ANALYTISCHER FORSCHUNGSBERICHT · PHILOSOPHENSTUDIO

Gesamturteil zur Beweislage des Hybridkriegs

Rechtsstaatliche Gesamtanalyse oeffentlich zugaenglicher Quellen und Belege

Erstellt von: Christer Häberli

Datum: 8. Oktober 2026

Aktenzeichen: CHH-2026-GES-001

Status: Analytisches Arbeitsdokument

ANALYTISCHES DOKUMENT · KEIN AMTLICHER SCHRIFTSATZ

FÜHRT RUSSLAND NACHWEISLICH EINEN HYBRIDEN KRIEG GEGEN DEUTSCHLAND UND DEN WESTEN? EINE ABSCHLIESSENDE BEWEISBILANZ

Christer Häberli, October 08, 2026

GESAMTURTEIL IN EINEM ABSATZ

Russland führt nach der öffentlich zugänglichen Beweislage nachweislich einzelne geheimdienstliche, cybergestützte und informationspolitische Operationen gegen Deutschland und andere westliche Staaten durch oder lässt sie durch staatliche Stellen durchführen. Gerichtlich besonders belastbar sind mehrere konkrete Agenten- und Spionagefälle; offiziell attribuiert und durch technische Indizien erheblich gestützt sind insbesondere der Bundestag-Hack von 2015 sowie die Desinformationskampagne „Doppelgänger“. Nicht nachgewiesen ist dagegen eine einheitliche, zentral koordinierte russische Gesamtstrategie, in der sämtliche Cyberangriffe, Brandanschläge, Kabelschäden, Wahleinflüsse, Medieninhalte und Infrastrukturvorfälle als Teile eines einzigen vom Kreml geführten „hybriden Krieges“ zusammenlaufen. Für Nord Stream spricht die öffentliche deutsche Ermittlungsrichtung gerade nicht für Russland. Bei Ostsee-Kabelschäden, Telegram-Wegwerfagenten, pauschalen AfD-Finanzierungsvorwürfen und der Wirkung von Desinformation bleiben entscheidende Attributionsglieder offen. Das Ergebnis ist deshalb weder „alles Kreml-Propaganda“ noch „alles bewiesener russischer Hybridkrieg“ sondern abgestuft: Es gibt bewiesene russlandbezogene Einzeloperationen, starke amtliche Attributionen ohne Urteil, zahlreiche strukturell schwer beweisbare Vorgänge und eine politische Tendenz, diese heterogenen Sachverhalte unter einem weiter reichenden Gesamtbegriff zusammenzufassen, als es die öffentliche Beweislage zulässt.

1. BEGRIFF UND BEWEISMETHODIK

1.1 Operative Definition von „hybridem Krieg“

„Hybrider Krieg“ ist keine eigenständige strafrechtliche Kategorie. Der Begriff bezeichnet im Folgenden eine auf politische oder strategische Ziele ausgerichtete Kombination unterschiedlicher offener und verdeckter Mittel unterhalb, neben oder im Umfeld konventioneller militärischer Gewalt. Dazu können gehören:

- Spionage und geheimdienstliche Agententätigkeit;
- Cyberausspähung, Datenentwendung und digitale Sabotage;
- Vorbereitung oder Ausführung physischer Sabotage;
- verdeckte Rekrutierung von Hilfspersonen;
- Desinformation und Identitätstäuschung;
- verdeckte politische oder finanzielle Einflussnahme;
- wirtschaftlicher, diplomatischer und kommunikativer Druck.

Diese Definition enthält noch keine Aussage darüber, wer eine konkrete Handlung begangen hat. Sie darf insbesondere nicht so verwendet werden, dass der Oberbegriff die fehlende Beweisführung im Einzelfall ersetzt. Erst wenn mehrere Operationen zuverlässig einem Staat zugerechnet und ihre funktionale Koordination nachgewiesen werden, kann von einer staatlich koordinierten hybriden Kampagne gesprochen werden. Der bloße Umstand, dass verschiedene Ereignisse russischen Interessen nützen könnten, genügt nicht.

Auch der Ausdruck „Krieg“ ist mit Vorsicht zu verwenden. Spionage, Desinformation, Sabotage und bewaffnete Gewalt unterscheiden sich nach Ziel, Wirkung und Rechtslage. Politisch kann eine langfristige Mischung dieser Mittel als „hybrider Krieg“ bezeichnet werden. Dieser Sprachgebrauch beweist aber weder einen bewaffneten Konflikt noch eine zentrale Befehlskette. Er ist eine strategische Deutung, keine Tatsachenfeststellung.

1.2 Die fünf Ebenen der Zuschreibung

Jeder Fall wird auf fünf getrennten Ebenen geprüft:

1. **Ereignis:** Hat der Angriff, die Ausspähung, Zahlung oder Beschädigung stattgefunden?
2. **Unmittelbarer Täter:** Welche Person oder operative Gruppe führte die Handlung aus?

3. **Technische oder organisatorische Zuordnung:** Welche Infrastruktur, Schadsoftware, Tarnorganisation oder Nachrichtendiensteinheit wurde verwendet?
4. **Staatliche Zurechnung:** Handelte ein russisches Staatsorgan oder eine Person in dessen Auftrag, unter dessen Weisung oder Kontrolle?
5. **Strategische Einordnung:** War die konkrete Tat Bestandteil einer zentral koordinierten Gesamtstrategie gegen Deutschland oder den Westen?

Diese Ebenen sind nicht austauschbar. Eine russische IP-Adresse beweist keinen russischen Operator. Ein als APT28 bezeichnetes Malware-Cluster beweist für sich allein keine GRU-Mitgliedschaft. Die Zugehörigkeit eines Täters zu einem Nachrichtendienst beweist noch keinen persönlichen Auftrag des russischen Präsidenten. Und eine staatlich zurechenbare Einzeloperation beweist noch keinen allumfassenden Gesamtplan.

1.3 Die verbindlichen Kategorien A, B und C

Dieser Bericht verwendet ausschließlich die verlangte Dreiteilung:

Kategorie A, gerichtlich bewiesen

Kategorie A setzt kumulativ voraus:

- ein Urteil liegt vor;
- der Täter oder die Täter sind identifiziert;
- der staatliche russische Auftrag oder Dienstbezug ist gerichtlich festgestellt.

Ein Urteil über Spionage „für Russland“ kann Kategorie A erfüllen, sofern der Auslandsdienstbezug Bestandteil der gerichtlichen Feststellungen ist. Ein Haftbefehl, eine Anklage oder ein Sanktionsbeschluss reicht nicht. Auch Kategorie A beweist nur die abgeurteilte Einzeloperation. Für die weitergehende Behauptung einer koordinierten Gesamtstrategie wäre ein zusätzlicher Nachweis erforderlich.

