Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Generalsekretariat EFD
Rechtsdienst EFD

11. Dezember 2020

Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen
Rechtliche Grundlagen

Inhaltsverzeichnis

1 Ausgangslage

Der Bundesrat hat bei der Beantwortung des Po.17.3475 «Meldepflicht bei schwerwiegenden Sicherheitsvorfällen bei kritischen Infrastrukturen» beschlossen, bis Ende 2020 die Einführung einer Meldepflicht für Sicherheitsvorfälle zu prüfen[1].

Gemäss Postulatsbericht sind die bereits bestehenden sektoriellen Meldestellen geeignet, um Meldungen von schwerwiegenden Sicherheitsvorfällen entgegenzunehmen. Für Cybervorfälle bestehen demgegenüber noch keine Meldepflichten; allfällige Vorfälle können aber der Melde- und Analysestelle zur Informationssicherung (MELANI)[2] sowie den sektoriellen Cybermeldestellen (Sektoren-CERTs) freiwillig gemeldet werden[3]. Basierend auf einer Auftragsstudie[4] werden im Postulatsbericht drei Varianten[5] für einen Ausbau der bestehenden Meldestellen bzw. -pflichten beschrieben:

- Zentrale Meldestelle: Es wird eine zentrale, sektorübergreifende Meldestelle für alle Sicherheitsvorfälle von kritischen Infrastrukturen geschaffen.
- Dezentrale Meldestellen: Die bestehenden dezentral aufgestellten Meldestellen in den verschiedenen Sektoren werden gestärkt und die Meldepflichten ihnen gegenüber ausgebaut (insbesondere in Bezug auf Cybervorfälle). In Sektoren, wo keine Meldestellen vorhanden sind, werden solche aufgebaut.
- Ergänzung der dezentralen Meldestellen durch eine zentrale Meldestelle für Cybervorfälle: Diese Variante sieht eine gemischte Form von Meldestellen vor. Primärer Ansprechpartner für Sicherheitsvorfälle ist die sektorspezifische Meldestelle. Für die Aufarbeitung aller Cybervorfälle wird eine übergreifende, zentrale Meldestelle festgelegt. Dabei ist noch zu klären, ob die Meldung direkt an die zentrale Meldestelle für Cybervorfälle oder über eine sektorspezifische Cybermeldestelle (Sektor-CERT) erfolgen soll.

2 Auftrag

Bis im Herbst 2020 soll der Rechtsdienst GS EFD in Zusammenarbeit mit dem BJ und dem NCSC abklären, welche rechtlichen Folgen die drei Varianten hätten. Konkret ist zu prüfen, welcher Anpassungsbedarf an den bestehenden rechtlichen Normen bei den einzelnen Varianten nötig wäre und wie diese Anpassungen umgesetzt werden könnten. Für diese Rechtsabklärung hat der NCSC dem GS EFD einen Fragenkatalog unterbreitet, dessen Beantwortung am Schluss erfolgt (siehe 3.4).

[1] Varianten für Meldepflichten von kritischen Infrastrukturen bei schwerwiegenden Sicherheitsvorfällen, Bericht des Bundesrates vom 13. Dezember 2019 in Erfüllung des Postulates 17.3475 Graf-Litscher vom 15.06.17 (Postulatsbericht), S. 15.
[2] MELANI wurde per 1. Juli 2020 in das nationale Zentrum für Cybersicherheit (NCSC) integriert.
[3] Postulatsbericht S. 6, 9 f.
[4] Prüfung einer Meldepflicht bei Sicherheitsvorfällen, Studie von PwC Schweiz im Auftrag des Informatiksteuerungsorgans des Bundes (ISB) vom Oktober 2019 (PwC-Studie).
[5] Zum besseren Verständnis wird vorliegend durchgehend von „Varianten“ (wie im Postulatsbericht) und nicht „Modellen“ (wie in der PwC-Studie) gesprochen.

3 Rechtsabklärung

3.1 Begriffliches

Als **kritische Infrastrukturen (KI)** werden Prozesse, Systeme und Einrichtungen bezeichnet, die essenziell für das Funktionieren der Wirtschaft bzw. das Wohlergehen der Bevölkerung sind[6]. Das Spektrum der kritischen Infrastrukturen (KI) umfasst neun Sektoren, unterteilt in 27 Teilsektoren (Branchen) und Einzelobjekte[7]. Dabei gelten sämtliche Elemente (Betreiberfirmen, IT-Systeme, Anlagen, Bauten usw.) als Teil der KI, die Leistungen in einem der Teilsektoren erbringen[8].

Behörden	Forschung und Lehre Kulturgüter Parlament, Regierung, Justiz, Verwaltung
Energie	Erdgasversorgung Erdölversorgung Stromversorgung Fern- und Prozesswärme
Entsorgung	Abfälle Abwasser
Finanzen	Finanzdienstleistungen Versicherungsdienstleistungen
Gesundheit	Medizinische Versorgung Labordienstleistungen Chemie und Heilmittel
Information und Kommunikation	IT-Dienstleistungen Telekommunikation Medien Postdienste
Nahrung	Lebensmittelversorgung Wasserversorgung
Öffentliche Sicherheit	Armee Blaulichtorganisationen (Polizei, Feuerwehr, Sanität) Zivilschutz
Verkehr	Luftverkehr Schienenverkehr Schiffsverkehr Strassenverkehr

[6] siehe Definition in der Nationalen Strategie zum Schutz kritischer Infrastrukturen 2018-2022 vom 8. Dezember 2017 (Strategie SKI) BBl 2018 511 sowie seit 1. Juli 2020 auch in Art. 3 lit. g Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung vom 27. Mai 2020 (Cyberrisikenverordnung, CyRV; SR 120.73).

[7] Im Hintergrundbericht vom 8. Dezember 2017 und im Leitfaden vom 17. Dezember 2018 zur Strategie SKI sowie in der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken 2018-2022 vom April 2018 (NCS) werden 28 Teilsektoren (und nicht 27 Teilsektoren wie in der Strategie SKI) erwähnt; die Auflistung ist aber in allen drei Dokumenten identisch und umfasst 27 Teilsektoren.

[8] Innerhalb der Teilsektoren wird nicht mehr zwischen kritischen oder nicht kritischen Infrastrukturen unterschieden. Deshalb sind im Teilsektor Stromversorgung beispielsweise grundsätzlich sämtliche rund 900 Elektrizitätsversorgungsunternehmen als KI-Betreibende zu betrachten (Leitfaden SKI S. 6).

Das Bundesamt für Bevölkerungsschutz betreibt ein Informationssystem zur Inventarisierung der Objekte, die kantonal und national als kritische Infrastrukturen gelten. Es handelt sich zum einen um Objekte, die eine zentrale Bedeutung bei der Versorgung mit wichtigen Gütern und Dienstleistungen (und damit eine hohe Kritikalität[9]) haben und zum andern um Objekte, von denen ein erhebliches Gefahrenpotenzial ausgeht. Das sog. SKI-Inventar ist als geheim klassifiziert; Berechtige (z. B. einzelne Kantone oder einzelne Teilsektoren) erhalten auf Anfrage Auszüge aus einzelnen Bereichen, die jedoch nur einen Teil der Informationen enthalten und als vertraulich klassifiziert sind[10].

Der **Schutz kritischer Infrastrukturen (SKI)** ist deshalb wichtig, weil erhebliche Störungen der Energieversorgung, der Verkehrssysteme, des Gesundheitswesens oder der öffentlichen Sicherheit schwerwiegende gesellschaftliche und volkswirtschaftliche Schäden verursachen können. Die Schutzmassnahmen für KI haben zum Ziel, die Eintrittswahrscheinlichkeit und/oder das Schadensausmass einer Störung zu reduzieren beziehungsweise die Ausfallzeit zu minimieren[11]. Zur Verbesserung der Resilienz[12] soll deshalb die Schaffung von Rechtsgrundlagen für eine Meldepflicht für schwerwiegende Sicherheitsvorfälle geprüft werden[13].

Der Begriff «**Sicherheitsvorfall**» wird in der Strategie zum Schutz kritischer Infrastrukturen nicht definiert[14]; es wird auch in keinem Erlass der systematischen Rechtssammlung des Bundes (SR) umschrieben, was unter einem Sicherheitsvorfall bei einer kritischen Infrastruktur zu verstehen ist[15]. Der Postulatsbericht weist darauf hin, dass es schwierig sei, zu beurteilen, welche Ereignisse als schwerwiegende Sicherheitsvorfälle zu bezeichnen sind und welche nicht[16]. Aus der Zielsetzung der Strategie SKI lässt sich ableiten, dass ein schwerwiegender Sicherheitsvorfall sicher dann vorliegt, wenn wichtige Güter und Dienstleistungen einer kritischen Infrastruktur nicht mehr wie gewohnt verfügbar sind und dadurch das Wohlergehen der Bevölkerung sowie das Funktionieren von Wirtschaft und Staat in schwerwiegendem Masse beeinträchtigt ist[17]. Mit anderen Worten definiert sich ein schwerwiegender Sicherheitsvorfall nicht über die Natur des Vorfalls, sondern über sein Schadenspotential. Die zu prüfende Meldepflicht bezieht sich somit nur auf Sicherheitsvorfälle, die als schwerwiegend gelten, weshalb nachfolgend der Einfachheit halber nur von «Sicherheitsvorfällen» gesprochen wird.
Ein Sicherheitsvorfall in einer kritischen Infrastruktur kann vom Ausmass her ein «*bevölkerungsschutzrelevantes Ereignis von nationaler Tragweite*» sein - oder sich dazu entwickeln. Als solches gelten natur-, technik- und gesellschaftsbedingte Katastrophen und Notlagen, die

[9] Die Kritikalität ist ein relatives Mass für die Bedeutung, die ein Ausfall der KI für die Bevölkerung und deren Lebensgrundlagen hat. Sie ist abhängig von der jeweiligen Betrachtungsebene: So gibt es KI, die auf lokaler oder kommunaler Ebene eine grosse Kritikalität haben (z. B. eine Trafo-Station im Strom-Verteilnetz), andere haben dagegen aus nationaler oder sogar internationaler Perspektive eine grosse Kritikalität (z. B. zentrale Steuerungssysteme im Übertragungsnetz) (Strategie SKI BBl 2018 512).
[10] Im Hintergrundbericht vom 8. Dezember 2017 zur Strategie SKI wird bemängelt, dass das BABS für die Führung des SKI-Inventars über keine ausreichende Rechtsgrundlage verfüge und deshalb die Zusammenarbeit mit den Betreibern der entsprechenden Objekte und die Meldung von Angaben zu diesen Objekten – mit teils sensitiven Informationen - auf freiwilliger Basis erfolge.
[11] Als Massnahme zum Schutz von kritischen Infrastrukturen gilt insbesondere die Informationssicherung (Art. 3 Abs. 11 der Verordnung vom 9. Dezember 2011über die Informatik und Telekommunikation in der Bundesverwaltung, [Bundesinformatikverordnung, BinfV; SR 172.010.58).
[12] Fähigkeit eines Systems, einer Organisation oder einer Gesellschaft, intern oder extern verursachten Störungen zu widerstehen und das ordnungsgemässe Funktionieren zu erhalten oder dieses möglichst rasch und vollständig wiederzuerlangen, vgl. Art. 3 lit. d CyRV.
[13] Strategie SKI BBl 2018 508, 524, Massnahme 8.
[14] Auch der Leitfaden und Hintergrundbericht zur Strategie SKI definieren nicht, was unter einem (schwerwiegenden) Sicherheitsvorfall zu verstehen ist. Die PwC-Studie weist auf das Fehlen einer Definition in der Strategie SKI hin. Die von der PwC-Studie angeführte Definition für Sicherheitsvorfall bezieht sich, wie es scheint, vor allem auf Cybervorfälle: „Ein Sicherheitsvorfall bezeichnet einen nicht autorisierten Zugriff oder Zugriffsversuch auf ein System und deutet darauf hin, dass Massnahmen und deren Schutz fehlgeschlagen sind. Es wird zwischen einem „passiven Angriff (unautorisierte Informationsgewinnung, Verlust der Vertraulichkeit) und einem aktiven Angriff (unautorisierte Modifikation von Daten, Verlust der Integrität oder Verfügbarkeit)“ unterschieden. Grundsätzlich spricht man von einem Vorfall, wenn der normale Betrieb gestört wird“ (S. 5, 29, 67).
[15] Der Entwurf zum Informationssicherheitsgesetz spricht von Informationssicherheitsvorfällen (Botschaft ISG BBl 2017 3020); Art. 14 Abs. 4 CyRV statuiert die bundesverwaltungsinterne Pflicht für den Leistungserbringer, entdeckte Sicherheitsvorfälle den Leistungserbringern zu melden.
[16] Postulatsbericht S. 7.
[17] Strategie SKI BBl 2018 504, 508, 527; Leitfaden zur Strategie SKI S. 39.

einen grossen Teil der Bevölkerung oder deren Lebensgrundlagen betreffen oder gefährden. Sie können einen oder mehrere Kantone, die ganze Schweiz oder das Ausland betreffen[18]. Ein Angriff auf eine kritische Infrastruktur – der vermutungsweise ebenfalls einen Sicherheitsvorfall darstellt - ist eine *konkrete Bedrohung der inneren oder äusseren Sicherheit*, wenn ein bedeutendes Rechtsgut wie Leib und Leben oder die Freiheit von Personen oder der Bestand und das Funktionieren des Staates betroffen ist[19].

Im Fokus der möglichen Sicherheitsvorfälle, die bei kritischen Infrastrukturen auftreten können, steht aufgrund der technologischen Entwicklung insbesondere der **Cybervorfall**[20]. Dieser wird definiert als ein unbeabsichtigtes oder von Unbefugten beabsichtigtes Ereignis, das dazu führt, dass die Vertraulichkeit, Integrität, Verfügbarkeit oder Nachvollziehbarkeit von Daten beeinträchtigt ist oder es zu Funktionsstörungen kommen kann[21]. Ein Cybervorfall betrifft Informations- und Kommunikationsinfrastrukturen (Hard- und Software), die untereinander Daten austauschen, diese erfassen, speichern, verarbeiten oder in (physische) Aktionen umwandeln, und die dadurch ermöglichten Interaktionen zwischen Personen, Organisationen und Staaten[22]. Hinter Cybervorfällen stehen häufig kriminelle Absichten; solche Cybervorfälle werden als **Cyberangriffe** bezeichnet. Sie werden je nach Zweck des Angriffs, der Akteure und dem Kreis der Betroffenen in fünf Kategorien eingeteilt: Cyber-Kriminalität (Bedrohung mit höchster Eintrittswahrscheinlichkeit), Cyber-Spionage, Cyber-Sabotage und –Terrorismus, Desinformation und Propaganda, Cyberangriffe als Mittel und Unterstützung der Kriegführung oder für politisch-militärische Zwecke unterhalb der Kriegsschwelle. Cybervorfälle können auch durch **menschliches Fehlverhalten** und **technische Ausfälle** verursacht werden[23]. Ausgehend von diesen Bedrohungen wird Cyber-Sicherheit umschrieben als anzustrebender Zustand innerhalb des Cyber-Raums, bei dem die Kommunikation und der Datenaustausch zwischen Informations- und Kommunikationsinfrastrukturen wie ursprünglich beabsichtigt funktionieren[24].
Wenn ein Cybervorfall bei einer kritischen Infrastruktur auftritt und schwerwiegende Auswirkungen auf die Güter- und Dienstleistungsversorgung zeitigt, wird er in aller Regel als Sicherheitsvorfall meldepflichtig. Ein Cybervorfall kann mithin Ursprung und Auslöser eines Sicherheitsvorfalls sein[25]. Es ist aber auch denkbar, dass ein Cybervorfall durch die Folgen eines Sicherheitsvorfalles begünstigt oder ermöglicht wird.
Im Gegensatz zu einem Sicherheitsvorfall, der sich primär am Schadenspotential seiner Auswirkungen orientiert, wird ein Cybervorfall über die Natur des Vorfalls definiert. Als Cybervorfall gelten deshalb alle cyberspezifischen Unregelmässigkeiten, also auch unbedeutende Vorgänge (z.B. SPAM) oder Manipulationsfehler von Mitarbeitenden. Bei der Einführung einer Meldepflicht für Cybervorfälle[26] ist es daher wichtig, eine sinnvolle, allenfalls sektorspezifisch differenzierte Schwelle für meldepflichtige Cybervorfälle herauszuarbeiten. Die nachfolgenden Abklärungen konzentrieren sich daher auf Cybervorfälle, die als Cyberangriffe zu

[18] Art. 1 Abs. 2 Verordnung vom 2. März 2018 über den Bundesstab Bevölkerungsschutz (VBSTB; SR 520.17).
[19] Art. 19 Abs. 2 lit. d Bundesgesetz vom 25. September 2015 über den Nachrichtendienst (Nachrichtendienstgesetz, NDG; SR 121).
[20] Siehe Leitfaden SKI S. 20 sowie die nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) für die Jahre 2018-2022.
[21] Art. 3 lit. b CyRV.
[22] Die Definition für Cyber-Raum findet sich neben dem Glossar zur NCS 2018-2022 auch in: Die Sicherheitspolitik der Schweiz, Bericht des Bundesrates vom 24. August 2016 (Sipol 2016), BBl 2016 7884.
[23] NCS S. 4 f.
[24] NCS S. 31 f.
[25] Postulatsbericht S. 8.
[26] NCS S. 18, Massnahme 9: „Zur Verbesserung des Lagebilds zu Cyber-Bedrohungen ist die Einführung einer Meldepflicht für Cyber-Vorfälle zu prüfen und über ihre Einführung zu befinden. Dabei sind zunächst die Fragen zu klären, für wen eine Meldepflicht gelten soll, welche Vorfälle sie betrifft und an wen sie gemeldet werden müssen und ob eine Meldepflicht im Vergleich zu heute das Lagebild substanziell verbessern kann. Es werden Varianten für die Umsetzung von Meldepflichten in den verschiedenen Sektoren erarbeitet und aufgezeigt, welche gesetzlichen Grundlagen dafür nötig sind. Dies erfolgt unter Einbezug der jeweils zuständigen Behörden, der Privatwirtschaft und der Verbände, in Koordination mit der nationalen Strategie zum Schutz kritischer Infrastrukturen und unter Berücksichtigung der internationalen Entwicklungen. Auf der Basis dieser Abklärungen wird anschliessend über die Einführung einer Meldepflicht entschieden und die nötigen Schritte falls nötig eingeleitet“.

werden sind. Dabei sollte die Meldepflicht auch solche Cybervorfälle erfassen, die im Einzelfall keinen grossen Schaden angerichtet haben, aber z.B. ein hohes Schadenspotenzial aufweisen oder ein neues Angriffsmuster zeigen.
In den meisten Fällen führt ein Cybervorfall zu einer Gefährdung oder Verletzung der Datensicherheit (Art. 7 DSG[27])[28]. Gemäss revidierten Datenschutzgesetz[29] liegt eine Verletzung der Datensicherheit vor, wenn sie dazu führt, *«dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden»* (Art. 5 Bst. h nDSG). Das revidierte Datenschutzgesetz sieht für solche Verletzungen eine Meldepflicht an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) – und je nach Umständen auch an die betroffene Person – vor. Diese Meldepflicht gilt für Verantwortliche einer Datenbearbeitung, aber auch für Auftragsbearbeiter wie z.B. Cloud-Provider. In einem Strafverfahren darf eine entsprechende Meldung nur mit Einverständnis der meldepflichtigen Person gegen diese verwendet werden (Art. 24 nDSG).

