

# Physische Angriffe auf das Bahnsystem – ein historischer Rückblick

Anschläge auf die Kommunikationstechnik im Jahr 2022 rückten die physische Verwundbarkeit des Bahnsystems in den Vordergrund. Das Deutsche Zentrum für Schienenverkehrsforschung beschäftigt sich in einem Projekt mit der Bewertung und Abwehr bestehender Angriffspotenziale. Dieser Artikel widmet sich bisherigen physischen Angriffen.



## 1. Einleitung

Der Anschlag auf Kabelanlagen des GSM-R-Systems der DB Netz AG [1] im Oktober 2022 rückte die Verwundbarkeit des Eisenbahnsystems verstärkt in den Fokus. Durch das gezielte Durchtrennen von Kommunikationskabeln an zwei unterschiedlichen Orten gelang es den Angreifern, die Funkkommunikation in einem großen Teil des norddeutschen Bahnnetzes außer Gefecht zu setzen. Auch die russische Invasion in der Ukraine im Frühjahr 2022 rückt die Verwundbarkeit der Bahn in den betroffenen Gebieten in die öffentliche Wahrnehmung – Eisenbahnanlagen sind nicht nur attraktive militärische Ziele, sondern auch im Visier von Partisanen.

Seit Anfang 2021 läuft im Auftrag des Deutschen Zentrums für Schienenverkehrsforschung (DZSF) beim Eisenbahn-Bundesamt das Projekt „Identifikation bestehender Angriffspotenziale für das System Bahn“ („Revealing Existing Attack Vulnerabilities in the Rail System“, kurz REAVRS). Auftragnehmer sind die Universität der Bundeswehr in München, die CreaLab GmbH und die Ingenieurgesellschaft für Verkehrs- und Eisenbahnwesen mbH (IVE mbH). Das Projekt beschäftigt sich mit Angriffspotenzialen auf das Eisenbahnsystem sowohl auf physischer als auch auf Cyber-Ebene. Ein erstes Ziel des Projekts bestand dabei in einer historischen Aufarbeitung physischer Angriffe.

Dabei ist ein systematisch strukturierter Datensatz entstanden, der in diesem Artikel beschrieben und ausgewertet wird. Betrachtet werden die unterschiedlichen Angreifertypen, die Art der Angriffsmittel,

die Ziele der Angriffe und die eingetretenen Schäden. Die Ergebnisse zeigen unter anderem, dass die Anzahl der Angriffe über die Zeit stark zugenommen hat und im letzten Jahrzehnt eine Diversifizierung der Angriffe erfolgt ist. Die Einschätzung der Sicherheitslage wird aufgrund dieser gestiegenen Vielfältigkeit der Angriffsscharakteristika komplexer.

Abschließend werden ein Ausblick auf die weitere Forschungsarbeit des DZSF in diesem Bereich gegeben und Trends der Eigenschaften physischer Angriffe aufgezeigt, die sich seit den Anfängen des laufenden Jahrzehnts andeuten.

## 2. Methodik der Recherche und Datensatzstruktur

Basierend auf einer Internet- und Bibliotheksrecherche wurden weltweit erfolgte physische Angriffe auf das Eisenbahnsystem recherchiert und ausgewertet, wobei keine zeitliche Einschränkung vorgegeben wurde. Die Liste der verwendeten Quellen wird aufgrund der hohen Anzahl an Referenzen im Projektbericht zu finden sein, der voraus. Ende 2023 erscheint. Es werden lediglich Angriffe betrachtet, die nicht während regulärer Kampfhandlungen ausgeführt wurden. So werden Einsätze von Spezialeinheiten im Hinterland betrachtet, aber z.B. nicht Bombardierungen oder Angriffe mit Raketenartillerie auf Bahnstationen, wie der Angriff auf den Bahnhof Kramatorsk am 8.4.2022 im Rahmen der russischen Invasion in der Ukraine [2].

