

Generelle Bemerkungen zur Teilrevision des Fernmeldegesetzes (FMG) im Bereich Sicherheit

Eher Ablehnung

Mit Schreiben vom 27. Mai 2026 hat der Bundesrat das Vernehmlassungsverfahren für eine Teilrevision des Fernmeldegesetzes (nachfolgend «E-FMG») im Bereich Sicherheit eröffnet. Diese bezweckt die Verbesserung der Sicherheit der Fernmeldeinfrastrukturen und -dienste vor Cyberbedrohungen sowie weitere Themen. Gleichzeitig hat der Bundesrat dazu auch Änderungen verschiedener Verordnungen in die Vernehmlassung gegeben (nachfolgend «E-FDV», «E-FAV», etc.). Diese Änderungen stützen sich auf die Kompetenzdelegation des geltenden Art. 48a Abs. 2 FMG ab, welche im Rahmen der FMG-Teilrevision beibehalten und im Gesetzesvorentwurf neu in Abs. 4 von Art. 48a E-FMG vorgesehen ist. Ein gewichtiger Teil der Ordnungsänderungen betrifft den Betrieb der Mobilfunknetze und soll im Hinblick auf die geplante Neuvergabe der 2012 zugeteilten Mobilfunkfrequenzen für die Jahre ab 2029 frühzeitig in Kraft treten, so dass den Bieterinnen in der Frequenzauktion die zukünftigen Bedingungen zum Betrieb der Mobilfunknetze bekannt sein werden. Aufgrund weiterer vorgesehener Kompetenzdelegationen im FMG-Vorentwurf ist davon auszugehen, dass in Kürze weitere Anpassungen der Verordnungen zum FMG im Bereich Netzsicherheit und Cyberschutz durch BAKOM und Bundesrat folgen werden. Die Regulierungskadenz für Fernmeldediensteanbieterinnen (nachfolgend «FDA») bleibt damit hoch, was für die Branche und viele insbesondere kleinere Anbieterinnen eine Herausforderung darstellt.

Für unsere Anträge zu den geplanten Änderungen des Ordnungsrechts verweisen wir auf das entsprechende Dossier im Online-Tool (Plattform Consultations). Wir halten uns dort mit allgemeinen Bemerkungen kurz und verweisen hierfür auf den vorliegenden Vernehmlassungsbeitrag.

1. Suissedigital

Suissedigital ist der Dachverband der Schweizer Telekommunikationsnetzunternehmen und vertritt die Interessen von ca. 170 privatrechtlich oder öffentlich-rechtlich organisierten Unternehmen verschiedener Grösse, die lokal, regional oder landesweit Telekommunikationsinfrastrukturen (Fest- und Mobilfunknetze) betreiben und darüber verschiedene Fernmeldedienste erbringen. Das grösste Verbandsmitglied ist die Sunrise GmbH (nachfolgend «Sunrise»), die als grösstes privates Telekommunikationsunternehmen in der Schweiz ein eigenes konzessioniertes Mobilfunknetz betreibt, das auch eine Vielzahl von anderen Mitgliedern von Suissedigital als Mobile Virtual Network Operator (MVNO) zur Vermarktung eigener Mobilfunkdienste nutzen. In Bezug auf die geplante Regulierung der sogenannten Full MVNO in der E-FDV ist zu erwähnen, dass Mitglieder von Suissedigital beabsichtigen, zukünftig eigene Mobilfunkdienste unter diesem MVNO-Modell zu erbringen.

Die Mitglieder von Suissedigital sind in Bezug auf ihre Organisationsstruktur unterschiedlich aufgestellt. Der Betrieb der Fernmeldenetze und die Bereitstellung der Fernmeldedienste erfolgen in der Regel in arbeitsteiligen Prozessen. Je nach Grösse und Struktur der Unternehmen wird dabei in unterschiedlichem Ausmass und Organisationsgrad auf Dienste und Produkte Dritter (Lieferanten) zurückgegriffen. Dabei setzen sie im Netzbetrieb unterschiedliche Netztechnologien und -architekturen ein.

2. Einleitung zu den generellen Bemerkungen

Angesichts zunehmender Angriffe auf digitale Systeme in der Schweiz sowie der zunehmenden Unruhe der allgemeinen geopolitischen Lage haben wir Verständnis für das verstärkte Tätigwerden von Gesetz- und Verordnungsgeber im Bereich Netzsicherheit und Abwehr von Cyberbedrohungen. Wir möchten jedoch daran erinnern, dass die Schweizer FDA in den letzten Jahren nicht untätig waren und der technischen Entwicklung sowie der damit einhergehenden veränderten Bedrohungslage durch Cyberangriffe auf ihre Netze und Kundenschaft nicht einfach tatenlos zugesehen haben (vgl. beispielsweise auch die Gründung eines Konsortiums zur proaktiven Betrugsbekämpfung durch Swisscom und Sunrise). So bilden die Sicherheit der Fernmeldeinfrastruktur und deren Dienste für die Mitglieder und Suissedigital selbst seit langem ein zentrales strategisches Verbandsthema, wobei der technische Wandel und die Innovation in diesem Bereich aufmerksam verfolgt werden (so beispielsweise auch in Bezug auf den möglichen Einsatz Künstlicher Intelligenz bei der Überwachung, Detektion und Analyse von Cyberzwischenfällen im Netz).

Der seit Jahren stattfindende Infrastrukturwettbewerb sowie die konvergierten digitalen Dienste haben dazu geführt, dass sich in der Schweiz zahlreiche Anbieterinnen miteinander konkurrenzieren. Dabei kommen für den Netzbetrieb unterschiedliche Technologien und Architekturen zum Einsatz. Teilweise betreiben sie ihre Netze auch parallel zueinander, kleinere kommunale und regionale Netzbetreiberinnen neben grossen nationalen Netzbetreiberinnen. Diese fragmentierte regionale Netzvielfalt mit unterschiedlichen Technologien, Architekturen und Betriebsmodellen, die von unabhängigen Netzbetreiberinnen bereitgestellt wird und sich teilweise überlagert, führt bereits für sich genommen zu einer hohen Widerstandsfähigkeit des gesamten Systems und zu einer höheren Versorgungssicherheit in der Telekommunikation. Föderale, regionale und fragmentierte Infrastrukturen sind schwieriger anzugreifen als zentral geführte Monopolinfrastrukturen.

Den Vernehmlassungsunterlagen lassen sich keine Informationen zu einer Regulierungsfolgenabschätzung entnehmen. Aus unserer Sicht sollte eine solche nach Verarbeitung der eingegangenen Vernehmlassungen einerseits im Hinblick auf die parlamentarische Beratung der FMG-Teilrevision und andererseits im Hinblick auf die Ausarbeitung der finalen Verordnungen unbedingt erfolgen.

3. Unterstützung des vorliegenden Projekts mit gewichtigen Vorbehalten

Wir unterstützen das Ziel, die Cybersicherheit und die Widerstandsfähigkeit der Fernmeldeinfrastrukturen besser gegen Cyberangriffe zu schützen. Das vorgeschlagene Teilrevisionsprojekt geht aber in mehreren zentralen Punkten zu weit und sieht Massnahmen vor, deren Nutzen für eine erweiterte Sicherheit der Fernmeldeinfrastrukturen nicht gegeben oder teilweise sogar kontraproduktiv sind, die aber grosse Auswirkungen für die Netze und deren Betrieb durch die FDA nach sich ziehen würden. Die Revision sollte daher streng auf risikobasierte, technologieneutrale und verhältnismässige Massnahmen fokussieren, die sich konsequent an anerkannten technischen Standards und nicht an geopolitische Tendenzen orientieren.

