Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Eidgenössisches Finanzdepartement EFD**

Nationales Zentrum für Cybersicherheit (NCSC)

Bern, 12.01.2022

Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen

# Änderung des Bundesgesetzes über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020

Erläuternder Bericht
zur Eröffnung des Vernehmlassungsverfahrens

Inhaltsverzeichnis

# Übersicht

In den letzten Jahren haben Cybervorfälle bei Privaten, in Unternehmen und auch bei Behörden stark zugenommen, mit teilweise gravierenden Auswirkungen. Der vorliegende Vernehmlassungsentwurf sieht die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen vor. Dank der Meldepflicht können Cyberangriffe frühzeitig entdeckt, ihre Angriffsmuster analysiert und andere Betreiberinnen kritischer Infrastrukturen rechtzeitig gewarnt werden. Die Meldepflicht kann dadurch einen wesentlichen Beitrag zur Erhöhung der Cybersicherheit in der Schweiz leisten.

Der Bundesrat erteilte dem EFD am 11. Dezember 2020 den Auftrag, einen Vernehmlassungsentwurf mit Rechtsgrundlagen für die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen zu erstellen.

Der nun vorliegende Vernehmlassungsentwurf sieht vor, dass die gesetzliche Grundlage für die Meldepflicht ins Informationssicherheitsgesetz (ISG), das am 18. Dezember 2020 vom Parlament verabschiedet wurde, aufgenommen werden soll. Zusätzlich zur Meldepflicht sollen im ISG auch die Aufgaben des nationalen Zentrums für Cybersicherheit (NCSC) und dessen Funktion als Meldestelle verankert werden.

Inhaltlich soll die Meldepflicht nur für Cyberangriffe gelten, die ein gewisses Schadenspotential aufweisen. Sie gilt für Betreiberinnen kritischer Infrastrukturen, worunter jene Prozesse, Systeme und Einrichtungen zu verstehen sind, die essenziell für das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung sind. Die Funktion als zentrale Meldestelle übernimmt das NCSC, das auch freiwillige Meldungen zu Cybervorfällen und Schwachstellen in Informatikmitteln entgegennimmt.

# Erläuternder Bericht

## 1 Ausgangslage

### 1.1 Handlungsbedarf und Ziele

In seinem Bericht vom 13. Dezember 2019 zum Postulat «Meldepflicht von schwerwiegenden Sicherheitsvorfällen bei kritischen Infrastrukturen» stellte der Bundesrat fest, dass es in der Schweiz keine Meldepflicht für Cybervorfälle bei kritischen Infrastrukturen gibt[1] und erteilte dem Nationalen Zentrum für Cybersicherheit (NCSC) den Auftrag, die Einführung einer Pflicht zur Meldung von Cybervorfällen zu prüfen.

Dieser Prüfauftrag war breit abgestützt, etwa durch die Strategien zum Schutz kritischer Infrastrukturen (SKI-Strategie 2018–2022, Massnahme 2) und zum Schutz der Schweiz vor Cyberrisiken (NCS 2018–2022, Massnahme 9) sowie den Expertenbericht zur Zukunft der Datenbearbeitung und Datensicherheit[2]. In den parlamentarischen Debatten zur Totalrevision des Bevölkerungs- und Zivilschutzgesetzes (BZG, Debatte des Nationalrats vom 14.6.2019) und zum Erlass des Informationssicherheitsgesetzes (ISG, Debatte des Nationalrats vom 04.06.2020) wurde die Frage der Meldepflicht ebenfalls aufgegriffen. Nach einer vertieften Abklärung möglicher rechtlicher Grundlagen und insbesondere zur bundesstaatlichen Zuständigkeit[3] erteilte der Bundesrat dem EFD am 11. Dezember 2020 den Auftrag, bis Ende 2021 eine Vernehmlassungsvorlage für die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen auszuarbeiten.

In dieser Vorlage war zu klären, wer welche Art von Angriffen wann wem melden muss. Bei der Klärung dieser Fragen wurde deutlich, dass das 2019 geschaffene Nationale Zentrum für Cybersicherheit (NCSC) – welches in der Vorlage als zentrale Meldestelle für Cyberangriffe vorgesehen ist – nicht über die nötigen gesetzlichen Grundlagen verfügt, um seine Aufgaben als Kompetenzzentrum des Bundes für Cybersicherheit gemäss den Forderungen des Parlaments[4] wahrzunehmen. Mit der Vorlage zur Einführung der Meldepflicht sollen deshalb auch die Aufgaben und Kompetenzen des NCSC auf Gesetzesstufe geregelt werden.

### 1.2 Geprüfte Alternativen und gewählte Lösung

#### 1.2.1 Ausbau des freiwilligen Informationsaustausches

In der Schweiz ist der Informationsaustausch zwischen kritischen Infrastrukturen und dem Bund gut etabliert. Kritische Infrastrukturen tauschen sich seit 2004 mit der damaligen Melde- und Analysestelle für Informationssicherheit (MELANI) und heute mit dem NCSC aus. Dieses Modell stösst jedoch zunehmend an Grenzen. Damit ein freiwilliger Austausch funktioniert, braucht es ein gut etabliertes Vertrauensverhältnis zwischen allen Beteiligten. Ein solches lässt sich aufbauen, wenn die Anzahl der Beteiligten überschaubar ist und die Möglichkeit besteht, sich regelmässig direkt auszutauschen. In der heutigen Lage, bei der Cyberangriffe zu einer Bedrohung für eine Vielzahl von Unternehmen in den kritischen Sektoren geworden sind, kann nicht mehr gewährleistet werden, dass zu allen relevanten Akteuren eine ausreichende Vertrauensbasis hergestellt werden kann. In

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).
2 Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit vom 17. August 2018 (Empfehlung 28). Die Expertengruppe wurde vom EFD in Umsetzung der Motion Rechsteiner (13.3841) «Expertenkommission zur Zukunft der Datenbearbeitung und Datensicherheit» am 27. August 2015 mit Befristung auf drei Jahre eingesetzt.
3 Vgl. Bericht «Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen, Rechtliche Grundlagen» vom 25. November 2020, Beilage 01 zum BRA vom 11.12.2020.
4 17.3508 Mo. Eder «Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund».

der Konsequenz hat sich der Informationsaustausch über die letzten Jahre so entwickelt, dass mit einigen Unternehmen und Organisationen die etablierte Zusammenarbeit weiterhin gut funktioniert, eine Ausweitung dieses Modells aber nicht mehr realistisch ist.

Beim Meldeeingang kann dieser Fokus auf wenige Unternehmen zu einem unvollständigen oder gar verzerrten Lagebild führen. Es kann nicht festgestellt werden, welche Cyberbedrohung in der Schweiz welche Breitenwirkung entfacht. Zusätzlich führt der freiwillige Austausch auch zu falschen Anreizen. Unternehmen, welche sich nicht am Austausch beteiligen, erhalten dank der Meldung anderer Firmen trotzdem Warnungen und technische Hinweise, da das NCSC Betreiberinnen von kritischen Infrastrukturen solche wichtigen Hinweise nicht vorenthalten kann. Es besteht dadurch die Gefahr, dass es für Unternehmen einfacher ist, sich darauf zu verlassen, wichtige Meldungen ohnehin zu erhalten, statt sich aktiv am Informationsaustausch zu beteiligen.

Insgesamt ist also die Einführung einer Meldepflicht der Weiterführung des freiwilligen Informationsaustausches vorzuziehen, weil sie eine vollständigere Lageübersicht zulässt und sicherstellt, dass niemand sich der Pflicht zur gegenseitigen Frühwarnung entziehen kann. Dennoch soll die über den Informationsaustausch entwickelte Kultur der Zusammenarbeit und des gegenseitigen Vertrauens weitergeführt werden. Entscheidend dabei ist, dass den Unternehmen und Organisationen über die Einführung der Meldepflicht auch ein Mehrwert entsteht.

### 1.2.2 Verhältnis zu anderen Meldepflichten und Informationsaustausch unter den Behörden

Die Einführung einer Meldepflicht für Cyberangriffe tangiert bereits bestehende Meldepflichten und führt zur Frage, wie und wann die beim NCSC eingegangenen Meldungen an andere Behörden weitergeleitet werden können.

Beim Verhältnis zu bereits bestehenden Meldepflichten wurde überprüft, ob es möglich ist, die Meldepflicht für Cyberangriffe in diesen zu verankern und darauf zu verzichten, eine sektorübergreifende Meldepflicht einzuführen. Diese Variante wurde verworfen, da die Regelungen zu Sicherheitsvorfällen in den verschiedenen Sektoren uneinheitlich sind und teilweise gar keine solchen bestehen. Wenn an einer Meldepflicht für Cyberangriffe gegenüber einer zentralen Meldestelle festgehalten wird, muss jedoch geklärt werden, welche Meldungen wann bei wem erfasst werden müssen. Hier gilt, dass die Meldepflicht für Cyberangriffe die bestehenden Meldepflichten nicht ersetzt, sondern nur ergänzt. Gleichzeitig wurde darauf geachtet, dass die gesetzlichen Grundlagen eine gleichzeitige Erfüllung verschiedener Meldepflichten erlauben. Der Aufwand für die Erfüllung der verschiedenen Meldepflichten soll so möglichst geringgehalten werden. Dies gilt vor allem, aber nicht nur für das Verhältnis zur datenschutzrechtlichen Meldepflicht nach Artikel 24 des revidierten Datenschutzgesetzes (nachfolgend: nDSG)[5], da es in der Praxis häufig der Fall ist, dass Cyberangriffe zu Datenverlusten führen. Die gewählte Lösung sieht vor, dass es den Meldenden offensteht, die Meldung des Cyberangriffs gleichzeitig mit der Übermittlung an das NCSC anderen Meldestellen weiterzuleiten, um damit anderweitige Meldepflichten zu erfüllen. Umgekehrt wird das NCSC auch Meldungen zu Cyberangriffen entgegennehmen, welche in Erfüllung einer anderweitigen Meldepflicht abgegeben wurden, sofern sie die benötigten Inhalte umfasst. Damit soll verhindert werden, dass Betroffene den gleichen Vorfall unterschiedlichen Stellen über unterschiedliche Verfahren melden müssen.

Klärungsbedürftig ist in diesem Zusammenhang auch der Informationsaustausch zwischen den Behörden. Wenn Unternehmen und Organisationen dem NCSC freiwillig oder in Erfüllung der Meldepflicht Cyberangriffe melden, müssen sie Klarheit darüber haben, was mit ihrer Meldung geschieht und wer darüber in Kenntnis gesetzt wird. Auch in dieser Hinsicht sollen die Grundsätze aus dem bisherigen Informationsaustausch beibehalten werden. Eine Weiterleitung von Meldungen oder Teilen davon erfolgt nur mit Einverständnis der Betreiberin der betroffenen kritischen Infrastruktur oder anonymisiert.

Die Weitergabe von Informationen, die Rückschlüsse auf die Meldenden oder Betroffenen erlauben, soll dem NCSC jedoch in zwei Fällen auch ohne deren Einverständnis erlaubt sein. Erstens ist eine Weiterleitung an die Strafverfolgungsbehörden möglich, wenn die Meldung Informationen über eine

5 Bundesgesetz vom 25. September 2020 über den Datenschutz (Datenschutzgesetz, DSG, SR **235.1**), BBl 2020 7639.

schwere Straftat enthält. Zwar ist das NCSC von der Anzeigepflicht gemäss Artikel 22*a* des Bundespersonalgesetzes vom 24. März 2000[6] ausgenommen, die Leiterin oder der Leiter des NCSC kann aber Informationen an Strafverfolgungsbehörden weiterleiten, wenn sie oder er zum Schluss kommt, dass dies auf Grund der Schwere der Straftat nötig ist. Die Weiterleitung an die Strafverfolgungsbehörden wird keine strafrechtlichen Konsequenzen für die Betreiberin der kritischen Infrastruktur haben, da sich das Strafverfahren in der Regel ausschliesslich gegen die Angreifer richten wird. Sollte die Betreiberin der kritischen Infrastruktur ausnahmsweise selber Gegenstand der Strafverfolgung werden, so darf die Meldepflicht nicht dazu führen, dass sie sich durch die Meldung selber belasten muss. Es wurde daher eine Bestimmung aufgenommen, um dem Selbstbelastungsverbot als zentralem Grundsatz der Strafverfolgung Rechnung zu tragen. Vorbild dafür war die Regelung, die für die Meldepflicht bei Verletzungen der Datensicherheit im revidierten Datenschutzrecht vorgesehen ist (vgl. Art. 24 Abs. 6 nDSG).

Der zweite Fall einer zulässigen Weiterleitung betrifft Informationen, welche für den Nachrichten dienst des Bundes (NDB) für seine Aufgaben der frühzeitigen Erkennung und Verhinderung von Bedrohungen der inneren oder äusseren Sicherheit, für die Beurteilung der Bedrohungslage oder für die nachrichtendienstliche Frühwarnung zum Schutz von kritischen Infrastrukturen nach Artikel 6 Absatz 1 Buchstabe a, Absatz 2 und 5 des Nachrichtendienstgesetzes vom 25. September 2015 (NDG)[7] relevant sind. Dadurch ist sichergestellt, dass der NDB als zuständige Behörde für die Frühwarnung von kritischen Infrastrukturen und für die Einschätzung der Bedrohungslage die nötigen Informationen erhält.