3.2 Aktuelle Rechtslage auf Bundesebene (de lege lata)

3.2.1 Bestimmungen zum Schutz kritischer Infrastrukturen

Der Schutz der kritischen Infrastrukturen wird in erster Linie durch die Betreibenden und die Fachämter sichergestellt. Die Nachrichtendienste des Bundes und der Armee unterstützen die KI-Betreibenden im Falle von Cyberangriffen durch Frühwarnung und ergreifen nötigenfalls Massnahmen zur Cyberdefence. Treten Cybervorfälle auf, bietet das nationale Zentrum für Cybersicherheit (NCSC) den KI-Betreibenden subsidiäre Unterstützung für die Ereignisbewältigung an. Führen sicherheitsrelevante Vorfälle zu erheblichen Störungen und Ausfällen von kritischen Infrastrukturen, die den Charakter eines bevölkerungsschutzrelevanten Ereignisses haben, wird der Bevölkerungsschutz mit seinen Partnerorganisationen aktiv, zu denen auch der Zivilschutz zählt. Bei der Ereignisbewältigung werden die zivilen Behörden subsidiär durch die Armee und den Assistenzdienst unterstützt. Falls der Ausfall von lebenswichtigen Gütern und Dienstleistungen zu einer (drohenden) schweren Mangellage führt und die Wirtschaft keine Abhilfe schaffen kann, trifft das Bundesamt für Landesversorgung (BWL) die notwendigen Massnahmen zur Sicherstellung der wirtschaftlichen Landesversorgung. Ferner übernehmen auch gewisse Fachämter eine aktive Rolle bei der Überwachung von Krisensituationen, die durch einen Cybervorfall hervorgerufen werden können.

Die gesetzlich vorgesehenen Massnahmen zum Schutz kritischer Infrastrukturen beziehungsweise zur Ereignisbewältigung im Falle von sicherheitsrelevanten Vorfällen werden nachfolgend für die einzelnen Akteure kurz skizziert:

Der *Nachrichtendienst des Bundes (NDB)* beschafft sich Informationen, die dem frühzeitigen Erkennen und Verhindern von Bedrohungen der inneren oder äusseren Sicherheit dienen, die von Angriffen auf Informations-, Kommunikations-, Energie-, Transport- und weitere Infrastrukturen ausgehen, die für das Funktionieren von Gesellschaft, Wirtschaft und Staat unerlässlich sind (kritische Infrastrukturen). Der NDB stellt die nachrichtendienstliche Frühwarnung für Cyberangriffe auf kritische Infrastrukturen sicher[30]. Werden Computersysteme und -netzwerke, die sich im Ausland befinden, für Angriffe auf kritische Infrastrukturen in der Schweiz verwendet, so kann der NDB in diese Computersysteme und -netzwerke eindringen, um den Zugang zu Informationen zu stören, zu verhindern oder zu verlangsamen[31]. Der

[27] Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG; SR 235.1).
[28] PwC-Studie S. 11.
[29] Das totalrevidierte Datenschutzgesetz wurde am 25. September 2020 verabschiedet (BBl 2020 7639). Das Datum des Inkrafttretens ist noch nicht bekannt (Stand November 2020).
[30] Art. 6 Abs. 1 lit. a Ziff. 4 und Abs. 5 NDG; vgl. auch Art. 8 Abs. 6 CyRV.
[31] Vgl. Art. 37 Abs. 1 NDG.

NDB und der Nachrichtendienst der Armee können zur Aufklärung der Cyber-Bedrohung und zum allgemeinen Schutz kritischer Infrastrukturen Funkaufklärungsaufträge zur Beschaffung von sicherheitspolitisch bedeutsamen Informationen über Vorgänge im Ausland erteilen[32]. Der NDB führt das nachrichtendienstliche Lage- und Analysezentrum der Melde- und Analysestelle zur Informationssicherung MELANI[33].

Das *nationale Zentrum für Cybersicherheit (NCSC)* sorgt mit den zuständigen Kooperationspartnern in der Bundesverwaltung für die subsidiäre Unterstützung der KI-Betreibenden – d.h. es leistet Hilfestellungen, welche nicht auf dem Markt beschafft werden können – und fördert den Informationsaustausch zu Cyberrisiken. Zum Schutz kritischer Infrastrukturen vor Cyberrisiken arbeitet das NCSC eng mit den für die jeweiligen kritischen Sektoren zuständigen Stellen (Verwaltungseinheiten, Kantone, Kommissionen) sowie mit dem Bundesamt für Bevölkerungsschutz (BABS) und dem Bundesamt für wirtschaftliche Landesversorgung (BWL) zusammen[34]. Das NCSC betreibt die nationale Anlaufstelle für Cyberrisiken, die freiwillige Meldungen zu Cybervorfällen aus der Bundesverwaltung, der Wirtschaft, den Kantonen und der Bevölkerung entgegennimmt. Das NCSC verfügt zudem über ein «Computer Emergency Response Team» (GovCERT); dieses ist die nationale Fachstelle für die technische Vorfallbewältigung, die Analyse technischer Fragestellungen, die Einschätzungen der Bedrohungslage aus technischer Sicht und die technische Unterstützung der nationalen Anlaufstelle für Cyberrisiken. Das NCSC trägt mit gezielten Informationen zur Sensibilisierung der Bundesverwaltung und der Öffentlichkeit in Bezug auf Cyberrisiken bei, informiert über die aktuelle Lage und gibt Anleitungen für präventive und reaktive Massnahmen heraus. Es kann, sofern dies direkt oder indirekt dem Schutz der Bundesverwaltung vor Cyberrisiken dient, Daten zu Cybervorfällen und damit verbundenen Kommunikationsflüssen bearbeiten und sie staatlichen und privaten Sicherheitsteams bekanntgeben, sofern der Datenlieferant einverstanden ist und keine gesetzlichen Geheimhaltungspflichten verletzt werden[35].

Im Rahmen des Bevölkerungsschutzes sind Bund, Kantone und KI- Betreibende zur Zusammenarbeit verpflichtet, wenn es um die Vorsorge und Bewältigung von bevölkerungsschutzrelevanten Ereignissen von nationaler Tragweite – beispielsweise die Auswirkungen von sicherheitsrelevanten Vorfällen in kritischen Infrastrukturen – geht[36]. Im Ereignisfall informieren die beteiligten Bundesstellen und Kantone den *Bundesstab Bevölkerungsschutz (BSTB)*[37]. Dieser leitet den Einsatz zur Ereignisbewältigung, wenn die Ereignisse in die Zuständigkeit des Bundes fallen oder der Bundesrat ihn damit beauftragt. Er koordiniert und unterstützt die Kantone bei der Ereignisbewältigung, wenn diese ihn darum ersuchen. Jeder Kanton bezeichnet gegenüber dem BSTB eine Kontaktstelle für die Vorsorge und eine Alarmmeldestelle für den Einsatz. Der BSTB regelt die Zusammenarbeit mit den KI-Betreibenden, sorgt für die Bereitstellung der Informationsgrundlagen und die Koordination zwischen Bund, Kantonen und Dritten[38].

Die *Armee* sowie der *Assistenzdienst* unterstützen die zivilen Behörden im Inland, wenn deren Mittel beim Schutz von Personen und besonders schutzwürdigen Sachen, insbesondere

[32] Art. 3 Abs. 2 und 3 lit. f[bis] der Verordnung vom 17. Oktober 2012 über die elektronische Kriegführung und die Funkaufklärung (VEKF; SR 510.292); diese stützt sich auf Art. 38 Abs. 3 und 79 Abs. 4 NDG, Art. 99 Abs. 1[bis] MG sowie auf Art. 26 Abs. 2 und 48 Abs. 1 des Fernmeldegesetzes vom 30. April 1997 (FMG; SR 784.10). Art. 25 Abs. 2 der Verordnung vom 16. August 2017 über den Nachrichtendienst (Nachrichtendienstverordnung, NDV; SR 121.1), die sich auf das NDG stützt, enthält eine gleichlautende Bestimmung.
[33] Art. 8 Abs. 4 lit. e der Organisationsverordnung für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport vom 7. März 2003 (OV-VBS; SR 172.214.1).
[34] Art. 12 Abs. 1 lit. b CyRV; Erläuterungen zur Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung vom 27. Mai 2020 S. 5. Die Cyberrisikenverordnung stützt sich auf das RVOG sowie Art. 30 des Bundesgesetzes vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit (BWIS; SR 120), welches sich auf Art. 54 Abs.1 und 57 Abs. 2 BV sowie auf die Zuständigkeit des Bundes zur Wahrung der inneren und äusseren Sicherheit der Eidgenossenschaft stützt.
[35] Art. 12 Abs. 1 lit. a- c und h und Abs. 2 CyRV.
[36] Art. 1 Verordnung über die Warnung, die Alarmierung und das Sicherheitsfunknetz der Schweiz vom 18. August 2010 (Alarmierungs- und Sicherheitsfunkverordnung, VWAS; SR 520.12).
[37] Art. 1 ff., 5 ff., 10 VBSTB.
[38] Art. 1, 4, 5 und 14 der Verordnung vom 2. März 2018 über den Bundesstab Bevölkerungsschutz (VBSTB; SR 520.17).

von Infrastrukturen, die für Gesellschaft, Wirtschaft und Staat unerlässlich sind (kritische Infrastrukturen), nicht mehr ausreichen[39]. Die Armee und die Militärverwaltung können im Fall eines Angriffs auf ihre Informationssysteme und ihre Informatiknetzwerke Massnahmen zum Eigenschutz und zur Selbstverteidigung ergreifen. Unter militärischer Cyberabwehr versteht man umfassende Aktionen im Cyberraum mit dem Ziel, den Eigenschutz und die Selbstverteidigung der militärischen Informationssysteme und Informatiknetzwerke mit Aktionen im Cyberraum auf militärstrategischer und operativer Führungsstufe wahrzunehmen; sie umfasst die Cyberverteidigung, die Cyberaufklärung und den Cyberangriff[40].

Das *Bundesamt für wirtschaftliche Landesversorgung (BWL)* bzw. der Delegierte für wirtschaftliche Landesversorgung trifft vorsorgliche Massnahmen zur Verhinderung von schweren Mangellagen, beispielsweise durch entsprechende Pflichtlagerhaltung. Besteht bereits eine schwere Mangellage, kann der Bundesrat subsidiär zu den getroffenen Massnahmen der Wirtschaft staatliche Massnahmen einleiten, so z.B. zur Rationierung von Lebensmitteln[41].

3.2.2 Ausgewählte sektorielle Meldestellen

In den einzelnen Sektoren resp. Teilsektoren bestehen bereits gewisse Meldepflichten; die jeweiligen Meldeverfahren und die Funktionsweise der Meldestellen sind recht unterschiedlich ausgestaltet. Die meist aufsichtsrechtlich motivierte Meldepflicht richtet sich nach sektor- und branchenspezifischen Bedürfnissen. Im Rahmen der vorliegenden Rechtsabklärung wird die Funktionsweise von ausgewählten Meldestellen genauer betrachtet und deren Rechtsgrundlagen vorgestellt. Von Interesse sind gemäss Fragenkatalog des NCSC vorliegend insbesondere die Meldestelle für Geldwäscherei (MROS), die Schweizerische Sicherheitsuntersuchungsstelle (SUST) und das Schweizerische Heilmittelinstitut (Swissmedic).

Die *Meldestelle für Geldwäscherei (MROS)* stützt ihre Tätigkeit auf Art. 23 des Geldwäschereigesetzes[42]. Dieses unterstellt verschiedene Akteure einer Meldepflicht bei Geldwäschereiverdacht, namentlich Finanzintermediäre und Händler (Art. 9), Revisionsstellen (Art. 15 Abs. 5), Aufsichtsbehörden und -organisation (Art. 16). Der Bund hat das Geldwäschereigesetz gestützt auf seine verfassungsrechtlichen Regelungskompetenzen auf dem Gebiet der privatwirtschaftlichen Tätigkeit (Art. 95 BV) sowie im Bereich von Banken und Versicherungen (Art. 98 BV) erlassen. Auf Grundlage des Geldwäschereigesetzes konnte die besagte sektorspezifische Meldepflicht für Geldwäschereiverdacht eingeführt werden.

Die *Schweizerische Sicherheitsuntersuchungsstelle (SUST)*[43] ist eine ausserparlamentarische Kommission[44], die dem eidgenössischen Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) administrativ zugeordnet ist. Die SUST untersucht Zwischenfälle in der Luftfahrt, im öffentlichen Verkehr und in der Seeschifffahrt[45]. Die Untersuchungen bestehen aus einer unabhängigen Abklärung der technischen, betrieblichen und menschli-

[39] Art. 1 Abs. 2 lit. c, Art. 67 Abs. 1 lit. b des Bundesgesetzes vom 3. Februar 1995 über die Armee und die Militärverwaltung (Militärgesetz, MG; SR 510.10).
[40] Art. 1 der Verordnung vom 30. Januar 2019 über die militärische Cyberabwehr (MCAV; SR 510.921). Diese Verordnung stützt sich auf Art. 100 Abs. 4 MG.
[41] Vgl. Art. 1 ff., 5 ff., 31 ff. des Bundesgesetzes vom 17. Juni 2016 über die wirtschaftliche Landesversorgung (Landesversorgungsgesetz, LVG; SR 531); Art. 1 und 2 der Verordnung vom 10. Mai 2017 über die wirtschaftliche Landesversorgung (VWLV; SR 531.11).
[42] Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung vom 10. Oktober 1997 (GwG; SR 955.0).
[43] Am 1. November 2011 wurden das Büro für Flugunfalluntersuchungen (BFU) und die Unfalluntersuchungsstelle Bahnen und Schiffe (UUS) zur Schweizerischen Unfalluntersuchungsstelle (SUST) zusammengelegt. Per 1. Februar 2015 wurde die Schweizerische Unfalluntersuchungsstelle (SUST) in die Schweizerische Sicherheitsuntersuchungsstelle (SUST) umbenannt.
[44] Art. 57a-57g des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG; SR 172.010).
[45] Verordnung über die Sicherheitsuntersuchung von Zwischenfällen im Verkehrswesen (VSZV; SR 742.161); Erläuterungsbericht zur Verordnung über die Sicherheitsuntersuchung von Zwischenfällen im Verkehrswesen (VSZV).

chen Umstände und Ursachen, die zum Zwischenfall geführt haben. Das Ziel der Untersuchungen ist die Verhütung von weiteren ähnlichen Vorfällen. Die Art der Zwischenfälle, die eine unverzügliche Meldepflicht an die SUST auslösen, ist recht unterschiedlich (z.B. Sabotage, Unfälle, aussergewöhnliche Ereignisse) und wird genau umschrieben[46]. Gewisse Zwischenfälle (z.B. Sachschaden über CHF 100'000.-, wesentliche Störungen des Verkehrs, grössere Explosionen) müssen – zusätzlich zur unverzüglichen Meldepflicht an die SUST – dem Bundesamt für Verkehr (BAV) innerhalb von 30 Tagen gemeldet werden[47]. Die SUST ihrerseits meldet Zwischenfälle auf schweizerischem Hoheitsgebiet, an denen ausländische Unternehmen beteiligt sind, den zuständigen Behörden in den Sitzstaaten dieser Unternehmen[48].
Zur Verbesserung der Sicherheit in der Luftfahrt wurde parallel zur SUST eine weitere Meldestelle für «besondere Ereignisse» innerhalb des Bundesamtes für Zivilluftfahrt (BAZL) eingerichtet, die organisatorisch unabhängig vom BAZL als Aufsichtsbehörde ist. Das Meldeverfahren orientiert an den Vorgaben der EU[49]. Unfälle und schwere Vorfälle in der Luftfahrt sind zudem unverzüglich dem UVEK zu melden[50].
Die Grundlagen für das Meldeverfahren an die SUST finden sich unter anderem im Luftfahrt- und im Eisenbahngesetz[51]. Für den Erlass dieser beiden Bundesgesetze konnte sich der Bund auf seine verfassungsrechtlichen Regelungskompetenzen in diesen Bereichen (Art. 87, 87a BV) sowie im Post- und Fernmeldewesen (Art. 92 BV) stützen.