Im Datensatz wurden die Angriffe strukturiert aufgearbeitet. Jeder Angriff hat die folgenden Eigenschaften, die



**Dr. Lukas Iffländer**

Deutsches Zentrum für Schienenverkehrsforschung  
IfflaenderL@dzsf.bund.de



**Dr. Thomas Buder**

Deutsches Zentrum für Schienenverkehrsforschung  
BuderT@dzsf.bund.de

wiederum oft aus mehreren Untereigenschaften bestehen:

- **Datum:** Bei Angriffen mit einer Dauer von mehreren Tagen oder bei Angriffen um Mitternacht wurde der erste relevante Tag verwendet. Das Angriffsdatum ist in Ortszeit angegeben.
- **Ort:** Der Ort gibt das Land und die Stadt an, in der das Ereignis stattfand. Wenn verfügbar, wurde auch der Name des Bundesstaates angegeben. Zusätzlich wurden der Längen- und Breitengrad des Ereignisortes recherchiert. In Fällen, in denen die Quellen ungenaue Ortsangaben enthielten (z.B. nur den Streckenabschnitt zwischen zwei Bahnhöfen), wurde eine angemessene Vereinfachung vorgenommen (z.B. wurde im genannten Beispiel die Mitte zwischen den beiden Bahnhöfen verwendet). Schließlich wurde, sofern verfügbar, auch der Name

der Strecke erfasst. Wenn es nicht möglich war, die Strecke zu identifizieren, wurden beispielsweise der angegriffene Bahnhof oder das angegriffene Teilsystem angegeben.

- **Angreifer:** Der Angreifer wurde einem der folgenden drei Typen zugeordnet: (1) staatliche Akteure, (2) nichtstaatliche Akteure und (3) unbekannte Akteure. Bei nichtstaatlichen Akteuren wird berücksichtigt, ob Staaten die Aktivitäten aktiv unterstützen. Bei den bekannten Akteuren wird zusätzlich angegeben, ob es sich um Einzelpersonen oder Gruppen handelt. Abschließend werden Name od. Pseudonym des Akteurs angegeben.
- **Angriffsziel:** Es werden sieben Angriffsziele unterschieden:
  - *Gleise:* Gleise umfassen die Schienen selbst, Schwellen, Befestigungen sowie Unter- und Oberbau.
  - *Brücken:* Brücken werden als Ziel betrachtet, wenn Angriffe direkt auf die Brücke gerichtet sind (z.B. Sprengung von Stützpfählern). Angriffe, die auf die Gleise einer Brücke abzielen

(z.B. durch das Lösen von Befestigungselementen), fallen unter die Kategorie Gleise.

- *Bahnhöfe:* Angriffe an und in Bahnhofsgebäuden werden in dieser Kategorie betrachtet.
- *Rollendes Material:* In diese Kategorie fallen Anschläge, die sich direkt gegen rollendes Material richten (z.B. Bomben in einem Waggon).
- *Fahrgäste:* Diese Kategorie umfasst Angriffe, die sich direkt gegen Fahrgäste richten (z.B. Messerangriffe auf Fahrgäste).
- *Kommunikation:* Diese Kategorie umfasst alle Angriffe auf die Kommunikationsinfrastruktur (z.B. das Abschalten der drahtlosen Kommunikation der Bahn) sowie auf Signal- und Stellwerkskomponenten (z.B. Brandanschläge auf Kabel, die für den Betrieb eines Stellwerks verwendet werden).
- *Sonstige:* Diese letzte Kategorie umfasst alle Ziele, die nicht unter die anderen Kategorien fallen. Ein

Beispiel aus dem Datensatz ist ein Angriff auf ein Gebäude der Bundesbahnverwaltung.

Bei einigen Ereignissen fehlt in den verfügbaren Quellen die Angabe des konkreten Angriffsziels. Manche Ereignisse haben mehrere Angriffsziele (z.B. Bomben, die in Zügen explodieren, wenn diese durch Bahnhöfe fahren).

- **Angriffsmittel:** Es werden folgende Angriffsmittel unterschieden:
  - Sprengstoffe
  - Hindernisse
  - Nahkampfaffen: In diese Kategorie fallen z.B. Messer, Pfefferspray oder Schlagstöcke.
  - Feuer: Diese Kategorie schließt sekundäre Brände wie Explosionen aus.
  - Manipulation der Gleise: Diese Kategorie schließt sekundäre Manipulationen am Gleis, z.B. durch eine Explosion gebrochene Schienen, aus.
  - Schusswaffen
  - Selbstmordattentäter
  - Gas
  - Raketen



## Dir ist wichtig, spannende Großprojekte mitzugestalten?

**Wir suchen dich als Bauüberwacher:in.**

Begleite unsere Projekte im Infrastrukturbereich in den Gewerken:

