –Kanäle in Zusammenarbeit mit SVS und KKJPD erledigt
--------------	--

2. Durchführung der Cyber-Landsgemeinde

Projektbeschreibung	Jährlich wird eine Cyber-Tagung für die Kantone durchgeführt. Diese dient dem Informationsaustausch unter den Kantonen und zwischen Kantonen und Bund.
Zuständigkeit	SVS
Meilensteine	 Q2/2019 Durchführung Landsgemeinde Q2/2020 Durchführung Landsgemeinde Q2/2021 Durchführung Landsgemeinde Q2/2022 Durchführung Landsgemeinde

3. Entwicklung und Verbreitung gemeinsamer Sicherheitsvorgaben von Bund und Kantonen

Projektbeschreibung	Entwicklung und Verbreitung eines minimalen Cyber-Sicherheits-Standards für die Schweizer Behörden
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit, BWL, Kantonsvertretungen (SIK, SVS)
Meilensteine	 Q4/2020 Bedarfsklärung (Anforderungskatalog) durchgeführt Q4/2021 Standard verabschiedet Q2/2022 Vorgehen für Pflege und allfällige Weiterentwicklung des Standards durch Kantone und Bund ist geklärt

4. Schaffung einer Schnittstelle zum ETH-Bereich

Projektbeschreibung	Das gemeinsame Forschungs- und Unterstützungszentrum der beiden ETHs bietet eine ideale einheitliche Schnittstelle, um die Interaktionen der Kantone mit den Universitäten im Bereich der Cyber-Sicherheit zu koordinieren und das Handeln von Bund und Kantonen im Hinblick auf die jüngsten disruptiven Entwicklungen zu überwachen und anzupassen.
Zuständigkeit	EPFL und ETHZ
Meilensteine	 Q2/2019: Koordination mit dem SVS Q2/2020: Durchführung konkreter Massnahmen Q1/2021: Gemeinsame Koordination

7.4 Standardisierung / Regulierung

IKT-Standardisierungen und -Regulierungen sind wichtige Instrumente zum Schutz vor Cyber-Risiken. Minimalanforderungen zu Schutzvorkehrungen stärken die Prävention und Vorgaben zum Umgang mit Vorfällen (z.B. Meldepflichten) tragen zu einer verbesserten Reaktion bei. Standardisierung und Regulierung sind auch im internationalen Umfeld wichtig, da sie mehr Transparenz und Vertrauen in der globalisierten digitalen Gesellschaft schaffen. Bei der Einführung von Standardisierungen und Regulierungen gilt es aber, die grossen Unterschiede zwischen den Wirtschaftssektoren und den Unternehmen verschiedener Grösse zu beachten. Zudem ist in jedem Fall das internationale Umfeld zu beachten. Standards und Regulierungen müssen im grenzüberschreitenden Cyber-Raum international möglichst kompatibel sein. Überprüfbare IKT-Minimalstandards sind relevant für Sicherheit und Vertrauen in der digitalen Wirtschaft und Gesellschaft und sollen in Zusammenarbeit mit der Privatwirtschaft evaluiert und wo sinnvoll eingeführt werden. Ebenfalls zu prüfen ist, ob und wie eine Meldepflicht für Cyber-Vorfälle eingeführt werden soll. Der internationale Kontext wird bei den Massnahmen berücksichtigt und beeinflusst diese wesentlich, weshalb die Entwicklungen weiterhin verfolgt werden müssen.

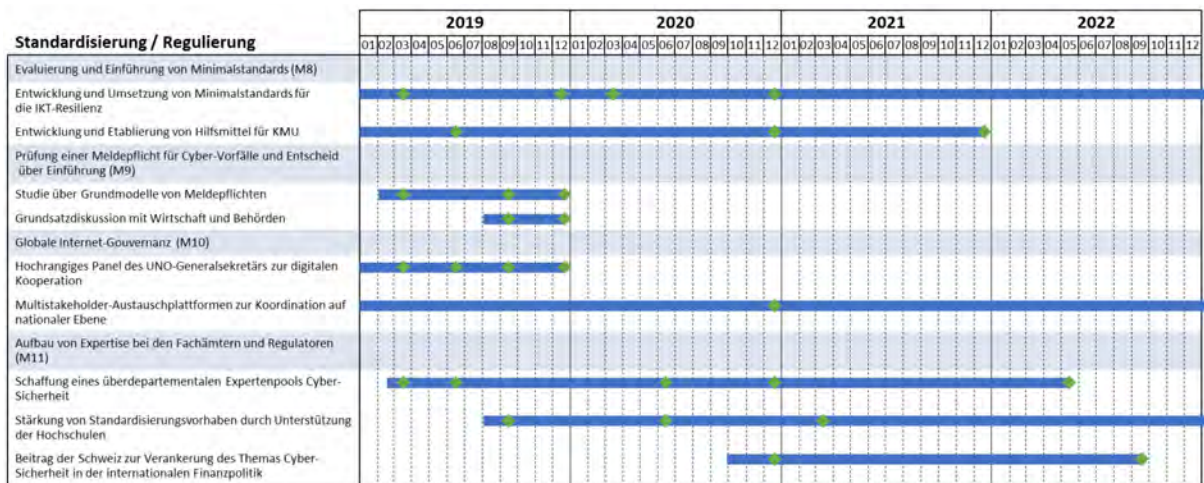


Abbildung 8 Roadmap Standardisierung / Regulierung

7.4.1 Evaluierung und Einführung von Minimalstandards (M8)

Übersicht Gesamtmassnahme	
Massnahmenziel	Auf der Basis der durchgeführten Risiko- und Verwundbarkeitsanalysen werden in enger Zusammenarbeit zwischen den Fachbehörden, der Privatwirtschaft und den Verbänden überprüfbare IKT-Minimalstandards erarbeitet und eingeführt. Die zu erarbeitenden IKT-Minimalstandards bauen auf bestehenden Standards (bspw. IKT-Minimalstandard der WL) auf. Die zuständigen Behörden prüfen, für welche Organisationen und Tätigkeiten die Standards verbindlich sein sollen.
Verantwortung für Massnahme	BWL
Beteiligung Bundesstellen	Kompetenzzentrum Cyber-Sicherheit, BABS, Fachämter (BABS, BAG, BAKOM, BAV, BAZL, BFE)

Beteiligung Dritter	Regulatoren, Branchenverbände und Verbände tätig im Bereich Cybersicherheit (bspw. ICTSwitzerland, Schweizer Verband für das Gütesiegel der Cybersicherheit, SVV), SATW (Beisteuern Expertise, Sensibilisierung) und Hochschulen
Bestehende Gremien / Prozesse / Konzepte	• Risiko- und Verwundbarkeitsanalysen aus der NCS 2012 – 2017 • Schlussbericht der Expertengruppe „Zukunft der Datenbearbeitung und Datensicherheit“ • Bestehende Zusammenarbeit zwischen Wirtschaft und Bund im Rahmen der Wirtschaftlichen Landesversorgung • Bestehende sektorielle Zusammenarbeit
Rechtsetzungsbedarf	In den Sektoren ist abzuklären, ob und wenn ja welcher Rechtsetzungsbedarf für eine Einführung von Minimalstandards zur Cyber-Sicherheit besteht.
Umsetzungsprojekte der Massnahme	1. Entwicklung und Umsetzung von Minimalstandards zur Verbesserung der IKT-Resilienz 2. Entwicklung und Etablierung von Hilfsmitteln für KMU

Umsetzungsprojekte

1. Entwicklung und Umsetzung von Minimalstandards für die IKT-Resilienz	
Projektbeschreibung	Basierend auf dem internationalen NIST-Standard für Cybersicherheit wurde für die Schweiz ein Minimalstandard für die IKT-Resilienz erarbeitet und Hilfsmittel für seine Umsetzung entwickelt. In Zusammenarbeit mit den Branchenverbänden werden auf der Grundlage des allgemeinen IKT-Minimalstandards der WL sektorspezifische IKT-Minimalstandards erstellt und eingeführt. In Sektoren mit bestehenden Regulierungen zur IKT-Sicherheit, gehen diese vor.
Zuständigkeit	BWL in Zusammenarbeit mit den Fachbehörden, Fachämtern (BAG, BAKOM, BAV, BAZL, BFE) und Branchenverbänden; Einbezug der zuständigen Fachämter und Regulatoren der kritischen Teilsektoren, Unternehmen/Organisationen und der Hochschulen
Meilensteine	 Q2/2018 Publikation des IKT-Minimalstandards und Hilfsmittel für das Assessment Q2/2018 Minimalstandard «Handbuch Grundschatz» des Verbands Schweiz. Elektrizitätsunternehmen (VSE) Q1/2019 Wasserversorgung Q1/2019 Lebensmittel Q4/2019 Erdgasversorgung Q1/2020 Öffentlicher Verkehr Q4/2020 Telekommunikation

2. Entwicklung und Etablierung von Hilfsmittel für KMU	
Projektbeschreibung	Zur Unterstützung KMU erarbeitet der Bund gemeinsam mit der Wirtschaft und Verbände Hilfsmittel, mit welchen Unternehmen einfach und schnell erkennen, wie sie in Bezug auf die Cyber-Sicherheit aufgestellt sind, die Bewertung ihre Cyber-Risiken und mit welchen Massnahmen sie ihre Sicherheit verbessern können. Geprüft wird auch, ob und allenfalls durch wen Labels oder Normen für Cyber-Sicherheit geschaffen oder unterstützt werden sollen.
Zuständigkeit und eingesetzte Ressourcen	Kompetenzzentrum Cyber-Sicherheit, BWL, Wirtschaftsverbände
Meilensteine	 Q3/2018 Publikation Cybersecurity-Schnelltest für KMU (SATW) Q2/2019 Bedarfsanalyse zu weiteren Hilfsmittel (technische Hilfsmittel, Labels, Leitfäden, Anleitungen) für KMU Q4/2020 Prüfung möglicher Einführung von Labels und Normen ist abgeschlossen Q4/2021 Analyse geschaffener Hilfsmittel und bei Bedarf Konzeption weiterer Instrumente

7.4.2 Prüfung einer Meldepflicht für Cyber-Vorfälle und Entscheid über Einführung (M9)

Übersicht Massnahme	
Massnahmenziel	Eine Meldepflicht für Cyber-Vorfälle wird geprüft und es wird über ihre Einführung entschieden. Dabei wird zunächst geklärt, für wen eine Meldepflicht gelten soll, welche Vorfälle sie betrifft, an Meldung erstattet werden muss und ob eine Meldepflicht im Vergleich zu heute das Lagebild substanziell verbessern kann. Basierend auf diesen Fragen werden Varianten für die Umsetzung von Meldepflichten in den verschiedenen Sektoren erarbeitet und aufgezeigt, welche gesetzlichen Grundlagen dafür nötig sind. Die Arbeiten erfolgen unter Einbezug der zuständigen Behörden, der Wirtschaft, der Hochschulen und der Kantone. Sie bilden die Grundlage für den Entscheid über die Einführung einer Meldepflicht.
Verantwortung für Massnahme	Kompetenzzentrum Cyber-Sicherheit
Beteiligung Bundesstellen	BABS, Fachämter (BAG, BAKOM, BAV, BAZL, BFE), fedpol
Beteiligung Dritter	Wirtschaftsverbände (bspw. SVV), Kantone, FINMA (Meldepflicht), Hochschulen, ICTswitzerland
Bestehende Gremien / Prozesse / Konzepte	Es bestehen sektorielle Meldepflichten (z.B. in den Bereichen Fernmeldewesen, Kernanlagen, Luftfahrt). Im Fernmeldebereich werden Weiterentwicklung der bestehenden Pflichten zu prüfen sein.

Rechtssetzungsbedarf	Die rechtlichen Grundlagen für die Einführung einer Meldepflicht müssen erarbeitet oder überarbeitet werden, soweit sie nicht bereits vorliegen (z.B. Fernmeldegesetz).
Umsetzungsprojekte der Massnahme	1. Studie über Grundmodelle von Meldepflichten 2. Grundsatzdiskussion mit Wirtschaft und Behörden

Umsetzungsprojekte

1. Studie über Grundmodelle von Meldepflichten	
Projektbeschreibung	Erarbeitung von Grundlagen mittels Erfassung von bestehenden Meldepflichten sowie Erarbeitung von Grundmodellen von Meldepflichten zu (Cyber-) Sicherheitsvorfällen
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit, BABS, Mitwirkung Fachämter und FINMA
Meilensteine	 Q1/2019 Ausschreibung Grundstudie «Prüfung einer Meldepflicht bei (Cyber-) Sicherheitsvorfällen» Q3/2019 Durchführung der Grundstudie «Prüfung einer Meldepflicht bei (Cyber-) Sicherheitsvorfällen» Q4/2019 Berichterstattung über die Grundmodelle sowie Empfehlungen hierzu

2. Grundsatzdiskussion mit Wirtschaft und Behörden	
Projektbeschreibung	Schaffung von Entscheidungsgrundlagen durch Führung einer Grundsatzdiskussion über Varianten von «Meldepflichten bei (Cyber-) Sicherheitsvorfällen» mit Wirtschaft und Behörden
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit, BABS, Mitwirkung Fachämter, FINMA und ICTswitzerland
Meilensteine	 Q3/2019 Bewertung der Modelle durch Wirtschaft und Politik auf Basis der Ergebnisse der Grundstudie Q4/2019 Berichterstattung mit Empfehlung zur Meldepflicht und weiterführende Information an das Parlament

7.4.3 Globale Internet-Gouvernanz (M10)

Übersicht Massnahme	
Massnahmenziel	Die Schweiz soll sich aktiv und koordiniert für ein internationales Regelwerk zur Nutzung und Weiterentwicklung des Internets einsetzen, welches mit den Schweizer Vorstellungen von Freiheit, Demokratie und (Eigen-)Verantwortung, Grundversorgung, Chancengleichheit, Sicherheit, Menschenrechten und Rechtsstaatlichkeit vereinbar ist. Diesbezüglich sind die nationalen Interessenträger miteinzubeziehen und ihnen gegenüber die relevanten Entwicklungen aufzuzeigen.
Gesamtverantwortung für Massnahme	BAKOM
Beteiligung Bundesstellen	EDA

Beteiligung Dritter	EPFL, ETH
Bestehende Gremien / Prozesse / Konzepte	Übersicht relevanter Prozesse inkl. Priorisierung; Swiss Internet Governance Forum (SwissIGF), Plateforme Tripartite, Geneva Internet Platform (GIP)
Umsetzungsprojekte der Massnahme	1. Hochrangiges Panel des UNO-Generalsekretärs zur digitalen Kooperation 2. Multistakeholder-Austauschplattformen zur Koordination auf nationaler Ebene

Umsetzungsprojekte

1. Hochrangiges Panel des UNO-Generalsekretärs zur digitalen Kooperation	
Projektbeschreibung	Der UNO-Generalsekretär hat das hochrangige Panel zur digitalen Kooperation einberufen, um Vorschläge für eine bessere Kooperation aller staatlichen und privaten Akteure im Bereich der digitalen Gouvernanz zu erarbeiten. Dadurch soll das Vertrauen zwischen den Akteuren und somit auch die Sicherheit im Cyber-Raum gefördert werden. Die Schweiz will die inhaltliche und strategische Ausrichtung dieses Panels mitprägen. Ziel ist die Entwicklung von zukunftsgerichteten Gouvernanz-Strukturen für den digitalen Raum, welche auf Werten und Grundprinzipien wie Rechtstaatlichkeit, Menschenrechte und Demokratie basieren.
Zuständigkeit	BAKOM in Zusammenarbeit mit dem EDA
Meilensteine	 Q2/2018 Lancierung des Panels Q3/2018 Erstes Treffen in New York Q1/2019 Zweites Treffen in Genf Q2/2019 Drittes Treffen in Helsinki Q3/2019 Abschlussbericht Q4/2019 Evaluation Umsetzungsmöglichkeiten

