Bund Deutscher Kriminalbeamter

Wenn öffentliche staatliche Informationen zum Sicherheitsrisiko werden

07.09.2026

BDK fordert einen neuen Umgang mit staatlicher Transparenz im Zeitalter von KI und hybriden Bedrohungen.

Deutschland investiert in den Schutz kritischer Infrastruktur. Anlagen werden physisch gesichert, Anforderungen an die Cybersicherheit erhöht und Staat wie Wirtschaft stärker auf Sabotage, Spionage und hybride Bedrohungen vorbereitet. Mit dem seit März 2026 geltenden KRITIS-Dachgesetz ist erstmals ein sektorübergreifender Rahmen für die physische Resilienz kritischer Anlagen geschaffen worden.

Aus Sicht des BDK greift die bisherige Debatte dennoch zu kurz. Denn während Deutschland seine Infrastruktur gegen physische und digitale Angriffe härtet, wächst gleichzeitig ein bislang wenig beachteter Informationsraum: der Bestand öffentlich zugänglicher staatlicher Daten über Infrastruktur, Behörden, öffentliche Unternehmen und ihre gegenseitigen Beziehungen.

Die jüngsten mutmaßlichen Sabotagehandlungen und -versuche an Teilen der Energieinfrastruktur verleihen dieser Frage zusätzliche Aktualität. Sie sind Anlass für die Frage, nicht ihr Beweis. Es gibt keinen Beleg dafür, dass bei diesen Taten staatliche Veröffentlichungen zur Vorbereitung genutzt wurden. Unabhängig davon stellt sich jedoch eine grundsätzliche sicherheitspolitische Frage:

> „Wir reden zu Recht darüber, wie wir kritische Infrastruktur besser schützen. Dazu gehört aber auch die Frage, welches Lagebild über diese Infrastruktur wir selbst öffentlich erzeugen“, sagt der BDK-Bundesvorsitzende Dirk Peglow.

Der BDK hat diese Frage in einem eigenen Test untersucht. Das Ergebnis: Aus öffentlich zugänglichen staatlichen Quellen ließ sich innerhalb kürzester Zeit mithilfe frei zugänglicher KI-Anwendungen – Large Language Models wie GPT-5.6 – durch systematische Verknüpfung ein deutlich weitergehendes Bild sicherheitsrelevanter Zusammenhänge gewinnen, als es die einzelnen Veröffentlichungen jeweils erkennen ließen.

Ein Informationsraum, den niemand als Ganzes geplant hat

Wer sich ein Bild von kritischer Infrastruktur und ihren Zusammenhängen machen will, muss keineswegs zuerst nach geheimen Informationen suchen. Bund, Länder und Kommunen veröffentlichen täglich enorme Mengen an Daten über sich selbst – aus jeweils nachvollziehbaren Gründen und verteilt über unterschiedlichste Informationssysteme.

Parlamente veröffentlichen Antworten auf Kleine und Große Anfragen, teilweise mit umfangreichen Tabellen und Anlagen. Umwelt- und Planungsverfahren enthalten Angaben über Standorte, Vorhaben und technische Veränderungen. Vergabeunterlagen können Projekte und beteiligte Unternehmen erkennen lassen, Haushaltspläne Investitionen und Zeiträume. Hinzu kommen öffentliche Register und Geodaten, Geschäftsberichte öffentlicher Unternehmen, Energie- und Klimaberichte, Projektseiten, Immobilieninformationen, Genehmigungsunterlagen und Pressemitteilungen.

Besonders interessant können dabei gerade Veröffentlichungen sein, die mit Innerer Sicherheit auf den ersten Blick nichts zu tun haben. Eine Umweltunterlage, ein Bericht zum Ausbau erneuerbarer Energien oder eine parlamentarische Anfrage über öffentliche Gebäude kann Informationen enthalten, die in einem anderen Zusammenhang eine völlig neue Bedeutung erhalten. Denn Sicherheitsrelevanz hängt nicht davon ab, was über einem Dokument steht.

