Zusammenfassung der eingereichten Rückmeldung

Teilrevision des Fernmeldegesetzes (FMG) im Bereich Sicherheit

Eröffnung	27.05.2026
Frist der Einreichung	17.09.2026
Zuständiges Departement	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK)
Zuständige Bundesstelle	Bundesamt für Kommunikation (BAKOM)
Zuständige Organisation	Telecomrecht
Adresse	Zukunftstrasse 44, 2500, Biel/Bienne
Projektseite	https://fedlex.data.admin.ch/eli/dl/proj/2026/38/cons_1
Kontaktperson	Joëlle Pizarro (tp-secretariat@bakom.admin.ch) , Stéphane Bondallaz (tp-secretariat@bakom.admin.ch)
Telefon	+41 58 46 05876

Kontakt Information der einreichenden Stelle

Name (Firma/Organisation)	Landeskanzlei des Kantons Basel-Landschaft
Zuständige Stelle	--
Adresse	Rathausstrasse 2, 4410 Liestal
Kontaktperson Vorname	Sabine
Kontaktperson Name	Oldenburg
Telefonnummer (Rückfragen)	+41615225302
Eingereicht am	--

Rückmeldung zu: Teilrevision des Fernmeldegesetzes (FMG) im Bereich Sicherheit: Fernmeldegesetz (FMG)

Generelle Stellungnahme

Rückmeldung zur Gesamtvorlage	Zustimmung
Begründung	Wir begrüssen die vorliegende Teilrevision des Fernmeldegesetzes im Bereich Sicherheit. Wir er-achten jedoch verschiedene Präzisierungen als notwendig, um die Praxistauglichkeit der gesetzli-chen Regelungen sicherzustellen. Wir beantragen insbesondere: Verankerung der öffentlichen Sicherheit im Gesetzeszweck Das Fernmeldegesetz soll ausdrücklich festhalten, dass sichere, resiliente und vertrauenswürdige Fernmeldeinfrastrukturen eine wesentliche Voraussetzung für die öffentliche Sicherheit sowie die Aufrechterhaltung der staatlichen Handlungsfähigkeit darstellen. Stärkung der Notkommunikation Die bewährten Notrufnummern 117, 118 und 144 sind weiterhin als primäre Notrufnummern beizu-behalten und durch die europäische Notrufnummer 112 zu ergänzen. Die direkte Erreichbarkeit der zuständigen Notrufzentralen gewährleistet eine rasche fachliche Lagebeurteilung und verhindert unnötige Vermittlungs- und Triageschritte. Verbindliche Sicherheits- und Resilienzanforderungen Betreiberinnen kritischer Fernmeldeinfrastrukturen sollen verpflichtet werden, angemessene orga-nisatorische und technische Sicherheitsmassnahmen, Risikoanalysen, Wiederanlaufverfahren, Not-fallorganisationen sowie regelmässige Sicherheits- und Krisenübungen umzusetzen. Hersteller von Fernmeldeanlagen und Endgeräten sind im Rahmen ihres Einflussbereichs ebenfalls in die Verant-wortung für den Schutz der Integrität der Notkommunikation einzubeziehen. Sicherstellung einer verursachergerechten Finanzierung der Test- und Integrationsplatt-form Die Kosten für Betrieb und Weiterentwicklung der Plattform sollen verursachergerecht auf deren Nutzerinnen und Nutzer verteilt werden, damit deren langfristige Finanzierung sichergestellt bleibt. Verzicht auf eine generelle Dual-Vendor-Strategie Die vorgesehene Verpflichtung wird als organisatorisch und betrieblich nicht umsetzbar beurteilt und führt zu zusätzlicher Komplexität, höheren Kosten sowie potenziellen Sicherheitsrisiken. Ent-scheidend für die Sicherheit kritischer Kommunikationssysteme ist nicht die Anzahl der Anbieter, sondern eine robuste Sicherheitsarchitektur, wirksame organisatorische Mass-nahmen und eine hohe Resilienz der eingesetzten Systeme. Koordinierte Umsetzung der gesetzlichen Neuerungen Für die Umsetzung der neuen Anforderungen sind angemessene Übergangsfristen vorzusehen. Ebenso muss die Einführung neuer Kommunikationsdienste in enger Abstimmung zwischen Bund, Kantonen, Notruforganisationen und weiteren betroffenen Akteuren erfolgen. Anpassung der Bestimmungen über missbräuchlich verwendete Telefonnummern und In-ternet-Domains (Art. 6a und 6b FMG) Sperrmöglichkeiten sollen auch für ordnungsgemäss registrierte, jedoch nachweislich missbräuch-lich verwendete Rufnummern gelten. Antragsberechtigt sollen neben fedpol auch die zuständigen kantonalen und kommunalen Strafverfolgungsbehörden sein. Sperrmassnahmen sollen bei sämtli-chen schweren Straftaten möglich sein und sich auf alle von der Schweiz aus erreichbaren Inter-net-Domains erstrecken können.
Anhang	

