

P MAGAZIN PRIVATBAHN

| TECHNIK | LOGISTIK | UNTERNEHMEN | VERKEHRSPOLITIK |

DAS
BUSINESS
MAGAZIN

DER BAHN
BRANCHE



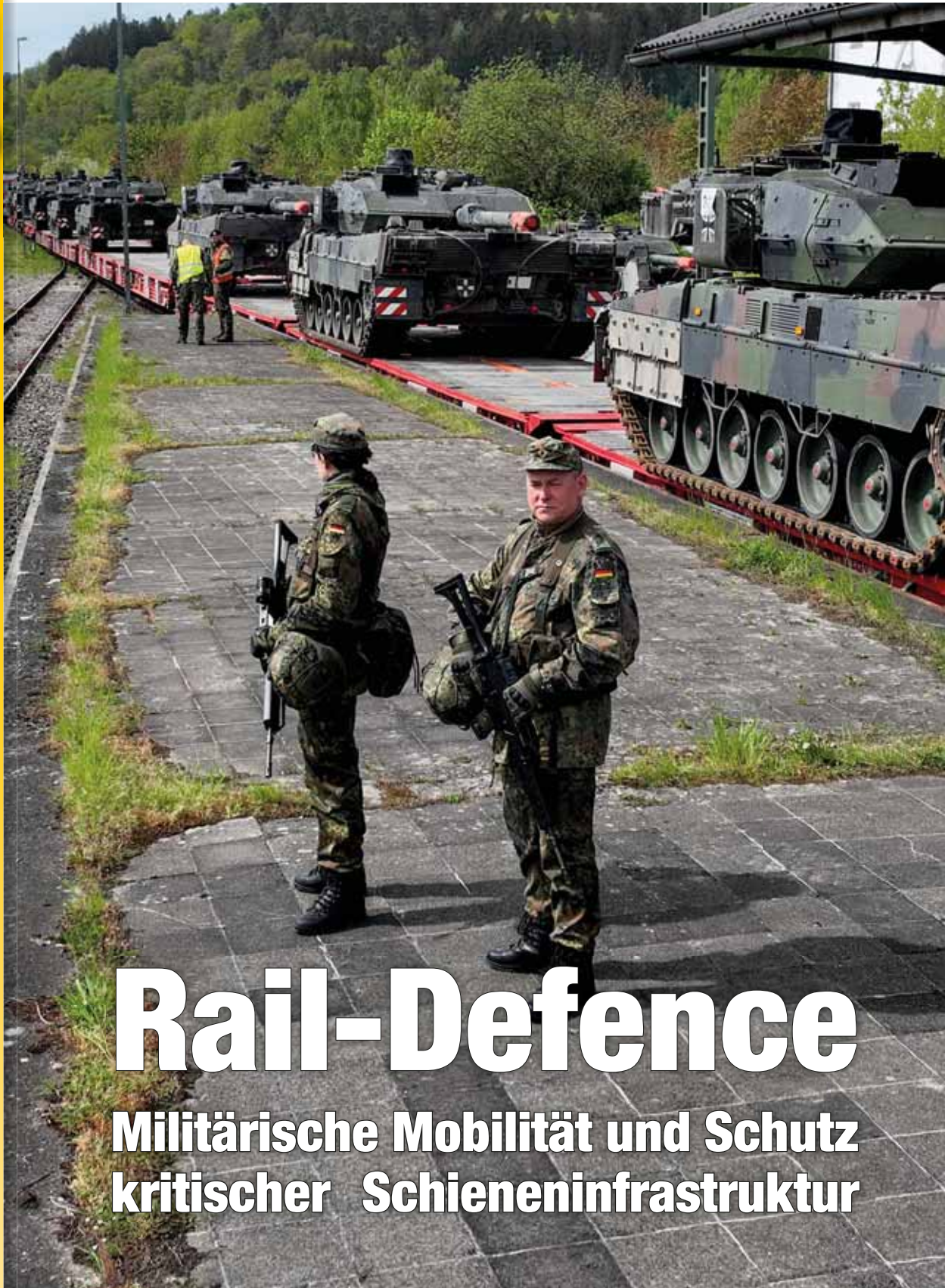
Rüdiger Just Winkler
Oberst i. G. über Anforderun-
gen der Bundeswehr Seite 20



Verena Jackson
Die Schiene als Zielscheibe hy-
brider Bedrohung Seite 34



Dennis-Kenji Kipker
Der Cybersicherheitsexperte
zum GSM-R-Ausfall Seite 44



Rail-Defence

Militärische Mobilität und Schutz
kritischer Schieneninfrastruktur



「Freiheit,
schöner
Götterfunken.」



#PressefreiheitIstDeineFreiheit
www.mvfp.de

MVFP
Medienverband
der freien Presse

Europas Sicherheit: Handeln hier und jetzt



Liebe Leserinnen,
liebe Leser,

die InnoTrans 2026 ist der Treffpunkt des globalen Bahnsektors, neue Produkte werden vorgestellt, Chancen und Herausforderungen für den Sektor diskutiert. Zur selben Zeit öffnet in Essen mit der EURO DEFENCE EXPO (EUDEX) erstmals eine internationale Fachmesse der Verteidigungsindustrie in Deutschland ihre Tore. Dass beide Veranstaltungen auf denselben vier Tagen liegen, ist ein treffendes Bild für das Thema dieses Sonderhefts: Zivile Bahnwelt und Sicherheitspolitik müssen zusammenwachsen – in Echtzeit.

Nicht nur das Extremwetter der letzten Monate, auch zunehmende geopolitische Spannungen und Europas technologische Abhängigkeiten setzen die Schiene neuen Bedrohungen aus, während institutionelle Komplexität und ein langsamer Rollout digitaler Standards die EU schlecht auf solche Szenarien vorbereiten. Glücklicherweise wurden die europäischen Eisenbahnen bislang nicht in dem Ausmaß herausgefordert wie ihre ukrainischen Kolleginnen und Kollegen.

In den letzten Jahren hat sich die Geopolitik von einer wertebasierten Kooperation demokratischer Staaten zu einer transaktionalen Weltordnung gewandelt. Die EU wurde trotz ihrer wirtschaftlichen Stärke an den Rand gedrängt. Geringere Militärausgaben und fehlende strategische Resilienz haben die Abhängigkeit Europas von externen Mächten erhöht – insbesondere in sicherheits- und technologiekritischen Bereichen wie Halbleiterfertigung oder Künstlicher Intelligenz. Wirtschaftliche Resilienz muss daher als Bestandteil der europäischen Sicherheitspolitik anerkannt werden; dazu gehören die Diversifizierung kritischer Lieferketten, technische Souveränität und belastbare Cyber-Security-Maßnahmen.

Im November 2025 stellten die Europäische Kommission und der Hohe Vertreter für Außen- und Sicherheitspolitik das Paket zur militärischen Mobilität vor, um den reibungslosen Transport von Truppen, Ausrüstung und militärischen Ressourcen innerhalb der EU zu gewährleisten. Rail-Defence ist aber nicht nur militärische Mobilität. Die Bahn muss Teil einer umfassenden Sicherheitsstrategie für Europa sein und auch zur Sicherstellung der Versorgung der Bevölkerung mit Lebensmitteln und Energie beitragen. Die grundlegenden Probleme Europas – etwa die Fragmentierung entlang nationaler Grenzen – spiegeln sich auch im Eisenbahnsektor, einschließlich der militärischen Mobilität, wider.

Es bedarf eines sicherheitspolitischen Weckrufs: Im Interesse der europäischen Sicherheit müssen wir uns der Herausforderung unserer Generation stellen. Europäische Souveränität ist im Kern eine Frage der Entscheidungs- und Handlungsfähigkeit. Das bedeutet auch, dass Europa im Technologiebereich von Forschungsprojekten und Piloten zu konsequenter, wirksamer Umsetzung übergehen muss. Die InnoTrans 2026 kann das Forum bieten, von Diskussionen ins Handeln zu kommen.

Dr. Josef Doppelbauer
Exekutivdirektor der European Union Agency for Railways (ERA) a. D. und
Mitglied im Redaktionsbeirat des Privatbahn Magazins

Military Mobility. Schieneninfrastruktur als strategisches Asset

Military Mobility ist mehr als ein infrastrukturelles oder logistisches Vorzeigeprojekt, sondern Teil der europäischen Verteidigungsbereitschaft. Streitkräfte müssen in der Lage sein, sich innerhalb Europas rasch und grenzüberschreitend zu bewegen. Nötig sind belastbare Verkehrswege, leistungsfähige Knotenpunkte, geeignete Umschlagkapazitäten und ein Verkehrssystem, das auch unter Druck funktionsfähig bleibt. Die Sicherheit Europas beginnt nicht erst an den Grenzen, sondern hängt davon ab, ob Europa im Krisenfall in der Lage ist, Soldaten und Material schnell, sicher und zuverlässig an den Ort des Bedarfs zu verlagern.

Die Eisenbahn ist ein strategischer Verkehrsträger. Sie ermöglicht den Transport großer Verbände und schweren Geräts über weite Distanzen und verbindet militärische Standorte, Seehäfen, Industriezentren und Knotenpunkte. Insbesondere bei großräumigen Verlegungen kann die Eisenbahn ihre Stärken ausspielen: Massenleistungsfähigkeit, Schnelligkeit, Netzbildungsfähigkeit, Berechenbarkeit, Bedienungshäufigkeit und Sicherheit.

Mit der Digitalisierung der Eisenbahn verändern sich die Anforderungen an Resilienz und Sicherheit. Moderne Leit- und Sicherungssysteme, vernetzte Sensorik und digitale Steuerungsmöglichkeiten erhöhen zwar die Massenleistungsfähigkeit, Berechenbarkeit und Bedienungshäufigkeit, schaffen jedoch Risiken. Cyberresilienz, der Schutz kritischer Systeme und die Fähigkeit, auch bei Ausfällen handlungsfähig zu bleiben, müssen Teil von Eisenbahnplanungen sein.

Auf europäischer Ebene werden durch das Projekt Military Mobility 2.0 physische, regulatorische und digitale Barrieren abgebaut, im Infrastrukturausbau ist die militärische Sichtweise zu berücksichtigen, grenzüberschreitende Truppenverlegungen müssen erleichtert werden, die Bereitstellung strategischer Transportmittel (zum Beispiel Dieseltraktion und Schwerlasttransportwagen) wird gefördert. Entscheidend ist die Zusammenarbeit der EU-Mitgliedstaaten und die Verbindung ziviler und militärischer Akteure. Nationale Streitkräfte, Infrastrukturbetreiber, Industrie, Behörden und internationale Partner müssen früher und enger zusammenwirken. Military Mobility ist deshalb ein Beispiel für einen umfassenden europäischen Ansatz, in dem Verteidigung, Verkehr, Digitalisierung und Resilienz zusammengebracht werden.

Die Zukunft der militärischen Mobilität wird nicht durch neue Gleise, Brücken, erweiterte Tunnels, Terminals und digitale Systeme entschieden. Die Zukunft wird davon abhängen, wie gut über nationale und institutionelle Grenzen hinweg die Zusammenarbeit zwischen dem zivilen und militärischen Sektor gelingt.

Die Eisenbahn ist für viele ein selbstverständlicher Teil des Alltags. Sie verbindet Regionen, transportiert Menschen und Güter und ist „der Motor der Wirtschaft“. Für das Militär, das seit vielen Jahren mit der Eisenbahn arbeitet, ist die Eisenbahn weit mehr: ein komplexes Netzwerk und ein zentraler Bestandteil der kritischen Infrastruktur.

Die aktuelle Entwicklung in Europa hat die Bedeutung der Eisenbahn in das allgemeine Bewusstsein gerückt. Eine leistungsfähige Eisenbahn ist nicht nur für Wirtschaft und Gesellschaft unverzichtbar. Sie ist entscheidend, wenn große Mengen, Personal und Versorgungsgüter, rasch und zuverlässig über weite Strecken bewegt werden müssen.

Damit gewinnt die zivil-militärische Zusammenarbeit an Bedeutung. Diese darf nicht erst in einer Krise beginnen. Eisenbahnbetreiber kennen die Eisenbahn, die betrieblichen Abläufe und die Grenzen des Systems. Dieses Wissen muss frühzeitig in die Planungen der Military Mobility einfließen. Voraussetzung sind gegenseitiges Verständnis, klare Zuständigkeiten und Vertrauen.

Die Eisenbahn muss auch nach Ausfällen oder Schäden rasch wieder handlungsfähig werden. Zur Erreichung dieses Ziel werden Redundanzen, alternative Strecken und Umschlagmöglichkeiten, belastbare Kommunikationswege und qualifiziertes Personal benötigt. Resilienz beginnt nicht erst bei der Technik, sondern mit guter Vorbereitung und gemeinsamer Planung.

Kritische Infrastruktur ist schutzbedürftig. Nicht alles, was technisch verfügbar ist, sollte öffentlich zugänglich sein. Informationen über sensible Infrastruktur, Kapazitäten oder mögliche Verwundbarkeiten müssen verantwortungsvoll behandelt werden.

Ebenso besteht im Eisenbahnrecht Anpassungsbedarf. Bestehende Regelungen sind dahingehend zu überprüfen, ob den Anforderungen einer veränderten Sicherheitslage, der Resilienz und einer zivil-militärischen Zusammenarbeit entsprochen wird.

Military Mobility 2.0 kann wichtige Impulse setzen, entscheidend bleibt: Die Stärke der Eisenbahn liegt in ihrem zivilen Charakter. Deshalb muss sie gemeinsam weiterentwickelt werden, damit sie im Alltag funktioniert und unter außergewöhnlichen Belastungen handlungsfähig bleibt. Das gelingt nur, wenn Politik, Behörden, Betreiber, Eisenbahnunternehmen und Streitkräfte frühzeitig miteinander kommunizieren und gemeinsam Lösungen entwickeln. Eine leistungsfähige, sichere und resiliente Eisenbahn ist nicht nur ein Fundament moderner Mobilität, sondern auch ein Baustein für ein Europa, das handlungsfähig bleibt – im Alltag, in Krisen und im Ernstfall.



Prof. Mag. Dr. Gerhard H. Gürtlich
Sektionschef i. R., Vizepräsident des Aufsichtsrates
der ÖBB-Infrastruktur AG, Wien



Brigadier Mag. Stefan Lampl
Direktor Logistik, EU-Militärstab, Brüssel



Was „kriegstüchtig“ für die Schiene eigentlich bedeutet

Nicole Knapp, bei Erscheinen dieses Beitrages Geschäftsführerin Eisenbahnverkehr im VDV, macht deutlich, dass die militärische Einsatzfähigkeit der Schiene zur gesamtstaatlichen Aufgabe werden muss, und fordert ein Militärisches Eisenbahngrundnetz. Nur mit gezielten Investitionen und der Einbindung privater Bahnen könne die Schiene ihre sicherheitspolitische Rolle erfüllen.

Seite 26



30 Jahre Funkstille beenden

Rampen abgebaut, Übungen eingestellt, Rüstungsfabriken geschlossen – Brigadier Andreas Stupka zeichnet beim Forum Verkehr in Wien ein ernüchterndes Bild der militärischen Bahnlogistik Österreichs.

Seite 30



14 Anschläge in sechs Monaten

In der Schweiz liegen Signalleitungen doppelt und dreifach, Norwegen zäunt alle Bahnstrecken ein. In Deutschland fehlen Redundanzen nahezu flächendeckend – ein durchtrenntes Kabel legt oft ganze Streckenabschnitte lahm. Was hinter der Serie von 14 Anschlägen steckt und warum Kameras und Drohnen das strukturelle Problem nicht lösen.

Seite 40



Nur 10 Kasernen ...

Nur zehn von 45 Bundeswehrstandorten haben einen eigenen Gleisanschluss – Bestandsaufnahme einer Schwachstelle militärischer Logistik.

Seite 32



Tod durch tausend Papierschnitte

Digitalisiert, vernetzt, eng getaktet – und als Drehscheibe des Operationsplans Deutschland zentral für die NATO-Bündnisfähigkeit: Die Bahn ist ein strategisch verdichteter Zielraum für hybride Aktivitäten. Kabelbrände, manipulierte Signale, eine Entgleisung vor einem US-Militärkonvoi: Ob Defekt oder Sabotage der Auslöser war, ist dabei zweitrangig, denn es zählt die Wiederholung, nicht der Einzelfall. Sönke Marahrens erklärt, warum Redundanz allein nicht genug ist, wie weit das Täterspektrum – von ahnungslosen Mitläufern bis zu operativen Agentengruppen – reicht und weshalb Resilienz eine täglich neu zu erbringende Leistung ist: eine Investition, die sich auch ohne Krise auszahlt.

Seite 49



Kommunikation:

Ein Fehler. Ein ganzes Land im Stillstand.

Ein einzelner Softwarefehler beim Austausch einer Netzwerkkomponente. Mehr brauchte es nicht, um in der Nacht vom 23. auf den 24. Juni 2026 den Bahnverkehr in ganz Deutschland zum Erliegen zu bringen. Damit stellt sich eine unbequemere Frage, als es die Suche nach einem einzelnen Schuldigen wäre: Wie verwundbar ist eine Infrastruktur, die längst mehr ist als ein Verkehrsträger – die Rohstoffe, Chemieprodukte und Industriegüter transportiert, von der Häfen und Lieferketten abhängen, und die im Zuge der Zeitenwende auch militärisch an Bedeutung gewinnt? **ab Seite 12**



Im Interview: Oberst i. G. Rüdiger Just Winkler

... ist seit 2024 Referatsleiter im Operativen Führungskommando der Bundeswehr. Er verantwortet die operative Planung der logistischen Unterstützung für nationale und internationale Einsätze sowie die Landes- und Bündnisverteidigung. Mit dem PriMa sprach er ausführlich über die Anforderungen der Bundeswehr an die Schiene. **ab Seite 20**



Im Interview: Verena Jackson

Drohnen: Bahninfrastruktur ist verwundbarer als lange angenommen. Sicherheitsexpertin Verena Jackson erklärt, warum hybride Bedrohungen integrierte Schutzkonzepte erfordern – und wo die Grenze privater Verantwortung liegt. **Seite 34**



Im Interview: Dennis-Kenji Kipker

Cybersicherheitsexperte Dennis-Kenji Kipker erklärt im Interview, warum der GSM-R-Ausfall zeigt, wie verwundbar kritische Infrastruktur schon ohne Angriff ist, und was das KRITIS-Dachgesetz wirklich leistet. **Seite 44**

Systemresilienz 8 – 11

Das Netz hat keine Puffer mehr	8
Panzer sind nicht das Problem	10

Kommunikation 12 – 19

GSM-R: Was der Funk-Ausfall bedeutet	12
Im Interview: Stefan Katzenbeisser – „Wir müssen Resilienz mitdenken“	15
Ein Hersteller, ein Ausfall	16
Im Interview: Marcel Haar – „Sicherheit liegt in unserer DNA“	18

Military Mobility 20 – 33

Im Interview: Rüdiger Just Winkler – 1800 Kilometer zur Ostflanke	20
CEF: Vierfach überzeichnet	24
Wo der Nachschub ankommt	25
Militärisches Eisenbahngrundnetz sichern	26
Polen: Absichtserklärung mit Lücken	29
Österreich: 30 Jahre Funkstille beenden	30
Nur 10 Kasernen mit Gleisanschluss	32

Drohnen 34 – 39

Im Interview: Verena Jackson – Offenes System als Zielscheibe	34
Rail-BB: Zwischen Logistik, Sicherheit und Resilienz	36
Kontrolle ohne Sichtkontakt	38
Drohnen hören, bevor man sie sieht	39

Kritische Infrastruktur 40 – 43

14 Anschläge in sechs Monaten	40
Zehn Minuten Widerstand	42

Cybersecurity 44 – 49

Im Interview: Dennis-Kenji Kipker – Kein Angriff nötig	44
Wartungsfenster? Gibt es nicht.	46
Ein DO-326A für die Schiene	48
Tod durch tausend Papierschnitte	49

Rubriken

Ausblick	50
Impressum	50



Drohnen verändern die Sicherheitslage kritischer Infrastruktur – auch auf der Schiene.

Bedrohungslage

Das Netz hat keine Puffer mehr

Die Schiene gilt als Rückgrat der deutschen Mobilität – doch sie ist zugleich ein offenes System. Gleise, Kabel, Stellwerke und digitale Steuerung bilden ein Netzwerk, das effizient, aber angreifbar ist. Neue Analysen und Vorfälle aus den Jahren 2025 und 2026 zeigen, dass die Debatte sich verschiebt: weg von der klassischen Betriebssicherheit hin zur Frage, wie widerstandsfähig dieses System gegen gezielte Störungen ist und sein kann.

Neue Sicht auf ein altes System

Über Jahrzehnte wurde die Sicherheit der Bahn vor allem technisch verstanden: Signale, Redundanzen, Wartung. Diese Logik greift heute zu kurz. Die Infrastruktur ist nicht nur ein technisches System, sondern Teil einer vernetzten, geopolitisch relevanten Umgebung. Angriffe müssen hier nicht besonders komplex sein, um Wirkung zu entfalten. Ein durchtrenntes Kabel kann ausreichen, um ganze Korridore lahmzulegen.

Mehrere Vorfälle entlang stark frequentierter Strecken haben genau das gezeigt. In Nordrhein-Westfalen kam es zuletzt zu einer Reihe gezielter Eingriffe in Stellwerks- und Kabelsysteme. Die Auswirkungen reichten weit über den Ort des Geschehens hinaus, weil die Bahn nicht linear funktioniert,

sondern als eng gekoppeltes Netzwerk ineinandergreift. Ein Ausfall an einer Stelle erzeugt wie in einem Dominoeffekt Verzögerungen und Stillstände an vielen anderen – die wiederum weitere Effekte haben können.

Das ist der erste Perspektivwechsel: Die Verletzbarkeit liegt weniger im einzelnen Objekt als im System selbst.

Fähigkeit, Störungen zu verkraften

Aktuelle Studien zeichnen ein differenzierteres Bild dieser Verwundbarkeit. Während die klassische Betriebssicherheit der Bahn als hoch gilt, wird die Fähigkeit, gezielte Störungen zu verkraften, deutlich kritischer bewertet. Besonders exponiert sind Knotenpunkte wie Stellwerke, Kommunikationsleitungen und digitale Schnittstellen – also genau jene Elemente, die das Sys-

tem zusammenhalten. Eine Analyse im Umfeld der Münchner Sicherheitskonferenz beschreibt die Schieneninfrastruktur als Teil eines „vernetzten Systems kritischer Dienste“, dessen Stabilität nicht isoliert betrachtet werden kann.

Der ehemalige US-Heimatschutzminister Michael Chertoff hat diesen Zusammenhang einmal prägnant formuliert: „Resilienz bedeutet nicht, Angriffe zu verhindern, sondern sicherzustellen, dass Systeme weiter funktionieren, wenn sie angegriffen werden.“ Diese Verschiebung des Blicks ist entscheidend. Es geht nicht mehr nur um Schutz, sondern um Durchhaltefähigkeit.

Parallel dazu entstehen auf nationaler und regionaler Ebene neue Strukturen. Einige Bundesländer haben begonnen, eigene Resilienz-Strategien für kritische Infrastrukturen zu entwickeln, in die Verkehrssysteme ausdrücklich einbezogen werden: In Sachsen-Anhalt hat die Landesregierung Anfang 2026 einen ressortübergreifenden Resilienzstab eingerichtet, der ausdrücklich auch Verkehrsinfrastruktur einbezieht; zugleich schafft das auf Bundesebene in

FOTOS: EUROPEAN COMMISSION, MAGNIFIC

Kraft getretene KRITIS-Dachgesetz erstmals einen verbindlichen Rahmen für den Schutz kritischer Infrastrukturen und verstärkt damit den Druck, Resilienz systematisch und sektorübergreifend zu organisieren.

Mit anderen Worten: Die Schiene ist nicht nur wichtiger Verkehrsträger, sondern als sicherheitspolitischer Faktor erkannt!

Angriffe folgen einer neuen Logik

Die Art der Bedrohung hat sich dabei grundlegend verändert. Klassische Sabotage – etwa das Durchtrennen von Kabeln – ist nur eine Variante. Hinzu kommen digitale Angriffe auf Informationssysteme und hybride Szenarien, in denen beides kombiniert wird.

Ein Cyberangriff auf IT-Systeme der Bahn im Februar 2026 hat gezeigt, wie stark der Betrieb inzwischen von digitalen Plattformen abhängt. Auch wenn Züge weiterfahren, können gestörte Buchungs- und Informationssysteme das Vertrauen der Nutzer untergraben und die operative Steuerung erschweren. In solchen Fällen ist die physische Infrastruktur intakt, doch das System funktioniert nur eingeschränkt.

Gerade diese Kombination macht moderne Angriffe so wirkungsvoll. Sie zielen nicht auf Zerstörung im klassischen Sinne, sondern auf Störung, Verunsicherung und Überlastung. Ursula von der Leyen betonte im Rahmen der EU-NATO-Taskforce zur Resilienz kritischer Infrastruktur: „Wir müssen mehr tun, um ihre Widerstandsfähigkeit zu gewährleisten. Das ist unerlässlich, um grundlegende Dienstleistungen für die Bürgerinnen und Bürger zu schützen und unsere Volkswirtschaften zu unterstützen.“

Die stille Verwundbarkeit des Netzes

Ein zweiter Aha-Effekt liegt in der Zugänglichkeit der Infrastruktur. So verlaufen zum Beispiel große Teile der Leit- und Signaltechnik offen, technische Informationen sind teilweise öffentlich und auch über das Internet verfügbar. Das war lange Ausdruck von Transparenz und Effizienz. In einer ver-



Für Ursula von der Leyen ist die Widerstandsfähigkeit kritischer Infrastruktur eine strategische Aufgabe Europas.

änderten Sicherheitslage wird es zur Schwachstelle.

Gleichzeitig sind viele Komponenten historisch gewachsen. Kabeltrassen verlaufen parallel zu Gleisen, Weichen oder Schaltschränke lassen sich kaum schützen und Redundanzen sind nicht überall vorhanden; auch die Überwachung weiter Streckenabschnitte bleibt aufwendig. Das bedeutet nicht, dass die Schiene völlig ungeschützt und unsicher ist – aber sie ist in bestimmten Punkten leichter angreifbar als andere kritische Infrastrukturen, die stärker zentralisiert oder abgeschottet sind.

Was Resilienz heute bedeutet

Die eigentliche Herausforderung liegt deshalb nicht in einzelnen Schutzmaßnahmen, sondern in einem neuen Verständnis für die Schieneninfrastruktur. Resilienz entsteht aus dem Zusammenspiel mehrerer Ebenen: technischer Schutz, Überwachung, organisatorische Vorbereitung und systemische Redundanz.

Entscheidend ist, wie schnell ein System auf Störungen reagieren kann. Wie rasch lassen sich Schäden lokalisieren? Wie flexibel kann Verkehr umgeleitet werden? Welche Ersatzsysteme stehen bereit? Diese Fragen rücken in den Mittelpunkt – und sie betreffen nicht nur die Bahn selbst, sondern auch Energieversorgung, Kommunikation und Lo-

gistik. Die Schiene wird damit Teil einer größeren strategischen Architektur. Ihre Stabilität hängt zunehmend davon ab, wie gut sie in dieses Gesamtsystem eingebettet ist.

Eine Infrastruktur im Wandel

Für die Verkehrspolitik und das Management der Eisenbahninfrastrukturunternehmen ergibt sich daraus eine klare, aber unbequeme Erkenntnis: Die klassische Trennung zwischen Effizienz und Sicherheit verliert an Bedeutung. Ein überlastetes wie auch hochoptimiertes System ist anfällig, wenn es keine Puffer mehr hat. Ein resilientes System braucht dagegen Spielräume – was in der Regel höhere Kosten verursacht. In Zeiten knapper Haushalte keine gute Nachricht.

