3562/AB-BR/2021
vom 09.04.2021 zu 3841/J-BR

bmi.gv.at

Bundesministerium
Inneres

Karl Nehammer, MSc
Bundesminister

Herrn
Präsidenten des Bundesrates
Mag. Christian Buchmann
Parlament
1017 Wien

Geschäftszahl: 2021-0.113.429

Wien, am 7. April 2021

Sehr geehrter Herr Präsident!

Die BundesrätInnen Korinna Schuman, Stefan Schennach und Wolfgang Beer, Genossinnen und Genossen haben am 9. Februar 2021 unter der Nr. **3841/J-BR** an mich eine schriftliche parlamentarische Anfrage betreffend „Was tun, wenn das Internet zerreißt?" gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zur Frage 1:

- *Gibt es einen konkreten Anlassfall, um die Frage eines Netz-Blackouts zu untersuchen?*
  a. *Wenn ja: Welchen?*
  b. *Wenn ja: Geben Sie bitte konkrete Information zu dem Anlassfall (Datum, Ort, Sachverhalt, etc.)*
  c. *Wenn nein: Aus welchem Grund wird dieses Szenario jetzt verstärkt bearbeitet?*

Nein, das Thema „Internet-Ausfall“ ist ein Referenzszenario in der laufenden Schwerpunktsetzung der Arbeit des Staatlichen Krisen- und Katastrophenmanagements (SKKM) im Bereich „Vernetze Krisen“. Nach der Befassung mit dem Thema Stromkrise in den Jahren 2019 und 2020 wird im SKKM nun plangemäß das Thema „Ausfall des Internet“ im Sinn einer Folgenanalyse für den Ausfall internetbasierter Leistungen als

Referenzszenario bearbeitet; in diesem Zusammenhang erfolgt auch die Beteiligung an der besagten KIRAS-Studie.

Zur Frage 2:

- *Wie hoch sind die Gesamtkosten für das jetzt durch KIRAS gestartete Projekt „ISIDOR"? Aus welchen Budgetmitteln werden diese gedeckt?*

Die Beantwortung dieser Frage fällt nicht in meinen Zuständigkeitsbereich.

Zur Frage 3:

- *Liegen Ihnen bereits Erkenntnisse aus dem Projekt „ISIDOR" vor?*
  a. *Wenn ja: Welche?*
  b. *Wenn nein: Bis wann ist mit ersten Erkenntnissen zu rechnen?*

Es liegen noch keine Zwischenergebnisse vor.

Zur Frage 4:

- *Welche Maßnahmen sind von Seiten Ihres Ministeriums für den Fall eines Netz-Blackouts geplant?*

Eingangs darf festgehalten werden, dass der grundlegende rechtliche Rahmen für die Sicherheit und Integrität des Betriebs von öffentlichen Kommunikationsnetzen und die diesbezüglichen Pflichten der Betreiber durch das Telekommunikationsgesetz (TKG) festgelegt wird. Die zuständige Regulierungsbehörde ist hier die RTR, für welche die Bundesministerin für Landwirtschaft, Regionen und Tourismus zuständig ist.

Betreiber öffentlicher Kommunikationsnetze oder -dienste haben der Regulierungsbehörde Sicherheitsverletzungen oder einen Verlust der Integrität in der von der Regulierungsbehörde vorgeschriebenen Form mitzuteilen, sofern dadurch beträchtliche Auswirkungen auf den Netzbetrieb oder die Dienstebereitstellung eingetreten sind. Die Regulierungsbehörde hat eine entsprechend erfolgte Mitteilung unverzüglich an den Bundesminister für Inneres weiterzuleiten.

Das Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) sieht konkrete Strukturen und Aufgaben im Falle einer Cyberkrise vor. Demnach liegt die Entscheidung über das Vorliegen einer Cyberkrise beim Bundesminister für Inneres. Zur Beratung des Bundesministers für Inneres in Bezug auf die Entscheidung über das

Vorliegen einer Cyberkrise und die operativen Maßnahmen zur Bewältigung einer Cyberkrise sowie der Bundesregierung zur Koordination der Öffentlichkeitsarbeit wird ein Koordinationsausschuss eingerichtet. Der Koordinationsausschuss wird vom Generaldirektor für die öffentliche Sicherheit geleitet und setzt sich aus dem Chef des Generalstabs, dem Generalsekretär des Bundeskanzleramtes und dem Generalsekretär für auswärtige Angelegenheiten zusammen. Der Ausschuss ist um weitere Vertreter von Bundes- oder Landesbehörden, Betreiber wesentlicher Dienste und Computer-Notfallteams sowie Einsatzorganisationen zu erweitern, wenn dies zur Bewältigung der Cyberkrise erforderlich ist.