2. Multistakeholder-Austauschplattformen zur Koordination auf nationaler Ebene	
Projektbeschreibung	Eine möglichst demokratische und auf rechtstaatlichen Prinzipien bauende Gouvernanz des Cyber-Raums führt zu mehr Sicherheit. Die Schweiz unterstützt Plattformen, insbesondere das Swiss Internet Governance Forum und die Geneva Internet Platform (GIP), welche die Interessen aller Anspruchsgruppen im Bereich Internet Governance koordinieren und es allen ermöglichen, sich an den Diskussionen zu beteiligen. Ein Austausch mit allen Anspruchsgruppen sowie eine breite Abstützung der Schweizer Positionen hilft, diese besser in den massgeblichen internationalen Gremien und Veranstaltungen einzubringen.
Zuständigkeit	BAKOM, EDA, EPFL und ETH in Zusammenarbeit mit weiteren interessierten Akteuren aus allen Anspruchsgruppen

Meilensteine	 Q4/2018 Swiss-IGF 2018 Q4/2020 Swiss-IGF 2020 Fortlaufend Unterstützung der GIP
--------------	--

7.4.4 Aufbau von Expertise bei den Fachämtern und Regulatoren (M11)

Übersicht Gesamtmassnahme	
Massnahmenziel	Die Fachämter und Regulatoren sollen gezielt Massnahmen erarbeiten, welche zur Stärkung der Cyber-Sicherheit führen. Dazu gehören auch (aber nicht nur) regulatorische Eingriffe. Vielen zuständigen Fachbehörden fehlt aber das spezifische Know-how im Cyber-Bereich. Innerhalb des Kompetenzzentrums Cyber-Sicherheit wird deshalb ein Expertenpool aufgebaut, welcher ergänzt mit dem Fachwissen des BWL im Bereich Standardisierung und des BABS im Bereich Risiko- und Verwundbarkeitsanalysen den zuständigen Stellen zur Verfügung gestellt wird.
Verantwortung für Massnahme	Kompetenzzentrum Cyber-Sicherheit
Beteiligung	Fachämter (BAG, BAKOM, BAV, BAZL, BFE), Regulatoren (FINMA, ElCom, ComCom), BABS, BWL, armasuisse W+T, SIF (Verantwortlich für den Beitrag der Schweiz beim Aufbau von Cyber-Kapazitäten in der internationalen Finanzpolitik)
Bestehende Gremien / Prozesse / Konzepte	Etablierte Zusammenarbeit zwischen MELANI, BABS, BWL, Fachämter und Regulatoren
Rechtssetzungsbedarf	Zu erarbeitende Vereinbarungen zwischen den beteiligten Verwaltungseinheiten
Umsetzungsprojekte der Massnahme	1. Schaffung eines überdepartementalen Expertenpools Cyber-Sicherheit zur Unterstützung der Fachämter 2. Stärkung von Standardisierungsvorhaben durch die Unterstützung der Hochschulen 3. Beitrag der Schweiz zur Verankerung des Themas Cyber-Sicherheit in der internationalen Finanzpolitik

Umsetzungsprojekte

1. Schaffung eines überdepartementalen Expertenpool Cyber	
Projektbeschreibung	Die Aufgaben und Ressourcen des Expertenpools sind zu definieren und es wird festgelegt, wer Kompetenzen zur Verfügung stellt und welche Stellen diese zu welchen Bedingungen beziehen können.
Zuständigkeit und eingesetzte Ressourcen	Kompetenzzentrum Cyber-Sicherheit, BABS, BWL, armasuisse W+T, BIT, FUB, Mitwirkung Fachämter

Meilensteine	 Q1/2019 Bedarfsabklärung mit den betroffenen Stellen Q2/2019 Konzeption des Expertenpools und Beschluss der Ressourcen Q2/2020 Vereinbarungen zwischen betroffenen Stellen sind unterzeichnet Q4/2020 Rekrutierungen abgeschlossen, Expertenpool ist fertig ausgebaut Q2/2022 Evaluation des Expertenpools und Vorschläge zur Weiterentwicklung
--------------	---

2. Stärkung von Standardisierungsvorhaben durch die Unterstützung der Hochschulen

Projektbeschreibung	Das gemeinsame Forschungs- und Unterstützungszentrum der beiden ETHs wird die Beteiligung der beiden Hochschulen an Standardisierungsaktivitäten im Bereich Cybersicherheit unterstützen..
Zuständigkeit	EPFL und ETHZ
Meilensteine	 Q3/2019 Konzept der Gemeinsamen Forschungs- und Unterstützungsstelle EPFL-ETHZ erstellt Q2/2020 Überblick über die Aktivitäten der Schweiz in diesem Bereich erstellt Q1/2021 Umsetzung der Aktivitäten in den als strategisch identifizierten Arbeitsgruppen

3. Beitrag der Schweiz zur Verankerung des Themas Cyber-Sicherheit in der internationalen Finanzpolitik

Projektbeschreibung	Die Schweiz engagiert sich aktiv in den internationalen Gremien zur Cyber-Sicherheit in der Finanzwirtschaft (z.B. G20 und Financial Stability Board) und trägt zur Stärkung der Schweizer Interessen im Bereich der internationalen Cyber-Sicherheit in diesem Sektor bei.
Zuständigkeit	SIF
Meilensteine	 Q4/2020 Erster Zwischenbericht zu den Aktivitäten zur Stärkung der internationalen Cyber-Kapazitäten in der Finanzwirtschaft Q3/2022 Zweiter Zwischenbericht zu den Aktivitäten zur Stärkung der internationalen Cyber-Kapazitäten in der Finanzwirtschaft

7.5 Vorfallbewältigung

Da es keinen vollständigen Schutz gegen Cyber-Vorfälle gibt und mit einer zunehmenden Anzahl gezielter Angriffe zu rechnen ist, gehört der Aufbau und Betrieb einer Organisation zur Bewältigung von Vorfällen (Incident-Management) zu den Kernaufgaben im Umgang mit Cyber-Risiken. Für die Bewältigung dieser Aufgabe braucht es Fachkompetenzen, Analyseinstrumente, eine gut funktionierende Organisation und eine intensive Zusammenarbeit zwischen allen relevanten Stellen. Entscheidend ist der Informationsaustausch zwischen vertrauenswürdigen Partnern über Vorfälle und mögliche Gegenmassnahmen, da Vorfälle oft verschiedene Stellen gleichzeitig betreffen und deshalb schneller und effektiver bewältigt werden können, wenn alle betroffenen Stellen relevante Informationen austauschen. Für die Bewältigung von Cyber-Vorfällen haben viele Organisationen in der Schweiz spezialisierte Teams aufgebaut oder beauftragt. Der Bund betreibt zur Unterstützung der Betreiber kritischer Infrastrukturen die Melde- und Analysestelle Informationssicherung (MELANI) im Kompetenzzentrum Cyber-Sicherheit. Mit der Erweiterung der Zielgruppe der NCS muss auch die Unterstützung bei Vorfällen auf weitere Kreise ausgeweitet werden. Die heute schon enge Zusammenarbeit mit den relevanten Kompetenzzentren ist gezielt zu intensivieren, um die beschränkten spezialisierten Ressourcen in der Schweiz möglichst effektiv und effizient zu nutzen.

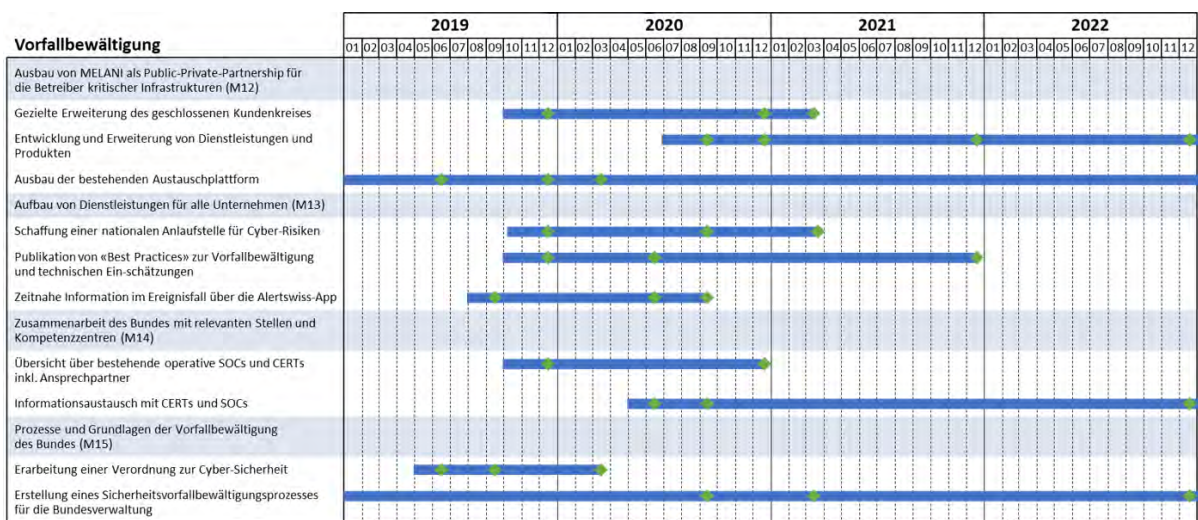


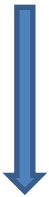
Abbildung 9 Roadmap Vorfallbewältigung

7.5.1 Ausbau von MELANI als Public-Private-Partnership für die Betreiber kritischer Infrastrukturen (M12)

Übersicht Massnahme	
Massnahmenziel	MELANI betreibt für Betreiber kritischer Infrastrukturen eine Plattform den Informationsaustausch. Diese Unterstützung in Form einer Public-Private Partnership für Cyber-Sicherheit wird weiter ausgebaut mit dem Ziel, alle Sektoren in den Informationsaustausch einzubinden und diesen auch sektorübergreifend zu pflegen. Gleichzeitig soll die bisherige Qualität sichergestellt und klar definiert werden, wer Zugang zu welchen Dienstleistungen und Informationen erhält.
Verantwortung für Massnahme	Kompetenzzentrum Cyber-Sicherheit unter Einbezug NDB
Beteiligung Dritter	Betreiber kritischer Infrastrukturen

Bestehende Gremien / Prozesse / Konzepte	Bestehender geschlossener Kundenkreis von MELANI
Rechtssetzungsbedarf	MELANI basiert auf den rechtlichen Grundlagen im Nachrichtendienstgesetz NDG (Art. 6) zur Frühwarnung von kritischen Infrastrukturen und in der Bundesinformatikverordnung (BinfV). Für den Ausbau von MELANI ist eine rechtliche Grundlage zu schaffen, welche über die Aufgabe der Frühwarnung hinausgeht.
Umsetzungsprojekte der Massnahme	1. Gezielte Erweiterung des geschlossenen Kundenkreises 2. Entwicklung und Erweiterung von Dienstleistungen und Produkten 3. Ausbau der bestehenden Austauschplattform

Umsetzungsprojekte

1. Gezielte Erweiterung des geschlossenen Kundenkreises	
Projektbeschreibung	Definition eines bedarfsgerechten Zugangs zu MELANI Produkten und Informationen für alle kritischen Sektoren und deren Fachämter
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit unter Einbezug NDB
Meilensteine	 Q4/2019 Situationsanalyse über Nutzung von MELANI durch die verschiedenen kritischen Sektoren ist erstellt Q4/2020 Konzept über die Gestaltung des Kundenkreises von MELANI ist erstellt Q1/2021 Kundenkreis ist gezielt ausgebaut
2. Entwicklung und Erweiterung von Dienstleistungen und Produkten	
Projektbeschreibung	Ausbau der Produkte sowie Dienstleistungen von MELANI zur Unterstützung der Mitglieder des geschlossenen Kundenkreises bei der Vorfallbewältigung, der Detektion, der Analyse und des Monitorings.
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit unter Einbezug NDB
Meilensteine	 Q3/2020 Analyse der bestehenden MELANI Produkte und Dienstleistung sowie des bestehenden Bedarfs Q4/2020 MELANI Produkte- und Dienstleistungs-Portfolio mit Roadmap erstellt Q4/2021 Erster Kurzbericht zum Ausbau des Portfolios gemäss Roadmap Q4/2022 Zweiter Kurzbericht zum Ausbau des Portfolios gemäss Roadmap

3. Ausbau der bestehenden Austauschplattform	
Projektbeschreibung	Bedarfsgerechter Ausbau der Kollaborationsplattform «MELANI-NET» als Informationsdrehscheibe für die Mitglieder des geschlossenen Kundenkreises von MELANI
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit unter Einbezug NDB
Meilensteine	 Q3/2018 Studie mit Variantenempfehlung zu MELANI-NET 2.0 erstellt Q2/2019 PoC (Proof of Concept) zur empfohlenen Variante durchgeführt Q4/2019 Konzept MELANI-NET 2.0 vorhanden Q1/2020 MELANI-NET 2.0 produktiv

7.5.2 Aufbau von Dienstleistungen für alle Unternehmen (M13)

Übersicht Massnahme	
Massnahmenziel	Die Schweizer Wirtschaft und insbesondere kleine und mittlere Unternehmen sollen durch MELANI unterstützt werden. MELANI erweitert deshalb die Zielgruppe und entwickelt für diese ein ergänzendes Dienstleistungsangebot im Bereich Prävention und Vorfallbewältigung. Die Unterstützung erfolgt subsidiär zu den Angeboten im Bereich Schutz und Vorfallbewältigung, welche auf dem Markt verfügbar sind
Verantwortung für Massnahme	Kompetenzzentrum Cyber-Sicherheit
Beteiligung Dritter	Wirtschaftsverbände (bspw. ICTSwitzerland)
Bestehende Gremien / Prozesse / Konzepte	Bestehende Dienstleistungen von MELANI für die Öffentlichkeit (Warnungen, Best Practices, Anleitungen)
Rechtsetzungsbedarf	Rechtliche Grundlagen für die beschriebenen Dienstleistungen sind noch zu erarbeiten.
Umsetzungsprojekte der Massnahme	1. Schaffung einer nationalen Anlaufstelle für Cyber-Risiken 2. Publikation von «Best Practices» zur Vorfallbewältigung und technischen Einschätzungen 3. Zeitnahe Information im Ereignisfall -> Alertswiss-App

Umsetzungsprojekte

1. Schaffung einer nationalen Anlaufstelle für Cyber-Risiken	
Projektbeschreibung	Schaffung einer nationalen Anlaufstelle (primär ein Online-Portal) für Cyber-Risiken. Dieses beinhaltet die Möglichkeit Cyber-Vorfälle zu melden, Instrumente für die Hilfe zur Selbsthilfe sowie weitere Informationen und Anleitungen.
Zuständigkeit und eingesetzte Ressourcen	Kompetenzzentrum Cyber-Sicherheit
Meilensteine	 Q4/2019 Grobkonzept für das Online-Portal für die Meldung von Cyber-Vorfällen erstellt Q3/2020 Online-Portal für die Meldungen von Cyber-Vorfällen steht der Öffentlichkeit zur Verfügung Q1/2021 Integration in die Informationsplattform zu Cyber-Risiken ist erfolgt (vgl. M29)
2. Publikation von «Best Practices» zur Vorfallbewältigung und technischen Einschätzungen	
Projektbeschreibung	Bereitstellung von Produkten bzw. «Best Practices» zur Cyber-Vorfallbewältigung und technischen Einschätzungen für die Schweizer Wirtschaft
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit
Meilensteine	 Q4/2019 Situations- und Bedarfsanalyse zu möglichen «Best Practices» (Arbeitsinstrumenten/Tools usw.) zur Cyber-Vorfallbewältigung sowie technische Analysen für die Öffentlichkeit erstellt Q2/2020 Konzept über «Best Practices» (Arbeitsinstrumenten/Tools usw.) zur Cyber-Vorfallbewältigung sowie technische Analysen, sowie deren Kommunikationsmitteln und -Kanälen verfasst Q4/2021 Bedürfnisgerechte Ent-/Weiterentwicklung von MELANI Informationen und Dienstleistungen zu «Best Practices» und deren Bereitstellung für die Schweizer Wirtschaft erfolgt
3. Zeitnahe Information im Ereignisfall über die Alertswiss-App	
Projektbeschreibung	Die App «Alertswiss» des BABS wird verwendet, um bei Vorfällen rasch eine ein grosses Publikum über akute Cyber-Bedrohungen zu informieren.
Zuständigkeit	BABS, Kompetenzzentrum Cyber-Sicherheit

