ASSESSMENT PAPER

FACHLICHE EINORDNUNG DER POINT OF RESOLUTION GMBH · AUSGABE 01 / 2026

SICHERHEIT · KRITISCHE INFRASTRUKTUR · ANALYSE

Hybride Bedrohungen und kritische Infrastrukturen

Begriffe, Analysegrenzen, Indikatoren und Konsequenzen für Betreiber

GEGENSTAND	Fachliche Einordnung öffentlich verfügbarer sicherheitspolitischer und analytischer Quellen, übertragen auf Betreiber kritischer und verteidigungswichtiger Infrastruktur – ohne Veröffentlichung operativ nutzbarer Schwachstellen- oder Angriffsinformationen.
STAND	20. September 2026
VERSION	1.1
DOKUMENTTYP	Fachliche Einordnung
AUSSAGEEBENE	Strategisch · operativ · technisch
QUELLENBASIS	BMVg · bpb · Atlantik-Brücke · BKA · POR
STATISTIK	Keine Ereignis- oder Fallstatistik

> **LEITGEDANKE DIESER EINORDNUNG**
>
> *Nicht jede Störung ist Sabotage. Nicht jede Auffälligkeit ist eine Bedrohung. Entscheidend ist, was verifiziert werden kann – und welche Bedeutung es für die kritische Funktion hat.*

00

HINWEISE ZUR INTERPRETATION

Was dieses Dokument leistet – und was nicht

Die Darstellungslogik trennt Quellenlage, Definitionsrahmen, Befund, Einschränkungen und Konsequenzen konsequent voneinander.

PUNKT	EINORDNUNG
Kein Lagebild	Dieses Dokument stellt kein behördliches oder nachrichtendienstliches Lagebild dar und erhebt keinen Anspruch auf Vollständigkeit des tatsächlichen Bedrohungsgeschehens.
Keine Häufigkeitsaussage	Die Quellen erlauben keine belastbare Aussage darüber, wie häufig hybride Vorfälle in Deutschland auftreten. Einzelbeispiele sind keine statistische Verteilung.
Quellen mit unterschiedlicher Funktion	BMVg liefert den sicherheitspolitischen Rahmen, die bpb methodische Konfliktanalyse, die Atlantik-Brücke eine Betreiberperspektive; POR überträgt diese Ansätze auf technische Infrastruktur.
Attribution getrennt behandeln	Ein technischer oder physischer Befund beweist weder Absicht noch Urheberschaft. Ursache, Motiv und Akteur sind eigene Analysefragen.
Schutz der Informationssicherheit	Konkrete Schwachstellen, Umgehungsmöglichkeiten, Zugangspfade und Angriffsschritte werden nicht dargestellt.
Keine Rechtsberatung	Regulatorische Bezüge dienen der Einordnung. Betreiberpflichten sind im Einzelfall anhand der geltenden Rechtslage zu prüfen.

LESESCHLÜSSEL

QUELLENAUSSAGE: Aussage der Quelle. POR-EINORDNUNG: analytische Übertragung. METHODISCHE FOLGERUNG: abgeleitete Arbeitsregel.

WARUM DIE BKA-LOGIK ALS FORMALE REFERENZ PASST

Die Polizeiliche Kriminalstatistik trennt Datenbestand, Interpretationshinweise, Tabellenbeschreibung und Auswertung. Für hybride Bedrohungen ist dieselbe Disziplin nötig – mit einem Unterschied: Eine vergleichbare Vollerhebung liegt hier nicht vor.

KURZFASSUNG

Sechs Kernaussagen

Die Auswertung verdichtet sich auf sechs Punkte mit unmittelbarer Bedeutung für Lageverständnis, Resilienz und Entscheidungsfähigkeit von Betreibern.

01 **Hybride Bedrohungen sind Kombinationen.**

Die BMVg-Darstellung beschreibt das Zusammenspiel militärischer, wirtschaftlicher, cyberbezogener und informationeller Mittel. Eine siloartige Betrachtung ist für Betreiber deshalb unzureichend.

02 **Kritische Infrastruktur ist Funktionsraum, nicht nur Objekt.**

Sicherheit entsteht nicht allein am Standort. Entscheidend sind technische Funktionen, vor- und nachgelagerte Abhängigkeiten, Betriebsprozesse und die Fähigkeit, relevante Veränderungen rechtzeitig zu erkennen.