Ein innerer Kreis der operativen Koordinierungsstruktur unterstützt den Koordinationsausschuss durch Erstellung von anlassbezogenen Lagebildern und sein technisches Fachwissen.

Zur Frage 5:

- *Welche Maßnahmen setzen Sie bzw. Ihr Ministerium, um Österreich bestmöglich vor einem Netz-Blackout zu schützen?*

Das Bundesministerium für Inneres ist nicht für den technischen Schutz vor einem „Netz-Blackout“ zuständig; die denkmöglichen Folgewirkungen werden im Rahmen der Arbeiten im Staatlichen Krisen- und Katastrophenmanagement (SKKM) bzw. durch den Bereich Zivilschutz adressiert. Das Bundesministerium für Inneres führt regelmäßige Beratungs- und Sensibilisierungsgespräche mit Betreibern kritischer Infrastruktur durch, um deren Resilienz zu stärken. Dadurch sollen Unternehmen dabei unterstützt werden, ausreichende Vorsorgemaßnahmen zu setzen.

Durch das Netz- und Informationssystemsicherheitsgesetz (NISG) werden Betreiber wesentlicher Dienste verpflichtet, Sicherheitsvorkehrungen im Bereich Cybersicherheit zu treffen. Die Sicherheitsvorkehrungen haben gemäß Netz- und Informationssystem-sicherheitsverordnung (NISV) auch die Bereiche Betriebskontinuitätsmanagement, Notfallmanagement und Krisenmanagement zu umfassen. Mit dem NISG wurde zudem ein staatliches Cyberkrisenmanagement eingeführt.

Zur Frage 6:

- *Existieren Zahlen, die eine Abschätzung des Risikos eines Netz-Blackouts zulassen?*
  - *a. Wenn ja: Wie hoch ist die Wahrscheinlichkeit eines flächendeckenden NetzBlackouts:*
    - *i. In einem einzelnen Bundesland bzw. maximal drei Bundesländern?*

   ii. *Im gesamten Bundesgebiet?*
   iii. *In Teilen Europas?*
   iv. *In ganz Europa?*
   v. *Weltweit?*
   b. *Wenn ja: Nennen Sie bitte die Quelle der Zahlen und den Ort, wo diese abgerufen werden können.*
   c. *Wenn nein: Auf welche Quellenlage stützen Sie sich dann?*

Eine Abschätzung „in Zahlen“, wie sie in der Fragestellung erbeten wird, ist in einer hochkomplexen Umgebung kaum seriös möglich und sollte auch nicht angestrebt werden.

Zur Frage 7:

- *Gibt es für den Fall eines Netz-Blackouts eine staatliche Backbone-Strategie?*
  a. *Wenn ja: Wie konkret gestaltet sich diese?*
  b. *Wenn ja: Wie rasch ist diese verfügbar?*
  c. *Wenn ja: Welche Ressourcen sind für deren Schaffung und Inbetriebnahme erforderlich und sind diese dauerhaft verfügbar?*
  d. *Wenn ja: Welche Zeitspanne kann mit dieser Ersatz-Infrastruktur überbrückt werden, bevor auch diese zusammenbricht?*

Die Beantwortung dieser Frage fällt nicht in meinen Zuständigkeitsbereich.

Zur Frage 8:

- *Ist Österreich im Besitz von Internetadressen oder sind diese mit einem Totalzusammenbruch unwiederbringlich verloren?*

Die internationale Vergabe der Internetadressen durch die RIRs (Regionale Internet Registries) ist nicht direkt an das Funktionieren des Internets gekoppelt, ein Internetausfall hat hier keinen Effekt (Analogie: ein Ausfall einer Telefonleitung bedeutet auch nicht, dass danach die Rufnummer verloren geht bzw. jemand anderem zugewiesen wird).

Zur Frage 9:

- *Das sogenannte Staatsgrundnetz, das völlig - etwa auch von der öffentlichen Energieversorgung - funktionierte, ist seit 2001 nicht mehr vorhanden. Denken Sie an eine Wiedereinführung eines solchen Netzes?*
  a. *Wenn ja: Wie sieht die konkrete Umsetzung aus?*
  b. *Wenn ja: bis wann?*

c. Wenn nein: Warum nicht?

Unter den Forschungstiteln HAMMOND bzw. BONTEMPI wird die netzwerktechnische Vorsorge als Ersatz für das 2001 aufgelassene, auf reiner Sprachkommunikation basierende Staatsgrundnetz im Rahmen des KIRAS-Sicherheitsforschungsprogramms erforscht.

Darüber hinaus verweise ich auf das aktuelle Regierungsprogramm, das die Schaffung eines Krisenkommunikationsnetzes als System zur zuverlässigen, sicheren und krisenfesten Kommunikation vorsieht.