Das *Schweizerische Heilmittelinstitut (Swissmedic)* ist die schweizerische Zulassungs- und Aufsichtsbehörde für die Entwicklung und Überwachung von Arzneimitteln. Sie ist eine öffentlich-rechtliche Anstalt mit eigener Rechtspersönlichkeit; ihre Grundlagen finden sich im Heilmittelgesetz[52]. Dieses sieht verschiedene Meldepflichten an die Swissmedic vor, so insbesondere bei illegalen Heilmittelhandel, bei unerwünschten Wirkungen oder Qualitätsmängeln von Heilmitteln sowie beim Einsatz von Antibiotika in der Veterinärmedizin[53]. Neben dieser Funktion als Meldestelle ist die Swissmedic auch zuständig für die Regulierung im Heilmittlebereich, so beispielsweise für die Einhaltung von Bewilligungs- und Meldepflichten bei der Herstellung von Arzneimitteln, beim Inverkehrbringen von Medizinprodukten oder für klinische Versuche.
Zur Sicherstellung der Landesversorgung werden bestimmte Handels- und Herstellerunternehmen zur Lagerhaltung für gewisse Arzneimittel verpflichtet, die verschiedene Meldepflichten an die Genossenschaft Helvecura mit sich bringt[54]. Bei Versorgungsengpässen oder Lieferunterbrüchen für Humanarzneimittel unterstehen Zulassungsinhaber zudem einer Meldepflicht an die Organisation für wirtschaftliche Landesversorgung, die mit Swissmedic zusammen arbeitet[55]. Die Verordnungsbestimmungen zu diesen spezifischen Meldestellen stützen sich auf das Landesversorgungsgesetz[56].
Für den Erlass des Heilmittelgesetzes konnte sich der Bund auf seine verfassungsrechtlichen Regelungskompetenzen für privatwirtschaftliche Tätigkeiten (Art. 95 Abs. 1 BV) und betreffend den Umgang mit Heilmitteln und die Bekämpfung von übertragbaren Krankheiten (Art. 118 Abs. 2 BV) stützen. Für das Landesversorgungsgesetz wiederum berief er sich auf seine (subsidiäre) Kompetenz zur Sicherstellung der Landesversorgung (Art. 102 BV).

[46] Art. 4, 15, 17 VSZV.
[47] Art. 16 VSZV.
[48] Art. 19 Abs. 1 VSZV.
[49] Art. 20 des Bundesgesetzes vom 21. Dezember 1948 über die Luftfahrt (Luftfahrtgesetz, LFG; SR 748.0); Art. 77 ff. Verordnung vom 14. November 1973 über die Luftfahrt (Luftfahrtverordnung, LFV; SR 748.01).
[50] Art. 23 Abs. 1 LFG.
[51] Art. 24 ff. LFG; Art. 15 ff. des Eisenbahngesetzes vom 20. Dezember 1957 (EBG; SR 742.101).
[52] Bundesgesetz über Arzneimittel und Medizinprodukte vom 15. Dezember 2000 (Heilmittelgesetz, HMG; SR 812.21).
[53] Art. 59ff. HMG.
[54] Verordnung vom 10. Mai 2017 über die Pflichtlagerhaltung von Arzneimitteln (SR 531.215.31).
[55] Verordnung vom 12. August 2015über die Meldestelle für lebenswichtige Humanarzneimittel (SR 531.215.32).
[56] Bundesgesetz vom 17. Juni 2016 über die wirtschaftliche Landesversorgung (Landesversorgungsgesetz, LVG; SR 531).

Der Vergleich von MROS, SUST und Swissmedic zeigt, dass die Aufsichtsbehörde des jeweiligen Sektors nicht zwingend auch die Funktion einer sektoriellen Meldestelle wahrnehmen muss. Im Gegenteil, im vorliegenden Vergleich ist Swissmedic ist die einzige Zulassungs- und Aufsichtsbehörde, die auch als Meldestelle agiert. Dabei fällt auf, dass die Swissmedic trotz dieser Doppelfunktion im Wirkungsbereich eingeschränkt ist, zumal die Kontrolle der Heilmittelabgabe durch den Detailhandel (Drogerien, Apotheken) kompetenzrechtlich den Kantonen obliegt.
Die drei Beispiele MROS, SUST und Swissmedic zeigen ferner, dass parallele, sektorbezogene Meldestellen kein Einzelfall sind. So wurden beispielsweise im Heilmittelsektor neben der Swissmedic zwei weitere Meldestellen eingerichtet, die die Sicherstellung der Heilmittelversorgung gewährleisten sollen. Auf dem Gebiet der Luftfahrt wiederum gibt es parallel zur Meldepflicht an die SUST und das BAV als Aufsichtsbehörde für die Personenbeförderung im öffentlichen im Bereich weitere Meldepflichten für Vorfälle betreffend die Luftfahrt.
Der Aufgabenbereich von MROS, SUST und Swissmedic ist auf den jeweiligen Sektor ausgerichtet und entsprechend an sektorspezifische Gegebenheiten angepasst. Im Umfeld der Geldwäscherei ist es beispielsweise naheliegend, dass die MROS neben ihrer Funktion als Meldestelle auch eine Relais- und Filterfunktion zu den Strafverfolgungsbehörden wahrnimmt, indem sie gewisse Verdachtsmeldungen an letztere weiterleitet.
Das Meldeverfahren ist bei allen drei Meldestellen einstufig ausgestaltet, was bedeutet, dass die Meldestellen die erhaltenen Meldungen in der Regel nicht einer übergeordneten Meldestelle weiterleiten müssen[57]. Für Meldungen an die SUST besteht nur insofern eine Meldekaskade, als die SUST international relevante Vorfälle an die entsprechenden ausländischen Stellen melden muss. Bezogen auf die Schweiz gilt für alle drei Meldestellen daher grundsätzlich ein einstufiges Meldeverfahren. Das hat zur Folge, dass die Meldestellen neben der Funktion einer ersten Anlaufstelle auch die Letztverantwortung für das Meldeverfahren tragen. Sie entscheiden abschliessend darüber, ob Massnahmen in Bezug auf die eingegangenen Meldungen zu ergreifen sind.

3.2.3 Meldeverfahren bei Störfällen

Nach diesem Einblick in die Funktionsweise von ausgewählten Meldestellen scheint es im vorliegenden Kontext nutzbringend, das auf dem Gebiet des Umweltschutzes eingeführte Meldeverfahren für Störfälle kurz zu beleuchten.

Als Störfall gilt ein ausserordentliches Ereignis in einem Betrieb, auf einem Verkehrsweg oder an einer Rohrleitungsanlage, das zur Freisetzung von gefährlichen Stoffen oder Organismen führt, die Bevölkerung oder Umwelt erheblich schädigen können[58]. Ein Störfall kann verschiedene Ursachen haben; er kann die Folge eines Sicherheitsvorfalls oder und allenfalls auch eines Cyberangriffs sein. Ob und wann ein Störfall als Sicherheitsvorfall gilt, kann mangels Begriffsdefinition des letzteren vorliegend nicht geklärt werden.

Für Störfälle wird grundsätzlich ein zweistufiges Meldeverfahren vorgesehen. Bei Auftreten eines Störfalls muss der Inhaber des Betriebs, des Verkehrswegs oder der Rohrleitungsanlage die kantonale Meldestelle darüber informieren, die ihrerseits Meldung an die nationale Alarmzentrale (NAZ) macht[59]. Bei konkreter und akuter Gefahr für die Bevölkerung, z.B. durch Überflutung einer Stauanlage, muss der Inhaber der betreffenden Stauanlage für die rechtzeitige Auslösung der Warnung oder Alarmierung der Bevölkerung sorgen; er hat den Störfall unverzüglich dem Standortkanton und dem Bundesamt für Energie mitzuteilen, die

[57] Ein einstufiges Meldeverfahren gilt auch für Fernmeldedienstanbietende. Diese müssen Netzstörungen an die BAKOM melden, wobei mehrere Meldungen abzusetzen sind, um den Beginn, den Zwischenstand und das allfällige Ende einer Störung anzuzeigen. Diese Staffelung von Meldungen wird in der PwC- Studie als mehrstufiger Meldeprozess bezeichnet (S. 12). Davon abzugrenzen ist der Ausdruck des ein- oder mehrstufigen Meldeverfahrens im Sinne einer Kaskade von Meldestellen, von dem im vorliegenden Kontext die Rede ist.
[58] vgl. Art. 2 Abs. 4 Verordnung über den Schutz vor Störfällen vom 27. Februar 1991 (Störfallverordnung, StFV; SR 814.012).
[59] Art. 11 und 12 StFV.

ihrerseits die NAZ informieren[60]. Tritt ein radioaktiver Vorfall - als sog. schneller Störfall - ein[61], muss der Inhaber der betroffenen Kernanlage unverzüglich und gleichzeitig die NAZ, das eidgenössische Nukelarsicherheitsinspektorat (ENSI) und den Standortkanton informieren sowie die Aufträge zur Alarmierung und zur Verbreitung von Verhaltensanweisungen an die Bevölkerung erteilen[62]. Die speziellen Regelungen bei unmittelbarer Überflutungs- und Radioaktivitätsgefahr zeigen, dass das Meldeverfahren für Störfälle nicht in allen Fällen nach dem Grundschema abläuft, sondern je nach Art des Vorfalls ein- oder zweistufig und allenfalls mit parallelen Meldepflichten ausgestaltet ist. Interessant ist ferner, dass die NAZ über eine eigenständige Alarmierungskompetenz verfügt für den Fall, dass sie weder von den Betriebs- oder Anlageinhabern, bei denen ein Störfall eingetreten ist, noch von den zuständigen Behörden eine entsprechende Anweisung zur Alarmierung erhalten sollte[63]. Die subsidiäre Alarmierungszuständigkeit der NAZ berücksichtigt damit die Eventualität, dass die Störfälle selber oder andere Faktoren den geplanten Ablauf des Meldeverfahrens beeinträchtigen.

Ob und inwiefern es Sinn macht, im Falle der vorliegend interessierenden Meldepflicht für sicherheitsrelevante Vorfälle auf bestehende Meldemechanismen zurückzugreifen, hängt unter anderem davon ab, was das jeweilige Meldeverfahren zum primären Ziel hat. Davon abgesehen ist bei der Ausgestaltung des Meldeverfahrens neben sektorspezifischen Eigenheiten auch der möglichen Entwicklung der Bedrohungslage prospektiv Rechnung zu tragen. Damit ein Meldeverfahren auch unter erschwerten Bedingungen durchführbar ist, wäre allenfalls zu prüfen, ob eine Instanz wie die NAZ, die über eine Drehscheibenfunktion mit subsidiärer Alarmierungskompetenz verfügt, zu schaffen wäre.

3.3 Ausbau von Meldepflichten und -stellen (de lege ferenda)

Der Postulatsbericht präsentiert drei Varianten, wie die bestehenden Meldestellen für Sicherheitsvorfälle durch sektorübergreifende Meldestellen ersetzt oder ergänzt werden könnten und skizziert verschiedene Arten von Meldeverfahren für den Fall, dass eine Meldepflicht für Cyberangriffe eingeführt würde.

3.3.1 Ziel und Zweck von Meldepflichten im Allgemeinen

Grundsätzlich haben Meldepflichten zum Ziel, den Schutz der Wirtschaft und des Staates zu stärken. Es gibt im Wesentlichen fünf mögliche Beweggründe für die Einführung von Meldepflichten: die Aufsichtspflicht des Staates gegenüber der Wirtschaft, die Prävention von Sicherheitsvorfällen, die Beurteilung der Bedrohungslage (insbesondere bei Cyberangriffen) die Frühwarnung durch Informationsaustausch sowie die Koordination der Ereignisbewältigung[64].

Die Risiko- und Verwundbarkeitsanalysen, die das BABS, BWL und NCSC in den 28 (bzw. 27) kritischen Teilsektoren durchgeführt haben, um die Resilienz der kritischen Infrastrukturen zu überprüfen, hat folgendes Gefährdungsbild ergeben: in 14 Teilsektoren bestehen neben Cyber-Risiken auch weitere relevante Risiken, die zu schwerwiegenden Störungen in den jeweiligen Bereichen führen können (z. B. Stromausfall oder Erdbeben), während in den übrigen 14 Teilsektoren nur IKT-Verwundbarkeiten festgestellt wurden[65].

[60] Art. 12 Verordnung über die Warnung, die Alarmierung und das Sicherheitsfunknetz der Schweiz vom 18. August 2010 (Alarmierungs- und Sicherheitsfunkverordnung (VWAS; SR 520.12).
[61] Die Meldepflichten der Betreiber von Kernanlagen gemäss Art. 38 und 39 KEV sowie die ausführenden Erlasse des ENSI greifen bereits bei Anzeichen eines gestörten Betriebs.
[62] Art. 5 Abs. 3, Art. 11 VWAS.
[63] Botschaft zur Totalrevision des Bevölkerungs- und Zivilschutzgesetzes vom 21. November 2018 BBl 2019 544.
[64] Postulatsbericht S. 6.
[65] Hintergrundbericht vom 8. Dezember 2017 zur Strategie SKI S. 4.

Der Postulatsbericht hält dafür, dass die bestehenden sektoriellen Meldestellen grundsätzlich geeignet seien, um Meldungen zu Sicherheitsvorfällen entgegenzunehmen, wobei in einigen Sektoren noch keine Meldestelle eingerichtet worden sei. Die Meldepflicht für Sicherheitsvorfälle diene primär der sektoriellen Aufsicht sowie der Ereignisbewältigung. Demgegenüber bestehe noch keine spezifische Meldepflicht für Cybervorfälle, soweit diese nicht als Sicherheitsvorfälle meldepflichtig werden[66]. Die Einführung einer cyberspezifischen Meldepflicht würde insbesondere der Prävention (auch von Sicherheitsvorfällen), der präziseren Beurteilung der Bedrohungslage sowie der Frühwarnung durch Informationsaustausch dienen.

3.3.2 Meldepflicht für Cybervorfälle im Besonderen

Angesichts der weit formulierten Definition von «Cybervorfall» sowie der bekanntlich hohen Anzahl von freiwilligen Meldungen von Cyberangriffen an die Analyse- und Meldestelle MELANI[67] ist es für die Einführung einer Meldepflicht für Cybervorfälle entscheidend, die Schwelle der meldepflichtigen Cybervorfälle möglichst sachgerecht und zweckmässig festzulegen[68], damit die zuständige Meldestelle nicht mit Meldungen geflutet wird und in der Lage ist, die heiklen Cybervorfälle sorgfältig zu analysieren und den betroffenen Unternehmen bei der Ereignisbewältigung nötigenfalls Unterstützung zu bieten.
Um den Umfang der Meldepflicht einzugrenzen hat beispielsweise die FINMA, als sie im Frühling 2020 die bestehende aufsichtsrechtliche Auskunfts- und Meldepflicht im Finanzmarktsektor auf Cybervorfälle ausweitete, ein Kriterienraster entwickelt, damit die betroffenen Institutionen den Schweregrad der jeweiligen Vorfälle selber ermitteln können. Für die Schweregradeinstufung sind insbesondere die Dauer und das Ausmass der Beeinträchtigung in Bezug auf die Verfügbarkeit, Integrität und Vertraulichkeit der kritischen Aktiven (Daten, Technologiestruktur, Gebäude, Personal) massgebend. Anlässlich der Meldung eines Cybervorfalls haben die meldepflichtigen Institutionen unter anderem Angaben zu den Angriffsvektoren (Mail, Software-Schwachstellen, Identitätsdiebstahl usw.) und dem Angriffstypus (DDoS, unautorisierter Zugriff, Malware usw.) zu machen[69].

Im Rahmen der vorliegenden Rechtsabklärung ist davon auszugehen, dass die neu einzuführende, sektorübergreifende Meldepflicht für Cybervorfälle in erster Linie das sicherheitspolitische Ziel verfolgt, kritische Infrastrukturen vor Angriffen zu schützen (Angriffe im Sinn absichtlicher schädigender Einwirkungen) oder deren Auswirkungen möglichst rasch und effizient einzudämmen, um flächendeckende und langandauernde Güter- und Dienstleistungsausfälle zu verhindern. Die Meldepflicht für Cybervorfälle soll mithin dazu dienen, neben wichtigen Landesinteressen auch die innere und äussere Sicherheit und Stabilität zu wahren.