Kategorie B, offiziell attribuiert, nicht gerichtlich belegt

Kategorie B umfasst:

- konkrete Attributionen durch Bundesregierung, Auswärtiges Amt, Generalbundesanwalt, EU oder andere benannte staatliche Stellen;
- Anklagen und Haftbefehle;
- gerichtlich bestätigten dringenden Tatverdacht ohne Endurteil;
- administrative Sanktionen mit konkreter Verantwortungszuweisung.

Kategorie B kann sehr überzeugend sein. Sie bleibt aber unterhalb eines rechtskräftigen Schuldurteils. Zu prüfen ist stets, welche öffentliche Grundlage genannt wird, ob die Beweiskette unabhängig nachvollzogen werden kann und welches Glied für einen gerichtsfesten Staatsnachweis fehlt.

Kategorie C, strukturell unbeweisbar oder spekulativ

Kategorie C umfasst:

- bloße Behauptungen ohne veröffentlichte tragfähige Beweiskette;
- Fälle, in denen die Verbindung zwischen unmittelbarem Täter und russischem Staat nicht nachgewiesen ist;
- technische Indizien, die mehrere Täterschaftshypothesen zulassen;
- geheimdienstliche Bewertungen, deren entscheidende Grundlage öffentlich nicht überprüfbar ist;
- Vorgänge, bei denen Wegwerfkonten, Mittelsmänner oder unwissende Hilfspersonen die Befehlskette kappen.

„Strukturell unbeweisbar“ bedeutet nicht, dass eine behauptete russische Steuerung unmöglich oder widerlegt wäre. Es bedeutet, dass das entscheidende Bindeglied mit den öffentlich zugänglichen Mitteln nicht positiv bewiesen werden kann. Fehlende Beweise sind kein Freispruch; sie können aber auch keine positive Staatszuschreibung tragen.

1.4 Beweiswerte verschiedener Quellentypen

Ein rechtskräftiges Urteil besitzt den höchsten öffentlichen Beweiswert, ist aber auf den entschiedenen Sachverhalt begrenzt. Ein Haftbefehl bestätigt einen qualifizierten Tatverdacht, keine Schuld. Eine Anklage enthält die Darstellung der Staatsanwaltschaft und unterliegt der Unschuldsvermutung. Ein Sanktionsbeschluss ist eine administrative oder politische Attribution, kein Strafurteil.

Technische Forensik ist stark für Angriffspfad, Malware, Infrastruktur und wiederkehrende Verhaltensmuster. Sie wird schwächer, wenn aus diesen Spuren unmittelbar auf einen Staat geschlossen wird. Schadsoftware kann kopiert, Infrastruktur kompromittiert und Metadaten können manipuliert werden. Der Angriff „Olympic Destroyer“ zeigt, dass technische Merkmale gezielt so verändert werden können, dass sie auf einen anderen Akteur hindeuten. Daraus folgt die Pflicht zur Mehrquellenprüfung, nicht die Vermutung, jede Attribution sei eine Täuschung.

Nachrichtendienstliche Erkenntnisse können die tatsächlich stärksten Informationen enthalten. Weil Quellen und Methoden häufig geheim bleiben, kann die Öffentlichkeit ihre Zuverlässigkeit jedoch nicht selbst prüfen. Geheimhaltung ist eine reale Sicherheitsnotwendigkeit aber kein Beweisersatz. Die angemessene Formulierung lautet dann „amtlich attribuiert“ und nicht „öffentlich bewiesen“.

1.5 Symmetrischer Maßstab

Dieselben Regeln müssen für russische und westliche Handlungen gelten. Die dokumentierte NSA- und BND-Überwachung zeigt, dass auch westliche Staaten Partner ausspähen. Das deutsche Verfahren wegen der mutmaßlichen Überwachung Angela Merkels wurde eingestellt, weil der konkrete Vorgang nicht gerichtsfest bewiesen werden konnte. Zugleich belegten parlamentarische Untersuchungen erhebliche Kontrollmängel in der BND-NSA-Kooperation; Mitte 2015 wurden 39.082 problematische Selektoren identifiziert, von denen ungefähr 68,7 Prozent gegen Regierungsstellen in der EU gerichtet waren.

Diese westlichen Fälle widerlegen russlandbezogene Beweise nicht. Sie widerlegen aber die Vorstellung, amtliche westliche Zuschreibungen dürften ohne Prüfung als neutrale Tatsachen behandelt werden. Symmetrie bedeutet gleiche Beweisanforderungen, nicht die Behauptung, alle Akteure oder Wirkungen seien identisch.

2. ORIENTIERUNGSMATRIX

Behauptung oder Fall	Hauptkategorie	Sicher feststellbar	Quelle beziehungsweise Träger der Zuschreibung	Fehlendes Glied	Angemessene Schlussfolgerung
Bundestag-Hack 2015	**B**	Angriff, Eindringen und erheblicher Datenabfluss; technische Zuordnung zu APT28; Haftbefehl gegen Dmitry Badin	Bundesregierung, Auswärtiges Amt, deutsche Strafverfolgung, EU-Rat	Strafurteil gegen Badin; vollständig öffentliche Beweiskette vom Operator zum GRU-Auftrag	Starke amtliche GRU-Attribution aber nicht Kategorie A
Nord-Stream-Sabotage	**C** hinsichtlich Russland	Leitungen wurden vorsätzlich durch Explosionen beschädigt; deutsche Ermittlungen verfolgen ukrainische Verdächtige	Generalbundesanwalt und BGH hinsichtlich konkreter Verdächtiger	Endurteil; staatliche Befehlskette; positiver Beleg für Russland	Keine tragfähige Russland-Zurechnung
Balticconnector und weitere Kabelschäden	**C** hinsichtlich Russland	Beim Balticconnector wurde ein Schiffsanker als physische Ursache identifiziert	Finnische Ermittlungsbehörden	Vorsatz, Auftrag, russische staatliche Steuerung	Unfall, Fahrlässigkeit, private Sabotage und staatliche Sabotage bleiben zu trennen