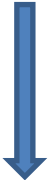
Meilensteine	 Q3/2019 Anforderungskklärung bezüglich Alarmierung, Warnung und Information der Öffentlichkeit im Cyber-Vorfall zwischen Kompetenzzentrum und BABS ist erfolgt Q1/2020 Konzept zur Integration der Cyber-Informationen im Alertswiss-App ist erstellt Q3/2020 Information der Öffentlichkeit im Cyber-Ereignis über Alertswiss-App ist möglich Q3/2020 (Medien-) Information über die Neuerung (Cyber-Ereignis) im Alertswiss-App publiziert
--------------	--

7.5.3 Zusammenarbeit des Bundes mit relevanten Stellen und Kompetenzzentren (M14)

Übersicht Massnahme	
Massnahmenziel	Die heute schon enge Zusammenarbeit und Abstimmung von MELANI mit weiteren relevanten Stellen in Bund und Kantonen wird gezielt weiter gestärkt und der Austausch zw. diesen Stellen gefördert.
Verantwortung für Massnahme	Kompetenzzentrum Cyber-Sicherheit
Beteiligung Bundesstellen	CSIRT BIT, milCERT
Beteiligung Dritter	Switch, kantonale SOC's
Bestehende Gremien / Prozesse / Konzepte	CH-CERT: Plattform für den Austausch zwischen den CERTs der Schweiz
Rechtsetzungsbedarf	Rechtliche Grundlagen für die Zusammenarbeit von MELANI mit weiteren Stellen sind zu erarbeiten.
Umsetzungsprojekte der Massnahme	1. Übersicht über bestehende operative SOC's inkl. Ansprechpartner 2. Informationsaustausch mit CERTs und SOC's

Umsetzungsprojekte

1. Übersicht über bestehende operative SOC's und CERTs inkl. Ansprechpartner	
Projektbeschreibung	Schaffung einer aktualisierten Übersicht über bestehende operative SOC's und CERTs, sowie den entsprechenden Ansprechpartnern.
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit
Meilensteine	 Q4/2019 Erhebung der bestehenden operativen SOC's und CERTs inklusive Ansprechpartner durchgeführt und dokumentiert Q4/2020 Prozess sowie Verantwortung zur laufenden Aktualisierung der Übersicht geklärt

2. Informationsaustausch mit CERTs und SOC's	
Projektbeschreibung	Es wird der Bedarf geklärt, welche Informationen zwischen den CERTs und SOC's ausgetauscht werden können und wie dieser Austausch organisiert werden kann.
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit
Meilensteine	 Q2/2020 Analyse zum Bedarf und den Möglichkeiten eines systematischen Informationsaustausches Q3/2020 Projekte für die Etablierung des Informationsaustausches sind definiert und zugewiesen Q4/2022 Die definierten Projekte sind umgesetzt

7.5.4 Prozesse und Grundlagen der Vorfallbewältigung des Bundes (M15)

Übersicht Massnahme	
Massnahmenziel	Um die Vorfallbewältigung innerhalb der Bundesverwaltung zu standardisieren, wird ein Prozess erarbeitet, welcher die Meldewege und Zuständigkeiten aufzeigt.
Verantwortung für Massnahme	Kompetenzzentrum Cyber-Sicherheit
Beteiligung	alle Eidg. Departemente
Bestehende Gremien / Prozesse / Konzepte	Ausschuss Informatiksicherheit des Bundes (A-IS)
Rechtsetzungsbedarf	Bestehende Grundlage ist die Bundesinformatikverordnung (BinfV). Eine Anpassung auf das Kompetenzzentrum ist nötig.
Umsetzungsprojekte der Massnahme	1. Erarbeitung einer Verordnung zur Cyber-Sicherheit 2. Erstellung eines Sicherheitsvorfallbewältigungsprozesses für die Bundesverwaltung

Umsetzungsprojekte

1. Erarbeitung einer Verordnung zur Cyber-Sicherheit	
Projektbeschreibung	Es wird eine Verordnung als rechtliche Grundlage für das Kompetenzzentrum «Cyber-Sicherheit» erarbeitet und darin festgehalten, dass das Kompetenzzentrum bei der Bewältigung von IKT-Sicherheitsvorfällen in der Bundesverwaltung die Federführung übernehmen kann.
Zuständigkeit	Generalsekretariat EFD
Meilensteine	 Q2/2019 Erarbeitung der Verordnung Q3/2019 Beschluss der Verordnung durch den Bundesrat Q1/2020 Inkrafttreten der Verordnung

2. Erstellung eines Sicherheitsvorfallbewältigungsprozesses für die Bundesverwaltung	
Projektbeschreibung	Zur Konkretisierung der in der Verordnung zur Cyber-Sicherheit festgelegten Zuständigkeits- und Kompetenzzuordnung wird ein Prozess für die Bewältigung von Sicherheitsvorfällen in der Bundesverwaltung definiert.
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit
Meilensteine	 Q3/2018 Erster Entwurf für einen Prozess, Diskussion mit Leistungserbringern und betroffenen Stellen Q3/2020 Prozess ist auf die Verordnung Cyber-Sicherheit angepasst Q1/2021 Prozess ist eingeführt Q4/2022 Überprüfung des Prozesses und Vorschläge für Anpassungen

7.6 Krisenmanagement

Cyber-Vorfälle können gravierende Konsequenzen haben und soweit eskalieren, dass ein Krisenmanagement auf nationaler Ebene nötig wird. Entscheidend für die Bewältigung von Krisen sind ein aktuelles, einheitliches und umfassendes Lagebild, die Definition von effizienten Prozessen zur Entscheidungsfindung und die Festlegung einer Kommunikationsstrategie. Das Krisenmanagement ist grundsätzlich szenariounabhängig. Das bedeutet, dass das allgemeine Krisenmanagement (Führungsabläufe und -prozesse) der Kantone und des Bundes auch für Krisen mit Cyber-Ausprägungen gültig bleibt. Wichtig bei solchen Krisen ist aber die Unterstützung der Stäbe durch fachspezifisches Wissen und eine intensive Zusammenarbeit aller kompetenten Stellen aus Bund, Kantonen und Wirtschaft. Weil bei der Bewältigung von Krisen keine Zeit verloren gehen darf, müssen die Prozesse im Vorhinein geübt und Konzepte zur Führung und Kommunikation ausgearbeitet werden.

Es braucht einen direkten Einbezug der zuständigen Fachstellen aus dem Bereich Cyber-Sicherheit in das Krisenmanagement auf Stufe Bund, welches durch die bestehenden oder ad-hoc eingesetzte Stäbe ausgeführt wird.

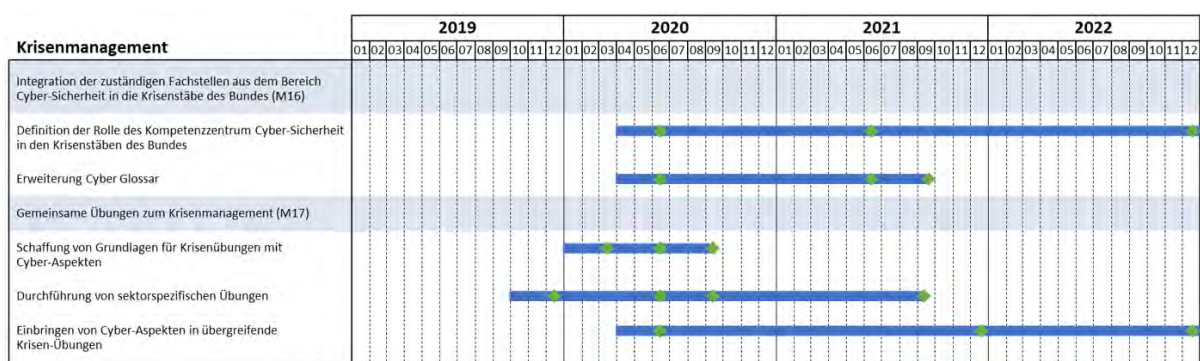


Abbildung 10 Roadmap Krisenmanagement

7.6.1 Integration der zuständigen Fachstellen aus dem Bereich Cyber-Sicherheit in die Krisenstäbe des Bundes (M16)

Übersicht Massnahme	
Massnahmenziel	Für die Bewältigung von Cyber-Krisen werden die bestehenden Krisenstäbe (insb. Bundesstab Bevölkerungsschutz und BWL-Krisenstab) genutzt oder ad-hoc Krisenstäbe gebildet. Für die Bewältigung von Krisen gemeinsam mit der Wirtschaft sind zudem branchenspezifische Krisenorganisationen aufzubauen und zu nutzen. Die zuständigen Fachstellen aus dem Bereich Cyber-Sicherheit sind mit den Stäben zu vernetzen und müssen über die Fähigkeiten verfügen, bei einer Krise mit Cyber-Aspekten die fachliche Koordination zu übernehmen.
Verantwortung für Massnahme	Kompetenzzentrum Cyber-Sicherheit
Beteiligung	BABS, BK, BWL, GS VBS, NDB
Bestehende Gremien / Prozesse / Konzepte	Konzept für Führungsabläufe und -prozesse bei Krisen mit Cyber-Ausprägung
Umsetzungsprojekte der Massnahme	1. Definition der Rolle des Kompetenzzentrum Cyber-Sicherheit in den Krisenstäben des Bundes 2. Erweiterung Cyber Glossar

Umsetzungsprojekte

1. Definition der Rolle des Kompetenzzentrum Cyber-Sicherheit in den Krisenstäben des Bundes	
Projektbeschreibung	Klärung der Vertretung, der Kommunikationskanäle sowie der Kompetenzen des Cyber-Kompetenzzentrums in den bestehenden Krisenstäben
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit
Meilensteine	 Q2/2020 Das Kompetenzzentrum hat seine Rolle in den Krisenstäben in Abstimmung mit den Stäben definiert Q2/2021 Prüfung allfälliger Anpassung der normativen Vorgaben der Stäbe Q4/2022 Beteiligung des Kompetenzzentrums in den Stäben ist etabliert

2. Erweiterung Cyber Glossar	
Projektbeschreibung	Klärung der wichtigsten Cyber-Begriffe für ein gemeinsames Verständnis
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit
Meilensteine	 Q2/2020 Bestandesaufnahme der vorhandenen Definitionen Q2/2021 Cyber-Glossar über-/erarbeitet Q3/2021 Information über Cyber-Glossar kommuniziert

7.6.2 Gemeinsame Übungen zum Krisenmanagement (M17)

Übersicht Massnahme	
Massnahmenziel	In gemeinsamen Übungen von Bund, Kantonen und Vertretern kritischer Infrastrukturen wird das Krisenmanagement in Bezug auf die Cyber-Aspekte getestet. Dabei sind sowohl Cyber-Aspekte in generelle Übungen einzubeziehen, als auch spezifische Übungen zur Bewältigung von Krisen mit Cyber-Ausprägungen durchzuführen. Die Übungen werden ausgewertet und fliessen in die Optimierung der Führungsabläufe und -prozesse ein.
Verantwortung für Massnahme	Kompetenzzentrum Cyber-Sicherheit, GS VBS
Beteiligung Bundesstellen	Fachämter (BAG, BAV, BAKOM, BFE, BAZL, fedpol), BWL, BABS, BSTB, GS-VBS, SVS

Beteiligung Dritter	Branchenverbände, Bankenvertreter (sektorspez. und übergreifenden Übungen), FINMA (sektorspez. Übungen) und Hochschulen
Bestehende Gremien / Prozesse / Konzepte	Strategische Führungsübung (SFU) Sicherheitsverbundübung (SVU) Strategische Gesamtübung Cyber-Pakt des VBS Beteiligung an internationalen Übungen
Umsetzungsprojekte der Massnahme	1. Schaffung von Grundlagen für Krisenübungen mit Cyber-Aspekten 2. Durchführung von sektorspezifischen Übungen 3. Einbringen von Cyber-Aspekten in übergreifende Krisen-Übungen

Umsetzungsprojekte

1. Schaffung von Grundlagen für Krisenübungen mit Cyber-Aspekten	
Projektbeschreibung	Es wird eine Übersicht über bestehende und geplanten nationalen sowie internationalen Krisenübungen mit Cyber-Aspekten in ausgewählten Teilsektoren erarbeitet und analysiert, welche zusätzlichen Übungen nötig sind. Zudem wird systematische Expertise zu Szenarien für Übungen mit Cyber-Aspekten erarbeitet.
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit, GS VBS; mit Einbezug der Hochschulen
Meilensteine	 Q1/2020 Bestandesaufnahme der bestehenden und geplanten nationalen und internationalen Krisenübungen mit Cyber-Aspekten Q2/2020 Expertise zu Szenarien und Übungen mit Cyber-Aspekten ist aufgebaut Q3/2020 Analyse über Priorisierung und Bedarf an weiteren Übungen

2. Durchführung von sektorspezifischen Übungen	
Projektbeschreibung	Durchführung von spezifischen Krisenübungen mit Cyber-Aspekten in risikoreichen Teilsektoren
Zuständigkeit	Fachämter der Sektoren und FINMA für Finanzsektor mit fachlicher Unterstützung durch GS VBS und unter Koordination des Kompetenzzentrums Cyber-Sicherheit in Zusammenarbeit BABS/BWL

Meilensteine	 Q4/2019 Bedarfsanalyse zu sektorspezifischen Krisenübungen ist erfolgt Q2/2020 Roadmap sowie Verantwortlichkeiten mit den involvierten Partnern ist geklärt Q3/2020 Krisenübungs-Konzept/e (Art, Ziele, Teilnehmende, Infrastruktur, Steuerung, Drehbuch usw.) mit den identifizierten Sektoren bzw. deren Vertretern erarbeitet Q3/2021 Sektorspezifische Übungen durchgeführt und dokumentiert
--------------	--

3. Einbringen von Cyber-Aspekten in übergreifende Krisen-Übungen	
Projektbeschreibung	Einbringung von Cyber-Aspekten in grossangelegten übergreifenden Krisen- / Sicherheitsübungen
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit, GS VBS, BSTB
Meilensteine	 Q2/2020 Abstimmung mit den verantwortlichen Übungspartnern zum Einbezug der relevanten Cyber-Kriterien in der Übung durchgeführt Q4/2021 Cyber-Aspekte sind in SFU/SVU/GNU und weitere Übungen berücksichtigt worden Q4/2022 Cyber-spezifische Erkenntnisse reflektiert und mit Vertretern der bestehenden Krisenstäbe diskutiert

7.7 Strafverfolgung

Die über das Internet verfügbare digitale Infrastruktur eröffnet potenziellen Straftätern neuartige Möglichkeiten mit enormem Schadenspotenzial für Gesellschaft und Wirtschaft. Zeitliche und räumliche Einschränkungen für Taten gibt es kaum mehr. Vor diesem Hintergrund gilt es, gesamtschweizerisch und in Zusammenarbeit mit internationalen Partnern die Interoperabilität und Reaktionsfähigkeit zu verbessern sowie die fachlichen, technischen und personellen Kompetenzen wirksam aufeinander abzustimmen, ohne dabei die Befugnisse zwischen den verschiedenen Behörden und Staatsebenen zu verschieben.

