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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Informatiksteuerungsorgan des Bundes ISB
Eidgenössisches Finanzdepartement EFD

Inhaltsverzeichnis

1 Einleitung

Seit der Erarbeitung der ersten Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) im Jahr 2012 hat sich die Cyber-Thematik sehr stark weiterentwickelt und in der öffentlichen Wahrnehmung massiv an Bedeutung gewonnen. Verantwortlich dafür ist die Tatsache, dass Cyber-Risiken immer relevanter werden für unser Land. Die Digitalisierung verstärkt unsere Abhängigkeit von funktionierenden IKT-Infrastrukturen im Alltag und gleichzeitig steigen die Bedrohungen durch Cyber-Angriffe weiter an. Dies manifestiert sich an der weiterhin zunehmenden Cyber-Kriminalität, an der Häufung von Fällen der Cyber-Spionage, aber auch am Einsatz von Cyber-Mitteln zur Erreichung von politischen Zielen. Das Ausmass, in welchem Cyber-Angriffe im Rahmen von politischen Destabilisierungskampagnen eingesetzt werden, war 2012 noch kaum absehbar.
Nach fünf Jahren war es deshalb an der Zeit, die NCS grundsätzlich zu überarbeiten und sie auf die intensivierte Bedrohungslage anzupassen. Der Bundesrat hat folglich 2017 das Informatiksteuerungsorgan des Bundes damit beauftragt, in Zusammenarbeit mit den Departementen, den Kantonen, der Wirtschaft und den Hochschulen eine neue NCS zu erarbeiten. Am 18. April 2018 wurde die neue Strategie durch den Bundesrat verabschiedet. Sie enthält nun 10 Handlungsfelder mit 29 Massnahmen und definiert dadurch ein weitreichendes Programm zum Schutz der Schweiz vor Cyber-Risiken.
Jede Strategie ist jedoch nur so gut wie seine Umsetzung. Bereits bei der Verabschiedung der Strategie im April 2018 hat der Bundesrat erkannt, dass diese nur gelingen kann, wenn der Bund seine bestehenden Ressourcen klarer strukturiert und diese gezielt ausbaut. Aus dem Parlament und der Wirtschaft wurden gleichzeitig der Aufbau eines Cyber-Kompetenzzentrums im Bund gefordert. 2018 war deshalb stark geprägt von den Arbeiten zum Aufbau der neuen Strukturen und von der Erarbeitung eines detaillierten Umsetzungsplans zur NCS. Es gelang – dank der guten Zusammenarbeit aller beteiligten Akteure – diese Arbeiten weit voranzutreiben, so dass der Bundesrat Ende Januar 2019 die Organisation des Bundes im Bereich Cyber-Risiken festlegen und im April darauf den Umsetzungsplan verabschieden konnte.
Der vorliegende Bericht geht nochmals auf die Resultate dieser Arbeiten ein, da sie die Grundlage für die Umsetzung der NCS bilden. Weiter werden aber zugleich die vorangegangene Umsetzung von wichtigen NCS-Massnahmen aufgezeigt. Bei allen wichtigen Entwicklungen auf strategischer und organisatorischer Ebene soll nicht vernachlässigt werden, dass zahlreiche Akteure aus der Verwaltung, der Wirtschaft, den Kantonen und den Hochschulen bereits massgebliche Fortschritte bei der Umsetzung von konkreten Massnahmen erzielt haben. Die Berichterstattung bezieht sich dabei auf den Zeitraum von 2018 bis im Mai 2019, da so die Entscheide des Bundesrats zur Umsetzungsplanung vom Mai 2019 in den Bericht integriert werden können.

2 Die NCS 2018 – 2022 auf einen Blick

Am 18. April 2018 hat der Bundesrat die «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS2018 – 2022» verabschiedet und am 15. Mai 2019 – nach der Klärung der organisatorischen Fragen, welche sich aus der NCS ergeben haben – den Umsetzungsplan dazu beschlossen.

2.1 Die Inhalte der Strategie

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. Sie 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:

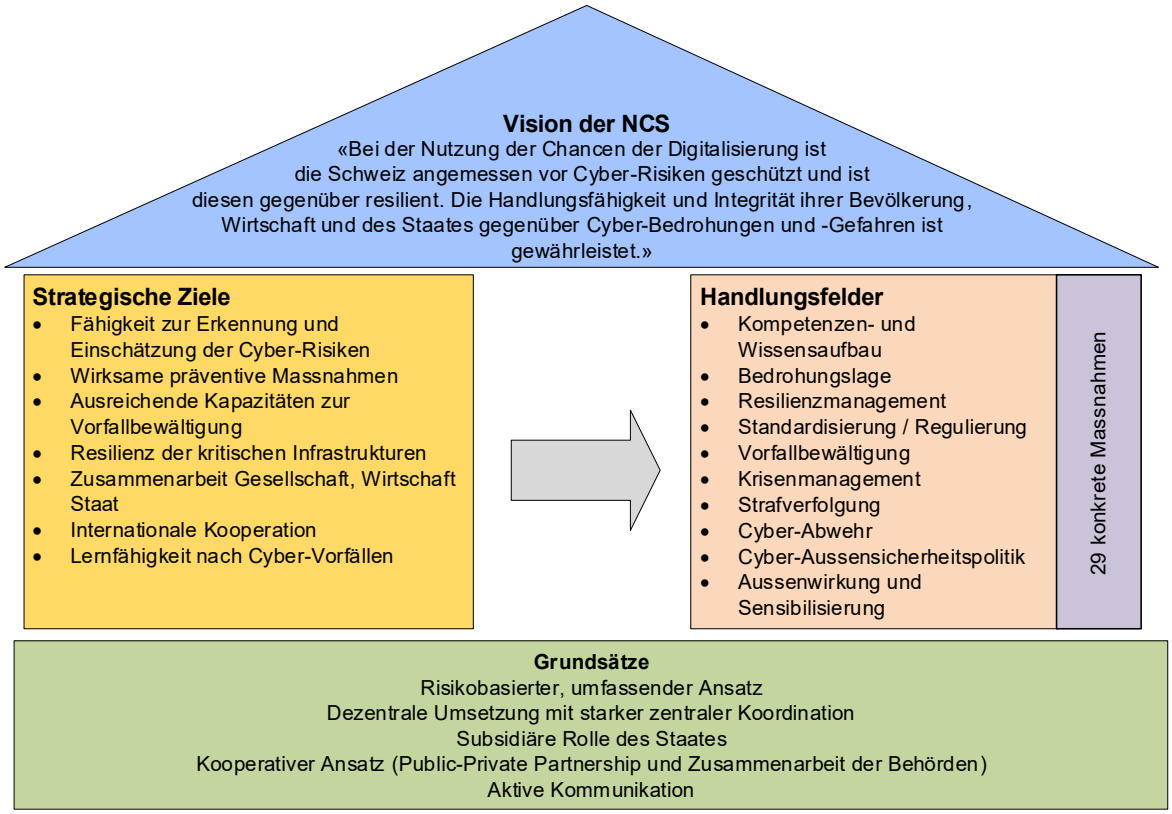


Abbildung 1 Inhalte der NCS 2018–2022

2.2 Umsetzungsplan

Im Umsetzungsplan werden für alle 29 Massnahmen der NCS konkrete Umsetzungsprojekte definiert. Der Plan legt die Verantwortlichkeiten, die zu erreichenden Leistungsziele und die Meilensteinplanung für diese Projekte fest.[1] Er wurde gemeinsam unter Beteiligung der verantwortlichen Bundesstellen, der Kantone, der Wirtschaft und den Hochschulen Ende 2018 und Anfangs 2019 im Rahmen von folgenden vier Workshops erarbeitet:

- 06. Dez. 2018: Handlungsfeld «Kompetenzen- und Wissensaufbau»
- 22. Jan. 2019 Handlungsfelder «Bedrohungslage», «Vorfallbewältigung», «Krisenmanagement» und «Aussenwirkung und Sensibilisierung»
- 31. Jan. 2019 Handlungsfelder «Resilienz-Management» und «Standardisierung/Regulierung»
- 19. Feb. 2019 Einbezug der Kantone und deren Umsetzungsplan

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

[1] Eine Übersicht über alle Umsetzungsprojekte inklusive Meilensteine findet sich im Anhang 1.

3 Organisation

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 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.

3.1 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.

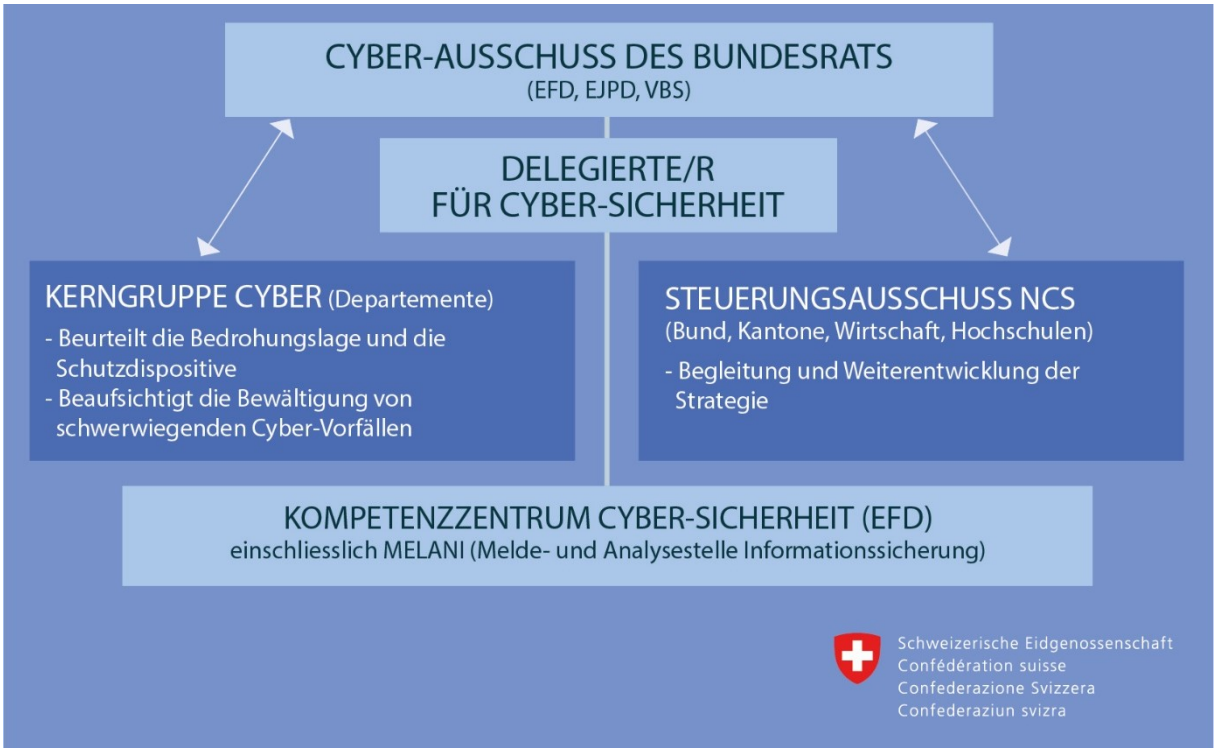


Abbildung 2 Organisation des Bundes im Bereich Cyber-Risiken

Mit Bezug auf die NCS 2018–2022 ist die Aufgabenteilung zwischen diesen neu geschaffenen Gremien und Funktionen wie folgt definiert:

- Der **Cyber-Ausschuss des Bundesrats,** welcher sich aus den Vorstehenden der Departemente Eidgenössisches Finanzdepartement (EFD), Eidgenössisches Justiz- und Polizeidepartement (EJPD) und Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) zusammensetzt, hat die Aufgabe, die Umsetzung der NCS zu beaufsichtigen.
- Das **Kompetenzzentrums 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.
- Die/der **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-Sicherheit** 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.

3.2 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.

3.2.1 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 Polizei-direktorinnen 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.
Der/dem Delegierten für Cyber-Sicherheit kommt bei der Zusammenarbeit auf politisch-strategischer Ebene ebenfalls eine bedeutende Rolle zu. Sie/er ist die zentrale Ansprechperson des Bundes für Fragen zur Cyber-Sicherheit, nimmt politische Anliegen auf und legt diese dem Cyber-Ausschuss des Bundesrates vor.

3.2.2 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;[2]
- Vertretungen der Kantone und der Koordinationsgremien zwischen Bund und Kantonen durch das Generalsekretariat der Kantonalen Konferenz der Justiz- und Polizeidirektorinnen und –direktoren (KKJPD), den 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 die/den Delegierte/n des Bundes für Cyber-Sicherheit. Das Sekretariat des Gremiums übernimmt die Geschäftsstelle Cyber-Sicherheit der/des Delegierten.