Die Debatte über die Zukunft der Schiene wird deshalb zwangsläufig auch eine Debatte über Prioritäten sein. Geht es primär um maximale Auslastung oder auch um Belastbarkeit im Krisenfall? Die Antwort darauf ist nicht nur technisch, sondern vor allem politisch. Die Schiene bleibt das Rückgrat der Mobilität. Doch ihre Stärke wird künftig daran gemessen, wie gut sie mit Störungen umgehen kann. In einer Welt zunehmender Unsicherheiten ist das kein Nebenaspekt mehr, sondern eine zentrale Voraussetzung für ihre Zukunft.

cwk



Moderne Stellwerke steuern den Zugverkehr heute per Software – und machen den Bahnbetrieb damit ebenso abhängig von stabiler Strom- und Datenversorgung wie von intakten Gleisen.

Abhängigkeit

Panzer sind nicht das Problem

Wenn über militärische Mobilität gesprochen wird, denken viele zunächst an Panzerzüge, Schwerlastwagen und NATO-Transporte auf europäischen Korridoren. Doch die eigentliche Herausforderung liegt tiefer. Die Fähigkeit, Soldaten, Fahrzeuge und Versorgungsgüter im Krisenfall schnell durch Europa zu bewegen, hängt heute von einem eng verflochtenen System aus Schienenwegen, Energieversorgung, Kommunikationstechnik und digitaler Infrastruktur ab. Fällt eines dieser Systeme aus, geraten auch die anderen unter Druck. Military Mobility ist deshalb längst nicht mehr nur ein Thema für Streitkräfte. Sie wird zunehmend zum Gradmesser für die Widerstandsfähigkeit moderner Gesellschaften.

Die Diskussion über militärische Mobilität hat in den vergangenen Jahren auch innerhalb der Bahnbranche deutlich an Bedeutung gewonnen. Der russische Angriff auf die Ukraine, die verstärkte NATO-Präsenz an der Ostflanke und die sicherheitspolitische Neubewertung in Europa haben dazu geführt, dass der Schienenverkehr wieder verstärkt unter dem Blickwinkel der Landes- und Bündnisverteidigung betrachtet wird. Doch wer Military Mobility ausschließlich als Frage militärischer Transporte versteht, greift zu kurz. Die eigentliche Frage lautet: Wie widerstandsfähig ist die Infrastruktur, auf die sich militärische und zivile Transporte gleichermaßen stützen?

Gerade die Eisenbahn nimmt dabei eine Schlüsselrolle ein. Kein anderes Verkehrssystem kann große Mengen an Personal, Fahrzeugen, Munition oder Versorgungsgütern so effizient und ressourcenschonend über weite Entfernungen transportieren. Deshalb gilt die Schiene in nahezu allen aktuellen NATO- und EU-Planungen als unverzichtbarer Bestandteil militärischer Mobilität.

Schiene funktioniert nicht isoliert

Doch die Schiene funktioniert nicht isoliert. Ein moderner Bahnbetrieb ist auf eine Vielzahl anderer Systeme angewiesen. Stellwerke benötigen Strom. Leitstellen benötigen Telekommunikation.

Bahnübergänge benötigen Energieversorgung. Digitale Betriebsführung benötigt funktionierende Datennetze. Selbst dort, wo Diesellokomotiven zum Einsatz kommen, endet die Abhängigkeit nicht.

Führungskräfte der Bundeswehr weisen schon seit einiger Zeit darauf hin, dass militärische Transporte nicht ausschließlich auf elektrische Traktion setzen sollten. Die Überlegung erscheint auf den ersten Blick plausibel. Fällt die Stromversorgung aus, können Diesellokomotiven weiterhin verkehren. Doch auch diese Betrachtung greift nur einen Teil des Problems auf.

Denn eine Diesellokomotive muss betankt werden. Moderne Tankanlagen arbeiten elektrisch. Fällt der Strom aus, wird auch die Versorgung mit Dieselmotorkraftstoff schnell zur Herausforderung. Wie weitreichend die Folgen eines großflächigen Stromausfalls wären, beschrieb die Süddeutsche Zeitung jüngst eindrucksvoll. Nicht nur Züge und Aufzüge kämen zum Stillstand. Auch Stellwerke, Signaltechnik, Leitstellen, Bahnübergänge, Ampelanlagen und Tankstellen wären betroffen. Selbst der

FOTOS: DEUTSCHE BAHN AG/OLIVER LANG; BUNDESWEHR/TORBEN SCHREIBER

Verkehr mit Fahrzeugen, die fossile Kraftstoffe nutzen, könnte binnen kurzer Zeit im Chaos versinken.

Die entscheidende Erkenntnis lautet daher: Militärische Mobilität hängt nicht allein von Fahrzeugen oder Strecken ab. Sie hängt von der Funktionsfähigkeit eines hochkomplexen Gesamtsystems ab. Besonders deutlich wird dies beim Blick auf die Energieversorgung. Im Stromnetz gilt seit Jahrzehnten das sogenannte N-1-Prinzip. Vereinfacht ausgedrückt muss das System den Ausfall einer wichtigen Stromtrasse verkraften können, ohne seine Stabilität zu verlieren. Hinter dieser Regel steht die Erkenntnis, dass kritische Infrastrukturen Redundanzen benötigen.

Wenn eine Trasse ausfällt

Die gleiche Frage stellt sich zunehmend auch für die Schieneninfrastruktur: Was geschieht, wenn ein wichtiger Schienekorridor ausfällt? Gibt es leistungsfähige Ausweichstrecken? Sind diese von ihrem Zustand her und auch technisch in der Lage, zusätzliche Schwerlastverkehre aufnehmen zu können? Oder wurden Reserven im Laufe der vergangenen Jahrzehnte so weit zurückgebaut, dass Störungen sofort zu erheblichen Einschränkungen führen?

Die Diskussion erinnert an eine Aussage von Dirk Witthaut, Leiter des Institute of Climate and Energy Systems am Forschungszentrum Jülich. Mit Blick auf die Energieversorgung erklärte er kürzlich: „Wenn wir unsere Strom-Infrastruktur so verkommen ließen wie die Bahn ihr Schienennetz, dann wären auch wir in 10 bis 15 Jahren an einem Punkt, wo es gefährlich wird.“

Unabhängig davon, ob man dieser Einschätzung in allen Punkten folgt, verweist sie auf eine unbequeme Realität: Resilienz entsteht nicht erst in Krisenzeiten. Sie entsteht durch kontinuierliche Investitionen, Instandhaltung und Pflege der Infrastruktur und deren Reserven.

Genau darin liegen Herausforderung und Chance für den Schienenverkehr: Über Jahrzehnte wurde die Schieneninfrastruktur vor allem unter Effizienzgesichtspunkten betrachtet. Kapazitäts-



Naheliegend, aber nicht der Kern des Problems: Auch die Verladung eines Kampfpanzers auf die Schiene funktioniert nur, solange Stellwerke, Leitstellen und Stromversorgung intakt sind.

reserven galten häufig als wirtschaftlich nachteilig. Redundanzen wurden vielerorts reduziert. Parallel dazu stieg die technische Komplexität der Systeme.

Stresstest für die Widerstandsfähigkeit

Heute benötigen wir einen anderen Blickwinkel, denn plötzlich werden Fragen relevant, die lange Zeit nur eine untergeordnete Rolle spielten: Wie robust sind unsere Netze? Wie schnell können Störungen behoben werden? Welche Reserven stehen zur Verfügung? Und wie reagieren Verkehr, Energieversorgung und Kommunikation, wenn mehrere Krisen gleichzeitig auftreten? Military Mobility wird damit zu weit mehr als einer logistischen Aufgabe der Streitkräfte. Sie wird zu einem Stresstest für die Widerstandsfähigkeit der Staaten in der Europäischen Union. Für Eisenbahnverkehrsunternehmen, Infrastrukturbetreiber und politische Entscheidungsträger auf Bundes-, Landes- und kommunaler Ebene ergibt sich daraus eine gemeinsame Verantwortung. Es geht nicht allein um zusätzli-

che Kapazitäten für militärische Transporte. Es geht um die Frage, wie belastbar kritische Infrastruktur insgesamt ist. Und in diesem Zusammenhang könnte die Schieneninfrastruktur der NE-Bahnen als Redundanzreserve verstärkt in den Fokus rücken.

Denn im Ernstfall entscheidet nicht nur die Verfügbarkeit von Fahrzeugen oder Personal über die Handlungsfähigkeit eines Landes. Entscheidend ist, ob das Gesamtsystem auch dann noch funktioniert, wenn einzelne Komponenten ausfallen. Die Zukunft militärischer Mobilität wird deshalb nicht allein auf Kasernenhöfen, Truppenübungsplätzen oder in Lagezentren entschieden. Sie entscheidet sich ebenso in Umspannwerken, Stellwerken, Rechenzentren, Tankanlagen und auf den vielen Kilometern Schienenweg dazwischen. Wer über Military Mobility spricht, spricht deshalb über die Resilienz unserer gesamten Gesellschaft – und die Gesellschaft muss letztendlich entscheiden, wie viel Geld ihr die Sicherheit und Leistungsfähigkeit der Schieneninfrastruktur wert ist. *cwk*



Wie das Bahnnetz selbst hat auch die Sicherheits- und Steuerungsstruktur Knotenpunkte. Fallen diese aus, lahmmt das ganze Netzwerk.

Ein Fehler.

Was der Funk-Ausfall bedeutet

Der Ausfall des Bahnfunks war weit mehr als eine technische Störung. Er wirft die Frage auf, wie resilient die deutsche Schieneninfrastruktur tatsächlich ist – und ob wir kritische Single Points of Failure mit Blick auf die Anforderungen der Verkehrswende, KRITIS-Schutz und Military Mobility tolerieren können.

In der Nacht vom 23. auf den 24. Juni 2026 kam es zu einem Vorfall, der weit über die übliche Debatte über Verspätungen, Baustellen oder technische Störungen hinausgeht. Nach Angaben der Deutschen Bahn führte eine Störung des digitalen Zugfunks GSM-R zu massiven Beeinträchtigungen des Eisenbahnbetriebs. Über Stunden hinweg kam der Bahnverkehr in ganz Deutschland zum Erliegen.

Wie die DB InfraGO am 26. Juni mitteilte, war die Ursache ein einzelner Softwarefehler beim planmäßigen Austausch einer Netzwerkkomponente: Er verhinderte, dass eine vorhandene Redundanz automatisch aktiviert wurde. Erst nachdem ein Cyberangriff nach rund 90 Minuten Prüfung ausgeschlossen war, schaltete man manuell auf die Rückfallebene um.

Doch unabhängig davon beginnt die eigentliche Geschichte nicht mit der Frage, was ausgefallen ist. Sie beginnt mit einer anderen Frage.

Die falsche Frage

Nach größeren Infrastrukturstörungen richtet sich die öffentliche Aufmerksam-

Wie kann ein einzelner Fehler derart weitreichende Auswirkungen entfalten?

keit meist auf die unmittelbare Ursache: Was war der Auslöser, welcher Server ist ausgefallen? Welche Komponente war betroffen? Wer hat einen Fehler gemacht, brauchen wir moderne Systeme? Diese Fragen sind legitim und notwendig. Für die langfristige Sicherheit und Leistungsfähigkeit eines Systems sind sie jedoch nicht die wichtigsten. Die entscheidende Frage muss stattdessen lauten: Warum führte ein Fehler zu einem bundesweiten Ausfall? Denn technische Fehler sind keine Ausnahme. Sie gehören zum normalen Betrieb komplexer Systeme. Hardware fällt aus. Software enthält Fehler. Updates verursachen Probleme. Datenverbindungen werden unterbrochen.

Die Kunst, resilientere Infrastruktur zu schaffen, besteht deshalb nicht darin, über modernste Systeme zu verfügen oder Fehler vollständig zu verhindern. Sie besteht darin, ihre Auswirkungen zu begrenzen. In der Luft- und Raum-

fahrt, der Energiewirtschaft oder in militärischen Führungs- und Kommunikationssystemen wird genau von dieser Grundannahme ausgegangen: Irgendwann wird etwas ausfallen. Ist ein Fehler möglich, wird er auch eintreten – die Frage ist nur, wann. Deshalb werden kritische Systeme so konstruiert, dass sie Fehler tolerieren können.

Redundanz ist kein Luxus

Wer heute in ein Verkehrsflugzeug steigt, denkt kaum darüber nach, dass viele der entscheidenden Systeme mehrfach vorhanden sind. Flugsteuerungsrechner arbeiten oft parallel. Fällt ein System aus oder liefert fehlerhafte Daten, übernehmen andere Komponenten. Sensoren werden miteinander verglichen. Stromversorgungssysteme verfügen über Reserven. Kommunikationswege sind mehrfach abgesichert. Auch die ESA bestätigt auf Anfrage, in

Fehlertoleranz bedeutet, dass ein Fehler nicht unmittelbar zum Funktionsverlust führt.

vielen kritischen Systemen des Kontrollzentrums ESOC in Darmstadt mit Redundanzen zu arbeiten – zu Details des operativen Vorgehens äußert sich die Behörde aus Sicherheitsgründen nicht öffentlich.

GRAFIK: BMW MIT KI-UNTERSTÜTZUNG; FOTOS: DEUTSCHE BAHN AG/OLIVER LANG; UNSPLASH.COM/VC SIU

Die Fachbegriffe dafür lauten Redundanz, Fehlertoleranz und Resilienz. Redundanz bedeutet, dass eine Funktion mehrfach vorhanden ist. Daraus entsteht Resilienz und das bedeutet, dass das Gesamtsystem trotz Störungen handlungsfähig bleibt.

Die Frage, die sich vor diesem Hintergrund nach dem GSM-R-Ausfall stellt, lautet daher nicht, ob ein Fehler aufgetreten ist. Die Frage lautet: Weshalb war die vorhandene Systemarchitektur anscheinend nicht in der Lage, diesen Fehler aufzufangen?

Ein Single Point of Failure ist nicht einfach ein technischer Defekt. Er ist ein Hinweis auf strukturelle Verwundbarkeit.

Strukturelle Verwundbarkeit

Ingenieure verwenden für besonders kritische Schwachstellen einen präzisen Begriff: Single Point of Failure (SPoF). Gemeint ist ein einzelner Punkt innerhalb eines Systems, dessen Ausfall unverhältnismäßig große Auswirkungen entfaltet.

Die Untersuchung durch DB InfraGO zeigt: Ein klassischer Single Point of Failure im engeren Sinn – eine fehlende Redundanz – lag hier gar nicht vor. Die Rückfallebene existierte. Der eigentliche Schwachpunkt war die Erkennungs- und Umschaltlogik, die im Ernstfall nicht wie vorgesehen griff. Das ist eine unbequemere Erkenntnis, als es eine fehlende Redundanz gewesen wäre. Es reicht nicht, Redundanz zu bauen – man muss auch sicherstellen, dass sie im Ernstfall tatsächlich aktiviert wird.

Die entscheidende Erkenntnis bleibt jedoch unabhängig vom konkreten Ergebnis bestehen: Wenn der Ausfall eines einzelnen Systems bundesweite Auswirkungen haben kann, stellt sich zwangsläufig die Frage nach der Architektur der dahinterliegenden Infrastruktur. Und: Es geht dabei nicht um Schuldzuweisungen. Es geht um Risikomanagement.



In der Luft- und Raumfahrt werden Redundanzen von Anfang an mitgedacht, wie schon ein kurzer Blick ins Cockpit aufzeigt: Alles ist doppelt vorhanden.

Vom Schienenverkehr zur Sicherheitsfrage

Noch vor wenigen Jahren wäre ein solcher Vorfall vor allem als Eisenbahn-

Die Schiene ist Teil der kritischen Infrastruktur Europas.

thema betrachtet worden, doch diese Sichtweise greift heute zu kurz. Die Schiene ist längst mehr als ein Verkehrsträger. Sie ist Teil der kritischen Infrastruktur Deutschlands und Europas. Über die Schiene werden Rohstoffe, Fahrzeuge, Chemieprodukte, Energiekomponenten und industrielle Vorprodukte transportiert. Häfen sind auf funktionierende Schienenverbindungen angewiesen. Industrieunternehmen kalkulieren ihre Lieferketten auf Basis verlässlicher Transportzeiten.

Hinzu kommt ein weiterer Aspekt: Mit dem russischen Angriff auf die Ukraine hat die Bedeutung militärischer Mobilität in Europa erheblich zugenommen. Die NATO betrachtet die Schiene als einen zentralen Bestandteil ihrer Logistik. Truppen, Fahrzeuge, Munition und Versorgungsgüter lassen sich über große Distanzen kaum effizienter transportieren als auf der Schiene. Vor diesem Hintergrund erhält die Aussa-

ge des stellvertretenden SPD-Fraktionsvorsitzenden Armand Zorn besonderes Gewicht. Er bezeichnete nach dem Totalausfall des Funknetzes einen krisenfesten Bahnverkehr als Frage der nationalen Sicherheit. Und tatsächlich reicht die Bedeutung inzwischen weit darüber hinaus, denn ein resilientes Schienensystem ist auch eine Frage der europäischen Sicherheit.

Graceful Degradation

In Diskussionen und Beiträgen wird Resilienz häufig mit Redundanz gleichgesetzt. Das ist nicht ganz falsch, greift aber zu kurz.

Raum- und Luftfahrt sprechen in diesem Zusammenhang häufig von „Graceful Degradation“. Gemeint ist die Fähigkeit eines Systems, bei Ausfällen zwar kontrolliert Leistung zu verlieren, aber nicht vollständig zusammenzubrechen.

Übertragen auf die Schiene ergibt sich daraus eine interessante Frage: Warum führte der Ausfall nicht zu einem eingeschränkten Betrieb, sondern verursachte gleich solche massiven Auswirkungen auf das Gesamtsystem? Und weitere Fragen folgen daraus: War ein schrittweises Auffangen des Problems technisch nicht möglich? Waren alternative Betriebsverfahren überhaupt

vorgesehen? Wie schnell konnten Notfallsysteme aktiviert werden – weshalb wurden sie nicht aktiviert? Und welche Lehren ergeben sich daraus für die zukünftige Systemarchitektur?

Diese Fragen dürften für Infrastrukturmanager, Sicherheitsexperten und den Bundesverkehrsminister weit wichtiger sein als die konkrete Ursache des ursprünglichen Fehlers.

Was wissen wir noch nicht?

Für die DB InfraGO und die politischen Entscheidungsträger ergibt sich aus dem Vorfall eine noch grundsätzlichere Herausforderung. Nicht die Frage „Welcher Server ist ausgefallen?“ ist dabei interessant, sondern: Welche weiteren Single Points of Failure schlummern möglicherweise noch in unserer Schieneninfrastruktur, was wissen wir noch nicht und wie hoch ist das Gefahrenpotenzial?

Moderne Infrastrukturen basieren heute auf einer Vielzahl digitaler und physischer Abhängigkeiten. Kommunikationssysteme, Leit- und Sicherungstechnik, Rechenzentren, Energieversorgung, Datennetze, Cloud-Dienste, Satellitenkommunikation und so weiter. Je stärker diese Systeme miteinander

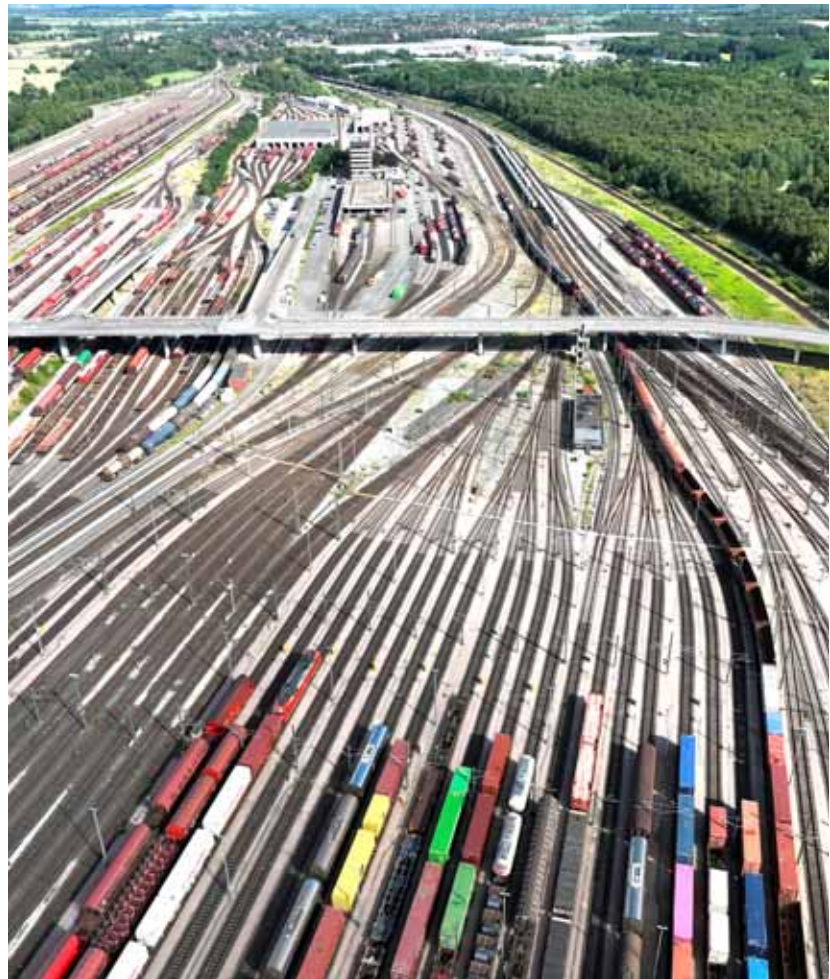
Ein wirklich resilientes System muss nicht jeden Fehler verhindern. Es muss in der Lage sein, trotz eines Fehlers weiterzuarbeiten.

der vernetzt werden, desto größer wird die Bedeutung ihrer Fähigkeit, bei einem vorhandenen Fehler verlässlich weiterarbeiten zu können.

Die Digitalisierung erhöht die Leistungsfähigkeit von Infrastrukturen erheblich. Gleichzeitig kann sie neue systemische – und damit sehr gefährliche – Risiken schaffen, wenn kritische Abhängigkeiten nicht ausreichend berücksichtigt werden.

Eine Debatte, die geführt werden muss

Die Ursache ist inzwischen bekannt – die eigentliche Debatte darüber, was da-



Auch Maschen, Europas größter Rangierbahnhof, hängt an einem Flaschenhals: Das Ein- und Ausfahrgleis genügt, um zu zeigen, was ein Single Point of Failure in der Praxis bedeutet – fällt es aus, steht die gesamte Anlage.

raus folgt, hat gerade erst begonnen. Und wie auch immer das Ergebnis aussehen wird: Der jüngste Ausfall darf nicht als isoliertes Betriebsereignis betrachtet werden. Er sollte als Anlass dienen, eine grundsätzliche Debatte über die Resilienz der deutschen Schieneninfrastruktur zu führen. Es geht um die Fragen, welche Anforderungen eine moderne Industrienation an ihre kritische Infrastruktur stellen darf und muss – und wie sichergestellt werden kann, dass die Anforderungen eingehalten werden.

Bundesamt für Schieneninfrastruktur?

Mit dem KRITIS-Dachgesetz, das am 17. März 2026 in Kraft trat, existiert inzwischen ein bundesweiter Rahmen: Betreiber kritischer Anlagen – auch im Schienenverkehr – müssen sich beim Bundesamt für Bevölkerungsschutz

und Katastrophenhilfe registrieren und perspektivisch Resilienzpläne vorlegen. Ob das ausreicht, um Vorfälle wie den GSM-R-Ausfall künftig zu verhindern, ist damit aber noch nicht beantwortet: Das Gesetz verlangt Verfahren und Nachweise, aber bislang keine konkreten technischen Schutzziele für einzelne Systeme wie den Zugfunk.

Vielleicht wäre die von dem Verband „Die Güterbahnen“ gestellte Forderung nach einem Bundesamt für Schieneninfrastruktur ein möglicher Schritt in die richtige Richtung. Doch damit allein ist es vermutlich noch nicht getan. Es kommt darauf an, welche Kompetenzen es letztlich hat und wie dieses Bundesamt aufgebaut ist. Und eins ist sicher: Die Bundeswehr braucht rasch einen festen Platz – entweder in einem solchen neuen Bundesamt oder aber innerhalb der DB InfraGO. cwk

Drei Fragen an Stefan Katzenbeisser

„Wir müssen Resilienz mitdenken“

Der GSM-R-Ausfall hat gezeigt: Redundanz ist nicht gleich Resilienz. Im Kurzinterview erklärt Prof. Dr. Stefan Katzenbeisser, warum sicherheitskritische Bahnsysteme bei Fehlern abschalten statt weiterzulaufen.

Privatbahn Magazin: Herr Prof. Dr. Katzenbeisser, beim GSM-R-Ausfall wurde die vorhandene Redundanz nicht automatisch aktiviert. Ist das aus Ihrer Forschungserfahrung ein typisches Muster bei sicherheitskritischen Bahnsystemen?

Stefan Katzenbeisser: Eigentlich nicht. Die Software in sicherheitskritischen Systemen wird nach sehr hohen Qualitätsstandards entwickelt und vor dem Einsatz umfangreich getestet. Warum der großflächige Ausfall von GSM-R geschehen ist, wird untersucht werden müssen, auch um ähnliche Fehler in der Zukunft zu vermeiden. Aber immerhin war es – meines Wissens – der erste große Ausfall durch einen Softwarefehler seit Jahrzehnten. Das zeigt schon, dass das System an sich recht robust ist.

Wie unterscheidet sich ein resilientes Systemdesign, das Fehler nicht nur verkraftet, sondern auch automatisch erkennt und behebt, von der heutigen Praxis?

Man muss klar zwischen Redundanz und Resilienz unterscheiden. Die meisten in Betrieb stehenden Systeme sind redundant ausgelegt, um Fehler in Komponenten oder einzelne Ausfälle kompensieren zu können. Dadurch wird aber nicht automatisch Resilienz erreicht, bei der zumindest ein Teil der Funktionalität trotz Fehlern aufrechterhalten werden kann. Wir haben das bei dem GSM-R-Ausfall im Oktober 2022 in Norddeutschland gesehen: Heute wissen wir, dass Kupferdiebe zwei zentrale Kabel unabhängig voneinander durchtrennt haben. Trotz technisch vorhandener Redundanz war ein Aufbau von GSM-R-Verbindungen danach nicht mehr möglich.

Echte Resilienz wird in Zukunft immer wichtiger werden: Wir digitalisieren

und vernetzen immer größere Bereiche des Bahnbetriebs, dadurch steigt die Komplexität der eingesetzten Systeme. Gleichzeitig werden wir immer verwundbarer – das können „banale“ Softwarefehler sein, aber auch Cyberangriffe oder hybride Bedrohungen durch staatliche Akteure. Gerade im Kontext des Kriegs in der Ukraine haben wir gesehen, dass Eisenbahninfrastruktur vielfältigen Bedrohungen ausgesetzt ist und dass wir lernen müssen, mit solchen Vorfällen umzugehen – also trotz Bedrohungen Bahnbetrieb aufrechtzuerhalten.

Das ist heute nur sehr eingeschränkt möglich. Ein grundlegendes Designprinzip sicherheitskritischer Systeme ist, bei Fehlern in einen „sicheren Zustand“ überzugehen, aus dem keine weiteren Risiken entstehen. Oftmals bedeutet das eben, keinen Betrieb mehr zuzulassen. Beim Design künftiger Systeme müssen wir Resilienz daher mitdenken. Da stehen wir ganz am Anfang.

Mit der fortschreitenden Digitalisierung durch ETCS und FRMCS wächst die Vernetzung im Bahnsystem. Nimmt dadurch die Gefahr kaskadierender Ausfälle zu – und was müsste ein Betreiber wie DB InfraGO konkret anders machen, um genau das zu verhindern?