Zu den Fragen 10 und 11:

- *Welche Backup-Maßnahmen existieren aktuell für ein Netzblackout?*
- *Welche Backup-Maßnahmen sind für ein Netz-Blackout geplant und bis wann werden diese umgesetzt?*

Ausgewählte Betreiber kritischer Infrastrukturen wurden in den vergangenen Jahren mit behördlichen BOS-Digitalfunkgeräten ausgestattet. Dadurch soll gewährleistet sein, dass im Falle des Ausfalls der Telefonie/des Netzes mit Versorgern aus den Sektoren Energie, Wasser, Gesundheit etc. kommuniziert werden kann. Darüber hinaus bestehen auf gesamtstaatlicher, regionaler und lokaler Ebene eine Reihe verschiedener – auch analoger – Kommunikationsmöglichkeiten unter Einbindung von Strukturen der Behörden bzw. der Einsatzorganisationen bis hin zu ORF und APA.

Zu den Frage 12 und 13:

- *Wieso gibt es laut KIRAS-Homepage keine Zusammenarbeit mit dem Bundesministerium für Landesverteidigung?*
- *Wäre es mit Blick auf die Einsatzbereitschaft in einem Krisenfall nicht dringend erforderlich das Bundesheer und somit auch das Bundesministerium für Landesverteidigung in die Planung einzubeziehen?*

Das Projekt hat Bezugspunkte zu vielen staatlichen und nichtstaatlichen Stellen; im Projektkonsortium können nur eine beschränkte Anzahl von Organisationen vertreten sein. Das Bundesministerium für Inneres nimmt am Projekt in seiner Rolle als Ausrichter des SKKM teil, in dem sämtliche Bundesministerien und Bundesländer kooperieren. Das Bundesministerium für Landesverteidigung ist, so wie alle anderen Ministerien, über das SKKM in diese Arbeiten eingebunden.

Zur Frage 14:

- *Welche Kommunikationsmittel stehen für den Fall eines Netz-Blackouts oder eines totalen Blackouts zur Verfügung?*
  a. *Wenn ja: Wer ist mit der Einrichtung der Kriseninfrastruktur betraut?*
  b. *Wenn ja: Wie rasch kann ein flächendeckendes Krisenkommunikationsnetz errichtet werden und für welche Zeitdauer kann es das reguläre Netz ersetzen?*
  c. *Stehen für den Fall eines Totalausfalls der digitalen Kommunikationsinfrastruktur analoge Kommunikationsmittel zur Verfügung?*
     Falls ja: Nenne sie diese bitte vollständig.

Das im Zusammenwirken mit den Bundesländern und dem Bundesministerium für Inneres errichtete und betriebene digitale Bündelfunksystem „Digitalfunk BOS Austria“ zur Versorgung aller Sicherheitsbehörden und Einsatzorganisationen Österreichs ist im Rahmen des Wirtschaftlichkeitsgebots resilient ausgelegt. Diese Resilienz wird einerseits durch die Vorsorge für die zentrale Vermittlungstechnik in vier georedundanten, USV- und notstromversorgten Rechenzentren und andererseits durch Batteriekapazitäten bis zu 48 Stunden bei schwer erreichbaren Basisstationsstandorten und der Möglichkeit von externen Einspeisepunkten an den Standorten sichergestellt. Im Bereich des Vermittlungsnetzwerks (angemietete Signalwege) wurden Investitionen gesetzt, um aktive Komponenten gegen Stromnetzausfälle abzusichern. Für eine völlige Absicherung dieses Netzwerks verbleibt letztlich das Spannungsfeld zwischen einem wirtschaftlichen Betrieb der Infrastruktur, also dem Marktdruck, und dem staatlichen Interesse der immerwährenden Verfügbarkeit.

Die Errichtung und der Betrieb des Digitalfunk BOS Austria ist durch Übereinkommen zwischen den einzelnen Bundesländern und dem Bundesministerium für Inneres geregelt. Dem Grunde nach sind die Bundesländer für die bauliche Errichtung der Standorte inklusive der Energieversorgung und das Bundesministerium für Inneres für die Systemtechnik und die Steuerung (Betriebsüberwachung) zuständig.

Theoretisch ist der Betrieb durch die Energieeinspeisung an den Standorten durch Kleingeneratoren auch längerfristig möglich. Limitierend sind hier eher die logistischen Herausforderungen mit zahlreichen topologisch exponierten Standorten, um die Nachbetankung und Wartung der Generatoren sicherzustellen. Ausfälle der Energieversorgung konnten jedoch bislang ohne Einbruch der Versorgung bewältigt werden.

