BIGS ESSENZ

Brandenburgisches Institut für **Gesellschaft** und **Sicherheit**

EIN RESILIENTES GLASFASERNETZ FÜR DEUTSCHLAND

Gastbeitrag von Albrecht Broemme

Deutschlands digitale Infrastruktur ist ein zentrales Element der Sicherheitsinfrastruktur. Wenn Verwaltung, Industrie, Energie, Gesundheit und Logistik digital gesteuert werden, trifft ein Ausfall nicht nur Server und Leitungen, sondern vielmehr Versorgung, Produktion und staatliche Handlungsfähigkeit.

Die Bedrohungslage ist real. Das BSI kommt für 2025 zu dem Befund, die IT-Sicherheitslage in Deutschland bleibe „weiterhin auf angespanntem Niveau".[1] Unzureichend geschützte Angriffsflächen machten Deutschland verwundbar. Zugleich zeigt die Bitkom-Wirtschaftsschutzstudie 2025, wie groß die aktuellen Schäden sind: 87 Prozent der Unternehmen waren von Datendiebstahl, Spionage oder Sabotage betroffen oder vermuten dies. Der gesamtwirtschaftliche Schaden lag 2025 bei nahezu 300 Milliarden Euro.[2]

Einerseits kommen diese Gefahren von außen: Bitkom berichtet, dass 46 % der betroffenen Unternehmen Russland und China als Herkunft von Angriffen angeben. Andererseits gibt es Risiken im Inneren: durch Social Engineering, unzureichende Schulungen, Fehlkonfigurationen, organisatorische Schwächen sowie Binnentäter.

In Anbetracht dieser Lage muss die Netzinfrastruktur neu bewertet werden. Deutschland braucht ein Netz, das resilient gebaut, sicher betrieben und leistungsfähig genug für den Krisenfall ist. Genau daran fehlt es bislang in der Fläche. Es gibt leistungsfähige Teilstücke, lokale Redundanzen und historisch gewachsene Strukturen. Was fehlt, ist ein bundesweit zusammenhängendes, systematisch auf Ausfallsicherheit und Angriffswiderstand ausgelegtes Backbone-Netz.

1 Bundesamt für Sicherheit in der Informationstechnik (2025): Die Lage der IT-Sicherheit in Deutsch-land 2025. Bundesamt für Sicherheit in der Informationstechnik (BSI). https://medien.bsi.bund.de/lagebericht/de/ [06.03.2026].

2 Bitkom (2025): Wirtschaftsschutz 2025. Lagebild der deutschen Wirtschaft. Bitkom e.V. DOI: 10.64022/2025-wirtschaftsschutz [

Ein solches Netz muss drei Voraussetzungen erfüllen:

Erstens: Resilienz durch Architektur.

Ein moderner Backbone braucht eine hochvermaschte Struktur, mehrfach redundante Verbindungen zwischen Netzknoten und unterschiedliche Trassen. Nur so kann bei Beschädigungen, Ausfällen oder Sabotage automatisch umgeroutet werden. Resilienz ist keine Reaktion auf Krisen, sondern eine Eigenschaft des Netzes. Es muss auch funktionieren, wenn es angegriffen wird.

Zweitens: Sicherheit von Ende zu Ende.

Sicherheit beginnt bei der Auswahl vertrauenswürdiger Komponenten und reicht über segmentierte Betriebs- und Managementstrukturen bis zum Monitoring „rund um die Uhr" und Notbetriebsfähigkeit. Ein belastbares Netz muss gegen Störungen aller Art, gegen kompromittierte Prozesse und gegen organisatorische Schwachstellen geschützt sein.

Drittens: Hochleistungsfähigkeit als Sicherheitsreserve.

Glasfaser ist die Basis für Cloud, KI, industrielle Steuerung und vernetzte Standorte. Hohe Leistung ist nicht nur ein Standortvorteil, sie ist auch eine Reserve für den Krisenfall: für Umleitungen, Ausweichrouten und stabile Verbindungen unter Last.