Detaillierte Stellungnahme

Titel	Art. 6a Sperrung des Zugangs zu Telefonie und Internet
Akzeptanz	Zustimmung mit Anpassung
Anpassungen / Gegenvorschlag	--
Begründung	Art. 6a Anwendungsbereich In der Regel weiss nur der Dienst Überwachung Post- und Fernmeldeverkehr (nachfolgend DÜPF) und der jeweils betroffene mitwirkungspflichtige Fernmeldeanbieter (nachfolgend FDA), welcher Anschluss bereits einer laufenden Überwachung unterliegt. Artikel 6a Abs. 2 nimmt jedoch die «zuständigen Behörden» in die Pflicht. Zur Sperrung verpflichtet sind die Fernmeldeanbieter. Eine solche Sperrung erfolgt nicht durch die Strafbehörden. Vor der Sperrung eines überwachten Anschlusses muss deshalb der betroffene Fernmeldeanbieter mit dem DÜPF Rücksprache nehmen und darf erst sperren, wenn der DÜPF grünes Licht dazu gibt. Dazu muss der DÜPF seinerseits mit der (die Überwachung) anordnenden Behörde Rücksprache nehmen, bevor er die die Sperrung erlaubt. Der DÜPF nimmt dabei eine Art Drehscheibenfunktion wahr. Der Gesetzestext muss deshalb konkret festhalten, dass •vor einer Sperrung nach Art. 6a Abs. 1 VE-FMG, der betroffene Fernmeldeanbieter immer zuerst mit dem DÜPF Kontakt aufnimmt zwecks Rücksprache mit der anordnenden Strafbehörde einer bereits laufenden Überwachung und •bis zur Rückmeldung keine Sperrung erfolgen darf. Art. 6a sollte ausdrücklich auch jene Fälle erfassen, in denen eine Rufnummer zwar ordnungsgemäss registriert wurde, jedoch nachweislich für missbräuchliche oder strafbare Handlungen verwendet wird. Die Beschränkung auf unrechtmässig registrierte Rufnummern greift zu kurz und lässt wesentliche Erscheinungsformen moderner Cyberkriminalität unberücksichtigt. Wir schlagen daher die Schaffung eines neuen Buchstaben d vor: "Wenn die Rufnummer zwar korrekt registriert wurde, jedoch nachweislich für missbräuchliche Handlungen verwendet wird." Ebenso ist klarzustellen, welche Behörden Sperrmassnahmen anordnen beziehungsweise beantragen können. Aus polizeilicher Sicht dürfen diese Kompetenzen nicht ausschliesslich dem Bundesamt für Polizei vorbehalten bleiben. Da der überwiegende Teil der Strafverfahren von den Kantonen geführt wird, müssen auch die zuständigen kantonalen und kommunalen Strafverfolgungsbehörden entsprechende Anträge stellen können. Die vorgesehenen Sperrmöglichkeiten sollten zudem nicht ausschliesslich auf Betrugsdelikte beschränkt werden. Sie müssen zumindest bei sämtlichen Verbrechen sowie bei schweren Ver-gehen nach Strafgesetzbuch zur Verfügung stehen. Dies betrifft insbesondere Delikte wie Identitätsmissbrauch, organisierte Cyberkriminalität, Verbreitung kinderpornografischer Inhalte oder andere schwere Straftaten, bei welchen Kommunikationsmittel gezielt als Tatmittel eingesetzt werden. Ferner erscheint die vorgesehene Dauer einer Sperrmassnahme zu kurz bemessen. Aus Sicht der Polizei sollte eine ausreichend lange Sperrdauer vorgesehen werden, damit Strafverfolgungsbehörden die notwendigen Ermittlungen durchführen können und Täter nicht unmittelbar auf dieselben Kommunikationsmittel zurückgreifen können. Im Bereich der Internet-Domains sollte sich die gesetzliche Regelung nicht auf schweizerische Domain-Endungen beschränken. Vielmehr sollte eine Sperrung sämtlicher von der Schweiz aus erreichbaren Domains möglich sein, sofern diese nachweislich für strafbare Handlungen verwendet werden. Vergleichbare Mechanismen bestehen bereits in anderen Rechtsbereichen und haben sich in der Praxis bewährt. Schliesslich ist sicherzustellen, dass Sperrmassnahmen laufende strafprozessuale Überwachungen nicht beeinträchtigen. Vor der Umsetzung einer Sperre sollte deshalb zwingend eine Abstimmung mit dem Dienst ÜPF erfolgen, da nur dieser über die notwendigen Informationen verfügt, ob eine Telefonnummer oder Internetverbindung Gegenstand einer angeordneten Fernmeldeüberwachung ist. Gleichzeitig sollten neben Meldungen des Bundesamtes für Cybersicherheit auch Erkenntnisse der kantonalen Polizeikorps ausdrücklich in die Beurteilung einbezogen werden.
Anhang	