### 1.2.3 Durchsetzung der Meldepflicht mittels Anreizen und Sanktionen

Direkt verbunden mit der Einführung der Meldepflicht ist die Frage, über welche Instrumente sie durchgesetzt werden soll. Die Bereitschaft, der Meldepflicht nachzukommen, kann durch drei Faktoren beeinflusst werden.

Erstens muss es so einfach wie möglich sein, die Meldung zu verfassen. Dies wird sichergestellt, indem das NCSC ein elektronisches Meldeformular zur Verfügung stellt, über welches die Meldung rasch erfasst und einfach übermittelt werden kann.

Zweitens braucht es positive Anreize für die Meldung. Diese bestehen in erster Linie in der durch das NCSC angebotenen technischen Einschätzung und Unterstützung bei der Bewältigung des Angriffs. Diese sollen im Sinne einer ersten Hilfe erfolgen und nur soweit gehen, dass sie nicht in Konkurrenz stehen zu Dienstleistungen, die am Markt erhältlich sind. Für Betreiberinnen kritischer Infrastrukturen kann es aber sehr wertvoll sein, wenn eine Bundesstelle mit Überblick über die Gesamtbedrohungslage ihnen bei der ersten Einschätzung hilft und sie bei der Umsetzung von Sofortmassnahmen unterstützt.

Der dritte Faktor zur Durchsetzung der Meldepflicht besteht in negativen Anreizen in Form einer Busse. Wenn es trotz Rücksprache mit der kritischen Infrastruktur zu einer Verletzung der Melde- oder Auskunftspflicht kommen sollte, besteht die Möglichkeit, dass das NCSC als ultima ratio eine Verfügung mit Bussandrohung erlässt. Die Obergrenze der Busse liegt bei 100'000 Franken, wobei sie bis zu 20'000 Franken direkt dem Geschäftsbetrieb auferlegt werden kann, welcher die kritische Infrastruktur betreibt. Als Vorlage für diese verwaltungsrechtliche Sanktionsmöglichkeit diente das revidierte Datenschutzgesetz, das in Artikel 63 f. eine ähnliche Regelung für den Fall einer Missachtung von Verfügungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) enthält.

Aufgrund der langbewährten Zusammenarbeit mit den kritischen Infrastrukturen geht das NCSC davon aus, dass diese Bestimmung weitgehend symbolischen Charakter hat und in erster Linie dazu dient, der Meldepflicht die nötige Beachtung zu verschaffen.

6 SR **172.220.1**
7 SR **121**

### 1.3 Verhältnis zur Legislaturplanung und zur Finanzplanung sowie zu Strategien des Bundesrates

Die Vorlage wurde in der Botschaft vom 29. Januar 2020 zur Legislaturplanung 2019–2023[8] und im Bundesbeschluss vom 21. September 2020 über die Legislaturplanung 2019–2023[9] angekündigt. In der Botschaft LP wurde insbesondere auf die Notwendigkeit hingewiesen, Cybervorfälle bei kritischen Infrastrukturen rasch erkennen und bewältigen zu können und die IKT-Resilienz zu erhöhen. In Artikel 19 des Bundesbeschlusses LP steht als Ziel 18: «Der Bund tritt Cyberrisiken entgegen und unterstützt und ergreift Massnahmen, um die Bürgerinnen und Bürger sowie die kritischen Infrastrukturen zu schützen». In der Botschaft sowie im Bundesbeschluss zur Legislaturplanung wird auf die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–2022 vom 18. April 2018 und den dazugehörigen Umsetzungsplan verwiesen.

Im Voranschlag 2022 mit integriertem Aufgaben- und Finanzplan 2023-2025 wird die Verbesserung der Cybersicherheit im Bund und in der Schweiz als strategischer Schwerpunkt definiert und die Meldepflicht als Geschäft aufgeführt. Es wird festgehalten, dass das NCSC einen Mehrwert zum Schutz vor Cyberrisiken in der Schweiz leiste[10].

In der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken 2018–2022 werden die Abklärungen sowie der Entscheid über die Einführung der Meldepflicht für Cyberangriffe in Massnahme 9 aufgeführt. Diese Massnahme 9 wird mit der vorliegenden Vernehmlassungsvorlage vollständig umgesetzt[11].

8 BBl 2020 1777, hier 1866.
9 BBl 2020 8385, hier 8392.
10 Voranschlag 2022 mit IAFP 2023–2025, Band 2B, S. 11 ff., abrufbar unter: «www.efv.admin.ch > Finanzberichte > Finanzberichte > Voranschlag mit integriertem Aufgaben- und Finanzplan» https://www.efv.admin.ch/dam/efv/de/dokumente/Finanzberichte/finanzberichte/va_iafp/2022/va2b-2022.pdf.download.pdf/VA2B-6-8-d.pdf.
11 Vgl. Bericht zum Umsetzungsstand der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022 vom August 2021, S. 10, 15 f. (: «www.ncsc.admin.ch > NCSC Strategie > Berichte und Studien» https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/strategie/Bericht-Umsetzungsstand_NCS_2021_DE.pdf.download.pdf/Bericht-Umsetzungsstand_NCS_2021_DE.pdf).

## 2 Rechtsvergleich, insbesondere mit dem europäischen Recht

Seit der Verabschiedung der EU-Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) im Juli 2016 sind EU-Mitgliedsstaaten verpflichtet, eine Meldepflicht für Cybervorfälle umzusetzen. Die Frist für die Umsetzung ist im Mai 2018 abgelaufen. Die Meldepflicht betrifft «Anbieter wesentlicher Dienste», worunter gemäss Artikel 4 private Unternehmen oder öffentliche Einrichtungen fallen, die in den Bereichen Gesundheitswesen, Verkehr, Energie, Banken und Finanzmarktinfrastrukturen, digitale Infrastruktur und Wasserversorgung eine wichtige Rolle bei der Gewährleistung der Sicherheit spielen[12]. Der Adressatenkreis entspricht damit weitegehend den in der Vernehmlassungsvorlage definierten meldepflichtigen kritischen Infrastrukturen.

In Bezug auf den Umfang der Meldepflicht lässt die NIS-Richtlinie den Mitgliedstaaten der EU relativ viel Spielraum offen. Meldepflichtig sind gravierende Vorfälle, wobei Artikel 14 festhält, dass bei der Beurteilung insbesondere die Zahl der betroffenen Nutzer, die Dauer des Sicherheitsvorfalls und die geografische Ausbreitung zu berücksichtigen sind. Im Unterschied zur erarbeiteten Vernehmlassungsvorlage beschränkt sich die NIS-Richtlinie jedoch nicht auf die Einführung einer Meldepflicht. Sie verpflichtet die Anbieter wesentlicher Dienste zugleich dazu, Sicherheitsvorkehrungen zu ergreifen. Dazu gehören die Risikovorsorge, die Gewährleistung der Sicherheit von Netz- und Informationssystemen und Massahmen, welche die Auswirkungen von Sicherheitsvorfällen so gering wie möglich halten (Art. 14).

Die Vernehmlassungsvorlage beschränkt sich darauf, die gesetzlichen Grundlagen für solche Anforderungen im Stromsektor zu schaffen. Eine durch das Bundesamt für Energie (BFE) beauftragte Studie hat in diesem für die wirtschaftliche Versorgung und die Sicherheit des Landes entscheidenden Sektor einen hohen Handlungsbedarf bei der Cybersicherheit festgestellt.[13] In den übrigen Sektoren muss zunächst geklärt werden, ob der Bund die Kompetenz hat, rechtsverbindliche Normen für die Cybersicherheit festzulegen und in welchen Bereichen welche Anforderungen gestellt werden sollen.

12 RICHTLINIE (EU) 2016/ 1148 DES EUROPÄISCHEN PARLAMENTS UND DES RATES - vom 6. Juli 2016 - über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (europa.eu).

13 Strategie Cyber Security für die Schweizer Stromversorgung vom 28. Juni 2021, «Strategie Cyber Security für die Schweizer Stromversorgung vom 28. Juni 2021, www.bfe.admin.ch > Versorgung > Digitalisierung im Energiesektor» https://www.bfe.admin.ch/bfe/de/home/news-und-medien/publikationen.exturl.html/aHR0cHM6Ly9wdWJkYi5iZmUuYWRtaW4uY2gvZGUvcHVibGljYX/Rpb24vZG93bmxvYWQvMTA1MjQ=.html.

# 3 Grundzüge der Vorlage

## 3.1 Die beantragte Neuregelung

Das Hauptmotiv für die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen ist bei der Frühwarnung und bei der besseren Übersicht zur Bedrohungslage zu verorten. Da Angreifer oft mehrmals ähnliche Vorgehensweisen und Angriffsmuster für mehrere kritische Infrastrukturen in verschiedenen Sektoren verwenden, kann die Meldepflicht wesentlich dazu beitragen, durch frühzeitiges Erkennen der Angriffsmethoden und entsprechende Warnungen die Cybersicherheit von kritischen Infrastrukturen zu stärken.

Die Meldepflicht umfasst nur Cyberangriffe, die ein erhebliches Schadenspotenzial aufweisen. Nicht meldepflichtig sind Cybervorfälle, die auf menschliches Fehlverhalten, also beispielsweise eine unbeabsichtigte fehlerhafte Manipulation eines Mitarbeiters, zurückzuführen sind. Schliesslich wurde auch davon abgesehen, die Meldepflicht auf Schwachstellen in Informatikmitteln auszudehnen. Unabhängig von der Einführung der Meldepflicht für Cyberangriffe ist es weiterhin möglich, Meldungen zu Cybervorfällen und Schwachstellen freiwillig zu melden. Diese Möglichkeit steht jeder Person offen und ist nicht auf kritische Infrastrukturen beschränkt.

Mit der Einführung der Meldepflicht für Cyberangriffe werden gleichzeitig die Aufgaben des NCSC auf Gesetzesstufe geregelt, welche aktuell nur in der Cyberrisikenverordnung (CyRV)[14] definiert sind. Dies ist einerseits nötig, da das NCSC die Funktion der Meldestelle übernimmt. Andererseits wird mit dieser der Neuorganisation der Bundesverwaltung im Bereich Cybersicherheit Rechnung getragen, insbesondere der Gründung des NCSC, die erst während der parlamentarischen Debatten zum ISG erfolgte.

## 3.2 Abstimmung von Aufgaben und Finanzen

Das NCSC führt bereits heute eine Anlaufstelle, welche auf freiwilliger Basis Meldungen zu Cybervorfällen entgegennimmt. Es baut dabei auf die langjährige Erfahrung von MELANI auf, welche diese Aufgabe seit 2004 für Meldungen von kritischen Infrastrukturen und aus der Bevölkerung ausgeführt hat.

Das NCSC nutzt für die Entgegennahme von Meldungen ein elektronisches Meldeformular. Dieses lässt sich so anpassen, dass es auch für die Entgegennahme von Meldungen in Erfüllung der Meldepflicht verwendet werden kann. Für die nötigen Abstimmungen mit anderen Stellen, welche ebenfalls Meldungen entgegennehmen (z.B. EDÖB, FINMA, ENSI), und für die Konfiguration des Meldeformulars fällt ein Initialaufwand an, der jedoch über die bestehenden Ressourcen des NCSC aufgefangen werden kann. Für die Umsetzung der Vorlage muss das NCSC jedoch sicherstellen können, dass die in Erfüllung der Meldepflicht eingegangenen Meldungen korrekt erfasst, quittiert und dokumentiert werden und die Meldung zum Zweck der Frühwarnung an die richtigen Stellen weitergeleitet werden. Dieser zusätzliche Aufwand muss beim weiteren Ausbau des NCSC berücksichtigt werden.

Nach einem Cyberangriff wird das NCSC die betroffene kritische Infrastruktur bei der Vorfallbewältigung unterstützen. Auch diese Unterstützungsleistung ist dank der langjährigen Erfahrung des NCSC (und früher von MELANI) bereits gut eingespielt. Dennoch ist zu erwarten, dass sich der Aufwand für das NCSC durch die Einführung der Meldepflicht erhöhen wird. Erstens ist damit zu rechnen, dass mehr Meldungen eingehen und zweitens ist das NCSC neu in der Pflicht, mindestens eine erste Einschätzung und Empfehlungen zur Bewältigung des Vorfalls abzugeben. Das technische Analyseteam des NCSC (GovCERT) muss deshalb ebenfalls weiter ausgebaut werden.

14 SR **120.73**

## 3.3 Umsetzungsfragen

### 3.3.1 Notwendigkeit einer gesetzlichen Grundlage

Aus dem Legalitätsprinzip (Art. 5 Abs. 1 der Bundesverfassung, BV[15]) und den Bestimmungen zur Gesetzgebung von Artikel 164 Absatz 1 BV ergibt sich, dass die Meldepflicht für Cyberangriffe mindestens in den Grundzügen auf Gesetzesebene zu regeln ist. Entsprechend enthält die Vernehmlassungsvorlage die wesentlichen Elemente der Meldepflicht für Cyberangriffe. Dazu zählen der Auslöser und Umfang der Meldepflicht (Cyberangriffe mit Schadenspotential), der Adressatenkreis der Meldepflichtigen (Betreiberinnen kritischer Infrastrukturen, die in bestimmten Bereichen tätig sind), der Inhalt der Meldungen sowie deren Verwendung durch das NCSC. Die Meldepflicht stellt für die meldepflichtigen Betreiberinnen kritischen Infrastrukturen einen Eingriff in Rechte von Privaten oder, bei kantonaler oder kommunaler Trägerschaft, in deren föderalistische Autonomie dar. Die Meldepflicht ist aber nicht ein Eingriff von grosser Tragweite und hat kaum finanzielle Auswirkungen auf die betroffenen Unternehmen.