Vor diesem Hintergrund ist das Konzept eines Unternehmens aus Rahms (Rheinland-Pfalz) strategisch bemerkenswert. Der Bundeskanzler kam im Februar 2026 ins dortige Technologiezentrum der Niedax-Gruppe, um sich zu informieren. Netz 33 verfolgt das Vorhaben eines bundesweit einheitlichen, vermaschten Glasfaser-Backbonenetzes aus einer Hand, hochverfügbar, krisensicher und zukunftsfähig. Mit einer geplanten Länge von 33.000 Kilometern entlang der Bahntrassen geht es um ein neues, flächendeckendes Rückgrat für Deutschlands digitale Souveränität bis in den ländlichen Raum.

Entscheidend ist dabei das Produktprofil. Im Zentrum steht ein homogener Backbone, das auf deutschlandweite Konnektivität, hohe Verfügbarkeit und skalierbare Leistungsfähigkeit ausgelegt ist. Für Unternehmen, die öffentliche Hand und Betreiber kritischer Infrastrukturen sind entscheidend: planbare Redundanz, belastbare Vernetzung und ein Netz, das nicht aus Einzelteilen zusammengesetzt wirkt, sondern als integrierte Infrastruktur gedacht ist.

Ein so konzipiertes resilientes Netz, setzt auf eine hochvermaschte Architektur mit mehrfach redundanten Verbindungen der Netzknoten. Hinzu kommt der höchste Automatisierungsgrad als Ende-zu-Ende-Ansatz – entscheidend für schnelle Failover, kurze Entstörzeiten und stabilen Betrieb unter Störungslast.

„Entlang von Bahntrassen" bedeutet nicht, dass diese Infrastruktur ungeschützt oder frei zugänglich wäre. Bahn- und Verkehrskorridore sind betriebsrelevante, verwaltete und baulich strukturierte Räume. Entscheidend ist zudem, dass hier Resilienz nicht allein über den Verlauf der Trasse hergestellt werden soll, sondern über die eigentlichen Designprinzipien des Netzes: Vermaschung, Redundanz, Automatisierung und schnelle Wiederherstellungsfähigkeit.

Hinzu kommt ein mehrschichtiges Sicherheitskonzept, das es in Deutschland bislang noch nicht gibt: mit Hilfe von „Fiber Optic Sensing (FOS)" können die Betreiber reagieren, bevor ein Schaden bei Angriffen oder natürlichen Störfällen wie u. a. Hochwasser oder Erdrutschen eintritt. Ergänzt wird dies durch Partnerunternehmen, unter anderem Corning, Bechtle und MBS, sowie durch Mitarbeiter von Netz33 an kritischen Standorten in Deutschland.

Auch die physische Sicherung der Infrastruktur ist Teil dieses Konzepts. Die verbauten Kabeltröge sollen durchgängig abgedeckt und nach aktuellem Stand der Sicherheitstechnik verschlossen werden. Der Einsatz von Sicherheitskräften ist eine Möglichkeit, Vorfälle am Kabelkanal überprüfen zu lassen. Dies kann auch durch automatisiert eingesetzte Drohnen ergänzt werden. Wie die Sicherheits- und Betriebsprozesse im Detail umgesetzt werden, wird aus nachvollziehbaren Sicherheitsgründen nicht öffentlich gemacht.

Resilient und sicher allein aber reicht nicht aus, denn ein bundesweites Netz muss mit Blick auf die immer größer werdenden Datenströme auch hochleistungsfähig sein. Und auch hier versprechen die Rheinland Pfälzer, den Blick in die Zukunft der kommenden drei Jahrzehnte zu richten.

Das photonische Weitverkehrsnetz wird deutschlandweite Übertragungsleistungen von mehr als 800 Gbit/s, perspektivisch bis zu 1,6 Tbit/s, ermöglichen. Die Basis hierfür ist ein Glasfaser-Konzept, das neben der Standard-Faser G.652.D den leistungsfähigen Fasertyp G.654.E vorsieht und in Kombination mit der homogenen Netzarchitektur die Reichweite und Performance deutlich verbessern wird. Das ist nicht nur ein technologischer Fortschritt. Es ist auch sicherheitspolitisch relevant, weil Leistungsfähigkeit im Krisenfall immer auch Reservefähigkeit bedeutet.