Titel	Art. 6b Sperrung von Telefonnummern und Domain-Namen
Akzeptanz	Zustimmung mit Anpassung
Anpassungen / Gegenvorschlag	--
Begründung	Art. 6b Verhältnis zu den Zwangsmassnahmen der StPO Im Strafrecht spricht man von Anfangsverdacht, hinreichendem Tatverdacht oder dringendem Tatverdacht. Die Formulierung «bei einem begründeten Verdacht» in Absatz 1 (betrifft nur die deutsche Version) ist kein Terminus technicus, weshalb er zu streichen ist. Die fünftägige Sperrung in Absatz 1 halten wir mit Blick auf die Praxis für zu kurz. Sie sollte deutlich länger sein und mindestens auf 10 Tage ausgedehnt werden. Die Sperrung nur bei Vorliegen eines Betruges ist zu eng definiert und schliesst andere Delikte wie z.B. Verbreitung von Kinderpornografie, Identitätsmissbrauch etc. aus. Unseres Erachtens müsste die Sperrung mindestens bei allen Verbrechen, besser auch bei schweren Vergehen möglich sein. Absatz 1 des Vorentwurfs sieht weiter vor, dass die Sperrung auf Hinweis von fedpol erfolgt. Die in Absatz 1 genannten Betrugsmeldungen gehen jedoch in der Regel bei den Kantonspolizeien ein – oft auch in Fällen, bei denen (noch) kein Schaden entstanden ist. Weder Vorlage noch Erläuterungen bieten hier Informationen dazu, wie hier der Meldeweg ausgestaltet werden soll. Soll die Kantonspolizei den Fall dem fedpol melden und diese wiederum der Anbieterin? Das wäre schwerfällig und angesichts der Dringlichkeit des Handlungsbedarfs in solchen Fällen zu langwierig. Die Sperrungen müssen deshalb auch auf Hinweis der kantonalen Polizeistellen durchgesetzt werden können. Zu Absatz 2: Es sollten nicht nur schweizerische Domainnamen (.ch / .swiss) gesperrt werden können, sondern alle von der Schweiz aus erreichbaren Domainnamen. Dieses Vorgehen wird bereits bei illegalen Geldspielangeboten erfolgreich umgesetzt (vgl. Art. 86 ff. Geldspielgesetz). Zu Absatz 3: Da die Sperrungen auch auf Hinweis der kantonalen Polizeistellen zu erfolgen haben, müsste das BACS sowohl fedpol als auch die kantonalen Polizeistellen unterstützen. Zu Absatz 5: Der Artikel 6b bezieht sich in den Absätzen 1 – 4 auf Telefonnummern und Internet-Domains, somit sollte auch Absatz 5 beide Fälle abdecken.
Anhang	

