Bern, 27.11.2019

Bericht über die Organisation des Bundes zur Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken

Bericht des Bundesrates in Erfüllung der Postulate 16.4073 Golay vom 15.12.16 und 18.3003 SiK NR vom 22.01.18 und der Motion 17.3508 Eder vom 15.06.2017

Inhaltsverzeichnis

1 Einleitung

Die Cybersicherheit hat in den vergangenen Jahren auf allen Ebenen stark an Bedeutung gewonnen. Sie spielt zunehmend eine zentrale Rolle in der nationalen und internationalen Aussen- und Sicherheitspolitik, wird immer stärker zu einem wichtigen Faktor für den Wirtschaftsstandort der Schweiz und aus der Bevölkerung war schon jede siebte Person direkt von einem Cyberangriff betroffen.[1]
Der Bundesrat hat in Reaktion auf diese Entwicklung verschiedene Beschlüsse getroffen, um die Aktivitäten des Bundes im Bereich Cybersicherheit zu stärken. Im April 2018 hat er die «Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken 2018–2022» beschlossen, im Juli 2018 Grundsatzentscheide zur Organisation des Bundes im Bereich Cyberrisiken getroffen, diese im Januar 2019 mit der Schaffung eines Kompetenzzentrums Cybersicherheit unter der Leitung der ebenfalls neuen Stelle des/der Delegierten des Bundes für Cybersicherheit konkretisiert und schliesslich im Mai 2019 den Umsetzungsplan und eine erste Tranche der dafür benötigten Ressourcen verabschiedet. Mit diesen Beschlüssen ist der Bundesrat auch verschiedenen Vorstössen aus dem Parlament nachgekommen. Mit dem vorliegenden Bericht wird dem Parlament der Umsetzungsstand zur 17.3508 Mo. Eder dargelegt und die in den beiden Postulaten 16.4073 Golay und 18.3003 SIK-N gestellten Fragen beantwortet.

1.1 Auftrag

Die beiden Postulate 16.4073 Golay und 18.3003 SiK NR verlangen einen Bericht des Bundesrates über die Organisation des Bundes bei der Umsetzung der «Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken» (NCS). Die Motion 17.3508 Eder verlangt vom Bundesrat die Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund. Im Wortlaut verlangen die überwiesenen Vorstösse folgende Massnahmen des Bundes:

16.4073 Po. Golay «Cyberrisiken. Für einen umfassenden, unabhängigen und wirksamen Schutz»: Der Bundesrat wird gebeten, einen Bericht über die Anwendung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) vorzulegen. Bevölkerung und Wirtschaft konnten davon nämlich bisher nicht viel wahrnehmen. Der Bericht soll insbesondere Fragen zur Aufteilung der Kompetenzen zwischen dem Eidgenössischen Finanzdepartement (EFD) und dem Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) sowie die mit der Aufteilung verbundenen Risiken behandeln. Ausserdem sollen folgende Aspekte beleuchtet werden: die Führung bei grossen nationalen Krisen, Fragen und Risiken im Zusammenhang mit der Abhängigkeit von im Ausland ansässigen oder in ausländischem Besitz befindlichen Dienstleistungsanbietern, der Erhalt von hochstehendem Fachwissen in der Schweiz sowie die Intensivierung der Zusammenarbeit zwischen Wissenschaft, Industrie und Bund.

18.3003 Po. SiK NR «Eine klare Cyber-Gesamtstrategie für den Bund»: Der Bundesrat wird beauftragt, bis Ende 2018 ein klares Gesamtkonzept zum Schutz und zur Verteidigung des zivilen und militärischen Cyberraumes zu erstellen. Die gegenwärtig laufenden Arbeiten der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) sind dabei zu berücksichtigen. Die Zusammenführung bereits bestehender oder in Erarbeitung befindlicher Departementskonzepte (Aktionspläne) ist kein Gesamtkonzept (eins plus eins muss mehr ergeben als zwei). Das Gesamtkonzept soll mindestens enthalten:
- eine klare Definition des Auftrags der Armee im Bereich Cyberverteidigung;
- Eine klare Definition des Auftrags der zivilen Cyberbehörden;

[1] Studie «Sicherheit im Internet – Repräsentative der Deutsch- und Westschweizer Bevölkerung», gfs-zürich, 2019.

- woraus sich ergibt: die Abgrenzung und Visualisierung der Kompetenzen (Organigramm mit allen im Bereich Cyber involvierten Stellen inklusive Pflichtenheften beim Bund);
- ein Konzept für die Finanzierung (einschliesslich allfälliger Beschaffungen und folgender Betriebskosten) und realistische Personalrekrutierung für die Verteidigung und zivile Cyberbehörden;
- einen internationalen Vergleich zwischen der Schweiz und hinsichtlich Struktur, Mengengerüst und Herangehensweise relevanten Ländern hinsichtlich der Ressourcen und Finanzen für den militärischen und zivilen Cyberbereich.

Der Bericht soll a) die subsidiäre Unterstützung der zivilen Behörden und b) den möglichen Ernst- und Verteidigungsfall, in dem der Bundesrat Teile der Armee als strategische Reserve einsetzt, beinhalten. Der Bundesrat wird beauftragt, ein klares Gesamtkonzept zum Schutz und zur Verteidigung des zivilen und militärischen Cyberraumes zu erstellen. Das Gesamtkonzept soll klare Definitionen der Aufträge der Armee und der zivilen Behörden enthalten, so dass diese in einem Organigramm festgehalten werden können. Geklärt werden sollen auch die Fragen der Finanzierung und der Personalrekrutierung sowie die Frage, wie die Armee die zivilen Behörden subsidiär unterstützen kann und welche Rolle sie im Verteidigungsfall übernimmt. Schliesslich soll in einem internationalen Vergleich aufgezeigt werden, wie vergleichbare Länder den militärischen und zivilen Cyberbereich schützen.