[2] Jedes Departement und die BK verfügen über mindestens eine Vertretung

3.2.3 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 der/des Delegierten für Cyber-Sicherheit.

4 Stand der Umsetzung der NCS

Handlungsfeld «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.

Massnahmen

1) Früherkennung von Trends und Technologien und Wissensaufbau
2) Ausbau und Förderung von Forschungs- und Bildungskompetenz
3) Schaffung von günstigen Rahmenbedingungen für eine innovative IKT-Sicherheitswirtschaft in der Schweiz

---

Umgesetzte oder laufende Arbeiten:

- **Neuer Abschluss als «ICT-Security Expert» mit eidgenössischem Diplom:** Im November 2018 fanden die ersten eidg. Höheren Fachprüfungen «ICT Security Expert mit eidg. Diplom» stattt. 12 Prüfungsteilnehmende (2 Frauen, 10 Männer) erhielten das Diplom.
- **Neuer Abschluss als «Cyber Security Specialist» mit eidgenössischem Fachausweis:** Auf Anregung der Schweizer Armee wurde die neue Berufsprüfung «Cyber Security Specialist» unter der Leitung von ICT-Berufsbildung Schweiz erarbeitet. Mit der Genehmigung der Prüfungsordnung am 6. Mai 2019 durch das SBFI sind die rechtlichen Grundlagen geschaffen. Der Projektabschluss ist auf Ende 2019, die erste Prüfung im 2020 vorgesehen. Die Berufsprüfung wurde in Zusammenarbeit mit Vertretern aus Wirtschaft, Verwaltung, Armee und Bildung erarbeitet.
- **Cyberlehrgang der Schweizer Armee:** Am 17. Mai 2019 wurde der erste Cyberlehrgang der Armee mit 18 Teilnehmer abgeschlossen. Der Lehrgang startete am 6. August 2018 nach einer Vorbereitungszeit von nur 5 Monaten und dauerte 40 Wochen. Die Armee führt pro Jahr zwei Cyberlehrgänge mit jeweils maximal 25 Teilnehmern durch. Nach Abschluss des Lehrgangs können die Teilnehmer mit einem ICT Berufsabschluss freiwillig und ohne weiteren Besuch einer Ausbildung die Berufsprüfung zum "Cyber Security Specialist" ablegen. Der Lehrgang wird zudem durch die Hochschule Luzern mit 21 ETCS-Punkten für das Bachelor-Studium "Information & Cyber Security" anerkannt. Abklärungen mit weiteren Hochschulen laufen.
- **Cyber Defence Campus:** Im Januar 2019 hat der Cyber-Defence Campus (CYD Campus) des VBS seinen Betrieb aufgenommen. Unter der Federführung von armasuisse

W+T haben sich Experten aus dem VBS, der Industrie und Hochschulen zusammengeschlossen, um in allen cyberrelevanten Themen ein breites Know-how aufzubauen. Der CYD Campus hat zum Ziel laufende Entwicklungen in der "Cyber-Welt" früh zu erkennen, zu beobachten und Handlungsstrategien zu entwickeln.

- **Gemeinsamens Forschungszentrum der beiden ETH zu Cyber-Sicherheit:** Die beiden ETH haben ein Konzept erarbeitet für die Schaffung eines gemeinsamen Forschungs- und Supportzentrum im Bereich Cyber-Sicherheit. Das Zentrum soll Bund und Kantone mit Fachwissen aus den beiden ETH unterstützen.
- **Gemeinsamer Studiengang Cyber-Security der ETH und der EPFL:** Die beiden ETH bieten ab dem Studienjahr 2019/2020 einen gemeinsamen Master zu Cyber-Security an.

Handlungsfeld «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.

Massnahmen

4) Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyber-Bedrohungslage

---

Umgesetzte oder laufende Arbeiten:

- **Definition der Zielgruppen und Klärung der Bedürfnisse:** Im Rahmen der Workshops zur Umsetzungsplanung der NCS wurden die Bedürfnisse der Wirtschaft und der Behörde in Bezug auf die Lagedarstellung erfasst und Konzepte für die Erstellung der Bedrohungslage entwickelt.
- **MELANI Halbjahresberichte:** MELANI veröffentlicht alle sechs Monate umfassende Berichte über die aktuelle Bedrohungslage. Der Halbjahresbericht 2/2018 wurde am 30. April 2019 publiziert.

Handlungsfeld «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.

Massnahamen

5) *Verbesserung der IKT-Resilienz der kritischen Infrastrukturen*
6) *Verbesserung der IKT-Resilienz in der Bundesverwaltung*
7) *Erfahrungsaustausch und Schaffung von Grundlagen zur Verbesserung der IKT-Resilienz in den Kantonen*

Umgesetzte oder laufende Arbeiten:

- **Round Tables für die kritischen Sektoren:** Es fanden Round Tables zur Cyber-Sicherheit für die Sektoren Luftverkehr (16. Okt. 2018), Verwaltung (20. Juni 2018 / 19. März 2019), Finanzen (28. Juni 2018 / 12. Dez. 2018), Energie (24. April 2018 / 07. Nov. 2018 / 14. Mai 2019) und Gesundheit (07. März 2018 / 12. Sept. 2018) statt.
- **Überarbeitung der Weisungen des Bundesrats über die IKT-Sicherheit in der Bundesverwaltung (WIsB):** Die überarbeitete Version wurde am 16. Januar 2019 durch den Bundesrat verabschiedet und per 15. Februar 2019 in Kraft gesetzt.
- **Cyber-Landsgemeinde und Arbeitsgruppen des SVS:** Am 28. März 2019 fand die Cyber-Landsgemeinde zur Förderung des Austausches zwischen Kantonen und Bund im Bereich Cyber-Risiken statt. Der SVS ist zudem im Begriff zur Umsetzung der NCS in den Kantonen dem Umsetzungsplan der Kantone entsprechende Arbeitsgruppen zu gründen. Die im Umsetzungsplan definierten Projekte sind folgende: «Entwicklung eines Weiterbildungskonzepts und –moduls für kantonale Verwaltungen», «Malware Information Sharing Platform von MELANI für die und mit den Kantonen», «Erhebungstool zur Verbesserung der IKT-Resilienz in den Kantonen», «Verstärkter Erfahrungsaustausch über die Schweizerische Informatikkonferenz (SIK) mit der Schaffung von Grundlagen», «Sensibilisierung für Cyber-Risiken», «Umsetzung der Netzwerksicherheitspolicy (NSP)», «Cyber-Übung mit kritischen Infrastrukturen im Gesundheitssektor», «Schaffung der kantonalen Organisation für Cyber-Sicherheit» und «Aktive Kommunikation zu den Tätigkeiten der Kantone im Rahmen der NCS».