Für die dazu notwendige Koordination ist 2018 das Cyberboard geschaffen worden, in welchem die zuständigen Stellen sich gegenseitig austauschen, Strategien entwickeln und sich operativ aufeinander abstimmen.

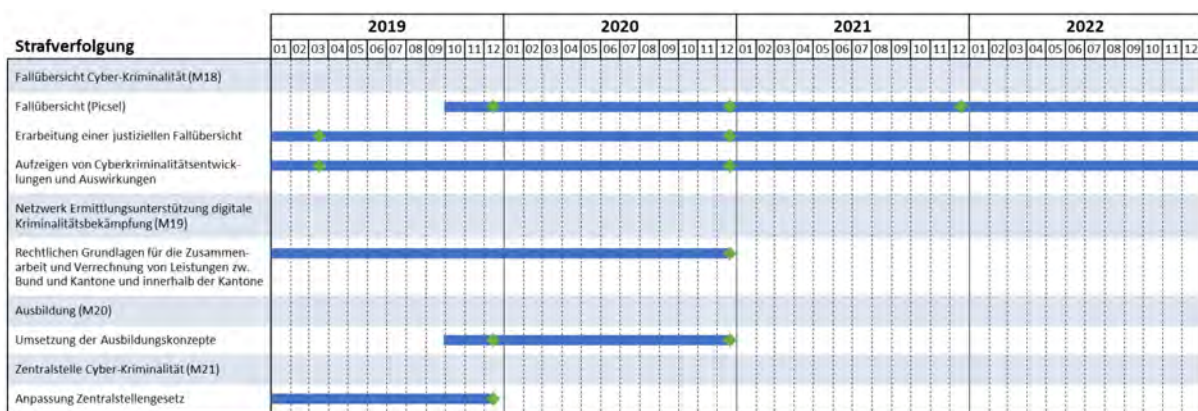


Abbildung 11 Roadmap Strafverfolgung

7.7.1 Fallübersicht Cyber-Kriminalität (M18)

Übersicht Massnahme	
Massnahmenziel	Bund (fedpol) und Kantone (KKPKS) prüfen und konzipieren die technischen Rahmenbedingungen für die Erarbeitung einer nationalen Fallübersicht Cyber-Kriminalität (polizeiliche Daten).
Verantwortung für Massnahme	fedpol in Rahmen der Tätigkeiten des Cyberboards
Beteiligung	Cyberboard, Obergericht / Militärjustiz / Militärpolizei
Bestehende Gremien / Prozesse / Konzepte	HPI, (Picar-Picse), NEDIK, Cyber-CASE
Umsetzungsprojekte der Massnahme	1. Fallübersicht (Picse) 2. Erarbeitung einer justiziellen Fallübersicht 3. Aufzeigen von Cyberkriminalitätsentwicklungen und Auswirkungen

Umsetzungsprojekte

1. Fallübersicht (PicSel)	
Projektbeschreibung	Kantonale polizeiliche Daten werden durch PicSel national zusammengefasst. Vorgehen in drei Phasen: • Schaffen der techn. Rahmenbedingungen • Rechtliche Rahmenbedingungen • Betrieb der Fallübersicht
Zuständigkeit	fedpol, HPI
Meilensteine	 Q4/2019 Testphase PicSel gestartet Q4/2020 Nationale Verbreitung über die Kantone erfolgt; mind. 3 Konkordate nehmen Teil Q4/2021 Techn. Rahmenbedingungen geklärt Q4/2023 ZentrG (rechtlich) in Kraft Q4/2023 PicSel im Betrieb (Daten ü. Kantone vorhanden)
2. Erarbeitung einer justiziellen Fallübersicht	
Projektbeschreibung	Erarbeitung eines Instrumentes zur nationalen Erfassung sämtlicher in den Kantonen hängigen Untersuchungskomplexe im Bereich Cybercrime (interkantonale Fallübersicht)
Zuständigkeit und eingesetzte Ressourcen	Cyberboard (Cyber-CASE, Kantone, BA & fedpol)
Meilensteine	 Q1/2019 Tool Cyber-CASE; Fallkomplex-Liste sämtlicher Cyber-SPOC-STA (bereits operativ) Q4/2020 Online Tool für die Verfahrensübersicht der laufenden Verfahren Q1/2021 <i>Kombination des polizeilichen Lagebildes (PicSel) mit der justiziellen Fallübersicht</i>
3. Aufzeigen von Entwicklungen, Szenarien und Auswirkungen	
Projektbeschreibung	Kontinuierlicher Aufbau von polizeilichen und justiziellen Produkten (Trends, Best Practices, Analysebericht usw.)
Zuständigkeit	Cyberboard (NEDIK, Kantone (Kantonspolizeien, Kantonale Staatsanwaltschaften), BA & fedpol) sowie Obergericht / Militärjustiz / Militärpolizei
Meilensteine	 Q1/2019 Monatliches Bulltin (polizeilich) Q4/2020 Verfahrensübersicht der laufenden Verfahren (polizeilich & justiziell)

7.7.2 Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung (M19)

Übersicht Massnahme	
Massnahmenziel	Bund (fedpol) und Kantone (KKPKS) erarbeiten die Rahmenbedingungen für die polizeiliche Zusammenarbeit und Koordination zwischen den kantonalen und nationalen Cyber-Kompetenzzentren im NEDIK.
Verantwortung für Massnahme	KKPKS
Beteiligung Bundesstellen	fedpol mit Cyberboard
Beteiligung Dritter	kantonale Polizei, KKPKS
Bestehende Gremien / Prozesse / Konzepte	Arbeitsgruppe NEDIK
Umsetzungsprojekte der Massnahme	1. Rechtlichen Grundlagen für die Zusammenarbeit und Verrechnung von Leistungen zw. Bund und Kantone und innerhalb der Kantone

Umsetzungsprojekte

1. Rechtlichen Grundlagen für die Zusammenarbeit und Verrechnung von Leistungen zw. Bund und Kantone und innerhalb der Kantone	
Projektbeschreibung	Erarbeiten der rechtlichen Grundlagen für die Zusammenarbeit und Verrechnung von Leistungen zw. Bund und Kantone und innerhalb der Kantone
Zuständigkeit	KKPKS und fedpol
Meilensteine	 Q4/2020 Vereinbarung(en) unterzeichnet und verabschiedet

7.7.3 Ausbildung (M20)

Übersicht Gesamtmassnahme	
Massnahmenziel	In Zusammenarbeit zwischen der Konferenz der kantonalen Polizeikommandanten (KKPKS) und der Schweizerischen Staatsanwälte-Konferenz (SSK) werden spezifisch Ausbildungskonzepte für einen nachhaltigen Aufbau der erforderlichen Kompetenzen in der Strafverfolgung geschaffen.
Verantwortung für Massnahme	KKPKS (inkl. fedpol), SSK (inkl. BA)
Beteiligung	Cyberboard
Bestehende Gremien / Prozesse / Konzepte	- Arbeitsgruppe Cybercrime Ausbildungen - Bestehende Ausbildungen (HEG-ARC ERMP) - Staatsanwälte-Akademie (HSLU) - Cyber-CASE

Umsetzungsprojekte der Massnahme	1. Umsetzung der Ausbildungskonzepte
----------------------------------	--------------------------------------

Umsetzungsprojekte

1. Ausbildungen	
Projektbeschreibung	Umsetzung des 5-Stufenmodells -> Ausbildungen
Zuständigkeit	SPI (Schweiz. Polizei-Institut), AG Cybercrime Ausbildungen
Meilensteine	 Q4/2019 Übersicht der Akad. Ausbildungsmöglichkeiten (polizeilich) Q4/2020 Ausbildungsangebote bei den Hochschulen können durch Polizei genutzt werden

7.7.4 Zentralstelle Cyber-Kriminalität (M21)

Übersicht Massnahme	
Massnahmenziel	fedpol veranlasst die Anpassung des Zentralstellengesetzes (ZentG) zwecks Schaffung einer Zentralstelle Cyber-Kriminalität und der notwendigen Grundlagen für die Zusammenarbeit mit den Kantonen bei der Bekämpfung der Cyber-Kriminalität.
Verantwortung für Massnahme	fedpol
Beteiligung	Cyberboard, Bundesamt für Justiz
Bestehende Gremien / Prozesse / Konzepte	Bundesgesetz über kriminalpolizeiliche Zentralstellen des Bundes (ZentG)
Umsetzungsprojekte der Massnahme	1. Anpassung Zentralstellengesetz (ZentG)

Umsetzungsprojekte

1. Anpassung Zentralstellengesetz	
Projektbeschreibung	Schaffung einer gesetzlichen Grundlage für eine Zentralstelle für Cyberkriminalität U.a. Regelung des polizeilichen Datenaustausches
Zuständigkeit und eingesetzte Ressourcen	fedpol und Bundesamt für Justiz (BJ)
Meilensteine	 Q4/2022 ZentG aktualisiert und verabschiedet

7.8 Cyber-Defence

Grossangelegte oder sehr gezielte Cyber-Angriffe auf kritische Infrastrukturen der Schweiz können die Sicherheit der Bevölkerung und der Wirtschaft gefährden. Die Schweiz braucht daher über alle Lagen Fähigkeiten und Ressourcen, um laufende Angriffe zu unterbinden und die dafür verantwortlichen Akteure zu identifizieren. Bei Angriffen, welche das Funktionieren kritischer Infrastrukturen gefährdet, müssen in Abstimmung mit den relevanten Fachbehörden nötigenfalls aktive Gegenmassnahmen ergriffen werden können, um deren Betrieb sicherzustellen. Die rechtlichen Grundlagen dafür wurden mit dem Nachrichtendienstgesetz und dem revidierten Militärgesetz geschaffen.

Die Cyber-Defence umfasst jene Massnahmen, die generell der Verteidigung kritischer Systeme und der Abwehr von Angriffen im Cyber-Raum über alle Lagen, also bis zu Konflikt- und Kriegszeiten dienen. In seinem «Aktionsplan für Cyber-Defence» (APCD) hat das VBS den Handlungs- und Ressourcenbedarf für diesen Bereich festgestellt, die Aufträge der verschiedenen Stellen (insbesondere auch der Armee) definiert und beschrieben welche Massnahmen zur Bewältigung der Aufgaben getroffen werden.

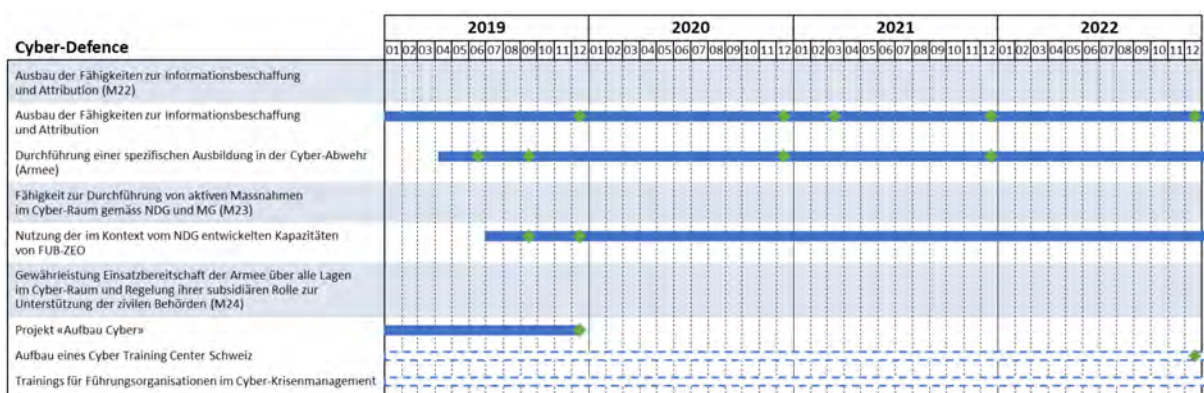


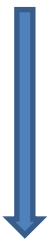
Abbildung 12 Roadmap Cyber-Defence

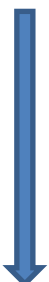
7.8.1 Ausbau der Fähigkeiten zur Informationsbeschaffung und Attribution (M22)

Übersicht Massnahme	
Massnahmenziel	Der NDB ist mittels einer systematischen Informationsbeschaffung und -auswertung in der Lage, neue Angriffsmuster möglichst frühzeitig zu entdecken. Er kann eine möglichst genaue Feststellung der Urheber-schaft von erfolgten Angriffen (Attribution) vornehmen, damit die Handlungsfreiheit der politischen Behörden und der Strafverfolgungsbehörden gewahrt wird. Bei Angriffen auf kritische Infrastrukturbetreiber ist der NDB unter Einbezug unterstützender Einheiten sowie Fachbehörden in der Lage, seinen Auftrag im Rahmen des NDG zu erfüllen. • Das vorhandene Spezialwissen und die Fähigkeiten des NDB zur Informationsbeschaffung zwecks Früherkennung von Cyber-Angriffen und zur Identifikation der Urheberschaft werden weiterentwickelt. • Der DB führt vertiefte Akteurs- und Umfeldanalysen durch • Der NDB nutzt und entwickelt technische Hilfsmittel, die Fernmeldeüberwachung und Methoden der Human Intelligence. • Erkannte Cyber-Angriffe werden systematisch aufgearbeitet und verfolgt.