Je komplexer ein System, desto anfälliger ist es für Ausfälle – und natürlich auch für Ausfälle, die durch unvorhergesehene, kaskadierende Fehler entstehen. Bei einem resilienten System sollten diese Kaskaden aufgebrochen werden. Man muss einfach damit rechnen, dass Teile eines Systems aufgrund eines Fehlers oder auch eines Angriffs ausfallen. Systeme müssen wieder kleinteiliger werden, auch eine räumliche Trennung kann helfen. So lassen sich



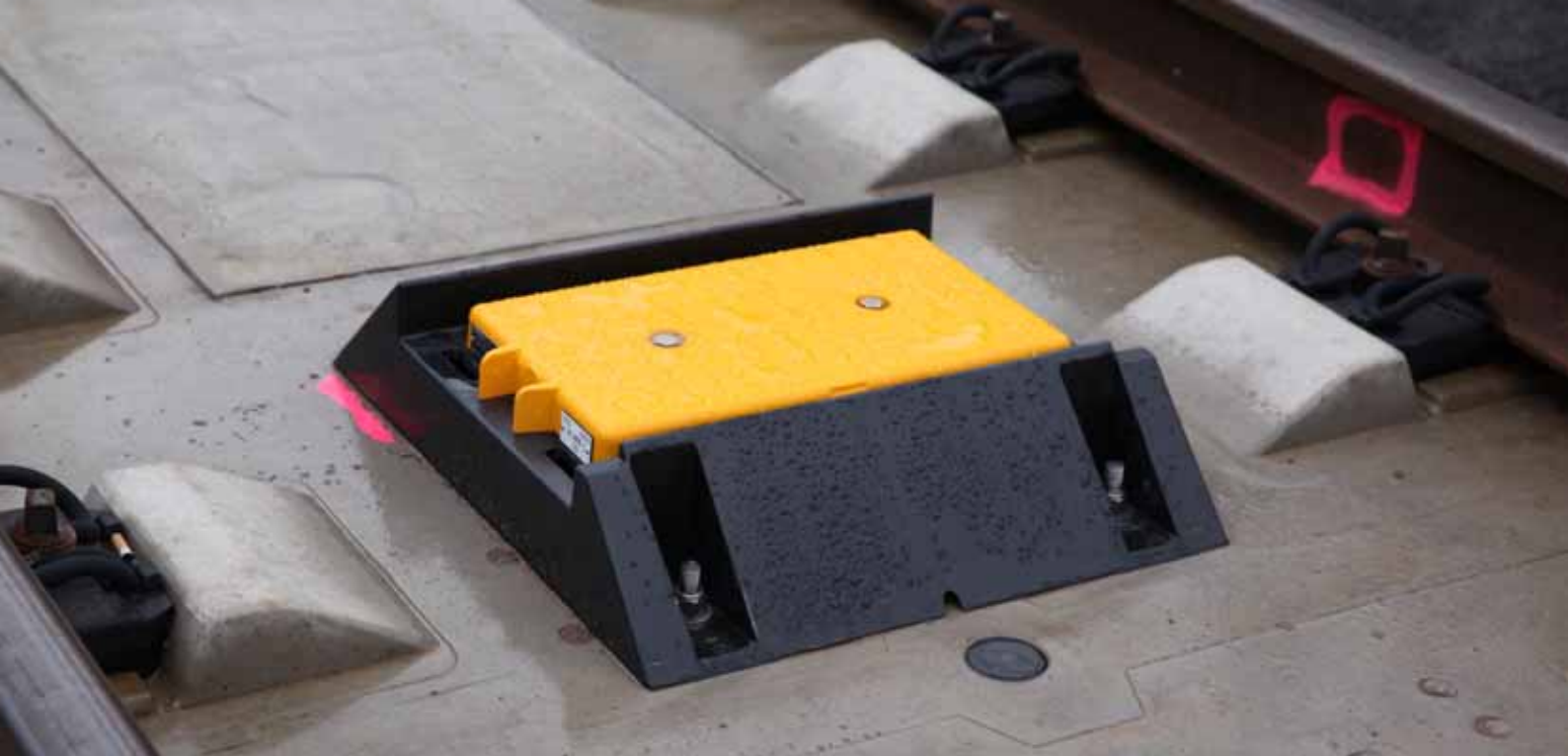
Prof. Dr. Stefan Katzenbeisser
ist Professor für Technische Informatik mit Schwerpunkt Cybersicherheit an der Universität Passau und Gründer sowie Leiter des Bereichs Railway Security Research bei der INCYDE GmbH. Er forscht seit über zehn Jahren zu Cybersicherheit im Eisenbahnwesen, unter anderem zur Sicherheitsarchitektur von Stellwerkstechnik.

die Auswirkungen von Fehlern zumindest örtlich begrenzen.

Wichtig wird aber auch sein, dass wir die Rückfallebenen betrachten. Wenn ein wichtiges System ausfällt – das kann wie im aktuellen Beispiel der Funk sein oder aber auch ein Stellwerk –, dann muss eine Rückfallebene vorhanden sein. Das kann etwa das öffentliche Mobilfunknetz sein, auf das stärker zurückgegriffen wird. Wir müssen uns aber auch die Betriebsverfahren selbst ansehen – das Fahren auf Befehl ist nicht mehr zeitgemäß und wird im Kontext von hybriden Bedrohungen neu gedacht werden müssen. Die Nutzung einer Rückfallebene wird zwar immer mit einer Kapazitätsreduktion verbunden sein, aber das Ziel muss sein, einen kompletten Stillstand zu verhindern.

Vielen Dank für das Gespräch, Herr Prof. Dr. Katzenbeisser.

Die Fragen stellte Dennis Tesch.



Unscheinbar, aber systemrelevant: Balisen könnten als Rückfallsysteme genutzt werden, um moderne Leittechnik auch bei Ausfällen noch nutzen zu können. Solche Systeme müssen bei der Digitalisierung von Anfang an mitgedacht werden.

Strukturelle Schwächen des Bahnfunks

Ein Hersteller, ein Ausfall

Ein Softwarefehler, ein Hersteller-Monopol, Schlüssel per USB-Stick: IT-Sicherheitsexperte Lukas Iffländer seziert, warum der GSM-R-Ausfall kein Ausreißer war, sondern System hat – und warum ein krisenfestes Bahnnetz längst eine Frage der nationalen Sicherheit ist.

Der GSM-R-Ausfall vom 23. Juni 2026 ist kein Einzelfall, wenn auch in seinem Ausmaß bisher einzigartig. Einen technisch ähnlichen Vorfall hatte DB InfraGO vor einiger Zeit bereits im Knoten Frankfurt, und offenbar hat man daraus nur beschränkt gelernt. An vielen Stellen im Bahnbereich ist Technik im Einsatz, deren Austausch und Upgrades nicht ordentlich durchsimuliert werden. Teilweise sind sie gar nicht durchsimulierbar, weil eine Testumgebung für die Alttechnik so groß sein müsste, dass sie wirtschaftlich nicht darstellbar ist. Hinzu kommt, dass offenbar kein ausreichendes Gefühl für das Gesamtsystem vorhanden ist. Man hat, wie bei KRI-TIS-relevanten Systemen vorgesehen, eine Risikoabschätzung durchgeführt und sich dann entschieden, den Tausch deutlich vor Mitternacht anzusetzen. Klassischerweise macht man so etwas nach ein Uhr nachts. Bei dieser Risikoabschätzung hat man sich also massiv verschätzt. Bei den älteren Systemen liegt das daran, dass man die Technik

teilweise schlicht nicht mehr überblickt; bei den neueren daran, dass die Entscheider mit den neuen Komponenten und Konzepten nicht vertraut genug sind, um das Risiko richtig einzuschätzen.

Ein Hersteller, ein Ausfall

Grundsätzlich zeigt der Fall ein strukturelles Problem: Wie vom Autor schon mehrfach betont, sollte auf heterogene Systeme gesetzt werden – das würde einen Sicherheitsgewinn bringen. Gerade bei GSM-R ziehen sich immer mehr Anbieter zurück, sodass an vielen Stellen nur noch einer existiert. Baut der eine schlechte Komponente oder eine mit einem Security-Problem, fällt im Extremfall das ganze deutsche Netz aus.

Beim neuen Zugfunk FRMCS besteht die Hoffnung, dass man es intelligenter hinkommt. Allerdings droht auch hier das Risiko, ein derart spezifisches System zu bauen, dass es wieder nur ein oder zwei Hersteller anbieten. Ähn-

lich sieht es in der Stellwerkstechnik aus. Bis auf ein kleines Scheidt & Bachmann teilen sich Siemens und Hitachi praktisch den gesamten Markt, und häufig bietet auf ein Projekt genau ein Hersteller. Dann kann man nicht den mit der besten Security wählen. Am Schluss reicht es, wenn jemand einen Hersteller hackt, und das gesamte deutsche System steht. Mit heterogenen Komponenten ließe sich das vermeiden, bis hin zu Systemen, in denen Bauteile unterschiedlicher Hersteller dieselbe Aufgabe übernehmen. Fällt das Vertrauen in einen Hersteller vorübergehend weg, übernehmen die anderen.

„Am Schluss reicht es, wenn jemand einen Hersteller hackt, und das gesamte deutsche System steht.“

Generell muss angemerkt werden, dass GSM-R etwas sicherer ist als GSM, aber von Anfang an mitgedacht war Cybersicherheit nicht. Aus verlässlicher

FOTOS: STÖRFIX VIA CC BY-SA 3.0 DE; HTW DRESDEN

und vertraulicher Quelle ist bekannt, dass bestimmte Länder keine Security haben wollten und sich beim Aufsetzen der Sicherheitsschicht für GSM-R und ETCS eingemischt haben. Deshalb ist schlicht zu wenig Sicherheit in den Systemen. Die größte Lücke zwischen Anspruch und Praxis sehe ich bei ETCS in der Schlüsselverwaltung. Der Zug muss wissen, dass das RBC, also die Zentrale, die ihm mit der Movement Authority die Freigabe für eine Fahrt schickt, valide ist, und genauso muss das RBC wissen, welche Züge valide sind. Bis heute werden diese Schlüssel manuell per USB-Stick in RBCs und Fahrzeugen installiert. Das kann dazu führen, dass eine Strecke längst mit ETCS ausgerüstet ist, die Züge aber noch wochenlang mit PZB fahren, bis sie endlich ihren Schlüssel bekommen haben. Bei einer Skalierung von ETCS auf alle Gleise in Europa ist so etwas nicht handelbar. Gerade beim Key-Management hat die Deutsche Bahn ein wirklich großes Problem, und das ist einer der vielen Gründe, warum es bei Stuttgart 21 nicht oder nur sehr schlecht funktioniert.

Ausweichsysteme und Rückfallebenen schaffen

Auch beim geplanten Nachfolgesystem FRMCS ist die Netzwerkabhängigkeit ein Thema, weil ETCS permanenten Funk braucht. Wenn wir FRMCS „gut machen“, darf nicht mit der Maxime „Wir bauen noch einmal GSM-R“ herangegangen werden. Vielmehr muss am Ende ein System mit ordentlichem Roaming zu den öffentlichen Mobilfunkanbietern stehen. Sind nur die Bahnmasten gestört, fährt der Zug dann vereinfacht gesagt mit Vodafone, Telekom, O2 oder 1&1 weiter. Bekommen wir das hin, werden wir sogar etwas weniger netzabhängig. Nach aktueller DB-Logik stellen wir den Betrieb allerdings ein, sobald der Funkempfang fehlt, und das muss man generell diskutieren. Zudem brauchen wir Rückfallebenen für den Fall, dass der Funk wirklich gestört wird. Das gilt weniger für den täglichen Personenverkehr, aber die Bahn ist kritische Infrastruktur und relevant für den militärischen Transport

„Wenn wir in der Lage sein müssen, im Ernstfall binnen kürzester Zeit Truppen Richtung Baltikum zu verlegen, können wir uns halbgarer IT-Sicherheitslösungen nicht erlauben.“

auf der Schiene. Denkbar ist ein gewisser Durchsatz über eine ETCS-Level-1-Rückfallebene, also im Kern Balisen und wenige Signale, um Militärzüge sicher abzufertigen. Kommt zusätzlich über ein Rückfallnetz eine Form von Internet auf die Züge, ließe sich darüber so etwas wie der digitale Befehl mit einer zusätzlichen Sicherheitsebene umsetzen.

Was das für die nationale Sicherheit bedeutet, ist dabei besonders wichtig: Ein krisenfestes Bahnsystem ist definitiv eine Frage der nationalen Sicherheit, und hier greift alles ineinander. IT-Sicherheit bedeutet nicht nur, ein System gegen Manipulation zu schützen, sondern umfasst auch dessen Verfügbarkeit. Genauso wie das System einem Hackerangriff standhalten muss, muss es auch funktionieren, während gerade eine Komponente ausgetauscht wird. Wenn wir in der Lage sein müssen, im Ernstfall binnen kürzester Zeit Truppen Richtung Baltikum zu verlegen, können wir uns halbgarer IT-Sicherheitslösungen nicht erlauben.

Und nicht zuletzt hat der Ausfall aus Fahrgastsicht das Vertrauen in die Zuverlässigkeit des Systems Bahn beschädigt. Eine persönliche Anmerkung, denn die Erfahrung betrifft bei mir Hauptberuf und Ehrenamt gleichermaßen: Meine Studentinnen und Studenten haben sehr gegrinst, als ich an dem Tag zehn Minuten zu spät in die Vorlesung marschiert bin, weil ich gerade das achte Interview gegeben hatte. Das zeigt, wie sehr ein so unzuverlässig laufendes System die Öffentlichkeit beschäftigt. Verkehrsminister Schnieder hat es so formuliert: Wenn die Bahn nicht ordentlich läuft, ist das demokratiefährdend.



Prof. Dr. rer. nat. Lukas Iffländer
ist Professor für Informationssicherheit an der Hochschule für Technik und Wirtschaft Dresden, mit Schwerpunkt auf der Schnittstelle von Safety und Security im Bahnwesen.

Er promovierte an der Julius-Maximilians-Universität Würzburg zu adaptiven, angriffsresistenten Sicherheitsmechanismen. Zuvor war er wissenschaftlicher Referent für Cybersicherheit am Deutschen Zentrum für Schienenverkehrsforschung (DZSF). Im März wurde Iffländer zum Bundesvorsitzenden des Fahrgastverbands Pro Bahn gewählt.

Jetzt anfangen!

Wir brauchen deshalb schnell eine Modernisierung auf resilientere Technologien wie 5G. Und wir müssen die Frage stellen, ob eine DB InfraGO, die permanent mit Feuerlöschern beschäftigt ist, weil es immer irgendwo im Schienennetz brennt, gleichzeitig innovativ sein kann. Vielleicht brauchen wir dafür eine Struktur innerhalb oder außerhalb des DB-Konzerns, geführt von kompetenten Ingenieuren und Informatikern statt einem ehemaligen Kanzleramtschef, die neue Technik entwickelt und zunächst auf einem Teilnetz zum Laufen bringt. Inselnetze wie die Usedomer Bäderbahn bieten sich für solche Leuchtturmprojekte an; von dort lässt sich das Ganze ins Gesamtnetz ausrollen. Wir sollten nicht wie bei Stuttgart 21 die 150-Prozent-Lösung suchen und hinterher merken, was man alles übersehen hat, sondern uns schrittweise an das Thema herantasten.

Lukas Iffländer



Hochverfügbare Kommunikations- und Informationssysteme bilden das Rückgrat für sichere, effiziente und zukunftsfähige Betriebsführung – von GSM-R bis FRMCS.

Im Interview: Marcel Haar

„Sicherheit liegt in unserer DNA“

Im Interview erklärt Frequentis-Deutschland-Chef Marcel Haar, was in Sachen Zugfunk auf den Bahnbetrieb zukommt und weshalb jetzt der richtige Zeitpunkt ist, den Übergang strategisch und mutig anzugehen. Ein Gespräch über FRMCS, Migration und Cyber-Resilienz.

Privatbahn Magazin: Herr Haar, Frequentis feierte 2025 40 Jahre in Deutschland. Wo steht das Unternehmen heute – und welche Rolle spielt die Bahn im Portfolio?

Marcel Haar: Frequentis ist heute in fünf Geschäftsfeldern aktiv, eines davon ist der Bahnbereich einschließlich ÖPNV. In Deutschland beschäftigen wir an acht Standorten rund 500 Mitarbeitende – mit wachsender Tendenz. Insgesamt haben wir weltweit mehr als 10.000 Bedienstete im Bereich Operations Communication ausgestattet. Dieses Know-how bringen wir heute in die Bahn ein. Unsere Wurzeln liegen in der Flugsicherung, Sicherheit – im Sinne hochverfügbarer, missionskritischer Kommunikation – liegt also in unserer DNA. Das übertragen wir auf andere sicherheitskritische Bereiche wie Bahn, Behörden und Organisationen mit Sicherheitsaufgaben (BOS) oder Verteidigung.

FRMCS gilt als Nachfolger von GSM-R. Welche sicherheitsrelevanten Verbesserungen bringt das neue System?

FRMCS – das Future Railway Mobile Communication System – ist im Grunde schon der übernächste Stan-

dard. Es basiert auf 3GPP-Telekommunikationsstandards und setzt konsequent auf Breitband und IP-Architekturen. Damit steigen Bandbreite, Datenrate und Flexibilität signifikant. Im Vergleich zu GSM-R bedeutet das höhere Betriebssicherheit, mehr Cybersecurity dank aktueller Verschlüsselungs- und Authentifizierungsverfahren, bessere Systemverfügbarkeit und Interoperabilität auf europäischer Ebene – zumindest ist das das klare Ziel.

Welche neuen Anwendungen werden durch FRMCS möglich?

Breitband als IP-Standard eröffnet enormes Potenzial. Neben Sprache rücken Daten, Video und perspektivisch KI-gestützte Auswertungen in den Vordergrund: Bildgebende Verfahren zur Streckenüberwachung und Lagebeurteilung können neu gedacht werden. Automatisierte Rangierprozesse im Depot sowie Unterstützung von ETCS und ATO werden möglich. Denn mit 5G – perspektivisch 6G – lassen sich große Datenmengen wirtschaftlich übertragen. Videostreams sind so deutlich günstiger geworden. In Verbindung mit KI können Anomalien erkannt, Alarme automatisiert ausgelöst und Entscheidungspro-

zesse beschleunigt werden. Je mehr valide Daten vorliegen, desto fundierter kann man reagieren. Konkretes Beispiel ist eines unserer Projekte mit den ÖBB: Dort werden automatisierte Drohnenüberwachungssysteme erprobt. Hangars sind in regelmäßigen Abständen entlang der Strecke positioniert. Bei einem Ereignis ist die Drohne das Auge der Leitstelle. Das hilft etwa, Strecken schneller wieder freizugeben – mit positiven Effekten auf Pünktlichkeit und Sicherheit.

Welche Rolle spielen Ihre Leitstellenlösungen in dieser Transformation?

Eine zentrale. Unser Kernsystem im Bahnbereich ist das FTS – das Fixed Terminal System –, ein hochverfügbares Sprachsystem für Leitstellen. Es integriert unterschiedlichste Kommunikationskanäle und sorgt für durchgängige, ausfallsichere Kommunikation zwischen Disponenten, Fahrdienstleitern und operativem Personal. Darüber hinaus entwickeln wir Incident-Management- und Messaging-Lösungen: GuardX unterstützt das Management von Zwischenfällen – inklusive gerichts-fester Dokumentation. OnSite mit MissionX Messenger ermöglicht sicherheitsrelevantes Messaging, etwa bei Unfällen, Vandalismus oder terroristischen Bedrohungen. Unser Anspruch ist es, dass sich Eisenbahnverkehrsunternehmen auf ihren Betrieb konzentrieren können, während wir

„hinter den Kulissen“ die Kommunikationsinfrastruktur zukunftsfähig machen.

Wo liegen aktuell die größten Herausforderungen bei der Migration von GSM-R zu FRMCS?

Die größte Herausforderung ist die Integration in den Bestand. Wir sprechen über jahrzehntealte Infrastrukturen, die weiter betrieben werden müssen. Deshalb plädieren wir für einen phasenweisen Übergang mit Interworking Functions. Systeme wie TETRA, GSM-R und FRMCS können parallel getestet und sukzessive vernetzt werden. So entsteht ein „Transition Progress“ mit klaren Meilensteinen. Privat nutzen wir alle Breitband längst seit fünf bis zehn Jahren. In sicherheitskritischen Infrastrukturen dauert ein Technologiewechsel jedoch 10 bis 15 Jahre. Deshalb ist jetzt die entscheidende Anfangsphase. Wer heute beginnt, legt die Grundlage für die nächsten Jahrzehnte.

Wir sehen dazu derzeit unterschiedliche Strategien: Die SNCF etwa baut 4G-Infrastruktur über öffentliche Netze aus – mit einem klaren „Just do it“-Ansatz. Die Deutsche Bahn verfolgt die Idee eines eigenen Netzes mit entsprechender Infrastruktur. Beide Wege haben Vor- und Nachteile, etwa in Bezug auf Abhängigkeit von großen Mobilfunknetzbetreibern (MNO).

Noch einmal: Wichtig ist, jetzt anzufangen. Die politischen Rahmenbedingungen – Stichwort Sondervermögen und gestiegene Sensibilität für kritische Infrastrukturen – schaffen ein Momentum, das genutzt werden sollte.

Welche Rolle spielen Standards und regulatorische Vorgaben?

Eine sehr große. Wir sind in internationalen Standardisierungs-gremien aktiv und beschäftigen uns intensiv mit Themen wie NIS2 und dem Cyber Resilience Act. Gerade in sicherheitskritischen, grenzüberschreitenden Bereichen sind europa- oder weltweite Standards essenziell. Sie vereinfachen Interoperabilität, beschleunigen Projekte und senken Kosten. Gleichzeitig geht es um technologische Souveränität. Regierungen wollen – etwa wie im Verteidigungsbereich – Standards setzen und

strategische Kontrolle behalten. Unsere Produkte sind modular aufgebaut und konsequent standardbasiert. Das ermöglicht es, Erfahrungen aus anderen Bereichen – etwa Luftfahrt oder BOS – in die Bahn zu übertragen.

Wie wichtig sind Redundanzkonzepte und Cyber-Resilienz in Ihrer Produktstrategie?

Sie sind das A und O. Unsere Herkunft aus der militärischen und zivilen Flugsicherung prägt uns. Dort ist Ausfall keine Option. Auch im Bahnbereich erleben wir derzeit ein Umdenken. Solange kein Schaden eintrat, wurde Redundanz oft als Kostenfaktor gesehen. Doch Blackout-Szenarien oder Cyberangriffe zeigen, wie verletzlich Infrastrukturen sein können. Cyber-Resilienz bedeutet für uns nicht nur Schutz, sondern auch schnelle Wiederherstellbarkeit.

Wo sehen Sie die größten sicherheitsbezogenen Herausforderungen für Bahnbetreiber in Deutschland?

In der Kombination aus alter Infrastruktur, steigenden Anforderungen und wachsender Bedrohungslage. Die Integration neuer Technologien in bestehende Systeme ist komplex – technisch wie organisatorisch.

Wir arbeiten bereits mit sieben der zehn größten Bahnen Europas zusammen, darunter die SBB, die ÖBB, die SNCF und Network Rail. Überall sehen wir: Der Wille zur Transformation ist da.

Wie sollte der FRMCS-Einstieg also konkret aussehen?

Flächendeckend zu denken, ist aus unserer Sicht der falsche Ansatz. Sinnvoller ist es, in klar abgegrenzten Korridoren zu beginnen – etwa im Rahmen von Grundsaniierungen wie Hamburg–Berlin. Solche Abschnitte eignen sich ideal für Proof-of-Concept-Projekte. Ziel ist es, zunächst Daten zu sammeln und auf dieser Grundlage eine realistische Roadmap für den Bestand zu entwickeln. Ein konkretes Beispiel ist der MCX System Trial bei der ÖBB, wo Frequentis Mission Critical Services im österreichischen Bahnnetz getestet werden. Einen weiteren Schritt gehen Pilotprojekte, welche die Brücke vom Legacy-



Marcel Haar

ist seit 2024 Geschäftsführer von Frequentis Deutschland. Der gebürtige Wiener startete 2016 bei Frequentis und baute die Marketing-Organisation für alle Regionen weltweit auf. Haar verfügt über mehr als 15 Jahre Erfahrung unter anderem in den Bereichen Finanzen, Marketing und Vertrieb. Er hat einen Bachelor und Master of Arts (Bank- und Finanzdienstleistungen) der Fachhochschule des BFI Wien.

System zum Breitband schlagen – sowohl auf der Strecke als auch in Bahnhöfen. Und das selbstverständlich unter Einhaltung aller Compliance- und Security-Standards. Jetzt braucht es Mut zum Start. Die Produkte sind vorhanden, die Standards werden definiert, die technologischen Grundlagen gelegt. Wenn wir heute beginnen, Interoperabilität und Cyber-Resilienz konsequent mitzudenken, schaffen wir ein Kommunikationsfundament, das den Bahnbetrieb der Jahrzehnte sicher trägt. Einen eindrucksvollen Praxisbeweis dafür lieferten kürzlich die Niederösterreichische Verkehrsorganisation (NÖVOG) und Frequentis mit einem Leuchtturmprojekt: Erstmals wurde MCX in Österreich ausschließlich für den Bahnbetrieb implementiert. Die Frequentis-Lösung ermöglicht bereits heute nahtlose, missionskritische Kommunikation für die Schneebergbahn – auf der Strecke von Puchberg zum Hochschneeberg über öffentliche Mobilfunknetze.

Vielen Dank für das Gespräch, Herr Haar!

Das Gespräch führte Dennis Tesch.



Rund 1000 Militärzüge jährlich bringt die Bundeswehr derzeit auf die Schiene. Quantitativ überschaubar – für Eisenbahnverkehrsunternehmen mit leistungsfähigen Lokomotiven jedoch ein strategisch interessantes Marktsegment.

Oberst i. G. Rüdiger Just Winkler im Interview

1800 Kilometer zur Ostflanke

Privatbahn Magazin: Herr Oberst Just Winkler, welche strategische Bedeutung hat die Durchführung von Militärtransporten auf der Schiene für die Bundeswehr angesichts der veränderten Sicherheitslage in Europa?

Rüdiger Just Winkler: Die seit 2014 mit der völkerrechtswidrigen Annexion der Krim sich verändernde Sicherheitslage hat zu einer Refokussierung der Bundeswehr auf die Aufgabe Landes- und Bündnisverteidigung geführt. Der im Februar 2022 begonnene vollumfängliche Angriff auf die Ukraine hat in der NATO die Notwendigkeit, Bündnisverteidigung weiter voranzutreiben, noch verstärkt und beschleunigt.

Bündnisverteidigung ist nun nicht etwas völlig Neues. Für Deutschland ergeben sich aber zwei ganz wesentliche Merkmale, die bis zum Ende des Kalten Krieges 1989 nicht im Fokus lagen. Zum einen war es die Fähigkeit der Bundeswehr, aufgrund der bestehenden Wehrpflicht im Ernstfall massiv aufzuwachsen und militärische Fähigkeiten zu generieren. Zum anderen – und hier kommt die Bahn ins Spiel – waren die Entfernungen, um Menschen und Material in ihre Einsatzräume an der innerdeutschen Grenze zu verbringen, recht überschaubar.

Wenn wir heute über Landes- und Bündnisverteidigung reden, dann findet diese an der NATO-Ostflanke statt. Dazu müssen wir erst einmal eine Distanz von 1500 bis 1800 Kilometern überwinden. Ausreichende Transportkapazitäten brauchen wir nicht nur für die Verlegung unserer Kräfte, sondern auch für die dann folgende logistische Versorgung. Große Mengen, gerade von schwerem und überbreitem Material, lassen sich sehr gut mit dem Verkehrsträger Schiene transportieren.

In der Zeit des Kalten Kriegs gehörten Militärtransporte auf der Schiene zum Tagesgeschäft. Nach 1990 verlor dieses Thema an Bedeutung. Muss die Bundeswehr die Fähigkeiten zur Zusammenarbeit mit der Eisenbahn erst wieder aufbauen?

Die Truppe übt Bahnverladungen regelmäßig und kann sich dabei auf erfahrene Experten des Logistikzentrums der Bundeswehr und der DB Cargo stützen. Das heißt: Nein, Bahntransporte gehören für die Bundeswehr unverändert zum Tagesgeschäft.

Die Zusammenarbeitsbeziehungen zwischen der Bundeswehr und der Deutschen Bahn AG und hier insbesondere mit der DB Cargo und der DB InfraGO sind ausgezeichnet.