03 **Attribution ist nachgelagert.**

Verschleierung und uneindeutige Urheberschaft sind Kernelemente hybrider Vorgehensweisen. Ein Betreiber muss dennoch entscheiden können, bevor ein Akteur sicher zugeordnet ist.

04 **Baseline schlägt Bauchgefühl.**

Eine Auffälligkeit wird erst im Verhältnis zu einem erwarteten Normalzustand aussagekräftig. Einzelindikatoren benötigen Kontext und möglichst eine zweite, unabhängige Quelle.

05 **Resilienz ist ein Zyklus.**

Vorbereitung, Beobachtung, Verifikation, Bewertung, Entscheidung, Wiederherstellung und Review bilden einen wiederkehrenden Prozess – kein einmaliges Sicherheitsprojekt.

06 **Öffentliche Fachkommunikation braucht Grenzen.**

Eine belastbare Einordnung darf Schutzbedarf, Abhängigkeiten und Analyseprinzipien erklären, ohne konkrete Schwachstellen oder nutzbare Angriffsmöglichkeiten offenzulegen.

01

QUELLENLAGE

Vier Perspektiven, unterschiedliche Aussagekraft

Die Quellen beantworten nicht dieselbe Frage. Ihre Stärke liegt in der Kombination – sofern die jeweilige Rolle transparent bleibt.

QUELLE	FUNKTION, STÄRKE UND GRENZE
BMVg · Was sind hybride Bedrohungen?	Offizieller sicherheitspolitischer Rahmen: Definition, Verschleierung, kritische Infrastruktur, Resilienz, Integrierte Sicherheit. Grenze: keine Betreiberstatistik, keine technische Detailanalyse.
BMVg 2016 · Hybride Kriegsführung	Historische und strategische Kontextualisierung: Informationsraum, Propaganda, Plausible Deniability, Medienvertrauen. Grenze: älterer Kontext, kein aktuelles Lagebild.
bpb · Kriege und Konflikte	Methodische und politische Bildung: Trennung von sichtbarem Verhalten und latenten Interessen, Vorsicht bei Motiven und Kategorisierung. Grenze: nicht auf KRITIS-Betrieb zugeschnitten.
Atlantik-Brücke · Rohé 2026	Industrie- und Betreiberperspektive: Verbindung physischer, digitaler und menschlicher Risiken, Führungsverantwortung, Resilienz. Grenze: Autorenbeitrag, keine amtliche Bewertung.
POR · Mission Brief 05	Sektorspezifische operative Übertragung: Baseline, Indikatoren, Abhängigkeiten und Mission-Logik am Beispiel Wasser und Abwasser. Grenze: eigene Analyse, sektorbezogen.

BEWERTUNGSREGEL

Je stärker eine Aussage in Richtung konkreter Bedrohungslage, Häufigkeit oder Urheberschaft geht, desto höher muss die Evidenzschwelle sein. Strategische Definitionen sind kein Nachweis eines konkreten Ereignisses.

02

BEGRIFFLICHE EINORDNUNG

Hybrid beschreibt die Kombination – nicht automatisch den Krieg

Arbeitsdefinitionen dieser Publikation. Sie sind bewusst enger gefasst als der politische Sprachgebrauch.

BEGRIFF	ARBEITSDEFINITION IN DIESER PUBLIKATION
Hybride Bedrohung	Koordinierte oder kombinierte Nutzung unterschiedlicher Einfluss-, Störungs- oder Druckmittel, deren Zusammenwirken Sicherheit, Handlungsfähigkeit oder Vertrauen beeinträchtigen kann.
Hybride Kriegsführung	Strategischer Begriff für die Verbindung militärischer und nichtmilitärischer Mittel in Konflikt- oder Kriegskontexten. Für Betreiberkommunikation zurückhaltend zu verwenden.
Kritische Funktion	Die konkrete Leistung, deren Ausfall erhebliche Folgen für Versorgung, Sicherheit, Betrieb oder verbundene Systeme auslöst.
Anomalie	Abweichung vom erwarteten technischen, betrieblichen, physischen oder informationsbezogenen Normalbild. Eine Anomalie ist noch keine Bedrohung.
Attribution	Begründete Zuordnung eines Ereignisses zu Ursache, Absicht oder Akteur – getrennt von der Feststellung des Ereignisses und seiner Wirkung.
Resilienz	Fähigkeit, Störungen vorzubereiten, zu erkennen, Auswirkungen zu begrenzen, kritische Funktionen aufrechtzuerhalten oder wiederherzustellen und aus dem Ereignis zu lernen.