Verantwortung für Massnahme	NDB
Beteiligung	FUB (CNO) und MND
Bestehende Gremien / Prozesse / Konzepte	• Cyber NDB für die Bearbeitung von nachrichtendienstlich relevanten Informationen im Zuständigkeitsbereich des NDB • SLA mit der FUB -> Anbindung der technischen Fähigkeiten der FUB zur Unterstützung des NDB
Umsetzungsprojekte der Massnahme	1. Ausbau der Fähigkeiten zur Informationsbeschaffung und Attribution 2. Durchführung einer spezifischen Ausbildung in der Cyberabwehr (Armee)

Umsetzungsprojekte

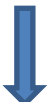
1. Ausbau der Fähigkeiten zur Informationsbeschaffung und Attribution	
Projektbeschreibung	Steigerung der allgemeinen (sprachlichen und geopolitischen) und technischen Analysekapazitäten sowie der Kapazitäten für die Informationsbeschaffung, mit passenden Fähigkeiten/Ressourcen
Zuständigkeit	NDB
Meilensteine	 Q4/2019 Ausbau erste Etappe ist erfolgt Q4/2020 Ausbau zweite Etappe ist erfolgt Q1/2021 Zwischenbericht zum Ausbau der Fähigkeiten liegt vor Q4/2021 Ausbau dritte Etappe ist erfolgt Q4/2022 Schlussbericht zum Ausbau der Fähigkeiten

2. Durchführung einer spezifischen Ausbildung in der Cyberabwehr (Armee)	
Projektbeschreibung	Der Ausbildungsbedarf der Armee wird ermittelt und eine spezifische Ausbildung mit Hilfe von EPFL/ETHZ-Expertise (technisches Fachwissen, aber auch pädagogisches Fachwissen) durchgeführt. Die bilateralen EPFL-VBS-Aktionen werden durch gemeinsame EPFL-ETHZ-VBS-Aktionen (Joint Master in Cybersecurity - Defence part) ergänzt.
Zuständigkeit	Bilaterale Komponente: EPFL + VBS Dreieckige Komponente: EPFL + ETHZ + VBS
Meilensteine	 Q2/2019 Erstes Training mit der Führungsunterstützungsbasis des Heeres Q3/2019 Start des gemeinsamen Masterstudiengangs EPFL ETHZ VBS Q3/2019 Erste EPFL-VBS-Schulungen Q4/2020 "Cyber Defense Curriculum" eingeführt Q4/2021 Durchführung von anderen Sensibilisierungsmaßnahmen, Ausbau erste Etappe ist erfolgt

7.8.2 Fähigkeit zur Durchführung von aktiven Massnahmen im Cyber-Raum gemäss NDG und MG (M23)

Übersicht Massnahme	
Massnahmenziel	Das VBS (NDB und Armee) verfügen über genügend qualitatives und quantitatives Kompetenzen und Kapazitäten um gegebenenfalls Angriffe auf kritische Infrastrukturen zu stören, zu verhindern oder zu verlangsamen. Der Einsatz solcher Massnahmen erfolgt abgestimmt mit den relevanten Fachämtern gemässe den gesetzlichen Vorgaben von NDG und MG.
Verantwortung für Massnahme	NDB, FUB-ZEO
Beteiligung	-
Bestehende Gremien / Prozesse / Konzepte	Die SLA (Service Level Agreement) mit FUB-ZEO wurde angepasst. Aufbau von Spezialwissen seitens FUB-ZEO ist erledigt.
Umsetzungsprojekte der Massnahme	1. Nutzung der im Kontext vom NDG entwickelten Kapazitäten von FUB-ZEO

Umsetzungsprojekte

1. Nutzung der im Kontext vom NDG entwickelten Kapazitäten von FUB-ZEO	
Projektbeschreibung	Angriffe gegen kritische Infrastrukturen stören, verhindern oder verlangsamen
Zuständigkeit	NDB, FUB-ZEO
Meilensteine	 Q3/2019 die geplanten Aktivitäten sind mit Fachämtern auf unerwünschte Kollateraleffekte abgesprochen Q4/2019 die Kapazitäten sind vorhanden

7.8.3 Gewährleistung Einsatzbereitschaft der Armee über alle Lagen im Cyber-Raum und Regelung ihrer subsidiären Rolle zur Unterstützung der zivilen Behörden (M24)

Übersicht Massnahme	
Massnahmenziel	Das VBS und insb. die Armee müssen in der Lage sein, in enger Zusammenarbeit mit ihren Partnern, der Wirtschaft und den Hochschulen, die folgenden Ziele zu erreichen: 1) Die in Anzahl, Intensität und Komplexität zunehmenden Formen der Cyber-Bedrohung zu bewältigen, sowohl im Alltag als auch im Falle einer Krise oder eines Konflikts; 2) Die Cyber-Aspekte des Nachrichtendienstgesetzes und des Militärgesetzes konkret umsetzen; 3) In der Lage sein, die Betreiber kritischer Infrastrukturen, die Opfer von Cyber-Angriffen wurden, bei Bedarf wirksam und nachhaltig (subsidiär) zu unterstützen.

Gesamtverantwortung für Massnahme	GS VBS und FUB in enger Zusammenarbeit
Beteiligung	Kdo Operationen, Kdo Ausbildung, LBA, NDB, armasuisse W+T, BABS
Bestehende Gremien / Prozesse / Konzepte	Der Aktionsplan Cyberdefence des VBS enthält / beschreibt insb. • die Prozesse (Einsatz z.G. des Militärs und Unterstützung der kritischen Infrastrukturen), • die Regeln der Subsidiarität, • die Koordinationsinstrumente.
Umsetzungsprojekte der Massnahme	1. Projekt "Aufbau Cyber" 2. Aufbau eines Cyber Training Center Schweiz 3. Trainings für Führungsorganisationen im Cyber-Krisenmanagement

Umsetzungsprojekte

1. Aufbau Cyber	
Projektbeschreibung	Mit diesem Vorhaben (seit 2015 in Entwicklung) wird die Armee schrittweis befähigt, ihre Leistungen im Cyberraum zu erbringen. Diese Leistungen decken die Bereiche Führung, Antizipation, Prävention, Schutz, Aktion, Reaktion und Unterstützung.
Zuständigkeit	FUB mit Unterstützung von Ressourcen der Armee, von armasuisse und des GS-VBS
Meilensteine	Gemäss Projektplan -> Projektabschluss: Q4/2019

2. Aufbau eines Cyber Training Center Schweiz	
Projektbeschreibung	Die Schweizer Armee baut ein Cyber Training Center (CTC) für die Schulung von Spezialisten und Führungspersonen zur Bewältigung von Cyber-Angriffen. Das CTC bildet Personal von Armee und Verwaltung aus. Es kooperiert eng mit Behörden, Betreiber kritischer Infrastrukturen und Hochschulen. Hauptziel damit ist es, die Anzahl des operationellen Personals rasch zu steigern.
Zuständigkeit	FUB (mit Ausbildungskommando der Armee)
Meilensteine	Zeitplan in Erarbeitung. Wir später präzisiert. Angestrebte Betriebsaufnahmen bis Ende 2022 vorgesehen.

3. Trainings für Führungsorganisationen im Cyber-Krisenmanagement	
Projektbeschreibung	Die Schweizer Armee bietet interessierten Dritten (Behörden, Krisenführungsorgane von Gemeinden bzw. Kantonen, Betreiber kritischer Infrastrukturen) die Möglichkeit, das Krisenmanagement bei einem Cyber-Vorfall (logisch im Rahmen des Sicherheitsverbundes) zu trainieren. Hauptziel damit ist es, die Interoperabilität des Sicherheitsverbundes.
Zuständigkeit und eingesetzte Ressourcen	FUB (mit Ausbildungskommando der Armee)
Meilensteine	Zeitplan in Erarbeitung. Wir später präzisiert. Angestrebte Betriebsaufnahmen bis Ende 2022 vorgesehen.

7.9 Aktive Positionierung der Schweiz in der internationalen Cyber-Sicherheitspolitik

Die Wahrung der aussen- und sicherheitspolitischen Interessen der Schweiz muss auch im Cyber-Raum sichergestellt werden. Die Schweiz engagiert sich daher sowohl auf diplomatischer als auch auf technisch-operativer Ebene für die Stärkung der internationalen Kooperation zur Minimierung von Cyber-Risiken. Sie setzt sich für die Anerkennung, Einhaltung und Durchsetzung des Völkerrechts im Bereich Cyber-Sicherheit ein, engagiert sich aktiv für die zwischenstaatliche Vertrauensbildung und unterstützt und entwickelt den Aufbau von Kapazitäten in Drittstaaten. Bei allen Aktivitäten gilt ein Augenmerk auch der Förderung der Schweiz und des internationalen Genfs als Plattform für Diskussionen zur Cyber-Aussensicherheitspolitik.

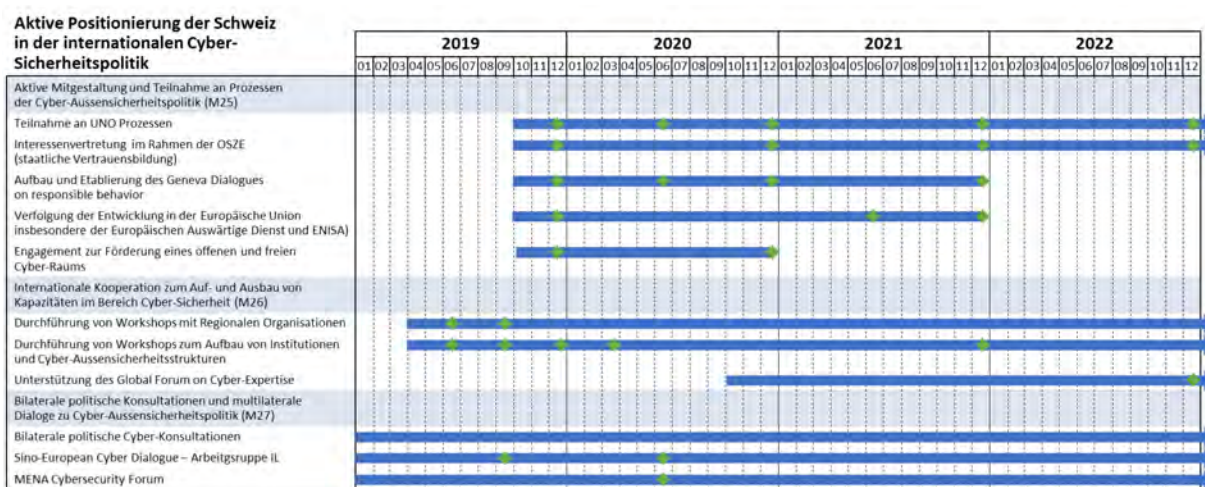


Abbildung 13 Roadmap Aktive Positionierung der Schweiz in der int. Cyber-Sicherheitspolitik

7.9.1 Aktive Mitgestaltung und Teilnahme an Prozessen der Cyber-Aussensicherheitspolitik (M25)

Übersicht Massnahme	
Massnahmenziel	Die Schweiz trägt zur Weiterentwicklung und Umsetzung von staatlichen und nichtstaatlichen Verhaltensnormen im Cyber-Raum bei. Sie setzt sich für die Anerkennung des Völkerrechts und den Schutz der Menschenrechte im Cyber-Raum ein und trägt zur Klärung von spezifischen Fragen zu dessen Anwendung bei. Sie engagiert sich bei der Schaffung von staatlichem Vertrauen im Cyber-Raum und baut dabei auf die bestehenden Massnahmen regionaler Organisationen, namentlich der OSZE auf. Die Schweiz setzt sich für die Durchsetzung der Exportkontrollregime mit Blick auf Überwachungstechnologien aktiv ein.
Verantwortung für Massnahme	EDA, Büro Sondergesandter für Cyber-Aussen- und Sicherheitspolitik, SECO
Beteiligung	EDA: DV, AIO, AMS; VBS: GS-VBS (Bereich SIPOL)
Bestehende Gremien / Prozesse / Konzepte	UNO, OSZE, EU, NATO, Rüstungskontrollregime, London Prozess

Umsetzungsprojekte der Massnahme	1. Teilnahme an UNO-Prozessen 2. Interessenvertretung im Rahmen der OSZE (staatliche Vertrauensbildung) 3. Etablierung des Geneva Dialogues on responsible behavior 4. Verfolgung der Entwicklungen in der Europäischen Union (insbesondere der Europäische Auswärtige Dienst und ENISA) 5. Engagement zur Förderung eines offenen und freien Cyber-Raums
----------------------------------	---

Umsetzungsprojekte

1. Teilnahme an UNO Prozessen	
Projektbeschreibung	Die Schweiz engagiert sich im Rahmen der UNO für die internationale Cybersicherheit. Sie tut dies u.a. im Rahmen der UN Governmental Group of Experts on Cyber Security (UN GGE) und in der Open Ended Working Group (OEWG). Beide Prozesse wurden durch die UN Generalversammlung einberufen. Die UN GGE erarbeitet Empfehlungen zu den Themen staatliche Verhaltensnormen, Vertrauensbildung, Kapazitätsaufbau und Anwendung des Völkerrechts. Zwei der insgesamt vier Debatten finden in Genf statt. Die OEWG hat zum Ziel, eine Reihe von insgesamt 13 Verhaltensregeln weiterzuentwickeln, diese, wo nötig, anzupassen und zu verändern. Sie sieht auch den Einbezug von nichtstaatlichen Akteuren vor.
Zuständigkeit	EDA, Büro Sondergesandter für Cyber-Aussen- und Sicherheitspolitik Für die Umsetzung der völkerrechtlichen Massnahmen: Direktion für Völkerrecht (DV)
Meilensteine	 Q4/2019-2022: Jährliche Berichterstattung Q4/ 2021: Weiterentwicklung der Empfehlungen im UN GGE-Bericht entlang der Schweizer Interessen Q2/2020: Mitgestaltung des Schlussdokuments der OEWG entlang der Schweizer Interessen

2. Interessenvertretung im Rahmen der OSZE (staatliche Vertrauensbildung)	
Projektbeschreibung	Die Schweiz setzt sich für die Entwicklungen und Umsetzung von vertrauensbildenden Massnahmen im Cyber-Bereich ein. Zu diesem Zweck unterstützt sie den OSZE-Prozess. Die OSZE hat 2013 und 2016 einen Katalog von vertrauensbildenden Massnahmen im Bereich Cyber-Sicherheit verabschiedet. Es handelt sich weltweit um die erste Vereinbarung dieser Art. Die Vereinbarung umfasst 16 Massnahmen mit dem Ziel, Risiken der neuen Informations- und Kommunikationstechnologien zu reduzieren, und Transparenz unter den OSZE-Mitgliedern zu verbessern.
Zuständigkeit	EDA, Büro Sondergesandter für Cyber-Aussen- und Sicherheitspolitik

Meilensteine	 Q4/2019-2022: Teilnahme an Verhandlungen und aktive Mitgestaltung des Prozesses. Q4/2019-2022: Jährliche Berichterstattung Q4/ 2021: Unterstützung von interregionalen Austausch
--------------	--

3. Aufbau und Etablierung des Geneva Dialogues on responsible behavior

Projektbeschreibung	Die Geneva Dialogue on Responsible Behavior ist eine Multistakeholder-Plattform, die Diskussionen zu den Rollen und Verantwortlichkeiten aller Akteure bei der Nutzung des Cyber-Raums anstösst, fasilitiert und als Konsultationsplattform für multilaterale Normierungsprozesse/Debatten dient. Der Geneva Dialogue umfasst einen Expertenprozess zur Klärung, wie völkerrechtliche Grundprinzipien im Cyberraum Anwendung finden. Die Schweiz stärkt dadurch ihre Rolle als Verfechterin des Völkerrechts und der Sicherheit im Cyberraum.
Zuständigkeit	EDA, Büro Sondergesandter für Cyber-Aussen- und Sicherheitspolitik Für die völkerrechtlichen Aspekte: DV Unterstützende Stelle: DV, MiGe, AIO
Meilensteine	 Q4/2019: Konzept für die Etablierung des Genfer Dialogs als Multistakeholder-Plattform im Bereich Cyber-Aussen- und Sicherheitspolitik für internationale Prozesse Q4/2019: 2-3 Dialogrunden des Expertenprozesses zur Anwendung des Völkerrechts auf den Cyber-Raum haben stattgefunden Q4/2021: Genfer Dialog ist als Multistakeholder-Plattform etabliert Q2/2020: Erkenntnisse aus dem Expertenprozess werden in UNGGE und OEWG eingespeist Q4/2020: Schweizer Interessen im Bereich der Anwendung des Völkerrechts auf den Cyberraum sind in den Schlussberichten der UNGGE und der OEWG reflektiert

4. Verfolgung der Entwicklungen in der Europäischen Union (insbesondere der Europäische Auswärtige Dienst und ENISA)

Projektbeschreibung	Die Europäische Union hat zahlreiche Massnahmen ergriffen, um der wachsenden Bedrohung durch Cyber-Angriffe zu begegnen. Die Schweiz als Nicht-Mitgliedstaat der EU ist in diese Arbeiten nicht einbezogen, wohl aber direkt/indirekt von den Massnahmen betroffen. Es ist daher wichtig, dass die ergriffenen und geplanten Massnahmen der EU analysiert und ihre Auswirkungen auf die Schweiz geprüft werden.
Zuständigkeit	Co-Zuständigkeit: Kompetenzzentrum Cyber-Sicherheit und EDA (Büro Sondergesandter für Cyber-Aussen- und Sicherheitspolitik), Unterstützende Stelle: DV, DEA