### 3.3.2 ISG als geeignete Rechtsgrundlage

Im Rahmen der Vorarbeiten wurde geprüft, ob die neuen Regelungen in einem eigenständigen Gesetz oder in einen bestehenden Erlass eingefügt werden sollen, dessen Zweck, Gegenstand und Anwendungsbereich mit einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen vereinbar ist[16]. Für die Verankerung der Meldepflicht kamen als gesetzliche Grundlagen insbesondere Erlasse in Betracht, die bereits Bestimmungen zum Schutz kritischer Infrastrukturen enthielten und den Schutz der öffentlichen Ordnung im Fokus hatten (BZG[17], LVG[18], BWIS[19], NDG und ISG[20]). Nach eingehender Prüfung erwies sich von diesen Erlassen nur das ISG als passendes Gefäss. Sein Ziel, die Sicherheit für die vom Bund bearbeiteten Informationen und eingesetzten Informatikmittel zu gewährleisten, hat einen direkten Bezug zur Cybersicherheit (obwohl das Gesetz den Begriff nicht verwendet). Dazu kommt, dass im ISG bereits Bestimmungen zur Unterstützung für kritische Infrastrukturen durch den Bund vorgesehen waren. Dieser Teil des Aufgabenbereichs des NCSC war damit bereits gesetzlich verankert. Damit war das ISG nicht nur geeignet, sondern eine ideale Basis, um die Meldepflicht für Cyberangriffe zu verankern. Dafür spricht auch, dass in den parlamentarischen Beratungen zum Gesetzesentwurf die Einführung einer Meldepflicht für KI-Betreibende bei «erheblichen Vorfällen» diskutiert, aber im Juni 2020 von der Mehrheit des Nationalrats jedoch abgelehnt wurde, nachdem der Bundesrat darauf hingewiesen hat, dass dazu eine Vorlage erarbeitet werden wird.

### 3.3.3 Ausführungsbestimmungen

Die gesetzlichen Vorgaben werden durch eine Verordnung konkretisiert. Diese wird die Aufgaben des NCSC und die Zusammenarbeit mit weiteren Stellen genauer umschreiben und präzisieren, wer wann welche Cyberangriffe über welche Verfahren zu melden hat. Die Verordnung wird jene Bestimmungen der heutigen CyRV integrieren, welche das Verhältnis des Bundes zur Öffentlichkeit und insbesondere zu den Betreiberinnen kritischer Infrastrukturen betreffen. Bei den Bestimmungen zum Adressatenkreis ist jeweils zu prüfen, ob eine Präzisierung in der Verordnung zur Meldepflicht oder in sektorspezifischen Verordnungen zu bevorzugen ist.

15 SR **101**
16 Vgl. Bericht «Meldepflicht für schwerwiegende Sicherheitsvorfälle bei kritischen Infrastrukturen, Rechtliche Grundlagen» vom 25. November 2020, Beilage 01 zum BRA vom 11.12.2020.
17 SR **520.1**
18 SR **531**
19 SR **120**
20 Bundesgesetz vom 18. Dezember 2020 über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG), BBl *2020* 9975.

### 3.3.4 Vollzugstauglichkeit der Meldepflicht

Das NCSC hat im April 2021 unter Betreiberinnen kritischer Infrastrukturen und Behörden eine Umfrage zur geplanten Einführung einer Meldepflicht für Cyberangriffe durchgeführt. Diese hat ergeben, dass die Akzeptanz gegenüber einer Meldepflicht grundsätzlich hoch ist, wenn es gelingt, diese so umzusetzen, dass ein geringer bürokratischer Aufwand entsteht. Abbildung 1 verdeutlicht die hohe grundsätzliche Zustimmung der Befragten.

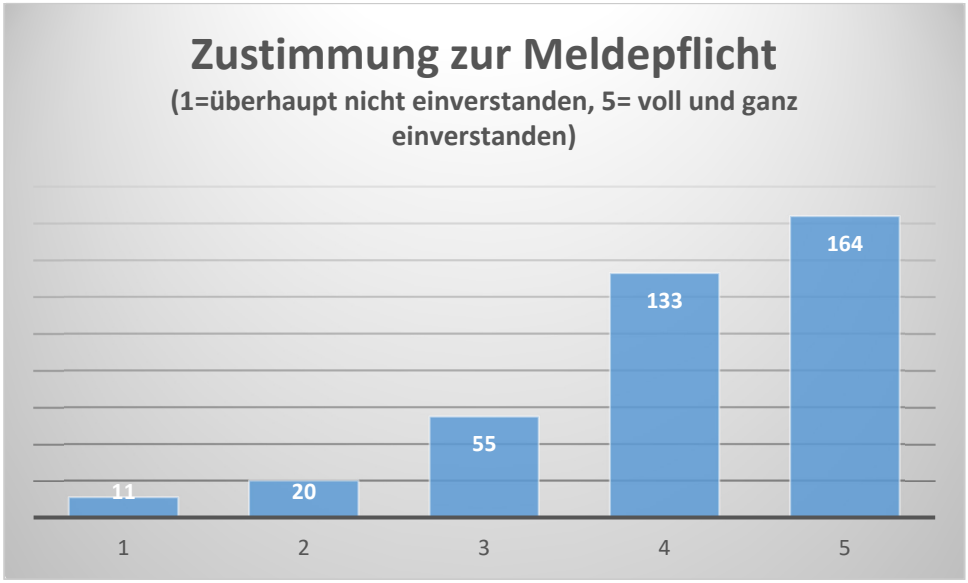


*Abbildung 1 Beurteilung der Meldepflicht*

Ein Cyberangriff auf eine kritische Infrastruktur kann neben der Meldepflicht an das NCSC weitere meldepflichtige Vorgänge betreffen und damit gleichzeitig mehrere Meldepflichten auslösen. Es sind beispielsweise folgende Überschneidungen denkbar:

- Für kritische Infrastrukturen, die im Finanzmarktsektor unter der Aufsicht der FINMA tätig sind, gilt bereits seit Mai 2020 eine Meldepflicht für Cybervorfälle gegenüber der FINMA[21]. Damit wird ein Cyberangriff in aller Regel sowohl der FINMA wie auch dem NCSC zu melden sein.

- Ein Cyberangriff auf eine kritische Infrastruktur kann zu einer Verletzung der Datensicherheit, die je nach Schwere der Verletzung gegenüber dem EDÖB meldepflichtig ist[22].

- Löst ein Cyberangriff Funktionsstörungen bei der kritischen Infrastruktur aus, z.B. einen radioaktiven Vorfall in einer Kernanlage, dann ist dieser Störfall ebenfalls meldepflichtig (ENSI, NAZ usw.).

Die neu einzuführende Meldepflicht für Cyberangriffe wird die bestehenden Meldepflichten nicht ersetzen; letztere gelten unverändert weiter. Deshalb ist es wichtig, dass der Aufwand für die Meldepflichtigen auch dann vertretbar ist, wenn sie gleichzeitig weitere Meldepflichten erfüllen müssen. Aus diesem Grunde wird das NCSC ein System für die elektronische Erfassung der Meldung zur Verfügung stellen (Formular, Meldemaske oder Ähnliches). Die Meldepflichtigen können selber entscheiden, ob sie die elektronisch erfasste Meldung mit möglichen Zusatzangaben an weitere Meldestellen schicken wollen. Sofern andere Meldestellen Hand bieten, könnte die Erfassung der Meldung auch so gegliedert werden, dass neben den allgemeinen Angaben zur kritischen Infrastruktur

21 Vgl. Artikel 29 FINMAG. Die allgemeine Meldepflicht umfasst auch Cybervorfälle (vgl. FINMA, Aufsichtsmitteilung 05/2020 vom 7.Mai 2020).
22 Artikel 24 nDSG.

die spezifischen Angaben für die Erfüllung der jeweiligen Meldepflicht nur für die betreffende Meldestelle bestimmt wären. Meldepflichtige würden mit der Erfassung und Weiterleitung steuern, welche Meldestelle welche Angaben erhält.

# 4 Erläuterungen zu einzelnen Artikeln

Die gesetzlichen Grundlagen der Meldepflicht für Cyberangriffe, sollen – abgesehen von wenigen Anpassungen im 1. Kapitel – im 5. Kapitel des ISG eingefügt werden. Das 5. Kapitel wurde grundlegend überarbeitet, um darin auch die Aufgaben des NCSC – die über die Meldepflicht hinausgehen und nicht spezifisch auf kritische Infrastrukturen ausgerichtet sind – aufnehmen zu können. Entsprechend wurde auch die Kapitelüberschrift angepasst («5. Kapitel: Massnahmen des Bundes zum Schutz der Schweiz vor Cyberrisiken»).

Die wesentlichen Regelungsinhalte der gesetzlichen Bestimmungen wurden in der Botschaft zum ISG (BBl 2017 3062 ff.) und unter den vorstehenden Ziffern teilweise bereits ausführlich beschrieben und begründet. Die Kommentierung der nachfolgende Artikel beschränkt sich daher auf Ergänzungen dazu.

### *1. Kapitel: Allgemeine Bestimmungen*

Im ersten Kapitel betreffen die Anpassungen nur die Artikel 1, 2 und 5. Die restlichen Artikel wurden nicht verändert.

#### *Artikel 1 Zweck*

Der Zweckartikel des ISG wurde in Absatz 1 ergänzt und zu diesem Zweck eine Unterteilung in Buchstabe a und b vorgenommen. In Buchstabe a wurde die ursprüngliche Formulierung übernommen, während in Buchstabe b die Zweckbestimmung in Bezug auf Cyberrisiken ergänzt wurde. Diese erweiterte Zweckbestimmung dient dazu, den durch die Einführung einer Meldepflicht für Cyberangriffe und der gesetzlichen Regelung der Aufgaben des NCSC eingefügten Aspekte Rechnung zu tragen.

#### *Artikel 2 Verpflichtete Behörden und Organisationen*

Hier wurde der Verweis in Absatz 5 auf die Bestimmungen, die für kritische Infrastrukturen gelten, angepasst, da Kapitel 5 neu mit Artikel 73*a* beginnt und mit Artikel 79 aufhört. Es wurde keine inhaltliche Anpassung dieses Artikels vorgenommen.

#### *Artikel 5 Begriffe*

Die Begriffsdefinitionen in Buchstabe a, b und c wurden nicht verändert.

#### *Buchstabe d*

Die neu aufgenommene Definition von «Cybervorfall» wurde aus Artikel 3 Buchstabe b CyRV übernommen und leicht angepasst. Die Definition umfasst auch den Missbrauch von Informatikmitteln, wie dies z.B. bei Phishing-Versuchen der Fall ist.

#### *Buchstabe e*

Neu definiert wurde der Begriff «Cyberangriff», der eine mögliche Erscheinungsform des Cybervorfalls darstellt. Der Begriff «Cyberangriff» ist als Abgrenzung zum Oberbegriff «Cybervorfall» deshalb von Bedeutung, weil nur die Angriffe auf kritische Infrastrukturen meldepflichtig sind, während Cybervorfälle und Schwachstellen freiwillig und von jeder Person gemeldet werden können.

### *5. Kapitel: Massnahmen des Bundes zum Schutz der Schweiz vor Cyberrisiken*

Im zweiten, dritten und vierten Kapitel wurden keine Anpassungen vorgenommen. Im fünften Kapitel wurden neben der Meldepflicht für Cyberangriffe auf kritische Infrastrukturen auch grundsätzliche

Bestimmungen zu den Aufgaben des NCSC aufgenommen. Zur besseren Übersicht wurde das 5. Kapitel daher neu in 3 Abschnitte gegliedert.

### *1. Abschnitt: Allgemeine Bestimmungen*

### *Artikel 73a Grundsatz*

In diesem Artikel werden die Aufgaben des NCSC unter Buchstabe a bis f beschrieben. Es handelt sich um eine nicht abschliessende Aufzählung. Im Zusammenhang mit der Entgegennahmen und Bearbeitung von Meldungen (Buchstabe e) ist zu präzisieren, dass es hier sowohl um die freiwilligen Meldungen zu Cybervorfällen und Schwachstellen geht wie auch um die Meldungen zu Cyberangriffe auf kritische Infrastrukturen, die meldepflichtig sind.

Die einzelnen Aufgaben sowie die Zusammenarbeit mit Behörden im In- und Ausland bilden Gegenstand von weiteren Artikeln, die deren Inhalt konkretisieren.

### *Artikel 73b Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen*

Das NCSC betreibt seit dem 1. Januar 2020 eine nationale Anlaufstelle für Cyberrisiken (vgl. Art. 12 Abs. 1 Bst. a CyRV), die Meldungen zu Cybervorfällen und Schwachstellen erfasst und bearbeitet. Die Meldestelle des NCSC wurde auf der Grundlage von MELANI aufgebaut, welche seit 2004 Meldungen entgegennimmt. Die Meldestelle des NCSC wird von Unternehmen und Bevölkerung rege genutzt. Im Jahr 2020 gingen 10'834 Meldungen bei ihr ein[23].