Der „Digitalfunk BOS Austria“ verfügt über mehrere Betriebsmodi. Neben dem Normalbetrieb über die Netzwerkinfrastruktur lässt sich jedes Endgerät auch im sogenannten Direct Modus Operation-DMO betreiben. Dies ermöglicht auf kurze Entfernungen den Betrieb von Endgerät zu Endgerät ohne Infrastruktur oder den Aufbau eines Ersatzfunkfelds durch den Einsatz von Repeatern. Über die Kooperation mit dem Bundesministerium für Landesverteidigung kann über den mobilen Richtfunk auch eine Überbrückung der ausgefallenen Netzwerkinfrastruktur erfolgen und mit einem TMO Repeater (Trunked Mode Repeater) die volle Funktionalität wiederhergestellt werden.

Zur Frage 15:

- *Ist Österreich auf ein Blackout oder ein Netz-Blackout vorbereitet?*
  a. *Wenn nein: Warum nicht?*

Hinsichtlich der Vorsorgemaßnahmen für den Fall eines Blackouts im Bereich des Bundesministeriums für Inneres verweise ich auf meine Beantwortungen der Anfragen 4411/J XXVII. GP des Abgeordneten Laimer vom 3. Dezember 2020 (4399/AB XXVII. GP) und der Anfrage 5046/J XXVII. GP des Abgeordneten Mag. Drobits vom 20. Jänner 2021.

Darüber hinaus verweise ich auf die Beantwortungen der Anfragen 4409/J XXVII. GP (4402/AB XXVII. GP), 4410/J XXVII. GP (4395/AB XXVII. GP), 4412/J XXVII. GP (4397/J XXVII. GP), 4413/J XXVII. GP (4405/AB XXVII. GP) und 4414/J XXVII. GP (4389/AB XXVII. GP) des Abgeordneten zum Nationalrat Laimer vom 3. Dezember 2020 durch die zuständigen Bundesministerinnen und Bundesminister.

Darüber hinaus sind Meinungen und Einschätzungen nicht Gegenstand des parlamentarischen Interpellationsrechts.

Zu den Fragen 16 und 17:

- *Wie beurteilen Sie mit Blick auf die Bedenken in der COVID-Krise die Lage bei der Versorgungssicherheit bei einem Netz-Blackout? Ist die Versorgungssicherheit der ÖsterreicherInnen in solch einem Fall gegeben?*
  a. *Wenn ja: Wie lange kann die Versorgung mit Lebensmitteln und Wasser aufrechterhalten werden?*
  b. *Wenn ja: Wie lange kann die Versorgung mit Gütern des täglichen Bedarfs aufrechterhalten werden?*
  c. *Wenn ja: Wie lange kann die Versorgung mit Medikamenten und medizinischen Produkten aufrechterhalten werden?*

   d. *Wenn ja: Wie lange kann die Energieversorgung und die Versorgung mit Betriebsmitteln für Verkehrsmittel aufrechterhalten werden?*
   e. *Wenn ja: Wie lange kann der öffentliche Verkehr aufrechterhalten werden?*
   f. *Wenn ja: Wie lange kann das Gesundheitssystem aufrechterhalten werden?*
   g. *Wenn nein: Wieso nicht?*
   h. *Wenn nein: Was werden Sie unternehmen um das zu ändern?*
- *Können Sie bei einem Zusammenbruch der digitalen Kommunikation die Sicherheit von Kraftwerken, insbesondere von Kernkraftwerken an den Grenzen Österreichs, garantieren?*
   a. *Wenn ja: Auf Basis welcher konkreten Fakten?*
   b. *Wenn nein: Warum nicht?*
   c. *Wenn nein: Was werden Sie konkret dagegen unternehmen?*

Die Beantwortung dieser Fragen fällt nicht in meinen Zuständigkeitsbereich.

Zur Frage 18:

- *Ist es mit den Ihnen zur Verfügung stehenden Mitteln möglich, nach einem Zusammenbruch der bestehenden Infrastruktur, ein deutschsprachiges Intranet aufrechtzuerhalten?*
   a. *Wenn ja: Für wie lange?*
   b. *Wenn ja: Welche Mittel stehen Ihnen dafür zur Verfügung und wie rasch können diese eingesetzt werden?*
   c. *Wenn nein: Was werden Sie dagegen unternehmen?*

Durch den Betrieb des Netzwerks des Bundesministeriums für Inneres und die Vorsorgen im zentralen Rechenzentrumsbereich ist ein deutschsprachiges Intranet im Falle der Nichtverfügbarkeit des öffentlichen Netzwerks möglich.

Karl Nehammer, MSc

	Datum/Zeit	2021-04-09T16:15:53+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-07,OU=a-sign-corporate-07,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	148769640
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2021-04-09T16:19:24+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	