Handlungsfeld «Standardisierung und 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.

Massnahmen

8) Evaluierung und Einführung von Minimalstandards
9) Prüfung einer Meldepflicht für Cyber-Vorfälle und Entscheid über Einführung
10) Globale Internet-Gouvernanz
11) Aufbau von Expertise zu Fragen der Standardisierung in Bezug auf Cyber-Sicherheit

---

Umgesetzte oder laufende Arbeiten:

- **IKT-Minimalstandard:** Das Bundesamt für wirtschaftliche Landesversorgung (BWL) hat im August 2018 den IKT-Minimalstandard veröffentlicht. (https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html)
- **Branchenstandards:** Der Verband Schweizerischer Elektrizitätsunternehmen (VSE) und der Schweizerische Verein des Gas- und Wasserfaches (SVGW) haben für ihre Sektoren basierend auf dem Minimalstandard sektorspezifische Standards entwickelt.
- **Cybersecurity Schnelltest für KMU:** Entwicklung und Umsetzung eines Schnelltests zur IKT-Sicherheit von KMU (https://ictswitzerland.ch/themen/cyber-security/check/).
- **Konzept Studie Meldepflicht:** Es wurde eine Studie zur Erarbeitung von möglichen Modellen für eine Meldepflicht in der Schweiz gestartet.
- **Globale Internet Gouvernanz:** Das hochrangige Panel des UNO-Generalsekretärs zur Verbesserung der globalen digitalen Zusammenarbeit hat im Juli 2018 seine Arbeit aufgenommen, wobei sich die Schweiz seither in Person von Altbundesrätin Doris Leuthard aktiv in die Arbeiten eingebracht hat, u.a. am Treffen im Januar 2019 in Genf. Der Abschlussbericht wird per Juni 2019 erwartet. Am 20. November 2018 fand zudem in Bern das Swiss Internet Governance Forum statt.
- **Expertenpool Standardisierung:** Beteiligte Stellen des Bundes haben sich am 15. Januar 2019 zu einer ersten Sitzung für die Gestaltung des künftigen Expertenpools getroffen. Der Expertenpool wird ab 2020 seine operative Tätigkeit aufnehmen können.

Handlungsfeld «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 Kompetenzzent-rum 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.

Massnahmen:

12) Ausbau von MELANI als Public-Private-Partnership für die Betreiber kritischer Infrastrukturen
13) Aufbau von Dienstleistungen für alle Unternehmen
14) Zusammenarbeit des Bundes mit relevanten Stellen und Kompetenzzentren
15) Prozesse und Grundlagen der Vorfallbewältigung des Bundes

---

Umgesetzte oder laufende Arbeiten:

- **Gezielte Erweiterung des geschlossenen Kundenkreises von MELANI:**
  2018:
  Firmen: Zunahme um 39 von 254 (01. Jan. 2018) auf 293 (31. Dez. 2018)
  Sektoren: 1 neuer Sektor («e-Health». Beide dort vertretenen Firmen waren vorher im Sektor «Gesundheitswesen»); Stärkste Zunahme in den Sektoren «Finanz» (+8), «Gesundheitswesen» (+7) und «Energie» (+6)
  2019 (Stand: 31. Mai 2019):
  Firmen: Zunahme um 9 von 293 (01. Jan. 2019) auf
  Sektoren: 2 neue Sektoren («Bildung und Forschung» / «NGO»)
  Stärkste Zunahme im Sektor «Energie» (+2), jeweils Zunahme um +1 in den Sektoren «Blaulichtorganisationen», «Versicherungen», «Vorsorgeeinrichtungen», «Bildung und Forschung», «Gesundheitswesen», «NGO» sowie «Transport und Logistik»
- **Beschluss des Kompetenzzentrums**: Mit seinen Entscheiden vom 4. Juli 2018 und vom 30. Januar 2019 hat der Bundesrat die Schaffung des Kompetenzzentrums für Cyber-Sicherheit beschlossen und dieses beauftragt, eine nationale Anlaufstelle für Cyber-Sicherheit zu etablieren.
- **Ausbau der Plattform zum Informationsaustausch:** Das Vorhaben zur Ablösung von Melani-NET wurde gestartet. Es wurde ein erster Proof of Concept (POC) realisiert.
- **Prozesse für die Vorfallbewältigung:** Als Grundlage für die noch zu erarbeitende Verordnung zur Cyber-Sicherheit in der Bundesverwaltung hat das ISB einen Sicherheitsvorfallbewältigungsprozess erarbeitet und diesen mit den Leistungserbringern und –bezügern diskutiert.

Handlungsfeld «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 Vornherein 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.

Massnahmen:

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

17) Gemeinsame Übungen zum Krisenmanagement

Umgesetzte oder laufende Arbeiten:

- **Übung Cyber PAKT:** Das VBS hat auch 2018 in seiner jährlichen Übung Cyber PAKT die Prozesse zur Krisenbewältigung bei Cyber-Vorfällen geübt und dabei die betroffenen Bundesstellen einbezogen.
- **Übung Cyber-Europe 2018:** Die Schweiz hat sich im 2018 an der Übung «Cyber-Europe» beteiligt, welche sich um das Szenario einer Attacke auf den Flugverkehr drehte.
- **Übung "Locked Shields" des Nato Cooperative Cyber Defence Centre of Excellence (CCDCOE):** An der Übung in Tallinn im April 2018 nahmen zivile und militärische Experten der Schweiz teil. Von Seiten der Armee nahmen neben Vertretern der Verwaltung auch die Absolventen des ersten Cyber-Lehrgangs an dieser Übung am Standort Bern teil.

Handlungsfeld «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.