Das NCSC wurde am 28. September 2021 Teil des weltweiten Netzwerks zur Verwaltung von Schwachstellen in Informatiksystemen und ist seither berechtigt, den gemeldeten Schwachstellen eine eindeutige Identifikationsnummer gemäss internationalem Referenzsystem zu vergeben[24]. Es ist deshalb wichtig zu präzisieren, dass das NCSC neben Meldungen zu Cybervorfällen auch solche zu Schwachstellen entgegennimmt.

#### *Absatz 1*

Cybervorfälle und Schwachstellen können dem NCSC nicht nur von den Betroffenen selber, sondern auch von Dritten – und falls gewünscht auch anonym – gemeldet werden. Das NCSC analysiert die Vorfälle und beurteilt, welche Bedeutung sie für den Schutz der Schweiz vor Cyberrisiken haben. Sofern die Meldungen nicht anonym erfolgen, kann das NCSC auf Wunsch der Meldenden basierend auf diesen Analysen auch Einschätzungen zum Vorfall und Empfehlungen für das weitere Vorgehen abgeben. Zudem verwendet das NCSC die Meldungen für statistische Zwecke und für die Warnung der Öffentlichkeit vor Cyberbedrohungen. Dabei werden keine Angaben der Meldenden oder der Betroffenen publiziert.

Das NCSC behandelt die Meldungen vertraulich. Diese Vertraulichkeit der Meldungen ist eine wichtige Voraussetzung, damit überhaupt Meldungen eingehen und der Meldestelle Vertrauen entgegengebracht wird.

#### *Absatz 2*

Das NCSC kann Informationen zu Cybervorfällen veröffentlichen oder an interessierte Behörden und Organisationen weiterleiten, sofern die Informationen keine Personendaten oder Daten juristischer Personen enthalten. Eine Veröffentlichung von Personendaten im Falle von Cybervorfällen ist ausgeschlossen. Weiterhin möglich ist die Veröffentlichung von Informationen aus der Meldung mit Zustimmung der betroffenen Person oder Organisation, wie beispielsweise im Falle des Missbrauchs von Logos bei Phishing-Angriffen.

23 Vgl. Bericht zum Umsetzungsstand der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022, verfasst im August 2021, S. 5 («www.ncsc.admin.ch > NCSC Strategie > Berichte und Studien» https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/strategie/Bericht-Umsetzungsstand_NCS_2021_DE.pdf.download.pdf/Bericht-Umsetzungsstand_NCS_2021_DE.pdf).

24 Vgl. Medienmitteilung des NCSC vom 28. September 2021: «www.ncsc.admin.ch > Dokumentation > Medienmitteilungen > Newslist > NCSC ist neu Teil des weltweiten Netzwerks zur Verwaltung von Schwachstellen in Informatiksystemen» https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/medienmitteilungen/newslist.msg-id-85280.html.

### *Absatz 3*

Bei Schwachstellen hingegen kann die schnelle Veröffentlichung der Schwachstelle mit Nennung der betroffenen Soft- oder Hardware notwendig sein, um weitere Cyberangriffe zu verhindern. Das Ausnutzen von Schwachstellen ist eine der häufigsten Vorgehensweisen bei Cyberangriffen. Nur mit diesen Informationen ist es den Nutzenden der Soft- oder Hardware möglich, umgehend die nötigen Massnahmen zum Schutz vor Cyberangriffen zu ergreifen. Absatz 3 bildet die gesetzliche Grundlage, damit das NCSC bei der Veröffentlichung der Schwachstellen die betroffene Hard- und Software – und damit implizit deren Hersteller – namentlich nennen darf.

## *Artikel 73c Weiterleitung von Informationen*

Artikel 73*c* definiert die Voraussetzungen, unter welchen es dem NCSC erlaubt ist, gewisse Informationen, die in einer Meldung enthalten sind, an den NDB oder die Strafverfolgungsbehörden weiterzuleiten (Absatz 1 und 2). Schliesslich wird auch der Umgang mit Informationen geregelt, sollte sich ein Strafverfahren gegen eine meldende Person richten (Absatz 3).

### *Absatz 1*

Absatz 1 hält fest, dass es dem NCSC erlaubt ist, Informationen an den NDB weiterzuleiten, wenn diese Informationen der Früherkennung und Verhinderung von Bedrohungen der inneren oder äusseren Sicherheit, für die Beurteilung der Bedrohungslage oder für die nachrichtendienstliche Frühwarnung zum Schutz von kritischen Infrastrukturen nach Artikel 6 Absätzen 1 Buchstabe a, 2 und 5 NDG relevant sind. Diese Weiterleitung ist nötig, damit der NDB seine Aufgaben auch in Bezug auf Cyberbedrohungen erfüllen kann. Sie beschränkt sich jedoch auf die dafür nötigen Informationen.

### *Absatz 2*

Absatz 2 regelt die Weitergabe von Informationen an die Strafverfolgungsbehörden. Die für Bundesangestellte geltende Anzeigepflicht entfällt für Informationen, welche das NCSC bei der Meldung eines Cybervorfalls oder bei dessen Analyse erhält, da diese Anzeigepflicht in einem Spannungsfeld zum Grundsatz der vertraulichen Behandlung der Meldung steht. Die Leiterin oder der Leiter des NCSC ist jedoch berechtigt, Informationen an die Strafverfolgungsbehörden weiterzuleiten. Sie oder er wägt dabei das Interesse des Staates an einer Strafverfolgung gegen das Interesse der meldenden Person an der Vertraulichkeit der Meldung ab. Diese Möglichkeit der Weiterleitung der Meldung nach entsprechender Interessenabwägung wurde vorgesehen, damit das NCSC bei schweren Straftaten an die Strafverfolgungsbehörden gelangen kann.

### *Absatz 3*

Über die Bestimmung von Absatz 3 wird sichergestellt, dass die meldende Person in einem gegen sie selber gerichteten Strafverfahren nicht gegen ihren Willen durch Informationen aus der Meldung belastet wird. In der Regel wird sich ein Strafverfahren gegen die Verursacher des Cybervorfalls, d.h. gegen die Angreifer, richten und nicht gegen die meldende Person. Sollte sich ein Strafverfahren ausnahmsweise gegen das Opfer eines Cyberangriffs richten, wurde eine analoge Regelung wie in Artikel 24 Absatz 6 nDSG aufgenommen. Diese Bestimmung setzt im Bereich der Meldepflicht bei Cyberangriffen den Grundsatz des Selbstbelastungszwangsverbots um (nemo tenetur). Sie ist also insbesondere für diejenigen Meldungen von Bedeutung, die in Erfüllung der Meldepflicht für Cyberangriffe erfolgen. Darüber hinaus soll dieses Privileg aber auch für freiwillige Meldungen gelten.

### *Absatz 4*

Für die Ausnahmefälle, in denen eine Weiterleitung von Informationen an den NDB oder Strafverfolgungsbehörden gemäss Absätzen 1 und 2 in Frage kommt, muss sich das NCSC gemäss den Vorgaben von Art. 320 StGB vom Amtsgeheimnis entbinden lassen, sofern die Informationen strafrechtlich geschützte Geheimnisse sind.

### *Artikel 74 Unterstützung für Betreiberinnen von kritischen Infrastrukturen*

Ergänzend zu den allgemeinen Aufgaben in Artikel 73*a* und der Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen gemäss Artikel 73*b* erbringt das NCSC für Betreiberinnen von kritischen Infrastrukturen weitergehende Leistungen beim Schutz vor Cyberrisiken (Absatz 1). Dabei ist zu beachten, dass die Definition für kritische Infrastrukturen gemäss Artikel 5 ISG sehr weit gefasst ist und daher eine gewisse Unschärfe besteht, wann eine Organisation als kritische Infrastruktur gilt und wann nicht. Das NCSC orientiert sich dabei an den in der Strategie zum Schutz kritischer Infrastrukturen (SKI)[25] aufgelisteten Sektoren und Teilsektoren.

#### *Absatz 2*

Das NCSC stellt den Betreiberinnen kritischer Infrastrukturen zu diesem Zweck Hilfsmittel zur Verfügung. Die wichtigsten davon werden in diesem Absatz beispielhaft aufgelistet. Es handelt sich um eine nicht abschliessende Aufzählung.

#### *Buchstabe a*

Der gegenseitige Informationsaustausch ist ein sehr wichtiges Mittel zum Schutz vor Cyberrisiken. Die hohe Dynamik bei der Entwicklung der Bedrohungslage und die Notwendigkeit von möglichen Schutzmassnahmen bedingen, dass die Verantwortlichen stets über den aktuellsten Wissensstand verfügen. Dieser lässt sich am effizientesten im Austausch mit anderen Verantwortlichen erreichen. Das NCSC bietet in Fortführung der bewährten Zusammenarbeit über MELANI den Betreiberinnen kritischer Infrastrukturen eine Plattform für diesen Informationsaustausch.

#### *Buchstabe b*

Informationen zu aktuellen Cyberrisiken und Schwachstellen sowie Empfehlungen für präventive Massnahmen beschränken sich auf Inhalte, die für kritische Infrastrukturen allgemein nützlich sein können. Es wird keine unternehmensspezifische Beratung durchgeführt.

#### *Buchstabe c*

Hilfsmittel und Anleitungen für die Früherkennung werden teilweise so konzipiert, dass sie allgemein für alle kritischen Infrastrukturen hilfreich sind. Sie können aber auch spezifisch für gewisse Gruppen von kritischen Infrastrukturen oder für bestimmte Tätigkeitsbereiche zugeschnitten sein. Sie ersetzen nicht die Schutzdispositive einzelner Unternehmen, sondern müssen in diese eingebunden werden.

#### *Absatz 3*

Bei Cybervorfällen unterstützt das NCSC die Betreiberinnen kritischer Infrastrukturen mit technischer Beratung. Die technische Unterstützung durch das NCSC erfolgt subsidiär zu den IT-Leistungen, die auf dem Markt erhältlich sind, sofern es sich um private Betreiberinnen handelt. Entscheidend ist dabei die Trägerschaft, nicht die Rechtsform. Es gilt ferner für alle Betreiberinnen, dass die Unterstützung durch das NCSC nur dann erfolgt, wenn sie zeitkritisch ist und ein erheblicher Schaden droht.

#### *Absatz 4*

Bei Cybervorfällen, insbesondere in Form von Cyberangriffen, soll das NCSC die Möglichkeit haben, zur Vorfallbewältigung oder zur Schadensbegrenzung auf die Systeme der betroffenen kritischen Infrastruktur zuzugreifen Dies natürlich unter dem Vorbehalt, dass die Betreiberin der kritischen Infrastruktur ihr Einverständnis erteilt. Die Betreiberin ist gegenüber dem NCSC von ihren Geheimhal-

25 Nationale Strategie zum Schutz kritischer Infrastrukturen 2018-2022: «www.babs.admin.ch > Weitere Aufgabenfelder > Schutz kritischer Infrastrukturen > Nationale SKI-Strategie» https://www.bAbsatzadmin.ch/de/aufgabenbabs/ski/nationalestrategie.html.

tungspflichten entbunden. Der zweite Satz bildet die gesetzliche Grundlage dafür, dass die Betreiberin dem NCSC den Zugriff auf ihre Informationen und Informatikmittel erlauben kann, ohne ihre gesetzlichen und vertraglichen Geheimhaltungspflichten zu verletzen.

### *2. Abschnitt: Pflicht zur Meldung von Cyberangriffen auf kritische Infrastrukturen*

### *Artikel 74a Meldepflicht*

In diesem Artikel wird die Meldepflicht in den Grundzügen definiert. Es wird festgehalten, dass Betreiberinnen kritischer Infrastrukturen im Falle von Cyberangriffen der Meldepflicht unterstellt sind und dass sie die Meldung des Cyberangriffs nach dessen Entdeckung so rasch wie möglich dem NCSC zu erstatten haben. Es ist für die Frühwarnung und die Prävention entscheidend, dass Angriffe unmittelbar nach deren Entdeckung gemeldet werden. In Artikel 74*e* wird präzisiert, dass die Anforderung der Unverzüglichkeit nicht für die gesamten verlangten Angaben gilt, sondern nur für die Erstmeldung auf der Basis der zu diesem Zeitpunkt verfügbaren Informationen.

### *Artikel 74b Bereiche*

Die Definition kritischer Infrastrukturen nach Artikel 5 ist breit gefasst. Sie ist nicht eindeutig genug, um zu bestimmen, welche Unternehmen oder Organisationen als kritische Infrastruktur gelten und darum unter die Meldepflicht fallen. Art. 74*b* listet deshalb konkret auf, für welche Unternehmen und Organisationen die Meldepflicht gelten soll. Grundlage für die Auflistung sind die in der Nationalen Strategie zum Schutz kritischer Infrastrukturen aufgeführten kritischen Teilsektoren. Der Geltungsbereich der Meldepflicht wird für diese Bereiche, soweit möglich, mit Verweisen auf bestehende rechtliche Grundlagen bestimmt. In Bereichen, in welchen kein solcher Verweis möglich ist – da keine rechtlichen Grundlagen bestehen, die für eine solche Eingrenzung geeignet sind – wird der betreffende Bereich möglichst genau bezeichnet. Dieses Vorgehen stellt sicher, dass ausreichende Klarheit darüber besteht, wer der Meldepflicht unterstellt ist.