POR ARBEITSGRUNDSATZ

POR beginnt nicht mit der Annahme einer Bedrohung. POR beginnt mit der kritischen Funktion, ihrem erwarteten Zustand und der verifizierbaren Veränderung dieses Zustands.

03

ANALYSEDIMENSIONEN

Ein Lagebild entsteht zwischen den Silos

Die folgenden Dimensionen sind keine Angriffstypologie. Sie strukturieren, welche Informationsräume für eine belastbare Bewertung zusammengeführt werden müssen.

DIMENSION	BEOBACHTUNGSGEGENSTAND UND BETREIBERFRAGE
Technisch	Anlagenzustand, Prozesse, Messwerte, Funktionsketten, Alterung. Leitfrage: Was funktioniert – und was hat sich verändert?
Physisch	Standort, Zugang, Umfeld, sichtbare Veränderungen, Ereignisspuren. Leitfrage: Gibt es eine physische Veränderung mit Betriebsrelevanz?
Digital / OT	Verfügbarkeit, Steuerungs- und Fernwirkbezug, Systemereignisse. Leitfrage: Ist die Funktion beeinträchtigt – oder nur ihre Sichtbarkeit?
Information	Öffentlich verfügbare Hinweise, Meldungen, Narrative, externe Ereignisse. Leitfrage: Welche externe Information verändert die Bewertung, und wie verlässlich ist sie?
Human / Organisation	Betriebswissen, Beobachtungen, Rollen, Dienstleister, Entscheidungswege. Leitfrage: Wer weiß was, wer entscheidet, welche Abhängigkeit ist personell?
Geospatial	Räumliche Beziehungen, Netze, Zonen, Zugänglichkeit. Leitfrage: Wo liegt die Abweichung im Verhältnis zur kritischen Funktion?
Wirtschaft / Lieferkette	Ersatzteile, Energie, Dienstleister, Beschaffung. Leitfrage: Welche Funktion fällt aus, wenn ein externer Input fehlt?

> **QUELLENAUSSAGE BMVG**
>
> *Das BMVg beschreibt hybride Taktiken ausdrücklich als Kombination klassischer militärischer Mittel mit wirtschaftlichem Druck, Cyberangriffen und Informationsbeeinflussung. Kritische Infrastrukturen werden als mögliche Ziele benannt.*

04

KRITISCHE INFRASTRUKTUR

Die kritische Funktion ist der Analyseanker

Ein Standort kann geschützt sein und trotzdem ausfallen. Ein Ereignis am Rand eines Systems kann gravierende Folgen im Kern erzeugen.

01	02	03	04	05	06
Funktion	Komponenten	Abhängigkeiten	Baseline	Abweichung	Wirkung

ANALYSEEBENE	LEITFRAGE UND ERGEBNIS
Funktion	Welche Leistung muss unter welchen Mindestbedingungen erhalten bleiben? Ergebnis: priorisierte kritische Funktion.
System	Welche technischen und organisatorischen Komponenten tragen diese Leistung? Ergebnis: Funktionskette und Systemmodell.
Abhängigkeit	Wovon hängt die Funktion intern und extern ab? Ergebnis: Versorgungs-, Kommunikations-, Personal- und Lieferkettenbezug.
Sichtbarkeit	Welche Zustände sind direkt messbar, welche nur indirekt erschließbar? Ergebnis: Sensor-, Daten- und Informationsmodell.
Fallback	Was bleibt sichtbar und steuerbar, wenn ein primäres System ausfällt? Ergebnis: Rückfallebene und Ersatzlagebild.
Entscheidung	Wer darf bei unvollständiger Information welche Maßnahme auslösen? Ergebnis: Entscheidungs- und Eskalationslogik.