Behauptung oder Fall	Hauptkategorie	Sicher feststellbar	Quelle beziehungsweise Träger der Zuschreibung	Fehlendes Glied	Angemessene Schlussfolgerung
Telegram-Agenten und Brandanschläge	**C** als Netzwerkaussage; einzelne Verfahren **A/B**	Einzelne Personen wurden wegen Agententätigkeit beziehungsweise Sabotageplanung verurteilt oder angeklagt	Deutsche Gerichte und Generalbundesanwalt	Rekrutierungskette von Wegwerfkonto oder Mittelsmann bis zu einem russischen Dienst	Einzeloperationen können bewiesen sein; ein umfassendes Telegram-Netzwerk meist nicht
RT, „Doppelgänger“, „Ghostwriter“	**B**	Staatlicher Medienbezug von RT; sichtbare Klonseiten und inauthentische Kampagnen; amtliche EU-Zuordnungen	EU-Rat, EEAS, Europäische Kommission	Gerichtliche Individualfeststellung und vollständige Befehlskette	Russische Informationsoperationen sind teilweise stark belegt aber nicht jeder Inhalt ist Desinformation
AfD-Finanzierung und Wahleinfluss	**C** für pauschale Finanzierung; **B** für bestimmte Einflusskampagnen	Auf Wahlen und demokratische Prozesse gerichtete Informationskampagnen existieren	EU-Institutionen bei „Doppelgänger“ und verwandten Netzwerken	Zahlungsnachweis an Partei, konkreter Empfänger, Gegenleistung, Urteil; messbarer Wahleffekt	Keine belastbare pauschale Finanzierungsaussage; Einflussabsicht ist nicht Wahlergebnis
Spionageverurteilungen in Deutschland	**A**	Mehrere identifizierte Personen wurden wegen Tätigkeit zugunsten russischer Stellen verurteilt	Deutsche Oberlandesgerichte und weitere Gerichte	Verbindung der Einzelfälle zu einer zentralen Gesamtstrategie	Russische Spionage in Deutschland ist nachgewiesen; ein Masterplan nicht
MH17	**C** für den hier zu prüfenden Gesamtstrategie-Schluss	Das vorliegende Material bezeichnet MH17 als stärkstes Einzelargument, liefert aber keine ausreichende fallbezogene Entscheidungsgrundlage für die strenge A-Schwelle	Niederländische und internationale Verfahren werden als maßgeblich vorausgesetzt	Im Material vollständig rekonstruierbare Urteilsfeststellungen zu staatlichem Auftrag sowie Übertragungsbrücke nach Deutschland	Selbst ein starker gerichtlicher MH17-Befund beweist nicht automatisch Operationen in Deutschland
NATO-Zusicherungen 1990	**C** als Beweis für russische Täterschaft; historischer Kontext belegt	Mündliche Zusicherungen einschließlich „not one inch“ sind dokumentiert; allgemeiner schriftlicher Erweiterungsverzicht fehlt	Archivunterlagen und Zwei-plus-Vier-Vertrag	Rechtlich bindende allgemeine Nicht-Erweiterungsklausel; Verbindung zu konkreten Taten	Vertrauensbruch ist politisch begründbar aber weder Rechtfertigung noch Täterschaftsnachweis

Die Matrix macht den Kernbefund sichtbar: Die stärkste Kategorie A findet sich vor allem bei klassischer Agententätigkeit. Die prominentesten Cyber- und Informationsfälle liegen in Kategorie B. Gerade die politisch spektakulären Infrastruktur- und Parteienvorwürfe fallen dagegen überwiegend in Kategorie C.

3. EINZELPRÜFUNG 1: CYBERANGRIFFE, BUNDESTAG-HACK 2015 UND APT28

Hauptkategorie: B, offiziell attribuiert, nicht gerichtlich belegt

3.1 Was sicher feststeht

Im April und Mai 2015 wurde die IT-Infrastruktur des Deutschen Bundestages kompromittiert. Der Angriff begann nach den ausgewerteten Darstellungen mit Spear-Phishing, also gezielt präparierten Nachrichten, die als Mitteilungen der Vereinten Nationen erschienen. Nach dem Anklicken eines Links wurde Schadsoftware installiert. Die Angreifer verschafften sich Zugang zu internen Systemen und entwendeten ungefähr 16 Gigabyte Daten, darunter E-Mail-Bestände.

Diese Tatsachen belegen den Angriff, den Datenabfluss und einen erheblichen Spionageschaden. Sie sagen zunächst nichts über den Staat hinter der Operation.

3.2 Technische Zuordnung zu APT28

APT28, auch Fancy Bear, Sofacy, Pawn Storm oder Strontium genannt, ist eine technische Clusterbezeichnung. Sie fasst Operationen anhand wiederkehrender Infrastruktur, Schadsoftware, Ziele und Arbeitsweisen zusammen. Im Bundestag-Fall wurden Übereinstimmungen mit der „Scaramouche“-Malwarefamilie, APT28-typischen Werkzeugen und bekannten Vorgehensweisen festgestellt.

Die technische Clusterzuordnung ist substanziell aber nicht exklusiv. Phishing wird von vielen Akteuren verwendet. Malware kann kopiert werden. Server können von Dritten übernommen sein. Zeitstempel und Spracheinstellungen lassen sich manipulieren. Erst die Kombination zahlreicher langfristig stabiler Merkmale erhöht den Beweiswert.

Der dokumentierte False-Flag-Fall „Olympic Destroyer“ zeigt, warum ein scheinbar eindeutiger Codefingerabdruck nicht allein tragen darf: Dort wurden technische Merkmale manipuliert, um unter anderem eine Verbindung zur nordkoreanisch zugeschriebenen Lazarus-Gruppe vorzutäuschen. Für den Bundestag-Hack ist damit keine konkrete False Flag bewiesen. Der Fall zeigt nur, dass die Attribution mehr als Malwareähnlichkeit benötigt.

3.3 Offizielle Attribution an den GRU

Die Bundesregierung und das Auswärtige Amt ordneten den Bundestag-Angriff dem russischen Militärnachrichtendienst GRU und dessen Einheit 26165 zu. Das Auswärtige Amt bestellte im Mai 2020 den russischen Botschafter ein und erklärte, es gebe belastbare Hinweise auf die Beteiligung Dmitry Badins und des GRU. Gegen Badin wurde am 29. April 2020 ein Haftbefehl wegen geheimdienstlicher Agententätigkeit und Datenausspähung erlassen. Der EU-Rat verhängte im Oktober 2020 Sanktionen gegen Badin, GRU-Chef Igor Kostyukov und die Einheit 26165.

Damit liegt mehr vor als eine politische Vermutung:

- ein technisch identifiziertes Aktivitätscluster;
- eine konkrete russische Militäreinheit;
- ein namentlich bezeichneter Beschuldigter;
- ein deutscher Haftbefehl;
- eine diplomatische Attribution;
- ein EU-Sanktionsbeschluss.

Die öffentliche Beweiskette bleibt dennoch unvollständig. Nicht sämtliche forensischen Rohdaten, Partnerinformationen und nachrichtendienstlichen Grundlagen wurden veröffentlicht. Ein deutsches Strafurteil gegen Badin liegt im Material nicht vor.

3.4 Was der Fall beweist und was nicht

Der Fall beweist in Kategorie B, dass deutsche und europäische Behörden einen schweren Cyberangriff auf das Parlament konkret dem GRU zuschreiben und diese Zuschreibung durch personenbezogene Ermittlungen und technische Indizien stützen. Er ist einer der stärksten öffentlich dokumentierten Fälle russischer Cyberaktivität gegen Deutschland.

Er beweist nicht:

- die strafrechtliche Schuld Badins nach Hauptverhandlung;
- die vollständige operative Befehlskette;
- eine persönliche Anordnung Wladimir Putins;
- dass jeder APT28 zugerechnete Angriff tatsächlich von denselben Personen ausgeführt wurde;
- dass der Bundestag-Hack Teil eines gerichtlich festgestellten Gesamtplans gegen den gesamten Westen war.