#### *Buchstabe a: Hochschulen*

Hochschulen sind für den Bildungs- und Wirtschaftsstandort Schweiz von grosser Bedeutung. Insbesondere ihre Forschung ist ein Treiber der Innovation. Dadurch sind Hochschulen aber auch ein attraktives Ziel für Cyberangriffe. Der Meldepflicht unterstellt sind die kantonalen Universitäten, die Eidgenössischen Technischen Hochschulen, die Fachhochschulen und die pädagogischen Hochschulen.

#### *Buchstabe b: Behörden*

Cyberangriffe auf Behörden aller föderalen Ebene sind meldepflichtig, da es wichtig ist zu wissen, wie oft und durch wen Behörden angegriffen werden. So können die Abwehrdispositive jeweils auf die relevanten Bedrohungen ausgerichtet werden. Die Meldepflicht gilt dabei nur für das hoheitliche Handeln dieser Behörden und Organisationen.

#### *Buchstabe c: Organisationen mit öffentlich-rechtlichen Aufgaben*

Organisationen, welche öffentlich-rechtliche Aufgaben in bestimmten Bereichen wahrnehmen, sind der Meldepflicht unterstellt. Buchstabe c zählt auf, welche Tätigkeiten damit konkret gemeint sind. Im Bereich Sicherheit und Rettung liegt der Fokus auf den Blaulichtorganisationen (Polizei, Feuerwehr, Sanität- und Rettungsdienste). Daneben sind auch Organisationen der Trinkwasserversorgung, der Abwasseraufbereitung und der Abfallentsorgung meldepflichtig.

#### *Buchstabe d: Energieversorgung, -handel, -messung und -steuerung*

Die Versorgung mit Energie ist für die Wirtschaft und Gesellschaft essentiell. Verschiedene Angriffe auf die Stromversorgung oder auf Pipelines in anderen Staaten haben gezeigt, dass diese Infra-

strukturen gezielt angegriffen werden, sei es aus politischen Motiven oder um möglichst hohe Summen zu erpressen. Unternehmen mit Tätigkeiten, die für die Versorgung mit Energie wichtig sind, werden deshalb der Meldepflicht unterstellt.

***Buchstabe e: Banken, Versicherungen und Finanzmarktinfrastrukturen***

Die Unternehmen des Finanzsektors sind stark betroffen von Cyberangriffen, da sie auf Grund der hohen finanziellen Mittel, welche sie verwalten, ein attraktives Ziel für Kriminelle darstellen. Für die Verlässlichkeit des Finanzplatzes Schweiz ist es wichtig, dass solche Angriffe gemeldet werden. Die bereits bestehende Meldepflicht für Cyberangriffe gegenüber der Finanzmarktaufsicht FINMA bleibt parallel dazu bestehen. Die FINMA und das NCSC werden sich so abgleichen, dass der Aufwand für die Meldepflichtigen so gering wie möglich ausfällt.

***Buchstabe f: Digitale Dienste***

Als Anbieterinnen digitaler Dienste gelten jene Unternehmen, welche im Internet Dienste anbieten, die in der Schweiz von einer grossen Zahl von Nutzenden beansprucht werden, eine hohe Bedeutung für die digitale Wirtschaft haben oder Sicherheits- und Vertrauensdienste beinhalten. Dies sind insbesondere Anbieterinnen von Online-Marktplätzen von bedeutender Grösse, Cloudcomputing und Suchmaschinen. Die Aufzählung ist nicht abschliessend. Als «weitere digitale Dienste» fallen insbesondere Dienstleistungen in den Bereichen Identitätsmanagement, Signaturen oder E-Voting in Betracht. Ferner werden auch Registrare von Domain-namen und Betreiberinnen von Rechenzentren erwähnt. Auf Verordnungsstufe werden Kriterien wie die Anzahl Nutzende, Anzahl Mitarbeitende, Umsatz oder Art der Tätigkeiten festgelegt, um zu konkretisieren, welche digitalen Dienste der Meldepflicht unterstehen.

***Buchstabe g: Spitäler***

Die Kantone führen Spitallisten. Die dort aufgeführten kantonalen und ausserkantonalen Spitäler gewährleisten die Deckung des Bedarfs an medizinischer Grundversorgung auf dem jeweiligen Kantonsgebiet. Die Meldepflicht für Cyberangriffe soll für diese Spitäler gelten, weil es zu verhindern gilt, dass die Grundversorgung durch solche Angriffe beeinträchtigt wird.

***Buchstabe h: medizinische Laboratorien***

Laboratorien, die mikrobiologische Untersuchungen zur Erkennung von übertragbaren Krankheiten durchführen, sind für die Gesundheitsversorgung wichtig. Bei ihren Analysen und in der Zusammenarbeit mit den Grundversorgern sind sie in grossem Ausmass von funktionierenden IT-Infrastrukturen abhängig. Cyberangriffe auf solche Laboratorien sollen deshalb meldepflichtig sein.

***Buchstabe i: Herstellung, Inverkehrbringen bzw. Vertrieb sowie Einfuhr von Arzneimitteln und Medizinprodukten***

Für die medizinische Versorgung der Bevölkerung ist die Herstellung, der Vertrieb und der Import von Arzneimittel von grosser Bedeutung. Unternehmen, welche in diesen Bereichen tätig sind, werden daher der Meldepflicht unterstellt. Zusätzlich sind auch Hersteller oder Distributoren von Medizinprodukten meldepflichtig.

***Buchstabe j: Sozialversicherungen***

Die Leistungen der Sozialversicherungen wurden in Anlehnung an die definierten Risiken in den Allgemeinen Bestimmungen des Bundesgesetzes über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG; SR 830.1) umschrieben, um möglichst alle Zweige der Sozialversicherungen abzudecken. Es wurde auf die Aufzählung einzelner Gesetze (z.B. IVG, AHVG) verzichtet, um nicht nur gesetzliche, sondern auch überobligatorische Leistungen, beispielsweise der beruflichen Vorsorge oder der Zusatzversicherung zur obligatorischen Krankenkasse, abzudecken. Bei der beruflichen Vorsorge werden alle registrierten und nicht registrierten Vorsorge- und Freizügigkeitseinrichtungen erfasst, jedoch nicht die gebundene oder freiwillige Selbstvorsorge (Säule 3a und 3b). Diese

letztgenannten Vorsorgemöglichkeiten werden in aller Regel von Banken und Versicherungen angeboten, die ihrerseits der Meldepflicht unterstehen.

Auf Verordnungsstufe kann der Bundesrat auch im Falle der Sozialversicherungen Einschränkungen für den Kreis der Meldepflichtigen vornehmen und beispielsweise den Adressatenkreis der meldepflichtigen Vorsorge- und Freizügigkeitseinrichtungen durch geeignete Kriterien einschränken.

### *Buchstabe k: Anbieterinnen von Fernmeldediensten*

Eine fernmeldetechnische Übertragung ist elektrisches, magnetisches, optisches oder anderes elektromagnetisches Senden oder Empfangen von Informationen über Leitungen oder Funk (Art. 3 Bst. c des Fernmeldegesetzes vom 30. April 1997, FMG[26]). Als fernmeldetechnische Übertragung gilt auch das Anbieten von Übertragungskapazität und die so genannten Over the Top (OTT)-Dienste. Bei Letzteren handelt es sich um Übertragungen von Informationen über Internetdienste. Bekannte Beispiele für solche Dienste sind Skype (Microsoft), WhatsApp (Facebook), Facetime (Apple), Hangouts (Google), Signal und Threema.

### *Buchstabe l: Schweizerische Radio- und Fernsehgesellschaft (SRG)*

Die SRG hat den Auftrag, die gesamte Bevölkerung inhaltlich umfassend mit gleichwertigen Radio- und Fernsehprogrammen in den drei Amtssprachen zu versorgen (Art. 24 Abs. 1 Bst. a des Radio- und Fernsehgesetzes vom 24. März 2006, RTVG)[27]. Sie hat zudem den Auftrag, zur freien Meinungsäusserung durch umfassende, vielfältige und sachgerechte Information insbesondere über politische, wirtschaftliche und soziale Zusammenhänge beizutragen (Art. 24 Abs. 4 Bst. a RTVG). Damit geht ihr Auftrag deutlich über die Bekanntmachungspflichten der übrigen konzessionierten Medien hinaus. Cyberangriffe auf die SRG können die Erfüllung dieser Aufträge gefährden.

### *Buchstabe m: Nachrichtenagenturen von nationaler Bedeutung*

Eine Nachrichtenagentur ist von nationaler Bedeutung gemäss Artikel 44a der Radio- und Fernsehverordnung vom 9. März 2007[28], wenn ihre Berichterstattung alle vier Sprachregionen abdeckt und sie regelmässig in drei Landessprachen erfolgt (vgl. Art. 18 Bst. a des Sprachengesetzes vom 5. Oktober 2007[29] i.V.m. Art. 13 Abs. 2 der Sprachenverordnung vom 4. Juni 2010[30]). Konkret gibt es in der Schweiz nur noch die Nachrichtenagentur Keystone-SDA (siehe Covid-19-Verordnung elektr. Medien)[31].

### *Buchstabe n: Anbieterinnen von Postdiensten*

Unternehmen, welche Kundinnen und Kunden in eigenem Namen Postdienste anbieten, unterliegen ebenfalls der Meldepflicht, sofern sie bei der Postkommission gemäss Artikel 4 Absatz 1 des Postgesetzes vom 17. Dezember 2010[32] registriert sind. Der Bundesrat kann auf Verordnungsebene kleinere Unternehmen von der Meldepflicht ausnehmen. Es wäre beispielsweise eine analoge Einschränkung denkbar, wie sie in Art. 4 Abs. 2 des Postgesetzes für Unternehmen vorgesehen ist, die einen geringen Umsatz erzielen.

### *Buchstabe o: Öffentlicher Verkehr (Personentransport plus Eisenbahngüterverkehr)*

Mit dem Verweis auf das Bundesgesetz vom 18. Juni 2010[33] über die Sicherheitsorgane der Transportunternehmen im öffentlichen Verkehr wird nur der wichtigste Bereich des öffentlichen Verkehrs, d.h. der konzessionierte Personenverkehr sowie der Güterverkehr und die Infrastruktur der Eisenbahn erfasst.

26 SR **784.10**
27 SR **784.40**
28 SR **784.401**
29 SR **441.1**
30 SR **441.11**
31 SR **784.402**
32 SR **783.0**
33 SR **745.2**

### *Buchstabe p: Unternehmen der Zivilluftfahrt*

Die Bestimmung unterstellt alle Unternehmen mit einer Bewilligung des Bundesamts für Zivilluftfahrt der Meldepflicht für Cyberangriffe.

### *Buchstabe q: Rheinschifffahrt*

Die Schweizerischen Rheinhäfen bilden den Zugang der Schweiz zu den Weltmeeren und für die Versorgung der Schweiz mit Gütern aller Art von grosser Bedeutung. Die Meldepflicht für Cyberangriffe gilt deshalb für die Schifffahrt auf dem Rhein zur Güterbeförderung nach dem Seeschifffahrtsgesetz vom 23. September 1953[34] und für die für den Betrieb und die Funktion vom Hafen Basel relevanten Prozesse.

### *Buchstabe r: Unentbehrliche Güter des täglichen Bedarfs*

In die Versorgung der Bevölkerung mit unentbehrlichen Gütern des täglichen Bedarfs, insbesondere Lebensmittel, ist eine Vielzahl von Akteuren eingebunden. Neben den Produzenten und Importeuren spielen auch die Verarbeiter, die Verteilzentren und die Detailhändler eine bedeutende Rolle. Nicht alle dieser Akteure sind gleichbedeutend für die Versorgungssicherheit der Schweiz. Die Meldepflicht für Cyberangriffe soll nur für jene Akteure gelten, welche in dieser Hinsicht eine wichtige Bedeutung haben. Der Bundesrat wird daher die Meldepflicht im Bereich der Versorgung mit unentbehrlichen Gütern des täglichen Bedarfs gemäss den Kriterien von Art. 74*c* auf Verordnungsebene einschränken.

### *Buchstabe s: Hersteller von Hard- und Software*

Vermehrt wird festgestellt, dass kritische Infrastrukturen über die Hersteller von Hard- und Software angegriffen werden. Die Cyberangreifer manipulieren dabei die Hard- und Software bereits vor der Auslieferung an die Endkunden, damit sie später Zugriff auf die Systeme erhalten. Für die Cybersicherheit sind deshalb die Hersteller von Hard- und Software von grosser Bedeutung.

Besonders relevant sind Cyberangriffe auf Hersteller von Software, wenn diese über Fernwartungszugänge verfügen. Angreifer können versuchen, über solche legitimen Zugänge direkt in die Systeme der kritischen Infrastrukturen einzudringen. Neben dem Kriterium des Fernwartungszugangs sind Hersteller von Hard- und Software dann meldepflichtig, wenn ihre Produkte in besonders heiklen Bereichen zum Einsatz kommen. Dies betrifft Hard- und Software zur Steuerung und Überwachung von Systemen (Industrial Control Systems) (Ziff. 1) sowie zum Betrieb von Medizintechnik und Fernmeldeanlagen (Ziff. 2). Der Fokus liegt sodann auch auf Hard- und Software, welche zur Gewährleistung der öffentlichen Sicherheit eingesetzt wird (Ziff. 3). Zu denken ist hier insbesondere an die Kommunikation von Blaulichtorganisationen oder die Systeme für die polizeiliche Ermittlung. Zudem sollen die Hersteller von Hard- und Software mit besonders heiklen Funktionen (IT-Sicherheit, Verschlüsselung, Identifikation, Zugriffs- und Zutrittsberechtigung) (Ziff. 4) der Meldepflicht unterstellt werden, da eine Manipulation solcher Produkte, die gerade beim erhöhtem Schutzbedarf eingesetzt werden, in jedem Fall heikel ist.