Im Interesse unserer Mitglieder, insbesondere der kleineren Anbieterinnen im Verband, müssen neue Vorschriften, Auflagen und Aufgaben effizient, in wirtschaftlicher Hinsicht tragbar und angemessen sein. Die fragmentierte Fernmeldeinfrastruktur in der Schweiz, die gerade deshalb auch einen grossen Beitrag zur Widerstandsfähigkeit des Systems beiträgt, darf dabei nicht aufs Spiel gesetzt werden. Kleinere Anbieterinnen dürfen nicht in Folge ineffizienter und überhöhter Auflagen aus dem Markt gedrängt werden. Dies würde für den Schweizerischen Fernmeldemarkt ein klassisches Eigentor darstellen. Wir plädieren deshalb aus Sicht unserer Mitglieder, aber auch aus Sicht der Schweizer Volkswirtschaft für eine wirtschaftlich tragbare und verhältnismässige Ausgestaltung der Sicherheitsanforderungen. Unter Umständen sind deshalb auch Abstufungen der Auflagen und Massnahmen nach Grösse und wirtschaftlicher Bedeutung der betroffenen Netze/betroffenen FDA oder grössenrelevante Ausnahmen vorzusehen. Weiter müssen neue Kompetenzdelegationen im Gesetz klar abgesteckt sein, dürfen sich nicht überschneiden und deren Folgen in der Praxis müssen voraussehbar

sein, damit die Rechtsunsicherheit für die FDA möglichst gering ausfällt.

4. Verbesserung der Sicherheit von Fernmeldeinfrastrukturen und Schutz vor Cyberbedrohungen

a. Einleitung

Mit den vorgeschlagenen Änderungen soll durch Verbesserung der Sicherheit von Fernmeldeinfrastrukturen der Schutz dieser Systeme gegenüber Bedrohungen aus dem Cyberraum verbessert werden. Dies ist thematisch der rote Faden, der sich durch alle Vernehmlassungsunterlagen zieht. Eine zentrale Rolle dabei spielen die geplanten Änderungen zu Art. 48a FMG (Sicherheit). Wie der erläuternde Bericht richtigerweise in Erinnerung ruft, hat diese Bestimmung seit ihrer Aufnahme ins Gesetz «die Bekämpfung von Cyberangriffen (z.B. Verteilung von Schadsoftware, Beeinträchtigung von Web-Diensten durch DDoS-Attacken) zum Ziel» (vgl. erläuternder Bericht, Seite 57 unten). Dies soll nun neu auch ausdrücklich als Aufgabe der FDA in der revidierten Bestimmung Erwähnung finden. Es geht also vorliegend in der Hauptsache um den verbesserten Schutz der FDA-Infrastruktur vor Cyberbedrohungen. Andere Risiken für den ordnungsgemässen Betrieb der Fernmeldeinfrastruktur werden mit der vorliegenden Teilrevision nicht adressiert, und werden auch im erläuternden Bericht nicht angesprochen. Wir denken dabei beispielsweise an Ausfälle aufgrund von Strommangel oder an Risiken im Zusammenhang mit dem physischen Zugang zur Infrastruktur (Vandalismus). Wenn also im erläuternden Bericht von Resilienz die Rede ist, so bezieht sich dies immer auf die Abwehr vor Cybervorfällen. Wir regen an, dies an geeigneter Stelle im erläuternden Bericht klarzustellen und zu präzisieren. Es bestehen Befürchtungen in der Branche, dass die geplanten Änderungen generell z.B. auch als Basis für Forderungen nach einer Härtung der Fernmeldeinfrastruktur gegen Stromunterbrüche etc. herangezogen werden.

b. Gesetzlich vorgeschriebene Diversifikation der Hersteller kritischer Netzbestandteile und behördliches Verbotsrecht ist ungeeignet und kontraproduktiv (Art. 48b Abs. 2 und 3 E-FMG)

Gemeinsam mit der gesamten Branche lehnen wir die vorgesehene Verpflichtung zu einer Diversifikation der Hersteller für kritische Netzkomponenten im Netz entschieden ab. Eine staatlich vorgeschriebene Verteilung der Komponenten auf mehrere Hersteller erhöht weder die Sicherheit noch reduziert sie die Abhängigkeit von einzelnen Herstellern und Lieferanten. Im Gegenteil führt sie zu einer höheren Komplexität des Netzes, gegebenenfalls auch durch die dadurch notwendige Integration verschiedener Systeme und unterschiedlicher Sicherheitskonfigurationen zu komplexen und gefährlichen neuen Schnittstellen und damit Einfallstore für Gefährder. Aufgrund der höheren Integrationsaufwände und gegebenenfalls wegfallender Synergieeinsparungen würde dies zudem zu deutlich höheren Verwaltungs- und Betriebskosten führen – und das in unverhältnismässig grossem Umfang für kleinere FDA, die ohnehin nur wenig Möglichkeiten haben, Markt und Preise bei der Gerätebeschaffung zu beeinflussen.

Auch das vorgesehene Kriterium, dass zumindest eine eingesetzte Herstellerin ihren Hauptsitz in einem Staat mit angemessenem Datenschutz haben muss, ist eine ungeeignete Massnahme zur Verbesserung der Sicherheit. Das Kriterium ist sachfremd, da über die Netzkomponenten keine Personendaten mit dem Hersteller ausgetauscht werden - andernfalls die Vorgabe automatisch auf das Zielland anwendbar wäre - und ein angemessener Datenschutz am Hauptsitz des Herstellers bietet keine Gewähr dafür, dass eine bestimmte Komponente keine Sicherheitslücken für einen Cyberangriff aufweist. Im Gegensatz zur aktuellen Bestimmung von Art. 96f Abs. 2 FDV (Betrieb NOC und SOC ausschliesslich in einem Staat mit angemessenem Datenschutz) stellt dieses Kriterium vorliegend ein untaugliches Mittel dar, um den Schutz zu erhöhen.

Der Anbietermarkt von Netzkomponenten ist beschränkt und in vielen Fällen setzen Hersteller in ihren Produkten Komponenten anderer Hersteller ein. Würden einzelne Komponenten verboten werden, könnten diese also trotzdem in anderen Produkten zum Einsatz gelangen. Wir lehnen die vorgesehene Kompetenz des BAKOM, Netzkomponenten zu verbieten bzw. solche aus dem Netz entfernen zu lassen, ab. Die FDA haben

selbst das grösste Interesse daran, ausschliesslich sichere Netzkomponenten inklusive dazugehöriger Software in ihren Netzen einzusetzen. Sie wählen die Produkte mit grösster Sorgfalt aus und berücksichtigen dabei internationale Erfahrungen und Standards. Technologien, Infrastrukturen und Cyberbedrohungen entwickeln sich ständig weiter, wie der erläuternde Bericht zu Recht festhält (vgl. erläuternder Bericht, Seite 62). Wie bereits einleitend erwähnt, verfolgen die FDA als Spezialistinnen diese technologischen Entwicklungen und können daher rasch und zielgerichtet auf neue und neu erkannte Risiken reagieren. Die FDA tauschen sich über Erfahrungen und Informationen zu möglichen einsetzbaren Bestandteilen und deren Risiken aus. Sinnvoll ist es, diesen Informationsfluss und -austausch unter Einbezug von Behörden und Organisationen, die im Bereich der Cybersicherheit tätig sind, zu stärken. Dies ist richtigerweise in der Gesetzesvorlage an verschiedenen Stellen auch so vorgesehen.

Bei der Lektüre des erläuternden Berichts zu dieser Bestimmung fällt zudem auf, dass der Bundesrat vor allem die Mobilfunknetze im Auge hat. Es werden Beispiele von Komponenten des Mobilfunk-Kernnetzes oder des Funkzugangsnetzes erwähnt (vgl. erläuternder Bericht, Seite 62). Unser Mitglied Sunrise setzt für sein Mobilfunknetz bereits seit Jahren risikobasiert und nach internationalen Sicherheitsstandards eine erfolgreiche Single- und Multi-Vendor-Strategie um, soweit dies technisch und wirtschaftlich sinnvoll ist. Und für Mobilfunknetzbetreiberinnen gelten bereits gemäss Art. 96d ff. FDV erhöhte Anforderungen an die Netzsicherheit, Organisation und internen Prozesse. Mit der gleichzeitigen Revision des Verordnungsrechts sollen diese Auflagen noch weiter ausgebaut werden. Der Regulator greift hier in Kernkompetenzen einer Netzbetreiberin ein und masst sich an, für die Stärkung von Resilienz geeignetere Massnahmen zu treffen als diese selbst. Es ist daran zu erinnern, dass eine Netzbetreiberin aus eigenen wirtschaftlichen Interessen für hohe Sicherheitsstandards sorgt.