Netz33 ist von Beginn an darauf ausgelegt, alle gesetzlich vorgeschriebenen Anforderungen aus dem jüngst verabschiedeten KRITIS-Dachgesetz, aus dem BSI-/NIS2-Regime sowie aus dem Telekommunikationsgesetz zu erfüllen. Gerade darin liegt seine besondere strategische Qualität: Resilienz, Sicherheit, Monitoring, Governance und Betriebsfähigkeit werden nicht nachträglich ergänzt, sondern von Anfang an als regulatorische und technische Kernanforderungen mitgedacht.

Ein solches Netz zu bauen, ist ambitioniert und nicht frei von Risiken. Aber – wer auch immer es baut – stärkt damit nicht nur Wachstum und Wettbewerbsfähigkeit, sondern auch die Resilienz unseres Landes. Dieses Projekt soll privat finanziert werden, nicht aus Steuermitteln. Das ist in Zeiten knapper öffentlicher Haushalte ein starkes Signal.

Das Investitionsvolumen beträgt 10 Milliarden Euro. Dies ist wenig im Vergleich zum jährlichen Schaden von mehreren 100 Milliarden Euro durch Spionage, Sabotage und Datendiebstahl. Wer in resiliente, sichere und leistungsfähige Netzinfrastruktur investiert, handelt also kostenbewusst und vernünftig. Die eigentliche Frage ist nicht, ob wir uns ein solches Netz leisten können. Die eigentliche Frage ist, ob wir es uns leisten können, weiter darauf zu verzichten. Hier geht es nicht um ein beliebiges Prestigevorhaben, sondern um ein Vorhaben von strategischer Bedeutung. Hier geht es um die Sicherheit Deutschlands.

Zum Autor:

Albrecht Broemme ist deutscher Experte für Katastrophenschutz, Krisenmanagement und den Schutz kritischer Infrastrukturen. Der Elektroingenieur war ab 1992 Landesbranddirektor und Leiter der Berliner Feuerwehr. In dieser Funktion verantwortete er über viele Jahre die operative Gefahrenabwehr in einer der komplexesten Metropolregionen Deutschlands.

Von 2006 bis Ende 2019 stand Broemme als Präsident der Bundesanstalt Technisches Hilfswerk (THW) an der Spitze der Bundesorganisation für technische Hilfe im In- und Ausland. In dieser Rolle prägte er maßgeblich die Weiterentwicklung des THW als zentrale Einsatz- und Resilienz-Organisation des Bundes und befasste sich intensiv mit Fragen der Versorgungssicherheit, Ausfallsicherheit und Krisenfestigkeit kritischer Systeme und Infrastrukturen.

Der Autor beschäftigt sich seit Jahren mit der Architektur des Projekts Netz33.

BIGS
BRANDENBURGISCHES INSTITUT
für GESELLSCHAFT und SICHERHEIT

Brandenburgisches Institut für Gesellschaft und Sicherheit
Geschäftsführender Direktor: Prof. Dr. Tim H. Stuchtey

Dianastraße 46 . 14482 Potsdam
Tel.: +49-331-704406-0 . Fax: +49-331-704406-19
E-Mail: info@bigs-potsdam.org . www.bigs-potsdam.org

IMPRESSUM

BIGS ESSENZ Nr. 24, MÄRZ 2026
ISSN 2191-6756

Autor:
Albrecht Broemme

Titel:
Ein resilientes Glasfasernetz für Deutschland

Herausgeber:
Brandenburgisches Institut
für Gesellschaft und Sicherheit gGmbH

Verantwortlicher im Sinne des Rundfunkstaatsvertrages:
Prof. Dr. Tim H. Stuchtey

Bild S. 1 & 4
@fernandocortes

Bild S. 3
shulz/Getty Images Signatures

Das Brandenburgische Institut für Gesellschaft und Sicherheit (BIGS) gGmbH ist ein unabhängiges, überparteiliches und nicht-gewinnorientiertes wissenschaftliches Institut, das zu gesellschaftswissenschaftlichen Fragen ziviler Sicherheit forscht. Das Institut publiziert seine Forschungsergebnisse und vermittelt diese in Veranstaltungen an eine interessierte Öffentlichkeit. Das BIGS entstand im Frühjahr 2010 in Potsdam und wird von der Universität Potsdam über ihre UP Transfer GmbH getragen, sowie von den Unternehmen IABG und W.I.S.. Alle Aussagen und Meinungsäußerungen in diesem Papier liegen in der alleinigen Verantwortung des Autors.

WWW.BIGS-POTSDAM.ORG