POR-EINORDNUNG

Schutzkonzepte, die ausschließlich vom Objekt ausgehen, erfassen Kaskaden nur unzureichend. Betreiber benötigen zusätzlich ein Modell der kritischen Funktion, ihrer Abhängigkeiten und derjenigen Signale, die eine relevante Zustandsänderung sichtbar machen.

05

ATTRIBUTION UND UNSICHERHEIT

Entscheiden, bevor die Urheberschaft geklärt ist

Verschleierung ist ein wesentliches Merkmal hybrider Vorgehensweisen. Ereignisfeststellung, Ursachenanalyse, Absicht und Akteur müssen getrennt dokumentiert werden.

OBSERVATION ≠ CAUSATION ≠ ATTRIBUTION

EBENE	WAS SICH FRAGEN LÄSST – UND WAS DARAUS NOCH NICHT FOLGT
Observation	Was wurde wann und wo beobachtet oder gemessen? Noch keine Aussage über Ursache oder Absicht.
Verification	Ist die Beobachtung belastbar, reproduzierbar oder durch eine zweite Quelle bestätigt? Keine automatische Kausalität.
Correlation	Treten mehrere Befunde zeitlich, räumlich oder funktional gemeinsam auf? Korrelation beweist keine gemeinsame Ursache.
Assessment	Welche Erklärungen passen zu den verifizierten Befunden und zur Systemlogik? Bewertung ist nicht identisch mit Attribution.
Attribution	Welche Ursache oder welcher Akteur lässt sich mit welcher Evidenz zuordnen? Restunsicherheit bleibt auszuweisen.
Decision Relevance	Welche Maßnahme ist unabhängig von der Attribution erforderlich? Die Entscheidung darf nicht unnötig auf die Täterzuordnung warten.

METHODISCHE FOLGERUNG AUS DER BPB-KONFLIKTANALYSE

Sichtbares Verhalten ist leichter festzustellen als Interessen, Ziele und Motive. Über die latente Ebene kann häufig nur mit Unsicherheit geschlossen werden. Für technische Lagen heißt das: erst Ereignis und Wirkung stabil beschreiben, dann Hypothesen prüfen.

06

POR ANALYSEMODELL

Vom Signal zur Entscheidung

Das Modell verbindet die in den Quellen wiederkehrenden Anforderungen an Früherkennung, Analyse und Resilienz mit einer technischen Betreiberlogik.

01	02	03	04
Baseline	**Observe**	**Detect**	**Verify**
05	06	07	08
Correlate	**Assess**	**Decide**	**Review**

SCHRITT	ZWECK
BASELINE	Erwarteten Zustand, Betriebsmodi und bekannte Schwankungsbreiten der kritischen Funktion dokumentieren.
OBSERVE	Technische, physische, räumliche und kontextuelle Informationen erfassen.
DETECT	Relevante Abweichungen vom Normalbild identifizieren – ohne vorschnelle Interpretation.
VERIFY	Quelle, Plausibilität und technische Konsistenz prüfen; wenn möglich eine zweite unabhängige Evidenz heranziehen.
CORRELATE	Zusammenhänge zwischen mehreren Beobachtungen prüfen und alternative Erklärungen offenhalten.
ASSESS	Auswirkung auf Funktion, Betrieb, Sicherheit und Resilienz bewerten; Unsicherheit explizit angeben.
DECIDE	Entscheidungsbedarf, Eskalationsstufe und mögliche Schutz- oder Stabilisierungsoptionen darstellen.
REVIEW	Nach Ereignis oder Übung Baseline, Indikatoren, Schwellen, Zuständigkeiten und Maßnahmen anpassen.

07

STATUSSPRACHE UND CONFIDENCE

Vier Statusstufen statt vorschneller Gewissheit

Status beschreibt den Reifegrad einer Information. Confidence beschreibt die Belastbarkeit einer Bewertung. Beides ist getrennt zu dokumentieren.