3.5 Teilurteil

Der Bundestag-Hack rechtfertigt die Formulierung: „Deutschland hat den Angriff nach technischen und nachrichtendienstlichen Ermittlungen dem GRU zugeschrieben; gegen einen mutmaßlichen GRU-Offizier besteht ein Haftbefehl.“ Nicht gerechtfertigt ist: „Ein deutsches Gericht hat bewiesen, dass Russland den Bundestag-Hack beging.“

Als Beleg für eine russische hybride Praxis ist der Fall stark. Als Beleg für eine zentral koordinierte Gesamtstrategie ist er ein gewichtiges Einzelindiz aber kein Vollbeweis.

4. EINZELPRÜFUNG 2: NORD-STREAM-SABOTAGE

Hauptkategorie: C, eine russische Täterschaft ist öffentlich nicht belegt

4.1 Gesicherter Kern

Im September 2022 wurden Nord Stream 1 und 2 durch Explosionen beschädigt. Vier Lecks entstanden an drei der vier Leitungsstränge. Die öffentliche deutsche Ermittlungsrichtung konzentrierte sich auf die Segelyacht *Andromeda* und mehrere ukrainische Staatsangehörige. Es wurden Haftbefehle erlassen und Verdächtige festgenommen.

Am 10. Dezember 2025 verwarf der Bundesgerichtshof die Haftbeschwerde eines Beschuldigten. Er bejahte deutschen Strafanspruch und dringenden Tatverdacht wegen verfassungsfeindlicher Sabotage in Tateinheit mit dem Herbeiführen einer Sprengstoffexplosion. Der Betroffene soll als Offizier einer ukrainischen Spezialeinheit eine koordinierende Rolle gespielt haben. Der BGH verneinte für einen verdeckten Gewaltakt gegen zivile Infrastruktur funktionelle Immunität und ein Kombattantenprivileg.

Ein Haftbeschluss ist kein Endurteil. „Dringender Tatverdacht“ bedeutet eine hohe vorläufige Verurteilungswahrscheinlichkeit, nicht rechtskräftige Schuld.

4.2 Warum Russland-Zuschreibung Kategorie C ist

Die ausgewertete öffentliche Verfahrenslage enthält keinen positiven Beleg für eine russische Operation. Im Gegenteil: Die konkreteste deutsche Ermittlungsrichtung betrifft ukrainische Verdächtige. Daraus folgt noch keine rechtskräftige Verantwortlichkeit des ukrainischen Staates. Nationalität, militärischer Hintergrund und mögliche Einbindung in eine Spezialeinheit müssen von einem staatlichen Auftrag unterschieden werden.

Für eine russische Zuschreibung fehlen:

- identifizierte russische Täter;
- russische Operationsmittel oder eine nachgewiesene russische Logistikkette;
- eine Anklage gegen Angehörige russischer Dienste;
- ein deutscher oder internationaler Haftbefehl gegen russische Tatverdächtige;
- ein Urteil;
- eine veröffentlichte Befehlskette.

Die häufig vorgetragene Motivfrage, wem die Zerstörung genutzt oder geschadet habe, ist kein Täterschaftsnachweis. Staaten können wirtschaftlich scheinbar gegen eigene Interessen handeln; Täter können fremde Motive vortäuschen; und Nutzen kann sich nachträglich anders verteilen als geplant.

4.3 Verbleibende Hypothesen

Nach dem öffentlichen Stand sind mindestens folgende Modelle zu unterscheiden:

- eine nichtstaatliche ukrainische Gruppe;
- ukrainische Staatsangehörige mit staatlichem Auftrag;
- ein anderer staatlicher oder nichtstaatlicher Akteur, der Spuren in ukrainische Richtung legte;
- eine gemischte Operation mit privaten und staatlichen Beteiligten;
- eine russische False-Flag-Operation.

Die letzte Hypothese ist logisch möglich aber ohne positive Belege spekulativ. Die bloße Möglichkeit einer False Flag kann den konkreten Tatverdacht gegen andere Personen nicht aufheben.

4.4 Teilurteil

Nord Stream ist kein Beleg für russischen hybriden Krieg gegen Deutschland. Wer den Anschlag als bewiesene russische Sabotage behandelt, widerspricht der öffentlich bekannten deutschen Ermittlungsrichtung. Ebenso voreilig wäre es, den ukrainischen Staat bereits als rechtskräftig überführt darzustellen. Der korrekte Befund lautet: vorsätzliche Sabotage erwiesen, konkrete ukrainische Verdächtige strafprozessual verfolgt, staatliche Auftragsebene und endgültige Schuld offen.

5. EINZELPRÜFUNG 3: UNTERSEEKABEL- UND PIPELINE-SCHÄDEN IN DER OSTSEE

Hauptkategorie: C, Russland-Zurechnung strukturell offen

5.1 Balticconnector

Am 8. Oktober 2023 kam es an der Gasleitung Balticconnector zwischen Finnland und Estland zu einem Druckabfall. Finnische Ermittler führten die physische Beschädigung auf den Anker des unter Hongkong-Flagge fahrenden Schiffes *Newnew Polar Bear* zurück. Die Untersuchung lief jedenfalls im Mai 2025 weiter; finnische Stellen kooperierten mit chinesischen und Hongkonger Behörden.

Damit ist eine physische Verursachung amtlich beschrieben. Nicht abschließend geklärt waren:

- ob der Anker absichtlich über den Meeresboden gezogen wurde;
- ob Fahrlässigkeit oder Navigationsfehler vorlagen;
- ob die Schiffsführung eigenständig handelte;
- ob ein privater Auftraggeber beteiligt war;
- ob ein Staat die Handlung anwies;
- welcher Staat dies gegebenenfalls war.

Flagge, Route, Besatzungsnationalität oder Anlauf eines russischen Hafens würden für sich genommen keine russische staatliche Steuerung beweisen.

5.2 Estlink 2 und andere Vorfälle

Die Beschädigung von Estlink 2 im Dezember 2024 wird in finnischen Regierungsunterlagen erwähnt. Das ausgewertete Material enthält aber keine hinreichend konkrete Ermittlungsdarstellung, die Russland, einen russischen Dienst oder identifizierte Täter belastbar zuordnet.

Bei einer Häufung von Schäden ist eine Sabotageserie eine ernsthafte Hypothese. Sie konkurriert jedoch mit:

- Ankerziehen durch Fehlbedienung;
- fahrlässiger Schiffsführung;
- Materialversagen;
- wetterbedingten Schäden;
- kommerziellen oder kriminellen Handlungen;
- vorsätzlicher Sabotage ohne staatlichen Auftrag;
- Sabotage durch unterschiedliche Staaten oder Gruppen.