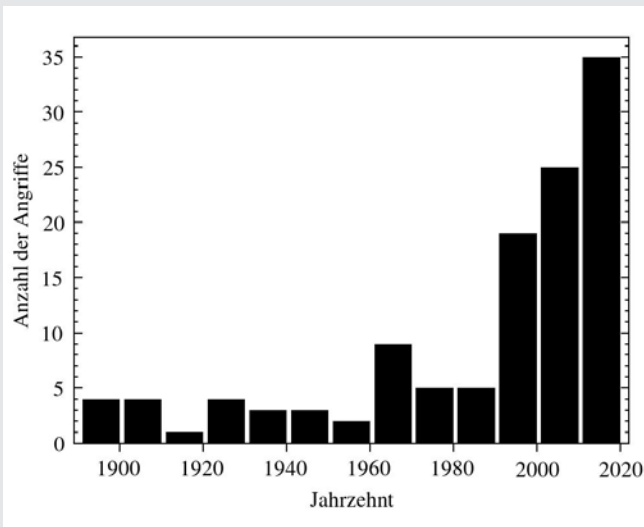
- Oberbau und/oder Konstruktiver Ingenieurbau
- Elektrotechnik
- Telekommunikation
- Leit- und Sicherungstechnik



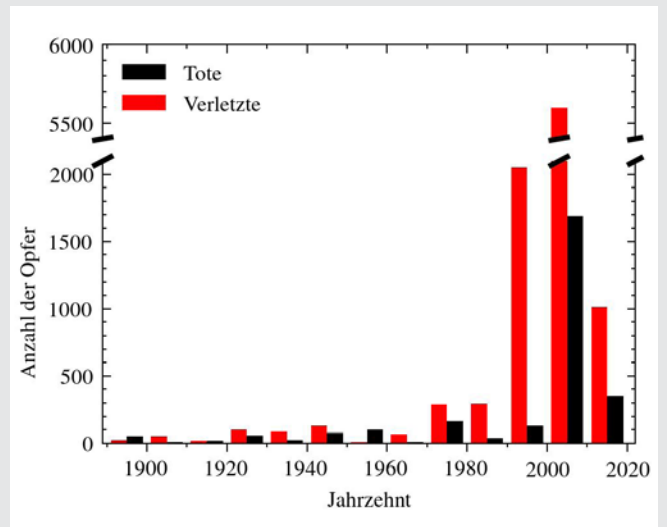
Jetzt informieren und bewerben:  
**db.jobs/db-ec**

Was ist dir wichtig?

Werde Teil der  
**DB Engineering  
& Consulting**



1: Entwicklung der Anzahl der physischen Angriffe pro Jahrzehnt. Angriffe von Anbeginn der Eisenbahn bis 1900 sind im ersten Balken zusammengefasst



2: Entwicklung der Anzahl der Angriffsoffer pro Jahrzehnt getrennt nach Verletzten und Toten. Angriffe von Anbeginn der Eisenbahn bis 1900 sind im ersten Balken zusammengefasst

- **Hacker:** Diese Kategorie bezieht sich auf physische Angriffe, die durch Hackerangriffe unterstützt werden, und schließt reine Hackerangriffe aus.

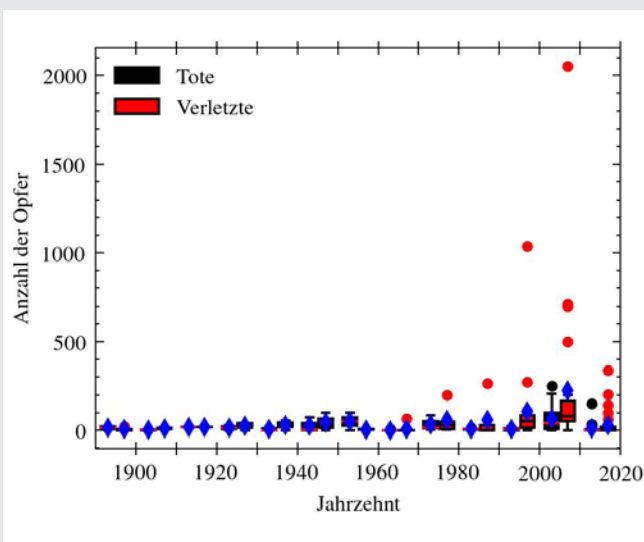
Auch hier gibt es Ereignisse, bei denen entweder keine Angaben zum verwendeten Angriffsmittel gemacht wurden oder bei denen mehr als ein Angriffsmittel zum Einsatz kam.

- **Wirkung:** In dieser Kategorie werden die tatsächlichen Auswirkungen beschrieben.