STATUS	BEDEUTUNG UND BEISPIELHAFTE AUSSAGEFORM
SIGNAL	Rohhinweis oder einzelne Beobachtung mit möglicher Relevanz. Aussageform: „Abweichung erkannt; Validierung läuft.“
VERIFIED	Beobachtung technisch oder durch unabhängige Quelle bestätigt. Aussageform: „Zustandsänderung bestätigt; Ursache offen.“
ASSESSED	Verifizierte Befunde sind in System- und Kontextlogik eingeordnet. Aussageform: „Technischer Defekt ist derzeit plausibler als externe Einwirkung.“
DECISION RELEVANT	Die Lage erfordert eine betriebliche oder organisatorische Entscheidung, auch wenn die Attribution offen bleibt. Aussageform: „Kritische Funktion gefährdet; Fallback aktivieren.“

CONFIDENCE	ARBEITSDEFINITION
NIEDRIG	Wenige oder indirekte Quellen; wesentliche Alternativerklärungen offen; Ergebnis vorläufig.
MITTEL	Mehrere stützende Befunde; Alternativen geprüft, aber nicht vollständig ausgeschlossen.
HOCH	Mehrere unabhängige und konsistente Evidenzlinien; wesentliche Alternativen weitgehend ausgeschlossen.

GOVERNANCE

Confidence ist kein Prozentwert und keine Behauptung mathematischer Sicherheit. Sie dokumentiert nachvollziehbar, wie belastbar eine Bewertung angesichts der verfügbaren Evidenz ist.

08

FRÜHERKENNUNG

Baseline vor Schwellenwert

Frühwarnung beginnt nicht mit einer Liste vermeintlicher Angriffe, sondern mit der Frage, welche Zustandsänderung bei einer konkreten Funktion überhaupt beobachtbar wäre.

INDIKATORGRUPPE	BEOBACHTBARE GRÖSSEN UND BEWERTUNGSPRINZIP
Technischer Prozess	Drücke, Durchflüsse, Temperaturen, Laufzeiten, Verfügbarkeiten, Qualitätsparameter. Bewertung: Abweichung vom erwarteten Betriebsmodus.
Energie / Versorgung	Last, Netzqualität, Notversorgung, Betriebsstoff- und Ersatzteilverfügbarkeit. Bewertung: funktionale Auswirkung statt isolierter Einzelwert.
Zugang / Umfeld	Veränderungen an Außenstandorten, Zugängen und Umfeld. Bewertung: Abgleich mit Betriebs- und Wartungsplanung.
Digital / Fernwirkung	Kommunikationsverfügbarkeit, Parameteränderungen, Fernzugriff, Systemereignisse. Bewertung: IT/OT-Kontext und bekannte Wartungsfenster berücksichtigen.
Baulich / räumlich	Zustandsänderungen, Setzungen, Zugänglichkeit, räumliche Muster. Bewertung: historischen Zustand und Geometrie als Baseline nutzen.
Extern / OSINT	Öffentliche Meldungen, Ereignisse, Störungen, relevante Narrative. Bewertung: Quelle, Aktualität, Unabhängigkeit und Funktionsbezug prüfen.

SEKTORBEISPIEL WASSER & ABWASSER

Im POR Mission Brief 05 werden hydraulische, bauliche, qualitative, energetische, zugangsbezogene und digitale Indikatoren getrennt betrachtet. Kein Indikator ist für sich aussagekräftig; relevant ist die Abweichung vom erwarteten Normalbild und die Bestätigung durch eine zweite Quelle.

09

INTEGRIERTES LAGEBILD

Informationsfusion mit klaren Grenzen

Der Ansatz der Integrierten Sicherheit im staatlichen Kontext ist breiter als die Rolle eines einzelnen Betreibers. Auf Betreiberseite lässt sich das Prinzip als integrierte Analyse relevanter Informationsräume übersetzen.

INPUT	BEITRAG ZUM LAGEBILD UND QUALITÄTSSICHERUNG
Technische Daten	Zustand und Funktion. Qualitätssicherung: Plausibilisierung, Zeitbezug, Sensor- und Datenqualität.
Physische Beobachtung	Umfeld und sichtbare Veränderungen. Qualitätssicherung: Dokumentation, Ort und Zeit, Vergleich mit dem Normalzustand.
GIS / 3D / UAV	Räumlicher Zusammenhang. Qualitätssicherung: Georeferenz, Aktualität, rechtmäßige Erhebung.
OSINT	Externer Kontext. Qualitätssicherung: Quellenkritik, Cross-Check, keine Gleichsetzung von Reichweite und Wahrheit.
Betriebswissen	Erfahrungswissen, Abläufe, Beobachtungen. Qualitätssicherung: Quellenrolle, mögliche Verzerrung, Need-to-Know.
IT/OT-Kontext	Digitale Abhängigkeit und Sichtbarkeit. Qualitätssicherung: Zuständigkeit, Logging, Trennung von Befund und Cyber-Attribution.