Titel	Art. 13 Abs. 1 und 3
Akzeptanz	Ablehnung
Anpassungen / Gegenvorschlag	--
Begründung	Art. 13 Abs. 3 Der Vorentwurf hebt Art. 13 Abs. 3 auf und verlagert die Auskunft in den generellen Abs. 1. Damit fällt die heutige Schranke weg, wonach über laufende Strafverfolgungen nur bei überwiegendem Interesse Auskunft erteilt wird. Aus Sicht der Strafverfolgung ist das heikel: Eine Auskunft an eine beliebige ersuchende Person kann ein hängiges Verfahren vorzeitig offenlegen und die Täterschaft warnen. Die vorgeschlagene Rücksprachepflicht erhält die Handlungsfähigkeit der verfahrensleitenden Staatsanwaltschaft, ohne die grundsätzliche Auskunftsöffnung des BAKOM in Frage zu stellen. Der Art. 13 Abs. 3 sollte daher beibehalten werden.
Anhang	

Titel	Art. 13b Sachüberschrift sowie Abs. 1–2bis und 4
Akzeptanz	Zustimmung mit Anpassung
Anpassungen / Gegenvorschlag	--
Begründung	Art. 13b Abs. 1 Wir empfehlen, Art. 13b Abs. 1 auf die Bereitstellung von Abdeckungskarten für die Notsuche zu erweitern und Art. 20a Abs. 3 so zu ergänzen, dass das BAKOM die Anforderungen gemeinsam mit den verantwortlichen Stellen des nationalen mobilen Sicherheitskommunikationssystems (MSK) festlegt. Bei der Beschränkung auf Personendaten entfällt möglicherweise die gesetzliche Grundlage für die Zurverfügungstellung von Abdeckungskarten bei Notsuchen. Das BAKOM sollte diesbezüglich aufzeigen, auf welcher Rechtsgrundlage künftig vorgegangen wird.
Anhang	

Titel	Art. 20c Kostentragung
Akzeptanz	Zustimmung mit Anpassung
Anpassungen / Gegenvorschlag	--
Begründung	Abs. 2: Wir bitten Sie zu prüfen, den Begriff "angemessenen" durch "verursachergerechten" zu ersetzen. Verfassung und Rechtsprechung zum Abgabenrecht sehen vor, dass die Höhe der Kosten auf Gesetzesstufe mit genügender Bestimmtheit festzulegen sind. Pflichtige müssen klar aus dem Gesetz ablesen können, mit welchen Kosten zu rechnen ist. Eine weitgehende Delegation an die Exekutive oder an Behörden ist nicht statthaft.
Anhang	

Titel	Art. 30a Datenbearbeitung sowie Amts- und Rechtshilfe
Akzeptanz	Zustimmung mit Anpassung
Anpassungen / Gegenvorschlag	--
Begründung	Art. 30a und 48d Beide Bestimmungen erlauben dem BAKOM Profilings, nötigenfalls ohne Wissen der Betroffenen, und die Weitergabe an die Strafverfolgungs- und «Cyberbehörden». Fliessen solche verwaltungs-rechtlich und verdeckt gewonnenen Ergebnisse ungeprüft ins Strafverfahren, droht eine Umgehung der Beweiserhebungsregeln der StPO und ein Verwertungsstreit vor Gericht. Für Erkenntnisse, die funktional einer geheimen Überwachung entsprechen, gelten die Schranken der Art. 269 ff. StPO. Klarzustellen ist deshalb, dass sich die Verwertung im Strafverfahren ausschliesslich nach der StPO richtet. Das schafft Rechtssicherheit und gibt der Staatsanwaltschaft Handlungssicherheit, indem die verwaltungsrechtliche Bekanntgabe von der strafprozessualen Beweisverwendung ge-trennt bleibt.
Anhang	

Titel	Art. 32b Fernmeldeanlagen sowie andere Anlagen und Vorrichtungen zur Wahrung der öffentlichen Sicherheit
Akzeptanz	Zustimmung mit Anpassung
Anpassungen / Gegenvorschlag	--
Begründung	Art. 32b Abs. 2 Art. 32b Abs. 2 Bst. a ermächtigt die Polizei-, Strafverfolgungs- und Strafvollzugsbehörden zum Betrieb störender Fernmeldeanlagen «zur Strafrechtspflege». Das liefert jedoch nur die fernmelderechtliche Betriebsgrundlage, nicht die strafprozessuale Einsatzgrundlage. Ohne Klarstellung bleibt offen, unter welchen Voraussetzungen, mit welcher Genehmigung und unter welcher Subsidiarität eine solche Anlage im konkreten Verfahren eingesetzt werden darf, mit entsprechendem Verwertungsrisiko für die daraus gewonnenen Erkenntnisse.
Anhang	