Es ist zu beachten, dass Angriffe auf einen Teil des Eisenbahnsystems gerichtet sein können, aber Auswirkungen auf andere Teile haben oder überhaupt keine Auswirkungen haben. Beispielsweise kann eine sabotierte Brücke unter einem Zug zusammenbrechen und neben Schäden am rollenden Material auch Todesopfer fordern. Auf der anderen Seite kann das Lösen von Befestigungen zwar auf die Gleise gerichtet sein, aber ent-

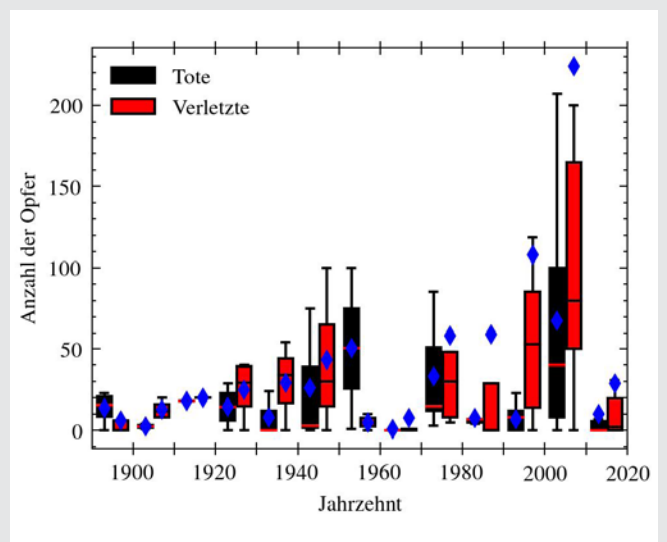
deckt werden und keine Auswirkungen haben. Es werden folgende Arten von Auswirkungen unterschieden:

- **Infrastruktur**
- **Fahrzeuge**
- **Verletzte:** Hier wird die Anzahl der verletzten Personen erfasst. Wenn möglich, wird zwischen leichten und schweren Verletzungen unterschieden, ansonsten werden alle gemeldeten Verletzungen als leicht eingestuft.



3: Entwicklung der Anzahl der Angriffsoffer pro Ereignis getrennt nach Verletzten und Toten. Angriffe von Anbeginn der Eisenbahn bis 1900 sind im ersten Balken zusammengefasst. Da einzelne extreme Ausreißer die Lesbarkeit in Bild 3a stark einschränken, wurden diese in Bild 3b weggelassen.

3a: Mit Ausreißern



3b: Ohne Ausreißer

stuf. Wenn die Quellen Spannen für die Anzahl der Verletzten angeben, wird die niedrigste Zahl verwendet.

- **Todesopfer:** Diese Kategorie umfasst die Anzahl der Todesopfer. Wenn die Quellen eine Spanne für die Anzahl angeben, wird die niedrigste Zahl verwendet.

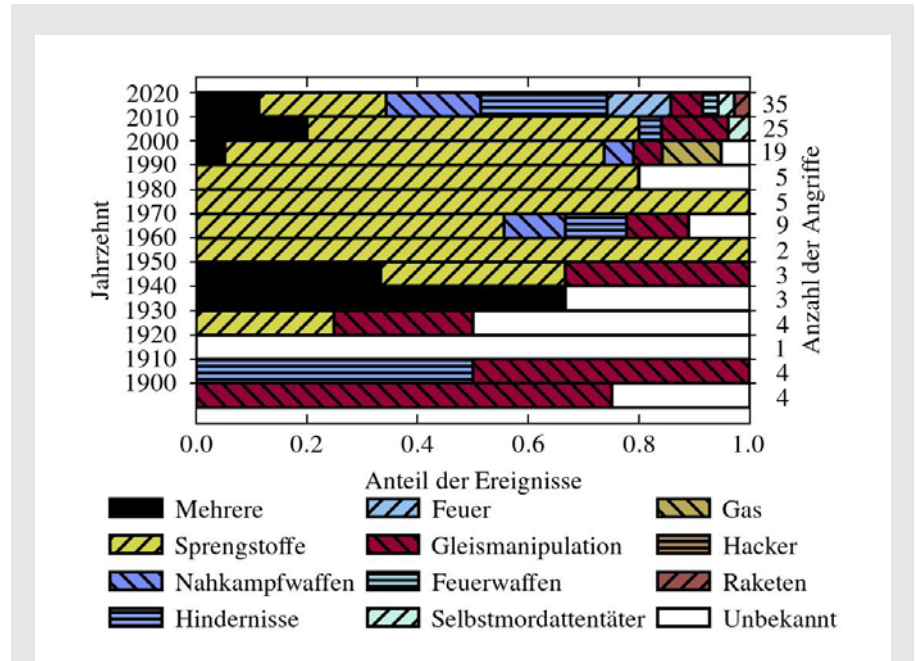
- **Beschreibung:** Dieses Element enthält die Beschreibung des Ereignisses in Textform.