POR DATA-MINIMISATION-PRINZIP

Das Ziel ist nicht maximale Datensammlung. Das Ziel ist die minimale, belastbare Informationsbasis, die eine verantwortliche Entscheidung ermöglicht.

ABGRENZUNG

POR beschreibt keinen staatlichen Gesamtverteidigungsansatz und ersetzt weder Behördenlagebilder noch spezialisierte Cyber-Forensik. Die Rolle liegt in der technischen und operativen Zusammenführung von Informationen dort, wo sie für die kritische Funktion entscheidungsrelevant sind.

10

RESILIENZ

Resilienz beginnt vor dem Ereignis

Die BMVg-Ausführungen benennen Resilienz als zentrale Antwort auf hybride Bedrohungen. Für Betreiber lässt sich daraus ein kontinuierlicher Fähigkeitszyklus ableiten.

01 **Understand**	02 **Baseline**	03 **Observe**	04 **Prepare**
05 **Respond**	06 **Recover**	07 **Review**	

PHASE	OPERATIVE KERNFRAGE
UNDERSTAND	Welche kritischen Funktionen, Mindestleistungen und Abhängigkeiten müssen verstanden sein?
BASELINE	Wie sieht der erwartete Zustand in verschiedenen Betriebsmodi aus?
OBSERVE	Welche Veränderungen können wir mit vertretbarem Aufwand und rechtmäßig erkennen?
PREPARE	Welche Rollen, Rückfallebenen, Kommunikationswege und Ressourcen sind vorab geklärt?
RESPOND	Wie stabilisieren wir die Funktion, während Ursache und Attribution noch geprüft werden?
RECOVER	Wie stellen wir priorisierte Leistungen kontrolliert und dokumentiert wieder her?
REVIEW	Welche Annahmen, Indikatoren und Maßnahmen müssen nach Ereignis oder Übung angepasst werden?

FÜHRUNGSAUFGABE

Die Atlantik-Brücke-Perspektive betont Resilienz als Management- und Führungsaufgabe. Für Betreiber heißt das nicht, operative Technik in die Vorstandsebene zu verlagern, sondern Entscheidungsfähigkeit, Rollen, Eskalationswege und Prioritäten verbindlich zu machen.

11

KONSEQUENZEN FÜR BETREIBER

Die belastbare Mindestfähigkeit

Nicht jeder Betreiber benötigt eine große Sicherheitsorganisation. Jede kritische Funktion benötigt jedoch ein Mindestmaß an vorbereitetem Wissen, Sichtbarkeit und Entscheidungsfähigkeit.

01 **Kritische Funktionen priorisieren.**

Nicht „die Anlage“ schützen, sondern festlegen, welche Leistung unter Störung zuerst erhalten oder wiederhergestellt werden muss.

02 **Abhängigkeiten dokumentieren.**

Energie, Kommunikation, Personal, Dienstleister, Lieferketten und nachgelagerte Nutzer in einer funktionsbezogenen Übersicht führen.

03 **Baseline definieren.**

Normalzustände, Betriebsmodi, bekannte Schwankungen und Wartungsfenster so dokumentieren, dass Abweichungen objektivierbar werden.

04 **Ersatzlagebild vorbereiten.**

Festlegen, welche Information bei Ausfall von Telemetrie, IT oder Kommunikation noch verfügbar ist – und wie sie erhoben wird.

05 **Status- und Eskalationssprache vereinheitlichen.**

SIGNAL, VERIFIED, ASSESSED und DECISION RELEVANT sowie klare Confidence-Angaben verhindern Sprachverwirrung im Ereignis.

06 **Üben und reviewen.**

Tabletop, technische Drills und After Action Review auf Entscheidungsfähigkeit ausrichten – nicht auf perfekte Drehbücher.

SICHERHEITSGRENZE DIESER PUBLIKATION

Diese Einordnung benennt bewusst keine objektspezifischen Angriffspfade, Schwachstellenkombinationen, Zugriffstechniken oder Umgehungsmethoden. Tiefergehende technische Analysen gehören in einen legitimierten, vertraulichen Auftrag mit Need-to-Know-Prinzip.