„Wir dürfen nicht mehr über Rückbau reden, sondern wir müssen den Ausbau voranbringen. Effektivität auch in der Krise ist eine bestimmte Forderung der Streitkräfte. Die Eisenbahn spielt dabei eine ganz zentrale Rolle.“

Was hat sich seit den Militärtransporten auf der Schiene in früheren Jahren zu den Transporten heute verändert?

Der wesentliche Faktor, der sich geändert hat, ist Zeit. Die steht, basierend auf den zugrunde liegenden Szenarien und den daraus resultierenden Plänen, leider nur begrenzt zur Verfügung. Es muss extrem schnell gehen, wenn wir durch unsere Präsenz an der NATO-Ostflanke ein glaubhaftes Abschreckungspotenzial entfalten wollen, damit es bestenfalls gar nicht erst zu einem heißen Konflikt kommt.

Wenn ich wenig Zeit habe, dann müssen Kapazitäten ad hoc zur Verfügung stehen. Sowohl die Durchlässigkeit für lademaßüberschreitende Verkehre als auch der Grenzübertritt muss bei einer

FOTOS: BUNDESWEHR/MARCO DOROW (2), FLORIAN KÜRTH (1); ER (4); WERNER (1)

Aktivierung der Kräfte bereits geregelt sein. Das funktioniert nur im engen Zusammenwirken der DB Cargo und der DB InfraGO.

Durch die Aufgabe von Standorten hat die Bundeswehr in den vergangenen Jahren vermutlich auch zahlreiche Umschlagplätze, Rampen und Verladegleise verloren. Gibt es für dieses Problem bereits Lösungsansätze – und wenn ja, welche?

Sicherlich hat nicht mehr jede Kaserne und Liegenschaft der Bundeswehr einen Gleisanschluss. Dennoch haben wir basierend auf der Stationierung der Bundeswehrverbände in Deutschland, die aufgrund ihres Materials einen signifikanten Bedarf an Eisenbahnverladekapazitäten haben, immer noch entsprechende Rampen zur Verfügung. Wir erarbeiten zur Verbesserung beziehungsweise Nachbesserung an einigen Orten Regionalkonzepte, die dann auch gleichzeitig für eine gewisse Redundanz sorgen sollen.

Und nicht zuletzt besitzt die Bundeswehr auch sogenannte mobile Kopframpen, die an beliebigen Orten auf ein Gleis montiert werden können und die Be- und Entladung von Fahrzeugen ermöglichen.

Kann sich grundsätzlich jedes Eisenbahnverkehrsunternehmen (EVU) um die Durchführung von Militärverkehren bemühen?

Ja, grundsätzlich kann sich jedes Verkehrsunternehmen an öffentlichen Ausschreibungen beteiligen. Diese werden durch das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) je nach Bedarf ausgeschrieben.

Welche Anforderungen stellt die Bundeswehr an EVU, die sich für Militärverkehre interessieren – etwa hinsichtlich Verfügbarkeit, Prozesssicherheit, Flexibilität und Fahrzeugausstattung?

Die Anforderungen der Bundeswehr für den Eisenbahntransport werden vor einem Vergabeverfahren durch das Logistikkommando der Bundeswehr in einer Leistungsbeschreibung zusammen-

„Grundsätzlich kann sich jedes Verkehrsunternehmen an öffentlichen Ausschreibungen beteiligen.“

mengefasst und ans BAAINBw übermittelt, das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr. Auf Basis einer Leistungsbeschreibung schreibt das BAAINBw entsprechende Bedarfe der Bundeswehr aus. Lassen Sie mich an dieser Stelle eine für die Truppe ganz wesentliche Anforderung ansprechen, die ein EVU erfüllen muss, das für die Bundeswehr militärische Eisenbahntransporte durchführen will. Etwa 85 Prozent der Eisenbahntransporte der Bundeswehr sind lademaßüberschreitend. Die Abwicklung lademaßüberschreitender Transporte in Deutschland und Europa ist daher eine ganz wesentliche Leistung, die ein EVU erbringen muss, das für die Bundeswehr militärische Güter auf der Schiene transportiert.

Und wie können sich diese EVU bei der Bundeswehr um die Durchführung von Militärverkehren bewerben oder vorab Informationen dazu erhalten?

Es ist einfach so, dass wir bei der Bundeswehr eine klare Aufgabentrennung haben. Der Einkauf zivilgewerblicher Transportdienstleistungen ist Sache der Bundeswehrverwaltung. Das BAAINBw als der zuständige Bedarfsdecker ist deswegen der richtige Ansprechpartner für die EVU. Die Streitkräfte, zu denen ich gehöre, sind der Bedarfsträger. Unsere Aufgabe ist es, die erforderlichen Haushaltsmittel zu beantragen, Bedarfe bestmöglich zu beschreiben und das BAAINBw fachlich zu unterstützen. Natürlich spreche ich auch mit EVU, weil das für die von mir erwartete Marktkennntnis unerlässlich ist. Dabei habe ich immer im Hinterkopf, dass EVU potenzielle Bieter in einem Vergabeverfahren sind, weswegen ich bei Fragen, die sich auf laufende oder zukünftige Vergabeverfahren beziehen, immer an das BAAINBw verweise [siehe Infokasten nächste Seite].



**Oberst im Generalstab (i. G.)
Rüdiger Just Winkler**

ist seit 2024 Referatsleiter J4 I (LogPlans) im Operativen Führungskommando der Bundeswehr in Berlin. In dieser Funktion verantwortet er die operative Planung der logistischen Unterstützung für nationale und internationale Einsätze sowie die Landes- und Bündnisverteidigung. Just Winkler (50) trat 1995 in die Bundeswehr ein und blickt auf zahlreiche logistische Verwendungen in der Truppe, in Kommandobehörden und im Bundesministerium der Verteidigung zurück. Er hat die deutsche und spanische Generalstabsausbildung absolviert.

Wir alle wissen, dass die Schieneninfrastruktur zurzeit in vielen Bereichen marode ist. Wie gehen Sie mit diesem Problem um und welche Erwartungen haben Sie aus militärischer Sicht an die Eisenbahninfrastruktur – zum Beispiel mit Blick auf Achslasten, Tragfähigkeit von Brücken, Lichtraumprofile oder Umschlagpunkte?

Grundsätzlich sind wir als Streitkräfte erst einmal der Kunde der DB Cargo, der einen Transport von A nach B in Auftrag gibt und dabei auch eine Zeitvorgabe für Abfahrt und Ankunft macht. Was der Vertragsnehmer dazwischen unternimmt, ist nicht in unserem Fokus. Ich will damit sagen, dass die Streckenführung erst einmal zweitrangig ist.

Dennoch gehören auch Streckenführungen aus den von Ihnen genannten



Militärtransporte sind logistisch anspruchsvoll – und Zeit ist dabei ein besonders knappes Gut.

Gründen inzwischen zu einem Themenfeld, bei dem wir in der Abstimmung mit dem Netzbetreiber sind. Wir haben gemeinsam mit dem Bundesministerium für Verkehr (BMV) das Ziel, ein Militäreisenbahngrundnetz zu definieren, bei dem wir mit einem für uns relevanten Lichtraumprofil jederzeit und ohne große Vorprüfung lademaßüberschreitende Transporte anmelden und durchführen lassen können. Sofern hier mit kleineren Maßnahmen, zum Beispiel dem Versetzen eines Mastes oder Ähnlichem, Langsamfahranteile oder Umwege für militärische Eisenbahntransporte reduziert werden können, hat die Bundeswehr sogar ein Verfahren, diese Baumaßnahmen zu finanzieren.

Welche Rolle spielen dabei Resilienz, Schutz vor Cyberangriffen oder sogar Anschlägen auf die Schieneninfrastruktur?

Da reicht heute ein Blick in die Tagespresse, um zu erkennen, wie gefährdet die deutschen Verkehrsnetze und insbesondere das Bahnnetz sind. Wer eine IP-Adresse hat, ist per se angreifbar, und wir wissen, dass Deutschland bereits heute im Fokus hybrider Einflussnahme durch den Gegner steht. Auch wenn die Attribuierung häufig schwierig ist und meist nicht schnell gelingt,

ist uns aus der jüngeren Vergangenheit natürlich bekannt, dass Kabelbrände für uns relevante Strecken lahmlegen, Funkkameras in Oberleitungen Zugbewegungen wohin auch immer melden und Drohnenüberflüge über militärisch relevanten Bahnanlagen nicht nur durch eisenbahninteressierte Train-spotter erfolgen.

Ich weiß aber, dass hier die Deutsche Bahn zusammen mit Bundespolizei und Bundesamt für Sicherheit in der Informationstechnik als ihren etablierten Sicherheitspartnern hart an Schutz- und Überwachungsmaßnahmen arbeitet.

„Etwa 85 Prozent der Eisenbahntransporte der Bundeswehr sind lademaßüberschreitend.“

Die DB InfraGO ist ein KRITIS-Betreiber, der zunächst selbst für seinen Schutz sorgen muss. Und letztlich gibt es auch die Notverfahren, die greifen, wenn es hier zu Ausfällen kommen würde. Durch den mit Bezug auf den Schutz kritischer Infrastruktur zum Tragen kommenden Ansatz der „Gesamtverteidigung“ hat sich in den vergan-

BAAINBw

Das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr hat seinen Sitz in Koblenz. Die Behörde ist für die Entwicklung, Erprobung, Beschaffung und das Nutzungsmanagement von Wehrmaterial verantwortlich – vom Unterhemd bis zum Kampfpanzer. Sie ist 2012 als Zusammenführung des Bundesamts für Wehrtechnik und Beschaffung (BWB) mit dem IT-Amt der Bundeswehr entstanden. Das BAAINBw ist die zuständige Stelle für Vergabeverfahren bei der Bundeswehr:



<https://www.bundeswehr.de/de/organisation/ausruestung-baainbw/vergabe>

genen Jahren bereits vieles getan. Die relevanten Behörden sind deutlich enger zusammengedrückt.

Welche Rolle spielt Deutschland im europäischen Kontext militärischer Mobilität – eher Transitland, logistischer Hub oder beides?

Ich würde die beiden Begriffe nicht voneinander trennen. Als Logistiker muss ich die Verlegung von Menschen und Material im Blick haben. Ich muss mich aber auch ab dem ersten Tag, an dem unsere Truppe an der NATO-Ostflanke ist, um deren Versorgung kümmern.

Deutschland wird im Falle einer Aktivierung der NATO-Verteidigungspläne – und sei dies erst einmal nur zur Abschreckung – als Erstes Transitland für Verbündete, danach aber sicher auch so etwas wie die Operationsbasis beziehungsweise die Versorgungsbasis für vieles, was dann täglich oder regelmäßig an die NATO-Ostflanke geliefert werden muss. Sich alleine darauf zu verlassen, dass unsere Aufnahmeländer (Host Nations) aus ihrer eigenen Volkswirtschaft Bedarfe decken können, wäre blauäugig.

„Wir brauchen als Europäer einen gemeinsamen Plan, wie wir unsere Verkehrsinfrastruktur fit für die Herausforderungen der Zukunft machen.“

Ergeben sich aus den militärischen Anforderungen besondere technische Bedarfe an Wagenmaterial, Lokomotiven, Umschlaglösungen oder Innovationen, die Sie sich von der Bahnindustrie wünschen?

Ich denke, wir brauchen grundsätzlich nichts Außergewöhnliches, was es nicht schon gibt. Wir machen uns mehr Gedanken um die zeitliche Verfügbarkeit und die Mengen an Material, die wir benötigen. Wenn ich also an die Anzahl der Bundeswehr-eigenen Flachwagen denke, dann freue ich mich darüber, dass das BAAINBw gerade damit befasst ist, den Bestand zu erhöhen. Wenn wir vom Trassenabstand zwischen zwei



Waffensysteme werden schwerer und breiter und machen Lastgrenzen sowie Lichtraumprofile zur planerischen Herausforderung.

Gleisen reden, wäre es sinnvoll, gleich so zu planen, dass auch überbreite Transporte ohne aufwendige Überprüfungen bei Begegnungsverkehr fahren können. Und wenn ich an die Traktion denke, dann haben für uns leistungsfähige hybride Lokomotiven oder Dieselloks trotz aller notwendigen Berücksichtigung des CO₂-Ausstoßes unverändert eine hohe Bedeutung. Wir sehen in der Ukraine, welche Konsequenzen Angriffe auf die Energieversorgung haben, und auf Szenarien dieser Art müssen wir vorbereitet sein.

Aber darüber hinaus ist natürlich jede Innovation willkommen, durch die wir entweder Zeit gewinnen oder das Ausfallrisiko für Bahnkapazitäten verringern.

Wenn Sie auf die kommenden Jahre blicken: Was ist aus Ihrer Sicht die zentrale Voraussetzung, damit militärische Mobilität auf der Schiene in Deutschland und Europa langfristig verlässlich und sicher funktioniert?

Wir brauchen als Europäer einen gemeinsamen Plan, wie wir unsere Verkehrsinfrastruktur fit für die Herausforderungen der Zukunft machen. Verkehrsinfrastruktur ist ein klassisches Dual-Use-Objekt. Wir brauchen leistungsfähige Verkehrsnetze, um unsere

Wirtschaft weiter erfolgreich auf hohem Niveau halten zu können, um dadurch Kosten- und gegebenenfalls Zeitvorteile zu erlangen. Zugleich ist aber auch eine leistungsfähige, resiliente, weil redundante, Verkehrsinfrastruktur die Basis für unsere Verteidigungsfähigkeit. Investitionen in die europäische Verkehrsinfrastruktur sind daher zwingend erforderlich und müssen sowohl zivilen als auch militärischen Zwecken dienen. Ich gehe davon aus, dass mit dem derzeit in Vorbereitung befindlichen neuen EU Military Mobility Package, das nicht nur die Verkehrsinfrastruktur im Fokus hat, den militärischen Bedarfen Rechnung getragen wird.

Aus meinen Gesprächen mit EVU weiß ich, dass Bundeswehr und EVU bei der militärischen Mobilität die gleichen Ziele verfolgen. Wir dürfen nicht mehr über Rückbau reden, sondern wir müssen den Ausbau voranbringen. Effektivität auch in der Krise ist eine bestimmende Forderung der Streitkräfte. Die Eisenbahn spielt dabei eine ganz zentrale Rolle.

Sehr geehrter Herr Oberst Just Winkler, vielen Dank für das Gespräch!

Die Fragen stellte
Christian Wiechel-Kramüller.



Die Schiene erhält wieder deutlich mehr militärische Bedeutung in Europa – dazu muss sie ausreichend finanziert werden.

CEF-Förderung

Vierfach überzeichnet

Moderne Kriegstaktiken wie Sabotage und Drohnenangriffe sowie geopolitische Spannungen erhöhen den Druck auf Europas Bahninfrastruktur. Die EU reagiert mit beschleunigten Investitionen und neuen Koordinierungsregeln. Für Infrastrukturbetreiber und Industrie entstehen daraus konkrete technische und operative Anforderungen.

Sabotageakte und militärische Angriffe verdeutlichen die strategische Bedeutung der Eisenbahn in Europa: Im Februar 2026 griffen polnische Sicherheitskräfte auf der Güterstrecke Stettin–Dorohusk ein, nachdem ein Verdächtiger die Handbremse eines Kesselwagens betätigt hatte. Die Strecke verbindet Westpolen mit der ukrainischen Grenze und gilt als zentrale Logistikachse. Bereits im November 2025 hatten Saboteure dort einen Sprengsatz gezündet. Parallel überwachen bis zu 10.000 Soldaten im Rahmen der polnischen Operation „Horyzont“ kritische Bahnstrecken. Auch in der Ukraine selbst sind Züge unmittelbares Ziel militärischer Angriffe: Ende Januar 2026 trafen russische Drohnen einen Personenzug in der Region Charkiw, fünf Menschen starben. Diese Vorfälle zeigen, dass die Schiene nicht nur zivile Infrastruktur ist, sondern Teil der sicherheitspolitischen Grundversorgung Europas. Entsprechend verschiebt sich der Fokus der europäischen Verkehrspolitik. Militärische Mobilität ist von einem langfristigen Infrastrukturthema

zu einer kurzfristigen operativen Priorität geworden.

Die Europäische Kommission stellte für militärische Mobilität im Rahmen der Fazilität „Connecting Europe“ (CEF) für den Zeitraum 2021 bis 2027 ursprünglich 1,7 Milliarden Euro bereit. Nach dem russischen Angriff auf die Ukraine im Februar 2022 wurde dieses Budget vollständig vorgezogen und bereits bis 2023 vergeben. Die hohe Priorität zeigt sich auch an der Überzeichnung der Förderaufrufe: Im letzten Call 2023 überstieg die beantragte Fördersumme das verfügbare Budget um das 4,7-Fache.

Ein erheblicher Anteil der Mittel floss in Schienenprojekte. Von insgesamt 95 geförderten militärischen Mobilitätsprojekten zwischen 2021 und 2023 hatten 45 einen Bahnbezug oder waren multimodal mit Schienenanteil. Rund 45 Prozent der Mittel entfielen direkt auf die Schiene. Deutschland erhielt mit etwa 270 Millionen Euro den größten Anteil der bahnbezogenen Fördermittel, während Polen die meisten Einzelprojekte verzeichnete.

Gefördert wurden vor allem Maßnahmen zur Anpassung bestehender Infrastruktur an militärische Anforderungen. Dazu zählen die Verstärkung von Brücken für höhere Achslasten, die Anpassung von Tunnelprofilen, der Ausbau von Gleisanlagen für längere und schwerere Züge sowie die Verbesserung von Hafenanbindungen. Diese Maßnahmen adressieren konkrete technische Einschränkungen, die den Transport militärischer Fahrzeuge bislang behindern.

Es braucht Finanzierung und Modernisierung

Verkehrsorganisationen wie der Verband europäischer Eisenbahnfahrzeugvermieter (AERRL), vertreten durch Generalsekretärin Carole Coune, fordern eine deutliche Aufstockung der europäischen Verkehrsinvestitionen. In einem offenen Brief verlangen 45 Organisationen ein CEF-Budget von mindestens 100 Milliarden Euro im nächsten Finanzrahmen. Neben Infrastrukturinvestitionen sehen sie insbesondere Finanzierungsbedarf für Digitalisierung und Interoperabilität, etwa durch ERTMS, FRMCS und die DAK. Diese Technologien verbessern nicht nur die betriebliche Effizienz, sondern auch die Fähigkeit, militärische Transporte schnell und grenzüberschreitend abzuwickeln.

dt

FOTO: BUNDESWEHR/MARCO DOROW

Allianz Deutsche Häfen

Wo der Nachschub ankommt

Die neue Allianz „Deutsche Häfen“ hat sich in Berlin vorgestellt. Sie fordert, See- und Binnenhäfen endlich als strategische Infrastruktur von nationaler Bedeutung zu finanzieren – und fordert Bundesmittel.

Mit einer Veranstaltung in der Landesvertretung Hamburg in Berlin hat die neue Allianz „Deutsche Häfen“ im Juni 2026 ein deutliches Signal an die Bundespolitik gesendet. Im Fokus stand die Rolle der Hafeninfrastruktur für Energieversorgung und sicherheitspolitische Handlungsfähigkeit.

Rund 140 Gäste aus Politik, Verwaltung, Wirtschaft und Wissenschaft folgten der Einladung, um über die Herausforderungen und Perspektiven der deutschen Häfen im Spannungsfeld von Energiekrise, globalen Lieferketten und veränderten sicherheitspolitischen Rahmenbedingungen zu diskutieren. Einigkeit bestand laut Allianz darüber, dass die Wettbewerbsfähigkeit und Resilienz der Häfen nur mit klaren politischen Weichenstellungen und verlässlichen Finanzierungsstrukturen langfristig gesichert werden könnten.

Zum Einstieg machte Melanie Leonhard, Senatorin für Wirtschaft, Arbeit und Innovation der Freien und Hansestadt Hamburg; eines klar: „Die Aussage ‚No Shipping, no Shopping‘ bringt es auf den Punkt – unsere Häfen sind Voraussetzung unserer strategischen Autonomie und ökonomischen Sicherheit und gehören ganz klar in den bundespolitischen Fokus.“

Die Paneldiskussionen mit Vertretern aus Politik, Wirtschaft, Bundeswehr und Energiewirtschaft machten deutlich, dass Häfen heute weit mehr sind als klassische Umschlagplätze. Sie sind zentrale Knotenpunkte der Energiewende und zugleich unverzichtbare logistische Drehkreuze für die Sicherheits- und Verteidigungsarchitektur Deutschlands. Für die Schiene ist das unmittelbar relevant: Militärisches Gerät, das über See ankommt, wird im Hafen auf Bahn oder Straße umgeschlagen. Die Gleisanbindung der Terminals entscheidet damit mit darüber, wie schnell Verlegungen Richtung Ostflanke anlaufen können. Wie eng die Zukunft der Industrie an eine funktionierende Logistik gekoppelt ist, verdeutlichte Christian Bruch, Vorstandsvorsitzender Siemens Energy AG: „Wenn Unternehmen weiter in Deutschland investieren sollen, brauchen wir Investitionen in die Hafeninfrastruktur. Denn ohne Häfen exportieren wir nichts.“

Für die „Deutschen Häfen“ unterstrich Lars Nennhaus, Vorstand Technik und Betrieb Duisburger Hafen AG, die partnerschaftliche Abhängigkeit zwischen Wirtschaft und Häfen: „Wir funktionieren nur gemeinsam. Stottert ein Hafen, stottert die Volkswirtschaft.“

Aus militärischer Sicht wurde die fundamentale Bedeutung der Häfen ebenfalls untermauert. Oberst i. G. Armin Schaus, Abteilungsleiter „Zivil-militärische Zusammenarbeit“ im operativen Führungskommando der Bundeswehr: „Wirtschaft muss auch in der Krise funktionieren. Die Häfen sind dabei zentral.“ Damit rücken die Häfen in dieselbe Debatte wie das Militärische Eisenbahngrundnetz: Beide sind zusammen zu denken.

Vor diesem Hintergrund bekräftigte die Allianz „Deutsche Häfen“ ihren Appell, die See- und Binnenhäfen als strategische Infrastruktur von nationaler Bedeutung anzuerkennen und entsprechend angemessen zu finanzieren.

Unterstützung für diese Forderung kam aus den Reihen der Politik von Christoph Ploß, Koordinator der Bundesregierung für Maritime Wirtschaft und Tourismus: „Wir brauchen dringend mehr Investitionen in die deutschen Häfen, weil für uns als Exportnation viel davon abhängt. Dazu gehört auch eine Flexibilisierung beim Sondervermögen.“

Das Credo der Vertreter der Allianz war eindeutig: „Die Bedeutung der Häfen für Deutschland steht in keinem Verhältnis zur bisherigen Beteiligung des Bundes an ihrer Finanzierung. Wer von leistungsfähigen Häfen profitiert, muss sich auch an ihrer Zukunftssicherung beteiligen.“ ■

FOTO: DEUTSCHE HÄFEN



Gelungene Auftaktveranstaltung: Die enorme wirtschaftliche wie strategische Bedeutung der deutschen Häfen wurde in Berlin betont.



Schwere Militärtransporte auf der Schiene: Nur die Bahn kann große Mengen Gerät und Material schnell und effizient verlegen.

Militärisches Eisenbahngrundnetz sichern

Was „kriegstüchtig“ für die Schiene eigentlich bedeutet

Nicole Knapp, bei erstmaligem Erscheinen dieses Beitrages VDV-Geschäftsführerin Eisenbahnverkehr, zeigt, dass die militärische Einsatzfähigkeit der Schiene zur gesamtstaatlichen Aufgabe werden muss, und fordert ein Militärisches Eisenbahngrundnetz. Nur mit Investitionen und der Einbindung privater Bahnen könne die Schiene ihre sicherheitspolitische Rolle erfüllen.

Dieser Beitrag erschien erstmals in **Privatbahn Magazin 5/2025**. Er dokumentiert den damaligen Stand der Debatte.

Die sicherheitspolitische Lage in Europa hat sich in den vergangenen Jahren grundlegend verändert. Angesichts neuer geopolitischer Spannungen und der gestiegenen Anforderungen an nationale und europäische Verteidigungsfähigkeit rückt ein bislang weitgehend verdrängtes Thema wieder in den Vordergrund: die militärische Einsatzfähigkeit der Schiene. „Kriegstüchtig“ – so hat es der Bundesverteidigungsminister formuliert – muss auch die Verkehrsinfrastruktur künftig wieder bedacht werden. Jahrzehntelanger Rückbau in Friedenszeiten hat Lücken in der Infrastruktur, beim rollenden Material und in der organisatorischen Abstimmung hinterlassen. Die Eisenbahn muss jetzt wieder in die Lage versetzt werden, in Krisen- und Konfliktfällen verlässlich

zu funktionieren – national wie international.

Schiene als strategisches Rückgrat

Die strategische Bedeutung der Eisenbahn für militärische Mobilität ist unbestritten. Schweres Gerät, große Truppenverbände und Gefahrgut lassen sich über keine andere Verkehrsform zugleich so schnell, effizient und flächendeckend verlegen wie über die Schiene. Die aktuellen Entwicklungen innerhalb der NATO und der Europäischen Union – insbesondere die strategischen Pläne für sogenannte Militärkorridore – zeigen: Militärische Bewegungen müssen auch unter Zeitdruck plan- und steuerbar sein. Das bedeutet konkret: Engstellen im Netz, insbesondere bei

Brücken, Tunneln und Grenzübergängen, müssen beseitigt, zusätzliche Kapazitäten geschaffen und spezielle Anforderungen des militärischen Transports berücksichtigt werden.

Voraussetzung: Militärisches Eisenbahngrundnetz

In diesem Kontext ist die Einrichtung eines Militärischen Eisenbahngrundnetzes (MEGN) ein entscheidender Schritt. Dieses Netz stellt das schienenseitige Pendant zum bereits existierenden Militärischen Straßennetz (MSGN) dar und ist Voraussetzung für die operative Umsetzung nationaler und internationaler Verteidigungspläne wie des „Operationsplans Deutschland“. Infrastrukturelle Engpässe werden derzeit in einer bundesweiten Analyse syste-

FOTOS: BUNDESWEHR/FLORIAN KRUTH (2); DEUTSCHE BAHN AG/GEORG WAGNER; VDV/OLIVER LANG

matisch identifiziert. Die Ergebnisse sollen in ein gezieltes Maßnahmenpaket zur Ertüchtigung münden – sowohl im Bestandsnetz als auch bei den rollenden Kapazitäten. Wichtig dabei ist: Ein MEGN darf nicht nur national, sondern muss unbedingt grenzüberschreitend gedacht und abgestimmt werden.

Betriebliche Einsatzfähigkeit muss gesichert sein

Auch auf der betrieblichen Seite sind grundlegende Voraussetzungen zu schaffen. Militärische Transporte lassen sich nicht kurzfristig aus dem Regelbetrieb ableiten – sie erfordern vorbereitete Logistikketten, geschultes Personal, spezifisch ausgestattetes Wagenmaterial und gegebenenfalls Sicherheitsvorkehrungen für Begleitwagen und Gefahrguttransporte. Eine rein zivile Optimierungslogik – orientiert an Wirtschaftlichkeit und Auslastung – greift hier zu kurz. Erforderlich ist stattdessen die strategische und langfristige Vorhaltung militärisch nutzbarer Ressourcen, die im Krisenfall sofort verfügbar sind. Das muss sich auch in Wirtschaftlichkeitsuntersuchungen und Förderkulissen gerade für die nicht-bundeseigenen Eisenbahnen niederschlagen.

Privatbahnen sind unverzichtbare Partner

Das Militärische bedingt das Zivile und andersherum: Dabei kommt den privaten Eisenbahnunternehmen eine wichtige Rolle zu. Bereits heute sichern sie – neben dem bundeseigenen Güterverkehr – einen wesentlichen Teil der logistischen Leistungsfähigkeit auf der Schiene ab. Mit einem Marktanteil von rund 50 Prozent im Schienengüterverkehr tragen sie erheblich zur Resilienz und Kapazität bei, insbesondere im Einzelwagenverkehr, der für mittelständische Industrie und kurzfristige militärische Anforderungen gleichermaßen essenziell ist.