### 3. Ergebnisse und Auswertung

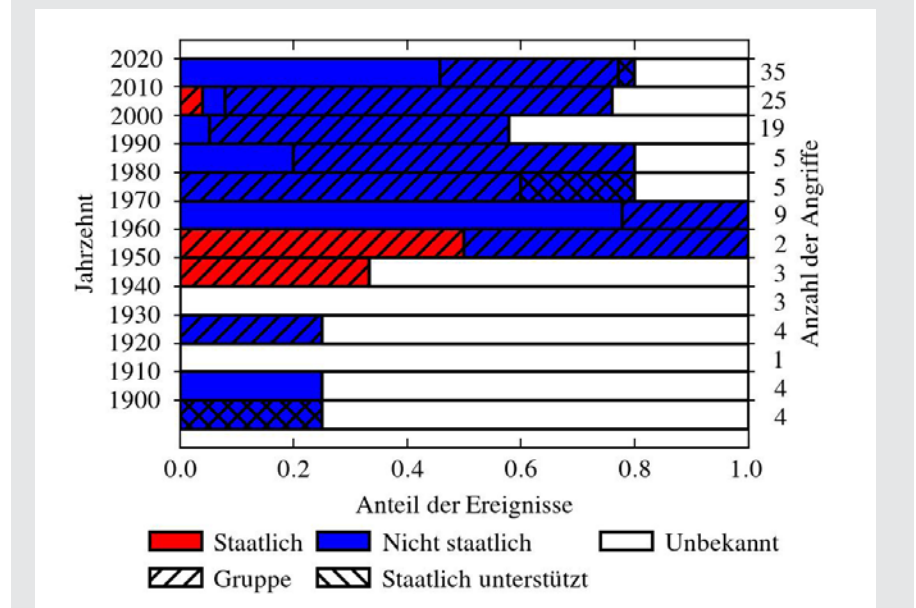
Insgesamt wurden 127 Vorfälle erfasst. Anhand einer deskriptiven Analyse wurden Trends und Erkenntnisse zu den Merkmalen der erfassten physischen Angriffe abgeleitet. Obwohl Daten über 2020 hinaus gesammelt wurden, wurden Angriffe nach 2020 nicht in die Analyse einbezogen. Diese Entscheidung wurde getroffen, weil viele Angriffe noch nicht aufgeklärt sind und z.B. die Identität eines Angreifers noch nicht bekannt ist, aber in naher Zukunft aufgedeckt werden könnte. Außerdem sind viele Ereignisse noch nicht erfasst. Insbesondere in Ländern, in denen die Pressefreiheit stark eingeschränkt ist, kann die Berichterstattung stark verzögert sein. In der Schlussbetrachtung wird jedoch ein Ausblick auf Ereignisse nach 2020 gegeben.

Zunächst wurde untersucht, wie sich die Zahl der Angriffe im Laufe der Zeit entwickelt hat. Wie Bild 1 verdeutlicht, steigt die Zahl der Angriffe seit den 1990er-Jahren deutlich an. Dieser Trend setzt sich in den folgenden Jahrzehnten fort und erreicht in den 2010er-Jahren ein Maximum von 35 dokumentierten Angriffen. Ein ähnliches Ergebnis gilt für die Analyse der Opferzahlen (Bild 2). Die Analyse der in Bild 3a und b dargestellten Opfer pro Ereignis zeigt, dass auch die durchschnittlichen Auswirkungen der Anschläge seit den letzten Jahrzehnten des 20. Jahrhunderts zugenommen haben. Dies wird besonders deutlich, da die Ausreißer nach oben bei der Zahl der Verletzten überwiegend erst seit den 1980er-Jahren auftreten (Bild 3a). Die hohen Werte der 2010er-Jahre sind auf mehrere Ereignisse mit hohen Opferzahlen zurückzuführen, z.B. die Bombenanschläge von Madrid 2004 (1.969 Leichtverletzte, 82 Schwerverletzte und 192 Tote) oder die Bombenanschläge von Mumbai 2006 (714 Verletzte und 207 Tote). Die Differenz zwischen Median und Mittelwert in den Abbildungen verdeutlicht diesen Effekt.