Wir fordern deshalb, dass die Wahl der Produkte und Lieferanten bei den Fachspezialisten, den FDA, verbleibt und nicht von einer Behörde vorgegeben wird. Eine Fokussierung auf die eingesetzte Hardware zur Verbesserung der Sicherheit setzt an der falschen Stelle an. Es ist vielmehr die Software oder das Zusammenspiel der verschiedenen Softwarekomponenten, die erfahrungsgemäss zu Lücken im Sicherheitsdispositiv führen können. Schliesslich könnten eine Diversifikationspflicht sowie Produktverbote für Komponenten des HFC-Netzes aufgrund des begrenzten Angebots schwerlich umsetzbar sein.

c. Zu offener Begriff der kritischen Bestandteile einer Fernmeldeinfrastruktur (Art. 48b Abs. 2 E-FMG)

In der Vorlage werden teilweise neue Begrifflichkeiten verwendet, deren materieller Gehalt unklar oder nicht genügend präzisiert ist. Beispiele dafür sind der Begriff «ein begründetes Sicherheitsrisiko» in Art. 48b Abs. 3 E-FMG oder auch der Begriff «ein geopolitisches Risiko» in Art. 48c Abs. 1 E-FMG. Dem FMG-Vorentwurf lässt sich auch keine präzise und widerspruchsfreie Definition von «kritischen Bestandteilen der Fernmeldeinfrastruktur» gemäss Art. 48b Abs. 2 E-FMG entnehmen. Dass gleichzeitig in der überarbeiteten FAV der neue Begriff der «kritischen Netzwerkanlage» (vgl. Art. 2 Abs. 1 Bst. c^{bis} E-FAV) eingeführt werden soll, sich der erläuternde Bericht aber nicht über das Verhältnis dieser Begriffe zueinander äussert, macht es nicht einfacher. Damit könnte eine FDA nicht zweifelsfrei im Voraus eruieren, welche Komponenten im Netz von der neuen Diversifikationspflicht betroffen wären und welche nicht. Dies hätte erhebliche Planungs- und Investitionsunsicherheiten bei den Netzbetreiberinnen zur Folge, was bedeutende und langfristige Investitionen gefährdet. Der Logik des Vorentwurfes folgend könnte sodann eine einmal gewählte und installierte Netzkomponente nach Art. 48b Abs. 3 E-FMG auf der schwarzen Liste des BAKOM landen und deren Ausserbetriebnahme verfügt werden, was enorm weitreichende Folgen für die gesamte Netzarchitektur haben kann, mit nach oben offenen Kostenfolgen für eine Anbieterin und negativen Konsequenzen für Endkunden. Schliesslich wird im erläuternden Bericht auch noch angeführt, dass der Bundesrat auf Grundlage von Art. 48a Abs. 4 E-FMG darüber hinaus weitere kritische Netzteile regulieren bzw. verbieten könnte. Das macht das anwendbare Regime noch einmal unübersichtlicher. Schon nur diese überlagernden Kompetenzen machen es kompliziert. Wir fordern deshalb die ersatzlose Streichung von Art. 48b Abs. 2 und 3 (vgl. detaillierte Stellungnahme) oder

eine präzise Definition und Kompetenzregelung auf Gesetzesstufe, die sich an international anerkannten Standards und Normen orientiert und die Beeinflussung durch geopolitische Interessen ausschliesst.

Sollte an den geplanten Änderungen von Art. 48b E-FMG im Grundsatz festgehalten werden, so müsste zwingend eine Abstufung der einzuhaltenden Vorgaben nach Grösse und Bedeutung des betroffenen Netzes/der betroffenen FDA vorgesehen werden. Auch wären dabei die beschränkten Möglichkeiten und Eigenheiten des Beschaffungsmarktes für HFC-Netze besonders zu berücksichtigen. Ein starrer Ansatz ist ungeeignet, unverhältnismässig und würde die bestehende dezentrale Fernmeldeinfrastruktur unnötig aufs Spiel setzen.

d. Unnötiges Herstellerverbot aufgrund geopolitischer Risiken

Was die vorgesehene Möglichkeit eines vollständigen Herstellerverbotes betrifft, so stellen wir dessen Relevanz in Frage. Wir anerkennen zwar aufgrund der geo- und sicherheitspolitischen Entwicklung ein Bedürfnis, die Verwendung von Netzkomponenten eines Herstellers vollständig zu verbieten. Die Bedingungen und Voraussetzungen für ein solches Verbot müssten jedoch im Gesetz präziser normiert sein. Dies gilt auch mit Blick auf den Begriff „geopolitisches Risiko“. Weiter sollte ein solches Verbot nur für kritische Netzelemente dieses Herstellers und auch nur dann ausgesprochen werden können, wenn keine anderen Sicherheitsmassnahmen ausreichen (Subsidiarität). Auch sollte für einen derart weitreichenden Entscheid zwingend das Parlament mitbezogen werden. Ein Verbot, gewisse Netzkomponenten eines Herstellers nicht mehr verwenden bzw. entfernen zu müssen, hätte sehr weitreichende finanzielle und technische Folgen, die es zu berücksichtigen gilt. Unseres Erachtens bieten demgegenüber die bestehenden Notstandsrechtsinstrumente bereits eine ausreichende Grundlage für derart ausserordentliche Situationen, die gleichzeitig auch den Einbezug des Parlaments gewährleisten.

5. Stärkung Notrufsystem

Wir unterstützen das Anliegen einer leistungsfähigen und robusten Notkommunikation. Die vorgeschlagenen Änderungen beinhalten jedoch teilweise Anforderungen, die die FDA technisch nicht umsetzen und gewährleisten können. Keine FDA kann sicherstellen, dass eine Notkommunikation jederzeit «End-to-End» funktioniert, da hierfür auch zahlreiche Akteure und Systeme ausserhalb ihrer Kontrolle verantwortlich sind. Die Einführung zusätzlicher Systemaufgaben, wie beispielsweise eines ausschliesslich für die Notkommunikation vorgesehenen ESInet, bringt keinen nachgewiesenen Sicherheits- und Verfügbarkeitsgewinn, erhöht jedoch die Komplexität des gesamten Systems und dessen Kosten.

6. Zusammenfassung generelle Bemerkungen

Suissedigital unterstützt weitere Massnahmen für eine höhere Cybersicherheit in Bezug auf die Netze, die Dienste sowie deren Benutzerinnen und Benutzer. Die Revision sollte sich jedoch ausschliesslich auf Massnahmen konzentrieren, die nachweislich die Sicherheit und Widerstandsfähigkeit erhöhen, risikobasiert, verhältnismässig und technisch umsetzbar sind und sich streng an international anerkannten Standards orientieren. Wir lehnen namentlich folgende Vorschläge ausdrücklich ab:

- Diversifikationspflicht nach Hersteller bei Netzkomponenten (Art. 48b Abs. 2 E-FMG);
- Behördliches Verbot von Netzkomponenten und Herstellern (Art. 48b Abs. 3 und 48c E-FMG);
- unklare und zu weit gefasste Resilienz- und Verfügbarkeitsanforderungen bei der Notkommunikation (Art. 20ff. E-FMG);
- Änderungen der Verordnungen bezüglich des Betriebs von NOC und SOC ausschliesslich in der Schweiz sowie weitreichende Kompetenz des BAKOM hinsichtlich kritischer Netzwerkanlagen.

Stattdessen soll die bestehende Zusammenarbeit zwischen den Fernmeldediensteanbieterinnen und den verschiedenen Fachorganisationen weiter gestärkt und ausgebaut werden.

Sollte trotzdem an Vorschriften über die Wahl von Hersteller- und Lieferanten sowie an der Möglichkeit behördlicher Produktverbote festgehalten werden, so müsste zwingend eine Abstufung nach Grösse und Bedeutung des betroffenen Netzes/der betroffenen FDA oder grössenrelevante Ausnahmen vorgesehen werden. Dabei wären die beschränkten Möglichkeiten und Eigenheiten des Beschaffungsmarktes für HFC-Netze besonders zu berücksichtigen.

Für unsere konkreten Änderungsanträge verweisen wir auf die detaillierte Stellungnahme. Keine Bemerkungen haben wir zu den geänderten Bestimmungen im Vorentwurf, die wir nicht kommentieren.