Meilensteine	 Q4/2019 Auslegeordnung der wichtigsten Akteure, Prozesse und Massnahmen der EU ist erstellt und es ist identifiziert welche Stellen der Schweiz sich in welchem Prozess engagieren Q2/2021 Mögliche Auswirkungen der verschiedenen EU-Massnahmen auf die Schweiz sind analysiert Q4/2021 Prozesse und Zuständigkeiten für Beobachtung der EU-Prozesse und allfällige Beteiligungen sind festgelegt
--------------	--

5. Engagement zur Förderung eines offenen und freien Cyber-Raums

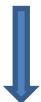
Projektbeschreibung	Die Schweiz setzt sich international für einen offenen, freien und sicheren Cyber-Raum ein. Dies umfasst neben der Gewährleistung der Sicherheit im Cyber-Raum auch den Schutz universeller Menschenrechte, wie der Schutz der Privatsphäre oder die Meinungsfreiheit im Internet. Die Schweiz vertritt hierbei den Grundsatz, dass die Menschenrechte online genau so gelten wie offline. Es gibt mehrere internationale Organisationen und Prozesse mit entsprechender Relevanz. Hier gilt es, die schweizerischen Interessen gezielt einzubringen. Voraussetzung hierfür ist es, eine Auslegeordnung zu machen der relevanten Prozesse und Organisationen.
Zuständigkeit	EDA, Büro Sondergesandter für Cyber-Aussen- und Sicherheitspolitik, AMS und DV
Meilensteine	Q4/2019 Auslegeordnung der relevanten internationalen Menschenrechtsprozesse und Foren Q4/2020 Beurteilung zur Schweizer Teilnahme an ausgewählten Prozessen und Foren

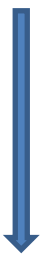
7.9.2 Internationale Kooperation zum Auf- und Ausbau von Kapazitäten im Bereich Cyber-Sicherheit (M26)

Übersicht Massnahme	
Massnahmenziel	Die Schweiz sucht gezielt den Austausch mit internationalen staatlichen und nichtstaatlichen Stellen zum Auf- und Ausbau von nationalen Fähigkeiten im Bereich Cyber-Risiken. Gleichzeitig trägt auch die Schweiz aktiv zum Auf- und Ausbau von Cyber-Fähigkeiten in Drittstaaten bei und hilft so mit, die globale Cyber-Sicherheit zu verbessern.
Verantwortung für Massnahme	EDA/ASP, Büro des Sondergesandten für Cyber-Aussen- und Sicherheitspolitik
Beteiligung	AIO, AMS, DV
Bestehende Gremien / Prozesse / Konzepte	CCDCoE, Global Forum on Cyber Expertise, G20 und Financial Stability Board (FSB) in der internationalen Finanzpolitik

Umsetzungsprojekte der Massnahme	1. Durchführung von Workshops mit regionalen Organisationen 2. Durchführung von Workshops zum Aufbau von Institutionen und Cyber-Aussensicherheitsstrukturen 3. Unterstützung des Global Forum on Cyber-Expertise
----------------------------------	---

Umsetzungsprojekte

1. Durchführung von Workshops mit Regionalen Organisationen	
Projektbeschreibung	Die Schweiz unterstützt die Mitglieder von regionalen Organisationen (z.B. Afrikanische Union) beim Aufbau von cyber-bezogenen Kapazitäten. Dazu organisiert sie eine Reihe von Workshops in Genf sowie in ausgewählten Weltregionen (z.B. Afrika, Addis Abeba).
Zuständigkeit	EDA, Büro Sondergesandter für Cyber- Aussen- und Sicherheitspolitik, AIO, DV
Meilensteine	 Q2/2019 Konzepterstellung und Planung der Veranstaltung Q3/2019 Erste Workshop Durchführung in Genf

2. Durchführung von Workshops zum Aufbau von Institutionen und Cyber-Aussensicherheitsstrukturen	
Projektbeschreibung	Die Schweiz unterstützt andere Staaten beim Auf- und Ausbau von Cyber-Aussensicherheitsstrukturen durch Expertise und Plattformen für den Erfahrungsaustausch. Sie führt Workshops und Seminare durch, um Wissen und Expertise rund um die internationalen Prozesse und Instrumente zu erhöhen und bietet hierzu in Zusammenarbeit mit den Hochschulen internationale Trainingsplattformen sowie Übungen an.
Zuständigkeit	EDA, Büro Sondergesandter für Cyber- Aussen- und Sicherheitspolitik, AIO, DV; in Zusammenarbeit mit der EPFL & ETHZ (zur akademischen Unterstützung wie Expertise, Ressourcen, Talentakquise usw.)
Meilensteine	 Q2/2019 Bedarfsanalyse und Unterstützungsmöglichkeiten Q3/2019 Training und Szenario-Entwicklung Q4/2019 Konzepterstellung und Planung der Veranstaltung Q1/2020 Erste Workshop Durchführung (in Genf) Q4/2021 Bereitstellung einer gemeinsamen Plattform

3. Unterstützung des Global Forum on Cyber-Expertise	
Projektbeschreibung	Die Schweiz unterstützt das globale Forum zu Cyber-Kapazitäten und beteiligt sich an den internationalen Bemühungen, um Wissen und Expertise zu Cyber-Risikominimierung auf- bzw. auszubauen. Dazu entwickelt sie bestehende Projekte weiter und prüft die Teilnahme an weiteren Initiativen.
Zuständigkeit	EDA, Büro Sondergesandter für Cyber- Aussen- und Sicherheitspolitik, AIO, DV; VBS: MELANI
Meilensteine	 Q4/2022 Fortsetzung des Projekts „critical information infrastructure protection“ Q4/2022 Fortsetzung des Projekts «e-diplomacy» Q4/2022 Aktive Mitgestaltung der Arbeitsgruppe „Diplomacy, international norms and CBMs“.

7.9.3 Bilaterale politische Konsultationen und multilaterale Dialoge zu Cyber-Aussensicherheitspolitik (M27)

Übersicht Massnahme	
Massnahmenziel	Die Schweiz führt mit ausgewählten Ländern Konsultationen zu Cyber-Aussensicherheitspolitik durch, insbesondere zur Bedrohungslage und zu Trends. Sie gestaltet multilaterale Dialoge aktiv mit (z.B. Sino-European Cyber-Dialog).
Verantwortung für Massnahme	EDA, Büro Sondergesandter für Cyber- Aussen- und Sicherheitspolitik
Beteiligung	Interessierte Bundesstellen in verschiedenen Departementen
Bestehende Gremien / Prozesse / Konzepte	Politische Konsultationen, Sino European Cyber Dialogue NATO CDC 29+1
Umsetzungsprojekte der Massnahme	1. Bilaterale politische Cyber-Konsultationen 2. Sino European Cyber Dialogue – IL Arbeitsgruppe 3. MENA Dialogue

Umsetzungsprojekte

1. Bilaterale politische Cyber-Konsultationen	
Projektbeschreibung	Die Schweiz führt mit ausgewählten Ländern Konsultationen zu Cyber-Aussensicherheitspolitik unter Beteiligung anderer Departemente durch, insbesondere zur Bedrohungslage und zu Trends. Die Auswahl der Länder, mit welchen solche Dialoge etabliert werden sollen, wird in Zusammenarbeit mit den Fachdepartementen getroffen
Zuständigkeit	EDA, Büro Sondergesandter für Cyber- Aussen- und Sicherheitspolitik; andere interessierte Departemente

Meilensteine	Etablierung entsprechender Konsultationen
--------------	---

2. Sino-European Cyber Dialogue – Arbeitsgruppe IL

Projektbeschreibung	Der Sino-European Cyber Dialogue (SECD) ist ein 1.5 Dialog, an dem sich chinesische und europäische Regierungs- und Nichtregierungsvertreter über Themen der internationalen Cyber-Sicherheit und Internet Gouvernanz austauschen. Der Dialog ist eine vertrauensbildende Massnahme an sich: der Informationsaustausch wird gefördert sowie die Transparenz verbessert. Die Schweiz setzt sich für die Konkretisierung des SECD ein und schlägt die Etablierung einer Arbeitsgruppe zum Thema Völkerrecht vor.
Zuständigkeit	EDA, Büro Sondergesandter für Cyber- Aussen- und Sicherheitspolitik, DV
Meilensteine	 Q3/2019: Weiterführung des SECD Q2/2020: Etablierung der Arbeitsgruppe International Law

3. MENA Cybersecurity Forum

Projektbeschreibung	Das MENA-Cybersecurity Forum bietet einen Diskussionsrahmen für Staaten der MENA-Region an. Es ermöglicht, eine breite Palette an Cyber-Sicherheitsthemen zu diskutieren. Das Forum wurde 2016 vom GCSP und mithilfe des EDA ins Leben gerufen. Das GCSP und EDA zielen auf die Weiterführung und Etablierung des Forums ab.
Zuständigkeit	EDA, Büro Sondergesandter für Cyber-Aussen- und Sicherheitspolitik, AMON, GCSP
Meilensteine	 Q2/2020: Weiterführung des MENA Cybersecurity Forums

7.10 Aussenwirkung und Sensibilisierung

Die rasche Entwicklung und Zunahme von Cyber-Risiken führen in der Bevölkerung und in der Wirtschaft zu Verunsicherungen. Die aktive Kommunikation über die ergriffenen Massnahmen und die erzielten Fortschritte gehören deshalb zu den Aufgaben der Strategieumsetzung. Zusätzlich zur Kommunikation über die NCS soll der Bund auch zur Sensibilisierung gegenüber Cyber-Risiken beitragen. Die Information der Bevölkerung über Cyber-Risiken und mögliche Schutzmassnahmen trägt zur Prävention und zur Verbesserung der Resilienz bei und hilft, Verunsicherungen zu mindern. Neue Vorfälle haben ebenfalls gezeigt, dass es weiterhin nötig ist, die Allgemeinheit für Cyber-Risiken zu sensibilisieren und auf grundlegende Schutzmöglichkeiten aufmerksam zu machen. Die Information der Öffentlichkeit über die Umsetzung der NCS soll künftig aktiver erfolgen, so dass über den Kreis der Fachpersonen hinaus bekannt wird, welche Massnahmen der Bund zum Schutz der Schweiz vor Cyber-Risiken umsetzt. Im Sinne der Prävention soll der Bund und Kantone zudem verstärkt dazu beitragen, Bevölkerung, Wirtschaft und Politik für Cyber-Risiken zu sensibilisieren und über mögliche Schutzmassnahmen zu informieren.

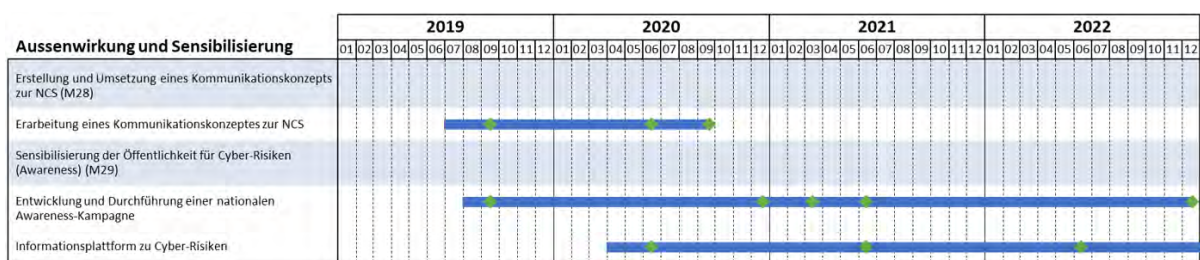


Abbildung 14 Roadmap Aussenwirkung und Sensibilisierung

7.10.1 Erstellung und Umsetzung eines Kommunikationskonzeptes zur NCS (M28)

Übersicht Massnahme	
Massnahmenziel	Die Kommunikationsleitlinien, Zuständigkeiten und Prozesse sind in einem Konzept festgehalten. Es wird dabei auch die Balance zwischen Vertraulichkeit und Informationsbedürfnis erörtert. Die Umsetzung des Konzepts über Medien- und Öffentlichkeitsarbeit soll zielgruppengerecht erfolgen und aktiv vorangetrieben werden.
Verantwortung für Massnahme	Kompetenzzentrum Cyber-Sicherheit
Beteiligung	In Abstimmung mit den NCS-Hauptakteuren
Bestehende Gremien / Prozesse / Konzepte	Laufende Sensibilisierungs- und Awareness-Kampagnen
Umsetzungsprojekte der Massnahme	1. Erarbeitung eines Kommunikationskonzeptes zur NCS

Umsetzungsprojekte

1. Erarbeitung eines Kommunikationskonzeptes zur NCS	
Projektbeschreibung	Erarbeitung eines Kommunikationskonzeptes zur NCS
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit
Meilensteine	 Q3/2019 Situationsanalyse erstellt Q2/2020 Kommunikationskonzept NCS (Ziele, Zielgruppen, Botschaften, Zielumsetzung (Strategie), Instrumente/Massnahmen, Erfolgsmessung sowie Budget) erarbeitet Q2/2020 Kommunikations-Verantwortlichkeiten sowie – Termine (Plan) definiert, sowie Abstimmung hierzu mit weiteren NCS-Akteuren erfolgt Q3/2020 Start der Umsetzung des Kommunikationsplans

7.10.2 Sensibilisierung der Öffentlichkeit für Cyber-Risiken (Awareness) (M29)

Übersicht Massnahme	
Massnahmenziel	Der Bund will mithelfen, die Öffentlichkeit für Cyber-Risiken zu sensibilisieren. Er verstärkt die Kommunikation zu Cyber-Risiken und nutzt die bestehenden Kapazitäten der in diesem Bereich bereits aktiven Vereinen, Verbände und Behörden.
Verantwortung für Massnahme	Kompetenzzentrum Cyber-Sicherheit
Beteiligung Bundestellten	GS-VBS, Fachämter
Beteiligung Dritter	Kantone, Bankenvertreter, SATW, ICTswitzerland
Bestehende Gremien / Prozesse / Konzepte	Kampagnen und Hilfsmittel folgender Organisationen: SATW (Unterrichtseinheiten für Lehrpersonen, Online-Challenge für Jugendliche 2019), Swiss Internet Security Alliance (StopThinkConnect), Schweiz. Kriminalprävention, E-Banking aber sicher, Schweiz. Verband für das Gütesiegel der Cyber-Sicherheit (Jugend&Medien), ICON NRO (KINDER4CYBER, Kit-Ausbildung), Zusammenarbeit zw. SVV und VBV (Ausbildungskonzept für Vertriebsmitarbeitenden für KMU-Sensibilisierungen) usw.
Rechtsetzungsbedarf	Die rechtlichen Grundlagen für die Aufgaben der Sensibilisierung sind zu erarbeiten.
Umsetzungsprojekte der Massnahme	1. Entwicklung und Durchführung einer nationalen Awareness-Kampagne 2. Informationsplattform zu Cyber-Risiken geführt durch die nationale Anlaufstelle