17.3508 Mo. Eder «Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund»: Der Bundesrat wird beauftragt, im Zusammenhang mit der laufenden Überarbeitung der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) ein Cybersecurity-Kompetenzzentrum auf Stufe Bund zu schaffen und dafür die notwendigen Massnahmen einzuleiten. Diese Organisationseinheit hat die Aufgabe, die zur Sicherstellung der Cybersecurity notwendigen Kompetenzen zu verstärken und bundesweit zu koordinieren. Sie soll departementsübergreifend wirksam sein, das heisst insbesondere, dass sie im Bereich Cybersecurity über Weisungsbefugnis gegenüber den Ämtern verfügen soll. Das Kompetenzzentrum arbeitet mit Vertretern der Wissenschaft (Hochschulen, Fachhochschulen), mit der IT-Industrie und mit den grösseren Infrastrukturbetreibern (insbesondere Energie, Verkehr) zusammen.

1.2 Ausgangslage

Zu bemerken ist, dass alle drei Vorstösse vor der Verabschiedung der NCS 2018–2022 am 18. April 2018 eingereicht worden sind. Die zu diesem Zeitpunkt gültige erste NCS 2012-2017 bezog sich explizit nur auf Massnahmen der zivilen Akteure und gab keine Vorgaben im Bereich Cyberdefence vor. Die sich aus dieser Trennung ergebenden Abgrenzungsprobleme wurden in der Evaluation zur NCS 2012-2017 erkannt. Als Reaktion darauf hat der Bundesrat beschlossen, den Bereich Cyberdefence in die NCS zu integrieren, so dass diese zur übergeordneten Dachstrategie für alle Aktivitäten zum Schutz der Schweiz vor Cyberrisiken wird.
Im Anschluss an die Verabschiedung der NCS im April 2018 hat der Bundesrat weitere Entscheide getroffen, welche den in den Postulaten formulierten Forderungen entgegenkommen. Tabelle 1 gibt einen Überblick zu den für die beiden Postulate relevanten Beschlüssen des Bundesrats:

Datum	BRB	Inhalt
18. April 2018	Verabschiedung der NCS 2018–2022	Beschluss der NCS mit 29 Massnahmen in 10 Handlungsfeldern. Die NCS unterscheidet bezüglich Organisation zwischen den drei Bereichen Cybersicherheit, Cyberdefence und Cyberstrafverfolgung.
04. Juli 2018	Grundsatzentscheide zur künftigen Organisation des Bundes im Bereich Cyberrisiken	Beschluss der Grundelemente der Organisation: • Cyberausschuss des BR (EFD, VBS, EJPD) • Kerngruppe Cyber zur Koordination zwischen EFD, VBS, EJPD (inkl. Einbezug der übrigen Departemente und der Kantone bei Bedarf) • Kompetenzzentrum Cybersicherheit im EFD unter der Leitung eines / einer Delegierten des Bundes für Cybersicherheit
30. Januar 2019	Beschluss der Organisation des Bundes im Bereich Cyberrisiken	Beschluss der gemäss Grundsatzentscheiden ausgearbeiteten Organisation.
30. Januar 2019	Verordnung über die militärische Cyberabwehr	In der Verordnung sind die Zuständigkeiten und Verantwortlichkeiten für die militärische Cyberabwehr definiert.
15. Mai 2019	Verabschiedung des Umsetzungsplans zur NCS 2018–2022	Definition der Zuständigkeiten und des Zeitplans für die Umsetzung der NCS. Schaffung von insgesamt 24 Stellen ab 2020.

Tabelle 1 Beschlüsse des Bundesrats zur Cybersicherheit seit 2018

Mit den getroffenen Beschlüssen verfügt der Bund nun über eine im Vergleich zum Zeitpunkt der Einreichung der Postulate deutlich klarer strukturierte Organisation. Es ist dem Bundesrat aber bewusst, dass weitere Schritte nötig sein werden, um die Organisation die nötige Durchschlagkraft zu verleihen. Die dynamische Entwicklung von Cyberrisiken erfordern eine regelmässige Überprüfung, ob die geschaffenen Strukturen und die vorhandenen Mittel den Herausforderungen angemessen sind. Über die geschaffenen Gremien, insbesondere den Cyberausschuss des Bundesrats und das Kompetenzzentrum Cybersicherheit ist sichergestellt, dass die dazu nötigen Analysen durchgeführt werden.

1.3 Aufbau des Berichts

Der Bericht ist folgendermassen strukturiert:

- Im Kapitel «Gesamtkonzept zum Schutz der Schweiz vor Cyberrisiken» wird die Organisationsstruktur des Bundes beschrieben und erläutert, welche Gremien und Organisationen welche Aufgaben übernehmen und wer gemäss Umsetzungsplan der Strategie für welchen Bereich zuständig ist. Aufgezeigt wir dabei auch, wie der Bund mit den Kantonen, der Wirtschaft und den Hochschulen zusammenarbeitet.
- Im Kapitel «Aufgabenteilung und Schnittstellen zwischen den Bereichen Cybersicherheit, Cyberdefence und Cyberstrafverfolgung» wird speziell auf die Aufgabenteilung zwischen den Departementen eingegangen und aufgezeigt, wie die Zusammenarbeit zwischen zivilen und militärischen Akteuren ausgestaltet wird, wie die Frage der subsidiären Unterstützung geregelt ist und nach welchen Grundsätzen die Bewältigung von Krisen geplant und geübt wird.
- Im Kapitel «Reduktion der Abhängigkeit vom Ausland durch Kompetenzbildung in der Schweiz» werden Massnahmen zur Reduktion der Abhängigkeit vom Ausland durch Kompetenzbildung in der Schweiz beschrieben.