Detaillierte Stellungnahme (Änderungsanträge)

Sperrung des Zugangs zu Telefonie und Internet: Art. 6a Abs. 2	Ablehnung
---	------------------

Begründung:

Eine gesetzliche Pflicht der zuständigen Behörde, vor einer Sperrung abzuklären, ob eine Überwachung läuft, schafft die klare Verantwortlichkeit, dass Behörden unter sich klären, wann auf eine Sperre zu verzichten ist. In der Praxis dienen oft die FDA als erste Informationsstelle und Informationsdrehscheibe für die Untersuchungsbehörden, fedpol und dem Dienst ÜPF, was nicht ihre Aufgabe ist. So sollten die Behörden direkt beim Dienst ÜPF die benötigten Informationen beschaffen.

Änderungsantrag:

~~Die zuständigen Behörden stellen sicher, dass auf eine Sperrung verzichtet wird, wenn ihnen bekannt ist, dass der betreffende Zugang zu Internet oder Telefonie Gegenstand eines Überwachungsauftrags des Dienst Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF) ist. In diesen Fällen erfolgt eine Rücksprache mit dem Dienst ÜPF. Die zuständigen Behörden klären beim Dienst Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF) ab, ob der betreffende Zugang zu Internet oder Telefonie Gegenstand eines Überwachungsauftrags ist. In diesen Fällen sorgt die zuständige Behörde dafür, dass auf eine Sperrung verzichtet wird.~~

Sperrung von Telefonnummern und Domain-Namen: Art. 6b Abs. 1 und 5	Ablehnung
---	------------------

Begründung:

Absatz 1: Grundsätzlich begrüssen wir die Möglichkeit, Telefonnummern und Domain-Namen aufgrund betrügerischer Aktivitäten zu sperren. Sperrungen von Telefonnummern sind jedoch immer heikel und stehen potenziell in Konflikt mit den Anforderungen des öffentlichen Telefondienstes sowie den vertraglichen Leistungsversprechen. Dabei stehen in erster Linie die FDA gegenüber der Kundschaft in der Verantwortung und haben über eine Sperrung Rechenschaft abzulegen. Es kann deshalb nicht sein, dass die FDA – bezüglich der Domain-Namen die Registerbetreiberinnen – auf Zuruf oder wie im Gesetz vorgesehen ist, «auf Hinweis» einer Behörde Telefonnummern sperren. Falls der Behörde ein begründeter Verdacht auf einen mutmasslichen Betrug vorliegt, so haben sie eine Sperrung zu verfügen. Die FDA kennen die genauen Hintergründe nicht und können dafür nicht die Verantwortung übernehmen. An verschiedenen Stellen in Gesetz und Verordnung sind explizit Sperren durch die FDA vorgesehen, welche mit der vorliegenden Revision weiter ausgebaut werden sollen. Dies beispielsweise zum Schutz der Infrastruktur, des Notrufs oder zur Unterbindung von Spoofing. Diese Sperren werden von den FDA indiziert. Sie kennen die Beweggründe, tragen hierfür die Verantwortung und müssen sich gegebenenfalls auch gegenüber der Kundschaft rechtfertigen. Im vorliegenden Fall hat das fedpol die Sperre deshalb anzuordnen. Sodann und entsprechend ist gegebenenfalls auch eine Entsperrung anzuordnen.

Es ist vorgesehen, dass eine solche Sperre längstens fünf Tage andauern darf, danach muss sie durch eine Massnahme der Staatsanwaltschaft oder des Gerichts abgelöst werden. Unseres Erachtens ist die vorgesehene Frist von fünf Tagen zu kurz bemessen, da das Einleitungsverfahren bei Staatsanwaltschaft oder Gericht erfahrungsgemäss viel mehr Zeit beansprucht. Die Frist ist angemessen zu verlängern. Weiter stellt sich die Frage, durch welche vorgesehene Massnahme im Strafverfahrensrecht die Sperre abgelöst werden soll. Durch eine Beschlagnahmung gemäss Art. 263ff. StPO? Es stellt sich somit die Frage, ob eine Telefonnummer oder ein Domain-Name im strafprozessrechtlichen Sinn beschlagnahmt werden kann. Diese Fragen sind zu klären, namentlich sollte vermieden werden, im FMG neue und dazu nicht ausreichend definierte strafprozessuale Bestimmungen und Grundlagen zu kreieren (Grundsatz der Einheit der Rechtsordnung).

Absatz 5 verpflichtet die zuständigen Behörden, bei Vorliegen eines Überwachungsauftrags des Dienstes Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF) auf eine Sperrung zu verzichten. Wir halten es für richtig, dass die Verantwortung für eine Sperrung bzw. Nicht-Sperrung eindeutig bei der zuständigen Behörde und nicht bei den FDA liegt.

Unklar ist, welche Abklärungen die zuständige Behörde unternehmen muss, um Kenntnis von einem Überwachungsauftrag zu erlangen. Die Erfahrung zeigt, dass bei Sperrungen oder dem Verzicht auf Sperrungen regelmässig die FDA von den Untersuchungsbehörden, dem fedpol oder dem Dienst ÜPF konsultiert werden. Die FDA dürfen jedoch nicht als Informationsdrehscheibe für die Behörden fungieren. Eine ausdrückliche Pflicht der zuständigen Behörden, vor einer Sperrung aktiv abzuklären, ob eine Überwachung läuft, schafft klare Verantwortlichkeiten und verhindert auch, dass sich ermittelnde und überwachende Behörden gegenseitig behindern.

Änderungsantrag:

¹Die Anbieterinnen von Fernmeldediensten müssen auf ~~Hinweis Anordnung~~ des Bundesamts für Polizei (fedpol) bei einem begründeten Verdacht auf einen mutmasslichen Betrug nach Artikel 146 des Strafgesetzbuchs (StGB) die betreffende schweizerische Telefonnummer sperren; ~~die Sperrung darf höchstens fünf Tage dauern. Das fedpol ordnet die Entsperrung an.~~

⁵ ~~Bei der Sperrung von Telefonnummern stellt die zuständige Behörde sicher, dass keine solche erfolgt, sofern ihnen bekannt ist, dass die betroffene Nummer Gegenstand eines Überwachungsauftrags des Dienstes ÜPF ist. In diesen Fällen erfolgt eine Rücksprache mit dem Dienst ÜPF. Die zuständigen Behörden klären bei einer Sperrung von Telefonnummern beim Dienst Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF) ab, ob die betroffene Nummer Gegenstand eines Überwachungsauftrags ist. In diesen Fällen sorgt die zuständige Behörde dafür, dass auf eine Sperrung verzichtet wird.~~

Notkommunikation

Grundsätze: Art. 20 Abs. 1 und 2	Ablehnung
---	------------------

Begründung:

Absatz 1: Eine funktionierende und zuverlässige Notkommunikation ist elementar. Die FDA engagieren sich gemeinsam mit den kantonalen Notrufzentralen (PSAP) und dem BAKOM intensiv für deren Sicherstellung und der kontinuierlichen Verbesserung.

Damit ein Notruf «End-to-End» funktioniert, müssen zahlreiche technische Komponenten sowie verschiedene Akteure reibungslos zusammenwirken. Die Anbieterinnen leisten hierzu zwar einen wichtigen Beitrag, können die Notkommunikation jedoch unmöglich jederzeit sicherstellen, wie im erläuternden Bericht richtigerweise festgehalten wird. So haben sie weder Einfluss auf die Funktionalität der Endgeräte noch auf jene der Notdienste (vgl. erläuternder Bericht, u.a. Seite 36 unten).

Im Mobilfunk gilt aus technischen Gründen grundsätzlich das Best-Effort-Prinzip. Absolute Garantien lassen sich deshalb in der Praxis nicht umsetzen. Absatz 1 weckt Erwartungen, die realistischerweise nicht erfüllt werden können.

Absatz 2: Wie bereits zu Absatz 1 ausgeführt, können die FDA nicht für sämtliche Elemente der Notkommunikation verantwortlich gemacht und zur Gewährleistung von Redundanz verpflichtet werden. Die PSAP werden bereits heute durch einen kommerziellen Zweitanbieter erschlossen. Die «minimale Rückfallebene» gemäss Referenzmodell «Notrufe» (Kapitel 6) beschreibt eine Redundanz durch einen Zweitanbieter. Diese Redundanz ist damit bereits heute gewährleistet. Die Formulierung in Absatz 2 könnte missverstanden werden. Wir schlagen vor, allein diese Rückfallebene gemäss Referenzmodell zu erwähnen.