Eine statistische Häufung kann Ermittlungen rechtfertigen, ersetzt aber keine fallbezogene Attribution.

5.3 Allgemeine Lagebewertung versus Einzelfallnachweis

Die Bundesregierung beschreibt Spionage, Sabotage, Cyberangriffe, Drohnenaktivitäten und Desinformation als Bestandteile einer verschärften hybriden Bedrohungslage und nennt Russland als wichtigen Akteur. Diese allgemeine Bewertung mag auf eingestuften Erkenntnissen beruhen. Sie beweist nicht, dass ein bestimmtes Kabel durch russischen Auftrag beschädigt wurde.

Der Schluss „Russland besitzt Fähigkeit und Motiv, daher war Russland Täter“ ist ebenso unzulässig wie der umgekehrte Schluss „Es gibt zivile Unfallmöglichkeiten, daher scheidet Sabotage aus“.

5.4 Teilurteil

Eine russische Sabotagestrategie gegen Ostsee-Infrastruktur ist eine ernstzunehmende Sicherheitsannahme aber bei den untersuchten Einzelfällen öffentlich nicht bewiesen. Balticconnector zeigt besonders deutlich, wie weit physische Kausalität und staatliche Verantwortung auseinanderliegen können: Der Anker kann identifiziert sein während Vorsatz und Auftraggeber offenbleiben.

6. EINZELPRÜFUNG 4: TELEGRAM-AGENTEN-NETZWERKE, BRANDANSCHLÄGE UND SPIONAGE

Hauptkategorie: C, das behauptete Netzwerk ist strukturell schwer attribuierbar

Unteraspekte: einzelne Täter und Teiloperationen A oder B

6.1 Das Wegwerfagenten-Modell

Beim Telegram-Wegwerfagenten-Modell rekrutiert ein Auftraggeber Personen über verschlüsselte oder pseudonyme Konten für begrenzte Aufgaben: Fotografieren eines Objekts, Anbringen eines Senders, Transport eines Pakets, Brandstiftung oder Beschädigung von Infrastruktur. Die angeworbene Person kennt den Auftraggeber häufig nicht persönlich. Zahlungen können über Bargeld, Kryptowährungen oder Mittelsmänner erfolgen. Nach Abschluss wird das Konto gelöscht oder aufgegeben.

Die Beweiskette kann dadurch an mehreren Stellen abbrechen:

1. Das Gericht kann feststellen, dass eine Zielperson einen Brand legte oder ein Objekt ausspähte.
2. Es kann Nachrichten eines pseudonymen Auftraggebers sichern.
3. Es kann möglicherweise einen Mittelsmann identifizieren.
4. Es kann aber offenbleiben, wer das Telegram-Konto tatsächlich kontrollierte.
5. Selbst bei einem russischsprachigen Operator bleibt die Verbindung zu GRU, FSB, SWR oder einer anderen staatlichen Stelle unbewiesen.
6. Auch ein identifizierter Dienstkontakt beweist noch nicht die politische Befehlskette bis zur Staatsspitze.

Diese Struktur erzeugt plausible Abstreitbarkeit. Sie kann bewusst gewählt sein, um staatliche Steuerung zu verschleiern. Methodisch darf aus der Verschleierungswirkung aber nicht automatisch auf den russischen Staat geschlossen werden. Gerade weil das Modell Attribution erschwert, benötigt die Staatszuschreibung zusätzliche positive Belege.

6.2 Dieter S.: gerichtsfester Unteraspekt

Dieter S. wurde im Oktober 2025 zu sechs Jahren Freiheitsstrafe verurteilt. Das Gericht sah nach den vorliegenden Berichten Spionage und Planungen für Brandanschläge auf militärische Anlagen und Bahninfrastruktur als erwiesen an. Ziel war demnach, die deutsche Unterstützung der Ukraine zu stören. Zwei Mitangeklagte erhielten Bewährungsstrafen.

Soweit der russische Auftrag beziehungsweise Dienstbezug Bestandteil der gerichtlichen Feststellungen war, erfüllt der Fall Kategorie A. Er beweist eine konkrete russlandbezogene Agenten- und Sabotageplanung. Er beweist nicht, dass geplante Anschläge ausgeführt wurden oder dass sämtliche ähnlichen Brände in Deutschland demselben Netzwerk zuzurechnen sind.

6.3 Paket- und Brandsatzkomplex

Im Paket- beziehungsweise Sabotagekomplex erhob die Bundesanwaltschaft Anklage wegen Agententätigkeit zu Sabotagezwecken im Auftrag eines russischen Dienstes. Ein 30-jähriger ukrainischer Staatsangehöriger wurde im August 2026 zu einem Jahr und drei Monaten Haft verurteilt. Zwei Mitangeklagte wurden freigesprochen, weil ihnen vorsätzliches Handeln nicht nachgewiesen werden konnte.

Der Fall zeigt zwei Dinge zugleich:

- Ein wissentlich handelnder Beteiligter kann gerichtlich überführt werden.
- Objektive Mitwirkung genügt nicht, wenn Wissen und Vorsatz fehlen.

Die Freisprüche sind deshalb ebenso wichtig wie die Verurteilung. Sie verhindern die pauschale Behauptung, alle Beteiligten einer Logistikkette seien bewusste russische Agenten gewesen.

6.4 Weitere Anklagen

Ilona W. wurde nach den ausgewerteten Angaben festgenommen und angeklagt. Die Bundesanwaltschaft wirft ihr vor, Informationen über Rüstungsindustrie, Drohnentests und politische Veranstaltungen gesammelt und einem als Diplomaten auftretenden russischen Nachrichtendienstmitarbeiter Zugänge verschafft zu haben. Das ist Kategorie B, nicht A.

Dasselbe gilt für laufende Verfahren gegen mutmaßliche Sabotagehelfer oder Hintermänner. Die Anklage kann konkrete Kommunikations- und Zahlungswege beschreiben, bleibt aber bis zum Urteil ein Vorwurf.

6.5 Alternative Erklärungen

Bei anonym rekrutierten Kleintätern sind ernsthaft zu prüfen:

- gewöhnliche Kriminalität;
- ideologisch motivierte Einzeltäter;
- bezahlte Handlungen ohne Kenntnis des politischen Zwecks;
- private russlandfreundliche Akteure;
- russische kriminelle Netzwerke ohne staatlichen Auftrag;
- staatlich geduldete oder informell unterstützte Akteure;
- direkte Steuerung durch einen russischen Nachrichtendienst;
- Inszenierung durch einen anderen Akteur.

Nicht alle Alternativen sind gleich wahrscheinlich. Aber ihre bloße Ausscheidung durch Plausibilitätserwägungen genügt nicht; entscheidend sind Kommunikations-, Zahlungs-, Geräte- und Personalbeweise.