Dabei geht es nicht nur um schwere Technik wie Panzer, sondern auch um Versorgungstransporte aller Art – von Munition über Kraftstoffe bis hin zu



Nicole Knapp

leitet seit Januar 2026 bei der DB InfraGO AG den Bereich Transformation und Kundenstrategie. Zuvor war sie Geschäftsführerin Eisenbahnverkehr beim Verband Deutscher Verkehrsunternehmen (VDV). Sie verfügt über umfangreiche und langjährige Erfahrungen im Eisenbahnsektor, sowohl im Personenverkehr als auch bei der Infrastruktur. Vor ihrem Posten beim VDV war sie zwölf Jahre im

DB-Konzern tätig, unter anderem als Leiterin Kommunikation für DB Fernverkehr. Insgesamt blickt sie auf rund 16 Jahre Berufserfahrung im Eisenbahnsektor zurück. Knapp ist Diplom-Kommunikationswirtin und Fachwirtin für Immobilien. Vor ihrem ersten Einstieg bei der Deutschen Bahn war sie unter anderem für das SPNV-Unternehmen Netinera und den Verband der Bahnindustrie in Deutschland (VDB) tätig.

„Wer von der Eisenbahn erwartet, dass sie im Krisenfall funktioniert, muss heute investieren.“

Nicole Knapp

Verpflegung und medizinischem Material.

Für die gesamte Branche bedeutet das: Die Verfügbarkeit militärischer Mobilität wird zu einem dauerhaften Anwendungsfall, der mitgedacht, eingeplant und vorgehalten werden muss – in Betrieb, Fahrzeugkonzepten, Personalstrategien und Instandhaltung. Und für die Politik ergibt sich daraus eine klare Verantwortung. Die notwendigen Investitionen in Infrastruktur und Betriebsmittel sind nicht allein Sache der Infra-

struktur- oder Verkehrsunternehmen – sie sind eine gesamtstaatliche Aufgabe, die im Sinne der nationalen Sicherheitsvorsorge geleistet werden muss.

Koalitionsvertrag: „Mehr Güter auf die Schiene“

Dass es dafür einer zusätzlichen Finanzierung bedarf, zeigt ein Blick in die aktuellen Zahlen des VDV für das Jahr 2023: Die verbandseigenen Mitgliedsunternehmen haben 2023 rund 290 Millionen Tonnen Güter klimafreundlich auf der Schiene transportiert. Dies entspricht einem Marktanteil von etwa 19 Prozent am gesamten Güterverkehr in Deutschland. Ziel der letzten Bundesregierungen war ein Anstieg auf 25 Prozent bis 2030, dies entspricht der Zahl aus dem Masterplan Schienengüterverkehr. Im aktuellen Koalitions-



Rheinquerungen wie diese zweigleisige Eisenbahnbrücke bei Duisburg gelten als neuralgische Punkte im Netz: Sie entscheiden mit, ob militärische Verkehre funktionieren.

vertrag heißt es schlicht: „Wir wollen mehr Güterverkehr von der Straße auf die Schiene verlagern.“ Ohne gezielte Investitionen in Infrastruktur, Digitalisierung und rollendes Material wird dieses Ziel ebenso wenig erreichbar sein wie eine verlässliche militärische Verladekette. Auch 740-Meter-Züge, die die Effizienz steigern könnten, scheitern bislang an mangelnden Voraussetzungen auf vielen Strecken. Aber welche Rolle spielen die Privaten bei diesem strategischen Thema? Das deutsche Schienennetz umfasst insgesamt rund 38.400 Kilometer. Davon entfallen etwa 33.400 Kilometer auf das Streckennetz der bundeseigenen DB InfraGO AG, während rund 5000 Kilometer von den nichtbundeseigenen Eisenbahnen betrieben werden [Anm. d. Red.: Diese Zahlen beziehen sich auf Streckenkilometer]. Diese Struktur verdeutlicht die hohe Relevanz der NE-Bahnen, auch im Hinblick auf militärische Anforderungen, die eine flächendeckende Netzverfügbarkeit voraussetzen. Die privaten Unternehmen sind bereit, ihre Kapazitäten für militärische

Anforderungen zur Verfügung zu stellen – doch auch sie brauchen Planungssicherheit, Zugang zu Fördermitteln, faire Trassenpreise und eine Einbindung in die strategische Gesamtplanung. Das Sondervermögen Infrastruktur und Klimaneutralität (SVIKG) in Höhe von 500 Milliarden Euro darf daher kein exklusives Instrument für bundeseigene Akteure sein. Gerade in diesem sicherheitsrelevanten Sektor ist die Einbindung aller Systempartner notwendig.

Finanzierung sicherstellen

Der Finanzierungsbedarf für Sicherstellung militärischer Mobilität ist erheblich und kann nicht aus den Finanzierungslinien für die zivile Nutzung des Schienennetzes mitgetragen werden. Für die Umsetzung der militärischen Anforderungen auf der Schiene müssen daher zusätzliche Mittel bereitgestellt werden – für das MEGN, für Spezialfahrzeuge, für Sicherheitsmaßnahmen, für Ausrüstung und Personal. Eine Finanzierung über den Einzelplan des Verteidigungshaushalts bietet sich an: Sie ist nicht gedeckelt, kann auf die

NATO-Quote angerechnet werden und entlastet gleichzeitig andere haushaltspolitisch stark beanspruchte Sondervermögen, etwa für die Infrastrukturfinanzierung im zivilen Bereich.

Gerade mit dem neuen Ziel, künftig fünf Prozent des Bruttoinlandsprodukts für Verteidigungsvorsorge zu mobilisieren – davon 1,5 Prozent für verteidigungsrelevante Infrastruktur –, sollten auch kritische Infrastrukturen wie das militärisch ertüchtigte Schienennetz mitgedacht und einbezogen werden. Klar ist: Wer von der Eisenbahn erwartet, dass sie im Krisenfall funktioniert, muss heute investieren. Die militärische Einsatzfähigkeit der Schiene ist keine abstrakte Vorsorgedebatte – sie ist eine konkrete, operative Herausforderung. Die Branche ist bereit, ihren Beitrag zu leisten. Doch dies gelingt nur gemeinsam – mit bundeseigenen und privaten Bahnen als gleichberechtigten Partnern einer resilienten Sicherheitsarchitektur. Denn Sicherheit beginnt im Fahrplan – und der muss künftig auch im Ausnahmefall halten.

Nicole Knapp



Einsatzvorbereitung auf dem Gleis: Soldaten sichern das verladene Gerät, denn ohne die richtige Logistik gehen Kriege verloren.

Rahmenabkommen in Polen

Absichtserklärung mit Lücken

Mit einem Rahmenabkommen ohne Finanzverpflichtungen macht Polen seine Bahninfrastruktur resilient: PKP Cargo stellt Terminals, Anschlussgleise und Diesellokomotiven für den Ernstfall bereit. Über 70 Prozent des Marktes liegen jedoch bei Wettbewerbern, die außen vor bleiben.

Polens Verteidigungsministerium (MON) und die in Restrukturierung befindliche PKP Cargo S.A. haben im Mai 2026 in Warschau ein Rahmenabkommen zur Zusammenarbeit im militärischen Schienengütertransport unterzeichnet. An der feierlichen Unterzeichnung nahmen der stellvertretende Ministerpräsident und Verteidigungsminister Władysław Kosiniak-Kamysz sowie Infrastrukturminister Dariusz Klimczak teil.

Im Zentrum der Vereinbarung steht das Prinzip der doppelten Nutzung: Schieneninfrastruktur und Fahrzeuge sollen im Frieden kommerziell genutzt werden, im Krisenfall, bei erhöhter Verteidigungsbereitschaft oder im Kriegsfall jedoch unmittelbar für die polnischen Streitkräfte zur Verfügung stehen. Konkret geht es laut PKP Cargo um Terminal- und Anschlussgleisinfrastruktur, Traktionsressourcen – darunter Lokomotiven für nichtelektrifizierte Strecken – sowie um Sicherheits- und Kommunikationslösungen des Unternehmens.

Kosiniak-Kamysz ordnete das Abkommen in den Kontext der NATO- und EU-Debatte um „militärische Mobilität“ ein und verwies auf bereits bestehende Vereinbarungen mit Deutschland und den Niederlanden zur reibungslosen Truppenverlegung sowie auf die wachsende Bedeutung der Ostseeregion für die europäische Sicherheitsarchitektur.

Wichtig für die Einordnung: Das Abkommen ist auf unbestimmte Zeit geschlossen, mit einer Kündigungsfrist von drei Monaten, und begründet nach übereinstimmenden Angaben mehrerer polnischer Medien und der Börsenmitteilung von PKP Cargo keine unmittelbaren finanziellen Verpflichtungen und

keine Pflicht zum Abschluss konkreter Ausführungsverträge. Einzelne Projekte und Abrechnungen sollen Gegenstand gesonderter Vereinbarungen sein. Es handelt sich also – trotz der symbolträchtigen Inszenierung – zunächst um eine Absichtserklärung, nicht um einen Beschaffungs- oder Dienstleistungsvertrag mit bezifferten Volumina.

PKP-Cargo-Vorstandschef Zbigniew Prus verwies laut Unternehmensangaben auf die Stellung des Konzerns als größter polnischer und zweitgrößter europäischer Güterbahnbetreiber sowie auf eine bereits langjährige Zusammenarbeit mit den Streitkräften im Transport- und Logistikbereich.

Marktanteil und NATO-Zielvorgaben

Diese Angaben sind teils fraglich, befindet sich PKP Cargo doch seit 2024 in einem gerichtlichen Sanierungsver-

fahren, und nach übereinstimmenden Medienberichten kontrolliert das Unternehmen nur noch einen kleinen Teil des polnischen Schienengüterverkehrsmarkts. Demnach liegt der Marktanteil konkurrierender Bahnen inzwischen bei über 70 Prozent.

Auf die Journalistenfrage, ob das Abkommen allein ausreiche, um die polnischen Zusagen aus dem NATO-Gipfel von Madrid (2022) zur Verlegungsfähigkeit von Truppen zu erfüllen, blieb Vizepremier Kosiniak-Kamysz bei der Pressekonferenz eine klare Antwort schuldig. Ob und wie andere Bahnbetreiber in vergleichbare Verpflichtungen eingebunden werden, ließen Regierungsvertreter offen.

Das Abkommen reiht sich damit in eine Serie europäischer Initiativen zur militärischen Mobilität ein und unterstreicht die zunehmende sicherheitspolitische Bedeutung ziviler Schieneninfrastruktur. Interessant ist hier aber besonders der Ansatz, explizit auf dual-use-fähige Infrastruktur und Rollmaterial für nichtelektrifizierte Strecken zu setzen. ■



Polen will künftig auf das Dual-Use-Prinzip in Schienenfragen setzen. Ein Konzept, das als Blaupause innerhalb der NATO dienen könnte.



Ein Bergepanzer schluckt 600 Liter auf 100 Kilometer – Transport auf der Schiene ist im Verteidigungsfall unabdingbar.

Österreichs Bundesheer und die Bahn

30 Jahre Funkstille beenden

Rampen abgebaut, Übungen eingestellt, Rüstungsfabriken geschlossen – Brigadier Andreas Stupka zeichnete beim Forum Verkehr in Wien ein ernüchterndes Bild der militärischen Bahnlogistik in Österreich. Sein Appell: Das Bundesheer und die Eisenbahn müssen dringend wieder zusammenfinden.

Auch in Österreich wird die Verbindung zwischen Heer und Eisenbahn stärker zum Thema. Das zeigte sich auch daran, dass zum vom Veranstaltungsinstitut imh in Wien abgehaltenen Forum Verkehr ein hoher Offizier des Österreichischen Bundesheeres als Referent eingeladen worden war, und am großen Interesse des Fachpublikums nach dessen Vortrag.

Brigadier (Brigadegeneral) Andreas Stupka, zuständig für die logistische Bereitstellung im Bundesheer, bezeichnete die Schiene als strategische Lebensader in Europa. Vieles an militärischem Personal und an Heeresgütern werde durch einzelne Länder geschleust. Dies gelte insbesondere für Österreich: „Wir müssen, wenn wir uns verteidigen wollen, im Ausland einkaufen, weil wir unsere Rüstungs- und

Munitionsfabriken geschlossen haben“, sagte Stupka.

Hinzu kommt die Entfremdung zwischen Bahn und Armee in der jüngsten Vergangenheit, als allgemein angenommen wurde, Europa werde künftig nicht mehr von Kriegen betroffen sein: „Wir haben in den letzten 30, 40 Jahren viele Rampen abgebaut“, klagte der Logistik-Offizier. 1991 habe die Zusammenarbeit anlässlich der Jugoslawienkrise noch hervorragend geklappt. „Aber 31 Jahre lang wurde das nicht geübt, das müssen wir jetzt wieder aktivieren“, sagte Stupka.

Gleichzeitig warnte der Offizier, dass die Bevölkerung den Frieden inzwischen als Normalzustand betrachte, der Krieg aber immer der „steinerne Gast“ in der Menschheitsgeschichte sei. Stupka nannte drei strategische Dreh-

scheiben, auf die Österreichs Verteidigung ihr Augenmerk legen müsse: das Wiener Becken, das Eferdinger Becken westlich von Linz und die Mur-Mürz-Furche mit dem Grazer Becken. Die Drohne habe das Kriegsbild in den letzten drei Jahren so fundamental verändert wie der Panzer im Gefolge des Ersten Weltkriegs oder die Eisenbahn im 19. Jahrhundert. Da helfe Österreich auch seine Neutralität nichts: „Wenn man zeigen will, dass man mitten in die NATO ohne Gegenwehr schießen kann, dann nimmt man sich die Schweiz oder Österreich“, sagte Stupka.

Eisenbahner in die Miliz?

Deshalb regte er eine intensive Zusammenarbeit zwischen Heer und Bahn an. Jedoch: „Wir können keine Truppen zum Schutz von Gleisanlagen abstellen, das muss die Bahn als Werkschutz machen. Es wäre wichtig, das Bahnpersonal militärisch auszubilden, weil es im Ernstfall ein Ziel sein könnte.“ Denkbar wäre es nach Stupkas Meinung, Bahnbedienstete nach absolvier-

FOTOS: R888 VIA CC-BY-SA 3.0; MAY

tem Wehrdienst in der Miliz nicht für den Kampfeinsatz, sondern bei der Bahn zu verpflichten.

Im Ernstfall werde bei der Eisenbahn nicht mehr alles funktionieren, sagte Stupka. Deshalb sei das Ziel im Sinn von Autarkie Low-Tech – nur so viel Technik wie nötig. Darum auch müssten Diesellokomotiven vorgehalten werden. „Anzustreben wären gemeinsame Übungen mit der Bahn“, schlug der Heeres-Logistiker vor.

100 Tonnen pro Tag

Anhand von Beispielen demonstrierte Stupka, welche enormen Mengen im Verteidigungsfall durch das Militär auf der Schiene bewegt werden müssten: So habe etwa ein Bergepanzer einen Verbrauch von rund 600 Litern Kraftstoff auf 100 Kilometern. Die Eisenbahn sei deshalb unabdingbar für den Transport von militärischem Material. Der Truppenaufmarsch mit Fahrzeugen und schwerem Gerät betreffe Nach- und Abschub, Munition, Verpflegung, Verwundete und Personen insgesamt. Eine Brigade mit 5.000 Soldaten und 900 Kraftfahrzeugen brauche 100 Tonnen Munition pro Tag. Gewichtsmäßig bedeute das: Eine Granate sei 50 Kilogramm schwer. Ein Container mit 30 Paletten zu je acht Granaten wiege 13 Tonnen. Der Drohnenverbrauch liege im Ukrainekrieg bei 10.000 bis 15.000 Stück pro Monat auf jeder Seite. Russland schiebe 3.000 Tonnen Munition pro Tag nach. Bei der kämpfenden Truppe sei mit 15 bis 25 Prozent Ausfällen zu rechnen, davon 25 Prozent Toten. Fünf Prozent würden aufgrund der Kampfeinwirkungen aus psychischen Gründen nicht mehr verwendbar, 25 Prozent würden schwer verwundet. Sie alle müssten hinter die Front zurückgebracht werden.

Umschlagen im Tunnel

Wichtig ist laut Stupka ein verdeckter Aufmarsch, also der Transport von militärischem Gerät in gedeckten Güterwagen. Die Oberleitung helfe gegen Drohnen, weil diese sich darin verfangen. Eisenbahntunnels seien wichtig: „Sie sollten so ausgebaut sein, dass man drinnen verdeckt umschlagen kann“,



Brigadier Andreas Stupka, zuständig für Heereslogistik, fordert gemeinsame Übungen von Bundesheer und Bahn – und eine militärische Ausbildung für Bahnpersonal.

sagte Stupka. „Anzudenken wären Gefechtsstandzüge. Die Schweiz hat das zum Teil.“ Das Fazit des hohen Bundesheeroffiziers: „In weiten Bereichen sind

wir derzeit dabei, auf beiden Seiten wieder zu lernen. Wir brauchen ein schnelles Zusammenwachsen zwischen Heer und Bahn.“ *Stefan May*



Panzer und Co. sind schweres Gerät – wortwörtlich. Die Schiene eignet sich hervorragend für ihren Transport. Ein guter Zugang zum Schienennetz ist ein wesentlicher Faktor in der militärischen Logistik. Hier gibt es in Deutschland Handlungsbedarf.

Standortanalyse

Nur 10 Kasernen mit Gleisanschluss

Für die militärische Logistik spielt die Eisenbahn schon seit dem 19. Jahrhundert eine entscheidende Rolle. Der Ukraine-Krieg zeigt, dass dies heute immer noch gilt. Dieser Artikel beleuchtet, inwieweit das deutsche Bahnsystem militärische Transporte ermöglicht.

Rollende Züge mit Panzern, Güterwagen voller Militärgerät – seit dem Beginn des russischen Aufmarschs Ende des Jahres 2021 sind diese Bilder keine Seltenheit in den sozialen Medien. In Deutschland gab es solche Bilder in der Vergangenheit auch, sie waren jedoch vor allem für Experten und Technikliebhaber von Interesse.

Dabei ist die Eisenbahn auch für die Bundeswehr und ihre Verbündeten innerhalb und außerhalb der NATO ein wichtiger Verkehrsträger: Militärische Fahrzeuge müssen an ihren Bestimmungsort kommen, was vor allem bei Kettenfahrzeugen selten „im Landmarsch“ passiert. Je größer die Distanz und je höher die Anzahl, desto vorteilhafter ist ein Transport mit der Bahn. Anlässe für solche Transporte bieten primär Manöver. Die Zahl innerdeutscher Transporte überwiegt dabei deutlich. Regelmäßig werden daneben im Rahmen rotierender Kontingente bei Auslandseinsätzen, zum Beispiel in Litauen, Fahrzeuge und Material mit der Bahn transportiert. Dies ist der eingeschliffene Regelbetrieb.

Auch wenn alle die Bilder des Ukraine-Kriegs vor Augen haben: Das Schreckensszenario „Verteidigungsfall“ (Artikel 115a GG) ist seit dem 24. Februar 2022 kaum wahrscheinlicher geworden – beim Szenario „Bündnisfall“ (Artikel 80a GG) ist man sich aber schon weniger sicher. Es lohnt sich daher, darüber nachzudenken, inwieweit das deutsche Bahnsystem militärische Transporte – auch im Ernstfall – ermöglicht.

Standorte

Das Heer als Landstreitmacht steht bei dieser Betrachtung im Mittelpunkt, ist aber in der Struktur der Bundeswehr nicht der einzige relevante Bereich: Organisiert werden alle Transporte seit 2000 von der Streitkräftebasis, einem übergreifenden Dienstleistungsbereich. Das Heer befindet sich hier in einer Art Kundenfunktion.

Bedeutende Heeresstandorte sind zum Beispiel die Generalfeldmarschall-Rommel-Kaserne in Augustdorf bei Detmold oder die Kyffhäuser-Kaserne in Bad Frankenhausen (Thüringen). Für eine umfassende Betrachtung – die

Gekürzter Nachdruck aus **Privatbahn Magazin 4/2022**. Der Beitrag dokumentiert den damaligen Stand der Debatte, die Langfassung steht im Archiv der PriMa-App.

Bundeswehr ist eine Bündnisarmee – sind auch Standorte Verbündeter wie die Rose Barracks (Grafenwöhr in Nordbayern) relevant.

Legen die Transportplaner der Bundeswehr die Standorte und das deutsche Eisenbahnnetz übereinander, so ergibt sich das Bild einer Armee, die in geringerem Maße als beispielsweise Russland oder auch die Vereinigten Staaten auf den Verkehrsträger Eisenbahn setzt. Nur zehn der betrachteten 45 aktiven Standorte verfügen über einen eigenen Gleisanschluss – also Bahngleise, die direkt auf das Kasernengelände führen. Die meisten Standorte müssen auf Verlademöglichkeiten in ein bis drei Kilometern Entfernung zurückgreifen – nah, aber eben nur über öffentliche Straßen erreichbar. Bei einigen Standorten müssen sogar über zehn Kilometer zurückgelegt werden, ehe eine nutzbare Verlademöglichkeit erreicht ist. Früher verfügten viele Kasernen zwar ebenfalls nicht über eigene Gleisanlagen; das dichtere Streckennetz, eine

FOTOS: BUNDESWEHR/PAO EFF, MAURICE FATEIGER

deutlich größere Zahl an gewerblichen Gleisanschlüssen und viele Ladestraßen/-rampen auch in kleinen Bahnhöfen machten die Logistik aber deutlich flexibler.

Jedoch war früher auch die militärische Ausgangslage eine andere: Die Bundeswehrstandorte lagen zur Zeit des Kalten Krieges – mehr oder weniger – direkt in der potenziellen Kampfzone. Dies ist heute zum Glück anders, erzeugt aber eben einen anderen Transportbedarf – einerseits größer aufgrund wachsender Distanzen, andererseits kleiner wegen weitaus geringerer Stückzahlen.

Beispiel: Verfügte die Bundeswehr 1985 noch über mehr als 4600 Kampfpanzer, waren es 2014 gerade noch 225, also eine Schrumpfung um über 95 Prozent. Nach der Krim-Annexion wurde 2015 ein Aufwuchs auf 320 Kampfpanzer beschlossen.

Military Mobility

Eine erweiterte Analyse der Bahnanbindung der Heeresstandorte zeigt, dass die Mehrzahl nur an eine Strecke (und nicht an Knoten im Bahnnetz) angebunden ist. Immerhin zehn Standorte liegen sogar nur an – eingleisigen – Stichstrecken, was die Anbindung besonders störanfällig macht.

Wie angedeutet, werden Verlegungen im Krisenfall regelmäßig zu internationalen Zugverbindungen führen, womit man schnell vor dem Problem der (mangelhaften) Interoperabilität im europäischen Bahnverkehr steht. Hilfreich wäre da ein möglichst direkter Anschluss an eine Strecke des Trans-europäischen Netzes beziehungsweise idealerweise an einen der Güterverkehrskorridore. Dies trifft jedoch nur auf deutlich weniger als die Hälfte der Standorte zu. Dies kommt wenig überraschend, da sich nicht wenige Standorte in eher strukturschwachen Gebieten, zum Beispiel in der Oberpfalz oder Mitteldeutschland, befinden.

Doch auch bei einem direkten Anschluss an einen Güterverkehrskorridor bleiben internationale Militärverkehre eine Herausforderung. Die EU versucht seit 2018, die „Military Mobility“ auf dem Kontinent zu verbessern, vor al-

lem durch die Reduzierung bürokratischer Hemmnisse. Daneben wird schon lange an einer Verbesserung der allgemeinen technischen und betrieblichen Interoperabilität des Sektors gearbeitet, die Technischen Spezifikationen für Interoperabilität (TSI) geben hier den normativen Rahmen vor. Von einer schnellen Realisierung würden (nicht nur) Militärtransporte besonders profitieren.

Traktion und weitere Parameter

Gerade Kampfpanzer sind mit bis zu 75 Tonnen buchstäblich Schwergewichte, die westlichen Modelle noch deutlich mehr als jene russischer/sowjetischer Bauart. Jedoch verfügen die betrachteten Strecken überwiegend über die Streckenklasse D4, was hinsichtlich Radsatz- und Meterlast unproblematisch ist, angesichts der meistverwendeten vierachsigen Flachwagen zum Beispiel der Bauart Rlmmms. Bei niedrigeren Streckenklassen müssen gegebenenfalls sechssachsige Wagen eingesetzt werden.

Komplizierter sind die Abmessungen der Fahrzeuge: Obgleich unproblematisch in der Höhe, führen Militärfahrzeuge durch ihre Breite regelmäßig zu Lademaßüberschreitungen. Dies gilt für Schützenpanzer wie den Puma noch



Philipp Schneider
hat bis 2021 an der TU Berlin unter anderem zur Resilienz von Eisenbahnen geforscht, 2022 angestellt bei der DB Netz AG.

mehr als für Kampfpanzer. Nichtsdestotrotz setzt die Bahn-Transportierbarkeit seit jeher schon in der Konstruktionsphase eines Militärfahrzeugs das Limit bei den Abmessungen.

Sei es zur Evakuierung von Menschen, zur Versorgung mit zivilen oder militärischen Gütern oder zum Export von Getreide: Der Ukraine-Krieg verdeutlicht die Bedeutung der Eisenbahn als kaum zu ersetzende, kritische Infrastruktur. Deutschland kann hieraus Lehren ziehen – für den Sektor als Ganzes, aber auch für eine gute militärische Nutzbarkeit des Systems.

Philipp Schneider



Der Transport von Militärtechnik ist strategisch wichtig: Auch Gerät wie der Brückenlegepanzer Leguan (hier ohne Brücke) wird per Bahn transportiert.



Drohnenüberflüge an kritischer Infrastruktur sind keine Seltenheit mehr. Im Interview rät Sicherheitsexpertin Verena Jackson dazu, sie im Verbund mit Sabotage und Cyberangriffen zu sehen.

Im Interview: Verena Jackson

Offenes System als Zielscheibe

Drohnen, Cyberangriffe, Sabotage: Bahninfrastruktur ist verwundbarer als lange angenommen. Sicherheitsexpertin Verena Jackson erklärt im Interview, warum hybride Bedrohungen integrierte Schutzkonzepte erfordern – und wo die Grenze zwischen privater Verantwortung und staatlicher Befugnis liegt.

Privatbahn Magazin: Die Eisenbahn gilt traditionell als robuste Infrastruktur – der Ukraine-Krieg zeigt jedoch, wie verletzlich offene Systeme gegenüber günstigen, flexibel einsetzbaren Drohnen und digitalen Angriffen sein können. Muss man Infrastruktur grundlegend anders denken und schützen als noch vor zehn oder zwanzig Jahren?

Verena Jackson: Ja, absolut. Die Bahninfrastruktur, die früher als robust galt, ist heute nicht mehr automatisch resilient. Sie ist ein offenes, weit verzweigtes System in der Fläche. Man kann nicht jeden Kilometer Gleis, jedes Stellwerk oder jede Oberleitung physisch schützen wie ein militärisches Objekt. Ein potenzieller Angreifer weiß das und macht sich das gezielt zunutze. Der Ukraine-Krieg und die aktuelle geopolitische Lage zeigen, dass gerade solche Infrastrukturen anfällig sind, wenn günstige Drohnen, Sabotage und Cyberangriffe zusammenkommen. Das bedeutet aber nicht, dass man die Eisenbahn „abschotten“ sollte, das ist auch gar nicht leistbar. Aber man muss insofern anders denken, als dass ein Be-

wusstsein für die veränderte Bedrohungslage vorhanden sein muss. Das heißt zum Beispiel: bessere Lagebilder, mehr Sensorik zur frühen Detektion von Gefahren, schnelle Meldewege, eingeübte Notfallkonzepte, Redundanzen und eine engere Verzahnung zwischen Betreiber und Sicherheitsbehörden. Offene Gesellschaften müssen ihre Offenheit nicht aufgeben. Aber sie müssen begreifen, dass Offenheit eben heute auch eine Verwundbarkeit darstellt, die aktiv gemanagt werden muss, sonst wird sie zur Zielscheibe.