### *Artikel 74c Ausnahmen von der Meldepflicht*

Der Adressatenkreis der Meldepflicht nach Art. 74*b* ist breit gefasst und kann auch Unternehmen umfassen, welche für sich alleine betrachtet nicht von essentieller Bedeutung für das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung sind, obschon sie in einem kritischen Teilsektor tätig sind. Art. 74*c* legt daher fest, dass der Bundesrat den Adressatenkreis weiter einschränkt. Er verwendet dazu die aufgelisteten Kriterien. Ein Ausschluss von der Meldepflicht wird vorgenommen, wenn ein Unternehmen oder Kategorien von Unternehmen nur eine geringe Risikoexposition gegenüber Cyberangriffen haben, weil ein solcher als unwahrscheinlich beurteilt werden kann oder die Unternehmen in ihrem Betrieb nur in geringem Ausmass von Informatikmittel abhängen (Buchstabe a). Ein Ausschluss kann auch erfolgen, wenn ein Ausfall oder eine Störung

34 SR **747.30**

der Unternehmen nur geringe Auswirkungen auf die Wirtschaft oder das Wohlergehen der Bevölkerung haben. Messbar sind solche Auswirkungen an der Anzahl der betroffenen Personen, der Substituierbarkeit der Dienstleistung oder dem volkswirtschaftlichen Schadenspotential (Buchstabe b).

### *Artikel 74d Zu meldende Cyberangriffe*

#### *Absatz 1*

Der Umfang der Meldepflicht, d.h. welche Art von Cyberangriffen zu melden sind, ist auf Gesetzesebene zu verankern. In Absatz 1 enthalten die Buchstaben a bis d die entsprechenden Kriterien, um bei einem Cyberangriff auf ein erhebliches Schadenspotential oder eine hohe Relevanz für den Schutz anderer kritischer Infrastrukturen schliessen zu können. Erfüllt ein Cyberangriff eines der Kriterien, so ist er meldepflichtig. Die Kriterien sind auf Verordnungsebene bei Bedarf weiter zu präzisieren.

#### *Absatz 2*

In Absatz 2 wird statuiert, dass bei strafrechtlich relevanten Begleitumstände ein Cyberangriff immer zu melden ist. Viele Cyberkriminelle versuchen über die Androhung oder Durchführung von Angriffen Betreiberinnen kritischer Infrastrukturen oder einzelne Mitarbeitende dieser Unternehmen zu erpressen (Beispielsweise über die Verschlüsselung mittels Ransomware, der Androhung von Angriffen auf die Verfügbarkeit mittels DDoS-Attacken oder der Androhung der Veröffentlichung von kompromittierenden Informationen über Einzelpersonen). Solche Angriffe sind zu melden, damit eingeschätzt werden kann, wie stark die Bedrohung kritischer Infrastrukturen durch Cyberkriminelle ist.

### *Artikel 74e Inhalt der Meldung*

Die wesentlichen Angaben, die für die Erfüllung der Meldepflicht notwendig sind, werden in Absatz 1 gesetzlich verankert. Der konkrete Inhalt der einzelnen Angaben wird in den Ausführungsbestimmungen präzisiert werden.

Absatz 2 präzisiert die Unverzüglichkeit der Meldungserstattung *(«so rasch als möglich»*) gemäss Artikel 74*a* dahingehend, dass sich diese nur auf die bereits bekannten Informationen bezieht. Bei Cyberangriffen ist sehr oft längere Zeit unklar, wie gravierend der Angriff ist und was genau passiert ist. Wenn diese Informationen zum Zeitpunkt der Meldung nur unvollständig vorliegen, sollen die Betroffenen daher die Möglichkeit haben, die gemäss Absatz 1 verlangten Angaben erst dann zu übermitteln, wenn sie über einen ausreichenden Kenntnisstand dazu verfügen.

### *Artikel 74f Übermittlung der Meldung*

#### *Absatz 1*

Damit die Meldepflicht mit möglichst geringem Aufwand erfüllt werden kann, wird das NCSC verpflichtet, ein sicheres elektronisches Meldeformular zur Verfügung zu stellen. Das Meldeformular wird im Gesetzestext angesichts der technologischen Entwicklung generisch mit «System zur Übermittlung der Meldung» umschrieben. Abgesehen von diesem Meldeformular bleibt es jedoch in jedem Fall zulässig, das NCSC auf andere Weise (Mail, telefonisch) über den Cyberangriff in Kenntnis zu setzen.

#### *Absatz 2*

Das Meldesystem bietet den Meldenden die Möglichkeit, die Meldung des Cyberangriffs oder seiner Auswirkungen (z.B. auf die Datensicherheit oder auf die Funktionsfähigkeit der kritischen Infrastruktur) als Ganzes oder Teile davon an weitere Stellen und Behörden zu übermitteln. Für diese Übermittlung via Meldesystem des NCSC an weitere Stellen und Behörden wird diesen gegenüber keine gesetzliche Meldepflicht vorausgesetzt; sie steht auch für freiwillige Meldungen an Drittstellen offen. Wichtig ist dabei, dass die Übermittlung der Meldung nur von der Betreiberin der betroffenen kritischen Infrastruktur übermittelt werden kann. Sie alleine bestimmt, welche Stelle oder Behörde –

ausser dem NCSC – die Meldung des Cyberangriffes oder seiner Auswirkungen erhalten soll. Das NCSC leitet keine Meldungen an andere Stellen und Behörden weiter. Vorbehalten sind die Ausnahmefälle in Artikel 73*c* Absatz 1 und 2.

### *Absatz 3*

Das NCSC kann das Meldesystem – auf Wunsch und in Zusammenarbeit mit weiteren Meldestellen – so ausgestalten, dass die meldepflichtige Betreiberin einer kritischen Infrastruktur allfällige zusätzliche Angaben erfassen kann, die für die Meldung an das NCSC nicht notwendig sind, um diese an eine oder mehrere weitere Meldestellen zu übermitteln. Diese Funktion soll dazu dienen, den Aufwand der Meldenden möglichst gering zu halten. Sie hilft ihnen, insbesondere bei Zusammentreffen von mehreren Meldepflichten, die entsprechenden Stellen und Behörden möglichst rasch, zeitnah und ohne grossen Aufwand informieren zu können. Diese zusätzlichen Informationen, die die Meldenden für andere Stellen und Behörden im Meldesystem des NCSC erfassen, werden von diesem nur übermittelt, ohne diese zu speichern. Das NCSC selber hat keine Zugriffsmöglichkeit auf diese Informationen.

## *Artikel 74g Auskunftspflicht*

Die Auskunftspflicht ist auf Informationen beschränkt, die benötigt werden, um das Angriffsmuster und die Angriffsmethode eines gemeldeten Cyberangriffs identifizieren (Frühwarnung) und damit Auswirkungen des Cyberangriffs auf andere kritische Infrastrukturen verhindern zu können.

## *Artikel 74h Verletzung der Melde- oder Auskunftspflicht*

### *Absatz 1*

Im Falle einer Verletzung der Melde- oder Auskunftspflicht macht das NCSC in einem ersten Schritt die Betreiberin der kritischen Infrastruktur auf die Pflichtverletzung aufmerksam. Diese hat somit nochmals Gelegenheit, ihren Pflichten nachzukommen. Sollten dazu Missverständnisse vorliegen, dann können diese geklärt werden. Das NCSC ist zu dieser ersten Kontaktaufnahme verpflichtet. Sie ist eine Voraussetzung für den Erlass einer Verfügung nach Absatz 2.

### *Absatz 2*

In einem zweiten Schritt, d.h. wenn die Betreiberin trotz offensichtlicher Pflichtverletzung nichts unternimmt, erlässt das NCSC eine Verfügung mit Bussandrohung. Das NCSC konkretisiert die verletzten Pflichten in der Verfügung soweit, dass für die Betreiberin der kritischen Infrastruktur kein Zweifel besteht, was sie zu tun oder zu lassen hat. Dies erleichtert auch die Arbeit der Strafverfolgungsbehörden, die im Falle der Missachtung dieser Verfügung auf Anzeige des NCSC hin den Sachverhalt ermitteln und ein Urteil bzw. einen Strafbefehl erlassen müssen (vgl. Artikel 74*i*).

## *Artikel 74i Widerhandlungen gegen Verfügungen des NCSC*

Dieser Artikel übernimmt weitgehend die Regelung, die in Artikel 63 ff. nDSG im Falle der Missachtung von Verfügungen des Beauftragten durch Geschäftsbetriebe vorgesehen wird. Wie in der Botschaft zum revidierten Datenschutzgesetz[35] ausgeführt wurde, gilt auch hier, dass sich diejenige Person strafbar macht, die innerhalb der kritischen Infrastruktur hätte dafür sorgen müssen, dass der Verfügung des NCSC Folge geleistet wird (vgl. Artikel 29 StGB[36]). Die verletzte Pflicht, die dem Unternehmen obliegt, wird der natürlichen Person zugerechnet. Der Verweis auf Artikel 6 des Bundesgesetzes vom 22. März 1974[37] über das Verwaltungsstrafrecht adressiert eine strafrechtliche Verantwortung an die Leitungsebene von Unternehmen, also an Führungspersonen, die Entscheidungs- und Weisungsbefugnisse haben. Dies ermöglicht eine sachgerechte Zuweisung der strafrechtlichen Verantwortung bei kritischen Infrastrukturen.

35 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl *2017* 6974, 6980, 7103 f.
36 SR **311.0**
37 SR **313.0**

### *Absatz 1*

Die Obergrenze der Busse wurde auf 100'000 Franken angesetzt, um der Bedeutung von kritischen Infrastrukturen für das ordnungsgemässe Funktionieren von Wirtschaft und Staat gebührend Rechnung zu tragen und deren Verantwortung für die Gewährleistung ihrer Cybersicherheit zu verdeutlichen. Der Höchstbetrag der Busse rechtfertigt sich auch dadurch, dass die Busse erst als ultima ratio nach einer Kaskade von Massnahmen zum Zug kommt. Angesichts der heterogenen Niveaus von Cybersicherheit in den einzelnen Sektoren und der zusätzlichen Anforderungen durch die neu eingeführte Meldepflicht für Cyberangriffe wurde bewusst darauf verzichtet, die Bussobergrenze des revidierten Datenschutzgesetzes von 250'000 Franken zu übernehmen. Eine Bussandrohung von 100'000 Franken sollte ausreichen, um die Verantwortlichen der kritischen Infrastrukturen zu pflichtkonformem Verhalten zu bewegen.

### *Absatz 2 und 3*

Bei der Bussauferlegung an Geschäftsbetriebe wurde die Regelung des revidierten Datenschutzgesetzes sinngemäss übernommen (Art. 64 nDSG). Bis zu einem Betrag von 20'000 Franken kann die Busse somit direkt der kritischen Infrastruktur anstelle der verantwortlichen natürlichen Person auferlegt werden, um aufwändige Ermittlungen zu vermeiden. Angesichts des Höchstbetrages von 100'000 Franken wurde der Betrag für diese «Bagatellfälle» auf 20'000 Franken angesetzt, um die kritischen Infrastrukturen als solche in die Pflicht zu nehmen und auf weitere Untersuchungen betreffend die Verantwortlichen zu verzichten. Wenn man bedenkt, dass die Meldepflicht auf die bedeutendsten kritischen Infrastrukturen fokussiert, die vielfach auch einen entsprechenden Marktanteil beanspruchen, gibt es kaum Argumente, um den Höchstbetrag von 20'000 Franken tiefer anzusetzen.

### *Absatz 4*

Aus Transparenzgründen wird in Absatz 4 – analog zu Art. 65 nDSG – auf die Zuständigkeit der kantonalen Strafverfolgungsbehörden hingewiesen, sollte einer Verfügung des NCSC keine Folge geleistet werden. Es wurde darauf verzichtet, das Anzeigerecht des NCSC zu erwähnen, da sich dieser Umstand aus dem Kontext ergibt.

## *3. Abschnitt: Datenschutz und Informationsaustausch*

Die Artikel 75 bis 79, die neu unter dem 3. Abschnitt zusammengefasst werden, mussten sowohl sprachlich wie auch inhaltlich angepasst werden, um der gesetzlichen Verankerung der Aufgaben des NCSC zu entsprechen. Das NCSC löst mit seiner Meldestelle die gemeinsam durch das damalige Informatiksteuerungsorgan des Bundes (ISB) und den NDB betriebene MELANI ab. Da der NDB einen gesetzlichen Auftrag zur Beurteilung der Bedrohungslage und zur Frühwarnung von Betreiberinnen kritischer Infrastrukturen hat, muss die Zusammenarbeit des NCSC mit dem NDB und die Weitergabe von Informationen und Daten soweit notwendig im ISG geregelt werden.