Es wird die Annahme getroffen, dass die Meldepflicht für Cybervorfälle grundsätzlich alle KI-Betreibenden der kritischen Teilsektoren erfassen soll, sofern keine sektorspezifischen Eingrenzungen und Ausnahmen definiert werden. Nicht meldepflichtig sind demnach alle Unternehmen, die nicht als kritische Infrastrukturen gelten sowie kritische Infrastrukturen, die aufgrund sektorieller Vorgaben von der Meldepflicht ausgenommen wurden. Diese nicht meldepflichtigen Betriebe sollen, wie bisher, allfällige Cybervorfälle freiwillig an die Meldestelle melden können.

---

[66] Es bestehen allerdings vereinzelte sektorspezifische Meldepflichten. So verlangt beispielsweise das ENSI in seiner Richtlinie ENSI-G22 explizit die Meldung von Cybervorfällen (IT-Sicherheitsereignisse und IT-Sicherheitsvorfälle) und sieht dafür abgestufte Auslösekriterien vor.
[67] Die bisherige Melde- und Analysestelle Informationssicherung (MELANI) wurde am 1. Juli 2020 ins Nationale Zentrum für Cybersicherheit (NCSC) integriert, das nun erste Anlaufstelle für Cyberrisiken ist.
[68] Welche Cybervorfälle konkret meldepflichtig sind, ist gemäss Postulatsbericht für jeden einzelnen Sektor getrennt zu klären (Postulatsbericht S. 10, 12). Mit Blick auf die Cyberrisikenverordnung wäre beispielsweise zu präzisieren, ab wann Schwachstellen und Sicherheitsvorfälle als eigentliche Cybervorfälle gelten und ob diese nur meldepflichtig sind, wenn sie aussen- oder sicherheitspolitisch bedeutend (vgl. Art. 13 Abs. 2 und Art. 8 Abs. 4 lit. d CyRV).
[69] FINMA, Aufsichtsmitteilung 05/2020 vom 7.Mai 2020.

In Bezug auf den Umfang der Meldepflicht ist anzunehmen, dass sie nicht alle Cybervorfälle erfassen soll. Einfache Fehlmanipulationen oder technische Ausfälle dürften mangels sicherheitspolitischer Relevanz kaum den notwendigen Schweregrad aufweisen, um unter die Meldepflicht zu fallen. Im Fokus der Meldepflicht stehen mitunter Vorfälle, die als Cyberangriffe konzipiert sind und kritische Infrastrukturen von aussen her bedrohen.

Näher zu prüfen sein wird, ob auch eine Meldepflicht für Sicherheitslücken eingeführt werden soll. Damit Cyberangriffe ausgeführt werden können, sei es versuchsweise oder gar erfolgreich, müssen die betreffenden kritischen Infrastrukturen cybertechnische Schwachstellen haben. Eine Meldepflicht für erhebliche Sicherheitslücken bei kritischen Infrastrukturen könnte für die Abwehr von Cyberangriffen durchaus einen Mehrwert bieten. In Bezug auf eine Meldepflicht für Sicherheitslücken stellen sich aber andere rechtliche und praktische Fragen als bei einer Meldepflicht für Cyberangriffe. Es wird näher zu prüfen sein, ob neben der Meldepflicht für Cyberangriffe auch für Sicherheitslücken eine Meldepflicht oder allenfalls eine freiwillige Meldemöglichkeit für Sicherheitslücken vorgesehen werden soll.

Es wird vorausgesetzt, dass die meldepflichtigen Vorgänge, die von KI-Betreibenden an die Meldestelle gemeldet werden, von dieser vertraulich behandelt werden. Eine Weiterleitung der Meldungen an andere Behörden ist auszuschliessen. Die Meldestelle erstellt anonymisierte Auswertungen der eingegangenen Meldungen. Diese bildet die Grundlage für die Analyse der Bedrohungslage, zur Frühwarnung vor Cyberangriffen sowie zur Verbesserung von bestehenden Sicherheitskonzepten.

3.3.3 Verfassungskompetenz

Für die Rechtsetzung in einem bestimmten Sachgebiet benötigt der Bund - gemäss dem in der Bundesverfassung festgelegten Prinzip der Einzelermächtigung (Art. 42 BV) - stets eine entsprechende verfassungsrechtliche Kompetenzgrundlage. Neue Bundeskompetenzen können nur durch eine Änderung der Bundesverfassung geschaffen werden (Art. 192 ff. BV). Für alle nicht dem Bund zugewiesenen Bereiche sind die Kantone im Rahmen ihrer subsidiären Generalkompetenz zuständig (Art. 3 und Art. 43 BV). Die Kompetenzausscheidung der Bundesverfassung bezweckt, dass eine bestimmte Aufgabe stets entweder dem Zuständigkeitsbereich des Bundes oder demjenigen der Kantone zugeordnet werden kann (sog. binäre Kompetenzordnung).

Zur Regelung von Sicherheits- oder Cybervorfällen, die kritische Infrastrukturen in ihrer Funktion beeinträchtigen, enthält die Bundesverfassung keine spezifische Kompetenzzuweisung. Eine Regelungskompetenz des Bundes kann aber auch durch das Zusammenspiel bestehender verfassungsrechtlicher Bundeskompetenzen begründet werden. In Betracht kommen neben den ausdrücklich verankerten Bundeskompetenzen auch inhärente Zuständigkeiten des Bundes (inherent powers), die sich aus der Existenz und der Natur der Eidgenossenschaft ergeben[70].

Als mögliche Kompetenzgrundlagen sind im vorliegenden Kontext insbesondere diejenigen Bundeskompetenzen von Interesse[71], die es dem Bund erlaubt haben, die geltenden Bestimmungen zum Schutz kritischer Infrastrukturen und zur Bewältigung von Sicherheitsvorfällen zu erlassen[72].

> ***Art. 54 BV (Auswärtige Angelegenheiten)***
> *[1] Die auswärtigen Angelegenheiten sind Sache des Bundes.*

[70] GIOVANNI BIAGGINI, BV-Kommentar, 2. Auflage, 2017, Vorbemerkungen zu Art. 42 bis 135, Rz. 10.
[71] Art. 54 Abs. 1 BV (Auswärtige Angelegenheiten), Art. 57 Abs. 2 BV (Sicherheit), Zuständigkeit des Bundes zur Wahrung der inneren und äusseren Sicherheit der Eidgenossenschaft, Art. 61 Abs. 1 BV (Zivilschutz), Art. 102 BV (Landesversorgung).
[72] NDG, MG, BWIS (CyRV), BZG (VBSTB), RVOG (OV-VBS, CyRV) und LVG.

> *[2] Der Bund setzt sich ein für die Wahrung der Unabhängigkeit der Schweiz und für ihre Wohlfahrt; er trägt namentlich bei zur Linderung von Not und Armut in der Welt, zur Achtung der Menschenrechte und zur Förderung der Demokratie, zu einem friedlichen Zusammenleben der Völker sowie zur Erhaltung der natürlichen Lebensgrundlagen.*
> *[3] Er nimmt Rücksicht auf die Zuständigkeiten der Kantone und wahrt ihre Interessen.*

Der Bund verfügt in der Aussenpolitik über eine ausschliessliche und umfassende Regelungskompetenz[73]. Der transnationale Charakter von Pandemien, ökologischen Veränderungen und grosstechnologischen Risiken verwischen die traditionelle Unterscheidung zwischen Innen- und Aussenpolitik[74]. Die Regelungskompetenz des Bundes für auswärtige Angelegenheiten darf dessen ungeachtet nicht extensiv ausgelegt werden. Das bedeutet, dass der Bund im innerstaatlichen Bereich an die verfassungsrechtliche Aufgabenteilung gebunden ist und sich nicht auf seine aussenpolitische Kompetenz für Regelungsbereiche berufen darf, für die er keine Kompetenz hat[75]. Art. 54 Abs. 1 BV ist beispielsweise keine geeignete Verfassungsgrundlage, damit der Bund nachrichtendienstliche Aktivitäten im Inland regeln kann[76]. Die Zuständigkeit des Bundes ist dann gegeben, wenn es neben einem grenzüberschreitenden Bezug auch um die Beziehung zu anderen Völkerrechtssubjekten geht[77].
Gestützt auf seine Regelungskompetenz für auswärtige Angelegenheiten hat der Bund das internationale Übereinkommen über die Cyberkriminalität für einen beschleunigten Informationsaustausch im Rechtshilfeverfahren ratifiziert, in dessen Rahmen das Bundesamt für Polizei (fedpol) die zuständige 7/24-Kontaktstelle für Straftaten im Zusammenhang mit Computersystemen und -daten ist[78].
Für den Erlass eines neuen Bundesgesetzes, das eine Meldepflicht für KI-Betreibende bei Cyber- oder Sicherheitsvorfällen innerhalb der Schweiz vorsieht, kann sich der Bund - ergänzend zu weiteren Verfassungskompetenzen - auf seine Zuständigkeit für auswärtige Angelegenheiten gemäss Art. 54 BV insbesondere dann berufen, wenn aller Wahrscheinlichkeit nach anzunehmen ist, dass allfällige grenzüberschreitende Auswirkungen die Staatsinteressen weiterer Länder betreffen können und deshalb die Ereignisbewältigung zwischenstaatlich zu koordinieren ist [79]. Innerstaatlich ist die Koordination der Ereignisbewältigung auf Bundesebene bei landesweiten Auswirkungen notwendig; die kantonalen Interessen und Zuständigkeiten werden dadurch nicht tangiert.

> ***Art. 57 BV (Sicherheit)***
> *[1] Bund und Kantone sorgen im Rahmen ihrer Zuständigkeiten für die Sicherheit des Landes und den Schutz der Bevölkerung.*
> *[2] Sie koordinieren ihre Anstrengungen im Bereich der inneren Sicherheit.*

Der Sicherheitsbegriff umfasst den integralen Schutz des Landes als Territorium und Lebensraum sowie seiner rechtlich geregelten Institutionen und Verfahren […] durch frühestmögliche Vorkehren und lagebezogene Massnahmen sowie Interventionen präventiver und

[73] ASTRID EPINEY, Basler Kommentar zur Bundesverfassung, Bernhard Waldmann, Eva Maria Belser, Astrid Epiney [Hrsg.], 2015, Art. 54, Rz. 20 ff.
[74] ROLAND KLEY/ROLAND PORTMANN, Die schweizerische Bundesverfassung, St. Galler Kommentar, Bernhard Ehrenzeller, Benjamin Schindler, Rainer J. Schweizer, Klaus A. Vallender [Hrsg.], 2014, Vorbemerkung zur Aussenverfassung, Rz. 4 ff.
[75] BERNHARD EHRENZELLER, Die schweizerische Bundesverfassung, St. Galler Kommentar, Bernhard Ehrenzeller, Benjamin Schindler, Rainer J. Schweizer, Klaus A. Vallender [Hrsg.], 2014. Art. 54 Rz. 15, 27, 53.
[76] RAINER J. SCHWEIZER/MARKUS H.F. MOHLER, Die schweizerische Bundesverfassung, St. Galler Kommentar, Bernhard Ehrenzeller, Benjamin Schindler, Rainer J. Schweizer, Klaus A. Vallender [Hrsg.], 2014, Vorbemerkungen zur Sicherheitsverfassung Rz. 38.
[77] ASTRID EPINEY, Basler Kommentar zur Bundesverfassung, Bernhard Waldmann, Eva Maria Belser, Astrid Epiney [Hrsg.], 2015, Art. 54, Rz. 17.
[78] Internationales Übereinkommen vom 23. November 2001 über die Cyberkriminalität (SR 0.311.43), das für die Schweiz am 1. Januar 2012 in Kraft getreten ist. Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18. Juni 2010 BBl 2010 4701.
[79] Seine Aussenkompetenz könnte der Bund ferner dazu nutzen, den Anwendungsbereich von ausländischen Meldepflichten für inländische KI-Betreibende zu klären (siehe dazu die Bemerkung in der PwC-Studie S. 9).

repressiver Art auf polizeilicher und verwaltungsrechtlicher Ebene. Sicherheitsfragen von gesamtschweizerischer Relevanz umfassen somit fast immer sowohl aussen- wie innerpolitische Aspekte. Die Aufgaben zur Wahrung der inneren Sicherheit beinhalten insbesondere die Sicherstellung des friedlichen Zusammenlebens, die Aufrechterhaltung funktionierender staatlicher Institutionen sowie die Verhinderung elementarer Gefährdungen der Gesellschaft und der Einzelnen.
Art. 57 Abs. 1 BV begründet keine neuen Bundeskompetenzen, sondern verweist auf bestehende Zuständigkeiten des Bundes. Von seiner Natur her ist Art. 57 Abs. 1 BV ein nichtkompetenzbegründender Handlungsauftrag. Für Bund und Kantone besteht gemäss Art. 57 Abs. 2 BV eine Koordinationspflicht bei der Erfüllung ihrer jeweiligen Aufgaben zur Wahrung der inneren Sicherheit. Diese Koordination wird durch die Organisation «Sicherheitsverbund Schweiz» in vertikaler (Bund – Kantone) und horizontaler Hinsicht (Kantone untereinander) umgesetzt. Auch Art. 57 Abs. 2 BV hat nach herrschender Meinung der Lehre keine kompetenzbegründende Wirkung für den Bund, sondern knüpft an anderweitige ausdrückliche oder stillschweigende Bundeskompetenzen an. Vereinzelt wird dafürgehalten, dass der Bund gestützt auf Abs. 2 Rechtssetzungskompetenzen für Fragen der inneren Sicherheit habe, sofern eine gesamtschweizerische Koordination unter Einbezug oder Leitung des Bundes notwendig sei[80]. Das BZG stützt sich beispielsweise neben Art. 61 BV (Zivilschutz) auch auf Art. 57 Abs. 2 BV (Sicherheit); die Botschaft zum BZG führt dazu aus, dass die partielle Bundeskompetenz im Bevölkerungsschutz sich aus Art. 57 Abs. 2 und Art. 61 BV ergebe[81].
Die Kompetenzzuweisung im Sicherheitsbereich ist umstritten, wobei gebietsbezogen anerkannt wird, dass die Kantone für die innere Sicherheit auf dem Kantonsgebiet verantwortlich sind (sog. kantonale Polizeihoheit), während der Bund die sicherheitsrechtlichen Aspekte in Bezug auf das ganze Staatsgebiet regelt. Als Fazit ist zu Art. 57 BV festzustellen, dass sich aus dieser Bestimmung keine Bundeskompetenzen ergeben, auf die sich ein Bundesgesetz zur Einführung von Meldepflichten für KI-Betreibende stützen könnte.

Inhärente Bundeskompetenz zur Wahrung der inneren und äusseren Sicherheit

Der Bund verfügt über eine inhärente und ausschliessliche Kompetenz zum Schutz der Eidgenossenschaft im Sinne einer sicherheitsrechtlichen Verantwortung für das gesamte Gebiet des Bundes. In der Lehre wird allgemein anerkannt[82], dass der Bund über eine ungeschriebene, inhärente Bundeskompetenz zur Wahrung der Landessicherheit verfügt; ihre konkrete Tragweite ist allerdings umstritten[83]. Es besteht Einigkeit darüber, dass sie insbesondere den Schutz der bundeseigenen Institutionen und Einrichtungen umfasst. Der Bund verfügt ferner über eine inhärente, ausschliessliche und umfassende Kompetenz zur Regelung des Staatsschutzes[84]. In der Praxis stützen sich sowohl das BWIS, das NDG, wie auch das E-ISG[85] auf die inhärente Kompetenz des Bundes zur Wahrung der inneren und äusseren Sicherheit der Eidgenossenschaft[86].

---

[80] OLIVER DIGGELMANN/TIULMANN ALTWICKER, Basler Kommentar zur Bundesverfassung, Bernhard Waldmann, Eva Maria Belser, Astrid Epiney [Hrsg.], 2015, Art. 57 Rz. 23.
[81] Botschaft zur Totalrevision des Bevölkerungs- und Zivilschutzgesetzes vom 21. November 2018 BBl 2019 534 f., 592.
[82] R. SCHWEIZER, M. MOHLER, Die schweizerische Bundesverfassung St. Galler Kommentar, Bernhard Ehrenzeller, Benjamin Schindler, Rainer J. Schweizer, Klaus A. Vallender [Hrsg.], 2014, Vorbemerkungen zur Sicherheitsverfassung Rz. 34.
[83] GIOVANNI BIAGGINI, BV-Kommentar, 2. Auflage, 2017, Vorbemerkungen zu Art. 42-135, Rz. 10.
[84] RAINER J. SCHWEIZER/MARKUS H.F. MOHLER, Die schweizerische Bundesverfassung, St. Galler Kommentar, Bernhard Ehrenzeller, Benjamin Schindler, Rainer J. Schweizer, Klaus A. Vallender [Hrsg.], 2014, Vorbemerkungen zur Sicherheitsverfassung Rz. 8, 11, 24, 35ff., 46; OLIVER DIGGELMANN/TIULMANN ALTWICKER, Basler Kommentar zur Bundesverfassung, Bernhard Waldmann, Eva Maria Belser, Astrid Epiney [Hrsg.], 2015, Art. 57 Rz. 24 ff., 35 ff.; GIOVANNI BIAGGINI, BV-Kommentar, 2. Auflage, 2017, Art. 57, Rz. 2 ff. 135, Rz. 10.
[85] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 3089.
[86] Formal ist im Ingress eines Gesetzes, das sich auf eine inhärente Bundeskompetenz stützt, Artikel 173 Absatz 2 BV – stellvertretend für einen expliziten Anknüpfungspunkt - zu nennen (Gesetzestechnische Richtlinien des Bundes, Randziffer 25). Art. 173 Abs. 2 BV ist aber keine Kompetenzgrundlage, sondern dient der horizontalen Kompetenzzuweisung zwischen den obersten Bundesbehörden (URS SAXER, THOMAS SÄGESSER, YVO HANGARTNER, BERNHARD EHRENZELLER, CHRISTOPH LANZ, PHILIPPE MASTRONARDI, CHRISTINA KISS, HEINRICH KOLLER, HANS VEST, Die schweizerische Bundesverfassung, St. Galler Kommentar, 2014, Art. 173 Rz. 169; MICHAEL MERKER/ PHILIP CONRADIN, Art. 173 Rz. 135; GIOVANNI BIAGGINI, BV-Kommentar, 2. A. 2017, Art. 173 Rz. 33; Vorbemerkung zu Art. 42-135, Rz. 19).