Viele Diskussionen konzentrieren sich auf die Drohne selbst. Tatsächlich entstehen neue Risiken oft erst durch die Verbindung von Aufklärung, KI-gestützter Datenauswertung, Navigation und Cyberangriffen. Welche Bedeutung messen Sie dieser hybriden Kombination aus physischer und digitaler Verwundbarkeit bei?

Dieser Punkt ist der Knackpunkt der aktuellen Bedrohungslage, der hybriden Bedrohungslage. Die Drohne allein ist oft gar nicht das eigentliche Pro-

blem, solange sie nicht selbst zum Beispiel mit Sprengstoff beladen als Waffe eingesetzt wird. Eine Drohne kann aufklären, Bilder liefern, Bewegungsmuster erkennen, Schwachstellen an Infrastruktur dokumentieren oder Reaktionen von Sicherheitskräften testen. Das ist aber nur ein Stein im „Mosaik“ der hybriden Bedrohungslage, in der wir uns befinden.

„Man darf weder Drohnen-vorfälle noch Sabotage noch Cyberangriffe als Einzelfälle betrachten.“

Wenn die Informationen dann genutzt werden, um sie mit Cyberangriffen oder Sabotageakten zu kombinieren und tatsächlichen Schaden anzurichten, entsteht eine ganz andere Bedrohungsqualität. Man darf weder Drohnenfälle noch Sabotage noch Cyberangriffe als Einzelfälle betrachten. Leider scheitert die Realität bislang noch am Anspruch und es fehlt ein gutes Lagebild.

Diese Technologie entwickelt sich häufig außerhalb klassischer Sicherheits- und Beschaffungszyklen weiter. Haben Betreiber kritischer Infrastruktur überhaupt noch genügend Zeit, organisatorisch und technisch Schritt zu halten?

FOTOS: U.S. ARMY 153PAD BY PFC. AYDEN NORCROSS; PUBLIC DOMAIN, VIA WIKIMEDIA COMMONS; CISS

Ich glaube, das eigentliche Problem ist nicht nur das Tempo der Technologie, sondern die Asymmetrie dahinter. Wer Drohnen missbräuchlich einsetzen will, kann sehr schnell improvisieren, illegal umbauen und kombinieren. Betreiber kritischer Infrastruktur wie die Deutsche Bahn dagegen müssen planen, genehmigen (lassen), beschaffen, abstimmen und rechtssicher handeln. Das führt zu einem strukturellen Nachteil. Die Angriffsseite kann am Recht vorbei handeln, ist schnell und agil, und die Schutzseite muss reguliert reagieren. Genau deshalb reicht es nicht, nur einzelne neue Systeme für Detektion und Abwehr anzuschaffen. Betreiber müssen schneller in die Lage kommen, neue Bedrohungen zu erkennen, intern zu bewerten und mit Behörden in konkrete Reaktionsabläufe zu übersetzen. Es geht also nicht nur um Technik, sondern um Reaktionsgeschwindigkeit und Effizienz. Und hier ist der Staat in der Pflicht, der die nötigen rechtlichen Rahmenbedingungen schaffen und einen Mindset-Shift gesamtgesellschaftlich fördern muss.

Wird beim Schutz kritischer Infrastruktur noch zu stark in getrennten Kategorien gedacht – physische Sicherheit, IT-Sicherheit, operative Betriebsführung –, obwohl moderne Bedrohungen zunehmend vernetzt auftreten?

Ja, meines Erachtens wird hier noch zu stark getrennt gedacht. Physische Sicherheit, IT-Sicherheit und operative Betriebsführung werden häufig organisatorisch getrennt behandelt. Moderne Bedrohungen halten sich aber nicht an diese (klassischen) Kategorien. Ein Drohnenüberflug über ein Stellwerk kann zunächst wie ein physisches Sicherheitsproblem wirken. Tatsächlich kann er aber der Vorbereitung eines Cyberangriffs dienen, der Aufklärung von Betriebsabläufen, der Identifikation von Schwachstellen oder der Vorbereitung späterer Sabotage. Umgekehrt kann ein Cyberangriff physische Auswirkungen auf den Bahnverkehr haben. Deshalb reicht es nicht, wenn jede Abteilung ihr eigenes „Süppchen kocht“. Kritische Infrastruktur muss stärker in-

tegriert geschützt werden. Es braucht gemeinsame Lagebilder, gemeinsame Risikobewertungen und eine Verbindung von physischer Sicherheit, IT-Sicherheit, Betrieb und Krisenmanagement. Sonst sieht jeder nur seinen Ausschnitt und niemand das Gesamtbild.

„Eine Abwälzung der Verantwortung weg vom Staat und den Sicherheitsbehörden auf private Betreiber kritischer Infrastruktur darf nicht stattfinden.“

Drohnen über Gleisanlagen oder Stellwerken sind längst Realität. Dürfen private Infrastrukturbetreiber heute aktiv gegensteuern – etwa durch Störsender – oder bleibt das rechtlich ausschließlich Bundespolizei und Bundeswehr vorbehalten?

Nach geltender Rechtslage ist die aktive Drohnenabwehr durch private Betreiber sehr begrenzt. Ein Betreiber wie die Deutsche Bahn darf natürlich Schutzkonzepte erstellen, Detektion organisieren, Vorfälle melden, Gelände sichern und mit Behörden zusammenarbeiten. Aber echte aktive Abwehrmaßnahmen wie Störsender, Eingriffe in Funkverbindungen oder das technische Neutralisieren einer Drohne sind rechtlich, sogar für die Sicherheitsbehörden, hochproblematisch.

Grundsätzlich liegt die eigentliche Gefahrenabwehr bei den zuständigen Sicherheitsbehörden, also je nach Lage insbesondere bei Polizei, Bundespolizei und in engen Ausnahmefällen mit unterstützenden Fähigkeiten auch bei der Bundeswehr.

Muss sich das ändern?

Wenn Betreiber kritischer Infrastruktur zwar die gefährdeten Objekte betreiben, aber im Ernstfall kaum selbst handeln dürfen, entsteht eine Lücke zwischen Verantwortung und Befugnis. Man muss deshalb zumindest darüber sprechen, ob private Betreiber unter engen gesetzlichen Voraussetzungen stärker in Abwehrkonzepte eingebunden werden müssen.



Verena Jackson

ist Rechtsanwältin und Senior Researcher am Center for Intelligence and Security Studies (CISS) der Universität der Bundeswehr München. Sie ist Transatlantic Technology Law Fellow an der Stanford University und war zuvor unter anderem am George C. Marshall European Center for Security Studies tätig. Sie berät Regierungen, Sicherheitsbehörden und internationale Institutionen, darunter die NATO, zu rechtlichen Fragen moderner Sicherheits- und Verteidigungspolitik. Ihre Schwerpunkte liegen an der Schnittstelle von Recht, Politik und neuen Technologien, insbesondere bei hybriden Bedrohungen, KI-Systemen und Cyberoperationen.

Ich wäre aber vorsichtig damit, privaten Betreibern einfach aktive Eingriffsbefugnisse zu geben. Das wäre rechtlich und auch praktisch heikel. Eine Abwälzung der Verantwortung weg vom Staat und den Sicherheitsbehörden auf private Betreiber kritischer Infrastruktur darf nicht stattfinden.

Sinnvoller ist aus meiner Sicht, dass Betreiber technisch und operationell vorbereitet sind, die Abwehrmaßnahmen aber dennoch größtenteils staatlich bleiben. Entscheidend sind in hybriden Lagen schnelle Schnittstellen, klare Einsatzkonzepte und effektive Zuständigkeiten.

Vielen Dank für das Gespräch, Frau Jackson.

Die Fragen stellte Dennis Tesch.



Mit den Infrastrukturen seiner Partner schafft RAIL-BB einen Erprobungsraum, in dem Drohnenanwendungen unter realen Bedingungen des Eisenbahn- und Logistikbetriebs getestet und für den späteren Praxiseinsatz weiterentwickelt werden können.

Drohnen-Testareale beim RAIL-BB e. V.

Zwischen Logistik, Sicherheit und Resilienz

Die Schiene ist verwundbar. Digitalisierung verändert das Risikoprofil: Cyberangriffe, Sabotage und Drohnenvorfälle rücken kritische Bahninfrastruktur in den Fokus. Auf dem Drohmentestareal des BahnTechnologie Campus Havelland in Wustermark werden neue Technologien für Überwachung, Resilienz und den Schutz sensibler Infrastruktur erprobt.

Am ehemaligen Rangierbahnhof Wustermark entsteht derzeit etwas, das weit über ein gewöhnliches Innovationsprojekt der Bahnbranche hinausgeht. Auf dem Gelände des BahnTechnologie Campus Havelland (BTC Havelland) befindet sich ein offizielles Drohnen-testareal, auf dem neue Anwendungen für Infrastrukturüberwachung, Logistikprozesse und Sicherheitslösungen erprobt werden können. Für die Bahnbranche markiert das einen bemerkenswerten Schritt: Kritische Schieneninfrastruktur wird zunehmend nicht mehr nur als Verkehrsnetz verstanden, sondern auch als sensibler Sicherheitsraum.

„Wir beobachten, dass sich Anforderungen an Bahninfrastruktur grundlegend verändern“, erklärt Dr. Ralf Böhme, Vorstandsmitglied des Vereins Railway Areas Innovation Lab – Berlin Brandenburg (RAIL-BB e. V.) und Geschäftsführer der Deutsche Eisenbahn Service und Anlagen GmbH (DE-SAG). „Neben Effizienz und Digitalisierung rücken zunehmend Fragen der Resilienz und der sicheren Verfügbarkeit in den Mittelpunkt. Unser Drohmentestareal leistet in dieser Hinsicht Pionierarbeit.“ Dabei geht es nicht allein um militärische Szenarien. Im Mittelpunkt stehen zunächst praktische Anwendungen: lo-

gistische Aufgaben, die Inspektion von Schienenfahrzeugen und Gleisanlagen, die Kontrolle schwer zugänglicher Infrastruktur, die digitale Erfassung von Schadensbildern oder die Unterstützung bei Betriebsstörungen. Gerade angesichts alternder Infrastruktur und wachsender Anforderungen an Verfügbarkeit gewinnen solche Technologien an Bedeutung. Drohnen können innerhalb weniger Minuten große Streckenabschnitte erfassen, ohne den Bahnbetrieb wesentlich zu beeinträchtigen.

Nicht nur fliegende Kamerasysteme

Bemerkenswert ist jedoch der größere Zusammenhang, in dem dieses Testareal betrieben wird. Denn mit der Digitalisierung der Schiene verändert sich auch das Risikoprofil der Infrastruktur. Moderne Bahnsysteme bestehen längst nicht mehr nur aus Stahl, Beton und

FOTOS: RAIL & LOGISTIK CENTER WUSTERMARK GMBH; REGIO INFRA GMBH & CO. KG (RIN); PIXABAY.COM/THIS_IS_ENGINEERING



Dr. Ralf Böhme
ist Vorstandsmitglied des Vereins
Railway Areas Innovation Lab –
Berlin Brandenburg (RAIL-BB e. V.)
und Geschäftsführer der
Deutsche Eisenbahn Service und
Anlagen GmbH (DESAG).



Drohnen mit professioneller Kameraausrüstung ermöglichen die präzise Inspektion von Gleisanlagen und Infrastruktur aus der Luft – schnell, sicher und ohne Betriebsunterbrechung.

Oberleitungen, sondern aus hochvernetzten Daten- und Kommunikationsstrukturen. Sensoren, Funktechnik, Leit- und Sicherungssysteme sowie digitale Anwendungen werden zunehmend Teil des operativen Betriebs. Genau hier erhält Wustermark eine strategische Bedeutung. Denn Drohnen sind nicht nur fliegende Kamerasysteme. Sie werden Bestandteil digitaler Prozessketten, liefern Echtzeitdaten und greifen auf Kommunikationsnetze

zu. Damit entstehen neue Anforderungen an Cybersecurity, Authentifizierung und den Schutz kritischer Systeme. Für die Bahnbranche lautet die zentrale Frage deshalb nicht mehr, ob solche Technologien eingesetzt werden, sondern wie sich ihre Integration sicher und resilient gestalten lässt.

Hinzu kommt ein weiterer Aspekt: Die Verwundbarkeit kritischer Infrastruktur ist in Europa zu einem politischen Thema geworden. Sabotageakte

gegen Energie- und Kommunikationsnetze, Cyberangriffe auf öffentliche Einrichtungen oder sicherheitsrelevante Drohnenvorfälle haben den Blick auf Infrastruktur verändert. Auch die Eisenbahn gerät damit stärker in den Fokus staatlicher Sicherheits- und Resilienzstrategien.

Standort mit Signalwirkung

Vor diesem Hintergrund gewinnt der Standort Wustermark Signalwirkung. Das Testareal steht beispielhaft für eine Entwicklung, bei der Infrastrukturbetreiber, Technologieunternehmen und öffentliche Stellen enger zusammenarbeiten müssen als früher. Sicherheit wird nicht mehr nur als Aufgabe von Polizei oder Behörden verstanden, sondern zunehmend als Bestandteil der Betriebsfähigkeit selbst. Für die Bahnbranche könnte daraus ein neues Verständnis von Infrastrukturmanagement entstehen: Resilienz, digitale Lagebilder und Schutzkonzepte werden künftig ebenso wichtig sein wie klassische Themen der Verfügbarkeit oder Instandhaltung. Der BahnTechnologie Campus Havelland könnte damit zu einem führenden Beispiel dafür werden, wie sich die Bahn in Europa verändert: weg von reiner Verkehrsinfrastruktur – hin zu einem intelligenten, vernetzten System, das sich selbst schützt.

cwk

Über den RAIL-BB e. V.

2021 haben sich Vertreter aus Wirtschaft, Wissenschaft und Forschung zusammengeschlossen, um den Verein Railway Areas Innovation Lab – Berlin Brandenburg (RAIL-BB) mit Sitz am BahnTechnologie Campus Havelland (BTC) zu gründen. RAIL-BB hat sich auf eine Reihe relevanter Themenfelder spezialisiert, die die Zukunft der Mobilität maßgeblich beeinflussen werden. Dazu zählen:

- **Digitalisierung und Automatisierung:** Intelligente Steuerungssysteme, vernetzte Züge und digitalisierte Bahninfrastrukturen.
- **Nachhaltige Logistiklösungen:** Innovative Ansätze zur Reduktion von Emissionen und zur Verbesserung der Versorgungsinfrastruktur zwischen urbanen und ländlichen Räumen.
- **Mobilität der Zukunft:** Lösungen für den Verkehr abseits der Hauptachsen, von der ländlichen Mobilität bis hin zu neuen Formen des Personen- und Güterverkehrs.

Mehr unter: www.rail-bb.de



Neue Perspektive über dem Gleis: BVLOS-Drohnen ermöglichen schnelle digitale Lagebilder entlang der Infrastruktur.

Automatisierte Drohnenflüge

Kontrolle ohne Sichtkontakt

Drohnen entwickeln sich im Schienenverkehr vom Vermessungswerkzeug zum strategischen Instrument der Infrastrukturüberwachung. Besonders BVLOS-Flüge könnten künftig eine wichtige Rolle beim Schutz von Schieneninfrastruktur spielen.

Drohnen gehören zum Alltag vieler Infrastrukturprojekte. Im Eisenbahnsektor geht die Entwicklung deutlich weiter: Automatisierte Flüge außerhalb der Sichtweite des Piloten rücken in den Fokus. Das BVLOS-Verfahren („Beyond Visual Line of Sight“) gilt als wichtiger Baustein einer digitalisierten und resilienteren Infrastrukturüberwachung. Die Vorteile bei langen und schwer zugänglichen Streckenabschnitten liegen auf der Hand: Oberleitungen, Brücken, Böschungen oder Vegetationsbereiche lassen sich aus der Luft schneller und mit geringerem Personaleinsatz erfassen als mit klassischen Verfahren.

Moderne Systeme

Eisenbahninfrastrukturbetreiber (EIU) und Technologieunternehmen in Europa beschäftigen sich seit Jahren mit solchen Anwendungen bei Infrastrukturprojekten und hochauflösenden Vermessungsaufgaben. Moderne Systeme erzeugen detaillierte 3D-Punktwolken und Orthofotos für Inspektion, Planung und Instandhaltung. Inzwischen geht die Entwicklung über reine Vermessungsaufgaben hinaus.

Mit der wachsenden Bedeutung kritischer Infrastruktur rückt die Frage in den Vordergrund, wie sich große Schienennetze schneller überwachen und im Ereignisfall kurzfristig kontrollieren lassen. Genau hier sehen Fachleute das Potenzial automatisierter BVLOS-Systeme. Die in Salzburg ansässige HERO.aero GmbH hat sich auf industrielle Drohnenanwendungen außerhalb der Sichtweite spezialisiert und ist sowohl in Österreich als auch in Deutschland aktiv. Geschäftsführer Martin Held betont: „Die Absicherung moderner Eisenbahninfrastruktur erfordert zunehmend flexible und schnell verfügbare Systeme. Drohnen im BVLOS-Verfahren ermöglichen es, Streckenabschnitte, Brücken oder andere kritische Anlagen innerhalb kurzer Zeit aus der Luft zu überprüfen und potenzielle Gefährdungen frühzeitig zu erkennen.“

Frage der Sicherheit

Held sieht darin nicht nur einen technologischen Fortschritt, sondern auch einen strategischen Wandel innerhalb der Branche: „Die Bahnbranche beginnt zu verstehen, dass Resilienz und Verfüg-

barkeit heute auch eine Frage der Sicherheit, der schnellen Aufklärung und digitalen Lageerfassung sind.“

Technisch entwickelt sich der Markt mit hoher Geschwindigkeit. HERO.aero setzt unter anderem auf LiDAR-Vermessungssysteme wie RIEGL VUX-120 in Kombination mit dem Velos Rotors V3. Künftig sollen neue Plattformen und „Drone-in-a-Box“-Systeme für automatisierte Einsätze im Notfallmanagement hinzukommen. Perspektivisch könnten Drohnen bei unklaren Lagen oder nach Infrastrukturereignissen vorausgeschickt werden, um Strecken aus der Luft zu erkunden. Damit entsteht über dem Gleis eine neue Ebene digitaler Infrastrukturüberwachung – als Ergänzung eines zunehmend vernetzten und resilienten Bahnsystems. cwk



FOTO: HERO.AERO GMBH

Für Martin Held gehören Lagebilder zur Resilienz moderner Bahninfrastruktur.

Intelligente Akustik aus Oldenburg

Drohnen hören, bevor man sie sieht

Eine Drohne muss nicht sichtbar sein, um erkannt zu werden. Das Fraunhofer IDMT in Oldenburg setzt dazu auf intelligente Akustik: Mithilfe maschinellen Lernens erkennt und lokalisiert die Technologie unbemannte Fluggeräte anhand ihres charakteristischen Klangmusters – das könnte auch genutzt werden, um weitere Systeme auszulösen.

Drohnen können für kritische Infrastrukturen, militärische Liegenschaften oder Großveranstaltungen zu einem Sicherheitsrisiko werden. Sie sind jedoch schwer erfassbar, wenn sie außerhalb der Sichtlinie fliegen, also die Sicht durch das Gelände, die Bebauung und das Wetter beeinträchtigt wird. Das Fraunhofer IDMT in Oldenburg hat eine intelligente akustische Sensorlösung entwickelt, die Drohnen anhand ihres charakteristischen Klangmusters erkennt und lokalisiert, auch ohne Sichtkontakt. Experten des Fraunhofer IDMT demonstrierten die Technologie während der Drone Days vom 26. bis 28. August 2026 in Hatten bei Bremen. Wenn sich ein unbemanntes Luftfahrzeug einem sensiblen Bereich nähert, zählt jede Sekunde. Sicherheitskräfte müssen möglichst früh erkennen, ob eine Drohne im Anflug ist, wo sie sich befindet und wie sich die Situation entwickelt. Klassische Detektionsverfahren liefern dafür wichtige Informationen, sind aber nicht in jeder Umgebung glei-

chermaßen zuverlässig: Sichtverbindungen können fehlen, Funkverbindungen gestört sein.

Akustische Sensorik eröffnet hier einen zusätzlichen Zugang. Als Ergänzung zu und in Verbindung mit Radar, Kamera und Lidar kann sie bestehende Sicherheitssysteme robuster machen und auch dort Hinweise liefern, wo optische oder funkbasierte Verfahren an Grenzen stoßen.

Akustischer Fingerabdruck

Die Forscher am Institutsteil Hör-, Sprach- und Audiotechnologie HSA des Fraunhofer IDMT analysieren dafür die akustischen Signale von Drohnen. Jede Drohne erzeugt ein charakteristisches Klangmuster – einen akustischen Fingerabdruck. Maschinelle Lernverfahren erkennen diese Muster auch in komplexen, lauten Umgebungen. Aus den Signalen mehrerer Mikrofone lässt sich zudem ableiten, aus welcher Richtung sich das Flugobjekt nähert. Auf diese Weise können Droh-

nen nicht nur detektiert, sondern auch lokalisiert und räumlich eingeordnet werden.

„Mit unserer akustischen Technologie bieten wir eine preiswerte und wartungsarme Ergänzung zu bestehenden Drohnerkennungssystemen“, erklärt Christian Rollwage, Gruppenleiter Audiosignalverbesserung am Fraunhofer IDMT in Oldenburg. „Gerade in bebauten oder bewaldeten Gebieten kann die Akustik einen entscheidenden Mehrwert liefern, weil sie Drohnen auch dann erfassen kann, wenn sie für andere Sensoren noch nicht sichtbar sind.“

Passiv und effizient

Während Radar- und Kamerasysteme hohe Kosten und Rechenleistung verursachen können, liegt ein besonderer Vorteil der akustischen Sensorik im geringen Energiebedarf: Sie erfasst passiv Schallemissionen und Schwingungen in der Umgebung, ohne selbst Signale auszusenden und damit ortbar zu sein. Die Technologie kann flächendeckend ausgebracht sowie autark betrieben werden. Sie eignet sich zudem als „Wake-up“-Komponente, die zusätzliche Sensorik erst dann aktiviert, wenn ein akustischer Hinweis auf eine Drohne vorliegt. Perspektivisch lässt sich die Technologie auch auf weitere akustische Ereignisse anwenden – etwa Fahrzeuge oder Schussgeräusche. Die Entwicklung basiert auf langjähriger Forschung am Standort Oldenburg. Seit 2016 hat das Fraunhofer IDMT die akustische Erkennung und Lokalisation von Drohnen unter anderem in den Verbundprojekten AMBOS und ALADDIN vorangetrieben. In weiteren internen Vorhaben wurden Algorithmen, Systemkomponenten und Integrationsmöglichkeiten kontinuierlich verfeinert. Heute stehen sowohl leicht integrierbare Softwarekomponenten als auch eine vollintegrierbare Systemlösung zur Verfügung. ■



FOTO: FRAUNHOFER IDMT/HANNES KALTER

Die Lösung des Fraunhofer IDMT detektiert und lokalisiert Drohnen auch außerhalb des Sichtfeldes mittels intelligenter akustischer Sensorik.



DB Sicherheit-Mitarbeiter beim Drohneneinsatz zur Streckenüberwachung. Der Konzern will künftig bis zu 100 Langstreckendrohnen bundesweit einsetzen – ein Baustein, den Experten jedoch nicht als hinreichenden Ersatz für bauliche Redundanzen werten.

Sabotage

14 Anschläge in sechs Monaten

Sabotageakte auf Bahnanlagen nehmen europaweit zu. Experten warnen: Das deutsche Streckennetz ist strukturell anfällig – fehlende Redundanzen, eingleisige Ausweichrouten und schleppende Digitalisierung machen selbst kleine Eingriffe potenziell systemkritisch.

Zwischen Juli und Dezember 2025 wurden in Nordrhein-Westfalen mindestens 14 Anschläge auf Bahnanlagen verübt – Brandanschläge auf Kabeltunnel, manipulierte Weichen, zerstörte Steuerungskabel. Auf einer Güterverkehrsachse im Ruhrgebiet entgleiste eine Lokomotive nahe Oberhausen-Borbeck. Sicherheitsbehörden gehen von einem Sabotageakt aus (PriMa berichtete). In Polen wurde ein Mann festgenommen, der auf einer strategisch wichtigen Strecke die Handbremse eines Kesselwagens betätigt hatte. Er hatte diverse Mobiltelefone und Dokumente in russischer Sprache bei sich. International gilt Sabotage an Bahninfrastruktur zunehmend als Instrument hybrider Bedrohungen.

Auch das deutsche Streckennetz ist, wie Markus Hecht von der Technischen Universität Berlin nüchtern formuliert, „an vielen Stellen leicht zu beschädigen und zu sabotieren.“ Der Grund ist strukturell: Redundanzen fehlen nahezu flächendeckend. Wer ein Signalkabel durchtrennt oder einen Kabeltunnel in

Brand setzt, legt oft ganze Streckenabschnitte lahm – weil kein zweites Kabel die Funktion übernehmen kann. Hecht verweist auf die Schweiz, wo Signalleitungen doppelt und teils dreifach an verschiedenen Orten verlegt sind. Norwegen zäunt alle Bahnstrecken ein – obwohl das Land dünn besiedelt ist. In Frankreich sind kritische Trassen doppelt eingezäunt, in Großbritannien ist Einzäunung flächendeckend Standard. Deutschland beziehungsweise die Deutsche Bahn hingegen vertritt die Position, das Netz sei nicht vollständig zu sichern.

Bestehender Schutz

Dennoch hat die DB ihren Sicherheitsapparat ausgebaut. Zum Einsatz kommen stationäre und mobile Videotechnik, Wärmebildkameras und Geräuschsensoren. Ergänzend überfliegen Drohnen das Streckennetz. Im September 2024 stellte der Konzern einen Prototyp einer Langstreckendrohne mit rund 150 Kilometern Reichweite vor; bis zu 100 solcher Geräte sollen künf-

tig deutschlandweit im Einsatz sein. Auch personell stockt die DB auf: Bis Ende 2025 sollten weitere 280 Mitarbeiter bei DB Sicherheit eingestellt werden. Zusätzliche mobile Präventionsstreifen sind bundesweit geplant. Hecht bewertet diese Maßnahmen zurückhaltend: Wärmebildkameras und Sensoren seien „besser als nichts“, könnten aber eine bauliche Redundanz nicht ersetzen. Die DB kündigte an, zusätzliche Netzredundanzen aufzubauen – konkrete Ausbauziele und Zeitrahmen blieb der Konzern bislang schuldig. Auf den Strecken Frankfurt–Mannheim und Hamburg–Berlin sollte im Zuge der laufenden Generalsanierungen das digitale Zugleitsystem ETCS eingebaut werden, das ohne Signalkabel auskommt. Die Entscheidung fiel dagegen. Deutschland liegt laut Hecht bei der Digitalisierung der Leit- und Sicherungstechnik unter allen EU-Ländern am weitesten zurück.

Eingleisig in die Krise

Bauliche Redundanz ist nicht nur eine Frage des Kabelschutzes – sie beginnt bei der Streckengeometrie. Ein liegengebliebener ICE auf dem eingleisigen Abschnitt der Strecke Stendal–Uelzen legte im November 2025 die wichtigs-

te Umleitungsstrecke der laufenden Korridor-Generalsanierung Hamburg–Berlin für mehr als einen halben Tag lahm. Tausende Reisende waren betroffen, Züge wurden über Hannover umgeleitet oder fielen aus.

Lukas Iffländer, stellvertretender Bundesvorsitzender des Fahrgastverbands PRO BAHN e. V., ordnet ein: „Dieser Vorfall ist kein Pech – er ist die vorhersehbare Konsequenz eines seit Jahrzehnten verschleppten Streckenausbaus.“ Denn das Grundproblem ist systemisch: Wer eine überwiegend eingleisige Strecke als Ausweichroute für einen hochbelasteten Korridor nutzt, schafft keine Resilienz, sondern verlagert die Verwundbarkeit. Jede kleine Störung kann zum Totalausfall werden.