- Im Kapitel «Finanzierung und Personalrekrutierung» wird aufgezeigt, welche Mittel für die Umsetzung der NCS bereitgestellt worden sind.
- Das letzte Kapitel «Die Schweiz im internationalen Vergleich» enthält Informationen zur Organisation und den Strukturen von Cyberfragen in anderen Ländern auf Basis einer ETH Studie und stellt die Ansätze der Schweiz im Bereich Cyberrisiken diesen Strukturen gegenüber.

2 Gesamtkonzept zum Schutz der Schweiz vor Cyberrisiken

Mit der Verabschiedung der NCS 2018–2022, den Entscheiden zur Organisationsstruktur des Bundes und dem Beschluss des Umsetzungsplans liegen seit Frühjahr 2019 alle Elemente des Gesamtkonzepts für den Schutz der Schweiz vor Cyberrisiken vor. Die NCS gibt dabei die strategischen Ziele zum Schutz vor Cyberrisiken über alle Bereiche (Cybersicherheit, Cyberdefence und Cyberstrafverfolgung) vor, mit der Organisationsstruktur des Bundes wurde die grundsätzliche Aufgabenteilung festgelegt und definiert, in welcher Form der Bund mit Kantonen, Wirtschaft und Hochschulen zusammenarbeiten will, und im Umsetzungsplan der NCS werden schliesslich die Zuständigkeiten der einzelnen beteiligten Stellen bestimmt.

2.1 Die strategischen Vorgaben durch die NCS 2018– 2022

Das übergeordnete Ziel der NCS ist, dass die Schweiz bei der Nutzung der Chancen der Digitalisierung angemessen vor Cyberrisiken 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:

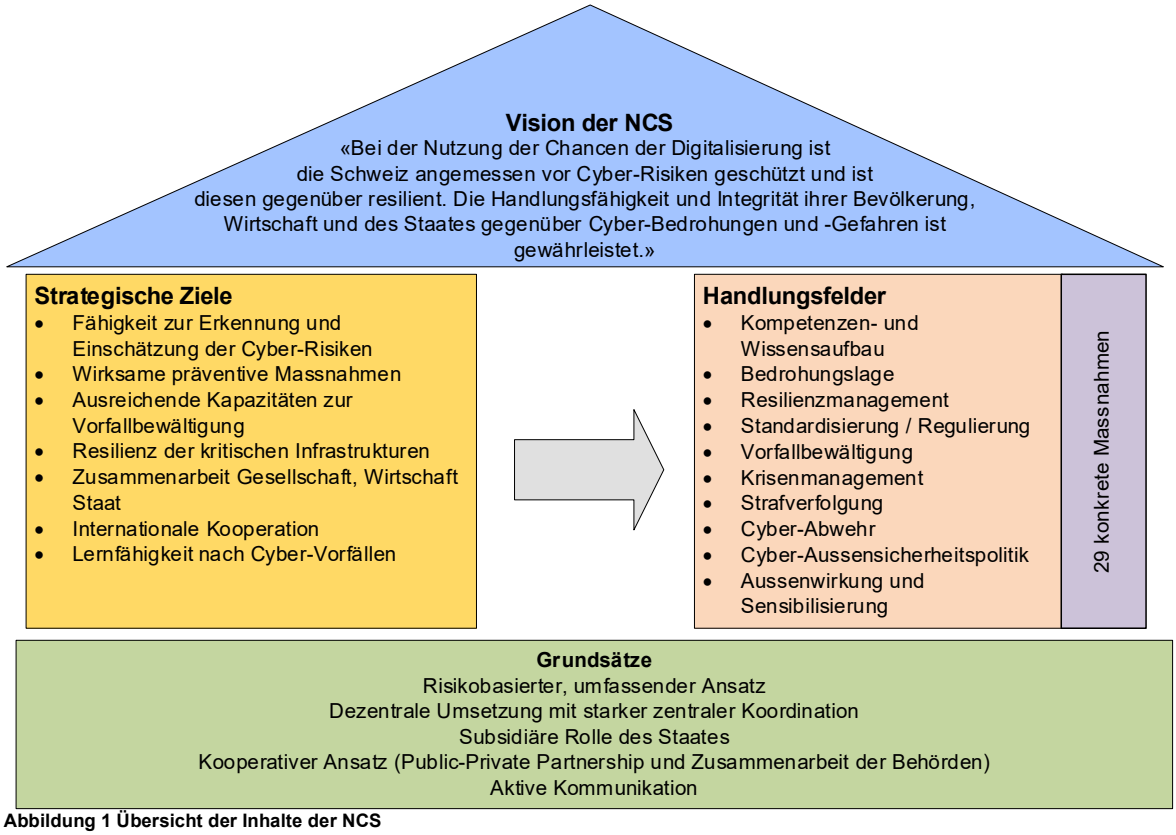

Abbildung 1 Übersicht der Inhalte der NCS

2.2 Organisation zur Umsetzung der NCS

Die NCS beschränkt sich auf die Vorgabe von strategischen Zielen und Massnahmen. Sie enthält keine Bestimmungen zur Organisation. Nach der Verabschiedung der Strategie hat der Bundesrat deshalb die Departemente damit beauftragt, eine Organisationsstruktur zu entwickeln, welche dem Querschnittscharakter der Aufgaben im Bereich Cyberrisiken gerecht wird, gleichzeitig sicherstellt, dass die Umsetzung koordiniert und zentral gesteuert abläuft, und die Zusammenarbeit mit den Kantonen, der Wirtschaft und der Hochschulen begünstigt. Mit den Beschlüssen vom 30. Januar 2019 hat der Bundesrat die Organisationsstruktur festgelegt.