Massnahmen:

18) Lagebild Cyber-Kriminalität
19) Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung
20) Ausbildung
21) Zentralstelle Cyber-Kriminalität

Umgesetzte oder laufende Arbeiten:

- **Gründung des Cyberboards:** Im Mai 2018 wurde das Cyberboard als Zusammenschluss aller relevanten mit der Cyber-Kriminalität befassten Akteure der Kantone und des Bundes gegründet. Seither finden regelmässige Sitzungen zum Austausch auf operativer Stufe (Cyber-CASE) und auf strategischer Stufe (Cyber-STRAT) statt.
- **Nationale Fallübersicht:** Das Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung hat mit der Erfassung der Fälle in den Kantonen begonnen.
- **Zentralstelle Cyber-Kriminalität:** Das Parlament hat die 17.3479 Motion Dobler «Zentrale Anlauf- und Koordinationsstelle zur Bekämpfung der organisierten und international tätigen Computerkriminalität» am 14. März 2018 überwiesen.

Handlungsfeld «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 Nachrichtendienstgesetzt 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.

Massnahmen:

22) Ausbau der Fähigkeiten zur Informationsbeschaffung und Attribution
23) Fähigkeit zur Durchführung von aktiven Massnahmen im Cyber-Raum gemäss NDG und MG
24) Gewährleistung Einsatzbereitschaft der Armee über alle Lagen im Cyber-Raum und Regelung ihrer subsidiären Rolle zur Unterstützung der zivilen Behörden

---

Umgesetzte oder laufende Arbeiten:

- **Überarbeitung Aktionsplan Cyber-Defence:** Der Aktionsplan Cyber-Defence wurde im Dezember 2018 überarbeitet. Er legt die Leistungen des VBS fest, insbesondere für subsidiäre Einsätze der Armeemittel für die zivilen Behörden.
- **Verordnung militärische Cyber-Abwehr:** Am 30. Januar 2019 hat der Bundesrat die Verordnung militärische Cyber-Abwehr verabschiedet. Diese regelt die Organisation und die Zuständigkeiten für die Wahrung der militärischen Sicherheit im Cyberraum. Sie ist am 1. März 2019 in Kraft getreten.
- **Cyber-Lehrgang:** Am 6. August 2018 wurde der erste Cyber-Lehrgang mit 18 Rekruten gestartet. Diese schlossen ihre Ausbildung nach 41 Wochen erfolgreich ab.
- **Das Organisationsprojekt «Cyber Defence Aufbau»** (Umsetzung PACD in der Führungsunterstützungsbasis) verläuft nach Planung und wird Ende 2019 abgeschlossen.
- **Cybertruppen in der Schweizer Armee:** Der Ausbau der Cybertruppen in der Schweizer Armee ist in Erarbeitung. Vorgesehen ist die Schaffung eines Fachstabes Cyber und eines Cyber Bataillons. Der Einsatz der Cybertruppen erfolgt im Rahmen und unter direkten Führung der Berufsorganisation FUB**.**

Handlungsfeld «Cyber-Aussen- und 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-Aussensicherheitspolitikgetroffen werden.

Massnahmen:

25) Aktive Mitgestaltung und Teilnahme an Prozessen der Cyber-Aussensicherheitspolitik
26) Internationale Kooperation zum Auf- und Ausbau von Kapazitäten im Bereich Cyber-Sicherheit
27) Bilaterale politische Konsultationen und multilaterale Dialoge zu Cyber-Aussensicherheitspolitik

---

Umgesetzte oder laufende Arbeiten:

- **UNO:** Der erste Ausschuss der UNO Generalversammlung hat 2018 zwei Resolutionen zu Cyber-Sicherheit verabschiedet und somit zwei parallellaufende Prozesse ins Leben gerufen. Die Schweiz ist Mitglied der UN Group of Governmental Experts und leistet einen Beitrag zur der Weiterentwicklung der staatlichen Verhaltensnormen. Daneben wird die Schweiz den zweiten Prozess, die Open Ended Working Group präsidieren.
- **Stärkung des internationalen Genfs:** Die Schweiz setzt sich aktiv dafür ein, das internationale Genf als Plattform für Diskussionen zur Cyber-Aussensicherheitspolitik zu positionieren. Vor diesem Hintergrund hat das EDA den Genfer Dialog zu verantwortlichem Verhalten aller Akteure ins Leben gerufen – eine Multistakeholder-Plattform, welche Vertreter aller Akteursgruppen vereint**.**
- **Expertenprozess Völkerrecht und Cyber-Sicherheit:** Die Schweiz trägt aktiv zur Klärung der Frage bei, wie die Prinzipien des Völkerrechts, einschliesslich der UNO-Charta-Verpflichtungen, Menschenrechte, des Völkergewohnheitsrechts und Internationalen Humanitären Rechts (HVR) sowie anderer Regeln im Cyberspace gelten. Vor diesem Hintergrund hat das EDA einen Expertenprozess eingeleitet, um die Anwendung bestehender Normen und Regeln des Völkerrechts auf den Cyberspace zu klären. Der Prozess soll in die internationalen Debatten (UNGGE und der OEWG) Eingang finden.
- **Förderung des diplomatischen Instruments zur Vertrauensbildung im Cyber-Raum:** Vertrauensbildende Massnahmen (VBM) wirken krisenpräventiv und konfliktverhütend. Mittels Transparenz und Kooperation sollen sie Vertrauen und Stabilität schaffen. Dadurch wird das Risiko von Missverständnissen und Fehlinterpretationen vermindert. Die Schweiz engagiert sich als OSZE-Mitglied aktiv für die Erarbeitung, Umsetzung und Weiterentwicklung der VBMs. So hat die Schweiz zusammen mit Deutschland einen Vorschlag zur Entwicklung eines OSZE-Konsultationsmechanismus unterbreitet.
- **Bilaterale sicherheitspolitische Konsultationen mit ausgewählten Ländern und Dialoge:** Die Schweiz führt mit einigen ausgewählten Ländern sicherheitspolitische Konsultationen durch; wo sinnvoll, ist Cyber Teil dieser Konsultationen. In diesen Gesprächen geht es darum, über Cyber-Bedrohungen zu sprechen, sich über die gegenseitigen Prioritäten auszutauschen sowie mehr über den Aufbau und die Organisation im Cyber-Bereich zu erfahren. Die Schweiz ist auch Mitglied des Sino-Europen Cyber Dialogue, der den Austausch zwischen China und europäischen Staaten im Bereich Cyber fördert, und gestaltet diesen als Mitglied aktiv mit**.**

Handlungsfeld «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.