KRITIS-Dachgesetz

Am 10. September 2025 beschloss der Bundestag das KRITIS-Dachgesetz – ein rechtlicher Rahmen, der Betreiber kritischer Infrastrukturen erstmals verpflichtet, physische Schutzmaßnahmen umzusetzen und Resilienzstrategien nachweisbar zu entwickeln. Das Gesetz erfasst alle relevanten Sektoren, auch das Transportwesen.

Markus Weidenauer, Geschäftsführer der SecCon Group GmbH mit Sitz in Unterschleißheim, beschreibt die Lage: „Zwischen politischem Willen, gesetzlicher Vorgabe und operativer Umsetzung besteht derzeit noch eine erhebliche Diskrepanz.“ Das Gesetz benenne das „Was“, nicht das „Wie“. Besonders kleinere Unternehmen ohne spezialisierte Sicherheitsabteilungen stünden vor erheblichen Umsetzungsproblemen. Hinzu komme eine regulatorische Grauzone: Viele Infrastrukturen fielen formal nicht unter das Gesetz, seien für die lokale Versorgung aber dennoch kritisch.

Für die Bahnbranche bedeutet das, nachprüfbare Maßnahmen umzusetzen: Zutrittskontrollen, Videoüberwachung, Notfallpläne – und deren regelmäßige Überprüfung durch Audits.

Keine technische Lösung

Ein verbreitetes Missverständnis besteht darin, Kamerasysteme und Zugangskontrollen als hinreichende



Sabotage an Bahnanlagen – Täter nutzen einfaches Werkzeug, und selbst kleine Eingriffe sind potenziell systemkritisch.

Schutzmaßnahmen zu betrachten. Angriffe auf kritische Infrastrukturen werden selten spontan verübt. Professionelle Akteure – staatlich gesteuert oder nicht – planen langfristig und beschaffen sich systematisch Informationen. Weidenauer plädiert daher für verdeckte sicherheitsrelevante Aufklärungsmaßnahmen: speziell geschultes Personal, das Bewegungsmuster erkennt und Verhaltensauffälligkeiten einordnet – noch bevor ein Schaden entsteht. Das aus dem Personenschutz bekannte Prinzip der präventiven Verhaltenserkennung lässt sich nach Einschätzung der SecCon Group auf Bahnanlagen und andere kritische Infrastrukturen übertragen. Voraussetzung ist qualifiziertes Personal.

Für ÖPNV-Betreiber, die oft weder über spezialisierte Sicherheitsabteilungen noch ausreichende finanzielle Mittel verfügen, liegt ein weiteres Problem vor: Vorfälle werden zwar erfasst, aber nicht systematisch ausgewertet. Serienschäden an Weichen oder manipulierte Sensoren bleiben als Muster unent-

deckt, weil kein Lagebild erstellt wird und keine strukturierte Zusammenarbeit mit Behörden besteht.

Dabei könnten, so Weidenauer, bereits einfache Lagebildanalysen Aufschluss über wiederkehrende Tätergruppen geben.

Fünf Schritte Konformität

Für Betreiber empfiehlt die SecCon Group einen fünfstufigen Ansatz: Zunächst gilt es, kritische Bereiche anhand der gesetzlichen Schwellenwerte zu identifizieren. Darauf aufbauend folgt eine Risikoanalyse, sowohl für Naturereignisse als auch gezielte physische Angriffe. Im dritten Schritt werden technische, organisatorische und personelle Schutzmaßnahmen konzipiert. Schritt vier ist die dokumentierte Umsetzung; Schritt fünf die kontinuierliche Überwachung.

Weidenauer fasst das übergeordnete Prinzip zusammen: „Man gewinnt Sicherheitskrisen nicht, wenn sie bereits eskalieren – sondern nur durch Vorsorge in ruhigen Zeiten.“ ■



Schaltschränke an der Strecke müssen besonders geschützt sein: vor Witterung, aber auch vor den Kräften vorbeifahrender Züge.

Schaltschränke

Zehn Minuten Widerstand

Gehäuse für Bahntechnik müssen besonderen Anforderungen standhalten. Nicht nur, dass sie starken Belastungen durch den Zugverkehr ausgesetzt sind, mit zunehmendem Fokus auf Sicherheit müssen sie auch einbruch- und vandalismussicher sein. Und nicht zuletzt muss die Digitaltechnik im Innern vor den Umwelteinflüssen geschützt werden.

Die Digitalisierungswelle rollt auch im Railway-Bereich. Vom digitalen Stellwerk über Zugbeeinflussungssysteme wie ETCS bis hin zu zukünftigen teil- und vollautonomen Zügen – überall wird der Standard von gestern oder analog-elektrische Bahntechnik durch smarte, digitale Technologien abgelöst. Diese Revolution erfordert entsprechend digitale Technik entlang der Strecke, die wiederum geschützt untergebracht werden muss.

Der Schutz bezieht sich dabei auf drei Bereiche: Erstens muss das Gehäuse selbst und die darin untergebrachte Technik den Umwelteinflüssen standhalten. Die Schränke und Container stehen oft an freier Strecke, in Bahnhöfen oder im Gleisvorfeld, wo die Witterung sie unmittelbar erreicht. Die einschlägigen Regularien fordern aus diesem Grund einen Korrosionsschutz, der über 30 Jahre erhalten bleibt. Ebenso wichtig ist der Schutz der im Inneren eingebauten Technik. Hitze im Sommer, Kälte im Winter und die immer vorhandene Luftfeuchtigkeit setzen der empfindlichen Digitaltechnik schnell zu. Das Gehäuse muss also dementsprechend isoliert und klimatisiert sein. Zweitens stehen die Einrichtungen in nächster Nähe neben Gleisen, auf denen

Züge mit bis zu 300 km/h vorbeibrausen. Ein vorbeifahrender Zug erzeugt gewaltigen Druck und Sog, die auf das Gehäuse einwirken. Noch stärkere Auswirkungen hat Schnee: Ein Schneeräumzug fährt mit bis zu 60 km/h und wirft den Schnee auf der Strecke mit dem vor der Lokomotive montierten Schild zur Seite. Dieser Schnee kann, wenn er etwa einen Schaltschrank trifft, auf einer Fläche von vier Quadratmetern eine Kraft von einer halben Tonne ausüben.

Und drittens sind Bahnanlagen das Ziel von Dieben, Vandalen und Saboteuren. Die Zeiten, in denen Kabel in offenen Wannen neben der Strecke verlegt werden konnten, sind lange vorbei. Kabel werden gestohlen, um das Kupfer zu verkaufen, oder ganze Bündel von Glasfasern beim Versuch des Kupferdiebstahls zerschnitten. Neben dem „ganz normalen“ Vandalismus kommen in der aktuellen politischen Lage Bedrohungen wie Datensabotage oder Datenmanipulation auf die Infrastruktur zu.

Deshalb müssen die an Bahnanlagen eingesetzten Schränke und Einhausungen einen hohen Einbruchschutz bieten. Die Bahnbetriebe verlangen einen Diebstahlschutz nach EN 1627. Einrichtungen an der Strecke müssen die Widerstandsklasse (Resistance Class,

RC) RC2 erfüllen. RC2 bedeutet, dass ein Einbrecher mindestens drei Minuten lang vom Eindringen abgehalten wird. Bei größeren Gehäusen, in denen entsprechend wichtigere und teurere Hardware verbaut ist, wird sogar RC4 erwartet, die erfahrene Einbrecher mindestens zehn Minuten draußen hält. In dieser Zeit sollte dann auch Alarm ausgelöst worden sein und die Bahnpolizei anrücken, sodass die Inhalte geschützt sind und der Betrieb nicht unterbrochen wird.

Nicht zuletzt erfordert der Einsatz in Bahnanlagen eine Vielzahl von Zertifizierungen, um im laufenden Bahnbetrieb nutzbar zu sein. Rittal bietet im Bahnbereich neben vielen weiteren Lösungen zwei Kernprodukte an: den Outdoor-Schaltschrank Toptec, der als Lösung für die Anforderungen FRMCS, Trafo, dBOS, als ELA und für viele weitere Bereiche dient, und den Railway-Cube, der als modulare Containerlösung für Bereiche wie FRMCS, GSM-R, dBOS, DWDM, GFK oder als mobiles Data Center zum Einsatz kommt.

Modulare Lösungen

Unter dem Namen Toptec bietet Rittal seit mehr als zwei Jahrzehnten Schaltschränke für den Außenbereich. Die für den Bahnbetrieb zertifizierten Modelle weisen eine Reihe von Besonderheiten auf. So sind sie komplett aus Edelstahl aufgebaut, während die Grundversionen mit Aluminium beplankt sind. Die Schränke erfüllen die Widerstands-

FOTOS: RITTAL

klasse RC2 und lassen sich beliebig anreihen und an allen Seiten mit Türen versehen. Das vorgefertigte Betonfundament ist ebenfalls anreihbar und schützt die von unten eingeführten Kabelstränge, die durch den Boden in den Schrank gelangen.

Beim RailwayCube handelt es sich um einen Container in Stahlbauweise, der bei je drei Metern Breite und Höhe bis zu zwölf Meter lang sein kann – also etwas größer als ein 40-Fuß-Seecontainer. Für die Anforderungen der Deutschen Bahn AG wurden vier Standardmodelle spezifiziert, die einen Raum auf 3, 4, 5 oder 6,5 Metern Länge oder zwei getrennte Räume auf 6,5 Metern Länge bieten. Auch hier bietet Rittal vorgefertigte Betonfundamente und Anschlussrohre, über die die Anschlussleitungen sicher in den Container geführt werden können. Die RailwayCubes bieten Einbruchschutz der Klasse RC4.

Die Toptec-Schränke sind doppelwandig ausgeführt, was Hitze und Kälte von den enthaltenen Bauelementen abhält. Die Dämmung der RailwayCube-Baureihe erfüllt die Anforderungen der DB mit einem U-Wert von unter 0,35.

Digitale Dokumentation

Als schlaue Ergänzung bietet Rittal das ePocket-System an, bei dem ein QR-Code, der von vornherein im Schrank oder Container angebracht ist, die Dokumentation vor Ort ersetzt. Statt sich über beschädigte, durchnässte oder fehlende Papierordner ärgern zu müssen, scannt der Wartungstechniker den QR-Code mit seinem Smartphone. Über die Cloud hat er Zugriff auf digitale Dokumente, Anleitungen und Hinweise, mit denen er seine anspruchsvolle Arbeit schnell erledigen kann.

Die Dokumentation des Schrankes oder Containers ist in der ePocket jedes Rittal-Schranks schon enthalten, weitere Dokumente lassen sich sehr einfach hinzufügen. So erhält jeder einzelne Schrank eine individuelle Sammlung genau der Dokumente für die in diesem Schrank verbauten Geräte.

In den nächsten Jahren sollen viele Milliarden Euro in die Erneuerung, die Digitalisierung und den Ausbau der Bahnstrecken investiert werden. Dabei setzt



Der Rittal RailwayCube ist ein Container in Stahlbauweise und bietet Einbruchschutz der Klasse RC4 – mit vorgefertigtem Betonfundament und Anschlussrohren, über die die Anschlussleitungen sicher in den Container geführt werden können.

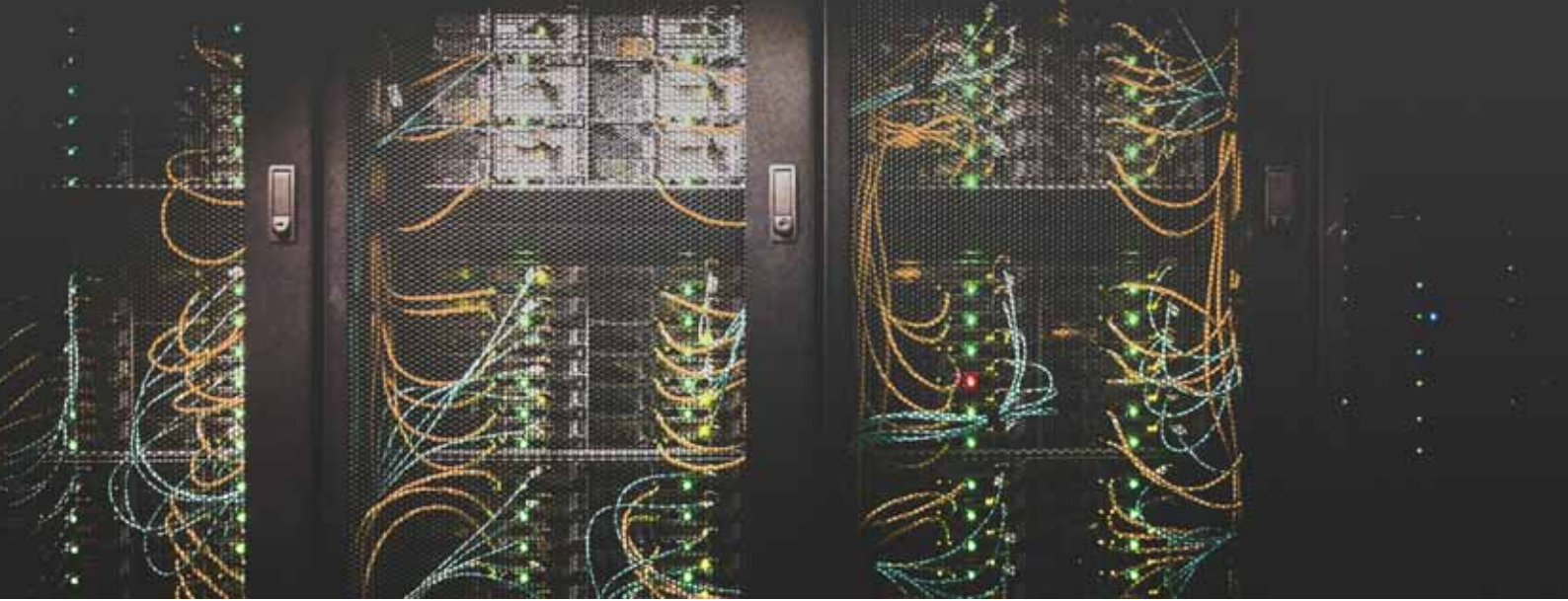


Rittal ePocket – die digitale Schaltplantasche: Über die Cloud erhalten Wartungstechniker Zugriff auf digitale Dokumente, Anleitungen und Hinweise.

die DB auf das Modell „Generalsanierung“. Dabei werden ebenfalls Stellwerke und Bahnanlagen auf digitale Technik umgerüstet, was einen kompletten Neubau vieler Bestandteile bedeutet. In diesen Großprojekten ist es sehr wichtig, dass Lieferanten nicht nur die richtigen, zertifizierten Produkte, sondern auch große Mengen schnell und zur richtigen Zeit an den richtigen Ort

liefern können. Hier hat Rittal als etablierter Schaltschranklieferant, der seit vielen Jahren im Bahnumfeld tätig ist, einen großen Vorteil. Die Railway-Produkte entsprechen sämtlichen Richtlinien, bringen die passenden Zertifizierungen und statischen Nachweise mit und sind ganz auf einfache Installation und langjährige Zuverlässigkeit ausgerichtet.

Ralf Steck



Ein einzelnes rotes Licht in einer Reihe grüner Systemanzeigen genügt manchmal, um ein ganzes Netz lahmzulegen.

Im Interview: Dennis-Kenji Kipker

Kein Angriff nötig

Cybersicherheitsexperte Dennis-Kenji Kipker erklärt im Interview, warum der GSM-R-Ausfall zeigt, wie verwundbar kritische Infrastruktur schon ohne Angriff ist, und was das KRITIS-Dachgesetz wirklich leistet.

Privatbahn Magazin: Herr Prof. Dr. Kipker, Sie haben den GSM-R-Ausfall als Beispiel für Kaskadeneffekte eingeordnet. Was unterscheidet ihn von einem klassischen Defekt – und ab wann wird ein solcher Vorfall sicherheitspolitisch relevant?

Dennis-Kenji Kipker: Ein klassischer technischer Defekt bleibt in der Regel lokal begrenzt und wirkt sich unmittelbar nur auf die betroffene Komponente aus, während ein Kaskadeneffekt entsteht, wenn ein einzelner Fehler ungebremst durch ein hochvernetztes System läuft und dabei nachgelagerte Sicherungsmechanismen mitreißt. Genau das ist beim GSM-R-Ausfall geschehen, denn ein einzelner Fehler beim Austausch einer Netzwerkkomponente hat dazu geführt, dass sich die Störung über das gesamte bundesweite Zugfunknetz ausgebreitet hat.

Sicherheitspolitisch relevant wird ein solcher Vorfall aus meiner Sicht immer dann, wenn er zeigt, dass ein einzelner Fehler in einem kritischen System geeignet ist, essenzielle Funktionen eines ganzen Landes lahmzulegen, unabhängig davon, ob die Ursache interner technischer Natur war oder auf einen gezielten Angriff von außen zurückgeht. Entscheidend ist also nicht die Herkunft der Störung, sondern die strukturelle

Verwundbarkeit, die dadurch sichtbar wird und die künftig in Zeiten hybrider Bedrohungen auch gezielt ausgenutzt werden könnte. Der GSM-R-Ausfall macht diesen Unterschied besonders deutlich, weil er zeigt, wie schnell aus einem einzelnen, an sich beherrschbaren Fehler eine Störung von nationaler Tragweite werden kann, sobald zentrale Rückfallmechanismen nicht wie vorgesehen greifen oder gar nicht adäquat vorhanden sind.

Die DB InfraGO hat einen Cyberangriff nach rund 90 Minuten Prüfung ausgeschlossen. Wie verlässlich sind solche schnellen Attributionsentscheidungen – und birgt eine öffentliche Entwarnung ein Risiko?

Dass Mitarbeitende innerhalb von rund neunzig Minuten einen Cyberangriff ausschließen, folgt zunächst nachvollziehbaren betrieblichen Abläufen, weil vor der Umschaltung auf die Rückfallebene geprüft werden muss, ob eine aktive Angriffslage vorliegt. Für eine belastbare forensische Bewertung reicht dieser Zeitraum allerdings kaum aus, denn eine vertiefte Analyse von Lieferketten, Firmware oder Fernzugriffen benötigt in der Regel deutlich mehr Zeit als eine erste betriebliche Einschätzung. Problematisch wird es vor allem dann,

wenn kritische Betreiber aus einer solchen ersten Einordnung eine öffentliche Entwarnung ableiten, denn damit entsteht der Eindruck einer abschließenden Klärung, die zu diesem Zeitpunkt tatsächlich noch gar nicht vorliegen kann. Wird eine solche frühe Einschätzung später revidiert oder ergänzt, leidet darunter nicht nur die Glaubwürdigkeit des jeweiligen Unternehmens, sondern auch das Vertrauen der Bevölkerung in die Versorgung und Kommunikation kritischer Infrastrukturen insgesamt.

„Entscheidend ist nicht die Herkunft der Störung, sondern die strukturelle Verwundbarkeit, die dadurch sichtbar wird.“

Reicht der regulatorische Rahmen des KRITIS-Dachgesetzes aus, um Vorfälle wie den GSM-R-Ausfall künftig zu verhindern oder zumindest schneller einzudämmen?

Das KRITIS-Dachgesetz setzt mit der Registrierungspflicht bis zum 17. Juli einen wichtigen ersten Schritt, doch die eigentliche Umsetzung der Vorgaben entfaltet sich erst in den nachgelagerten Monaten, wenn Betreiber eine Risikoanalyse und einen Resilienzplan vorlegen müssen. Für einen akuten Vorfall wie den GSM-R-Ausfall bedeutet dieser gestaffelte Zeitplan, dass er prä-

FOTOS: UNSPLASH.COM/TAYLOR VICK CI

ventiv in die Zukunft wirkt, aber kaum geeignet ist, eine konkrete technische Schwachstelle wie das Ausbleiben einer automatischen Umschaltung auf redundante Dienste unmittelbar zu verhindern. Insofern bleibt das Gesetz in weiten Teilen prozedural, weil es organisatorische Nachweispflichten und physische Resilienz in den Vordergrund stellt, während die konkrete technische Absicherung einzelner Systeme wie des Zugfunks eher in ergänzenden Regelwerken und in der betrieblichen Praxis der Unternehmen selbst verankert werden muss.

Damit eine solche Störung künftig tatsächlich besser eingedämmt werden kann, müsste der gesetzliche Rahmen enger mit konkreten technischen Vorgaben für Redundanz, Testverfahren und Notfallumschaltung verzahnt werden, statt sich überwiegend nur auf rechtliche Nachweis- und Dokumentationspflichten zu konzentrieren. Hier erhoffe ich mir in den kommenden Monaten weitere sinnvolle Konkretisierung.

Sie beraten auch die EU-Kommission. Gibt es europäische Vorgaben, die die Bahnbranche stärker in die Pflicht nehmen?

Mit der NIS2-Richtlinie, die in Deutschland über das novellierte BSI-Gesetz seit Dezember 2025 umgesetzt wird, existieren bereits europäische Vorgaben, die deutlich über die physische Resilienz des KRITIS-Dachgesetzes hinausgehen, weil sie konkrete Anforderungen an digitales Risikomanagement, Lieferkettensicherheit, Patch-Management und die Meldung von Sicherheitsvorfällen innerhalb kurzer Fristen stellen. Bahnunternehmen zählen dabei regelmäßig zu den wichtigen oder besonders wichtigen Einrichtungen und müssen beide Regelwerke parallel erfüllen, da das KRITIS-Dachgesetz die physische und organisatorische Seite abdeckt, während NIS2 die Cybersicherheit adressiert.

Hinzu kommt mit dem Cyber Resilience Act perspektivisch eine weitere europäische Vorgabe, die ab Ende 2027 Hersteller vernetzter Produkte zu Sicherheit von Beginn der Entwicklung

an verpflichtet und damit auch Zulieferer von Bahntechnik wie Zugfunksystemen umfassen kann, soweit keine Spezialvorgaben aus dem Eisenbahnrecht bestehen.

Sie ordnen solche Vorfälle in eine hybride Bedrohungslage ein, in der Angriffe bewusst unterhalb der Schwelle eines offenen Konflikts bleiben. Sehen Sie beim GSM-R-Ausfall Anhaltspunkte für ein Angriffsmuster – oder ist die Einordnung als „hybrid relevant“ unabhängig von der tatsächlichen Ursache?

Die Einordnung als „hybrid relevant“ setzt aus meiner Sicht keinen nachgewiesenen Angriff voraus, sondern beschreibt zunächst, dass ein Vorfall eine strukturelle Schwachstelle offenlegt, die sich unter anderen Umständen auch gezielt ausnutzen ließe. Im konkreten Fall des GSM-R-Ausfalls haben Sicherheitsbehörden und die Deutsche Bahn nach bisherigem Kenntnisstand weder Sabotage noch einen Cyberangriff festgestellt, sodass es sich aller Voraussicht nach tatsächlich um einen technischen Fehler im Zusammenhang mit einem geplanten Komponententausch gehandelt hat.

Gerade weil kein äußerer Angriff vorlag, zeigt sich aber umso deutlicher, wie verwundbar ein zentrales System der kritischen Infrastruktur bereits durch einen internen Fehler werden kann, und diese Erkenntnis bleibt unabhängig von der konkreten Ursache relevant für die Bewertung hybrider Bedrohungslagen, weil sie potenziellen Angreifern zeigt, an welcher Stelle ein System besonders empfindlich reagiert.

Nach dem iberischen Stromausfall 2025 wurde über europäische Netzresilienz diskutiert. Braucht es auch für die Schiene eine europäisch koordinierte Resilienzregulierung?

Der Stromausfall auf der Iberischen Halbinsel im vergangenen Jahr hat deutlich gemacht, dass eng verflochtene europäische Infrastrukturen nicht an nationalen Grenzen enden und dass Resilienzlücken in einem Land unmittelbar auf Nachbarstaaten durchschlagen können. Für die Schieneninfrastruktur



Prof. Dr. Dennis-Kenji Kipker
ist Professor für IT-Sicherheitsrecht an der Hochschule Bremen und wissenschaftlicher Direktor des *cyberintelligence.institute* in Frankfurt am Main und Berlin. Er berät Bundesregierung und EU-Kommission zu Cybersicherheit, Datensouveränität und digitaler Resilienz.

gilt das in besonderem Maße, weil Systeme wie GSM-R und künftig FRMCS europaweit nach denselben technischen Standards betrieben werden und ein struktureller Fehler damit potenziell in mehreren Ländern gleichzeitig auftreten kann. Die CER-Richtlinie hat mit dem KRITIS-Dachgesetz zwar einen gemeinsamen europäischen Rahmen geschaffen, doch die konkrete Umsetzung bleibt weiterhin nationalen Behörden überlassen, wodurch schon jetzt unterschiedliche Standards, Fristen und Prüfpraktiken entstehen.

Aus meiner Sicht braucht es daher gerade bei grenzüberschreitend genutzten Bahntechnologien eine noch stärker koordinierte europäische Resilienzregulierung, die über die bloße Angleichung nationaler Gesetze hinausgeht und gemeinsame technische Mindeststandards für sicherheitskritische Systeme verbindlich festlegt. Eine europäisch abgestimmte Regulierung würde zudem verhindern, dass beim europaweiten Umstieg auf den neuen, 5G-basierten Zugfunkstandard FRMCS dieselben strukturellen Schwächen in mehreren Ländern gleichzeitig neu entstehen.

Vielen Dank für das Gespräch, Herr Prof. Dr. Kipker.

Die Fragen stellte Dennis Tesch.



Der europäische Regulierungsrahmen wächst: Mit NIS2, Cyber Resilience Act und dem reformierten EU-Cybersicherheitsgesetz entstehen verbindliche Anforderungen für alle Akteure der Bahn-Lieferkette.

700 Anwendungen im Dauerbetrieb

Wartungsfenster? Gibt es nicht.

Drei Cyberangriffe auf europäische Bahnunternehmen innerhalb weniger Monate, staatliche Akteure im Hintergrund und ein wachsendes Regulierungspaket aus Brüssel: Der Bahnsektor steht unter Druck – technisch, politisch und strukturell. Was die Vorfälle über die Verwundbarkeit kritischer Infrastruktur verraten und was Betreiber und Zulieferer jetzt tun müssen.

Es war der 23. März 2025: Ukrzaliznytsia (UZ), die staatliche Eisenbahngesellschaft der Ukraine, meldete einen großflächigen Cyberangriff auf ihre IT-Infrastruktur. Onlinetickets konnten vier Tage lang nicht verkauft werden. 89 Stunden arbeiteten interne Teams, externe Cybersecurity-Spezialisten und die Cyber-Abteilung des ukrainischen Sicherheitsdienstes SBU an der Wiederherstellung. Der Fahrbetrieb blieb stabil – doch der Vorfall zeigt, wie eng digitale Systeme und betriebliche Verlässlichkeit verknüpft sind.

Am 18. Februar 2025 traf eine DDoS-Attacke die Deutsche Bahn AG: www.bahn.de und DB Navigator waren zeitweise nicht erreichbar, Buchungs- und Auskunftssysteme fielen aus. Laut einer Pressemitteilung der Deutschen Bahn griffen die Abwehrmaßnahmen. Medienberichte wiesen auf staatlich gesteuerte Angreifer aus Russland hin; eine offizielle Attribuierung blieb aus. Im Juli 2025 traf eine vergleichbare Überlastungsattacke die Website der S-Bahn Hannover.

Im Mai 2025 gelangten Angreifer über einen Dienstleister der Berliner Verkehrsbetriebe (BVG) an rund 180.000 Kundendatensätze – Namen, Adressen, E-Mail-Adressen und Vertragsnummern. Die BVG informierte Datenschutzbehörde und Kunden unmittelbar.

Diese drei Vorfälle illustrieren die Bandbreite: volumetrische Angriffe auf Kundensysteme, Datenlecks bei Subunternehmen, gezielte mehrschichtige Attacken auf Kriegsinfrastruktur. Der Bahnsektor ist verwundbar – und er wird bewusst ins Visier genommen.