Bild 4 zeigt die Entwicklung des Anteils der verschiedenen Angriffsarten über die



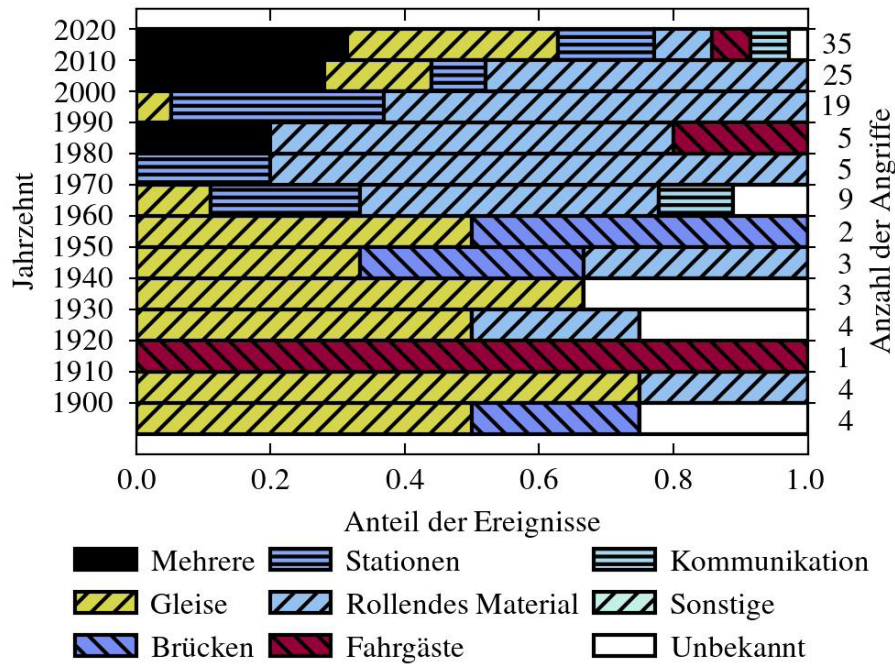
4: Anteil der unterschiedlichen Angriffsmittel pro Jahrzehnt. Angriffe von Anbeginn der Eisenbahn bis 1900 sind im untersten Balken zusammengefasst. Ereignisse mit mehreren eingesetzten Angriffsmitteln sind als „Mehrere“ und Ereignisse mit unbekanntem Angriffsmittel als „Unbekannt“ eingestuft



5: Anteil der unterschiedlichen Angreifertypen pro Jahrzehnt. Angriffe von Anbeginn der Eisenbahn bis 1900 sind im untersten Balken zusammengefasst. Ereignisse, die nicht als Gruppe markiert sind, wurden von Einzeltätern durchgeführt. Ereignisse, die nicht als staatlich unterstützt markiert sind, wurden ohne staatliche Unterstützung durchgeführt. Ereignisse mit unbekanntem Angriffsmittel sind als „Unbekannt“ eingestuft

Jahrzehnte. Zu Beginn wurden die meisten Angriffe entweder mit Hindernissen oder durch Manipulation an den Schienen ausgeführt. Vor allem in den ersten Jahrzehnten fanden sich viele unklare Quellen, die keine Angaben über das verwendete Angriffsmittel enthielten. Nach dem Zweiten

Weltkrieg wurde bei den meisten Anschlägen Sprengstoff verwendet. Dieser Trend setzte sich bis in das zweite Jahrzehnt des 21. Jahrhunderts fort, als Angriffe mit Nahkampfwaffen, Hindernissen und Schüssen einen erheblichen Anteil ausmachten und die Verteilung der Angriffsmittel insgesamt



6: Anteil der unterschiedlichen Angriffsziele pro Jahrzehnt. Angriffe von Anbeginn der Eisenbahn bis 1900 sind im untersten Balken zusammengefasst. Ereignisse mit mehreren Angriffszielen sind als „Mehrere“ und Ereignisse mit unbekanntem Angriffszielen als „Unbekannt“ eingestuft

heterogen war. Bemerkenswert ist, dass im letzten betrachteten Jahrzehnt (2010-2020) der erste Angriff mit Raketen stattfand. Auch das Auftreten von Selbstmordattentätern begann in den 2000er-Jahren.