12

POR CAPABILITY MAPPING

Drei Capabilities, ein Analyse- und Resilienzziel

Observation, Assessment und Action bleiben methodisch getrennt, greifen im Mission Cycle aber ineinander.

CAPABILITY	PRIMÄRER BEITRAG UND TYPISCHE OUTPUTS
DARK DALOS	Technische Aufklärung und persistente Beobachtung in schwer zugänglichen oder lagekritischen Umgebungen. Outputs: verifizierte Beobachtung, Zustandsdokumentation, zeitlicher Verlauf, Sensor- und Bildlage.
RISK INTELLIGENCE	Korrelation technischer, räumlicher, physischer und kontextueller Informationen. Outputs: integriertes Lagebild, Hypothesenprüfung, Confidence, Entscheidungsbedarf.
DIRECT ACTION	Preparedness, Koordination, Stabilisierung und Recovery im Rahmen der Betreiber- und Behördenzuständigkeiten. Outputs: Eskalationslogik, Maßnahmenkoordination, Ressourcenpriorisierung, Review.

01	02	03	04
Signal	**Verified**	**Assessed**	**Decision Relevant**

OPERATIVER GRUNDSATZ

Human Decision Authority bleibt erhalten. Automatisierte Systeme liefern Daten und Unterstützung, keine autonome Lageentscheidung.

DOMAINS

Das Modell ist sektorübergreifend anwendbar. Baseline, Indikatorik, Abhängigkeiten und Recovery-Logik müssen jedoch für jede Domain technisch neu hergeleitet werden. Eine generische Hybrid-Threat-Checkliste ersetzt keine Ingenieuranalyse.

13

SCHLUSSFOLGERUNG

Fachliche Einordnung statt Bedrohungsrhetorik

Die ausgewerteten Quellen verdichten sich zu einem konsistenten Befund: komplexe, schwer attribuierbare Bedrohungen verlangen integrierte Analyse und belastbare Resilienz – aber keine vorschnelle Dramatisierung einzelner Auffälligkeiten.

METHODISCHER KERN

Beobachtung ist nicht Interpretation. Korrelation ist nicht Kausalität. Auffälligkeit ist noch keine Bedrohung. Attribution erfordert zusätzliche Evidenz.

POR-FAZIT

Für Betreiber kritischer Infrastruktur ist die wichtigste Fähigkeit nicht, jeden Vorfall sofort einem Akteur zuzuordnen. Entscheidend ist, die eigene kritische Funktion zu verstehen, den Normalzustand zu kennen, relevante Abweichungen früh zu erkennen, Befunde zu verifizieren, Unsicherheit transparent zu machen und rechtzeitig eine verantwortliche Entscheidung zu ermöglichen.

QUELLEN UND DOKUMENTENBASIS

01 Bundesministerium der Verteidigung: „Was sind hybride Bedrohungen?“, Themenbereich Sicherheitspolitik, abgerufen am 20.09.2026.

02 Bundesministerium der Verteidigung: „Hybride Kriegsführung: Vertrauen in unsere Medien ist von strategischer Bedeutung“, 11.10.2016.

03 Bundeszentrale für politische Bildung: Dossier „Kriege und Konflikte“ sowie Lutz Schrader, „Was ist ein Konflikt?“, 17.07.2018; Dossier abgerufen am 20.09.2026.

04 Atlantik-Brücke e. V.: Benjamin Rohé, „Hybride Kriegsführung und kritische Infrastrukturen“, 18.03.2026.

05 POINT OF RESOLUTION: Mission Brief 05/2026, „Wasser & Abwasser – Sektoranalyse Kritische Infrastruktur“, September 2026.

06 Bundeskriminalamt: PKS-Darstellungs- und Interpretationslogik als formale Referenz; keine PKS-Falldaten verwendet.

PUBLIKATION

POINT OF RESOLUTION · Assessment Paper 01/2026 · Fachliche Einordnung Version 1.1
Stand 20.09.2026. Herausgeber: Ingo Zimmer, POINT OF RESOLUTION GmbH, Leipzig. Diese Publikation dient der fachlichen Einordnung und ersetzt weder behördliche Lagebilder noch Rechtsberatung oder objektspezifische Sicherheitsanalysen.