

Antrag

der Abg. Heilig-Hofbauer BA MBA, Klubobfrau Mag.^a Berthold MBA und Mag.^a Dr.ⁱⁿ Humer-Vogl
betreffend den Schutz der kritischen Infrastruktur

Kürzlich wurden dem Salzburger Busunternehmen Albus 34 Busse der Firma Yutong aus chinesischer Produktion ausgeliefert, die demnächst auf den Linien 17, 21, 22, 23, 24 und 34 in Betrieb genommen werden. Wie erst nach der Auftragsvergabe bekannt wurde, hat der norwegische Busbetreiber Ruter Ende Oktober 2025 über Ergebnisse von Tests berichtet, die sie unter anderem mit Yutong-Bussen durchgeführt haben. Dabei hat sich herausgestellt, dass diese Busse - theoretisch - von China aus gesteuert, angehalten oder verriegelt werden können.

Diese Testergebnisse haben in ganz Europa hohe Wellen geschlagen und - zu Recht - die Frage aufgeworfen, inwieweit hier Risiken für den Öffentlichen Verkehr als Teil der kritischen Infrastruktur bestehen. Ähnliche Kritik wurde laut, als kurz darauf die Westbahn chinesische Garnituren der China Railway Rolling Stock Corporation (CRRC) in Betrieb genommen hat, die nun zwischen Salzburg und Wien verkehren. Sowohl bei Yutong als auch bei CRRC handelt es sich weltweit um die jeweils größten Hersteller in ihrem Sektor, die ausgereifte und technisch hochwertige Produkte anbieten. In beiden Fällen wurde auch damit argumentiert, dass zahlreiche Komponenten der (Schienen-) Fahrzeuge aus europäischer Herstellung stammen würden und damit zumindest ein Teil der Wertschöpfung in Europa bleiben würde. Dies vermag aber das Risiko nicht zu vermindern, dass diese Fahrzeuge im Ernstfall möglicherweise auf Knopfdruck stillgelegt werden können.

Angesichts der gesamten weltpolitischen Lage rückt der Schutz unserer kritischen Infrastrukturen in den letzten Monaten verstärkt in den Fokus. Denn bisher scheint dieser Aspekt bei öffentlichen Ausschreibungen und Förderungen von Stadt, Land, Bund und EU noch zu wenig Beachtung gefunden zu haben. Im Fall der Yutong-Busse etwa erfolgte die Ausschreibung der Buslinien von der Stadt, die Beschaffung der Fahrzeuge lief über Albus und die EBIN-Förderung („Emissionsfreie Busse und Infrastruktur“) kam vom Bund bzw. aus EU-Mitteln.

Da sich die globale Lage immer unsicherer gestaltet, gilt es Entwicklungen in Betracht zu ziehen, die bis vor kurzem als äußerst unwahrscheinlich, um nicht zu sagen als unmöglich galten. So haben die USA unter anderem den venezolanischen Machthaber gekidnappt, einen Öltanker unter russischer Flagge beschlagnahmt und mit einer militärischen Intervention in bzw. einer Annexion von Grönland gedroht - auf Boden eines NATO-Partners. Es ist zu befürchten, dass diese expansive Machtpolitik, die eine Abkehr von der regelbasierten internationalen Ordnung zurück zum Recht des Stärkeren bedeutet, Nachahmer findet. So wird auch ein chinesischer Angriff auf Taiwan immer wahrscheinlicher. All diese weltpolitischen

Entwicklungen haben auch direkte und indirekte Auswirkungen auf unsere regionale Ebene. Denn Europa droht bei diesen eskalierenden Konflikten Spielball zwischen den Weltmächten USA und China zu werden. Mit möglicherweise hohen Kollateralschäden.

Zu beiden Seiten bestehen große technologische Abhängigkeiten. Diese beschränken sich nicht - wie eingangs geschildert - auf Risiken im öffentlichen Verkehr. Im Falle Chinas betrifft das viele weitere Hardware-Bereiche - von Akkus, über Telekommunikation und Netzwerktechnik bis zu Photovoltaikmodulen und Wechselrichtern. Zum Teil werden dahingehend bereits konkrete und auch weitreichende Initiativen gesetzt, wie etwa mit dem so genannten „Cybersecurity Act 2“ (CSA2) der Europäischen Kommission. Damit werden chinesische Netzwerkausrüster wie Huawei oder ZTE - ohne sie namentlich zu nennen - als „Hochrisiko-Anbieter“ eingestuft, da „nicht-technische Risiken“ vorliegen. Von solchen wird gesprochen, wenn ein Hersteller durch Gesetze gezwungen ist, Daten an den eigenen Geheimdienst weiterzugeben, wie etwa beim chinesischen Sicherheitsgesetz. In solchen Fällen wird der Zugang zum europäischen Markt verwehrt. Diese Regelung gilt allerdings nicht nur für neue Beschaffungsvorgänge, sondern auch für bereits bestehende Infrastruktur. Nach dem Motto „Rip and Replace“ sollen die Netzbetreiber nun 36 Monate Zeit bekommen, um Risiko-Technik aus ihren Systemen zu entfernen. Diese Regelungen gelten allerdings nur für die Lieferketten im Bereich der Informations- und Kommunikationstechnologie.