Eine Quelle nennt einen Standort, eine andere dessen Funktion. Eine Planungsunterlage beschreibt eine technische Veränderung, eine Ausschreibung ein beteiligtes Fachunternehmen, ein Haushaltsdokument den Zeitraum. Eine ältere parlamentarische Antwort dokumentiert möglicherweise noch den vorherigen Zustand. Jede einzelne Angabe kann für sich genommen unspektakulär sein. Zusammen können sie ein Bild ergeben, das keine staatliche Stelle jemals als Ganzes veröffentlicht hat.

Für die Kriminalpolizei ist dieses Prinzip vertraut. Ermittlungsarbeit besteht gerade darin, verstreute Einzelinformationen zusammenzuführen und daraus Beziehungen und Strukturen zu erkennen. Eine Telefonnummer, eine Zahlung oder eine Fahrzeugbewegung besitzt isoliert häufig nur begrenzten Erkenntniswert. Erst die Verbindung kann daraus ein Lagebild oder gar einen Tatverdacht werden lassen. Diese Logik funktioniert auch in der Gegenrichtung. Extremistische Akteure, organisierte Kriminalität oder potenzielle Saboteure müssen nicht nach dem einen geheimen Dokument suchen, wenn sich relevante Zusammenhänge aus vielen legal zugänglichen Informationen rekonstruieren lassen.

Der Staat veröffentlicht dokumentenbezogen. Ein möglicher Gegner analysiert erkenntnisbezogen.

KI verändert nicht die Information, sondern ihren Wert

Neu ist dieses Problem nicht. Neu ist seine Skalierbarkeit. Was früher langwierige Recherche, die Lektüre zahlreicher Dokumente und erhebliche Fachkenntnis erforderte, kann durch moderne Datenanalyse und KI erheblich beschleunigt werden. Systeme können Orte, Organisationen und technische Begriffe erkennen, unterschiedliche Bezeichnungen desselben Objekts zusammenführen, ältere und aktuelle Veröffentlichungen vergleichen, zeitliche Entwicklungen rekonstruieren und Beziehungen zwischen Informationen sichtbar machen.

Aus vielen Einzelveröffentlichungen kann so faktisch ein zusätzliches Dokument entstehen. Es wurde von keiner Behörde geschrieben, liegt in keiner Akte und wurde nirgendwo als Ganzes veröffentlicht. Es entsteht erst durch Verknüpfung. Das virtuelle zusätzliche Dokument ist das Lagebild hinter den Dokumenten.
Gerade darin liegt eine kriminalpolizeiliche Parallele. Der BDK fordert leistungsfähige Analyseinstrumente, weil moderne Ermittlungen große und heterogene Datenbestände zusammenführen müssen. Dieselbe technologische Entwicklung verändert aber zwangsläufig auch die Möglichkeiten derjenigen, die Informationen über kritische Strukturen gewinnen wollen.

> „Wir nutzen Datenanalyse, um aus einzelnen Spuren Täterstrukturen sichtbar zu machen. Wir müssen deshalb genauso professionell prüfen, welches Lagebild andere aus unseren eigenen veröffentlichten Informationen über den Staat und seine Infrastruktur erstellen können“, so Dirk Peglow.

Der BDK hat den Perspektivwechsel selbst getestet

Um zu prüfen, ob dieser Effekt lediglich theoretisch besteht, hat der BDK einen eigenen Test mit ausschließlich öffentlich zugänglichen staatlichen Informationen durchgeführt. Ausgangspunkt war bewusst kein Dokument über KRITIS, Sabotageschutz oder Innere Sicherheit, sondern eine umfangreiche parlamentarische Veröffentlichung aus einer deutschen Metropolregion zu Photovoltaik, Energieeffizienz und öffentlichen Gebäuden. Die konkrete Drucksache, die betroffene Region und die im weiteren Verlauf untersuchten Objekte benennt der BDK bewusst nicht. Nicht, weil die Quellen geheim oder schwer zugänglich wären. Das Gegenteil ist der Fall. Ihre Benennung würde jedoch verstreute Informationen erneut zusammenführen, auf besonders ergiebige Fundstellen hinweisen und damit genau jene Recherche erleichtern, deren sicherheitspolitische Wirkung der Test untersuchen sollte.