Umsetzungsprojekte

1. Entwicklung und Durchführung einer nationalen Awareness-Kampagne	
Projektbeschreibung	Durchführung einer nationalen Awareness-Kampagne zur Sensibilisierung der Öffentlichkeit für Cyber-Risiken (Awareness); über alle Bereiche der Cyber-Sicherheit, -Kriminalität sowie -Defence Nutzung von Synergien mit laufenden Kampagnen sowie bestehenden «Awareness»-Kapazitäten der in diesem Bereich bereits aktiven Akteure (Vereine, Verbände, Behörden usw.)
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit, in bereichsübergreifender Abstimmung mit aktiven Akteuren (fedpol, GS-VBS, SIP, SISA, SKP usw.), ICTswitzerland
Meilensteine	 Q3/2019 Abstimmung mit aktiven Akteuren zur konzeptionellen Erarbeitung einer nationalen Kampagne durchgeführt Q4/2020 Konzept zur nat. Kampagne erstellt Q1/2021 Umsetzungsplan vorhanden Q2/2021 Start / Produktion der nationalen Kampagne Q4/2022 Berichterstattung über die Durchführung sowie Wirksamkeit der nationalen Kampagne
2. Informationsplattform zu Cyber-Risiken	
Projektbeschreibung	Schaffung einer nationalen Informationsplattform zu Cyber-Risiken zur Prävention sowie Sensibilisierung. Die Plattform wird durch das Kompetenzzentrum Cyber-Sicherheit in enger Zusammenarbeit mit Wirtschaftsverbänden, Kantonen, Hochschulen und weiteren interessierten Stellen geführt.
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit
Meilensteine	 Q2/2020 Konzept für Plattform ist Entwickelt (Inhalte) Q2/2021 Lancierung der Plattform über die Sensibilisierungskampagne Q2/2022 Auswertung der Nutzung der Plattform und Anpassung der Inhalte

Abbildungsverzeichnis

Abbildung 1	Inhalte der NCS.....	4
Abbildung 2	Organisation des Bundes im Bereich Cyber-Risiken.....	6
Abbildung 3	Systematik des Umsetzungsplans	9
Abbildung 4	Roadmap Übersicht.....	12
Abbildung 5	Roadmap Kompetenzen- und Wissensaufbau.....	13
Abbildung 6	Roadmap Bedrohungslage.....	21
Abbildung 7	Roadmap Resilienz-Management.....	24
Abbildung 8	Roadmap Standardisierung / Regulierung	31
Abbildung 9	Roadmap Vorfallbewältigung.....	38
Abbildung 10	Roadmap Krisenmanagement.....	45
Abbildung 11	Roadmap Strafverfolgung.....	49
Abbildung 12	Roadmap Cyber-Defence.....	53
Abbildung 13	Roadmap Aktive Positionierung der Schweiz in der int. Cyber-Sicherheitspolitik.....	58
Abbildung 14	Roadmap Aussenwirkung und Sensibilisierung	65

Abkürzungsverzeichnis

AIO	Abteilung Vereinte Nationen und internationale Organisationen
AMS	Abteilung Menschliche Sicherheit
APCD	Aktionsplan für Cyber-Defence
BA	Schweizerische Bundesanwaltschaft
BABS	Bundesamt für Bevölkerungsschutz
BAG	Bundesamt für Gesundheit
BAKOM	Bundesamt für Kommunikation
BAV	Bundesamtes für Verkehr
BAZL	Bundesamt für Zivilluftfahrt
BFE	Bundesamt für Energie
BFI	Bildung, Forschung und Innovation
BinfV	Bundesinformatikverordnung
BIT	Bundesamt für Informatik und Telekommunikation
BJ	Bundesamt für Justiz
BLZ	Bundeslagezentrum
BSTB	Bundesstab Bevölkerungsschutz
BWL	Bundesamt für wirtschaftliche Landesversorgung
Canvas	Constructing an Alliance for Value-driven Cybersecurity
CBMs	confidence building measures
CCDCoE	Cooperative Cyber Defence Centre of Excellence
CDC	Cyber Defence Committee
CERT	Computer Emergency Response Team
CNO	Computer Network Operations
CSIRT	Computer Security Incident Response Team
CTC	Cyber Training Center
Cyber-SPOC-STA	Staatsanwaltschafts – Single Point of Contact
CYD-Campus	Cyber Defence Campus
DEA	Direktion für europäische Angelegenheiten
DV	Direktion für Völkerrecht
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EFD	Eidgenössisches Finanzdepartement
EJPD	Eidgenössisches Justiz- und Polizeidepartement
ENISA	Europäische Agentur für Netz- und Informationssicherheit
EPFL	École Polytechnique Fédérale de Lausanne
ETHZ	Eidgenössische Technische Hochschule Zürich
EU	Europäische Union
fedpol	Bundesamt für Polizei
FINMA	Eidgenössische Finanzmarktaufsicht
FSB	Financial Stability Board
FUB	Führungsunterstützungsbasis
G20	Gruppe der zwanzig wichtigsten Industrie- und Schwellenländer
GCSP	Geneva Centre for Security Policy
GIP	Geneva Internet Platform
GK	Geschlossener Kundenkreis
GNU	Gesamtnotfallübungen
GovCert	Governmental Computer Emergency Response Team
GS	Generalsekretariat
HPI	Harmonisierung der Schweizer Polizeiinformatik
HSLU	Hochschule Luzern
ICT	Information and Communication Technology
IKT	Informations- und Kommunikationstechnik
IOS	Informations- und Objektsicherheit

ISB.....	Informatiksteuerungsorgan des Bundes
Kdo.....	Kommando
KKJPD.....	Konferenz der kantonalen Justiz- und Polizeidirektorinnen und –direktoren
KKPKS.....	Konferenz der kantonalen Polizeikommandanten
LBA.....	Logistikbasis der Armee
MELANI.....	Melde- und Analysestelle Informationssicherung
MG.....	Militärsgesetz
MiGe.....	Ständige Mission der Schweiz beim Büro der Vereinten Nationen und den anderen internationalen Organisationen in Genf
MilCERT.....	Military Computer Emergency Readiness Team
MND.....	Militärischer Nachrichtendienst
NATO.....	North Atlantic Treaty Organization „Organisation des Nordatlantikvertrags“
NCS.....	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
NDB.....	Nachrichtendienst des Bundes
NDG.....	Nachrichtendienstgesetz
NEDIK.....	Netzwerk für die Ermittlungsunterstützung in der digitalen Kriminalität
OEWG.....	Open Ended Working Group
OIC.....	Operation Information Center
OSINT.....	Open Source Intelligence
OSZE.....	Organisation für Sicherheit und Zusammenarbeit in Europa
RK MZF.....	Regierungskonferenz Militär, Zivilschutz und Feuerwehr
SATW.....	Schweizerische Akademie der Technischen Wissenschaften
SBFI.....	Staatssekretariat für Bildung, Forschung und Innovation
SCE.....	Swiss Cyber Experts
SCION.....	Scalability, Control, and Isolation on Next-Generation Networks
SECD.....	Sino-European Cyber Dialogue
SFU.....	Strategische Führungsübung
SIB.....	Sensibilisierungskampagne IKT-Sicherheit in der Bundesverwaltung
SIF.....	Staatssekretariat für internationale Finanzfragen
SIK.....	Schweizerische Informatikkonferenz
SIPOL.....	Sicherheitspolitik
SISA.....	Swiss Internet Security Alliance
SKP.....	Schweizerische Kriminalprävention
SLA.....	Service-Level-Agreement
SOC.....	Security Operations Center
SPI.....	Schweizerisches Polizei-Institut
SSK.....	Schweizerische Staatsanwälte-Konferenz
StA NCS.....	Steuerungsausschuss NCS
SVS.....	Sicherheitsverbund Schweiz
SVU.....	Sicherheitsverbundübung
SVV.....	Schweizerische Versicherungsverband
SwissIGF.....	Swiss Internet Governance Forum
UN GGE.....	UN Governmental Group of Experts on Cyber Security
UNO.....	United Nations Organization; Vereinte Nationen
VBS.....	Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport
VBV.....	Berufsbildungsverband der schweizerischen Versicherungswirtschaft
VSE.....	Verband Schweizerischer Elektrizitätsunternehmen
W+T.....	Wissenschaft und Technologie
ZentG.....	Bundesgesetz über kriminalpolizeiliche Zentralstellen des Bundes
ZentrG.....	Zentralstellengesetz
ZEO.....	Zentrum elektronische Operationen

Anhang Umsetzungsplan der Kantone

Der Umsetzungsplan der Kantone zur Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018-2022 (NCS) wurde von einer Arbeitsgruppe des Sicherheitsverbundes Schweiz (SVS) erarbeitet und präsentiert sich eigenständig aber komplementär zum nationalen Umsetzungsplan. Es handelt sich konkret um 13 Umsetzungsprojekte in sieben von 10 Handlungsfeldern der NCS. Die Kantone äussern somit den Willen, in ihrer Zuständigkeit und aus eigener Initiative den Schutz ihrer Bevölkerung vor Cyber-Risiken weiter zu verbessern.

1. Kompetenzen- und Wissensaufbau

(1) Entwicklung eines Weiterbildungskonzepts und -moduls für kantonale Verwaltungen

M2 Ausbau und Förderung der Kompetenzbildung

Zielzustand	Eine proaktive und generelle Stärkung der Cyberkompetenzen ist eminent wichtig. Die kantonalen Verwaltungen und ihre zugehörigen Institutionen sind eine tragende Säule unserer Gesellschaft, ihr Personal muss deshalb zwingend in diesem Bereich geschult werden. Die kantonalen Informatikdienste haben das Umfeld, in dem wir uns bewegen, analysiert und setzen die erforderlichen technischen und organisatorischen Mittel zur Aufrechterhaltung einer sicheren Arbeitsumgebung ein. Vereinzelt wurden bereits Initiativen zum Ausbau der Kompetenzen des Personals ergriffen, bislang jedoch nicht systematisch, obwohl der Mensch unbestritten ein zentraler Faktor der Informationssicherheit ist.
Umsetzungsverantwortung	Haute école de gestion Arc – Institut de lutte contre la criminalité économique (ILCE) in Zusammenarbeit mit dem Service informatique de l'Entité neuchâteloise, dem Staatssekretariat für Bildung, Forschung und Innovation (SBFI), der Koordinationsstelle NCS und der Schweizerischen Informatikkonferenz (SIK)
Beteiligung	Hochschulen, Wirtschaftsverbände, Fachverbände (Schweizerischen Expertenvereinigung «Bekämpfung der Wirtschaftskriminalität» (SEBWK), Association suisse de la sécurité de l'information (CLUSIS) usw.)
Bestehende Gremien / Prozesse	In diesem Bereich bereits getroffene Massnahmen werden berücksichtigt und wo sinnvoll in das Vorgehen einbezogen.
Instrumente	• Vorschlag eines Ausbildungsprogramms für das Personal der kantonalen Verwaltungen mit klarer und pragmatischer Definition der angestrebten Ziele und Kompetenzen • Langfristige Sicherstellung des Ausbildungssystems zum Thema Cyber für Verwaltungsangestellte • Förderung der landesweiten Verbreitung dieser Ausbildung in allen betroffenen Behörden • Die Inhalte des Ausbildungsprogramms sollten idealerweise durch die Durchführung einer Pilot-Präsenzausbildung validiert werden; dies könnte in Neuenburg erfolgen, sobald das Ausbildungskonzept fertiggestellt ist.

Messbare Leistungsziele	• Erster Bericht; Ausgangslage • Ausbildungskonzept mit Zieldefinitionen nach Zielgruppen • Umfassendes, auf das Personal der kantonalen Verwaltungen zugeschnittenes Ausbildungsprogramm mit den folgenden Zielen: - o Entwicklung der Cybergrundkompetenzen aller Angestellten - o Den Angestellten die nötigen Mittel zur Verfügung stellen, um die Informationsflüsse angemessen steuern zu können, insbesondere jene von oder nach ausserhalb der Organisation - o Den Angestellten die Bedeutung von Informationen und damit den Nutzen von Massnahmen zur Sicherstellung gewisser Grundregeln betreffend Speicherung, Bearbeitung und Übermittlung von Informationen verständlich machen - o Den Angestellten die nötigen Kenntnisse vermitteln, damit sie gute Praktiken im Cyberbereich in ihrem privaten Umfeld vorleben können • Erarbeitung eines didaktischen Instruments, zum Beispiel im E-Learning-Format
-------------------------	--

2. Bedrohungslage

(2) #MISP⁴ – Malware Information Sharing Platform von MELANI für und mit den Kantonen

M4 Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyber-Bedrohungslage

Zielzustand	Zur Verbesserung ihrer Fähigkeiten der Beschreibung und Beurteilung von Cyberrisiken erstellen die Kantone einen Bedrohungsradar, für den sie die von MELANI zur Verfügung gestellten Informationen nutzen. Falls nötig integrieren sie darin kantonale Bedrohungsindikatoren. Die Kantone übernehmen in Zusammenarbeit mit dem Bund ein einheitliches Vokabular (Taxonomie), mit dem die Cyber-Bedrohungen schweizweit strukturiert und besser dargestellt werden können. Ergänzend dazu entwickeln sie einen Rahmen für die operative Zusammenarbeit, um Eindringversuche und Malware (Viren) besser abwehren zu können, und binden Nachrichtendienste und Stellen für das proaktive Monitoring der Cyber-Bedrohungen auf kantonaler Ebene ein.
Umsetzungsverantwortung	MELANI und die Kantone
Beteiligung	Hochschulen, Wirtschaftsverbände, Fachverbände, auf Cyber-Sicherheit spezialisierte private Akteure
Bestehende Gremien / Prozesse	• Cyber-Bedrohungsradar von MELANI • Plattform MISP (Malware Information Sharing Platform) von MELANI

⁴ MISP = Malware Information Sharing Platform, bezeichnet eine digitale Applikation, welche den Austausch zu Cyberbedrohungen und Informationen erleichtert.

Instrumente:	In Zusammenarbeit mit MELANI: 1. Adoption einer Taxonomie für eine kohärente und homogene Strukturierung und Darstellung der Cyberbedrohungen in der ganzen Schweiz (auf Ebene Bund, Kantone und Gemeinden) 2. Entwicklung eines kantonalen Modells des Cyberbedrohungsradsars 3. Einführung eines schweizerischen Netzwerks für den Informationsaustausch zu Malware, basierend auf einer MISIP-Lösung (Malware Information Sharing Platform) 4. Einführung eines Mindeststandards zur Prüfung der eigenen Vulnerabilität an der im Web exponierten Peripherie der kantonalen Netzwerke mittels regelmässiger Vulnerability Scans⁵ 5. Aufbau eines einfachen und effizienten Monitoring- und Analyseprozesses (OSINT – open-source intelligence), der zwischen Bund und Kantonen ausgetauscht werden kann Rahmenbedingung: • Einbindung kantonalen Experten für Cybersicherheit bei der Umsetzung der operativen Massnahmen in den Kantonen
Messbare Leistungsziele:	1. Adoption einer einheitlichen Taxonomie der Cyberbedrohungen durch Bund und Kantone 2. Kantonaler Cyberbedrohungsradar in Betrieb 3. Aktiver Austausch von operativen Informationen zu Malware zwischen den Kantonen 4. Regelmässige Evaluation der Sicherheit ihrer im Internet exponierten peripheren Netzwerkzugangspunkte durch die Kantone 5. Periodische Veröffentlichung von Berichten zum Monitoring der Cyberbedrohungen

3. Resilienzmanagement

(3) Erhebungstool zur Verbesserung der IKT-Resilienz in den Kantonen

M5 Verbesserung der IKT-Resilienz der kritischen Infrastrukturen

Zielzustand	Für eine Verbesserung der Resilienz (Widerstands- und Regenerationsfähigkeit) haben die Kantone minimale Anforderungen in Bezug auf relevante Prozesse, Aufgaben/Kompetenzen analysiert. Sie verwenden hierfür unter anderem ein Analyse-Tool, das sich an den vom Bundesamt für wirtschaftliche Landesversorgung⁶ publizierten Massnahmen zur Verbesserung der IKT-Resilienz in kritischen Teilsektoren orientiert und für ihre Bedürfnisse adaptiert wurde. Sie leiten aus den Erkenntnissen der Analyse weitere Massnahmen ab.
Umsetzungsverantwortung	Stv. Leiter Kantonale Informationssicherheit (Deputy CISO) des Kantons Basel-Stadt in Zusammenarbeit mit dem Sicherheitsverbund Schweiz

⁵ Vulnerability Scans sind mit einem Programm möglich, das Computer, Netzwerke und Anwendungen auf bekannte Schwachstellen untersucht.