Die kritischen Infrastrukturen haben eine hohe Sicherheitsrelevanz für Gesellschaft, Wirtschaft und Staat. Sie stehen unter besonderem Schutz, was auch erklärt, wieso ihr Inventar als geheim klassifiziert ist. Die potenziell schwerwiegenden und landesweiten Auswirkungen von Sicherheitsvorfällen und Cyberangriffen bei kritischen Infrastrukturen gefährden die Wohlfahrt des Landes und stellen eine Bedrohung für die innere und äussere Sicherheit dar. Die Einführung einer Meldepflicht dient mithin zur Wahrung der wirtschaftlichen, gesellschaftlichen und staatlichen Stabilität. Sie bildet die Grundlage dafür, dass die Ereignisbewältigung koordiniert und rasch eingeleitet werden kann. Die skizzierte Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen hat ferner zum Ziel, anhand der Meldungen eine Analyse der Bedrohungslage zwecks Frühwarnung und Gefahrenabwehr zu erstellen. Unter diesen Voraussetzungen ist die inhärente Bundeskompetenz zur Wahrung der inneren und äusseren Sicherheit eine geeignete Verfassungsgrundlage, um gestützt darauf Gesetzesbestimmungen für eine Meldepflicht für KI-Betreibende einzuführen.

> ***Art. 61 BV (Zivilschutz)***
> *[1] Die Gesetzgebung über den zivilen Schutz von Personen und Gütern vor den Auswirkungen bewaffneter Konflikte ist Sache des Bundes.*
> *[2] Der Bund erlässt Vorschriften über den Einsatz des Zivilschutzes bei Katastrophen und in Notlagen.*

Der Bevölkerungsschutz mit zivilen Mitteln ist eines von acht Instrumenten der schweizerischen Sicherheitspolitik (Aussenpolitik, Armee, Bevölkerungsschutz, Nachrichtendienst, Wirtschaftspolitik, Zollverwaltung, Polizei und Zivildienst). Der Bevölkerungsschutz besteht aus einem Verbundsystem von Polizei, Feuerwehr, Gesundheitswesen, technischen Betrieben (wie z.B. Elektrizität, Gasversorgung, Wasserversorgung und -entsorgung, Verkehr, Kommunikationsinfrastruktur). Zu den Aufgaben des Bevölkerungsschutzes zählen insbesondere vorsorgliche Planungen und Massnahmen basierend auf Gefährdungs- und Risikoanalysen. Im Fokus stehen dabei namentlich der Schutz kritischer Infrastrukturen, da sich grossflächige Ausfälle besonders schwerwiegend auf die Bevölkerung und ihre Lebensgrundlagen auswirken können[87].
Der Zivilschutz bildet eine der Partnerorganisationen des Bevölkerungsschutzes. Er dient nicht der Gefahrenabwehr, sondern dem Schutz vor deren Auswirkungen. Für den Einsatz des Zivilschutzes zur Vorsorge und Bewältigung von Katastrophen und Notlagen hat der Bund eine konkurrierende Gesetzgebungskompetenz, von der er mit Erlass des Bevölkerungs- und Zivilschutzgesetzes weitgehend Gebrauch gemacht hat. Die anderen Partnerorganisationen des Bevölkerungsschutzes sind kantonal geregelt[88].

Fazit: Im Bevölkerungsschutz verfügt der Bund nur über beschränkte Kompetenzen, insbesondere zur Koordination von Grossereignissen sowie für Vorgaben im Bereich des Zivilschutzes (Art. 61 BV). Der Zivilschutz als Teil des Bevölkerungsschutzes dient nicht in erster Linie der Gefahrenabwehr, sondern ist auf die Ereignisbewältigung fokussiert. Der Bund kann sich deshalb für ein Gesetzgebungsvorhaben, das Meldepflichten für KI-Betreibende vorsieht, nicht auf Art. 61 BV stützen.

> ***Art. 102 BV (Landesversorgung)***
> *[1] Der Bund stellt die Versorgung des Landes mit lebenswichtigen Gütern und Dienstleistungen sicher für den Fall machtpolitischer oder kriegerischer Bedrohungen sowie*

[87] VALÉRIE ANNE SCHMOCKER, Die schweizerische Bundesverfassung St. Galler Kommentar, Bernhard Ehrenzeller, Benjamin Schindler, Rainer J. Schweizer, Klaus A. Vallender [Hrsg.], 2014, Art. 61 Rz. 8, 22, 34 f., 37.
[88] VALÉRIE ANNE SCHMOCKER, Die schweizerische Bundesverfassung St. Galler Kommentar, Bernhard Ehrenzeller, Benjamin Schindler, Rainer J. Schweizer, Klaus A. Vallender [Hrsg.], 2014, Art. 61 Rz. 22, 34 f., 37. Für den Einsatz bei Katastrophen und Notlagen besteht gemäss Biaggini eine umfassende Regelungskompetenz des Bundes, während die Kantone in anderen Belangen des Bevölkerungsschutzes noch parallele Kompetenzen haben (GIOVANNI BIAGGINI, BV Kommentar, 2017, Art. 61 Rz. 2; OLIVER DIGGELMANN/TIULMANN ALTWICKER, Basler Kommentar zur Bundesverfassung, Bernhard Waldmann, Eva Maria Belser, Astrid Epiney [Hrsg.], 2015, Art. 61, Rz. 1ff, 10).

in schweren Mangellagen, denen die Wirtschaft nicht selbst zu begegnen vermag. Er trifft vorsorgliche Massnahmen.
[2] Er kann nötigenfalls vom Grundsatz der Wirtschaftsfreiheit abweichen.

Art. 102 BV erteilt dem Bund einen Gesetzgebungsauftrag und eine umfassende Gesetzgebungskompetenz zur Sicherstellung der Vorsorge für den Fall schwerer, marktbedingter Versorgungsstörungen, welchen die Wirtschaft nicht selbst zu begegnen vermag, sowie - ausserhalb des Versorgungsrechts - für den Schutz von Vermögenswerten. Seit der Revision des LVG fokussiert die Landesversorgung vermehrt auf die Sicherstellung von Dienstleistungen wie Transportlogistik, Telekommunikation und Informationstechnologie sowie auf den Schutz kritischer Infrastrukturen[89].

Aufgrund der Subsidiarität von Bundesmassnahmen in der wirtschaftlichen Landesversorgung sowie der Tatsache, dass auch vorsorgliche Massnahme des Bundes erst bei drohender schwerer Mangellage ergehen dürfen, kann ein Gesetzgebungsvorhaben, das Meldepflichten für KI-Betreibende vorsieht, nicht auf Art. 102 BV gestützt werden.

Als weitere Kompetenzgrundlage könnte allenfalls auch Art. 95 Abs. 1 BV (Ausübung der privatwirtschaftlichen Erwerbstätigkeit) geprüft werden. Da aber die meisten kritischen Infrastrukturen staatlich oder parastaatlich organisiert sind und damit nur beschränkt privatwirtschaftlichen Grundsätzen unterworfen sind, wird an dieser Stelle auf Ausführungen zu dieser Kompetenzgrundlage verzichtet.

3.3.4 Anforderungen an die Rechtsgrundlagen

3.3.4.1 Legalitätsprinzip

Bei der Schaffung von Rechtsgrundlagen für die Verankerung von Meldepflichten ist das Legalitätsprinzip zu beachten, wonach staatliches Handeln gesetzmässig sein muss (Art. 5 Abs. 1 BV). Aus dem Legalitätsprinzip folgt, dass staatliches Handeln auf einer genügend bestimmten generell-abstrakten Norm beruhen muss (Erfordernis des Rechtssatzes und der genügenden Normdichte). Die entsprechenden Rechtsgrundlagen sind zudem auf einer Normstufe zu verankern, die der Wichtigkeit des Regelungsinhaltes Rechnung trägt (Erfordernis der genügenden Normstufe).

Im Rahmen der vorliegenden Rechtsabklärung ist insbesondere das Erfordernis der genügenden Normstufe von Belang[90]. Gemäss Art. 164 Abs. 1 BV sind alle wichtigen rechtsetzenden Bestimmungen in der Form eines Bundesgesetzes zu erlassen, insbesondere die grundlegenden Bestimmungen über die Ausübung der politischen Rechte (lit. a), die Einschränkungen verfassungsmässiger Rechte (lit. b), die Rechte und Pflichten von Personen (lit. c), den Kreis der Abgabepflichtigen sowie den Gegenstand und die Bemessung von Abgaben (lit. d), die Aufgaben und Leistungen des Bundes (lit. e), die Verpflichtungen der Kantone bei der Umsetzung und beim Vollzug des Bundesrechts (lit. f) sowie die Organisation und das Verfahren der Bundesbehörden (lit. g). Die Wichtigkeit einer Rechtsnorm zeigt sich insbesondere in der Intensität des Eingriffs, der Zahl der von der Rechtsnorm Betroffenen, der finanziellen Bedeutung und der voraussichtlichen Akzeptanz der geplanten Massnahmen. Auf Gesetzesebene sind nur die Grundzüge zu regeln, während die Details und Fragen, die besondere Fachkenntnisse erfordern, auf Verordnungsstufe festgelegt werden. Der Erlass von Verordnungsbestimmungen hat den Vorteil, dass sie bei Bedarf rasch an veränderte Verhältnisse anpasst werden können (Flexibilitätsbedürfnis)[91].

[89] PETER HETTICH, Die schweizerische Bundesverfassung St. Galler Kommentar, Bernhard Ehrenzeller, Benjamin Schindler, Rainer J. Schweizer, Klaus A. Vallender [Hrsg.], 2014, Art. 102 Rz. 3, 7 f.
[90] Die Normdichte ist zu diesem frühen Abklärungszeitpunkt insofern relevant, als das Regelungskonzept schon heute festhalten sollte, dass auch die Verwendung der aus den Meldungen gewonnenen Informationen im Gesetz selber geregelt werden muss.
[91] HÄFELIN ULRICH, MÜLLER GEORG, UHLMANN FELIX, Allgemeines Verwaltungsrecht, 7. A., Zürich/St.Gallen 2016, Rz. 350ff.

Aus dem Erfordernis der genügenden Normstufe ist für das vorliegende Vorhaben zu schliessen, dass die Regelungen zur Meldepflicht je nach Wichtigkeit auf Gesetzes- oder Verordnungsstufe zu verankern sind. Unabhängig von der Ausgestaltung der Meldepflicht ist davon auszugehen, dass diese mit einem Eingriff in die Rechte Privater verbunden ist, so dass die Regelung zumindest in den Grundzügen auf Gesetzesstufe erfolgen muss. Ausgehend von diesem Prinzip ist beispielsweise anzunehmen, dass die Einführung einer sektorübergreifenden Meldestelle für Sicherheitsvorfälle (Variante 1) oder für Cyberangriffe (Variante 3) in den Grundzügen auf Gesetzesebene zu regeln ist, einschliesslich der grundsätzlichen Festlegungen betreffend die meldepflichtigen Akteure, zu meldenden Ereignisse, den Inhalt der Meldungen und die Verwendung der mit den Meldungen bekanntgegebenen Daten. Die konkreten Abläufe des Meldeverfahrens hingegen wären sinnvollerweise auf Verordnungsstufe zu verankern. Konkretere Aussagen zur erforderlichen Normstufe sind allerdings erst dann möglich, wenn die konkreten Regelungen zu den Meldemechanismen vorliegen und ersichtlich ist, welche Neuerungen gegenüber den bestehenden Bestimmungen damit konkret eingeführt werden sollen.

3.3.4.2 Verfassungskonformität

Gemäss Art. 5 Abs. 2 BV muss die Einführung einer Meldepflicht für Cyberangriffe dem Verhältnismässigkeitsprinzip entsprechen, d.h. sie muss für die Wahrung der inneren und äusseren Sicherheit geeignet, notwendig und angemessen sein.
Es ist davon auszugehen, dass mit der Einführung einer Meldepflicht für Cyberangriffe Eingriffe in Grundrechte, namentlich in jene der KI-Betreibenden, verbunden sein werden. Zu denken ist namentlich an das Grundrecht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) oder die Wirtschaftsfreiheit (Art. 27 BV). Solche Eingriffe sind zulässig, sofern sie den Vorgaben von Art. 36 BV Stand halten. Art. 36 BV verlangt, dass sich Grundrechtseingriffe auf eine gesetzliche Grundlage stützen, im öffentlichen Interesse liegen und verhältnismässig sind. Bei der Ausarbeitung der gesetzlichen Grundlage wird die Meldepflicht so auszugestalten sein, dass diesen Kriterien genügt wird. So wird eine Meldepflicht nur soweit vorgeschrieben werden können, wie sie für die Erreichung des verfolgten öffentlichen Interesses - der Wahrung der inneren und äusseren Sicherheit - geeignet und notwendig ist. Zudem darf die Schwere der damit verbundenen Eingriffe nicht in einem Missverhältnis zum damit verfolgten Zweck stehen.

Neben der Verfassungskonformität ist auch ein Augenmerk auf die Vereinbarkeit mit internationalem Recht zu legen[92].

3.3.5 Möglichkeiten zur Schaffung von Rechtsgrundlagen

Ob die zu schaffenden Rechtsgrundlagen als neues, eigenständiges Gesetz ausgestaltet oder als Änderungen in bestehende Erlasse eingefügt werden, ist vorerst nicht entscheidend. Es ist zunächst zu klären, wie die Regelung ausgestaltet werden soll, so dass in einem zweiten Schritt das geeignete gesetzgeberische Gefäss ermittelt werden kann. Im Sinne einer Übersicht werden nachfolgend diejenigen Erlasse aufgeführt, in denen eine Meldepflicht eingefügt werden könnte.

Im Allgemeinen kommt eine Ergänzung von bestehenden Erlassen dann in Betracht, wenn ein Gesetzgebungsvorhaben mit dem Zweck, Gegenstand und Anwendungsbereich des jeweiligen Erlasses im Grundsatz vereinbar ist oder sich eine Anpassung dieser Merkmale des Erlasses anbietet. Für die hier zu diskutierenden Varianten von Meldepflichten kommen als mögliche gesetzliche Grundlagen - neben den sektorspezifischen Erlassen - insbesondere

[92] Leitfaden für die Ausarbeitung von Erlassen des Bundes (Gesetzgebungsleitfaden) 2019 Rz. 686 ff.

diejenigen Bundeserlasse in Frage, die Bestimmungen zum Schutz kritischer Infrastrukturen im weiteren Sinne - also auch im Zusammenhang mit der Ereignisbewältigung bei Notlagen und Katastrophen - enthalten (BZG, LVG, BWIS, NDG)[93]. Als weitere mögliche Rechtsgrundlage ist für Variante 3 auch das künftige Informationssicherheitsgesetz ins Auge zu fassen, sofern dessen Entwurf vom Parlament verabschiedet wird.

Variante 1:
Sektorübergreifende Meldestelle für Sicherheitsvorfälle

Für die Umsetzung von Variante 1 ist zu untersuchen, wie die bestehenden Meldeverfahren für Sicherheitsvorfälle in den sektoriellen Erlassen anzupassen sind, damit KI-Betreibende bei Auftreten von Sicherheitsvorfällen zur Meldung an eine sektorübergreifende Meldestelle - anstelle der bestehenden sektoriellen Meldestellen - verpflichtet werden können. Abzuklären ist ferner, auf welcher Rechtsgrundlage eine neue, sektorübergreifende Meldestelle eingeführt werden kann.
Der in Variante 1 skizzierte Meldeablauf würde mit sich bringen, dass die sektoriellen Meldestellen - die in vielen Fälle zugleich Aufsichtsfunktionen ausüben – von den KI-Betreibenden nicht mehr direkt über Sicherheitsvorfälle in Kenntnis gesetzt würden. Die Meldepflicht gemäss Variante 1 würde nur bei entsprechender Weiterleitung der Meldung an die Aufsichtsbehörden oder paralleler Meldepflicht noch aufsichtsrechtlichen Zielen dienen. Wird nur eine Meldepflicht an die sektorübergreifende Meldestelle vorgesehen, würde sie primär den Informationsaustausch und die Koordination bei der Ereignisbewältigung fördern. Vor diesem Hintergrund ist fraglich, ob sich eine sektorübergreifende Meldepflicht in die bestehenden sektoriellen Erlasse einfügen lässt, wenn die Aufsichtsfunktion damit nicht gewahrt werden kann. Wenn die bisherigen Meldepflichten an die sektoriellen Meldestellen nicht aufgehoben, sondern durch eine parallele Meldepflicht an die sektorübergreifende Meldestelle ausgebaut würden, wäre eine Verankerung in den sektoriellen Erlassen allenfalls denkbar. Eine **Ergänzung der bestehenden Sektorerlasse** hätte den Vorteil, dass die Modalitäten des Meldeverfahrens sektorspezifisch ausgestaltet werden könnten. Als Rechtsgrundlage für die sektorübergreifende Meldestelle scheinen die Sektorerlasse demgegenüber weniger geeignet zu sein.