Schon die parlamentarische Ausgangsquelle erwies sich als bemerkenswert. Für ihre Beantwortung waren Informationen zahlreicher Behörden und öffentlicher Unternehmen eines Bundeslandes zusammengetragen worden. Dadurch fanden sich in einem gemeinsamen Datenbestand Angaben aus Energie- und Wasserversorgung, Verkehr, Hafen- und Luftverkehr ebenso wie zu Liegenschaften aus Polizei-, Feuerwehr- und Justizbereichen. Einzelne Angaben verbanden Standorte oder Gebäudefunktionen mit konkreten technischen Maßnahmen, Projektzeiträumen und weiteren Informationen. Das war nicht das Ergebnis einer Sicherheitsabfrage. Es entstand als Nebenprodukt einer parlamentarischen Fragestellung zu Energie und öffentlichen Gebäuden. Genau das ist der entscheidende Punkt: Sicherheitsrelevante Mosaiksteine liegen nicht zwingend in Sicherheitsdokumenten.

Der Test blieb jedoch nicht bei diesem Dokument stehen. Die Angaben wurden mit weiteren öffentlich zugänglichen staatlichen Quellen aus Planungs-, Umwelt- und Energiebereichen abgeglichen. Dabei ließen sich zusätzliche funktionale und technische Zusammenhänge nachvollziehen.

Am Beispiel eines Stromnetzes zeigte sich besonders deutlich, was dadurch möglich wird. Aus verschiedenen amtlichen Quellen ließ sich nicht nur erkennen, dass bestimmte technische Anlagen existieren. Veröffentlichungen ermöglichten darüber hinaus Rückschlüsse darauf, welche Netzebenen miteinander verbunden sind, welche Anlagen in Beziehung zueinander stehen und welche Einrichtungen innerhalb des Netzes eine besondere Knotenfunktion besitzen. Teilweise beschrieben öffentliche Planungsunterlagen bestehende oder geplante Versorgungsbeziehungen zwischen einzelnen Netzknoten.

Damit änderte sich die Qualität des Wissens. Es ist sicherheitsfachlich ein Unterschied, lediglich zu wissen, dass an einem Ort eine technische Anlage steht, oder einordnen zu können, welche Funktion diese Anlage innerhalb eines größeren Versorgungssystems besitzt.

Der Test untersuchte ausdrücklich nicht, wie eine konkrete Anlage technisch oder physisch beeinträchtigt werden könnte. Das war für den Befund weder erforderlich noch sinnvoll. Bereits die vorgelagerte Erkenntnis ist relevant: Öffentliche Informationen können helfen, aus einer Vielzahl sichtbarer Anlagen diejenigen herauszufiltern, deren Funktion und Vernetzung eine besondere systemische Bedeutung nahelegen.

Der Staat kann damit unbeabsichtigt einen Teil der Aufklärungsarbeit vorwegnehmen: Objekte auffinden, Informationen zuordnen, Zusammenhänge bestätigen und ihre Bedeutung innerhalb eines Systems verständlicher machen.

Wenn der Staat seine Informationen selbst zusammenführt

Der Test machte noch einen zweiten Effekt sichtbar. Gerade umfangreiche parlamentarische Anfragen führen häufig Informationen zusammen, die zuvor über verschiedene Behörden, öffentliche Unternehmen und Verwaltungsbereiche verteilt waren. Für eine Antwort werden Daten erhoben, vereinheitlicht und nach einer gemeinsamen Fragelogik geordnet. Mit der Veröffentlichung kann dadurch ein Informationsbestand entstehen, der vorher in dieser Form überhaupt nicht existierte. Der Staat veröffentlicht dann nicht nur Informationen. Er strukturiert sie zugleich.

Für einen externen Analysten reduziert das den Rechercheaufwand. Zuständigkeiten, unterschiedliche Objektbezeichnungen, organisatorische Zuordnungen oder Projektbeziehungen müssen teilweise nicht mehr selbst rekonstruiert werden, weil die Veröffentlichung bereits Verbindungen herstellt.

Hinzu kommt die Zeitdimension. Parlamentarische Datenbanken und andere staatliche Archive bewahren frühere Zustände dauerhaft auf. Eine ältere Veröffentlichung beschreibt einen Ausgangszustand, eine spätere kündigt eine Veränderung an und eine weitere bestätigt deren Umsetzung. Aus Momentaufnahmen entstehen Zeitreihen. Auch eine amtliche Bestätigung kann eine zuvor nur vermutete Beziehung belastbarer machen.