Massnahmen:

28) Erstellung und Umsetzung eines Kommunikationskonzepts zur NCS

29) Sensibilisierung der Öffentlichkeit für Cyber-Risiken (Awareness)

Umgesetzte oder laufende Arbeiten:

- **Swiss Cyber Security Days:** Am 27./28. Februar 2019 fanden in Fribourg die Swiss Cyber Security Days statt. Den Veranstaltern gelang es, über 2'000 Interessierten Informationen zu Cyber-Risiken zu vermitteln. Der Bund war durch Fachvorträge und zwei Ständen des VBS (einer mit Fokus auf die zivile Cyber-Sicherheit und einer zur Cyber-Defence) vertreten.
- **Bevölkerungsumfrage zu Cyber-Risiken:** Der Bund hat zusammen mit Partnern aus der Wirtschaft eine Bevölkerungsumfrage zu Cyber-Risiken durchgeführt. Diese Resultate bieten die Grundlage für die geplanten Sensibilisierungskampagnen.

5 Übersicht pendente Vorstösse (Motionen und Postulate)

5.1 Überwiesene Vorstösse

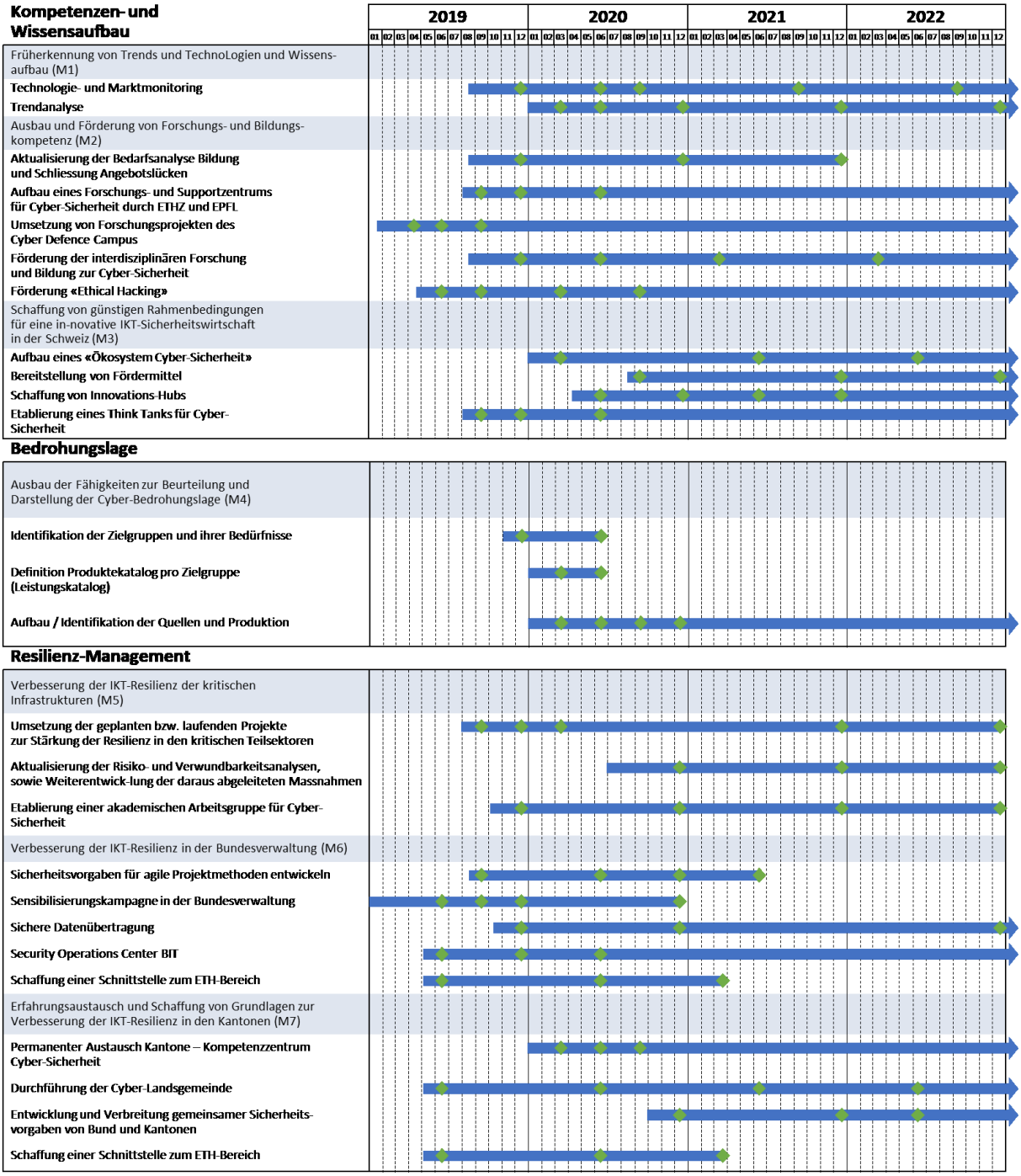
Vorstoss	Übersicht Inhalte
16.4073 Po. Golay «Cyber-Risiken: für einen umfassenden, unabhängigen und wirksamen Schutz» (überwiesen 28.2.18)	Bericht zur Aufteilung der Kompetenzen zwischen EFD und VBS.
17.3475 Po. Graf-Litscher «Meldepflicht bei schwerwiegenden Sicherheitsvorfällen bei kritischen Infrastrukturen» (überwiesen 13.12.2017)	Bericht über die Möglichkeiten einer Einführung von Meldepflichten für kritische Infrastrukturen.
17.3497 Mo. Dobler «Zentrale Anlauf- und Koordinationsstelle zur Bekämpfung der organisierten und international tätigen Computerkriminalität» (überwiesen 14.3.18)	Die Bekämpfung der organisierten und international tätigen Computerkriminalität ist zentral zu regeln mittels einer neuen gesetzlichen Grundlage.
17.3507 Mo. Dittli «Ein Cyberdefence-Kommando mit Cybertruppen für die Schweizer Armee» (überwiesen am 6.3.18)	Einrichtung eines Cyber-Defence-Organisation mit 100-150 professionellen Spezialisten und milizmässige Cybertruppen (400 bis 600 Angehörige der Armee).
17.3508 Mo. Eder «Schaffung eines Cyber-Security-Kompetenzzentrums auf Stufe Bund» (überwiesen 7.12.18)	Es ist ein Cyber-Security-Kompetenzzentrum auf Stufe Bund zu schaffen.
17.4295 Po. Glättli «Sicherheitsstandards für Internet-of-Things-Geräte prüfen, weil diese eine der grössten Bedrohungen der Cybersicherheit sind»	Bericht über Sicherheit bei IoT-Geräten.
18.3003 Po. SiK NR «Eine klare Cyber-Gesamtstrategie für den Bund» (überwiesen 6.3.18)	Erstellung eines Gesamtkonzepts zum Schutz und zur Verteidigung des zivilen und militärischen Cyberraumes.