6.6 Teilurteil

Einzelne russlandbezogene Spionage- und Sabotageplanungen sind gerichtlich bewiesen. Die weitergehende Aussage, Deutschland werde durch ein einheitliches, vom Kreml zentral geführtes Telegram-Agentennetz angegriffen, bleibt Kategorie C, solange die Rekrutierungs- und Befehlskette nicht durchgehend nachgewiesen ist. Das Wegwerfagenten-Modell erklärt, warum eine solche Kette tatsächlich existieren und dennoch öffentlich kaum beweisbar sein kann. Diese Möglichkeit darf aber nicht mit einem positiven Beweis verwechselt werden.

7. EINZELPRÜFUNG 5: DESINFORMATION, RT, „DOPPELGÄNGER“ UND „GHOSTWRITER“

Hauptkategorie: B, offiziell attribuiert, nicht gerichtlich belegt

7.1 RT und die Grenze zwischen Propaganda und verdeckter Operation

RT und Sputnik werden in den ausgewerteten EU-Dokumenten als staatliche beziehungsweise staatlich kontrollierte russische Kommunikationsakteure behandelt. Das belegt ihre institutionelle Verbindung zum russischen Staat, nicht die Falschheit jeder Veröffentlichung.

Zu unterscheiden sind:

- politische Meinung;
- einseitige Auswahl wahrer Tatsachen;
- nachweislich falsche Tatsachenbehauptung;
- offene staatliche Kommunikation;
- verdeckte Identitätstäuschung;
- koordinierte inauthentische Verstärkung.

Ein staatliches Medium kann zutreffende Informationen veröffentlichen. Ein formal privates Medium kann Falschinformationen verbreiten. Für den Vorwurf einer verdeckten Einflussoperation ist daher nicht allein die politische Tendenz entscheidend sondern Täuschung über Identität, Herkunft, Koordination oder Fakten.

Die Valdai-Transkripte sind in diesem Zusammenhang russische Selbstdarstellungen. Darin präsentiert die russische Führung den Westen als aggressiv, bezeichnet Sanktionen und maritime Maßnahmen als Teil einer gegen Russland gerichteten Politik und kündigt „spiegelbildliche“ Reaktionen auf Eingriffe in die Schifffahrt an. Das dokumentiert ein strategisches Narrativ und eine öffentliche Reziprozitätsdoktrin. Es beweist keine konkrete verdeckte Operation in Deutschland.

7.2 „Doppelgänger“

„Doppelgänger“ ist die am stärksten dokumentierte Informationsoperation im vorliegenden Material. Kennzeichnend sind:

- nachgebildete Websites etablierter Medien und staatlicher Stellen;
- gefälschte Artikel;
- inauthentische Social-Media-Konten;
- koordinierte Verstärkung;
- pro-russische beziehungsweise kremlfreundliche Narrative;
- Zielgruppen unter anderem in Deutschland, Frankreich, der Ukraine und den USA.

Die Existenz täuschend nachgebildeter Seiten ist direkt überprüfbar. Der EEAS ordnet die Kampagne russischen Akteuren zu. Der EU-Rat sanktionierte Personen und Organisationen, darunter Nikolai Tupikin, die Social Design Agency und Struktura. Die EU stellte außerdem Verbindungen zur russischen Präsidialadministration dar.

Die Beweiskette ist damit stärker als bei einer bloßen Behauptung:

- sichtbare Täuschungsinfrastruktur;
- technische Netzwerkanalysen;
- identifizierte Organisationen;
- offizielle EU-Attribution;
- administrative Sanktionen.

Was fehlt, ist ein Strafurteil gegen konkrete Operatoren, das den staatlichen Auftrag und die individuelle Tatbeteiligung feststellt. Deshalb Kategorie B.

7.3 „Ghostwriter“

„Ghostwriter“ verbindet nach der Darstellung der Europäischen Kommission Cyberzugriffe mit manipulativen Veröffentlichungen und richtete sich gegen NATO-Staaten und die Ukraine. Die Quellenlage nennt russische und belarussische Bezüge.

Diese gemischte Zuschreibung ist wichtig. Sie zeigt, dass Aktivitätscluster nicht immer eindeutig einem einzigen Staat oder Dienst zugeordnet werden können. Belegt sind Kampagnenmuster aus Kontenkompromittierung und anschließender Verbreitung manipulierter Inhalte. Nicht belegt ist in den ausgewerteten Daten eine deutsche strafgerichtliche Feststellung gegen konkrete Operatoren.

Daher ist „Ghostwriter“ Kategorie B, soweit eine konkrete Behörde die Kampagne attribuiert und hinsichtlich einzelner nicht offengelegter Zuordnungsglieder Kategorie C.

7.4 Storm-1516 als Grenzfall

Storm-1516 wird als russisch ausgerichtetes Netzwerk beschrieben, das gefälschte Whistleblower-Videos, KI-generierte Personen, manipulierte Dokumente und nachgeahmte Medienmarken verwendet. Einige Quellen bringen das Netzwerk mit der GRU-Einheit 29155 in Verbindung.

Die sichtbaren Inhalte und gefälschten Marken können überprüft werden. Die unmittelbare GRU-Steuerung ist im Material dagegen weder durch eine deutsche Anklage noch durch ein Urteil festgestellt. Deshalb wäre die pauschale Aussage „Storm-1516 ist gerichtlich erwiesen GRU“ falsch. Für das Netzwerk als solches spricht eine substantielle Indizienlage; für die Dienstzuordnung bleibt die öffentliche Kette teilweise offen.

7.5 Wirkung ist nicht mit Existenz gleichzusetzen

Aus einer nachgewiesenen Informationsoperation folgt nicht, dass sie erfolgreich war. Zu unterscheiden sind:

1. Produktion eines manipulativen Inhalts;
2. gezielte Verbreitung;
3. Reichweite;
4. Überzeugungswirkung;
5. Änderung politischen Verhaltens;
6. Veränderung eines Wahlergebnisses.

Die untersuchten Quellen tragen vor allem die ersten beiden Stufen und teilweise Reichweitenindikatoren. Einen kausalen Nachweis veränderter deutscher Wahlergebnisse liefern sie nicht.

7.6 Teilurteil

Russische staatliche oder staatlich angebundene Informationsoperationen sind in bestimmten Fällen erheblich besser belegt als pauschale Aussagen über „russische Propaganda“. „Doppelgänger“ rechtfertigt Kategorie B. RT ist als offener staatlicher Kommunikationsakteur einzuordnen aber nicht jede RT-Veröffentlichung ist deshalb Desinformation. „Ghostwriter“ und Storm-1516 zeigen reale Kampagnenmuster während einzelne staatliche Zuordnungsschritte öffentlich lückenhaft bleiben.