### *Artikel 75 Bearbeitung von Personendaten*

### *Absatz 1*

Anstelle der generischen Umschreibung der zuständigen Bundesstellen wurde das NCSC eingefügt und verdeutlicht, dass das NCSC nicht nur Personendaten, sondern im Zusammenhang mit Adressierungselementen auch besonders schützenswerte Personendaten bearbeiten darf. Als Adressierungselement gilt gemäss Artikel 3 Buchstabe f FMG eine «Abfolge von Ziffern, Buchstaben oder Zeichen oder andere Informationen zur Identifikation von Personen, Computerprozessen, Maschinen, Geräten oder Fernmeldeanlagen, die an einem fernmeldetechnischen Kommunikationsvorgang beteiligt sind». In Buchstabe a der Begriff «Cybersicherheit» eingefügt.

### *Absatz 2*

Die Formulierung in Absatz 2 übernimmt im Wesentlichen den alten Absatz 3, wurde aber von passiv auf aktiv geändert, wodurch deutlicher wird, dass die Datenbearbeitung vom NCSC vorgenommen wird. Zusätzlich wurden die Voraussetzungen konkretisiert, die vorliegen müssen, wenn die betroffene Person über die Datenbearbeitung nicht informiert wird.

### *Absatz 3*

In Absatz 3 wurde inhaltlich präzisiert, dass die vom Missbrauch von Adressierungselementen betroffene Person über diesen Umstand zu informieren ist.

## *Artikel 76 Zusammenarbeit im Inland*

Dieser Artikel bildet die gesetzliche Grundlage für den Informationsaustausch zwischen dem NCSC und den Betreiberinnen von kritischen Infrastrukturen (Absatz 1 und 2) sowie zwischen dem NCSC und den Fernmeldedienstanbieterinnen (Absatz 3 und 4).

Es wurden auch formelle Anpassungen vorgenommen. So wurde beispielsweise in jedem Absatz präzisiert, dass die Zusammenarbeit unter dem Vorbehalt steht, dass sie zum Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

### *Absatz 1 und 2*

Der in Absatz 1 geregelte Informationsaustausch zwischen dem NCSC und den Betreiberinnen von kritischen Infrastrukturen ist nicht auf die meldepflichtigen kritischen Infrastrukturen beschränkt, sondern richtet sich an alle interessierten kritischen Infrastrukturen mit Sitz in der Schweiz.

### *Absatz 3 und 4*

Der Informationsaustausch zwischen dem NCSC und den Fernmeldedienstanbieterinnen wurde in Absatz 3 und 4 explizit geregelt, da zwar die meisten, aber wohl nicht alle Fernmeldedienstanbieterinnen als kritische Infrastrukturen gelten.

## *Artikel 76a Unterstützung für Behörden*

Diese Bestimmung wurde neu eingefügt. Sie regelt, welche Informationen das NCSC anderen Behörden in welchem Umfang und zu welchem Zweck zur Verfügung stellt. Sie bestimmt insbesondere den Inhalt und Umfang sowie die Art und Weise des Informationsaustausches des NCSC mit dem NDB, den Strafverfolgungsbehörden und den kantonalen Stellen, die für Cybersicherheit zuständig sind (Absätze 2 bis 4). Ein wichtiger Aspekt bei der Zusammenarbeit des NCSC mit diesen Behörden ist der Austausch von Informationen über die Angreifer selber und über deren Methoden und Taktiken.

### *Absatz 1*

Im ersten Absatz dieser Bestimmung wird im Gegensatz zu den nachfolgenden Absätzen nicht der gegenseitige Informationsaustausch geregelt, sondern der Grundsatz statuiert, dass das NCSC dem NDB bei seinen Aufgaben durch spezifische Auswertungen zu Anzahl, Art und Ausmass von Cyberangriffen sowie technischen Analysen von Cyberrisiken behilflich ist. Diese «Lagebilder» enthalten keine konkreten, fallspezifischen Personendaten oder Informationen, sondern beschränken sich auf statistische und technische Auswertungen, die für die Beurteilung der Bedrohungslage und die Frühwarnung notwendig sind. Der NDB ist gestützt auf Artikel 6 Absatz 2 NDG zuständig für die Beurteilung der Bedrohungslage. Über die Meldestelle und die Meldepflicht verfügt das NCSC über eine wichtige Informationsquelle zur Bedrohungslage durch Cybervorfälle. Es muss dem NDB deshalb Informationen übermitteln können zur Anzahl, Art und Ausmass der Cyberangriffe. Zudem muss es den NDB mit technischen Analysen zu Angriffen unterstützen und diesem Erkenntnisse aus solchen Analysen weiterleiten können.

### *Absatz 2, 3 und 4*

In den Absätzen 2 bis 4 werden Inhalt und Umfang sowie die Art und Weise des Informationsaustausches des NCSC mit dem NDB, den Strafverfolgungsbehörden und den kantonalen Cybersicherheits-Stellen geregelt. Ein wichtiger Aspekt bei der Zusammenarbeit des NCSC mit diesen Behörden ist, wie bereits erwähnt, der Austausch von Informationen über die Angreifer selber und über deren Methoden und Taktiken. Diese Informationen können rein technischer Natur sein (z.B. Angriffsmuster oder Hashwerte von Malware) und keine Personendaten enthalten. Es werden zwischen diesen Behörden aber auch Informationen ausgetauscht, die personenbezogen sind oder für die ein Personenbezug hergestellt werden kann. Für den Informationsaustausch in Bezug auf diese Personendaten wird hier eine Rechtsgrundlage geschaffen. Konkret handelt sich um Adressierungselemente (wie Domainname, IP-Adresse, missbräuchlich verwendete Mailadressen) oder Angaben zu Finanztransaktionen (Bankkonten, IBAN-Nummer usw.).

Die berechtigten Behörden nach Absatz 2 bis 4 können auf die genannten Informationen auch im Abrufverfahren zugreifen. Dieses Vorgehen ist aufgrund der grossen Anzahl von Cyberangriffen und damit verbundenen technischen Informationen angezeigt. Eine Weiterleitung von Meldungen an den NDB oder die Strafverfolgungsbehörden mit Informationen zu den Betroffenen erfolgt nur in Ausnahmefällen und bleibt an die Bedingungen nach Artikel 73*c* Absatz 1 und 2 gebunden.

### *Artikel 77 Internationale Zusammenarbeit*

Diese Bestimmung wurde formell angepasst, indem das NCSC namentlich eingefügt wurde. Ferner wurde der Begriff «Daten» durch den Oberbegriff «Informationen» ersetzt, wo nicht spezifisch Personendaten gemäss Artikel 75 gemeint sind. Zum Umfang, Inhalt und Zweck des Informationsaustausches wurde konkretisierend eingefügt, dass er mit Stellen zulässig ist, die für die Cybersicherheit zuständig sind. Damit wurde die Formulierung «für den Schutz kritischer Infrastrukturen» durch «Cybersicherheit» ersetzt, da die erste Formulierung zu eng ist für die international bedeutenden Organisationen, die im Bereich Cybersicherheit tätig sind.

### *Artikel 78 Informationssystem zur Unterstützung von kritischen Infrastrukturen*

Dieser Artikel wurde in Anwendung der geänderten Rechtsgrundlagen durch die Revision des DSG gestrichen. Die Zwecke der Datenbearbeitung durch das NCSC ergeben sich aus seinen Aufgaben, die in den aufgeführten Artikeln ausreichend beschrieben sind. Sie geben vor, für was die Informationssysteme des NCSC bei der Bearbeitung von Personendaten verwendet werden dürfen.

### *Artikel 79 Datenaufbewahrung und -archivierung*

Dieser Artikel wurde nur in Bezug auf Absatz 1 leicht angepasst. Es wurde präzisiert, dass Personendaten höchstens fünf Jahre ab der letzten Verwendung aufbewahrt werden können. Der Hintergrund für diese Regelung ist, dass gewisse technische Informationen zu Cybervorfällen, wie z.B. Domainname, IP-Adresse oder missbrauchte Mailadressen, für den Abgleich von neu gemeldeten Cybervorfällen und die Analyse von Angriffsmethoden und -mustern eine zentrale Bedeutung haben. Ohne diese Vergleichsdaten kann das NCSC seine Analysen nicht oder nicht zielorientiert durchführen, die eine Grundvoraussetzung für seine Aufgabenerfüllung sind. Da diese technischen Daten aber auch personenbezogene Elemente enthalten und damit als Personendaten dem Datenschutz unterstehen, muss die Aufbewahrungsdauer klar eingegrenzt werden. Aus Gründen des Datenschutzes wurde im zweiten Teil des Satzes präzisiert, dass besonders schützenswerte Personendaten höchstens zwei Jahre ab der letzten Verwendung aufbewahrt werden.

### *Artikel 80 Bestimmungen des Bundesrats*

Dieser Artikel wurde gestrichen. Durch die erfolgten Konkretisierungen im Gesetzestext werden die in diesem Abschnitt vorgesehenen Delegationen an den Bundesrat obsolet. Die Kompetenz, Ausführungsbestimmungen zu erlassen, kommt dem Bundesrat auch ohne Gesetzesvorbehalt zu. Ferner sind die in Buchstabe c (Verantwortung für den Datenschutz und Datensicherheit) vorgesehenen Ausführungsbestimmungen bereits durch die Artikel 33 und 8 Absatz 3 nDSG abgedeckt.

### *Anhang 1 (Artikel 89 Änderung anderer Erlasse)*

Die Auflistung der Änderungen anderer Erlasse gemäss Artikel 89 in Anhang 1 wird wie folgt ergänzt.

### *Bundesgesetz vom 23. März 2007 über die Stromversorgung*[38]

Der Schutz vor Cyberrisiken, der neu in Artikel 8a des Stromversorgungsgesetzes explizit verankert werden soll, dient der Versorgungssicherheit. Die zu treffenden Massnahmen gemäss Absatz 1 sollen Cybervorfälle und damit insbesondere Funktionsstörungen der entsprechenden Anlagen verhindern respektive möglichst rasch beheben. Die Pflicht trifft neben den Netzbetreibern, die direkt via Steuertechnologie Einfluss auf den Netzbetrieb ausüben, auch die Erzeuger (bspw. Betreiber von Wind- oder Wasserkraftanlagen) und die Speicherbetreiber, zumal diese über die Ein- und Ausspeisung massgeblichen Einfluss auf die Versorgungssicherheit ausüben können. Bei der Frage, welcher Schutz als angemessen gilt, kommt es auf den Einfluss des entsprechenden Akteurs auf die Versorgungssicherheit an (bspw. Netzebene, Leistung, Anzahl betroffener Endverbraucher).

Der Bundesrat wird auf Verordnungsebene entsprechende Vorgaben, insbesondere zum Schutzniveau und der Auditierung festlegen. Dabei kann er sich an einschlägigen Fachnormen orientieren (bspw. am Handbuch des VSE Grundschutz für «Operational Technology» in der Stromversorgung, Ausgabe Juli 2018, zurzeit in Überarbeitung), welche er auch für verbindlich erklären kann. Für kleinere Akteure sind entsprechende Ausnahmen oder Erleichterungen vorzusehen.

Als weitere Beteiligte im Sinne von Absatz 2 kommen mit Blick auf den Zweck der Bestimmung lediglich Akteure in Frage, die einen massgebenden Einfluss auf die Versorgungssicherheit ausüben, namentlich entsprechend grosse Dienstleister im Elektrizitätssektor, beispielsweise in den Bereichen Handel, Messung, Steuerung, Flexibilität, Datenbearbeitung oder Elektromobilität.

### *Änderung des Datenschutzgesetzes vom 25. September 2020*[39]

Damit der EDÖB bei der Analyse einer eingetretenen Verletzung der Datensicherheit, die der Verantwortliche ihm gestützt auf Artikel 24 nDSG und Artikel 19 E-VDSG gemeldet hat, die technischen Fachspezialistinnen und Fachspezialisten des NCSC miteinbeziehen kann, wird in Artikel 24 Absatz 5$^{bis}$ nDSG vorgesehen, dass der EDÖB die Meldung einer Verletzung der Datensicherheit an das NCSC weiterleiten kann.

Die Weiterleitung kann jegliche Angaben gemäss Artikel 19 Absatz 1 E-VDSG enthalten, muss sich aber gleichzeitig auf die für das NCSC für die Analyse des Vorfalls notwendigen Daten beschränken. Dabei kann die Mitteilung des EDÖB an das NCSC auch Personendaten enthalten, einschliesslich besonders schützenswerter Personendaten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen des meldepflichtigen Verantwortlichen. Die für die Analyse eines Vorfalls notwendigen Informationen werden im Einzelfall selektiert, jedoch können unter Umständen damit auch indirekt Informationen über ein laufendes Verfahren an das NCSC gelangen. Daher ist eine gesetzliche Grundlage für die Bekanntgabe von besonders schützenswerten Personendaten zu schaffen.

Vorausgesetzt ist, dass der Verantwortliche, der zur Meldung an den EDÖB verpflichtet ist, vorgängig sein Einverständnis zur Weiterleitung gegeben hat. Ausserdem darf die Weiterleitung nicht dazu führen, dass Artikel 24 Absatz 6 revDSG umgangen wird, wonach die Meldung nur mit Einverständnis der meldepflichtigen Person im Rahmen eines Strafverfahrens verwendet werden darf. Der neue Absatz 5$^{bis}$ in Artikel 24 nDSG ermöglicht dem EDÖB keine systematische Weiterleitung von Meldungen an das NCSC. Vielmehr darf der EDÖB von dieser Möglichkeit nur in Einzelfällen, wo das technische Fachwissen des NCSC für die Abklärung eines Vorfalls erforderlich ist, Gebrauch machen.