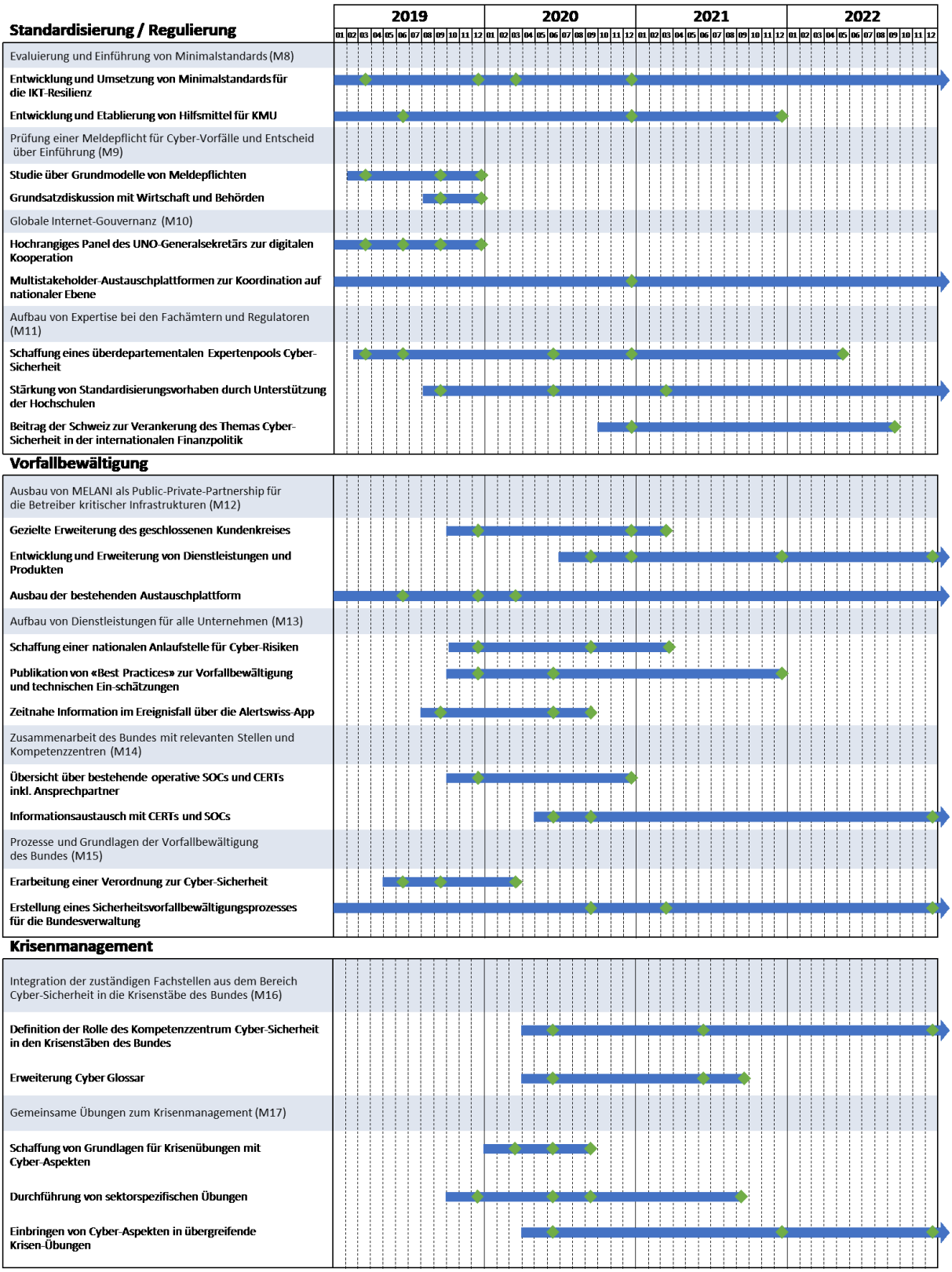
5.2 Im Parlament noch nicht behandelte Vorstösse

Vorstoss	Übersicht Inhalte
18.3565 Po. CVP-Fraktion «Schadensdeckung. Ereignislimite bei Cyberangriffen»	Prüfung einer Ereignislimite bei Cyberangriffen, ab welcher der Bund die Schadensdeckung übernimmt.
18.4051 Mo. Golay «Cybersicherheit, Cyberabwehr. Wo stehen wir?»	Jährlicher Bericht zur Cyber-Sicherheit.
18.4387 Mo. Gugger «Bundesrat und VBS geben der Cybersecurity 2019 höchste Priorität»	Schaffung eines überdepartementalen Kompetenzzentrums im VBS.
19.3199 Po. Reynard «Améliorer la sécurité des objets connectés»	Bericht wie der Datenschutz bei IoT-Geräten verbessert werden kann.
19.3121 Mo. Buffat «Traitement national des fuites de données»	MELANI soll systematisch Informationen über Datenlecks beschaffen und Informationen dazu Betroffenen weiterleiten.
19.3135 Po. Dobler «Haben wir die Cyber-Sicherheit bei Beschaffungen der Armee im Griff?»	Bericht zur Sicherheit von Lieferanten von Komponenten kritischer Infrastrukturen.
19.3136 Po. Dobler «Haben wir die Hard- und Softwarekomponenten bei unseren kritischen Infrastrukturen im Griff?»	Bericht zur Sicherheit von Lieferanten von Komponenten kritischer Infrastrukturen.

6 ANHANG

In nachfolgender Roadmap werden pro Handlungsfeld der NCS sämtliche Massnahmen aufgelistet und deren Umsetzungsprojekte mit den entsprechenden Laufzeiten visualisiert. Die Projekte in den Massnahmen und die auf der Roadmap grün markierten Meilensteine sind im Umsetzungsplan im Detail beschrieben.