8. EINZELPRÜFUNG 6: POLITISCHE WAHLEINFLUSSNAHME, AFD-VORWÜRFE UND FINANZIERUNGEN

Hauptkategorie: C, pauschale Parteienfinanzierung nicht belegt

Unteraspekt: russisch zugeschriebene Einflusskampagnen B

8.1 Einfluss ist nicht Finanzierung

Politische Einflussnahme umfasst sehr unterschiedliche Vorgänge:

- offene diplomatische Kontakte;
- Interviews in staatlichen Medien;
- ideologische Übereinstimmung;
- öffentliche Unterstützung;
- Lobbyismus;
- verdeckte Informationskampagnen;
- Sachleistungen;
- Geldzahlungen;
- illegale Parteienfinanzierung;
- operative Steuerung von Kandidaten.

Diese Vorgänge dürfen nicht ineinander geschoben werden. Wer russische Positionen vertritt, ist nicht schon deshalb russisch gesteuert. Wer mit russischen Amtsträgern spricht, erhält nicht notwendig Geld. Und eine einzelne rechtswidrige Zahlung würde nicht beweisen, dass eine ganze Partei fremdgesteuert ist.

8.2 Was bei digitalen Kampagnen belegt ist

EU-Stellen beschreiben „Doppelgänger“ und verwandte Netze als auf demokratische Prozesse und Wahlen gerichtete Einflussinstrumente. Geklonte Medienseiten, gefälschte Inhalte und koordinierte Verstärkung sind dokumentiert.

Daraus folgt, dass russisch attribuierte Akteure politische Wahrnehmungen in Deutschland beeinflussen wollten. Nicht daraus folgt, dass eine bestimmte Partei Empfängerin russischer Gelder war oder dass ein Wahlergebnis verändert wurde.

8.3 AfD-Finanzierungsbehauptungen

Für die pauschale Aussage, die AfD werde vom russischen Staat finanziert, fehlen im ausgewerteten Material die notwendigen Belege:

- kein identifizierter russischer staatlicher Zahler;
- kein konkret benannter parteilicher Empfänger mit gerichtsfester Feststellung;
- kein dokumentierter Betrag und Zahlungszeitpunkt;
- keine veröffentlichte Bank- oder Vertragsunterlage;
- keine bewiesene Gegenleistung;
- keine einschlägige Anklage;
- kein einschlägiges Urteil;
- keine ausreichend konkrete Feststellung einer zuständigen deutschen Kontrollinstanz.

Deshalb ist die pauschale Finanzierungsthese Kategorie C.

Dieser Befund ist keine Entlastung sämtlicher Einzelkontakte oder möglicher Unterstützungsleistungen. Er besagt nur, dass eine positive Feststellung nicht getragen wird. Auch ein später auftauchender Zahlungsbeleg müsste hinsichtlich Zahler, Empfänger, Wissen, Zweck und Gegenleistung einzeln geprüft werden.

8.4 Wahleinfluss versus Wahlergebnis

Eine Operation kann Wahlbeeinflussung bezwecken, ohne einen messbaren Erfolg zu erzielen. Für den Nachweis eines geänderten Wahlergebnisses wären mindestens erforderlich:

- belastbare Reichweitendaten;
- Abgrenzung echter von automatisierter Interaktion;
- Nachweis der Rezeption durch Wahlberechtigte;
- Kontrolle konkurrierender politischer Einflüsse;
- kausale Verbindung zwischen Inhalt und Wahlentscheidung;
- hinreichende Größenordnung für eine Ergebnisänderung.

Das Material enthält keine solche Kausalanalyse. Aussagen wie „Russland hat die deutsche Wahl entschieden“ wären daher nicht belegt.

8.5 Symmetrischer Kontext

Westliche Staaten betreiben ebenfalls politische Einflussnahme. Für die Ukraine sind amerikanische personelle Präferenzen im Nuland-Pyatt-Gespräch sowie langjährige NED- und USAID-Förderungen von Zivilgesellschaft, Medien, Wahl- und Antikorruptionsprogrammen dokumentiert. Diese Tatsachen belegen Einfluss und politische Interessen aber keine vollständige westliche Steuerung des ukrainischen Machtwechsels.

Der symmetrische Schluss lautet: Finanzierung, politische Nähe und operative Kontrolle sind auf beiden Seiten zu trennen. Westliche Einflussnahme widerlegt keine russische; russische Einflussversuche rechtfertigen keine pauschale Fremdsteuerung jeder oppositionellen Partei.

8.6 Teilurteil

Russisch attribuierte digitale Einflusskampagnen gegen demokratische Prozesse sind Kategorie B. Die pauschale Behauptung einer staatlich russischen Finanzierung der AfD ist Kategorie C. Ein messbarer Einfluss auf deutsche Wahlergebnisse ist nicht nachgewiesen.

9. EINZELPRÜFUNG 7: SPIONAGEFÄLLE MIT VERURTEILUNG IN DEUTSCHLAND

Hauptkategorie: A, gerichtlich bewiesene Einzeloperationen

Dieser Bereich bildet die stärkste öffentliche Evidenz für russische staatliche Aktivität in Deutschland. Zugleich muss jeder Fall auf seine tatsächliche Reichweite begrenzt bleiben.

9.1 Das „Illegalen“-Paar

Das Oberlandesgericht Stuttgart verurteilte 2013 ein Paar, das über rund zwei Jahrzehnte unter falschen Identitäten in Deutschland gelebt und den russischen Auslandsnachrichtendienst SWR mit Informationen versorgt hatte. Der Mann erhielt sechs Jahre und sechs Monate, die Frau fünf Jahre und sechs Monate Freiheitsstrafe.

Dieser Fall erfüllt Kategorie A, soweit Tätigkeit, Identität und SWR-Bezug Bestandteil des Urteils waren. Er belegt eine langjährige russische Geheimdienstoperation in Deutschland. Er beweist nicht den Umfang sämtlicher SWR-Tätigkeit oder eine Verbindung zu späteren Cyber- und Sabotagefällen.

9.2 Übermittlung von Bundestagsgrundrissen

Ein Mitarbeiter einer für den Bundestag tätigen Firma übermittelte Grundrisse von Parlamentsliegenschaften an einen GRU-Kontakt in der russischen Botschaft. Er wurde zu zwei Jahren Freiheitsstrafe auf Bewährung verurteilt.

Das ist Kategorie A, soweit der GRU-Bezug gerichtlich festgestellt wurde. Nicht daraus folgt, dass bereits ein Anschlagsplan existierte. Gebäudepläne können für Nachrichtendienstzwecke, Sicherheitsanalysen oder Sabotagevorbereitung relevant sein; die konkrete Verwendung muss gesondert bewiesen werden.

9.3 Reserveoffizier Ralph G.

Ralph G. wurde nach den ausgewerteten Angaben im November 2022 zu einem Jahr und neun Monaten auf Bewährung verurteilt. Gegenstand waren Informationen über das Reservistenwesen und weitere militärische oder sicherheitspolitische Themen, die einem russischen Nachrichtendienst zugänglich gemacht worden sein sollen.