Damit verändert sich die Funktion staatlicher Archive. Im KI-Zeitalter werden sie zunehmend zu einem maschinell erschließbaren Langzeitgedächtnis über die Funktionsweise des Staates.

Von der Mosaiktheorie zur systematischen Mosaikprüfung

Dass einzeln wenig aussagekräftige Informationen in ihrer Kombination eine neue und gegebenenfalls schutzwürdige Erkenntnis ergeben können, ist aus dem Informationsschutz schon seit Langem als Mosaiktheorie bekannt. Digitalisierung und KI verleihen diesem Prinzip eine neue praktische Dimension: Die Zahl der verfügbaren Mosaiksteine wächst, ihre Recherche wird einfacher und ihre Verknüpfung zunehmend automatisierbar.

Der BDK schlägt deshalb vor, daraus eine systematische Mosaikprüfung staatlicher Veröffentlichungen zu entwickeln. Sie ersetzt nicht die bisherige rechtliche Prüfung, ob eine Information veröffentlicht werden darf. Sie ergänzt sie um eine sicherheitsfachliche Perspektive: Was wird durch diese Veröffentlichung gemeinsam mit dem bereits öffentlich verfügbaren Wissen neu erkennbar?
Im Kern handelt es sich um einen Vorher-Nachher-Vergleich. Welche Erkenntnisse waren vor der Veröffentlichung belastbar möglich, welche danach und welche bislang fehlende Verbindung wird durch die neue Information geschlossen?

Dabei ist nicht die Menge der veröffentlichten Daten entscheidend. Ein hundertseitiger Bericht kann nahezu keinen zusätzlichen Erkenntniswert erzeugen. Eine einzige amtliche Zuordnung kann dagegen zwei bislang getrennte Informationsbestände miteinander verbinden.

Die Mosaikprüfung soll insbesondere erkennen, ob ein Objekt leichter identifizierbar wird, seine Funktion deutlicher hervortritt, Abhängigkeiten oder Netzbeziehungen sichtbar werden, neue Zustands- oder Zeitinformationen entstehen oder Beziehungen zu externen Unternehmen und anderen Akteuren hergestellt werden.

Ein positiver Befund bedeutet nicht automatisch Geheimhaltung. Er bedeutet zunächst, dass der zusätzliche Erkenntnisgewinn sicherheitsfachlich bewertet werden muss.

Informations-Red-Teaming: die eigene Informationslage mit fremden Augen betrachten

Für besonders relevante Bereiche sollte die Mosaikprüfung durch Informations-Red-Teaming ergänzt werden. Der Ansatz stammt vor allem aus der IT- und Cybersicherheit: Red Teams nehmen bewusst die Perspektive eines potenziellen Gegners ein, um Schwachstellen zu erkennen, bevor sie tatsächlich ausgenutzt werden. Auf den staatlichen Informationsraum übertragen würde ein Informations-Red-Team untersuchen, welches Lagebild sich ausschließlich aus öffentlich zugänglichen Quellen rekonstruieren lässt.

Dabei geht es ausdrücklich nicht darum, konkrete Angriffe auf Anlagen zu planen. Die entscheidende Frage liegt eine Stufe davor: Wie weit helfen staatliche Veröffentlichungen bereits dabei, relevante Objekte zu identifizieren, ihre Funktion zu verstehen, Beziehungen zu erkennen und ihre Bedeutung innerhalb eines größeren Systems einzuordnen?

Der BDK-Test war ein erster praktischer Perspektivwechsel dieser Art.

Auch die Transparenzregeln selbst müssen überprüft werden

Mosaikprüfung und Red-Teaming allein reichen jedoch nicht aus. Es wäre widersinnig, immer aufwendigere Sicherheitsprüfungen einzuführen, wenn gesetzliche Regelungen gleichzeitig detaillierte Veröffentlichungen verlangen, deren heutige Wirkung bei ihrer Entstehung kaum vorhersehbar war.

Viele Transparenz- und Beteiligungsregeln stammen aus einer anderen Informationswelt. Zwischen einer zeitlich begrenzten Einsichtnahme in Planunterlagen und einem dauerhaft weltweit verfügbaren, volltextdurchsuchbaren und automatisiert auswertbaren Dokumentenbestand besteht ein qualitativer Unterschied.