Mit Blick auf die Zielsetzung der Meldepflicht gemäss Variante 1 kommen als mögliche Rechtsgrundlagen für die Verankerung des Meldeverfahrens sowie der Meldestelle insbesondere diejenigen Bundeserlasse in Betracht, die eine sicherheitspolitische Ausrichtung aufweisen. Zu denken ist dabei insbesondere an das Bevölkerungs- und Zivilschutzgesetz, das Landesversorgungsgesetz, das Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit und das Nachrichtendienstgesetz.

Das kürzlich totalrevidierte **Bevölkerungs- und Zivilschutzgesetz (BZG)** bezweckt, die Bevölkerung und ihre Lebensgrundlagen bei Katastrophen und in Notlagen sowie im Falle bewaffneter Konflikte zu schützen und zur Begrenzung und Bewältigung von Schadenereignissen beizutragen. Das BZG regelt neben dem Zivilschutz auch die Zusammenarbeit von Bund und Kantonen im Bevölkerungsschutz[94]. Die Totalrevision des BZG hatte zum Ziel, das Zusammenspiel der Partnerorganisationen des Bevölkerungsschutzes (z.B. Blaulichtorganisationen, Zivilschutz) bei der Vorsorge und Ereignisbewältigung zu stärken und den Schutz kritischer Infrastrukturen sowie Abwehrmassnahmen gegen Cyber- und ABC-Risiken zu verbessern[95]. Das BZG sieht vor, dass der Bund Einsätze zum Bevölkerungsschutz leitet, wenn kantonsübergreifende oder schweizweite Ereignisse eintreten[96]. Die Leitung übernimmt in

[93] Das Militärgesetz eignet sich nicht als Rechtsgrundlage für die Einführung von Meldepflichten und -stellen, da die Armee beim Schutz kritischer Infrastrukturen nur subsidiär zu den zivilen Behörden tätig wird (Art. 1 Abs. 2 lit. a-d MG).
[94] Art. 1 und 2 BZG.
[95] Botschaft zur Totalrevision des Bevölkerungs- und Zivilschutzgesetzes vom 21. November 2018 BBl 2019 522.
[96] Art. 5 BZG, Art. 4 Abs. 1 VBSTB.

diesem Fall der Bundesstab Bevölkerungsschutz, dessen Aufgabenbereich und Funktionsweise auf Verordnungsebene geregelt wird[97]. Grundsätzlich sind aber die Kantone für die Ereignisbewältigung im Bevölkerungsschutz zuständig. Dem Bund kommt nur bei bevölkerungsschutzrelevanten Grossereignissen eine Führungsrolle zu. Angesichts der aktuellen Konzeption des BZG ist es daher fraglich, ob der Bund die geltende Zusammenarbeitspflicht für Bund, Kantone und KI-Betreibende dahingehend erweitern könnte, dass letzteren eine Meldepflicht für Sicherheitsvorfälle auferlegt wird. Ein solches Vorhaben wäre allenfalls dadurch zu rechtfertigen, dass es nach geltendem Recht Aufgabe des Bundestabs Bevölkerungsschutz ist, für den Informationsaustausch mit KI-Betreibenden zu sorgen und die Zusammenarbeit mit ihnen zu regeln[98]. Der Bundesstab Bevölkerungsschutz kommt aber erst dann zum Einsatz, wenn sich ein mögliches Ereignis abzeichnet[99]. Dieser Umstand wiederum wäre kaum mit dem präventiven Aspekt des Meldeverfahrens zu vereinbaren.
In der Gesamtbetrachtung scheint das BZG in seiner derzeitigen Konzeption keine geeignete Rechtsgrundlage zu sein, damit der Bund ein Meldeverfahren nach Variante 1 einführen könnte.

Das totalrevidierte und am 1. Juni 2017 in Kraft getretene **Bundesgesetz über die wirtschaftliche Landesversorgung (LVG)** bezweckt die Sicherstellung der Versorgung des Landes mit lebenswichtigen Gütern und Dienstleistungen in schweren Mangellagen, denen die Wirtschaft nicht selber zu begegnen vermag. Als lebenswichtige Güter und Dienstleistungen gelten neben Nahrungs-, Futter- und Heilmittel, Saat- und Pflanzgut, Energieträger, Roh- und Hilfsstoffe für Landwirtschaft, Industrie und Gewerbe auch Dienstleistungen wie Transport und Logistik, Information und Kommunikation, Übertragung und Verteilung von Energie und der Zahlungsverkehr[100].
Die Totalrevision des LVG hatte unter anderem das Ziel verfolgt, die Resilienz von Unternehmen zu stärken und deren Produktions-, Verarbeitungs- und Lieferbereitschaft zu sichern. Als mögliche Massnahme zur Sicherstellung der wirtschaftlichen Landesversorgung können deshalb Unternehmen zur Krisenvorsorge verpflichtet werden, sei es durch Sicherstellung der Funktionsfähigkeit besonders kritischer Produktions- und Verarbeitungsprozesse, Lager- und Distributionssysteme oder betrieblicher Einrichtungen (z. B. EDV-Anlagen, Telefonnetze) oder durch technische Vorkehrungen (z. B. Notstromanlagen, Mindestvorräte und ausreichende Transportkapazitäten), nicht aber durch strukturelle Massnahmen wie etwa eine Vorratshaltung von Energiereserven zur Stromproduktion für Kraftwerke[101].
Massnahmen des Bundes im Bereich der wirtschaftlichen Landesversorgung sind subsidiäre gegenüber Massnahmen der Wirtschaft und gegenüber Aufgaben, die bereits von anderen Bundesstellen wahrgenommen werden. Bundesmassnahmen sind deshalb unzulässig, solange die Privatwirtschaft noch in der Lage ist, die Versorgungsstörung selber und aus eigener Kraft zu beheben. Der Bund ist in seinen Massnahmen auch zeitlich eingeschränkt, denn er darf vorsorgliche Massnahmen frühestens dann einleiten, wenn eine schwere Mangellage unmittelbar bevorsteht[102].
Unter diesen Voraussetzungen und in der aktuellen Konzeption ist das LVG eindeutig keine geeignete Rechtsgrundlage für die Verankerung eines Meldeverfahrens für Sicherheitsvorfälle, das auch präventive Zwecke verfolgen würde (siehe dazu auch die Ausführungen zu Art. 102 BV unter **Fehler! Verweisquelle konnte nicht gefunden werden.**)[103].

Das **Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS)** regelt die vorbeugenden polizeilichen Massnahmen, die der Bund (fedpol) in diesem Bereich

[97] Verordnung vom 2. März 2018 über den Bundesstab Bevölkerungsschutz (VBSTB; SR 520.17).
[98] Art. 1, 5 und 14 der Verordnung vom 2. März 2018 über den Bundesstab Bevölkerungsschutz (VBSTB; SR 520.17).
[99] Erläuterungen zur Verordnung über den Bundesstab Bevölkerungsschutz, Stand 8. Februar 2018, S. 3
[100] Art. 1, 4 LVG.
[101] BBl 7120 ff., 7135, 7176 ff.
[102] Vgl. Art. 5 LVG.
[103] Es ist deshalb erstaunlich, dass die Bestimmungen zum Schutz der KI im Entwurf zum Informationssicherheitsgesetz auf die Bundeskompetenzen im Bereich der inneren und äusseren Sicherheit und im Bereich der Landesversorgung (Art. 102 BV) abgestützt wurden (Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 3089).

ergreifen darf. Es handelt sich konkret um Massnahmen gegen Gewaltpropagandamaterial und Gewalt anlässlich von Sportveranstaltungen, um sicherheitspolizeiliche Aufgaben zum Schutz von Personen und Gebäuden des Bundes sowie um völkerrechtliche Schutzpflichten. Der Entwurf des Nachrichtendienstgesetzes im Jahr 2014 wurde zum Anlass genommen, die Aufgaben des Bundesamtes für Polizei (fedpol) und des Nachrichtendienstes des Bundes klarer voneinander abzugrenzen. Bis zu diesem Zeitpunkt wurde die systematische Auswertung und Aufarbeitung von Informationen zur Wahrung der inneren Sicherheit im BWIS geregelt und fiel damit in den Zuständigkeitsbereich des fedpol[104]. Der Erlass des NDG gab den Ausschlag dafür, dass gewisse Bestimmungen vom BWIS ins NDG überführt wurden, so beispielsweise jene über die periodische Beurteilung der Bedrohungslage, die Bearbeitung von Informationen über die innere und äussere Sicherheit sowie die Datenbeschaffung und Frühwarnung bei Cyberangriffen auf kritische Infrastrukturen - deren Bedeutung aufgrund der technischen Entwicklung seit Erlass des BWIS stark gestiegen war[105]. Seit Inkrafttreten des Nachrichtendienstgesetzes am 1. Januar 2017 zählt die Informationsbeschaffung zu (Cyber-)Angriffen auf kritische Infrastrukturen nicht mehr zum Aufgabenbereich des fedpol, sondern fällt in jenen des Nachrichtendienstes des Bundes[106]. Bei dieser Ausgangslage fällt das BWIS in seiner aktuellen Konzeption und Ausrichtung als mögliche Rechtsgrundlage für die Verankerung einer Meldepflicht für KI-Betreibende ausser Betracht.

Das **Nachrichtendienstgesetz (NDG)** bezweckt den Schutz wichtiger Landesinteressen und regelt die Arbeitsweise des Nachrichtendienstes des Bundes (NDB)[107]. Zu den Aufgaben des NDB gehört es, Informationen zu Angriffen auf kritische Infrastrukturen zu beschaffen und zu bearbeiten, insbesondere zum Zweck der Frühwarnung. Für Behörden des Bundes und der Kantone sowie Organisationen, die öffentliche Aufgaben wahrnehmen, bestehen Auskunfts- und Meldepflichten für Vorkommnisse, die eine konkrete (und schwere) Bedrohung der inneren oder äusseren Sicherheit darstellen. Gewisse regulatorische Aufsichtsbehörden (z.B. Finma, ElCom, ComCom oder das eidgenössische Nuklearsicherheitsinspektorat) haben zudem eine besondere Auskunfts- und Meldepflicht gegenüber dem NDB. Dieser darf umgekehrt regulatorischen Aufsichtsbehörden Personendaten bekanntgeben, wenn dies dem Schutz kritischer Infrastrukturen vor Angriffen dient[108]. Ferner kann er zur Abwehr von Angriffen auf die Informations- oder Kommunikationsinfrastruktur bestimmte Dienstleistungen für Behörden erbringen[109]. Bei Cyber-Bedrohungen von kritischen Infrastrukturen ist der NDB befugt, Informationen durch Kabelaufklärung zu beschaffen. Zur Analyse von Cyberrisiken betreibt der NDB das nachrichtendienstliche Lage- und Analysezentrum MELANI und hat durch seine Mitwirkung entscheidend zum Erfolg von MELANI beigetragen[110].
Bei dieser Ausgangslage wäre das NDG für die Verankerung einer Meldepflicht für KI-Betreibende auf den ersten Blick im Grunde keine sachfremde Rechtsgrundlage. Der Aufgabenbereich des NDB ist allerdings auf den Schutz kritischer Infrastrukturen vor *Angriffen* beschränkt, währen die Meldepflicht für KI-Betreibende sich auch auf unbeabsichtigte Sicherheitsvorfälle (z.B. Fehlmanipulationen oder technische Ausfälle) erstrecken würde. Die Verankerung der Meldepflicht im NDG wäre auch deshalb nicht ideal, weil der NDB sich selber eher nicht in der Rolle der direkten Meldestelle sieht. Insgesamt scheint das NDG somit keine geeignete zweckmässige Rechtsgrundlage zu sein.

[104] Botschaft zum BWIS vom 7. März 1994, BBl 1994 II 1168 f., 1173.
[105] Botschaft zum Nachrichtendienstgesetz vom 19. Februar 2014, BBl 2014 2143, 2212.
[106] Art. 1 und 2 BWIS; Botschaft zum Nachrichtendienstgesetz vom 19. Februar 2014, BBl 2014 2210 f., 2143, 2212.
[107] Art. 1 lit. b, Art. 2 NDG.
[108] Art. 25 lit. e sowie Anhang 1 und 3 der Verordnung vom 16. August 2017über den Nachrichtendienst (Nachrichtendienstverordnung, NDV; SR 121.1).
[109] Art. 6, 19, 20 und 69 NDG; Art. 25 lit. e sowie Anhang 3 der Verordnung vom 16. August 2017 über den Nachrichtendienst (Nachrichtendienstverordnung, NDV; SR 121.1).
[110] Art. 8 Abs. 4 lit. e der Organisationsverordnung vom 7. März 2003 für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (OV-VBS; SR 172.214.1); vgl. Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2989 f.

Als Fazit ist zu den Umsetzungsmöglichkeiten der Meldepflicht für Sicherheitsvorfälle gemäss Variante 1 festzuhalten, dass die Sektorerlasse im Grunde nur vorbehältlich der Weiterführung der bestehenden sektoriellen Meldestellen überhaupt als mögliche Rechtsgrundlagen in Betracht kommen. Von den untersuchten, sektorübergreifenden Bundeserlassen aus dem Sicherheitsbereich (BZG, LVG, BWIS, NDG) scheint keiner – zumindest in der aktuellen Gesetzeskonzeption - geeignet zu sein, um eine Meldepflicht für Sicherheitsvorfälle an eine sektorübergreifende Meldestelle verankern zu können. Die Ausrichtung des Meldeverfahrens nach Variante 1 deutet aber darauf hin, dass die damit angestrebten Ziele durchaus bevölkerungsschutzrelevant und -wirksam sein könnten. Eine Zuordnung zum Bevölkerungsschutz wäre somit a priori zutreffend und im Grundsatz sachgerecht. Angesichts der überwiegend kantonalen Zuständigkeit für die Partnerorganisationen des Bevölkerungsschutzes und der grundsätzlich parallelen Zuständigkeit für die innere Sicherheit wäre daher eine gemeinschaftliche Regulierung durch Bund und Kantone ein möglicher Weg (siehe dazu die Ausführungen unter 3.3.6).

Variante 2:
Meldepflicht für Cyberangriffe an sektorielle Meldestellen

Für die Umsetzung von Variante 2 ist zu untersuchen, wie die bestehenden sektoriellen Meldestellen für Sicherheitsvorfälle zu stärken und auszubauen sind, damit sie auch Meldungen zu Cyberangriffen entgegennehmen können[111]. Zu prüfen ist weiter, wie die nationale Anlaufstelle für Cyberrisiken des NCSC, die seit dem 1. Juli 2020 an die Stelle der Analyse- und Meldestelle zur Informationssicherung (MELANI) getreten ist, in das neue Meldeverfahren und das System der sektoriellen Meldestellen eingebunden werden kann.
Bei der Variante 2 stellt die Meldepflicht für Cyberangriffe die wesentliche Neuerung dar. Da die Meldung an bestehende sektorielle Meldestellen erfolgen würde, könnte das Meldeverfahren weitgehend auf den bestehenden Strukturen aufbauen. Die Modalitäten der Meldepflicht für Cyberangriffe (Adressatenkreis, Zeitvorgaben, Umfang, allfällige Sanktionen im Unterlassungsfall) wären den Gegebenheiten des jeweiligen Sektors anzupassen und sektorspezifisch zu regeln. Unter diesen Voraussetzungen wäre es daher denkbar, das bestehende Meldeverfahren für Sicherheitsvorfälle auf Cyberangriffe zu erweitern.
Aktuell können KI-Betreibende sowie auch weitere Unternehmen, die nicht als KI inventarisiert sind, und auch Privatpersonen auf freiwilliger Basis allfällige Cyberangriffe der nationalen Anlaufstelle für Cyberrisiken melden. KI-Betreibende werden bei der Ereignisbewältigung nötigenfalls subsidiär vom «Computer Emergency Response Team» (GovCERT) unterstützt und über die aktuelle Lage zu Cyberrisiken informiert[112].
Um die nationale Anlaufstelle für Cyberrisiken ins Meldeverfahren für Cybervorfälle zu integrieren, könnte in den jeweiligen **Sektorerlassen** parallel zur Meldepflicht für Sicherheitsvorfälle eine Meldepflicht für Cyberangriffe verankert werden. Das bestehende Meldeverfahren für Sicherheitsvorfälle würde damit auf Cyberangriffe erweitert werden, wobei für letztere eine parallele Meldepflicht an die sektoriellen und die Cybermeldestelle gelten würde. Die Ausweitung des Meldeverfahrens könnte dazu führen, dass die sektoriellen Meldestellen stärker beansprucht werden. Durch die Einbindung der nationalen Anlaufstelle für Cyberrisiken wäre aber auch eine Entlastung bezüglich der Meldungen zu Cyberangriffen zu erwarten. Das NCSC hätte mit der Anlaufstelle und dem GovCERT die notwendige Fachexpertise, um eine Triage der Meldungen vorzunehmen und im Ereignisfall allenfalls auch Unterstützung zu bieten.