2019
2020
2021
2022
01 02 03 04 05 06 07 08 09 10 11 12
Standardisierung / Regulierung
Evaluierung und Einführung von Minimalstandards (M8)
Entwicklung und Umsetzung von Minimalstandards für die IKT-Resilienz
Entwicklung und Etablierung von Hilfsmittel für KMU
Prüfung einer Meldepflicht für Cyber-Vorfälle und Entscheid über Einführung (M9)
Studie über Grundmodelle von Meldepflichten
Grundsatzdiskussion mit Wirtschaft und Behörden
Globale Internet-Gouvernanz (M10)
Hochrangiges Panel des UNO-Generalsekretärs zur digitalen Kooperation
Multistakeholder-Austauschplattformen zur Koordination auf nationaler Ebene
Aufbau von Expertise bei den Fachämtern und Regulatoren (M11)
Schaffung eines überdepartementalen Expertenpools Cyber-Sicherheit
Stärkung von Standardisierungsvorhaben durch Unterstützung der Hochschulen
Beitrag der Schweiz zur Verankerung des Themas Cyber-Sicherheit in der internationalen Finanzpolitik
Vorfallbewältigung
Ausbau von MELANI als Public-Private-Partnership für die Betreiber kritischer Infrastrukturen (M12)
Gezielte Erweiterung des geschlossenen Kundenkreises
Entwicklung und Erweiterung von Dienstleistungen und Produkten
Ausbau der bestehenden Austauschplattform
Aufbau von Dienstleistungen für alle Unternehmen (M13)
Schaffung einer nationalen Anlaufstelle für Cyber-Risiken
Publikation von «Best Practices» zur Vorfallbewältigung und technischen Ein-schätzungen
Zeitnahe Information im Ereignisfall über die Alertswiss-App
Zusammenarbeit des Bundes mit relevanten Stellen und Kompetenzzentren (M14)
Übersicht über bestehende operative SOCs und CERTs inkl. Ansprechpartner
Informationsaustausch mit CERTs und SOCs
Prozesse und Grundlagen der Vorfallbewältigung des Bundes (M15)
Erarbeitung einer Verordnung zur Cyber-Sicherheit
Erstellung eines Sicherheitsvorfallbewältigungsprozesses für die Bundesverwaltung
Krisenmanagement
Integration der zuständigen Fachstellen aus dem Bereich Cyber-Sicherheit in die Krisenstäbe des Bundes (M16)
Definition der Rolle des Kompetenzzentrum Cyber-Sicherheit in den Krisenstäben des Bundes
Erweiterung Cyber Glossar
Gemeinsame Übungen zum Krisenmanagement (M17)
Schaffung von Grundlagen für Krisenübungen mit Cyber-Aspekten
Durchführung von sektorspezifischen Übungen
Einbringen von Cyber-Aspekten in übergreifende Krisen-Übungen

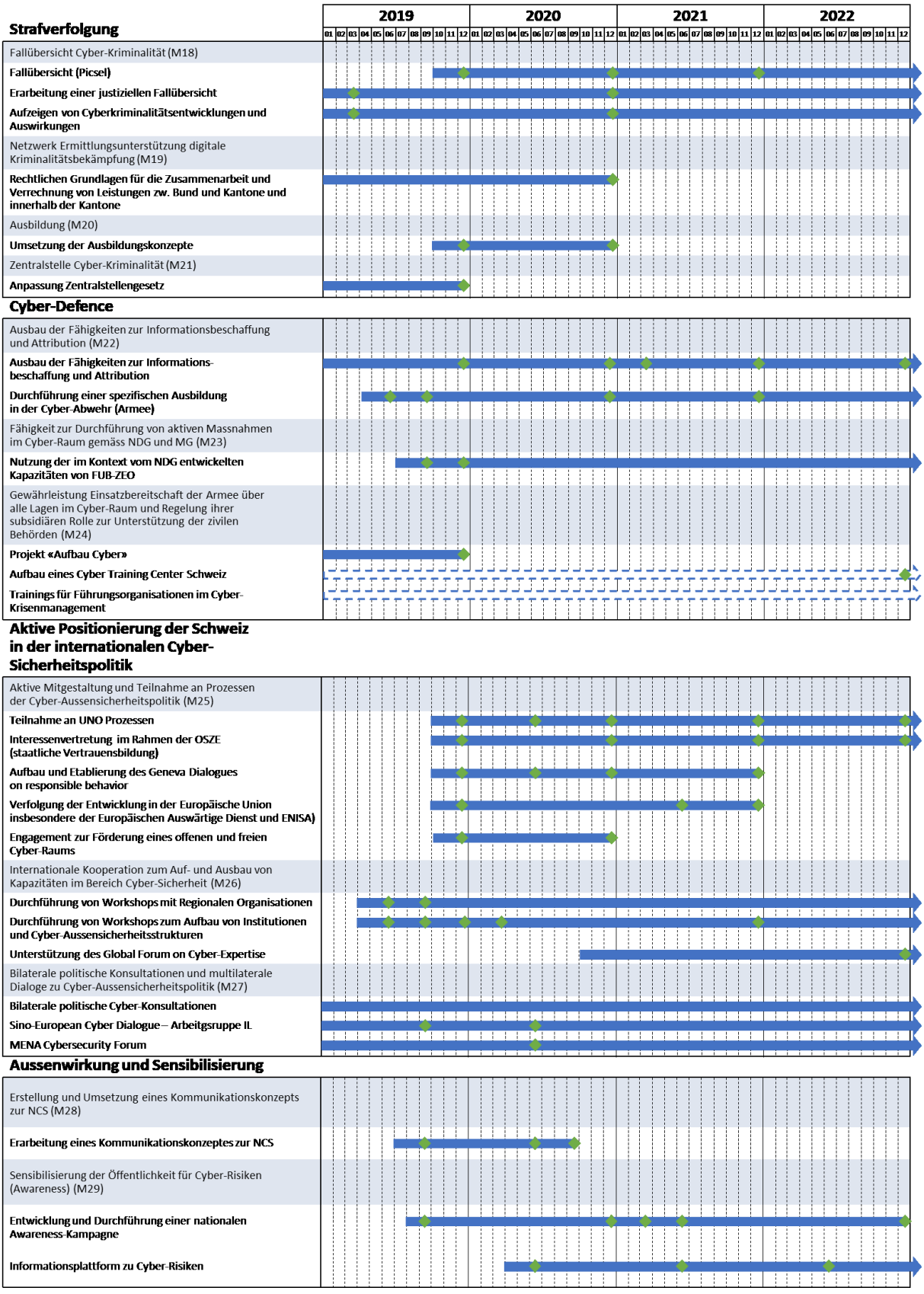


Abbildung 3 Roadmap Übersicht