Bild 5 zeigt die Verteilung der Angreifertypen. Es ist zu erkennen, dass in den ersten Jahrzehnten die meisten Angreifer unbekannt waren. Dies änderte sich gegen Mitte des 20. Jahrhunderts. Dies ist auf eine bessere Dokumentation der von staatlichen und staatlich unterstützten Akteuren durchgeführten Anschläge (auch die Unterstützung von Terrorgruppen erzeugt eine Papierspur, die nachträglich aufgeklärt werden kann) und den Wunsch von Terroristen nach Anerkennung für ihre Taten zurückzuführen. Staatlich unterstützte, nichtstaatliche Akteure sind selten und umfassen nur die konföderierten Guerillas im amerikanischen Bürgerkrieg, die Irisch-Republichanische Armee und eine vom pakistanischen Geheimdienst unterstützte Gruppe. Mit Ausnahme der 1940er- und 1950er-Jahre (u.a. Zweiter Weltkrieg und Vorlauf des Vietnamkriegs) wurden die meisten bekannten Anschläge von nichtstaatlichen Akteuren verübt. In den meisten Jahrzehnten wurden die häufigsten

Anschläge von Gruppen verübt. Nennenswerte Ausnahmen sind die 1960er-Jahre, als Alexander Bordan Hembluck mehrere Anschläge in Deutschland verübte, und die 2010er-Jahre, als ein einzelner Daesh-Anhänger ebenfalls in Deutschland mehrere Anschläge verübte.

Bild 6 visualisiert die Verteilung bezüglich der Angriffsziele. In den ersten Jahrhunderten konzentrierten sich die meisten Angriffe mit bekannten Zielen hauptsächlich auf die Infrastruktur (Gleise und Brücken). Der Ausreißer in den 1910er-Jahren ist darauf zurückzuführen, dass es in diesem Jahrzehnt nur einen Angriff gab. Ab den 1960er-Jahren nahm der Anteil der Angriffe auf Rollendes Material zu und bildete bis in die 2010er-Jahre die Mehrheit der bekannten Angriffsziele. In der Nachkriegszeit wurden auch Angriffe auf Bahnhöfe und Kommunikationsinfrastruktur registriert. Hinsichtlich der Angriffsmittel weisen die 2010er-Jahre eine sehr heterogene Zusammensetzung auf.

#### 4. Diskussion und Einschränkungen

Bei den zuvor dargestellten, in der deskriptiven Analyse erfassten 127 Ereignissen

zeigt sich die Zunahme der Angriffsanzahl und -schwere (der durchschnittlichen Auswirkungen pro Angriff). Zudem werden die Angriffsmittel und -ziele immer heterogener. Diese gesteigerte Vielfalt der Angriffsmerkmale erfordert eine allumfassende und breit angelegte Strategie für geeignete Sicherheitsmaßnahmen. Der jüngste systematisch durchgeführte Angriff auf die Kommunikationsinfrastruktur in Deutschland deutet darüber hinaus darauf hin, dass die Systemkenntnis der potenziellen Angreifer zunimmt. Klassische Angriffsmittel wie Messer oder Feuer spielen aber nach wie vor eine wichtige Rolle.

Die abgeleiteten quantitativen Abschätzungen von Trends und Merkmalen der Angriffe hängen natürlich von der Suchstrategie und der definierten Datenstruktur ab. Daraus ergeben sich zwei Hauptgründe für die Unvollständigkeit der recherchierten Angriffe. Erstens wurde nur in englischer und deutscher Sprache recherchiert, so dass Angriffe, die nur in anderen Sprachen gemeldet wurden, nicht erfasst wurden. Die Verteilung der recherchierten Angriffe umfasst jedoch die ganze Welt, was darauf hindeutet, dass zumindest eine Sammlung der relevantesten Angriffe

abgedeckt werden konnte. Zweitens konzentrierte sich die Recherche auf digitale Referenzen, was die Anzahl der erfassten Angriffe in früheren Jahren verzerrt haben könnte. Soweit verfügbar, wurden jedoch auch ältere und aktuelle Textquellen einbezogen (z.B. [3, 4]). Dies lässt vermuten, dass die Analyse die Anzahl der Angriffe bis Ende der 1990er-Jahre unterschätzt. Trotz dieser Einschränkung deutet der Datensatz darauf hin, dass die wichtigsten Angriffe in diesem Zeitraum erfasst wurden. Darüber hinaus bleibt der abgeleitete Trend, dass die Zahl der Angriffe in den 2000er-Jahren zugenommen hat, von dieser Einschränkung unberührt.