Änderungsantrag:

¹Die Anbieterinnen des öffentlichen Telefondienstes müssen sicherstellen, dass die Kommunikation zwischen den Benutzerinnen und Benutzern und den von den Notdiensten sowie den Hilfs- und Beratungsdiensten betriebenen Zentralen (Notkommunikation) jederzeit möglich ist ermöglichen.

² Sie müssen dazu insbesondere die Leitweglenkung, die Standortidentifikation und die Redundanz (eine minimale Rückfallebene) sicherstellen.

Systemaufgaben: Art. 20a Abs. 1 Bst. a, b und f	Ablehnung
--	------------------

Begründung:

Absatz 2, Bst. a verlangt ein ausschliesslich der Notkommunikation dienendes, jederzeit verfügbares Netz in Form eines «Emergency Services IP Network» (ESInet). Ein ESInet ist kein physisches, sondern ein virtuelles IP-Netz, über das die Notrufzentralen und PSAP neben Sprachdiensten auch Bild-, Video- und Textkommunikation übermitteln können (<https://www.etsi.org/newsroom/press-releases/2214-new-etsi-standard-enables-next-generation-emergency-services-communications>). Es ist ausschliesslich für die Kommunikation zwischen Notrufzentralen bzw. PSAP ausgelegt. Auf die Kommunikation zwischen Endnutzerinnen und Endnutzern sowie den Notrufzentralen hat ein ESInet keine Auswirkungen. Es bietet erweiterte Funktionalitäten für die Notkommunikation wie RTT und NGeCall (die jedoch auch über die bestehenden Netze funktionieren), erhöht jedoch die Ausfallsicherheit nicht. Der erläuternde Bericht weist auf Seite 73 in Fussnote 94 darauf hin, dass ein autonomes Netz nicht beabsichtigt ist. Mit einem ESInet steigt aber die Komplexität des gesamten Notkommunikationssystems und damit dessen Fehleranfälligkeit. Aus technischer Sicht besteht kein Bedarf für «ein ausschliesslich der Notkommunikation dienendes, jederzeit verfügbares Netz». Art. 20a Abs. 1 Bst. a und b sind deshalb zu streichen.

Bst. e verlangt den Betrieb einer Test- und Integrationsplattform, über die End-to-End-Tests für Geräte- und Fahrzeughersteller sowie für die Bevölkerung möglich sein sollen. Ein End-to-End-Test ist ein Funktionstest der Notrufkommunikation vom auslösenden Endgerät bis zur zuständigen Notrufzentrale. Dafür werden auch Test-Notrufzentralen benötigt, die die Entgegennahme von Testanrufen sicherstellen. Diese können nicht von den FDA betrieben werden. Dafür sind die Infrastruktur und die Fachkompetenz einer Notrufzentrale erforderlich.

Der Testumfang dieser Plattform muss im Rahmen der in Abs. 3 erwähnten technischen und administrativen Vorschriften (TAV) unbedingt klar definiert werden.

Bst. f: Die Akteure der Notkommunikation informieren sich schon heute umgehend und ausführlich über Fehlleitungen und Ausfälle. Die Bestimmung bringt einen administrativen Mehraufwand ohne klaren Mehrnutzen. Wir fordern deshalb die Streichung von Bst. f.

Änderungsantrag:

¹ Die Notkommunikation muss mit den folgenden übergeordneten Aufgaben (Systemaufgaben) durch eine oder mehrere Anbieterinnen sichergestellt werden:

- a. ~~Betrieb eines ausschliesslich der Notkommunikation dienenden, jederzeit verfügbaren Netzes;~~
- b. redundanter Betrieb des gesamten Netzes ~~nach Buchstabe a~~ oder von Teilen davon durch eine Zweitanbieterin;
- f. ~~Datenerhebung zur Überprüfung der Qualitätsvorgaben.~~

Kostentragung: Art. 20c Abs. 3 (neu)	Eher Zustimmung
---	------------------------

Begründung:

In Absatz 1 wird die Kostenbeteiligung der Anbieterinnen des öffentlichen Telefondienstes an den Systemaufgaben geregelt. Zu klären ist insbesondere die Rolle der Zweitanbieterin. Dient diese lediglich als Backup im Falle eines Ausfalls, kann sie ihre Kosten nicht angemessen decken. Daher müssen die Aufwendungen der Zweitanbieterin im Rahmen der Ausführungsbestimmungen entweder wie diejenigen der Anbieterin gleichwertig vergütet werden, oder es ist eine angemessene und diskriminierungsfreie Aufteilung der Kosten sicherzustellen.

Änderungsantrag:

³ *Werden gemäss Artikel 20b Absatz 1 mehrere Anbieterinnen mit derselben Systemaufgabe beauftragt, regelt der Bundesrat die Entschädigung so, dass die Anbieterinnen angemessen und diskriminierungsfrei entschädigt werden.*

End-zu-End-Tests: Art. 20d	Ablehnung
-----------------------------------	------------------

Begründung:

Art. 20d geht davon aus, dass die Betreiberin der Plattform für End-zu-End-Tests auch die Koordinationsstelle betreibt. Dies widerspricht dem Konzept, das verschiedene Anbieterinnen für unterschiedliche Systemaufgaben vorsieht. Gemäss Art. 20a Abs. 1 Bst. d kümmert sich die Koordinationsstelle um die Koordination «akuter Notkommunikationsanliegen». Ein End-to-End-Test ist kein akutes Anliegen und daher nicht Aufgabe der Koordinationsstelle. Art. 20d ist entsprechend anzupassen.

Änderungsantrag:

End-zu-End-Tests des Zugangs zur Notkommunikation sind auf der Test- und Integrationsplattform nach Artikel 20a Absatz 1 Buchstabe e durchzuführen ~~und über die Koordinationsstelle nach Artikel 20a Absatz 1 Buchstabe d zu koordinieren.~~

Schutz der Integrität der Notkommunikation: Art. 20e Abs. 2	Ablehnung
--	------------------

Begründung:

Der Zugang der Benutzerinnen und Benutzer des öffentlichen Telefondienstes zu den Notdiensten ist eine

wichtige fernmelderechtliche Pflicht. Eine Einschränkung oder gar eine vollständige Trennung einer Benutzerin oder eines Benutzers vom Netz stellt einen erheblichen Eingriff dar. Der Entscheid, ob eine solche Massnahme angemessen ist, darf daher nicht von einer FDA getroffen werden, da diese weder den Kontext noch den Inhalt eines Anrufs kennt. Die Verantwortung für eine Einschränkung oder Trennung vom Netz muss bei den von den Notdiensten sowie den Hilfs- und Beratungsdiensten betriebenen Zentralen verbleiben. Nur diese können beurteilen, welche Massnahmen zu welchem Zeitpunkt und für welche Dauer angemessen sind. Abs. 2 ist entsprechend anzupassen. Die FDA, die Massnahmen umzusetzen hat, muss in jedem Fall diejenige sein, von der die Störungen stammen.

Änderungsantrag:

² Sie stützen sich dabei ~~insbesondere~~ auf die Hinweise *der von den Notdiensten sowie den Hilfs- und Beratungsdiensten betriebenen Zentralen und koordinieren ihre Massnahmen über die der Koordinationsstelle nach Artikel 20a Buchstabe d.* Die Anbieterinnen ergreifen die Massnahmen umgehend ~~und so lange wie nötig.~~

Lokalisierung von Störungen: Art. 34a Abs. 1	Ablehnung
---	------------------

Begründung:

Gemäss Absatz 1 müssen Anbieterinnen, Eigentümerinnen und Betreiberinnen von Fernmeldeanlagen dem BAKOM Zugang gewähren und «die Gesamtheit der relevanten technischen Informationen betreffend den massgeblichen Zeitraum, insbesondere zu den Abstrahlungseigenschaften und den Abstrahlungseinstellungen der betroffenen Funkanlage, zur Verfügung stellen». Von welcher «Gesamtheit der relevanten technischen Informationen» die Rede ist, erschliesst sich nicht. Das BAKOM verfügt bei den Mobilfunknetzen bereits heute über Daten der MNOs zu Fake TAC, Fake Cell IDs oder Fake eNBIDs.