2.2.1 Überdepartementale Organisation des Bundes

Innerhalb der Bundesverwaltung werden in Bezug auf Cyberrisiken drei Bereiche unterschieden:

- Cybersicherheit: Der Bereich Cybersicherheit umfasst die Gesamtheit der Massnahmen, welche die Prävention, die Bewältigung von Vorfällen und die Verbesserung der Resilienz gegenüber Cyberrisiken zum Ziel haben. Der Bund ergreift die nötigen Massnahmen zur Erhöhung der eigenen Cybersicherheit und trägt unter Berücksichtigung des Grundsatzes der Subsidiarität zur Verbesserung der Cybersicherheit der Wirtschaft und Gesellschaft bei, wobei die zentrale Bedeutung der kritischen Infrastrukturen entsprechend gewichtet wird. Zu den Massnahmen zählt auch die Förderung der internationalen Zusammenarbeit im Bereich Cybersicherheit.
- Cyberdefence: Der Bereich Cyberdefence umfasst die Gesamtheit der zivilen nachrichtendienstlichen und militärischen Massnahmen, die der Verteidigung kritischer Systeme, der Abwehr von Angriffen im Cyberraum, 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.
- Strafverfolgung von Cyberkriminalität: Der Bereich Strafverfolgung von Cyberkriminalität umfasst alle Massnahmen der Polizei und der Staatsanwaltschaft von Bund und Kantonen im Kampf gegen die Cyberkriminalität.

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

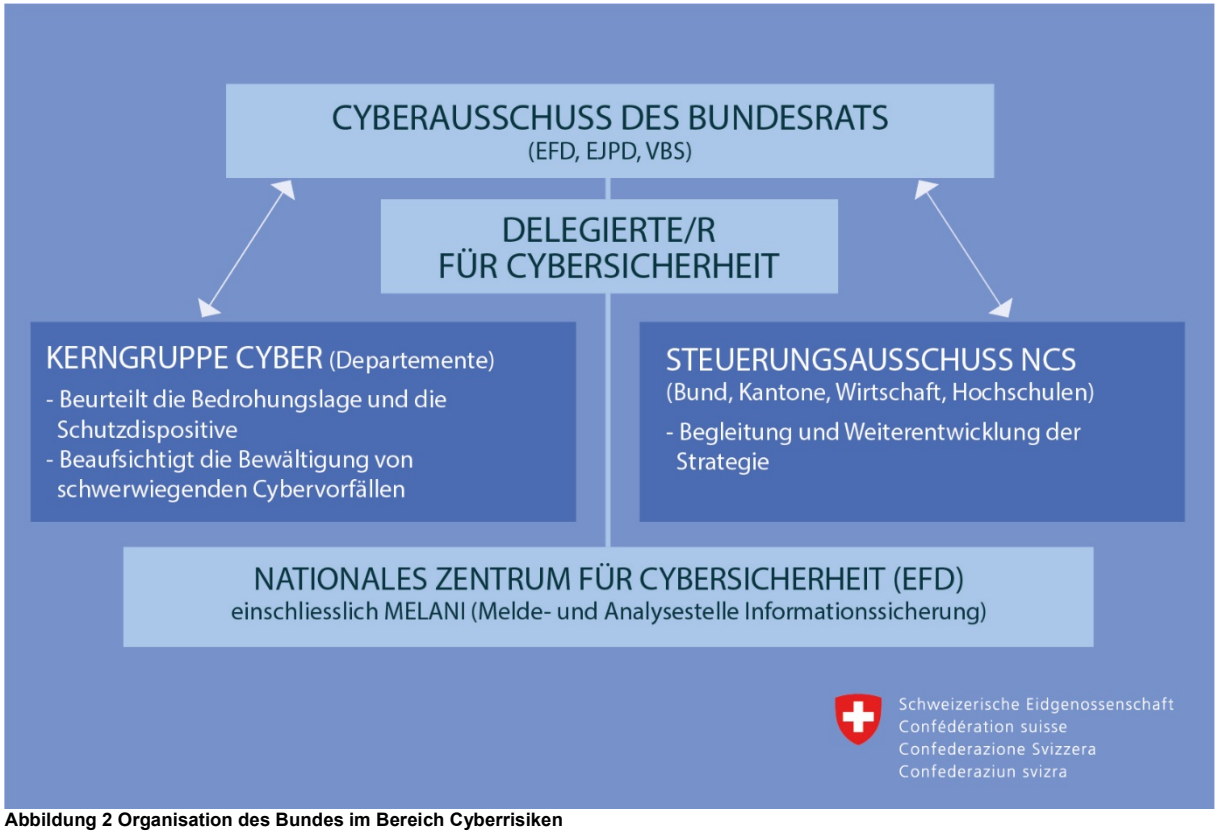

Abbildung 2 Organisation des Bundes im Bereich Cyberrisiken

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

- Der **Cyberausschuss des Bundesrats (CyA),** 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.
- Die/der **Delegierte/r des Bundes für Cybersicherheit** übernimmt die strategische Leitung der Cybersicherheit im Bund, leitet die vom Bund eingesetzten überdepartementalen Gremien (mit Ausnahmen des Cyberausschusses) und vertritt den Bund in weiteren Gremien.
- Die **Kerngruppe Cyber (KG-Cy)** 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.