Falls die sektoriellen Meldestellen bei der Bearbeitung von Meldungen zu Cyberangriffen auf die Unterstützung vom NCSC angewiesen wären, müsste der Aufgabenbereich des NCSC (vgl. Art. 12 CyRV) durch eine **Anpassung der CyRV** entsprechend erweitert werden.

[111] Nach Variante 2 sollen in denjenigen Sektoren, die keine Meldestellen haben, solche geschaffen werden. Der Postulatsbericht präzisiert aber nicht, welche Sektoren keine Meldestellen haben; dies geht auch nicht aus der PwC-Studie hervor. Aus diesem Grund wird dieser Punkt nachfolgend nicht weiter vertieft.
[112] Art. 12 Abs. 1 lit. a, c und h CyRV.

Für den Fall, dass die sektoriellen Meldestellen nicht nur durch das NCSC unterstützt, sondern zur Zusammenarbeit mit ihm verpflichtet werden sollen oder falls das Meldeverfahren in einigen Sektoren mangels Bundeszuständigkeit nicht angepasst werden kann, wäre die Meldepflicht für Cybervorfälle sowie die Zusammenarbeitspflicht der sektoriellen Meldestellen mit dem NCSC formell-gesetzlich in einem sachgebietsübergreifenden Bundesgesetz, allen voran dem **Informationssicherheitsgesetz**, festzulegen (siehe dazu die Ausführungen zu Variante 3).

Als Fazit kann zur Umsetzung von Variante 2 im Wesentlichen festgestellt werden, dass zum einen die Möglichkeit besteht, die sektoriellen Meldeverfahren für Sicherheitsvorfälle auf Cybervorfälle zu erweitern. Diese Einschätzung steht aber unter dem Vorbehalt, dass sich das bestehende Meldeverfahren für Sicherheitsvorfälle in den sektoriellen Erlassen auch tatsächlich ohne Weiteres und in jedem der 27 Teilsektoren erweitern lässt, was vorliegend nicht überprüft wurde. Als Alternative oder ergänzend zur Anpassung der sektoriellen Regelungen wäre es deshalb prüfenswert, eine Meldepflicht für Cybervorfälle durch eine Verankerung im Informationssicherheitsgesetz sektorübergreifend einzuführen. Dieses Vorgehen wäre auch deshalb interessant, weil das Informationsschutzgesetz (ISG) auch eine geeignete Rechtsgrundlage für eine allfällige Verankerung der Zusammenarbeitspflicht der sektoriellen Meldestellen mit dem NCSC (dessen Grundlage sich im ISG findet) wäre. Insgesamt scheint die Variante 2 von allen Varianten deshalb am einfachsten umsetzbar zu sein.

Variante 3:
Meldepflicht für Cyberangriffe an sektorübergreifende Cybermeldestelle

Bei Variante 3 gilt es abzuklären, unter welchen Voraussetzungen eine Meldepflicht für Cyberangriffe an eine sektorübergreifende Meldestelle eingeführt werden kann (Variante 3b) und wie es sich verhalten würde, wenn die Cyberangriffe zuerst an sektorielle Cybermeldestellen (sog. Sektoren-CERTs) im Sinne eines kaskadenartigen Meldesystems erfolgen würde (Variante 3a)[113]. Laut Postulatsbericht sollen die Modalitäten des Meldeverfahrens teilweise sektorspezifisch (Kreis der meldepflichtigen KI-Betreibenden), teilweise einheitlich durch die sektorübergreifende Cybermeldestelle (Schwelle der Meldepflicht) festgelegt werden. Die bestehenden sektoriellen Meldestellen für Sicherheitsvorfälle sind bei Variante 3 beizubehalten; das Zusammenspiel dieser Meldestellen mit den Sektoren-CERTs und der sektorübergreifenden Cybermeldestelle wird vorliegend nicht vertieft.
Für die Ausführungen zur Variante 3 wird im Rahmen dieser Rechtsabklärung die Annahme getroffen, dass die nationale Anlaufstelle für Cyberrisiken des NCSC die Funktion einer sektorübergreifenden Cybermeldestelle ausüben würde. Der Aufgabenbereich des NCSC wird, wie bereits erwähnt, in der **Cyberrisikenverordnung (CyRV)** geregelt[114], während seine Rechtsgrundlage im Informationssicherheitsgesetz (ISG) zu finden ist.

Variante 3a:
Meldepflicht für Cyberangriffe an Sektoren-CERTs

Damit KI-Betreibende allfällige Cyberangriffe zunächst den jeweiligen Sektoren-CERTs (und nicht direkt der sektorübergreifenden Cybermeldestelle) melden würden, wäre es grundsätzlich denkbar, eine entsprechende Meldepflicht (in Anlehnung an die Regelung für Sicherheitsvorfälle) in den jeweiligen **Sektorerlassen** (oder den **Rechtsgrundlagen der Sektoren-**

[113] Die PwC-Studie geht bei ihren Ausführungen zu Modell 3 - im Gegensatz zum Postulatsbericht - davon aus, dass die Meldung von Cybervorfällen zunächst an die sektoriellen Meldestellen für Sicherheitsvorfälle erfolgt und von diesen gegebenenfalls an die sektorübergreifende Cybermeldestelle weitergeleitet wird (S. 29 ff.). Die im Postulatsbericht als Variante 3 skizzierte Möglichkeit einer direkten Meldung von Cybervorfällen an eine sektorübergreifende Meldestelle erwähnt die PwC-Studie als Variante 1.2 zu Modell 1 (S. 27). Sowohl der Postulatsbericht wie die PwC-Studie enthalten keine Bestandesaufnahme dazu, ob und in welchen Sektoren CERTs eingerichtet wurden. Daher kann Variante 3a vorerst nur rein theoretisch erörtert werden.
[114] vgl. Art. 12 CyRV.

CERTs, soweit solche vorhanden sind) zu verankern. Der Kreis der meldepflichtigen KI-Betreibenden könnte somit sektor- bzw. branchenspezifisch definiert werden. Um die Sektoren-CERTs ihrerseits zu verpflichten, die gemeldeten Cyberangriffe an die sektorübergreifende Cyberstelle weiterzuleiten, könnte allenfalls eine Melde- oder Zusammenarbeitspflicht im Informationssicherheitsgesetz (ISG) vorgesehen werden (siehe dazu Variante 3b). Die möglichen Rechtsgrundlagen für die Einführung einer sektorübergreifenden Cybermeldepflicht werden nachfolgend erläutert (siehe Variante 3b).

Variante 3b:
Meldepflicht für Cyberangriffe an sektorübergreifende Cybermeldestelle

Falls KI-Betreibende Cyberangriffe nicht zuerst den Sektoren-CERTs (Variante 3a), sondern direkt einer sektorübergreifenden Cybermeldestelle, also der nationalen Anlaufstelle für Cyberrisiken des NCSC, melden sollen, dann bilden die sektoriellen Erlasse keine geeignete Rechtsgrundlage für die Verankerung einer entsprechenden Meldepflicht. Gleiches gilt auch die Verankerung der sektorübergreifenden Cybermeldestelle. Es kommen daher für die Umsetzung von Variante 3b in erster Linie sachgebietsübergreifende Bundeserlasse aus dem Sicherheitsbereich in Frage, allen voran das geplante Informationssicherheitsgesetz (ISG). Die bei Variante 1 gemachten Ausführungen zum BZG, BWIS und NDG gelten - mutatis mutandis - auch für die Umsetzung von Variante 3b, d.h. sie eignen sich nicht als mögliche Rechtsgrundlagen für die Verankerung einer sektorübergreifenden Meldepflicht für Cyberangriffe.

Das **Informationssicherheitsgesetz (ISG)**, dessen Entwurf vom 22. Februar 2017 noch nicht vom Parlament verabschiedet wurde[115], hat zum Ziel, die Sicherheit für die vom Bund bearbeiteten Informationen und eingesetzten Informatikmittel zu gewährleisten[116], namentlich durch Massnahmen betreffend Risiko-Management, Klassifizierung von Informationen, Informatiksicherheit, Personensicherheitsprüfungen, Sicherheit bei sensitiven Beschaffungen und Unterstützung für KI-Betreibende. Mit dem Erlass des ISG soll ein einheitlicher Rahmen für die Informationssicherheit beim Bund geschaffen werden, deren Grundlagen bisher hauptsächlich in der Bundesinformatikverordnung (BinfV) und der Informationsschutzverordnung (ISchV)[117] geregelt waren. Mit den Massnahmen zur Informationssicherheit (oder IKT-Sicherheit) soll die Authentizität, Vertraulichkeit, Integrität und Verfügbarkeit eines informations- und kommunikationstechnischen Systems und der darin verarbeiteten und gespeicherten Daten geschützt werden[118].
Im Vernehmlassungsverfahren wurde auf die Einführung einer behördlichen Meldepflicht für Sicherheitsvorfälle für KI verzichtet, weil der Bundesrat für die Bundesverwaltung und die Armee eine entsprechende Meldepflicht anordnen kann. Es wurde auch davon abgesehen, einheitliche Mindeststandards für KI einzuführen. Damit KI-Betreibende effizient unterstützt werden können, soll die Bearbeitung von Adressierungselementen im Fernmeldebereich (insb. Domainnamen, IP- und E-Mail-Adressen) im ISG formell-gesetzlich verankert werden[119]. In den parlamentarischen Beratungen zum Gesetzesentwurf wurde die Einführung einer Meldepflicht für KI-Betreibende bei «erheblichen Vorfällen» erneut diskutiert, im Juni 2020 von der Mehrheit des Nationalrats jedoch abgelehnt[120].
Nach dem Gesagten scheint das Informationssicherheitsgesetz den idealen Rahmen zu bilden, um für KI-Betreibende eine Meldepflicht für Cyberangriffe einzuführen. Die Einführung dieser sektorübergreifenden Verpflichtung für KI-Betreibende – sowie der damit allenfalls verbundene Eingriff in kantonale sektorielle Regelungen – liesse sich mit der inhärenten

[115] Der Entwurf des Informationssicherheitsgesetzes stützt sich auf Art. 54 Abs. 1, 60 Abs. 1, 101, 102 Abs.1 und 173 Abs. 1 lit. a und b sowie Abs. 2 BV.
[116] Art. 1 Abs. 1 E-ISG.
[117] Verordnung vom 4. Juli 2007 über den Schutz von Informationen des Bundes; SR 510.41.
[118] NCS S. 31; Erläuternder Bericht vom 26. März 2014 zum Entwurf eines Bundesgesetzes über die Informationssicherheit (ISG), S. 3.
[119] Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017, BBl 2017 2954, 2988 ff., 3008, 3066, 3089.
[120] BR 17.028.

Bundeskompetenz zur Wahrung der Landesinteressen rechtfertigen, auf die sich das ISG bereits abstützt. Aus systematischer Sicht könnte die Meldepflicht innerhalb des ISG im «5. Kapitel: Kritische Infrastrukturen» eingefügt werden.
Mit dem Erlass des ISG wird eine formell-gesetzliche Grundlage für das NCSC geschaffen, dessen Existenz und Aufgaben bislang nur in der Cyberrisikenverordnung geregelt sind. Die Regelung in Art. 75 E-ISG sieht vor, dass der Bund eine zuständige Stelle bezeichnet, die KI-Betreibende unterstützt, damit allfällige Netz- und Systemunterbrechungen sowie Missbräuche selten, von kurzer Dauer, beherrschbar und von geringem Schaden sind (Abs. 1 und 5). Diese Bestimmung bildet die Grundlage des NCSC mit der nationalen Anlaufstelle für Cyberrisiken und dem GovCERT. Art. 75 E-ISG eignet sich grundsätzlich auch als Rechtsgrundlage für eine allfällige sektorübergreifende Cybermeldestelle, sollte diese nicht von der nationalen Anlaufstelle betrieben werden. Das ISG regelt ferner datenschutzrechtliche Fragen für die Datenbearbeitung des NCSC sowie die Datenbekanntgabe an Dritte.
Die **Cyberrisikenverordnung** wäre das ideale Gefäss, um die Funktionsweise der Cybermeldestelle und die Modalitäten des Meldeverfahrens (Schwelle der Meldepflicht, Kreis der meldepflichtigen KI-Betreibenden) festzulegen. Entsprechend wären im Ingress der Cyberrisikenverordnung neben den Bestimmungen des RVOG und BWIS auch auf die einschlägigen Artikel des ISG (Art. 75 ff.) zu erwähnen. Diese breitere Abstützung der Cyberrisikenverordnung wird mit Inkrafttreten des ISG aber auch im Hinblick auf die gesetzlichen Grundlagen für das NCSC notwendig werden.

Als Fazit ist zu Variante 3 festzuhalten, dass das Informationsschutzgesetz als mögliche Rechtsgrundlage für die Verankerung einer sektorübergreifenden Meldepflicht für Cyberangriffe, die für KI-Betreibende gelten soll, geeignet erscheint. Die Ausführungsbestimmungen könnten in der Cyberrisikenverordnung eingefügt werden. Abgesehen von diesen beiden Erlassen wurden keine weiteren geeigneten Rechtsgrundlagen für die Umsetzung von Variante 3 gefunden.

3.3.6 Weitere Regelungsmöglichkeiten

Neben der Möglichkeit, die neu einzuführenden Meldepflichten und -stellen im Bundesrecht durch Ergänzung oder Schaffung von neuen Bundesgesetzen zu verankern, bestehen noch weitere Regelungsmöglichkeiten.

Es wäre beispielsweise denkbar, dass die Kantone unter sich ein Konkordat über den Ausbau von Meldepflichten und -stellen zu Sicherheitsvorfällen und Cyberangriffen abschliessen, dem der Bund anschliessend beitritt (vgl. Art. 48 Abs. 1 und 2 BV).

Als weiteres Regelungsinstrument böte sich an, dass Bund und Kantone eine Vereinbarung über den Ausbau von Meldepflichten und -stellen abschliessen und gestützt darauf parallel legiferieren. Allfällige Vorarbeiten für eine solche Vereinbarung könnte möglicherweise die Organisation «Sicherheitsverbund Schweiz», in der Bund und Kantone paritätisch vertreten sind, aufgleisen oder koordinieren.

Diese beispielhaft erwähnten alternativen Regelungsmöglichkeiten erscheinen allerdings von untergeordneter Bedeutung zu sein, zumal der Regelungsgegenstand (Schutz kritischer Infrastrukturen durch Meldepflichten) einer koordinierten Lösung bedarf. Angesichts der potentiellen erheblichen und möglicherweisen grenzüberschreitenden Auswirkungen von Sicherheitsvorfällen oder Cyberangriffen hat der Bund die Ereignisbewältigung im Bevölkerungsschutz zu leiten. Diese Umstände sprechen für die Sachnotwendigkeit einer «Bundeslösung».

3.4 Beantwortung der Fragen

Nachfolgend werden die Fragen, die vom NCSC für die vorliegende Rechtsabklärung in einem Fragenkatalog zusammengestellt wurden, der Reihe nach beantwortet[121].

3.4.1 Grundsatzfragen

Verfassungsgrundlagen: bestehen ausreichende Grundlagen in der Verfassung, damit der Bund eine Meldepflicht für Cyberangriffe einführen kann?

Die Bundesverfassung enthält keine ausdrückliche Bestimmung, die den Bund zur Regulierung von KI-Betreibenden oder zur Vorsorge in Bezug auf Cyber- oder Sicherheitsvorfällen ermächtigen würde. Der Bund verfügt aber über verschiedene Kompetenzen im Sicherheitsbereich. Für die Regelung von auswärtigen Angelegenheiten ist er umfassend zuständig, während er zur Wahrung der inneren Sicherheit fragmentarische Kompetenzen (Staatsschutz, Institutionen und Organe) hat. Angesichts der potenziell landesweiten, allenfalls grenzüberschreitenden und erheblichen Auswirkungen von Sicherheitsvorfällen und Cyberangriffen bei kritischen Infrastrukturen ist insbesondere seine inhärente Kompetenz zur Wahrung der Landesinteressen im Sinne einer Letztverantwortung für den Schutz des Gesamtstaates von Bedeutung.
Eine Bundesregelung zur Meldepflicht bei Cyberangriffen ist mit dem Subsidiaritätsprinzip (Art. 5a i.V.m. 43a BV) grundsätzlich vereinbar, denn es bedarf eines einheitlichen Meldeverfahrens, um Cyberangriffe möglichst zeitnah und zentral erfassen sowie um im Ereignisfall umgehend Fachwissen bereitzustellen und koordinierte, schweizweite Vorkehren treffen zu können.
Als Fazit ist festzustellen, dass die bestehenden verfassungsrechtlichen Kompetenzen des Bundes ausreichen dürften, damit er unter sicherheitspolitischen Aspekten eine Meldepflicht für KI-Betreibende bei Cyberangriffen einführen kann. Auf welche Kompetenz sich der Bund bei der Legiferierung konkret abzustützen hat, hängt von der konkreten Zielsetzung der Meldepflicht sowie von der Ausgestaltung des Meldeverfahrens ab.