Im erläuternden Bericht wird diese neue Regelung mit adaptiven Antennenmodulen begründet. Dort wird ausgeführt, dass das BAKOM wissen müsse, welcher Beam zu einem bestimmten Zeitpunkt aktiv war und wie sich das Strahlungsdiagramm über einen bestimmten Zeitraum beziehungsweise zu einem bestimmten Zeitpunkt gestaltet hat. Damit soll das BAKOM die Bedingungen zum Zeitpunkt einer Störung rekonstruieren können. Beams adaptiver Antennenmodule ändern ihre Ausrichtung und ihr Verhalten jedoch innerhalb von Millisekunden. Eine Rekonstruktion der Bedingungen zu einem bestimmten Zeitpunkt ist daher technisch kaum zielführend. Absatz 1 ist deshalb an die technischen Gegebenheiten anzupassen.

Änderungsantrag:

¹ Um den Ursprung von Störungen des Fernmeldeverkehrs oder des Rundfunks oder einer Stark- oder Schwachstromanlage zu bestimmen, ist dem BAKOM Zugang zu allen Fernmeldeanlagen sowie Stark- und Schwachstromanlagen zu gewähren. Auf Verlangen müssen die Anbieterinnen, Eigentümerinnen und Betreiberinnen von Fernmeldeanlagen zur Bereitstellung von Fernmeldediensten dem BAKOM ~~die Gesamtheit der relevanten technischen Informationen betreffend den massgeblichen Zeitraum, insbesondere zu den Abstrahlungseigenschaften und den Abstrahlungseinstellungen der betroffenen Funkanlage, zur Verfügung stellen.~~

Kinder- und Jugendschutz: Art. 46a Abs. 1	Ablehnung
--	------------------

Begründung:

Absatz 1: Es gibt verschiedene Produkte auf dem Markt, die zuverlässig pornografische und nicht jugendfreie Webseiten und Inhalte beim Surfen im Internet herausfiltern, indem sie entweder ganze Webseiten blockieren

oder explizite Inhalte ausblenden. Diese setzen technisch an unterschiedlichen Punkten an (DNS-Server, WLAN-Router, Apps auf Endgerät). Auch die verschiedenen Endgeräte-Betriebssysteme enthalten meist Kindersicherungsoptionen, die aktiviert werden können. Die geplante Regulierung, wonach den Kundinnen und Kunden *durch die FDA* Mittel zum Jugendschutz anzubieten sind, hätte in der Praxis für die FDA einen Kontrahierungszwangs bezüglich des Einkaufs solcher Drittprodukte zur Folge. Sie müssten dazu zwingend ein «Re-selling» mit einem Anbieter von Jugendschutzprodukten vereinbaren. Die FDA informieren und beraten schon heute ihre Kundschaft zu den verschiedenen Möglichkeiten des Kinder- und Jugendschutzes, auch auf den diversen Endgeräten. Dies tun sie aufgrund des zugenommenen Kundeninteresses und der höheren Nachfrage auch aus eigenen Interessen. Zudem sind sie auch dazu verpflichtet (vgl. Art. 89a FDV). Wir haben keine Einwände, dies nun auf Stufe Gesetz festzuschreiben. Kleinere Anbieterinnen haben aber nur beschränkte Möglichkeiten, ein bestimmtes Drittprodukt in ihr Sortiment aufzunehmen, oder im Fall eines Kaufzwangs, nur zu ungünstigen kommerziellen Bedingungen. Zudem sind die Bedürfnisse kundenseitig unterschiedlich, so dass hier ein Standard-Produkt nicht automatisch alle Anforderungen erfüllt. Wir beantragen deshalb, dass die gesetzliche Bestimmung lediglich eine Beratung und eine Hinweispflicht auf wirksame Mittel vorsieht.

Änderungsantrag:

¹ Die Anbieterinnen von Internetzugängen müssen ihre Kundinnen und Kunden über die Möglichkeiten im Bereich des Kinder- und Jugendschutzes beraten und ~~auf ihnen Mittel bieten~~ *hinweisen*, mit denen Kinder und Jugendliche wirksam vor pornografischen Inhalten geschützt werden können.

Resilienz der Fernmeldeinfrastrukturen und Schutz vor Cyberbedrohungen: Art. 48a Abs. 2, 3 und 4	Ablehnung
---	------------------

Begründung:

Artikel 48a lässt in der vorgeschlagenen Form einen grossen Interpretationsspielraum zu und hat dadurch potenziell erhebliche technische und finanzielle Auswirkungen. Sicherheit wird nicht allein durch Regulierung geschaffen. Das FMG muss sich darum auf wesentliche Massnahmen zum Schutz der Fernmeldeinfrastrukturen beschränken. Der Regulierungsumfang muss verhältnismässig ausgestaltet sein.

Die FDA schützen ihre Systeme und Infrastrukturen vor Cyberbedrohungen und unbefugten Manipulationen aus eigenen wirtschaftlichen und betrieblichen Interessen. Davon profitieren auch ihre Kundinnen und Kunden, soweit diese Teil des jeweiligen Systems sind. Einen umfassenden Schutz vor Cyberangriffen für sämtliche Elemente, die an die Fernmeldeinfrastrukturen der FDA angeschlossen sind, können die FDA jedoch nicht gewährleisten. Der erläuternde Bericht ist in diesem Punkt zu unpräzise und irreführend.

Absatz 2 überträgt dem BAKOM die Aufgabe, Risikofaktoren zu überwachen, zu ermitteln und zu bewerten. Dafür müssen die FDA die entsprechenden Informationen bereitstellen. Der Schutz vor Cyberbedrohungen ist ein hochdynamisches Umfeld. Schwachstellen und Sicherheitslücken müssen rasch behoben werden, ansonsten werden sie von Gefährdern ebenso rasch ausgenützt. Die FDA stehen in ständigem Austausch mit spezialisierten Unternehmen und Organisationen. Ihre Spezialistinnen und Spezialisten sowie die eingesetzten Systeme sind darauf ausgerichtet, tatsächliche Risiken von vermeintlichen Gefahren zu unterscheiden und Daten und Infrastrukturen auch gegen neue Bedrohungsformen zu schützen. Weiterhin sollen sie auch durch das Bundesamt für Cybersicherheit (BACS) unterstützt werden. Dieses verfügt bereits über die erforderlichen Kompetenzen und ist in der Lage, Risiken korrekt einzuschätzen und in geeigneter Form zu moderieren.

Absatz 2 schafft nur Doppelspurigkeiten, erhöht das Risiko von Mehrfachregulierung und unnötigem administrativem Zusatzaufwand. Wir beantragen deshalb, Absatz 2 ersatzlos zu streichen.

Absatz 3 ist entsprechend anzupassen. Im Übrigen ist, bezogen auf die Ausführungen im erläuternden Bericht (Seite 58), zu erwähnen, dass die dort erwähnten «Verkehrsdaten» unter Umständen auch sogenannte Randdaten beinhalten, die zusammen mit den jeweiligen Kommunikationsinhalten dem Fernmeldegeheimnis unterliegen.

Absatz 4: Der Bundesrat soll die Massnahmen nach Absatz 1 präzisieren können. Dabei sollte er sich zwingend an international anerkannten Standards und Zertifikaten orientieren. Nur sie schaffen die notwendige Qualität und Sicherheit.

Änderungsantrag:

² Das BAKOM überwacht, ermittelt und bewertet Risikofaktoren, welche die Resilienz der Fernmeldeinfrastrukturen gefährden oder den Schutz vor Cyberbedrohungen beeinträchtigen können. Es evaluiert dabei insbesondere das Vorliegen eines Sicherheitsrisikos für die Fernmeldeinfrastrukturen nach Artikel 48b.

³ Die Anbieterinnen von Fernmeldediensten haben dem BAKOM die zur Erfüllung seiner Aufgaben nach Absatz 2 notwendigen Auskünfte, einschliesslich der Verkehrsdaten, bekannt zu geben, sofern sie darüber verfügen. Sie können untereinander und mit für Cybersicherheit zuständigen anerkannten privaten und öffentlichen Stellen zusammenarbeiten, um Gefährdungen durch Cyberbedrohungen festzustellen und zu beurteilen.