Titel	Art. 34a Lokalisierung von Störungen
Akzeptanz	Zustimmung mit Anpassung
Anpassungen / Gegenvorschlag	--
Begründung	Abs. 1 Unklar ist, ob die Ausnahmen nach Art. 32b Abs. 2 auch hier gelten. Wir bitten Sie um Klarstellung in der Bestimmung. Abs. 2 Art. 34a Abs. 2 sieht die automatisierte optische Fahrzeugerfassung vor und verlangt die unverzügliche Löschung, «sofern die Daten nicht als Beweismittel benötigt werden». Wer nach welchen Kri-terien über diese Beweismitteleigenschaft entscheidet, bleibt offen. Die Aufbewahrungsdauer delegiert Abs. 3 an den Bundesrat. Für die Verwertbarkeit und eine lückenlose Beweiskette braucht es die ausdrückliche Entscheidzuständigkeit der Strafverfolgungsbehörde und eine Dokumentationspflicht, andernfalls ist die Herkunft der Daten im Verfahren angreifbar.
Anhang	

Titel	Art. 46a Kinder- und Jugendschutz
Akzeptanz	Ablehnung
Anpassungen / Gegenvorschlag	--
Begründung	Art. 46a Abs. 3 (Löschkoordination): Sicherung vor Löschung Art. 46a Abs. 3 verpflichtet BAKOM, fedpol und die kantonalen Stellen, die rasche und weltweite Löschung von Inhalten nach Art. 197 Abs. 4 und 5 StGB zu koordinieren. «Rasch und weltweit löschen» und Beweissicherung stehen im Zielkonflikt: Wird zuerst gelöscht, ist das Beweismaterial entfernt, bevor es gesichert werden konnte. Klarzustellen ist, dass die zuständige Strafverfolgungsbehörde über die Reihenfolge entscheidet: erst sichern, dann löschen. So wird verhindert, dass die legitime Löschkoordination die spätere Beweisführung im Strafverfahren vereitelt. Der Verzichtsvorbehalt hält das Verfahren dort schlank, wo kein Sicherungsbedarf besteht.
Anhang	

Titel	Art. 48b Sicherheit von Fernmeldeinfrastrukturen
Akzeptanz	Ablehnung
Anpassungen / Gegenvorschlag	--
Begründung	Art. 48b Abs. 2 (Sicherheit von Fernmeldeinfrastrukturen) Wir beurteilen wird die vorgeschlagene Dual-Vendor-Strategie klar ab. Wir beantragen eine ersatz-lose Streichung von Artikel 48b Abs. 2. Wir lehnen eine gesetzlich erzwungenen Hersteller-Diversität im Bereich kritischer Komponenten der Fernmeldeinfrastruktur vollumfänglich ab. Die im erläuternden Bericht angestrebte Erhöhung der Resilienz bewirkt in der operativen Praxis das ge-naue Gegenteil und gefährdet die Systemstabilität. Es ist für uns nicht ersichtlich, wie eine solche Vorgabe für kritische Komponenten der Fernmeldeinfrastruktur in der Praxis zuverlässig umgesetzt werden kann. Die damit verbundene technische Komplexität erhöht den Betriebsaufwand, verursacht erhebliche Mehrkosten und kann zusätzliche Sicherheitsrisiken schaffen. Weiter birgt die Kombination mehrerer Anbieter Datenschutzrisiken. Die Sicherheit kritischer Infrastrukturen wird nicht zwangsläufig durch die Anzahl der beteiligten Anbieter erhöht, son-dern durch die Qualität der Sicherheitsarchitektur, die Resilienz der Systeme sowie die Wirksamkeit der organisatorischen und technischen Schutzmassnahmen. Wir beantragen, auf eine Verpflich-tung zur Umsetzung einer Dual-Vendor-Strategie zu verzichten.
Anhang	

Titel	Art. 48d Bearbeitung von Daten und Zusammenarbeit
Akzeptanz	Zustimmung mit Anpassung
Anpassungen / Gegenvorschlag	--
Begründung	Art. 30a und 48d Beide Bestimmungen erlauben dem BAKOM Profilings, nötigenfalls ohne Wissen der Betroffenen, und die Weitergabe an die Strafverfolgungs- und «Cyberbehörden». Fliessen solche verwaltungsrechtlich und verdeckt gewonnenen Ergebnisse ungeprüft ins Strafverfahren, droht eine Umgehung der Beweiserhebungsregeln der StPO und ein Verwertungsstreit vor Gericht. Für Erkenntnisse, die funktional einer geheimen Überwachung entsprechen, gelten die Schranken der Art. 269 ff. StPO. Klarzustellen ist deshalb, dass sich die Verwertung im Strafverfahren ausschliesslich nach der StPO richtet. Das schafft Rechtssicherheit und gibt der Staatsanwaltschaft Handlungssicherheit, indem die verwaltungsrechtliche Bekanntgabe von der strafprozessualen Beweisverwendung getrennt bleibt.
Anhang	