Verhältnis Kantone: kann der Bund eine Meldepflicht für die Kantone selber (kantonale Verwaltungen) und für Sektoren (z.B. Entsorgung) einführen, welche unter kantonaler Hoheit stehen?

Wenn der Bund aus sicherheitspolitischen Gründen, d.h. gestützt auf seine inhärente Bundeskompetenz zur Wahrung der Landessicherheit, eine Meldepflicht für KI-Betreibende bei Auftreten von Sicherheitsvorfällen oder Cyberangriffen einführt, greift er damit nur sehr punktuell in kantonal geregelte Sachbereiche ein. In denjenigen Sektoren, Teilsektoren oder Branchen, die in die kantonale Regelungszuständigkeit fallen, müssen sich KI-Betreibende daher weiterhin nach den kantonalen Vorschriften richten, selbst wenn sie zusätzlich der bundesrechtlichen Meldepflicht für Sicherheitsvorfälle oder Cyberangriffe unterstehen. Soweit von der Meldepflicht auch kantonale Institutionen und Organe betroffen sind, die als kritische Infrastrukturen gelten (z.B. Kantonsverwaltung, Universität, Blaulichtorganisationen), bedeutet eine bundesrechtliche Meldepflicht für KI-Betreibende keinen Eingriff in die Aufgaben- oder Organisationsautonomie der Kantone (Art. 47 Abs. 2 BV).

Welche Art von Gesetzgebung wird nötig bei welcher Variante: neues Gesetz, Änderungsgesetz, weitere Möglichkeiten?

[121] Die Abgrenzung zwischen «zentralen Meldestellen» und «dezentralen Meldestellen», die der Fragenkatalog aus dem Postulatsbericht und der PwC-Studie übernommen hat, kann mehrere Bedeutungen haben und sowohl die Abgrenzung von sektoriellen zu sektorübergreifenden Meldestellen, von kantonalen zu eidgenössischen Meldestellen oder von (geographisch) dezentralen zu zentral gelegenen Meldestellen beinhalten. Ferner ist es vorstellbar, dass eine kantonale Meldestelle sektorübergreifende Meldungen entgegennimmt oder dass eine nationale Meldestelle nur sektorspezifisch zuständig ist.

Die aufgezeigten Regelungsmöglichkeiten für die Einführung einer Meldepflicht, insbesondere deren Verankerung in bestehenden Bundeserlassen sowie mögliche Schwierigkeiten bei der Umsetzung der einzelnen Varianten werden hiervor ausführlich diskutiert, weshalb an dieser Stelle nur darauf verwiesen wird.

Grundsätzlich ist davon auszugehen, dass der Bund über die notwendigen verfassungsrechtlichen Kompetenzen im Sicherheitsbereich verfügt, um aus sicherheitspolitischen Gründen ein Gesetzgebungsvorhaben mit Meldepflichten für KI-Betreibende erlassen zu können (siehe dazu die Ausführungen unter **Fehler! Verweisquelle konnte nicht gefunden werden.**).
Für die Verankerung einer Meldepflicht ist sowohl die Schaffung eines neuen Bundesgesetzes als auch die Änderung bestehender Gesetze denkbar. Die verfassungsrechtlichen Voraussetzungen und das Gesetzgebungsverfahren sind in beiden Fällen gleich. Es empfiehlt sich, diese formale Frage erst zu beantworten, wenn die inhaltliche Ausgestaltung der Regelungspflicht in ihren Grundzügen geklärt ist.

Alternative Regelungsmöglichkeiten wie beispielsweise durch Vereinbarung oder parallele Rechtsetzung von Bund und Kantonen sind grundsätzlich denkbar (siehe dazu die Bemerkungen unter 3.3.6). Diese dürften aber praktische und rechtliche Probleme aufwerfen und sollten lediglich bei Vorliegen guter Gründe in Betracht gezogen werden.

3.4.2 Frage zu Variante 1

Welche rechtlichen Grundlagen bestehen für ähnliche zentrale Meldestellen (z.B. Meldestelle für Geldwäscherei MROS, Schweizerische Sicherheitsuntersuchungsstelle SUST, Swissmedic)?

Die Meldestellen MROS, SUST und Swissmedic, deren Funktionsweise unter 3.2.2 erläutert wurde, finden ihre Grundlage in Bundesgesetzen, die der Bund gestützt auf spezifische verfassungsrechtliche Sachkompetenzen erliess. Aus kompetenzrechtlicher Sicht war die Einrichtung dieser sektoriellen Meldestellen daher unproblematisch, da der Bund in den jeweiligen Sachgebieten über entsprechende Regelungskompetenzen verfügt. Für die Einrichtung einer sektorübergreifenden Meldestelle für Sicherheitsvorfälle bzw. Cyberangriffe benötigt der Bund demgegenüber eine sachgebietsübergreifende Regelungskompetenz, die es ihm erlaubt, geeignete Massnahmen zur Prävention und Bewältigung von Störungen und Ausfällen von KI zu treffen, um einen schwerwiegenden Schaden für Wirtschaft und Gesellschaft zu verhindern.

3.4.3 Fragen zu Variante 2

Ist ein Änderungsgesetz möglich, welches mehrere sektorspezifische Gesetze ändert?

Es ist sowohl auf Kantons- wie auf Bundesebene möglich, geplante Gesetzesänderungen, die verschiedene Sacherlasse betreffen, in einem Mantelerlass zusammenzufassen und gesamthaft dem Referendum zu unterstellen, sofern die Einheit der Materie durch den sachlichen Zusammenhang gewahrt ist. Typischerweise werden Mantelerlasse zur Regelung von Querschnittsaufgaben eingesetzt. Ein Mantelerlass enthält keine eigenen materiellen Bestimmungen, sondern dient nur als Gefäss für die einzelnen Gesetzesänderungen. Deshalb wird ein Mantelerlass auf Bundesebene nur in der amtlichen Sammlung (AS) publiziert, ohne

dass er eine Nummer für die Einordnung in der systematischen Rechtssammlung (SR) erhält[122].
Daneben bestünde auch die Option, ein neues Querschnittsgesetz oder eine Änderung eines Querschnittsgesetzes mit Änderungen anderer Erlasse zu kombinieren.
Keine entsprechende Kombinationsmöglichkeit gibt es hingegen, wenn Erlasse unterschiedlicher Stufen erlassen werden sollen (insb. Bundesgesetze und kantonale Gesetze, aber auch Gesetze und Verordnungen derselben Staatsebene). In einem solchen Fall muss geklärt werden, ob und in welcher Form der übergeordnete Erlass dem untergeordneten Rechtsetzungsorgan Vorgaben zu machen hat, um eine inhaltliche und zeitliche Koordination sicherzustellen.
Für die Umsetzung von Variante 2 wäre ein Mantelerlass deshalb interessant, weil dadurch sichergestellt würde, dass die Einführung der Meldepflicht zeitgleich und einheitlich erfolgen könnte. Man könnte sich auch eine Konstruktion mit einem zentralen Gesetz für alle Bereiche in kantonaler Kompetenz und gleichzeitigen Anpassungen von sektoriellen Bundesgesetzen vorstellen.

Ergänzend zu den obigen Ausführungen zur Umsetzung der sektorspezifischen Änderungen mittels Mantelerlass ist nachfolgend kurz auf die Möglichkeit hinzuweisen, dass die für alle Sektoren geltenden minimalen Vorgaben beispielsweise in einem «Dachgesetz» untergebracht werden könnten. Solche Dachgesetze sind beispielsweise das Bundesgesetz über den Allgemeinen Teils des Sozialversicherungsrechtes[123] oder das FINMAG[124]. Das ATSG ist auf die einzelnen Sozialversicherungsbereiche nur dann anwendbar, sofern und soweit die Spezialgesetze es im Sinne eines «opting in» für anwendbar erklären (vgl. Art. 2 ATSG). Das FINMAG regelt seinen Anwendungsbericht auf eine andere Art und Weise. Es nennt die einschlägigen Gesetze im Finanzmarktbereich ausdrücklich, auf die es anwendbar ist (Art. 1 Abs. 1 FINMAG). Die jeweiligen Spezialgesetze können im Sinne eines «opting out» einzelne ihrer Bestimmungen von der Anwendbarkeit des FINMAG ausnehmen (Art. 2 Abs. 1 FINMAG).

Ausgehend von der Regulierungstechnik des FINMAG wäre es beispielsweise denkbar, dass der Grundsatz der Meldepflicht in einem Dachgesetz verankert wird und es den einzelnen (Teil)Sektoren – für die z.T. die Kantone zuständig sind – überlassen bleibt, dieses Meldeverfahren für sie allenfalls nur teilweise als anwendbar zu erklären. Eine solche Regulierung hätte den Vorteil, dass die Einführung der Meldepflicht an sektorspezifische Gegebenheiten angepasst werden könnte.

In welchen Sektoren lassen sich Meldepflichten über Bundesgesetzgebung einführen / ausweiten, in welchen nicht?

Sofern und soweit eine Meldepflicht für Sicherheitsvorfälle oder Cyberangriffe zur Wahrung der Landesinteressen sinnvoll und notwendig ist, kann der Bund eine solche gestützt auf seine inhärente verfassungsrechtliche Kompetenz zur Wahrung der inneren und äusseren Sicherheit des Gesamtstaates einführen und in einem bestehenden oder neu erlassenen Bundesgesetz verankern. Der Bund kann gestützt auf die angerufene Querschnittskompetenz auch sektorspezifische Regelungen für Bereiche erlassen, die ansonsten in kantonaler Kompetenz liegen. Dabei kann er nicht nur Vorgaben zum Erlass von "Umsetzungsbestimmungen" machen, sondern auch Dinge direkt selber regeln (z.B. eine Meldepflicht einführen

[122] Vgl. zur Umsetzung der Änderungen mittels Mantelerlass die Botschaft zum Bundesgesetz über die Koordination und Vereinfachung von Entscheidverfahren vom 25. Februar 1998 BBl 1998 2610. Siehe zum Erfordernis der Einheit der Materie bei einem Mantelerlass Urteil BGer 2C_610/2019 vom 18.05.2020. Kritisch zu Mantelerlassen GEORG MÜLLER, Mantelgesetze und Einheit der Materie, in: LeGes 24 (2013) 2. Zum Ganzen: Gesetzestechnische Richtlinien (GTR), Ausgabe 2013, Rz. 278 ff.; Leitfaden für die Ausarbeitung von Erlassen des Bundes (Gesetzgebungsleitfaden) 2019 Rz. 168.
[123] Bundesgesetz vom 6. Oktober 2000über den Allgemeinen Teils des Sozialversicherungsrechtes (ATSG, SR 830.1).
[124] Bundesgesetz vom 22. Juni 2007 über die Eidgenössische Finanzmarktaufsicht (Finanzmarktaufsichtgesetz, FINMAG, SR 956.1).

und die zu meldenden Ereignisse sektorspezifisch festlegen). Da die Kantone zur Umsetzung von Bundesrecht verpflichtet sind (Art. 46 BV), müssten sie ihre kantonale Gesetzgebung im Falle der Einführung einer solchen sektorübergreifenden Meldepflicht auf Bundesebene entsprechend anpassen.

Falls eine Meldepflicht für Cyber- oder Sicherheitsvorfälle sich von ihrer Zielsetzung und Ausgestaltung her nicht auf die inhärente Regelungskompetenz des Bundes zur Wahrung der Landessicherheit stützen lässt, dann wäre ausgehend von der verfassungsrechtlichen Kompetenzordnung konkret zu untersuchen, in welchen Teilsektoren und Branchen der Bund zuständig ist und welche kantonal reguliert werden. Der Bund kann in diesem Fall nur innerhalb seines Zuständigkeitsbereichs gesetzgeberisch tätig werden.

3.4.4 Fragen zu Variante 3

Wie müsste die zentrale Meldestelle rechtlich abgestützt werden, damit sie Meldungen der dezentralen Stellen entgegennimmt?

Falls eine sektorübergreifende Cybermeldestelle eingeführt und beispielsweise vom NCSC betrieben würde, dann könnte die rechtliche Grundlage des NCSC in der Cyberrisikenverordnung weitgehend unverändert beibehalten und allenfalls mit Erlass des Informationssicherheitsgesetzes zusätzlich gesetzlich abgestützt werden.

Es scheint vor diesem Hintergrund unproblematisch, das NCSC zur Entgegennahme der Meldungen von sektoriellen Meldestellen zu verpflichten. Schwieriger dürfte es demgegenüber sein, die sektoriellen Meldestellen in Bereichen, die in kantonale Zuständigkeit fallen, zur Weiterleitung und Zusammenarbeit mit dem NCSC zu verpflichten. Falls sich der Bund für die Einführung der zentralen Meldestelle auf seine inhärente Regelungskompetenz zur Wahrung der Landesinteressen stützt, kann er auch die sektoriellen Meldestellen, die der kantonalen Zuständigkeit unterstehen, zur Zusammenarbeit mit der zentralen Meldestelle verpflichten.

Wie und wo müsste das Verhältnis zwischen den dezentralen und der zentralen Meldestelle geregelt werden?

Es gibt keine zwingende, einzig richtige systematische Platzierung der Regelung über das Verhältnis der zentralen und der dezentralen Meldestellen. Es ist aber auch hier davon auszugehen, dass das Informationssicherheitsgesetz auch dafür der passende Ort wäre.

3.5 Schlussbemerkung

Die vorliegende Rechtsabklärung hat den Charakter einer ersten Einschätzung und erhebt keinen Anspruch auf Vollständigkeit, sondern versteht sich primär als Diskussionsgrundlage. Für gewisse Aussagen in dieser Rechtsabklärung mussten Annahmen getroffen werden, weil keine entsprechenden Informationen verfügbar waren. Weitere Abklärungen wären beispielsweise notwendig, um sich ein genaueres Bild über die Zuständigkeitsordnung in den jeweiligen Teilsektoren machen zu können. Klärungsbedarf besteht auch in Bezug auf die Sektoren-CERTs: zum jetzigen Zeitpunkt ist unklar, in welchen Sektoren bereits Sektoren-CERTs eingeführt wurden, auf welche Rechtsgrundlagen sich diese stützen und wo solche erst geplant sind. Weiterer Klärungsbedarf besteht zudem hinsichtlich der Abgrenzung und Behandlung von Sicherheitsvorfällen und Cyberangriffen.

Bei der Durchsicht der vorhandenen Begriffsdefinitionen fällt auf, dass für den als Präfix genutzten Begriff «Cyber» keine Definition vorliegt, obschon er als Kompositum (Cyber-Angriff,

Cyber-Risiken, Cyber-Kriminalität, Cybervorfall) mehrfach definiert wurde. Bemerkenswert ist in diesem Zusammenhang, dass das Übereinkommen über die Cyberkriminalität vollends auf den Begriff «Cyber» verzichtet (ausser im Titel), dafür aber Definitionen für Computersysteme, Computerdaten, Dienstanbieter und Verkehrsdaten anbietet[125].

Ausgehend von einem weiten Begriff für Cybervorfälle ist anzustreben, die cyberspezifische Meldepflicht auf Cyber*angriffe* - entsprechend dem Aufgabengebiet des NDB - zu beschränken, da Meldungen zu unbeabsichtigten Fehlmanipulationen oder technischen Ausfällen vermutungsweise keinen Erkenntnisgewinn für die Cyberbedrohungslage bringen.

Näher zu prüfen sein wird, ob daneben auch eine Meldepflicht für Sicherheitslücken eingeführt werden soll. Damit Cyberangriffe ausgeführt werden können, sei es versuchsweise oder gar erfolgreich, müssen die betreffenden kritischen Infrastrukturen cybertechnische Schwachstellen haben. Eine Meldepflicht für erhebliche Sicherheitslücken bei kritischen Infrastrukturen könnte für die Abwehr von Cyberangriffen durchaus einen Mehrwert bieten. In Bezug auf eine Meldepflicht für Sicherheitslücken stellen sich aber andere rechtliche und praktische Fragen als bei einer Meldepflicht für Cyberangriffe. Es wird näher zu prüfen sein, ob neben der Meldepflicht für Cyberangriffe auch für Sicherheitslücken eine Meldepflicht oder allenfalls eine freiwillige Meldemöglichkeit für Sicherheitslücken vorgesehen werden soll.

Da Cyberangriffe auf kriminelle Vorgänge zurückzuführen sind, stellt sich natürlich auch die Frage, welche Schnittstellen zwischen der Tätigkeit der Meldestelle und der derjenigen der Strafverfolgungsbehörden bestehen und wie diese gegebenenfalls zu koordinieren wären. In diesem Zusammenhang wäre namentlich zu klären, ob und inwiefern die Meldestelle verpflichtet ist, die eingehenden Meldungen über Cyberangriffe an die (kantonalen) Strafverfolgungsbehörden weiterzuleiten und welcher Mehraufwand und welche möglichen Risiken damit verbunden sind. Zu prüfen wäre ferner, ob es für die Einhaltung der Meldepflicht förderlich wäre, wenn die Weiterleitung an die Strafverfolgungsbehörden nur mit Einverständnis der betroffenen kritischen Infrastrukturen erfolgen würde. Die Frage, ob und wie die Verletzung der neuen Meldepflicht sanktioniert werden soll, soll in diesem Gesamtkontext unter Berücksichtigung aller Interessen eingehend geprüft werden.

[125] Vgl. Art. 1 des Übereinkommens über die Cyberkriminalität, SR 0.311.43.