⁴ Der Bundesrat präzisiert die Massnahmen nach Absatz 1 *gemäss international anerkannten Standards*. Er kann zum Schutz vor Gefahren, zur Vermeidung von Schäden und zur Minimierung von Risiken Bestimmungen über die Sicherheit von Informationen sowie von Fernmeldeinfrastrukturen und -diensten erlassen, insbesondere bezüglich:
(...)

Sicherheit von Fernmedeinfrastrukturen: Art. 48b Abs. 1, 2 und 3	Ablehnung
---	------------------

Begründung:

Absatz 1: Wir unterstützen den Grundsatz «Secured by Design and by Default» bei der Wahl und Konfiguration der eingesetzten Produkte und Softwarekomponenten. Nicht sinnvoll ist jedoch die starre Vorgabe, wonach Sicherheitseinstellungen standardmässig aktiviert sein müssen. Je nach Leistungsumfang und Einsatzzweck kann eine standardmässige Aktivierung erforderlich, entbehrlich oder sogar kontraproduktiv sein. Absatz 1 ist daher an die technischen Gegebenheiten anzupassen. Statt einer standardmässigen Konfiguration und Aktivierung sollten Sicherheitseinstellungen gemäss international anerkannten Standards konfiguriert und aktiviert werden.

Absatz 2: Wie bereits in den generellen Bemerkungen zur vorgeschlagenen Mehrherstellerepflicht (Diversifikationspflicht) ausgeführt, lehnen wir diese Vorgabe im Namen aller unserer Mitglieder entschieden ab. Die Vorgabe wäre weder angemessen noch zielführend. Eine staatlich vorgeschriebene Diversifikationspflicht der eingesetzten Netzkomponenten, die sich an Anteilen und Mindestprozentsätzen orientiert, wäre nicht nur mit erheblichen Zusatzkosten verbunden, sondern würde weder die Sicherheit erhöhen noch die Abhängigkeit von einzelnen Herstellern verringern. Es ist eine Fehleinschätzung, dass sich das Abhängigkeitsrisiko durch eine Mehrlieferantenstrategie prinzipiell reduzieren lässt. Je nach Netztechnologie und -architektur kann der Ausfall eines Herstellers die Infrastruktur auch dann enorm beeinflussen, wenn mehrere Lieferanten eingesetzt werden. Das Kriterium des angemessenen Datenschutzes am Hauptsitz eines Herstellers ist sachfremd und kein taugliches Mittel, um die Produkte sicherer zu machen. Die Mitglieder von Suissedigital orientieren sich bei der Auswahl der eingesetzten Technik an internationalen Standards und Best Practices. Dabei wird nicht generell nach Herkunftsländern und Herstellern differenziert, sondern im Einzelfall nach Einsatzzweck der Komponenten entschieden.

Unklar ist auch, was mit «kritischen Bestandteilen der Fernmeldeinfrastruktur» gemeint ist und in welchem Verhältnis diese Bezeichnung zum in der E-FAV neu eingeführten Begriff der «kritischen Netzwerkanlage» (vgl. Art. 2 Abs. 1 Bst. c^{bis} E-FAV) steht. Dies sorgt für grosse Unsicherheit. Anstatt auf Stufe Gesetz für Klarheit und Rechtssicherheit zu sorgen, überträgt Absatz 2 dem Bundesrat indirekt eine weitreichende Definitionskompetenz, indem ihm die Möglichkeit eingeräumt wird, Kategorien, Anteile und Mindestprozentsätze in Bezug auf diese Netzkomponenten festzulegen. Dies entbehrt angesichts des umfangreichen Eingriffs in die Wirtschaftsfreiheit jeglicher Verhältnismässigkeit und ist verfassungswidrig.

Eine vorgeschriebene Mehrlieferantenstrategie hätte weitreichende, erhebliche Auswirkungen auf die Kosten, den Herstellermarkt sowie die Cyber- und Versorgungssicherheit. Die Schweizer FDA setzen in ihren Netzen bereits heute unterschiedliche Lieferantenstrategien um und nutzen Technologien verschiedener europäischer, amerikanischer und ostasiatischer Hersteller. Dadurch wird bereits ein höheres Mass an Diversität und Stabilität erreicht, als dies durch eine regulatorisch vorgeschriebene und starre Mehrlieferantenpflicht möglich wäre. Abs. 2 ist deshalb zu streichen.

Sollte wider Erwarten an dieser Vorgabe im Gesetzesentwurf an das Parlament festgehalten werden, so wäre bereits auf Stufe Gesetz eine Anforderung zur Abstufung der Vorgaben nach Grösse und Bedeutung des betroffenen Netzes bzw. der betroffenen FDA oder grössenrelevante Ausnahmen vorzusehen.

Absatz 3: Die Mitglieder von Suissedigital haben aus wirtschaftlichen und betrieblichen Gründen ein sehr hohes eigenes Interesse, ausschliesslich sichere Komponenten und Software einzusetzen. Hersteller und Produkte werden daher mit grösster Sorgfalt und nach international anerkannten Verfahren ausgewählt. Fehlentscheidungen haben nicht nur erhebliche Kosten, sondern auch nachhaltige Reputationsschäden zur Folge. Wird nach der Beschaffung ein Sicherheitsrisiko festgestellt, lassen sich Schwachstellen normalerweise durch Konfigurationsanpassungen oder Software-Updates beheben. Ein vollständiger Ersatz einer Komponente wird kaum je erforderlich sein. Würde die Ausserbetriebnahme eines Netzelements angeordnet, müsste – je nach betroffenem Element – mehrere Jahren Umsetzungszeit eingeräumt werden, um die Stabilität der Netze weiterhin sicherstellen zu können.

Im erläuternden Bericht wird richtigerweise darauf hingewiesen, dass sich Technologien, Infrastrukturen und Cyberbedrohungen ständig weiterentwickeln (Seite 62). Es ist anzunehmen, dass die Spezialistinnen und Spezialisten der FDA im Austausch mit anderen Unternehmen sowie dem Bundesamt für Cybersicherheit (BACS) sich am besten mit den technologischen Entwicklungen auskennen und deshalb rascher und zielgerichteter auf neue Risiken reagieren können. Eine Liste von Bestandteilen mit Sicherheitsrisiken aktuell zu halten, ist nicht möglich. Ihr Beitrag zur Erhöhung der Sicherheit der Fernmeldeinfrastrukturen wäre zudem höchst bescheiden.

Die Voraussetzungen, unter denen das BAKOM ein «begründetes Sicherheitsrisiko» feststellen und daraus Verbote, Ausserbetriebnahmen oder Entfernungspflichten ableiten darf, müsste aus rechtsstaatlicher Sicht im Gesetz hinreichend bestimmt, ausschliesslich kritische Netzkomponenten betreffen, objektiv nachvollziehbar und auf konkrete technische Risiken sowie international anerkannte Sicherheitsstandards abgestützt sein. Solche Massnahmen dürften nur angeordnet werden, wenn mildere, gleich geeignete technische Risikominderungsmassnahmen – insbesondere Konfigurationsanpassungen, Software-Updates oder andere Massnahmen – nicht ausreichen würden. Die Entfernung bereits rechtmässig installierter Komponenten darf nur als ultima ratio erfolgen. Zudem wären die betroffenen Unternehmen vor einem Verbot beziehungsweise vor der Aufnahme eines Bestandteils in eine Verbotsliste anzuhören, und der Entscheid müsste transparent, technisch fundiert und überprüfbar begründet werden sowie eine angemessene Umsetzungsfrist vorsehen. Soweit rechtmässig installierte und noch nicht amortisierte Komponenten betroffen sind, wäre schliesslich auch die Eigentumsgarantie zu wahren und damit einhergehend eine staatliche Entschädigungspflicht vorzusehen. Die Bestimmung schafft lediglich rechtliche und wirtschaftliche Unsicherheiten, ohne einen erkennbaren zusätzlichen Sicherheitsgewinn. Sie ist daher ersatzlos zu streichen.

Änderungsantrag:

¹ Die Anbieterinnen von Fernmeldediensten müssen Fernmeldeinfrastrukturen nutzen, welche die Vertraulichkeit, die Integrität und die Verfügbarkeit von Fernmeldediensten gewährleisten. Die Sicherheitseinstellungen müssen ~~standardmässig~~ *gemäss internationalen Standards* konfiguriert und aktiviert sein und auf dem neusten Stand gehalten werden.