Rückmeldung zu: Teilrevision des Fernmeldegesetzes (FMG) im Bereich Sicherheit: Fragebogen zur Vernehmlassungsvorlage

Generelle Stellungnahme

Rückmeldung zur Gesamtvorlage	Keine Rückmeldung
Begründung	--
Anhang	

Detaillierte Stellungnahme

Titel	Frage 1
Akzeptanz	Rückmeldung eingeben
Anpassungen / Gegenvorschlag	--
Begründung	Antwort: Wir stehen einem gesetzlichen Mitbenutzungsrecht für passive physische Infrastrukturen grundsätzlich offen gegenüber, sofern dadurch die Sicherheit, Verfügbarkeit und Resilienz kritischer Fernmeldeinfrastrukturen nicht beeinträchtigt werden. Fernmeldenetze bilden eine zentrale Grundlage für die öffentliche Sicherheit, insbesondere für die Notkommunikation sowie die Einsatz- und Führungsfähigkeit der Behörden und Organisationen für Rettung und Sicherheit (BORS). Ein Mitbenutzungsrecht darf deshalb nicht dazu führen, dass zusätzliche technische, organisatorische oder sicherheitsrelevante Abhängigkeiten entstehen, welche die Betriebsstabilität oder die Wiederherstellungsfähigkeit der Netze im Ereignis- oder Krisenfall beeinträchtigen. Voraussetzung für ein entsprechendes Mitbenutzungsrecht sind daher klare Regelungen bezüglich Verantwortlichkeiten, Unterhalt, Zutrittsrechten, Haftung sowie Informations- und Cybersicherheit. Betreiberinnen kritischer Fernmeldeinfrastrukturen müssen jederzeit in der Lage sein, ihre gesetzlichen Sicherheits- und Verfügbarkeitsanforderungen uneingeschränkt zu erfüllen. Sicherheitsrelevante Anforderungen dürfen gegenüber wirtschaftlichen oder infrastrukturellen Interessen nicht in den Hintergrund treten.
Anhang	

Titel	Frage 2
Akzeptanz	Rückmeldung eingeben
Anpassungen / Gegenvorschlag	--
Begründung	Antwort: Eine Ausweitung des Mitbenutzungsrechts auf Betreiberinnen von Strom-, Gas- und Wasserversorgungsnetzen ist differenziert zu beurteilen. Zwar kann eine koordinierte Nutzung bestehender Infrastrukturen Synergien schaffen und den Ausbau kritischer Infrastrukturen erleichtern. Gleichzeitig führt eine gegenseitige Mitbenutzung zu einer stärkeren Vernetzung und damit zu zusätzlichen gegenseitigen Abhängigkeiten zwischen verschiedenen kritischen Infrastrukturen. Dadurch erhöht sich das Risiko von Kaskadeneffekten bei technischen Störungen, Naturereignissen oder Cyberangriffen. Eine solche Ausweitung darf nur erfolgen, wenn die Sicherheit und Resilienz sämtlicher betroffenen kritischen Infrastrukturen nachweislich gewährleistet bleiben. Insbesondere müssen klare Vorgaben hinsichtlich physischer Sicherheit, Cybersicherheit, Zutrittsberechtigungen, Verantwortlichkeiten sowie Prioritäten bei Unterhalts- und Wiederherstellungsarbeiten bestehen. Eine gegenseitige Mitbenutzung darf insbesondere die Verfügbarkeit der Notkommunikation sowie die Einsatz- und Führungsfähigkeit der Sicherheitsbehörden unter keinen Umständen beeinträchtigen. Wo entsprechende Risiken bestehen oder nicht angemessen ausgeschlossen werden können, ist dem Schutz kritischer Infrastrukturen Vorrang gegenüber infrastrukturellen oder wirtschaftlichen Interessen einzuräumen.
Anhang	