Schiene als geopolitisches Angriffsziel

Die genannten Vorfälle sind kein Zufall. Nachrichtendienste und Sicherheitsbehörden mehrerer EU-Staaten beobachten seit Jahren eine systematische Ausweitung staatlich gesteuerter Cyberangriffe auf Verkehrsinfrastrukturen. Das Bundesamt für Verfassungsschutz und europäische Partner weisen dabei wiederholt auf Gruppen hin, die russi-

schen, chinesischen und nordkoreanischen Geheimdiensten zugerechnet werden. Deren Ziele sind selten rein destruktiv: Häufig geht es um das Sammeln nachrichtendienstlicher Erkenntnisse, das Einschleusen von Schadcode für spätere Aktivierung – sogenannte Pre-Positioning-Operationen – sowie das Austesten von Abwehrkapazitäten im Vorfeld möglicher militärischer Konflikte.

Die Ukraine-Erfahrung ist hier lehrreich: Ukrzaliznytsia war bereits vor dem Angriff im März 2025 wiederholt Ziel von Cyberoperationen, die nach übereinstimmenden Einschätzungen russischen Akteuren zugeordnet werden. Eisenbahnen sind in bewaffneten Konflikten strategische Infrastruktur – sie transportieren Truppen, Nachschub und Verwundete. Wer sie lahmlegt oder kontrolliert, gewinnt operative Vorteile. Diese Logik gilt nicht nur im Kriegsfall: Auch unterhalb der Kriegsschwelle können gezielte Störungen erheblichen politischen Druck erzeugen. Für Betreiber und Aufgabenträger bedeutet das: Die Bedrohungslage ist nicht allein ein IT-Problem, sondern eine sicherheitspolitische Frage. Technische Cyberabwehr und nachrichtendienstliche Lagebilder müssen stärker verzahnt werden.

GRAFIK: PIXABAY.COM/DARWIN LAGANZON; FOTO: DEUTSCHE BAHN AG / DOMINIC DUPONT

Bahnen sind besonders exponiert

Bahnunternehmen betreiben hochkomplexe IT-Landschaften. Die Deutsche Bahn AG nutzt über 700 individuelle Softwareanwendungen – ein Großteil für den Bahnbetrieb maßgeschneidert, kaum durch Standardprodukte ersetzbar. Leit- und Stellwerkstechnik, Ticketing und Instandhaltung sind historisch gewachsen und eng vernetzt. Schnittstellen zwischen Altsystemen und neuen Plattformen schaffen Angriffsflächen, die sich schwer vollständig absichern lassen.

Der 24/7-Betrieb erschwert Wartungsfenster; Patches müssen eingespielt werden, ohne laufende Prozesse zu unterbrechen. Gleichzeitig bleibt qualifiziertes Personal Mangelware: Studien belegen, dass 2023 im Bereich IT-Sicherheit bis zu 35 Prozent der Stellen unbesetzt blieben. Die Konvergenz von OT (Operational Technology) und IT – von ETCS-Steuerung bis zu Cloud-Dispositionssystemen – erweitert die Angriffsfläche kontinuierlich.

Regulierung im Aufbau

Der europäische Gesetzgeber reagiert. Marta García, Technical Affairs Manager beim Europäischen Eisenbahnindustrieverband UNIFE, beschreibt den Rahmen als vielschichtig: Die NIS2-Richtlinie wird gerade in nationale Gesetze umgesetzt. Der Cyber Resilience Act (CRA), der Cybersicherheit als Produkteigenschaft verankert, wurde im November 2023 vorläufig vereinbart. Ergänzt wird das Bild durch die Funkanlagenrichtlinie RED und die sektorspezifische Interoperabilitätsrichtlinie.

Der CRA ist nach Einschätzung von UNIFE das folgenreichste Instrument für die Zulieferindustrie. Er verpflichtet Hersteller digital vernetzter Produkte zu Cybersicherheit by Design, zur Bereitstellung von Sicherheitspatches über den gesamten Lebenszyklus und zur Meldung ausgenutzter Schwachstellen. Verstöße können mit erheblichen Bußgeldern geahndet werden. Für KMU in der Bahn-Lieferkette entsteht Mehraufwand: Prozesse müssen angepasst, Zertifizierungen durchgeführt



Der DB Navigator war im Februar 2025 Ziel einer DDoS-Attacke. Für Millionen Reisende wurde sichtbar, was Angriffe auf digitale Bahn-Infrastruktur bedeuten.

werden – parallel zur noch laufenden Normgebung.

Im Januar verabschiedete die Europäische Kommission Reformen des EU-Cybersicherheitsgesetzes. Titel IV ermächtigt die Kommission, risikoreiche Drittländer und IKT-Anbieter zu benennen und aus den Lieferketten kritischer Sektoren – einschließlich der Eisenbahn – auszuschließen. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) kann künftig mit nationalen Behörden Marktüberwachung betreiben und neue Produktkategorien für Prüfverfahren vorschlagen.

UNIFE fordert konsequentes Handeln

UNIFE-Generaldirektor Enno Wiebe fordert konkretes Handeln: Kommission und ENISA müssten ungeeignete Nicht-EU-Technologien in der Bahninfrastruktur vorrangig bewerten und Beschränkungen für risikobehaftete Lieferanten aussprechen. Hintergrund: Mehrere EU-Mitgliedstaaten investieren weiterhin in Systemtechnik nicht-europäischer Herkunft für sicherheitskritische Bahnanwendungen. Eingebettete Technologien in Stellwerken oder Kommunikationsinfrastrukturen geben Lieferanten potenziell Einblick in – oder Einfluss auf – Infrastruktur, die zivile Mobilität und militärische Logistik sicherstellt.

Der Angriff auf Ukrzaliznytsia hat diesen Zusammenhang deutlich gemacht. UNIFE verknüpft die Cyberdebatte

deshalb direkt mit der Reform des EU-Vergaberechts: Öffentliche Ausschreibungen sollen Schienenverkehr als strategischen Sektor behandeln.

Parallel zur Regulierung entwickelt der Sektor technische Standards. Die CENELEC TS 50701 zur Cybersicherheit in Bahnanwendungen wurde in die internationale Norm IEC 63452 überführt. Sie adressiert die bahnspezifische Komplexität: lange Lebenszyklen, Interoperabilität, Anforderungen an Verfügbarkeit und Integrität. Die technischen Normen zur CRA-Umsetzung entstehen zeitgleich zur Gesetzgebung – wer auf fertige Standards wartet, verliert Vorlaufzeit.

IT-Betrieb unter Druck

Cybersicherheit kostet – in einem Umfeld mit wachsenden IT-Betriebsaufwänden. Technische Rückstände und Fachkräftemangel treiben die Kosten. Studien legen nahe, dass Standardisierung und Konsolidierung den IT-Betrieb um bis zu 20 Prozent günstiger machen könnten. Wirksame Ansätze: Automatisierung von Monitoring und Incident-Management, Cloud-Migration, Outsourcing sicherheitsspezifischer Aufgaben. Sicherheitsarchitekturen müssen von Beginn an mitgedacht werden. Ein Softwarefehler im neuen elektronischen Stellwerk des Kölner Hauptbahnhofs im November 2025 zwang die DB zu einer zweiten Vollsperrung – kein Angriff, aber ein Signal, was fehlerhafte Software in sicherheitskritischen Systemen kostet.

Cybersicherheit im Bahnsektor ist somit keine optionale Zusatzleistung mehr, sondern Betriebsvoraussetzung. Mit NIS2, CRA und dem reformierten EU-Cybersicherheitsgesetz entstehen verbindliche Anforderungen für die gesamte Lieferkette. Wer als Betreiber oder Zulieferer noch keine strukturierten Prozesse für Schwachstellenmanagement, Incident Response und Lieferantenprüfung aufgebaut hat, gerät in Zugzwang. Die Koordination zwischen horizontalen EU-Regelwerken und sektoreigenen Normen wie IEC 63452 ist dabei entscheidend. Der Schutz kritischer Bahninfrastruktur ist eine gesamteuropäische Aufgabe. ■

DZSF-Forschungsprojekt

Ein DO-326A für die Schiene

Digitale Stellwerke, vernetzte Sensoren und IP-basierte Kommunikationssysteme machen die Eisenbahn leistungsfähiger – aber auch verwundbarer. Mit einem neuen Forschungsprojekt will das Deutsche Zentrum für Schienenverkehrsforschung (DZSF) verhindern, dass die digitale Schiene zur Achillesferse kritischer Infrastruktur wird.

Die Eisenbahn galt lange als robustes System aus Stahl, Beton und Signalen. Doch mit jedem digitalen Stellwerk, jeder zusätzlichen Schnittstelle und jeder neuen Kommunikationsarchitektur verlagert sich ihre Verwundbarkeit zunehmend in den digitalen Raum. Was früher mit Sabotage an Kabeln oder Gleisen versucht wurde, kann heute über Netzwerke, Schadsoftware oder manipulierte Datenströme erfolgen.

Moderne Systeme schaffen Angriffsfläche

Genau hier setzt das Projekt „Cybersecurity-Check für die digitale Schiene“ des Deutschen Zentrums für Schienenverkehrsforschung (DZSF) an. Ziel ist es, innovative Kommunikationsinfrastrukturen wie Vehicle-to-Vehicle-Systeme oder IP-basierte Netzwerke auf Schwachstellen zu prüfen und daraus künftige Sicherheits- und Zulassungsstandards abzuleiten. Das DZSF spricht ausdrücklich von der Entwicklung „eines Cybersecurity-Checks für innovative Kommunikationsinfrastrukturen der digitalen Schiene“.

Die Bedeutung reicht weit über technische Details hinaus. Moderne Bahnsysteme basieren zunehmend auf digitalen Technologien – von ERTMS über cloud-gestützte Betriebsführung bis zu IoT-Sensorik und automatisierten Diagnoseverfahren. Sie erhöhen Effizienz und Kapazität, schaffen aber zugleich neue Angriffsflächen. Ein erfolgreicher Cyberangriff könnte nicht nur einzelne Anlagen stören, sondern ganze Verkehrsachsen beeinträchtigen und erhebliche volkswirtschaftliche Schäden verursachen. Sicherheitsexperten warnen seit Jahren davor, dass kritische Infrastrukturen zunehmend hybride Ziele werden: phy-

sisch, digital und psychologisch. Gerade im Schienenverkehr sind Betriebsprozesse hochgradig vernetzt und voneinander abhängig. Störungen können sich innerhalb kurzer Zeit über große Teile des Netzes ausbreiten.

Reale Angriffsszenarien simulieren

Das DZSF-Projekt verfolgt deshalb einen praxisnahen Ansatz. Gemeinsam mit Industriepartnern sollen reale Angriffsszenarien simuliert, Schwachstellen analysiert und standardisierte Testverfahren entwickelt werden. Künftig könnten dabei auch KI-basierte Anomalieerkennung, Zero-Trust-Architekturen und widerstandsfähigere Verschlüsselungsverfahren eine zentrale Rolle spielen.

Damit nähert sich die Bahnbranche einem Sicherheitsverständnis an, das in der Luftfahrt längst etabliert ist. Tatsächlich könnte hier eine Art „DO-326A der Schiene“ entstehen – ein Sicherheitsstandard der Luftfahrtindustrie –, jetzt als europäischer Referenzrahmen für Cybersicherheit im Eisenbahnwesen. Die Dringlichkeit wächst. Mit der europäischen NIS2-Regulierung – einer EU-Richtlinie zur Cybersicherheit kritischer Infrastruktur – steigen die Anforderungen an Betreiber kritischer Infrastruktur erheblich. Gleichzeitig rücken militärische Mobilität, resiliente Lieferketten und der Schutz strategischer Verkehrsachsen stärker in den Fokus europäischer Sicherheitsvorsorge. Ein tiefgreifender Wandel für die Bahnbranche: Cyberresilienz wird vom Spezialthema zur Grundbedingung des Betriebs. Die digitale Schiene ist längst mehr als ein Verkehrsprojekt – sie wird Teil der kritischen Sicherheitsarchitektur Europas.

Walter Bloch



FOTO: ADOBE STOCK

Moderne Bahnsysteme setzen auf digitale Technologien – das erhöht Effizienz und Kapazität, eröffnet aber zugleich neue Angriffsflächen für Cyberattacken.

Hybride Aktivitäten

Tod durch tausend Papierschnitte

Digitalisiert, vernetzt, eng getaktet – und als Drehscheibe des Operationsplans Deutschland zentral für die NATO-Bündnisfähigkeit: Die Bahn ist ein strategisch verdichteter Zielraum für hybride Aktivitäten. Sönke Marahrens erklärt, warum Redundanz allein nicht reicht und wieso Resilienz eine täglich neu zu erbringende Leistung ist.

Wenn von hybriden Aktivitäten die Rede ist, denken die meisten an Cyberangriffe oder Desinformation – selten an den Zug, der einfach nicht kommt. Dabei ist die Eisenbahn als System aus Infrastruktur, Betrieb, Kommunikation und Personal aus zwei Gründen ein strategisch verdichteter Zielraum für hybride Aktivitäten. Zum einen: digitalisiert, vernetzt, auf enge Taktung angewiesen – strukturell anfällig für Kaskadeneffekte. Zum anderen: Als Drehscheibe des Operationsplans Deutschland soll dieselbe Bahn binnen 180 Tagen bis zu 850.000 NATO-Soldaten samt Gerät an die Ostflanke bringen. Eine Störung ist damit nie nur ziviles Ärgernis, sie berührt die deutsche Bündnisfähigkeit selbst.

Ein aktuelles Beispiel struktureller Anfälligkeit bot der GSM-R-Ausfall im Juni 2026: Ein planmäßiger Komponententausch legte binnen Stunden den gesamten Zugverkehr in Deutschland lahm, dabei handelte es sich noch nicht einmal um einen Angriff. Es handelte sich um einen Routinevorgang, der fehlschlug und dem eine nicht kalkulierte Kaskadenwirkung folgte. Dieser Fall liefert zwei Lehren:

1. Die Resilienz-Lektion: Die Rückfallebene war technisch voll funktionsfähig, wurde aber erst nach rund 90 Minuten manuell zugeschaltet, nachdem ein Cyberangriff ausgeschlossen war. Was fehlte, war nicht Redundanz, sondern organisationale Entscheidungsfähigkeit unter Ungewissheit: Redundanz beantwortet, was zu tun ist, wenn ein bekannter Fehlerfall eintritt; Resilienz, wie ein System handlungsfähig bleibt, solange Ursache und Ausmaß unklar sind. Resilienz erzeugt damit einen Puffer,

„Der hybride Akteur bleibt bewusst unter der Sichtbarkeitsschwelle, denn es zählt die Wiederholung, nicht der Einzelfall.“

der auch bei zielgerichteten Angriffen auf strukturelle Schwachstellen wirken kann.

2. Der Fall ist aber auch ein gutes Beispiel für die Wirkmächtigkeit hybrider Aktivitäten. Diese richten sich gezielt gegen systemische Schwächen und setzen dabei auf kaskadierende Effekte. Dabei haben sie neben den physischen Auswirkungen auf den Bahnverkehr auch immer eine psychologische Dimension: Kabelbrände bei Duisburg-Düsseldorf, manipulierte Signale in Gelsenkirchen, eine Entgleisung bei Essen vor einem US-Militärkonvoi – ob Defekt oder Sabotage der Auslöser war, ist dabei unerheblich; der hybride Akteur bleibt bewusst unter der Sichtbarkeitsschwelle, denn es zählt die Wiederholung, nicht der Einzelfall.

Das System Bahn erleidet schleichend den „Tod durch tausend Papierschnitte“: Nicht ein einzelner großer Vorfall bringt das System zu Fall, die Summe vieler kleiner Störungen zehrt am Vertrauen.

Die Tätergruppen reichen dabei von sogenannten „useful idiots“, die ungeprüft Desinformation über die Bahn teilen, über Wegwerf-Agenten, die für kleinere Taten angeheuert werden und teils nicht einmal wissen, dass sie für einen Geheimdienst arbeiten, über Sympathisanten, die sich aus innerer



Oberst Sönke Marahrens
ist Senior Fellow des Instituts für Sicherheitspolitik an der Universität Kiel (ISPK) und Offizier der Bundeswehr. Zuvor war er Direktor für Strategie und Verteidigung am European Centre of Excellence for Countering Hybrid Threats (HybridCoE) in Helsinki.

Überzeugung für die Sache des hybriden Akteurs einsetzen, bis hin zu operativ wirkenden Agentengruppen. Souveränität über die eigene Bahninfrastruktur ist keine permanente Eigenschaft, sondern eine Kapazität, die aktiv gegen Störungen – seien sie hybrider oder zufälliger Natur – erhalten werden muss. Dies obliegt nicht allein den Betreibern: Die Abwehr hybrider Bedrohungen ist eine gesamtgesellschaftliche Herausforderung.

Resilienzsteigerung ist dabei keine reine Verteidigungsausgabe ohne zivile Rendite: Die Befähigung zu resilienter Entscheidungsfindung verkürzt auch Ausfälle durch Wetter, Bauarbeiten oder Technik und zahlt damit täglich auf Pünktlichkeit und Wettbewerbsfähigkeit ein – eine Investition, die sich auch unter anderen Bedingungen auszahlt.

Für die Schiene heißt das: Verlässlichkeit im Zeitalter hybrider Aktivitäten ist kein Zustand, sondern eine täglich zu erbringende Resilienzleistung.

Sönke Marahrens

+++notizen+++

Der GSM-R-Ausfall im Juni 2026 hat gezeigt, wie schnell aus einem einzelnen technischen Fehler eine Frage von nationaler Tragweite werden kann. Sabotageakte auf Bahnanlagen, Drohnen-vorfälle über kritischer Infrastruktur und die wachsende Bedeutung der Schiene für die Landes- und Bündnis-verteidigung machen deutlich: Die Si-cherheit der Eisenbahn ist längst keine rein technische Frage mehr, sondern eine strategische.

Mit der Sonderausgabe „Rail-Defence“ hat das Privatbahn Magazin diesem Thema erstmals ein eigenes Format ge-geben. Der Zuspruch aus Politik, Indus-trie, Wissenschaft und Streitkräften hat gezeigt: Der Bedarf an einer Plattform, die Eisenbahnwirtschaft, Infrastruktur-betreiber, Sicherheitsbehörden, Streit-kräfte, Wissenschaft und Industrie zu-sammenbringt, ist größer, als es eine einzelne Ausgabe leisten kann.

Deshalb entwickeln wir Rail-Defence 2027 weiter – zu einer kontinuierlichen Plattform für den fachlichen Austausch über die sicherheitspolitische Dimen-sion der Schiene.

Im Fokus stehen fünf Themenfelder:

- Military Mobility
- KRITIS
- Cybersecurity
- Resilienz
- Dual Use

Sie arbeiten an einem Projekt, einer Technologie oder einer Lösung in diesem Bereich?

Sprechen Sie mit uns.

*Kontakt zur Redaktion
finden Sie nebenstehend.*



PRIVATBAHN MAGAZIN

20. Jahrgang

Verlag: Bahn-Media Verlag GmbH & Co. KG
Eingetragen im Handelsregister Lüneburg:
HRA 200919

pers. haft. Ges.: Bahn-Media Verwaltungs-GmbH, Lüneburg HRB 201912

Geschäftsführer:

Dipl.-Volksw. Christian Wiechel-Kramüller
USt-IdNr.: DE264819031
St.-Nr.: 47/200/32000
Salzwedeler Straße 5, D-29562 Suhlendorf
Telefon 05820 970 177-0
Telefax 05820 970 177-20

www.privatbahn-magazin.de

Herausgeber:

Prof. Dr. Uwe Höft

Redaktionsleitung:

Dennis Tesch (dt)
E-Mail: tesch@bahn-media.com
Telefon 05820 970 177-13

Redaktion:

Ulf Ringer (ur)
E-Mail: ringer@bahn-media.com
Christian Wiechel-Kramüller (cwk)
E-Mail: cwk@bahn-media.com
Telefon 05820 970 177-15

Friederike Heuer (Grafik)
E-Mail: heuer@bahn-media.com
Telefon 05820 970 177-17

Anfragen an die Redaktion:

E-Mail: redaktion@bahn-media.com

Autoren dieser Ausgabe:

Walter Bloch, Lukas Iffländer, Nicole Knapp,
Sönke Marahrens, Stefan May, Philipp Schnei-
der, Ralf Steck, Dennis Tesch, Christian Wie-
chel-Kramüller

Lektorat: Dr. Regine Anacker

Grafik, Layout: Dennis Tesch,
Friederike Heuer

Korrespondenten:

Peider Trippi (Schweiz)
Ralf Klingsieck (Frankreich)
Josef Müller (Österreich)

Anzeigenverkauf:

Andrea Wiechel-Kramüller
Telefon 05820 970 177-10
E-Mail: orga@bahn-media.com

Maike von Scheve

Telefon 05820 970 177-18
E-Mail: vscheve@bahn-media.com

Abonnement und Kundenservice:

Beatrix Hinrichs
Telefon 05820 970 177-10
E-Mail: orga@bahn-media.com

Marketing: Maike von Scheve

Telefon 05820 970 177-18
E-Mail: vscheve@bahn-media.com

Druck: FLYERALARM GmbH, 97080 Würzburg

Erscheinungsweise: 6 x jährlich
ISSN 1865-0163

Nachbestellen: Bitte geben Sie bei Ihrer Be-
stellung die gewünschte Heftnummer an.

SONDERAUSGABE RAIL-DEFENCE 2026

Redaktionsbeirat:

Dipl.-Ing. Martin Wischner

(Sprecher Redaktionsbeirat)

Vorstand Havelländische Eisenbahn AG

Dr. Stefan Buske

(stellvertretender Sprecher Redaktionsbeirat)

Rechtsanwalt – Smith, Gambrell & Russell LLP

Dr. Ansgar Burghof

Dipl.-Geogr. Clemens Bochynek

Geschäftsführendes Vorstandsmitglied

Studiengesellschaft für den Kombinierten

Verkehr e. V. – SGKV

Dr. Josef Doppelbauer

Exekutivdirektor der ERA a. D.

Dipl.-Ing. Sven Flore

Asset Manager bei der SBB Cargo Schweiz

Dipl.-Ing. Ulrich Fösel

Leiter Produktmanagement Lokomotiven

Siemens AG

Prof. Dr.-Ing. Markus Hecht

Geschäftsführender Direktor des Instituts für

Land- und Seeverkehr, TU Berlin

Dipl.-Verww. Jörg Hennerkes

Staatssekretär a. D.

Dipl.-Ing. Dipl.-Kaufm. Bernd Kaiser

Hauptgeschäftsführer Überwachungs-

gemeinschaft Gleisbau e. V. (ÜGG)

Nicole Knapp

Leiterin „Geschäftspartner und Kommunika-

tion“, DB InfraGO AG

Dipl.-Kaufm. Jost Knebel

Berater im Öffentlichen Personennahverkehr

Malte Lawrenz

Vorsitzender Verband

der Güterwagenhalter – VPI

Dr.-Ing. Bernd Seidel

Geschäftsführender Gesell. ConTrack Consul-

ting-Gesellschaft für Schienenfahrzeuge mbH

Dipl.-Ing. Jochen Slabon

Leiter Geschäftsbereich Regionalverkehr,

Alstom Transport Deutschland GmbH

Dr. Frank Thomas

Rechtsanwalt, K & L Gates LLP

Organschaften:

- Überwachungsgemeinschaft Gleisbau e. V.
- VNEI – Verband nichtbundeseigener Eisenbahn-Infrastrukturbetreiber e. V.



Der Bezug des Privatbahn Magazins ist im Mitglieds-beitrag der Überwachungsgemeinschaft Gleisbau e. V., in dem des VNEI – Verband nichtbundeseigener Eisenbahn-Infrastrukturbetreiber e. V. sowie in dem des Verbandes der Güterwagenhalter in Deutschland e. V. enthalten.

Mitgliedschaften des Verlags:

- Deutsche Fachpresse
- Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e. V.



Das Privatbahn Magazin ist Träger des Deutschen Schienenverkehrs-Preises 2023 in der Kategorie Medien.

TITELBILD: BUNDESWEHR/ANNE WEINRICH

BILDER EDITORIAL/GRUSSWORT: DOPPELBAUER, LAMPL, GÜRTLICH

Urheberrechte: Nachdruck, Reproduktionen oder sonstige Vervielfältigung – auch auszugsweise und mithilfe elektronischer Datenträger – nur mit vorheriger schriftlicher Genehmigung des Verlags. Namentlich gekennzeichnete Artikel geben nicht die Meinung der Redaktion wieder. Alle Verwertungsrechte stehen dem Verleger zu. Das Copyright 2025/2026 für alle Beiträge liegt beim Verlag.

Haftung: Für unverlangt eingesandte Manuskripte und Abbildungen wird keine Gewähr übernommen. Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion nicht übernommen werden, sofern nicht vorsätzlich oder grob fahrlässig gehandelt wurde.

Abonnenten-Service: Jahresabo (inkl. Porto) 162,00 Euro*. Das Abonnement kann innerhalb von zwei Wochen nach der Abo-Bestellung mit einer schriftlichen Mitteilung an den Verlag widerrufen werden. Das Abonnement verlängert sich um ein weiteres Kalenderjahr, wenn nicht sechs Wochen vor Ablauf des Berechnungszeitraums gekündigt wird. Im Falle höherer Gewalt hat der Abonnent keinen Anspruch auf Lieferung oder Rückerstattung der Abonnementgebühr. Die Nicht-erwähnung von Warenzeichen bedeutet nicht, dass ein Produkt ohne rechtlichen Schutz ist. *Preise im Ausland zzgl. Porto

Informieren? – Abonnieren!



Mit einem Abonnement des Privatbahn Magazins kommen alle aktuellen Nachrichten und Hintergrundinformationen aus der europäischen Bahnbranche alle zwei Monate direkt zu Ihnen nach Hause oder in Ihr Unternehmen. So verpassen Sie kein Heft und sind mit Sicherheit gut informiert.

Als Dankeschön schenken wir Ihnen ein Brillenputztuch – für klare Sicht und mehr Transparenz!



Wir sind auf jedem Weg für Sie erreichbar:



+49 5820 970 177-18



+49 5820 970 177-20



orga@bahn-media.com



www.privatbahn-magazin.de



JA, ich möchte das Privatbahn Magazin ab sofort bequem frei Haus lesen – 6 Hefte im Jahr für nur 162,00 Euro* – inklusive Versand und Mehrwertsteuer.

Name / Vorname / Firma

Straße / Nr.

PLZ / Ort

Telefon

Fax

E-Mail

☐ Ja, ich bin damit einverstanden, dass mich der Bahn-Media Verlag künftig per E-Mail oder Telefon über interessante Angebote und Aktionen informiert.

Ich abonniere das Privatbahn Magazin: ☐ als Printausgabe (162,- Euro) ☐ als App und ePaper (164,- Euro)

Zahlungsweise: ☐ gegen Rechnung ☐ bequem per Bankeinzug (SEPA)

Bahn-Media Verlag GmbH & Co. KG

Salzwedeler Straße 5

29562 Suhlendorf

IBAN

BIC

SEPA-Lastschriftmandat: Ich/Wir ermächtige(n) Bahn-Media Verlag GmbH & Co. KG, Zahlungen von meinem/unserem Konto mittels Lastschrift einzuziehen. Zugleich weise(n) ich/wir mein/unser Kreditinstitut an, die von Bahn-Media Verlag GmbH & Co. KG auf mein/unser Konto gezogenen Lastschriften einzulösen. Die Mandatsreferenz wird mir separat mitgeteilt. Ich kann/Wir können innerhalb von acht Wochen, beginnend mit dem Belastungsdatum, die Erstattung des belasteten Betrags verlangen. Es gelten dabei die mit meinem/unserem Kreditinstitut vereinbarten Bedingungen.

Datum/Unterschrift

* Das Abonnement gilt zunächst für ein Jahr und anschließend bis auf Widerruf. Ich kann es jeweils bis 6 Wochen vor Ablauf des Berechnungszeitraums kündigen. Im europäischen Ausland beträgt der Abo-Preis 212,00 € (inkl. MwSt. und Porto).



Bahn-Media Verlag GmbH & Co. KG
Salzwedeler Straße 5
D-29562 Suhlendorf
Telefon 05820 970 177-0
Telefax 05820 970 177-20

www.privatbahn-magazin.de