**5. Ausblick**

Die Erfassung der Angriffe gehört zum ersten Arbeitspaket des REAVRS Projekts. Weitere Pakete beschäftigen sich mit der Definition relevanter Angriffscharakteristika, deren Bedrohungsbewertung und die Ableitung und Bewertung von Gegenmaßnahmen. Zudem beinhaltet das Projekt auch die Erfassung und Analyse von Cyberangriffen, die methodisch ähnlich durchgeführt werden. Der Datensatz wurde veröffentlicht und ist beim Fachinformationsdienst Mobilitäts- und Verkehrsforschung (FID move) herunterzuladen [5]. Weiterhin soll im Kontext des Projekts die Möglichkeit geschaffen werden, Fehler

im Datensatz zu melden, Korrekturen vorzuschlagen und auch neue Angriffe beizusteuern. Derzeit wird geprüft, wie dies innerhalb der aktuellen und zukünftigen IT-Infrastruktur des EBA abgebildet werden kann. Wirft man einen Blick auf die Angriffe des laufenden Jahrzehnts, fällt auf, dass sie sich verstärkt auf Kommunikations- und Einrichtungen der Leit- und Sicherungstechnik beziehen und die Verfügbarkeit des Systems schwächen.

Da die Technologieentwicklung gerade in diesem Bereich schnell voranschreitet, untersucht das DZSF derzeit in einem weiteren Projekt „Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte für das System Bahn“, welche künftig notwendigen IT-Sicherheitskonzepte geeignet sind, den Schienenverkehr angemessen vor Cyberangriffen zu schützen. Der Bericht zur Technologieprognose ist bereits veröffentlicht [6].

**Literatur**

[1] Nach Sabotage: Bahnverkehr im Raum Norddeutschland normalisiert sich weiter, (2022), verfügbar unter: [https://www.deutschebahn.com/de/presse/pressestart\\_zentrales\\_uebersicht/Nach-Sabotage-Bahnverkehr-im-Raum-Norddeutschland-normalisiert-sich-weiter-8960922](https://www.deutschebahn.com/de/presse/pressestart_zentrales_uebersicht/Nach-Sabotage-Bahnverkehr-im-Raum-Norddeutschland-normalisiert-sich-weiter-8960922)  
 [2] News, B.B.C.: Kramatorsk station attack: What we know so far. BBC News. (2022) , verfügbar unter: <https://www.bbc.com/news/world-europe-61036740>

[3] Anschläge auf Kabelanlagen der DB. Eisenbahn-Revue International. 376 (2017).  
 [4] von Stockert, L.R.: Eisenbahnunfälle: ein Beitrag zur Eisenbahnbetriebslehre. W. Engelmann (1913).  
 [5] Iffländer, L., Buder, T., Loreth, T., Villota, M.A.: Physical Attacks on the Railway System, (2023), verfügbar unter: <https://data.fid-move.de/dataset/ef536b32-2dee-4c1f-9ce2-f8dbba0df0d1>  
 [6] Leining, M., Schubert, M., Heinrich, M., Katzenbeisser, S., Unger, S., Krauß, C., Scheuermann, D.: Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte: Teil 1: Technologieprognose. Deutsches Zentrum für Schienenverkehrsforschung beim Eisenbahn-Bundesamt (2022), verfügbar unter: [https://www.dzsf.bund.de/SharedDocs/Downloads/DZSF/Veroeffentlichungen/Forschungsberichte/2022/ForBe\\_20\\_2022\\_AP1.html?nn=3805352](https://www.dzsf.bund.de/SharedDocs/Downloads/DZSF/Veroeffentlichungen/Forschungsberichte/2022/ForBe_20_2022_AP1.html?nn=3805352)

**Summary**

**Physical attacks on the railway system – a review**

Attacks on communications technology in 2022 put the physical vulnerability of the railway system in the spotlight. The German Centre for Rail Traffic Research (DZSF) is involved in a project to evaluate and defend existing potential attacks. For this reason, a data set was designed that evaluates previous physical attacks. Particularly in the last decade, attacks have become more diverse in terms of means and targets, making the evaluation of the security situation more complex.

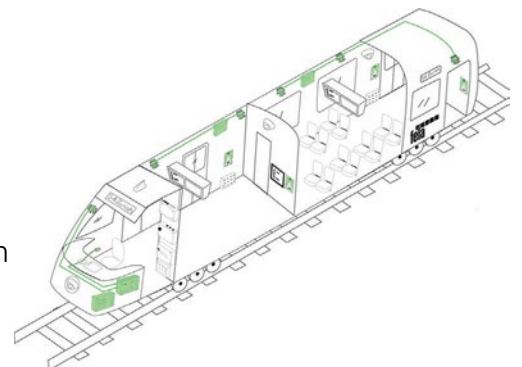


**Fahrgastinformation: PAN Audio Ecosystem**

- Audio Verstärker für Sprachausgabe
- Server für Infrastruktur und Call Handling
- Telefonbox mit Sprechstellen zur Kommunikation
- Vom Verstärker bis zum Lokführer-Mikrofon



Alles aus einer Hand – Swiss made



fela.swiss