2.2.2 Kompetenzzentrum Cybersicherheit

Das Kompetenzzentrum unter der Leitung des/der Delegierten des Bundes für Cybersicherheit übernimmt folgende vier Aufgaben: die strategische Leitung der Cybersicherheit des Bundes, den Betrieb der nationalen Anlaufstelle, die Fachstelle für Informations- und IKT-Sicherheit des Bundes und den Kompetenzpool Cybersicherheit. Die konkreten Aufgaben in diesen vier Bereichen sind in Abbildung 2 beschrieben. Es arbeitet zur Wahrnehmung dieser Aufgaben mit allen relevanten Stellen in der Schweiz zusammen und tauscht sich mit ähnlichen Stellen (nationale Zentren für Cybersicherheit) sowie internationalen Fachorganisationen aus.

Auch die Organisation des Kompetenzzentrums muss den Forderungen nach einer stärkeren Zentralisierung Rechnung tragen und gleichzeitig wo immer möglich auf bereits bestehende

Kompetenzen und Fähigkeiten zurückgreifen. Mit folgenden drei Massnahmen soll diesen Anforderungen begegnet werden:

1. Im Kompetenzzentrum soll die Geschäftsstelle und die nationale Anlaufstelle das nötige Gewicht erhalten, damit das Kompetenzzentrum über eine aktive Kommunikation und einer ausgebauten Dienstleistung für Unternehmen und Bevölkerung gegen aussen starke Wirkung entfalten kann und wirklich als zentrale Anlaufstelle wahrgenommen wird.
2. Innerhalb des Kompetenzzentrums soll ein Expertenpool geschaffen werden, der die zuständigen Ämter bei der Umsetzung von Massnahmen im Bereich Cybersicherheit unterstützt. Er soll insbesondere den Fachämtern in den Sektoren zur Verfügung stehen und so dazu beitragen, dass das sektorspezifische Wissen und die rechtlichen Kompetenzen bei Bedarf und projektbezogen mit Cyberfachwissen ergänzt werden.
3. Das Kompetenzzentrum soll schliesslich eng mit denjenigen Stellen zusammenarbeiten, welche über Fachwissen und Kapazitäten für bestimmte Aufgaben im Bereich Cybersicherheit verfügen. Über die Zusammenarbeit soll verhindert werden, dass mit dem Kompetenzzentrum bereits anderswo bestehende Fähigkeiten verdoppelt werden, es soll aber auch sichergestellt werden, dass die beteiligten Stellen ihr Aufgaben koordiniert und in enger Abstimmung mit dem Kompetenzzentrum wahrnehmen.

Aufgrund dieser Überlegungen schlägt das EFD folgende Organisation des Kompetenzzentrums vor (s. Abbildung 2):