38 SR **734.7**
39 Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) vom 25. September 2020, BBl *2020* 7639.

# 5 Auswirkungen

## 5.1 Auswirkungen auf den Bund

Das NCSC führt bereits heute eine Anlaufstelle, welche auf freiwilliger Basis Meldungen zu Cybervorfällen entgegennimmt. Es baut dabei auf die langjährige Erfahrung von MELANI auf, welche diese Aufgabe seit 2004 spezifisch für Meldungen von kritischen Infrastrukturen ausgeführt hat.

Das NCSC betreibt für die Entgegennahme von Meldungen bereits heute ein elektronisches Meldeformular. Dieses lässt sich so anpassen, dass es auch für die Entgegennahme von Meldungen in Erfüllung der Meldepflicht verwendet werden kann. Für die nötigen Abstimmungen mit anderen Stellen, welche ebenfalls Meldungen entgegennehmen (z.B. EDÖB, FINMA, ENSI) und für die Konfiguration des Meldeformulars fällt ein Initialaufwand an, der jedoch über die bestehenden Ressourcen des NCSC aufgefangen werden kann. Für den späteren Betrieb muss das NCSC jedoch sicherstellen, dass die in Erfüllung der Meldepflicht eingegangenen Meldungen korrekt erfasst, quittiert und dokumentiert werden und die Meldung zum Zweck der Frühwarnung an die richtigen Stellen weitergeleitet werden. Dieser zusätzliche Aufwand muss beim weiteren Ausbau des NCSC berücksichtigt werden.

Nach einem Cyberangriff wird das NCSC die Betreiberin der betroffenen kritischen Infrastruktur bei der Vorfallbewältigung unterstützen. Auch diese Unterstützungsleistung ist dank der langjährigen Erfahrung des NCSC (und früher von MELANI) bereits gut eingespielt. Dennoch ist zu erwarten, dass sich der Aufwand für das NCSC durch die Einführung der Meldepflicht erhöht. Erstens ist damit zu rechnen, dass mehr Meldungen eingehen und zweitens ist das NCSC neu in der Pflicht, mindestens eine erste Einschätzung und Empfehlungen zur Bewältigung des Vorfalls abzugeben. Das technische Analyseteam des NCSC (GovCERT) muss deshalb ebenfalls weiter ausgebaut werden.

Dieser Mehrbedarf ist bei den laufenden Arbeiten zum Ausbau des NCSC zu berücksichtigen. Er kann nicht vollständig losgelöst von den anderen Aufgaben des NCSC hinreichend abgeschätzt werden, weshalb das Ergebnis der aktuell noch laufenden Wirksamkeitsüberprüfung der Cyberorganisation des Bundes abgewartet wird. Der Ressourcenbedarf wird in Kenntnis des Ergebnisses dieser Vernehmlassung für die Botschaft der Änderung des ISG konkretisiert.

## 5.2 Auswirkungen auf Kantone und Gemeinden

Den Kantonen und Gemeinden werden mit dieser Vorlage keine neuen Aufgaben zugewiesen, sie sind aber von der Meldepflicht aus zwei Gründen betroffen. Erstens unterstehen die Kantons- und Gemeindebehörden selber gemäss Artikel 74b Buchstabe b der Meldepflicht und zweitens haben viele der meldepflichtigen Unternehmen kantonale oder kommunale Trägerschaften.

Im Gegenzug profitieren Kantone und Gemeinden aber auch von den Leistungen des NCSC, um sich besser vor Cyberrisiken schützen zu können. Bereits zum heutigen Zeitpunkt sind zahlreiche Kantone und Städte in den Informationsaustausch zwischen kritischen Infrastrukturen und dem NCSC integriert.

## 5.3 Auswirkungen auf die Volkswirtschaft und die Gesellschaft

Direkte Auswirkungen auf die Volkswirtschaft, die Gesellschaft und die Umwelt sind nicht zu erwarten. Von der Einführung einer Meldepflicht für Cyberangriffe werden die Volkswirtschaft und Gesellschaft indirekt profitieren, da die Verbesserung der Cybersicherheit von kritischen Infrastrukturen auch dazu dient, die Cybersicherheit in der Schweiz besser schützen zu können. Weiter trägt die Meldepflicht dazu bei, dass dank frühzeitiger Präventions- und geeigneter Abwehrmassnahmen verhindert werden kann, dass Cyberangriffe auf kritische Infrastrukturen Funktionsstörungen und -ausfälle von essentiellen Dienstleistungen verursachen, die das ordnungsgemässe Funktionieren von Wirtschaft und Staat gefährden.

Die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen hat kaum oder nur vernachlässigbare Auswirkungen auf die Volkswirtschaft oder auf die betroffenen Unternehmen. Es kann daher auf eine Regulierungsfolgenabschätzung (RFA) verzichtet werden.

Die Meldepflicht hilft, Transparenz über die Bedrohung durch Cyberangriffe zu schaffen und trägt dazu bei, die Bevölkerung für Cyberrisiken zu sensibilisieren. Eine erhöhte Cyberkompetenz der Bevölkerung ist eine wichtige Voraussetzung für die erfolgreiche Digitalisierung der Gesellschaft.

# 6 Rechtliche Aspekte

## 6.1 Verfassungsmässigkeit

Eine ausdrückliche Rechtsgrundlage für die Einführung einer Meldepflicht für Cyberangriffe ist der Bundesverfassung nicht zu entnehmen. Für die Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen kann sich der Bund auf seine inhärente Bundeskompetenz zum Schutz der inneren und äusseren Sicherheit der Eidgenossenschaft abstützen.

Die kritischen Infrastrukturen haben eine hohe Sicherheitsrelevanz für Gesellschaft, Wirtschaft und Staat. Die potenziell schwerwiegenden und landesweiten Auswirkungen von Cyberangriffen auf kritische 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 Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen hat ferner zum Ziel, anhand der Meldungen eine Analyse der Bedrohungslage zwecks Frühwarnung und Gefahrenabwehr zu erstellen. Aus dem Zweck der Meldepflicht ergibt sich, dass sie in ihrem Umfang auf Cyberangriffe auf kritische Infrastrukturen beschränkt werden soll. Das Melderecht bei Cybervorfällen und Schwachstellen, das jedermann offensteht, steht ergänzend zur weiteren Informationsgewinnung im Dienst des Schutzes der kritischen Infrastrukturen.

Entsprechend ist die inhärente Bundeskompetenz zur Wahrung der inneren und äusseren Sicherheit – mithin Zuständigkeiten, die dem Bund nicht explizit zugeteilt werden, ihm aber aufgrund seiner Staatlichkeit zukommen – eine geeignete Verfassungsgrundlage, um gestützt darauf Gesetzesbestimmungen für eine Meldepflicht für Cyberangriffe und ein Melderecht bei Cybervorfällen und Schwachstellen einzuführen.

Als Platzhalter für diese inhärente Bundeskompetenz wird aufgrund formell-gesetzestechnischer Konvention[40] Artikel 173 Absatz 2 BV zitiert. Das Informationssicherheitsgesetz erwähnt in seinem Ingress – neben Artikel 54 Absatz 1, 60 Absatz 1, 101, 102 Absatz 1 und 173 Absatz 1 Buchstaben a und b – auch Artikel 173 Absatz 2 als massgebende Kompetenzgrundlage. Es besteht somit kein Bedarf für die Ergänzung von Verfassungsbestimmungen im Ingress des ISG.

## 6.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Die Einführung einer Meldepflicht für Cyberangriffe tangiert keine bestehenden internationalen Verpflichtungen der Schweiz. Sie ist vergleichbar mit den Regulierungen, die viele andere Staaten, insbesondere die EU-Mitgliedstaaten, in den letzten Jahren eingeführt haben.

## 6.3 Erlassform

Als Gesetzesgrundlage für die Einführung der Meldepflicht scheint eine Ergänzung des bereits verabschiedeten ISG ideal, zumal dieses nicht nur durch Zweck, Gegenstand und Anwendungsbereich im Grundsatz mit der Meldepflicht für kritische Infrastrukturen vereinbar ist, sondern auch die formellgesetzliche Grundlage für das NCSC als Meldestelle bildet. Aus systematischer Sicht kann die Meldepflicht für Cyberangriffe sowie die Aufgaben des NCSC zum Schutz der Cybersicherheit im 5. Kapitel eingefügt werden.

Für die Ausführungsbestimmungen zur Meldepflicht wird noch zu entscheiden sein, ob für diese eine eigenständige Verordnung geschaffen oder die bestehende Cyberrisikenverordnung ergänzt soll.

40 Rz. 25 der Gesetzestechnischen Richtlinien des Bundes, www.bk.admin.ch > Dokumentation > Rechtsetzungsbegleitung > Gesetzestechnische Richtlinien GTR

## 6.4 Unterstellung unter die Ausgabenbremse

Mit der Vorlage werden weder neue Subventionsbestimmungen (die Ausgaben über einem der Schwellenwerte nach sich ziehen) geschaffen, noch neue Verpflichtungskredite / Zahlungsrahmen (mit Ausgaben über einem der Schwellenwerte) beschlossen.

## 6.5 Einhaltung des Subsidiaritätsprinzips und des Prinzips der fiskalischen Äquivalenz

Bei der Zuweisung und Erfüllung staatlicher Aufgaben ist der Grundsatz der Subsidiarität zu beachten (Artikel 5*a* BV). Gemäss Artikel 43*a* Absatz 1 BV übernimmt der Bund nur die Aufgaben, welche die Kraft der Kantone übersteigen oder einer einheitlichen Regelung durch den Bund bedürfen. Gleichzeitig hat der Bund von seinen Kompetenzen einen schonenden Gebrauch zu machen und den Kantonen ausreichend Raum für die Aufgabenerfüllung zu überlassen.

Eine Meldepflicht für Cyberangriffe auf kritische Infrastrukturen kann nicht wirkungsvoll umgesetzt werden, wenn sie nicht landesweit und sektorenübergreifend gilt. Ohne einheitliches Meldeverfahren und zentrale Meldestelle ist Cyberangriffen, die sich über geografische und sektorielle Grenzen hinweg ereignen, nicht beizukommen. Entsprechend der verfassungsmässigen Kompetenz des Bundes wurde die Meldepflicht auf Cyberangriffe bei kritischen Infrastrukturen beschränkt, da deren Auswirkungen eine Bedrohung für die Landessicherheit und das ordnungsgemässe Funktionieren des Staates darstellen können. Die Einführung der Meldepflicht stellt deshalb eine Massnahme dar, die mit dem Subsidiaritätsprinzip (Artikel 5*a* i.V.m. 43*a* BV) vereinbar ist.

Nach dem in Artikel 43*a* Absätze 2 und 3 BV statuierten Prinzip der fiskalischen Äquivalenz trägt das Gemeinwesen, in dem der Nutzen einer staatlichen Leistung anfällt deren Kosten; das Gemeinwesen, das die Kosten einer staatlichen Leistung trägt, kann über die Leistungen bestimmen. Im Zusammenhang mit der Einführung der Meldepflicht ist dieses Prinzip gewahrt, da die Kosten für den Betrieb der zentralen Meldestelle beim Bund anfallen werden. Für die kritischen Infrastrukturen ändert sich mit der Einführung der Meldepflicht wenig: sie können wie bisher auf die Unterstützung des NCSC bei der Vorfallbewältigung zählen. Im Vergleich zu freiwilligen Meldungen zu Cybervorfällen entsteht durch die Meldepflicht nur ein geringer Mehraufwand. Somit entstehen auch bei kritischen Infrastrukturen, die von Kantonen und Gemeinden betrieben werden, keine eigentlichen Zusatzkosten durch die Meldepflicht.

## 6.6 Delegation von Rechtsetzungsbefugnissen

Die für die Einführung der Meldepflicht für Cyberangriffe wesentlichen Eckwerte sollen gemäss dem vorliegenden Vernehmlassungsentwurf auf Gesetzesstufe verankert werden.

Der Bundesrat wird dazu Ausführungsbestimmungen erlassen, um die gesetzlichen Bestimmungen, sofern nötig, zu konkretisieren. Insbesondere obliegt es dem Bundesrat nach Art. 74c den Adressatenkreis der Meldepflicht weiter einzuschränken. Das Gesetz definiert die dafür anzuwendenden Kriterien, es muss aber durch den Bundesrat pro Sektor festgelegt werden, welche Kriterien wie angewendet werden (Beispielsweise über die Definition von geeigneten Schwellenwerten.

## 6.7 Datenschutz

Die Vernehmlassungsvorlage hat die datenschutzrechtlichen Vorgaben im Wesentlichen unverändert übernommen, wie sie vom Parlament im 5. Kapitel des ISG ursprünglich im Zusammenhang mit der Unterstützung für kritische Infrastrukturen verabschiedet wurden.

Bei der Erarbeitung der Vernehmlassungsvorlage wurde der EDÖB konsultiert. Es wurden dabei auch Koordinationsmöglichkeiten mit der Meldepflicht bei Verletzung der Datensicherheit diskutiert.