² ~~Die kritischen Bestandteile der Fernmeldeinfrastruktur einer Anbieterin von Fernmeldediensten müssen von verschiedenen Herstellerinnen stammen, wobei mindestens eine Herstellerin in einem Staat einen Sitz haben muss, dessen Gesetzgebung einen angemessenen Datenschutz gewährleistet. Der Bundesrat regelt die Einzelheiten; er kann Kategorien, Anteile und Mindestprozentsätze festlegen.~~

³ ~~Stellt das BAKOM ein begründetes Sicherheitsrisiko fest, so verbietet es den Anbieterinnen von Fernmeldediensten, betroffene Bestandteile in Betrieb zu nehmen. Es veröffentlicht eine Liste der verbotenen Bestandteile. Es kann die Ausserbetriebnahme oder Entfernung verbotener Bestandteile verfügen. Bei Bestandteilen, die für die Fernmeldeüberwachung nach dem BÜPF von Belang sind, nimmt das BAKOM vorgängig Rücksprache mit dem Dienst ÜPF.~~

Massnahmen betreffend Fernmeldeinfrastrukturen bei geopolitischen Risiken: Art. 48c E-FMG	Ablehnung
--	------------------

Begründung:

Es ist äusserst fraglich, ob das Fernmeldegesetz die geeignete gesetzessystematische Grundlage für einen derart weitreichenden, primär geo- und aussenpolitisch motivierten Eingriff bildet. Für den Austausch der kritischen Komponenten müsste mindestens zehn Jahre vorgesehen werden. Die wirtschaftlichen Auswirkungen wären erheblich und der Schweizer Telekommunikationsmarkt und die Versorgungssicherheit würden nachhaltig Schaden nehmen. Die Anbieterinnen müssten über Jahre hinweg hohe Investitionen in den dadurch erzwungenen Umbau ihrer Netze tätigen. Schliesslich würden dadurch technologische und kommerzielle Innovationen erheblich verzögert oder gar verhindert.

Der Anbietermarkt von Netzkomponenten ist beschränkt und die einzelnen Akteure über Lieferketten ihrerseits miteinander verbunden. So verwenden Hersteller in ihren Produkten immer auch Komponenten anderer Hersteller. Werden Hersteller verboten, sind deren Produkte nach wie vor im Einsatz. Ein Verbot von Bestandteilen eines bestimmten Herstellers würde deshalb keinesfalls eine komplette Unabhängigkeit von diesem Hersteller gewährleisten. Grundsätzlich dürfte ein solcher Entscheid nur dann erfolgen, wenn alle anderen Möglichkeiten ausgeschöpft wären. Der Eingriff müsste so gering wie möglich sein und sich ausschliesslich auf kritische Elemente der Netzinfrastruktur beschränken. Für die Umsetzung wären ausreichende Fristen von mehreren Jahren vorzusehen. Zudem wäre je nach Ausgangslage auch eine staatliche Entschädigungspflicht vorzusehen. Unseres Erachtens bieten demgegenüber die bestehenden Notstandsrechtsinstrumente bereits eine ausreichende Grundlage für derart ausserordentliche Situationen, die gleichzeitig auch den notwendigen Einbezug des Parlaments gewährleisten. Wir halten deshalb eine ersatzlose Streichung der vorgeschlagenen Bestimmung für angezeigt.

Änderungsantrag:**~~Art. 48c Massnahmen betreffend Fernmeldeinfrastrukturen bei geopolitischen Risiken~~**

¹ ~~Der Bundesrat kann den Anbieterinnen von Fernmeldediensten den Erwerb, die Inbetriebnahme und den Betrieb von Bestandteilen von Fernmeldeinfrastruktur verbieten, die von Herstellerinnen stammen, die für die Schweiz ein geopolitisches Risiko darstellen oder die sich im Besitz, unter der Kontrolle oder dem Einfluss eines ausländischen Staates befinden, der für die Schweiz ein geopolitisches Risiko darstellt.~~

² Er berücksichtigt bei der Beurteilung des geopolitischen Risikos die innere und äussere Sicherheit sowie den Schutz des Werk, Wirtschafts- und Finanzplatzes der Schweiz unter Einbezug: - der direkt oder indirekt verhängten Sanktionen gegen die Herstellerinnen nach dem Embargogesetz vom 22. März 2002¹²; - der wirtschaftlichen, technologischen und sicherheitsbezogenen Abhängigkeiten in Bezug auf die Herstellerinnen oder die Lieferkette; - der sicherheitsrelevanten Gefährdungslage durch Cyberangriffe, Sabotage und nachrichtendienstliche Aktivitäten; - der Androhung von Sanktionen oder Embargos, die die Sicherheit oder die Wirtschaft der Schweiz beeinträchtigen würden.
³ Der Bundesrat kann die Anbieterinnen von Fernmeldediensten verpflichten, Bestandteile, die von Herstellerinnen nach Absatz 1 stammen, aus ihrer Fernmeldeinfrastruktur zu entfernen. Er trägt dabei den wirtschaftlichen Auswirkungen Rechnung.

Bearbeitung von Daten und Zusammenarbeit: Art. 48d	Ablehnung
---	------------------

Begründung:

Wir lehnen die Befugnisse des BAKOM nach Art. 48a und 48b E-FMG ab. Entsprechend ist Art. 48d zu streichen.

Änderungsantrag**Art. 48d Bearbeitung von Daten und Zusammenarbeit**

¹ Das BAKOM ist befugt, für die Erfüllung der Aufgaben nach den Artikeln 48a und 48b Profilings durchzuführen, nötigenfalls auch ohne Wissen der betroffenen Personen, und dabei die folgenden besonders schützenswerten Personendaten zu bearbeiten: - biometrische Daten, die eine natürliche Person eindeutig identifizieren; - Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen.
² Das BAKOM kann diese Daten und Resultate von Profilings den für den Schutz vor Cyberbedrohungen zuständigen Schweizer Behörden und anderen für Cybersicherheit anerkannten privaten und öffentlichen Stellen nach Artikel 29 bekanntgeben, sofern diese Behörden im Rahmen der Erfüllung von Aufgaben im Bereich des Schutzes vor Cyberbedrohungen über eine entsprechende gesetzliche Grundlage verfügen.
³ Die Anbieterinnen von Fernmeldediensten können untereinander und mit für Cybersicherheit anerkannten privaten und öffentlichen Stellen nach Artikel 29 zusammenarbeiten, um Gefährdungen durch Cyberbedrohungen festzustellen und zu beurteilen.
⁴ Der Bundesrat regelt die Einzelheiten der Bearbeitung besonders schützenswerter Personendaten sowie der Durchführung von Profilings.
⁵ Die Artikel 13 und 13b sind auf die Bearbeitung dieser Daten durch das BAKOM und auf ihre Bekanntgabe an schweizerische oder ausländische Behörden anwendbar.

Nationaler Breitbandatlas: Art. 59a Abs. 1	Ablehnung
---	------------------

Begründung:

Absatz 1: Der bestehende Breitbandatlas soll auf eine gesetzliche Grundlage gestellt werden. Dabei ist im Gesetzesvorentwurf vorgesehen, dass die FDA sowie die Eigentümerinnen und Betreiberinnen nach Artikel 4a

dem BAKOM die Daten zu den Erschliessungen einzelner Gebäude liefern. Die bei den FDA vorhandenen Daten zu den HFC-Netzerschliessungen sind teilweise nicht in dieser Granularität vorliegend, weil sich diese Daten auf Informationen zu den erschlossenen Quartieren und Strassen beschränken. Das Breitbandatlas-Team des BAKOM kennt diese Umstände seit langem. Um zu vermeiden, dass die Bestimmung Zusatzaufwände bei den FDA auslöst, ist entsprechend zu präzisieren, dass die entsprechenden Daten nur, soweit vorhanden, zu liefern sind.

Änderungsantrag:

¹ Die Anbieterinnen von Fernmeldediensten und die meldepflichtigen Eigentümerinnen und Betreiberinnen nach Artikel 4a müssen dem BAKOM Daten über die Erschliessung von Gebäuden mit Fernmeldeanlagen liefern, *soweit diese vorhanden sind*.