⁶ Bundesamt für wirtschaftliche Landesversorgung; "Minimalstandard zur Verbesserung der IKT-Resilienz", Bern, 2018, abrufbar unter: https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html

Beteiligung	Jede Organisation resp. Betreiber einer kritischen Infrastruktur (KI) ist für die Informationssicherheit selber verantwortlich. Die Verantwortung trägt die Geschäftsleitung. Die Geschäftsprozessverantwortlichen, der Risikomanager, der Informationssicherheitsbeauftragte, der Informatikleiter und ev. der Notfallmanager sind die wichtigsten Ansprechpartner der Geschäftsleitung.
Bestehende Gremien / Prozesse	In der Organisation wird der Business Continuity Management (BCM) Prozess aufgebaut und von einer externen Stelle überprüft. Wichtige Ressourcen innerhalb des BCM sind: • Mitarbeitende • Gebäude und Räume • Informatik- und Telekommunikationsmittel (IKT) und Informationen • Externe Dienstleistende und Informationen
Instrumente:	Einsatz des Erhebungstools Mit der Durchführung der Erhebungen zur Einschätzung der eigenen IKT-Resilienz verstärken die Unternehmen ihre Sicherheitsorganisation. Die Erhebung bietet eine Grundlage für die Zuweisung von Verantwortlichkeiten, Kompetenzen und klaren Aufgaben. Ein rascher Indikator bietet der Erfüllungsgrad der empfohlenen Sicherheitsmassnahmen. Bei einem allfälligen Defizit können risikomindernde Massnahmen definiert werden. Anonyme Übersicht der beteiligten Organisationen Die Informationen (Identifizieren, Schützen, Detektieren, Reagieren und Wiederherstellen), die die beteiligten Organisationen dem SVS mitteilen, werden aufbereitet und anonymisiert. Die Resultate werden definierten Gremien in anonymisierter Form vorgestellt. BCM-Prozess Für den BCM-Prozess ist es notwendig, dass alle Geschäftsprozesse dokumentiert sind. Das Risikomanagement, das Notfallmanagement oder. Krisenmanagement und das IT-Notfallmanagement müssen zwingend vorhanden sein. Wichtige Informationen sind die maximale Ausfallzeit und eventuelle Ausweichszenarien, diese Vorgaben werden vom Geschäftsprozessverantwortlichen und von der Geschäftsleitung vorgegeben.
Messbare Leistungsziele:	• Betreiber kritischer Infrastrukturen in der Schweiz haben anhand des ihnen zur Verfügung gestellten Erhebungstools individuell ihre Defizite in Bezug auf die IKT-Resilienz festgestellt und entsprechende Massnahmen getroffen. Messgrössen sind: - o Erfüllungsgrad in % - o Risikoerhebung (tief, mittel oder hoch) - o Maximal zu erwartender Schaden in Abhängigkeit der Zeit. • Die Durchführung der Erhebung unter Betreibern kritischer Infrastrukturen hat dazu geführt, dass gezielte Massnahmen ausgeführt wurden und die IKT-Resilienz sich insgesamt verbessert. Die umgesetzten Massnahmen wurden auf ihre Wirksamkeit überprüft. Messgrössen sind: - o offene Massnahmen, - o Massnahme in Bearbeitung und - o umgesetzte Massnahmen • Die Resultate der Erhebung wurden in vordefinierten Gremien bspw. Staatsschreiberkonferenz (SSK), Schweizerische Informatikkonferenz (SIK) in anonymisierter Weise vorgestellt. Messgrössen sind: - o Übersicht der beteiligten Organisationen

	o Veranstaltungen, an denen die Resultate vorgestellt worden sind
--	---

(4) Verstärkter Erfahrungsaustausch über die Schweizerische Informatikkonferenz (SIK) mit der Schaffung von Grundlagen

M7 Erfahrungsaustausch und Schaffung von Grundlagen zur Stärkung der IKT-Resilienz in den Kantonen

Zielzustand	Mit einem institutionalisierten Erfahrungsaustausch und Dialog fördern die Kantone die Zusammenarbeit zur Stärkung der IKT-Resilienz. Sie nutzen dafür bestehende Netzwerke und erweitern diese wie angebracht. Sie nehmen aktiv an der Arbeitsgruppe Informatiksicherheit der SIK teil. Somit bauen sie beständig gegenseitiges Vertrauen auf, unterstützen sich gegenseitig und koordinieren ihr Vorgehen, nicht zuletzt im Ereignisfall. Sie erstellen gemeinsam hilfreiche Grundlagen (Konzepte, Checklisten, etc.).
Umsetzungsverantwortung	Arbeitsgruppe Informatiksicherheit der SIK in Zusammenarbeit mit den federführenden, kantonalen Regierungsstellen und deren Informationssicherheitsbeauftragten
Beteiligung	SVS
Bestehende Gremien / Prozesse	• Kantonale Informationssicherheitsbeauftragter • Arbeitsgruppe Informatiksicherheit innerhalb der SIK
Instrumente:	• Kantonale Informatikstrategie • Kantonales Risikomanagementsystem • Kantonale IT-Risikomanagement • Kantonales Ausbildungskonzept • Kantonales Informationssicherheitsmanagementsystem (ISMS)
Messbare Leistungsziele:	• Die Kantone stellen sicher, dass der Kantonale Informationssicherheitsbeauftragte Mitglied der Arbeitsgruppe „Informatiksicherheit“ der SIK ist. Nachweis: Die kantonalen Informatiksicherheitsbeauftragten arbeiten zusammen und vertrauen sich gegenseitig. Sie setzen die Empfehlungen der Arbeitsgruppe in ihren Kantonen um. • Die Kantone stellen sicher, dass ihre Mitarbeitenden und externen Partner regelmässig bezüglich aller Belange der Informationssicherheit und der Cybersecurity angemessen und stufengerecht geschult und ausgebildet werden. Nachweis: Übersicht der durchgeführten Kampagnen und Schulungen. • Ein IT-Risikomanagement (Teil des kantonalen Risikomanagements), das auch die Risiken der kritischen Infrastrukturen enthält, ist umgesetzt. Nachweis: Vorhandenes IT-Risikomanagement inkl. Übersicht der risikomindernden Massnahmen. • Ein der Organisation angepasstes Informationssicherheitsmanagementsystem (ISMS) ist eingeführt. Nachweis: das ISMS ist von der Leitung genehmigt und wird „gelebt“.

(5) Sensibilisierung der jungen und älteren Menschen für Cyberrisiken

Zielzustand	Für eine verbesserte Resilienz der Schweiz in Bezug auf Cyberrisiken werden sowohl die junge als auch die ältere Bevölkerungsschicht sensibilisiert. Mit einem verstärkten Bewusstsein für die Bedrohungen aus dem Cyberraum verändern sie ihr Verhalten so, dass sie die Möglichkeiten der Digitalisierung ausschöpfen können ohne vermeidbare Risiken einzugehen. Durch die Vermittlung von bestimmten, zielgruppengerechten Lerninhalten konnten die jungen und älteren Menschen ihr Wissen im Bereich der Digitalisierung und der daraus resultierenden Chancen und Risiken erhöht.
Umsetzungsverantwortung	Schweizerische Konferenz der kantonalen Erziehungsdirektion (EDK) in Zusammenarbeit mit der Konferenz der kantonalen Sozialdirektorinnen und Sozialdirektoren (SODK) und der Schweizerischen Kriminalprävention (SKP),
Beteiligung	pro senectute, pro juventute, privatim, SVS
Bestehende Gremien / Prozesse	
Instrumente	Die jungen und älteren Menschen in der Schweiz sollen über die Lehrpersonen einerseits und über das Pflegepersonal andererseits auf die Risiken, denen sie im Cyberraum begegnen können, aufmerksam gemacht werden.
Messbare Leistungsziele	• Etablierung und Konsolidierung einer Partnerschaft für die Sensibilisierung der jungen und älteren Menschen • Konzeption von zugeschnittenen Lerninhalten

4. Standardisierung/Regulierung

(6) Umsetzung der Netzwerksicherheitspolicy (NSP)

M8 Entwicklung und Einführung von Minimalstandards

Zielzustand	Die Kantone betreiben ihre Netze und Systeme sicher, indem sie die Ausschnittstellen zu ihren Informatiknetzwerken möglichst gut sichern und auch die Tätigkeiten innerhalb des eigenen Netzwerkes permanent überwachen. Mit dieser gemeinsamen Basis erhöhen die Kantone auch die Sicherheit innerhalb gemeinsam genutzter Netzwerke und Applikationen. • Förderung der Zusammenarbeit unter Einhaltung der vordefinierten Standards • Aufbau des gegenseitigen Vertrauens durch den Einsatz der definierten Standards • Geeignete Dokumentation (Konzepte, Checklisten, etc.) • Geeignete und sichere Dokumentenablage
Umsetzungsverantwortung	Konferenz der Kantonsregierungen (KdK)

Beteiligung	Schweizerische Informatikkonferenz SIK, SVS
Bestehende Gremien / Prozesse	- Arbeitsgruppe Informatiksicherheit innerhalb der SIK - Melde und Analysestelle der Informationssicherung MELANI
Instrumente:	- Netzwerk Netzwerk-Sicherheits-Politik (als Basis dient die NSP-SIK 2017) - Orientierung an weiteren bestehenden Standards - Geeignete Prozesse (Change-, Problem-, Incidents- Risiko- und Notfallmanagement) - Einsatz von definierten Standards und Empfehlungen bspw. ISO 2700x, BSI, SANS CSC, oder CIS 20
Messbare Leistungsziele:	- Kantonseigene Netzwerk-Sicherheits-Policy wurde erarbeitet und in Anlehnung an die Vorgaben der SIK (NSP-SIK 2017)⁷ umgesetzt. - Definierte und gelebte Standards - Ausgebildetes Personal - Definierte Prozesse (Change-, Problem-, Incident- Risiko-, Notfallmanagement sowie Berichtswesen)

5. Krisenmanagement

(7) Cyber-Übung mit kritischen Infrastrukturen im Gesundheitssektor

M17 Gemeinsame Übungen zum Krisenmanagement

Zielzustand	Die Koordination auf operativer Ebene zwischen Bund, den Kantonen und Vertretern kritischer Infrastrukturen in einer Krisensituation funktioniert. Das Lagebild ist in der Krise aktuell und kann von den betroffenen Stellen eingesehen werden. Das Konzept zur Führung in Krisen mit Cyber-Ausprägungen konnte getestet werden.
Umsetzungsverantwortung	SVS
Beteiligung	Bundeskanzlei, Gesundheitsdirektorenkonferenz
Bestehende Gremien / Prozesse	Allgemeines Krisenmanagement (Führungsabläufe und –prozesse) der Kantone und des Bundes unabhängig vom Szenario SVU19
Instrumente	Konzept M15 NCS I erweitert um Kantone und KI.
Messbare Leistungsziele	- Anzahl durchgeführter Übungen mit allen betroffenen Organisationen (1 Table Top Übung bis 2020, 1 Stabsrahmenübung bis 2021) - Ein aktuelles und präzises Lagebild war während der Übung jederzeit verfügbar und wurde von den teilnehmenden Akteuren adäquat bewertet (Evaluation) - Die an der Übung teilnehmenden Akteure konnten auf die Unterstützung der Stäbe durch fachspezifisches Wissen zählen (Einschätzung der Akteure der Übungserfahrung, Umfrage)

⁷ Die Netzwerksicherheitspolicy der Schweizerischen Informatikkonferenz ist über das Intranet der selbigen für alle Mitglieder abrufbar.

	• Die Beteiligten kennen die jeweiligen Zuständigkeiten und Ansprechstellen • Die Beteiligten kennen die Prozesse • Die Übungen wurden ausgewertet und die Lehren fliessen in die Optimierung der Führungsabläufe und –prozesse ein. Dafür wird ein Monitoringplan aufgesetzt. Die Erkenntnisse werden rapportiert.
--	---

(8) Schaffung der kantonalen Organisationen für Cyber-Sicherheit

Zielzustand	Analog zur neu geschaffenen Organisationsstruktur im Cyber-Bereich auf Stufe Bund beabsichtigt diese Massnahme die Schaffung kantonalen Organisationen für Cyber-Sicherheit. Diese kantonale Stelle mit Budgethoheit und Weisungsbefugnis behält zu jeder Zeit den Überblick, repräsentiert den Kanton in Cyber-Belangen, vertritt ihn im KFS und gewährleistet die Schnittstellen im Kanton, zwischen den Kantonen und zum Bund.
Umsetzungsverantwortung	Federführendes kantonales Departement
Beteiligung	Informationssicherheitsbeauftragte der Kantone, kantonale Führungsstäbe (KFS), Kantonspolizeien, Staatsanwaltschaften, Betreiber kritischer Infrastrukturen, SVS, Cyber-Delegierte/r des Bundes
Bestehende Gremien / Prozesse	Der SVS erarbeitet mit seiner Arbeitsgruppe Umsetzung NCS II mit den Kantonen einen Entwurf, der den Kantonen als Richtlinie und Vorlage zur Schaffung ihrer eigenen kantonalen Organisation für Cyber-Sicherheit zur Verfügung stehen soll.
Instrumente	
Messbare Leistungsziele	• Richtlinie/Vorlage durch die AG des SVS erarbeitet • in jedem Kanton wurde SOLL/IST-Analyse durchgeführt • Erstellung der kantonalen Cyber-Konzepte: Aufgaben, Kompetenzen und Verantwortung sind in einem kantonalen Cyberkonzept definiert • die kantonalen Exekutivbehörden haben zur Schaffung der kantonalen Cyberorganisation Beschluss gefasst

6. Aussenwirkung und Sensibilisierung

(9) Aktive Kommunikation zu den Tätigkeiten der Kantone im Rahmen der NCS II

M28 Erstellung und Umsetzung eines Kommunikationskonzepts zur NCS

Zielzustand	Die interessierte Bevölkerung im Allgemeinen und die Partner des Sicherheitsverbundes Schweiz im Spezifischen haben die Möglichkeit sich über verschiedene Kanäle zu den Arbeiten der Kantone im Rahmen der NCS II zu informieren. Die Medien- und Öffentlichkeitsarbeit erfolgt zielgruppengerecht und ist aktiv und dynamisch. Dabei legen die Stakeholder besonders Wert darauf, die Zusammenarbeit unter den Kantonen und über die Regierungsebenen hinweg zu unterstreichen, aber auch an die Eigenverantwortung zu appellieren. Ein Kommunikationskonzept wurde erarbeitet und umgesetzt.
Umsetzungsverantwortung	SVS

Beteiligung	SIK, KKJPD
Bestehende Gremien / Prozesse	
Instrumente	• Cyber-Landsgemeinde • Website des SVS • Jahresberichte zur Umsetzung der Projekte aus dem Plan • Medienmitteilungen
Messbare Leistungsziele	• Ein Kommunikationskonzept (Leitlinien, Zuständigkeiten, Prozesse) besteht und wurde umgesetzt. • Verschiedene Kommunikationsprodukte wurden über diverse Kanäle der interessierten Bevölkerung und den Partnern des SVS zielgruppengerecht und zeitnah zur Verfügung gestellt (Anzahl publizierter Kommunikationsprodukte, Resonanz, Reichweite) • Umfrage zum Bekanntheitsgrad