Aus Akteneinsicht ist digitale Dauerverfügbarkeit geworden. Aus digitaler Dauerverfügbarkeit wird durch KI verknüpfbares Lagewissen.

Bund und Länder sollten deshalb bestehende Veröffentlichungs- und Transparenzpflichten mit Bezug zu kritischer und sonstiger sicherheitsrelevanter Infrastruktur systematisch überprüfen. Das betrifft insbesondere Umwelt-, Energie-, Planungs- und Genehmigungsverfahren, kann aber ebenso parlamentarische Veröffentlichungen, Vergaben, Haushaltsinformationen und andere staatliche Datenbestände erfassen.

Dabei geht es nicht um die Alternative zwischen vollständiger Öffentlichkeit und Geheimhaltung. Entscheidend ist, welche Information für den jeweiligen parlamentarischen oder gesetzlichen Zweck tatsächlich erforderlich ist. Wo Aggregation oder geringere Detailtiefe genügen, muss nicht objektscharf veröffentlicht werden. Und wo Regelungen unter den Bedingungen automatisierter Analyse einen sicherheitspolitisch nicht mehr vertretbaren zusätzlichen Erkenntnisgewinn erzeugen, müssen sie auch geändert oder zurückgenommen werden können.

Das KRITIS-Dachgesetz liefert dafür einen bemerkenswerten Anknüpfungspunkt: Die nationale KRITIS-Resilienzstrategie soll ausdrücklich Erwägungen zu Transparenzpflichten für kritische Infrastrukturen enthalten. Der BDK hält es für notwendig, diesen Gedanken auf die staatliche Veröffentlichungsarchitektur insgesamt weiterzuentwickeln.

> *„Transparenz darf nicht bedeuten, dass der Staat seine eigene Verwundbarkeit immer präziser dokumentiert. Was für demokratische Kontrolle notwendig ist, muss öffentlich bleiben. Was darüber hinaus ohne Not sicherheitsrelevantes Lagewissen erzeugt, gehört neu bewertet“*, erklärt Peglow.

Informationsresilienz gehört zur Inneren Sicherheit

Der BDK fordert deshalb, Informationsresilienz als Bestandteil der Inneren Sicherheit und der Gesamtverteidigung zu etablieren. Bund und Länder sollten gemeinsame Standards für Mosaikprüfungen entwickeln, geeignete KI-Unterstützung aufbauen und besonders relevante Informationsräume durch Informations-Red-Teaming untersuchen.

Notwendig ist dabei eine ressortübergreifende Perspektive. Gerade der BDK-Test zeigt, dass das sicherheitsrelevante Gesamtbild nicht zwingend innerhalb eines Ressorts oder einer einzelnen Datenbank entsteht. Es kann sich erst aus Veröffentlichungen unterschiedlicher Parlamente, Behörden, öffentlicher Unternehmen und Rechtsgebiete ergeben. Die Sicherheitsbewertung muss deshalb dort zusammengeführt werden, wo auch diese Beziehungen sichtbar werden können.

Parallel dazu gehört die bestehende Veröffentlichungsarchitektur auf den Prüfstand. Denn moderne Resilienz kann nicht allein bedeuten, Anlagen physisch zu härten, IT-Systeme gegen Cyberangriffe zu schützen und Reaktionsfähigkeit für den Krisenfall aufzubauen. Sie muss bereits bei der Frage beginnen, welches Wissen über diese Strukturen der Staat selbst öffentlich erzeugt.

Gesamtverteidigung funktioniert ressortübergreifend. Kriminalistische Analyse funktioniert quellenübergreifend. Informationsschutz muss beides ebenfalls können. Der Staat muss deshalb nicht alles geheim halten. Er muss aber aufhören, maximale Informationsverfügbarkeit mit notwendiger Transparenz gleichzusetzen. Die kriminalpolizeiliche Logik dahinter ist einfach: Nicht der einzelne Mosaikstein entscheidet über den Erkenntniswert. Entscheidend ist das Bild, das sich daraus zusammensetzen lässt.

Dieses Bild muss der Staat künftig selbst kennen, bevor andere es für ihn zusammensetzen.
Schlagwörter
Bund KI
diesen Inhalt herunterladen: PDF