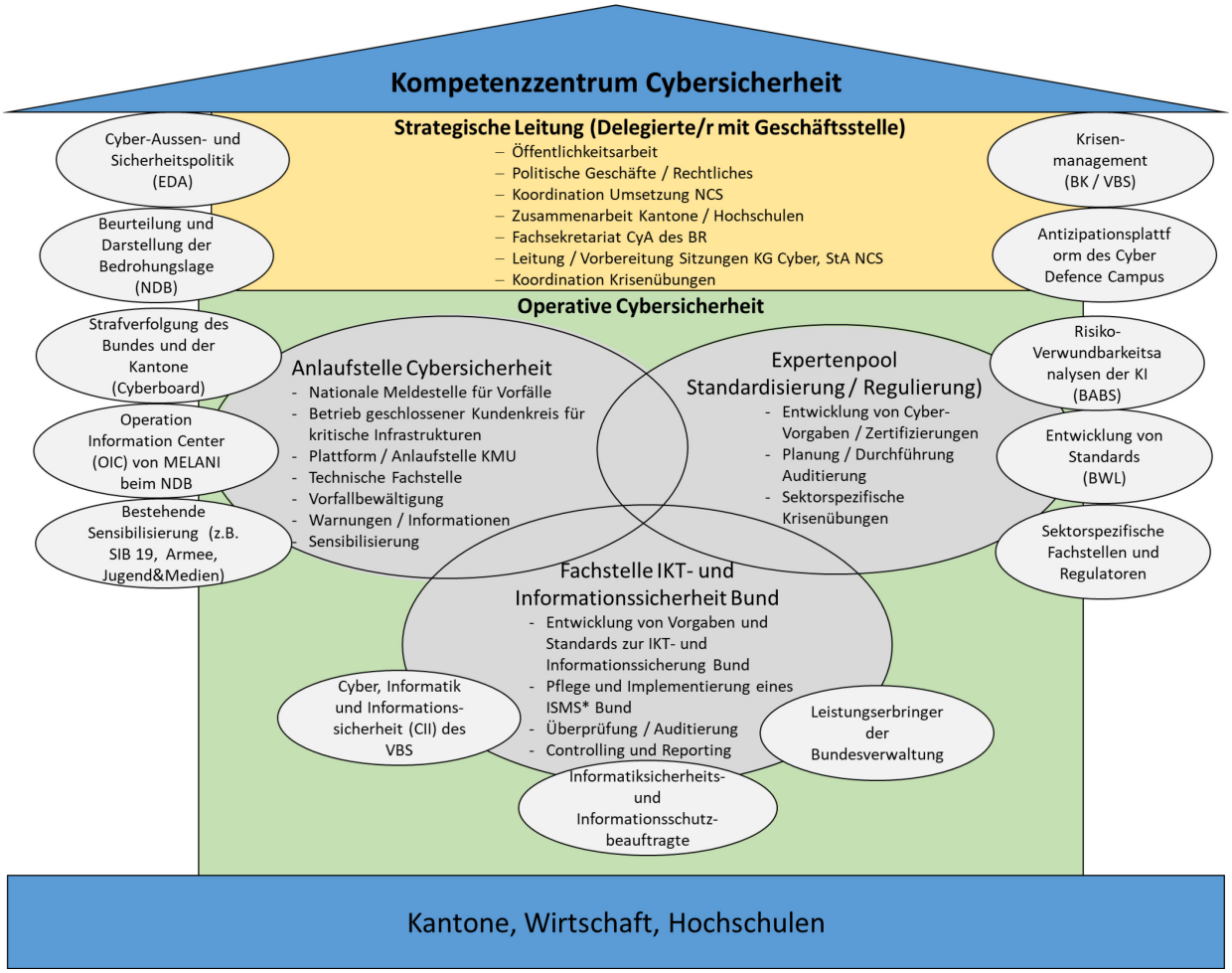

Abbildung 3 Organisation und Aufgaben des Kompetenzzentrums Cybersicherheit, Schnittstellen zu Partnerorganisationen in der Bundesverwaltung

2.2.3 Zusammenarbeit zwischen Bund, Kantonen, Wirtschaft und Hochschulen

Die Zusammenarbeit zwischen Bund, Kantonen, Wirtschaft und Hochschulen muss auf allen Stufen sichergestellt sein. Konkret soll sie über folgende Gremien und Mechanismen stattfinden:

- Die **Zusammenarbeit auf politisch-strategischer Stufe über eine Vertretung der Kantone im Cyberausschuss des Bundesrats**: 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 Cyberausschuss 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) aus.
- **Gemeinsames Projektmanagement durch den Steuerungsausschuss NCS**: 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.
- **Gemeinsame Umsetzung von NCS-Massnahmen:** Die Kooperation bei der Umsetzung von Massnahmen durch die jeweils operativ tätigen Einheiten ist die direkteste Form der Zusammenarbeit. Sie orientiert sich an den im Umsetzungsplan der NCS festgehaltenen Zuständigkeiten und Beteiligungen, kann jedoch flexibel angepasst und ausgeweitet werden.

Zentrale Anlaufstelle des Bundes für alle im Bereich Cyberrisiken engagierten Stellen ist das Kompetenzzentrum Cybersicherheit unter der strategischen Leitung der/des Delegierten des Bundes für Cybersicherheit.

3 Aufgabenteilung und Schnittstellen zwischen den Bereichen Cybersicherheit, Cyberdefence und Cyberstrafverfolgung

Mit der durch die NCS vorgegebenen Unterscheidung zwischen den Bereichen Cybersicherheit, Cyberdefence und Cyberstrafverfolgung wird die Differenzierung zwischen den verschiedenen Aufgabengebieten deutlicher. Die konkreten Zuständigkeiten für die Umsetzung der Massnahmen der NCS sind im Umsetzungsplan definiert.
Separat werden in diesem Kapitel die Organisation im Krisenmanagement und die subsidiäre Unterstützung der zivilen Behörden durch die Armee beschrieben.

3.1 Aufgabenzuteilung durch den Umsetzungsplan

Mit dem Umsetzungsplan der NCS 2018–2022 werden die Aufgaben und die Zuständigkeiten der beteiligten Organisationseinheiten der Bundesverwaltung definiert und ergänzend dazu ausgewiesen, welche Projekte von Dritten (Kantone, Wirtschaft, Hochschulen) im Rahmen der NCS ausgeführt werden. Basierend auf dem Umsetzungsplan und den darin festgehaltenen Vorhaben lässt sich die Aufgabenverteilung in der Bundesverwaltung wie folgt darstellen:

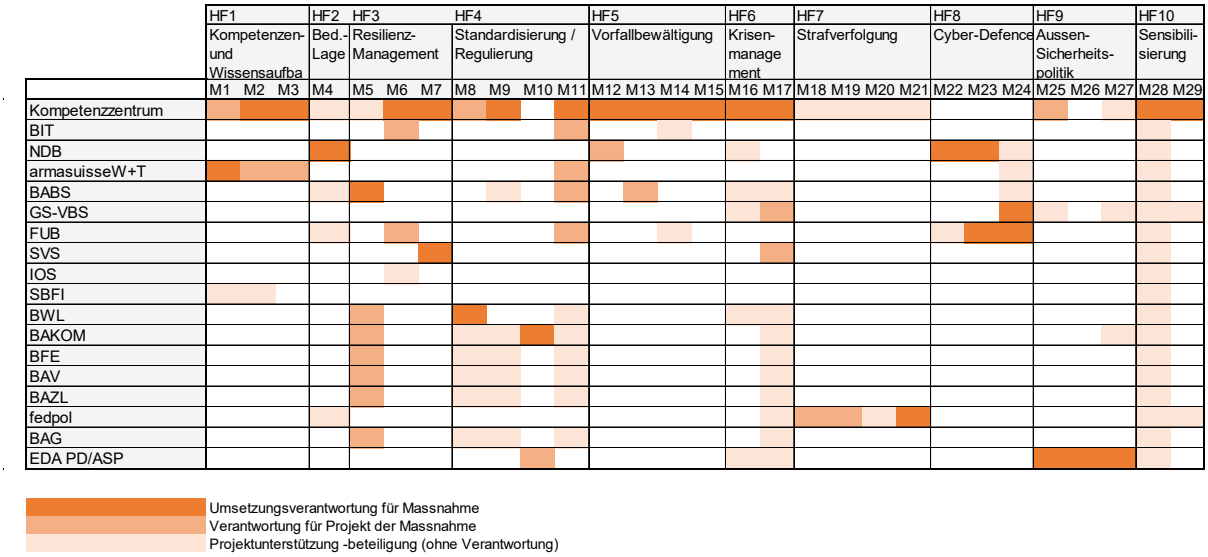

Abbildung 4 Aufgabenverteilung Umsetzung NCS gemäss Entwurf Umsetzungsplan

Es wird ersichtlich, dass das Kompetenzzentrum Cybersicherheit bei allen Handlungsfeldern in die Umsetzung einbezogen ist und in sechs der zehn Handlungsfeldern mindestens bei einer Massnahme federführend ist. Es wird aber auch deutlich, dass nach wie vor auf die Kompetenzen und Kapazitäten der in den verschiedenen Handlungsfeldern tätigen Verwaltungseinheiten zurückgegriffen wird. Der Umsetzungsplan hält so die Balance zwischen der von Parlament und Wirtschaft geforderten Zentralisierung und der Nutzung der in der Bundesverwaltung dezentral bereits vorhandenen Fähigkeiten, Kapazitäten und rechtlichen Kompetenzen.

3.2 Krisenmanagement

Cybervorfälle können gravierende Konsequenzen haben und soweit eskalieren, dass ein Krisenmanagement auf nationaler Ebene nötig wird. Zentral für das Krisenmanagement sind die Führungsabläufe und -prozesse der Entscheidungsträger. Diese sind in den «Weisungen über das Krisenmanagement in der Bundesverwaltung» vom 21. Juni 2019 festgehalten.[2] Sie gelten szenario-unabhängig, d. h. sie kommen auch bei durch Cybervorfälle ausgelösten Krisen zur Anwendung. Bewusst wird in den Vorgaben zum Krisenmanagement darauf verzichtet, Zuständigkeiten a priori festzulegen. Es obliegt dem Bundesrat, als oberstes Führungsorgan, festzulegen, welchen Stäben die Federführung bei der Bewältigung der Krise übertragen wird. Je nach Ausprägung der Krise und dem Kreis der Betroffenen wird er dabei auf bestehende (interdepartementale) Stäbe z.B. Bundestab Bevölkerungsschutz BSTB, EO fedpol/SOGE) zurückgreifen. Diese Flexibilität ist unabdingbar, weil nur so sichergestellt ist, dass die Verantwortung für die Bewältigung der Krise der jeweils kompetentesten Stelle zugewiesen werden kann.
Besonders wichtig ist bei Krisen, welche durch Cybervorfälle ausgelöst werden, ein einheitliches und umfassendes Lagebild, als Basis für die Entscheidungsfindung. Dafür zuständig sind die Fachstellen im Nachrichtendienst des Bundes und das technische Analyseteam im Kompetenzzentrum Cybersicherheit. Dieses unterstützt in Zusammenarbeit mit Experten weiterer Stellen im Krisenfall die Stäbe durch fachspezifisches Wissen.

3.3 Subsidiäre Unterstützung der zivilen Behörden durch die Armee

Das Militärgesetz regelt in den Artikeln 1 und 68-75 die Voraussetzungen für die Unterstützung von zivilen Behörden durch die Armee. Ein solcher Einsatz ist zur Abwehr schwerwiegender Bedrohungen der inneren Sicherheit und bei der Bewältigung anderer ausserordentlicher Lagen möglich, wenn die Mittel der zivilen Behörden nicht mehr ausreichen. Er erfolgt auf Gesuch der zivilen Behörden und wird vom Bundesrat bewilligt.
Mit dem Aufbau der Cyberkapazitäten und -Fähigkeiten der Armee werden subsidiäre Einsätze der Armee im Bereich Cybersicherheit möglich. Mit Massnahme 24 der NCS wir die Armee beauftragt, ihre Kader und Armeeangehörige entsprechend auszubilden und zusammen mit den zivilen Behörden aus Bund und Kantonen zu definieren, unter welchen Rahmenbedingungen sie subsidiäre Unterstützung bei Cybervorfällen leistet, welche Aufgaben sie dabei übernehmen kann und wie ein solcher Einsatz konkret ausgelöst wird.

4 Reduktion der Abhängigkeit vom Ausland durch Kompetenzbildung in der Schweiz

Die Abhängigkeit von ausländischen Herstellern von Hard- und Software und von Dienstleistern lässt sich mit wirtschaftlich tragbaren und technisch umsetzbaren Massnehmen nicht vollständig eliminieren. Wichtig ist aber, dass die Abhängigkeiten erkannt, die sich daraus ergebenden Risiken sorgfältig analysiert und Massnahmen zur deren Reduktion ergriffen werden.
Zu diesem Zweck braucht es gezielte Massnahmen zum Aufbau von Wissen und Kompetenzen in der Schweiz. Die NCS definiert diese im Handlungsfeld «Wissens- und Kompetenzenaufbau». In dieses Handlungsfeld gehört auch die Massnahme 3 der NCS, welche die Schaffung von günstigen Rahmenbedingungen für eine innovative IKT-Sicherheitswirtschaft in der Schweiz zum Ziel hat. Realisiert soll diese Massnahme mit folgenden Projekten:

[2] https://www.admin.ch/opc/de/federal-gazette/2019/4593.pdf

- **Aufbau eines «Ökosystems Cybersicherheit»:** Das Kompetenzzentrum Cybersicherheit etabliert sich als Vermittlungsstelle zwischen Wirtschaft, Hochschulen, Behörden und bestehenden Innovationszentren mit dem Ziel, ein innovatives Ökosystem für Cybersicherheit 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.
- **Fördermittel:** Es werden Fördermittel für Innovationsprojekte von Hochschulen, Verbände und Unternehmen im Bereich Cybersicherheit identifiziert und ausgewiesen. Es wird geprüft, über welche Förderinstrumente (z.B. nationale thematische Netzwerke, F&E Innovationsprojekte; eigenes Förderprogramm) die Innovation im Bereich Cybersicherheit am effektivsten gefördert werden kann.
- **Aufbau von Innovationszentren:** Es wird geprüft, wie rund um das Kompetenzzentrum Cybersicherheit ein Cyberhub (inklusive des Forschungszentrums der ETH, Einbezug Ökosystem Cybersicherheit und Campus Cyber Defence sowie Forschungsnetzwerk) aufgebaut werden kann. Als Teil des Netzwerks wird Innovation im Bereich Cybersicherheit an bestehenden oder neu geschaffenen regionalen Innovationszentren gezielt gefördert.

Zur Umsetzung dieser Projekte arbeitet der Bund eng mit den Hochschulen, der Wirtschaft und den Kantonen zusammen.

5 Finanzierung und Personalrekrutierung

Für die Umsetzung der beschlossenen Massnahmen werden so weit wie möglich bestehende Strukturen und Ressourcen (finanzieller und personeller Art) genutzt. Weil die NCS 2018–2022 jedoch in vielen Bereichen das Aufgabenspektrum der bestehenden Verwaltungseinheiten erweitert, sind zusätzliche Ressourcen nötig. Dies betrifft insbesondere das Kompetenzzentrum Cybersicherheit, welches zwar die bestehenden Ressourcen von MELANI nutzen wird, mit der Unterstützung der Bevölkerung und der KMU beim Schutz vor Cyberrisiken jedoch ein deutlich erweitertes Aufgabenspektrum erhält.

Die 2013 für die Arbeiten der ersten NCS geschaffenen und 2017 unbefristet verlängerten 30 Stellen genügen nicht, um die im Umsetzungsplan der NCS 2018–2022 beschriebenen neuen und intensivierten Aufgaben wahrzunehmen. Auf der Basis des Umsetzungsplans haben die beteiligten Bundesstellen einen Mehrbedarf von insgesamt 67 Stellen ausgewiesen. Dieser Bedarf soll bis im zweiten Quartal 2020 vertieft geprüft und wo möglich reduziert werden. Es ist zu untersuchen, wo verstärkt auf bestehende Ressourcen zurückgegriffen werden kann und welche Synergien genutzt werden können.

Prioritäre Massnahmen müssen jedoch unverzüglich umgesetzt werden können. Der Bundesrat hat deshalb am 15. Mai 2019 insgesamt 24 zusätzliche Stellen für die Umsetzung der NCS gesprochen. Zusätzlich zu den personellen Ressourcen wurden ebenfalls die finanziellen Mittel erhöht. Dem Kompetenzzentrum Cybersicherheit steht zusätzlich zu den bestehenden finanziellen Mitteln jährlich ein Million Franken für die Umsetzung der NCS sowie für den Aufbau und Betrieb des Kompetenzzentrums Cybersicherheit zur Verfügung. Anfang August hat der Delegierte des Bundes für Cyber-Sicherheit seine Funktion aufgenommen.

Mit der schrittweisen Aufstockung der Ressourcen entschärfen sich die Schwierigkeiten bei der Rekrutierung der Fachkräfte. Sie ermöglicht eine laufende Prüfung des ausgewiesenen Ressourcenbedarfs ohne dass dabei dringend benötigte Arbeiten verzögert werden.

6 Die Schweiz im internationalen Vergleich

Vergleich zwischen verschiedenen Staaten in Bezug auf die zivile und militärische Cybersicherheit können zwar aufschlussreich sein, sie müssen jedoch mit der nötigen Sorgfalt vorgenommen werden. Jedes Land gestaltet seine Dispositive so aus, dass sie zu seinem jeweiligen politischen System passen. Es bestehen beispielsweise grosse Unterschiede hinsichtlich der Zuständigkeiten der verschiedenen Staatsebenen und je nach strategischer Kultur und Staatsverständnis wird die Frage, welche Aufgaben der Staat beim Schutz vor Cyberrisiken übernehmen soll, unterschiedlich beantwortet. Solche grundsätzlichen Unterschiede sind bei Vergleichen zu berücksichtigen. Erschwerend kommt im Bereich der Cybersicherheit dazu, dass Regierungen kaum gewillt sind, Angaben über die finanziellen und personellen Ressourcen im Bereich der Cybersicherheit zu machen.
Um dennoch den schweizerischen Ansatz in einen breiteren internationalen Kontext zu stellen, hat das EFD das Center for Security Studies der ETH Zürich damit beauftragt, die Schweiz mit Deutschland, Finnland, Frankreich, Israel, Italien und den Niederlanden zu vergleichen. Die Studie zeigt auf, dass viele Länder ähnliche Strukturen im Bereich Cybersicherheit aufweisen wie die Schweiz und in vielen Ländern der Aufbau dieser Strukturen nach wie vor nicht abgeschlossen ist. Die Herausforderungen im Zusammenhang mit Cyberrisiken sowie die Herangehensweise an diese weichen nicht wesentlich von deren der Schweiz ab. In keinem der untersuchten Länder ist eine einzelne Organisation für alle Arbeiten in Bezug zu Cyberrisiken zuständig. Überall ist eine mehr oder weniger stark ausdifferenzierte Aufgabenteilung zwischen Verteidigung, ziviler Sicherheit und Strafverfolgung feststellbar. In keinem der untersuchten Staaten wird der Lead für den Schutz vor Cyberrisiken dem Militär übertragen.