Neben der Hardware bestehen vor allem auch im Software-Bereich große Risiken. Allerdings ist hier die Abhängigkeit von US-Anbietern besonders groß. Dass die USA auch bereit sind, politischen Druck über diese auszuüben, zeigen etwa die US-Sanktionen gegen Richter des Internationalen Strafgerichtshofes. Dabei handelte es sich konkret um einen britischen sowie einen französischen Staatsbürger, deren Verhalten den USA nicht genehm war. Mit weitreichenden persönlichen Konsequenzen für die Betroffenen. So können diese nun keine Dienste von US-Anbietern mehr nutzen - von Kreditkarten, über Google, Microsoft, Amazon und Uber bis Airbnb und Co wurden den Richtern alle Konten bei US-Anbietern gelöscht. Im Fall von sich weiter zuspitzenden Konflikten ist zu befürchten, dass die USA der von uns genutzten Software den Stecker zieht.

Doch auch hier formiert sich unter dem Motto „Digitale Souveränität“ langsam Widerstand. Und gerade Österreich zeigt sich dabei ambitioniert. So wurde im letzten September die Migration von 16.000 Benutzerkonten des Bundesheeres auf Libreoffice abgeschlossen. Fast gleichzeitig fand auf Initiative des Staatssekretärs für Digitalisierung ein Gipfel in Wien mit EU-Kommissarin Henna Virkkunen und Vertretern aller Mitgliedstaaten statt, in dem die Eckpunkte der Deklaration zur Europäischen Digitalen Souveränität erarbeitet wurden, wie Golem.de berichtete. Im Oktober gab dann das Bundesministerium für Wirtschaft den Vollzug des Umstiegs auf die freie Nextcloud-Software bekannt. Auf dem EU-Gipfel im November in Berlin wurde die Deklaration dann von allen Mitgliedsstaaten beschlossen. Die EU-Kommission hat mittlerweile auch öffentliche Konsultation zum Thema gestartet, die bis zum 3. Februar 2026 lief.

In Zeiten, in denen alte Sicherheiten nicht mehr gelten, gilt es keine Zeit zu verlieren und auch auf Landesebene dringend zu prüfen, wo kritische Infrastrukturen besonders gefährdet sind und welche Maßnahmen zu deren Schutz getroffen werden können. Wir sollten hier nicht den Fehler der Energiepolitik wiederholen, wo man sich viel zu lange auf vermeintlich billiges Russengas verlassen hat, was uns sehr teuer zu stehen gekommen ist. Neben dem Preis müssen andere Kriterien bei öffentlichen Vergaben und Förderungen im Bereich Mobilität, IT, Netzwerktechnik, Software und Energie berücksichtigt werden. Nämlich Sicherheit, Unabhängigkeit, Verlässlichkeit und Schutz kritischer Infrastrukturen.

In diesem Zusammenhang stellen die unterzeichneten Abgeordneten den

Antrag,

der Salzburger Landtag wolle beschließen:

Die Salzburger Landesregierung wird ersucht,

1. zu prüfen, in welchen Bereichen der kritischen Infrastrukturen (Mobilität, IT, Netzwerktechnik, Software und Energie) sich durch geänderte geopolitische Rahmenbedingungen neue Risiken abzeichnen,
2. unter Einbeziehung von Stakeholdern und Expert:innen einen Maßnahmenplan zu erarbeiten, wie diesen neuen Risiken etwa durch geänderte Ausschreibungs- und Förderbedingungen begegnet werden kann sowie
3. dem Landtag sechs Monate ab Beschlussfassung über die Ergebnisse zu berichten.

Dieser Antrag wird dem Ausschuss für Infrastruktur, Digitalisierung und Mobilität zur weiteren Beratung, Berichterstattung und Antragstellung zugewiesen.

Salzburg, am 4. Februar 2026

Heilig-Hofbauer BA MBA eh.

Mag.^a Berthold MBA eh.

Mag.^a Dr.ⁱⁿ Humer-Vogl eh.