Die im Urteil festgestellte Agententätigkeit ist Kategorie A. Einzelheiten, die nur aus der Anklageschrift stammen, dürfen nicht automatisch als gerichtliche Feststellungen behandelt werden.

9.4 Bundeswehrhauptmann Thomas H.

Thomas H., ein Bundeswehroffizier im Beschaffungsbereich, bot dem russischen Generalkonsulat in Bonn und der Botschaft in Berlin seine Zusammenarbeit an und versuchte, dienstlich erlangte Informationen über Beschaffungsvorhaben zu übermitteln. Das OLG Düsseldorf verurteilte ihn im Mai 2024 zu drei Jahren und sechs Monaten Haft.

Der Fall ist Kategorie A. Er zeigt zugleich, warum „russische Rekrutierung“ und „Agententätigkeit zugunsten Russlands“ nicht identisch sind: Nach der öffentlichen Darstellung ging die Initiative wesentlich von Thomas H. aus. Das Urteil belegt den Auslandsdienstbezug, nicht notwendig eine ursprüngliche russische Anwerbung.

9.5 Dieter S. und der Sabotagebezug

Dieter S. wurde wegen Spionage und geplanter Brandanschläge zu sechs Jahren Haft verurteilt. Dieser Fall ist besonders relevant, weil er klassische Nachrichtendiensttätigkeit mit Sabotageplanung verbindet.

Kategorie A bezieht sich auf das gerichtlich Festgestellte. Falls das Urteil nur Planung und Ausspähung, nicht aber vollendete Anschläge feststellte, darf der Fall nicht als Beweis tatsächlich ausgeführter russischer Brandanschläge dargestellt werden.

9.6 Paketkomplex und die Bedeutung der Freisprüche

Ein Beteiligter wurde wegen geheimdienstlicher Agententätigkeit verurteilt; zwei Mitangeklagte wurden mangels nachgewiesenen Vorsatzes freigesprochen.

Die gerichtliche Trennung ist methodisch vorbildlich. Sie zeigt, dass ein Netzwerk nicht kollektiv zugerechnet werden darf. Für den Verurteilten gilt Kategorie A, für die freigesprochenen Personen gerade keine positive Täterschaftsfeststellung.

9.7 Carsten L. und Arthur E. als Abgrenzung zu Kategorie B

Die Bundesanwaltschaft erhob gegen den BND-Beschäftigten Carsten L. und Arthur E. Anklage wegen besonders schweren Landesverrats. Nach der Anklage wurden neun BND-Dokumente an den FSB weitergegeben; Carsten L. soll 450.000 Euro und Arthur E. mindestens 400.000 Euro erhalten haben.

Die Detailtiefe macht den Vorwurf erheblich. Dennoch ist er im hier zugrunde gelegten Material Kategorie B, solange kein Urteil verwendet werden kann. Die Unschuldsvermutung gilt uneingeschränkt.

9.8 Markus R. als Warnung vor falscher Etikettierung

Der frühere BND-Mitarbeiter Markus R. wurde 2016 zu acht Jahren Haft verurteilt. Seine wesentliche nachgewiesene Tätigkeit galt nach der ausgewerteten Quellenlage der CIA; daneben soll er seine Dienste russischen Stellen angeboten haben.

Der Fall darf deshalb nicht schlicht als „für Russland verurteilter BND-Spion“ gezählt werden. Er zeigt, wie leicht Falllisten durch ungenaue Etiketten politisch verzerrt werden können.

9.9 Teilurteil

Russische beziehungsweise russlandbezogene Spionage in Deutschland ist gerichtlich bewiesen. Dies ist der stärkste positive Befund des gesamten Berichts. Die Urteile zeigen langfristige SWR-Agententätigkeit, GRU-Kontakte, militärische Informationsbeschaffung und in einzelnen Fällen Sabotageplanung.

Was sie nicht beweisen, ist eine zentral dokumentierte Gesamtleitung aller Fälle. Die Dienste, Zeiträume, Motive und Rekrutierungswege unterscheiden sich. Mehrere nachgewiesene Operationen ergeben ein Muster fortdauernder russischer Nachrichtendienstaktivität. Ein Muster ist aber noch kein gerichtlich bewiesener einheitlicher „Masterplan“.

10. EINZELPRÜFUNG 8: MH17 ALS STÄRKSTES EINZELARGUMENT

Hauptkategorie: C für den Schluss auf eine koordinierte Strategie gegen Deutschland

Möglicher Unteraspekt: gerichtliche Einzelfeststellungen sind von staatlicher Gesamtverantwortung zu trennen

10.1 Warum MH17 analytisch herausragt

MH17 wird häufig als stärkstes Einzelargument angeführt, weil der Fall einen tödlichen Gewaltereigniskomplex, individuelle Strafverfolgung, prorussische bewaffnete Gruppen und Fragen russischer Kontrolle beziehungsweise Verantwortung miteinander verbindet. Anders als bei einem bloßen Cyberangriff geht es nicht nur um Daten oder politische Kommunikation sondern um einen Vorgang mit massiven menschlichen Folgen.

Gerade deshalb muss die Beweisprüfung besonders genau sein. Vier Fragen sind auseinanderzuhalten:

1. Wodurch wurde MH17 zerstört?
2. Welche Personen waren strafrechtlich verantwortlich?
3. Welche Rolle spielten prorussische bewaffnete Gruppen?
4. In welchem Umfang übte Russland Kontrolle aus oder trug völkerrechtliche Verantwortung?

10.2 Grenzen des vorliegenden Materials

Das für diesen Bericht bereitgestellte Material enthält keine hinreichend ausgearbeitete fallbezogene Darstellung der niederländischen Urteilsgründe, der individuellen Verurteilungen, des Rechtskraftstatus und der genauen Feststellungen internationaler Verfahren zur

russischen Kontrolle. Nach der strikten Integritätsregel dürfen fehlende Tatsachen nicht aus allgemeinem Vorwissen ergänzt werden.

Damit kann die hohe Kategorie-A-Schwelle, Urteil, identifizierter Täter und gerichtlich nachgewiesener staatlicher Auftrag, hier nicht pauschal vergeben werden. Dass ein Urteil einzelne Täter und ihre Rolle in einem bewaffneten Verband feststellt, bedeutet nicht automatisch, dass zugleich ein konkreter staatlicher russischer Abschussbefehl bewiesen wurde. Ebenso ist die völkerrechtliche Kontrolle eines Gebietes oder einer bewaffneten Gruppe nicht ohne Weiteres identisch mit individueller strafrechtlicher Auftragserteilung.

10.3 Was internationale Verantwortung grundsätzlich beweisen würde

Falls ein internationales Gericht effektive russische Kontrolle oder staatliche Verantwortung für Handlungen in einem bestimmten Konfliktzeitraum feststellt, wäre dies ein außerordentlich gewichtiger Befund. Er würde je nach genauer Entscheidung belegen, dass prorussische bewaffnete Gruppen nicht als vollständig autonome lokale Akteure behandelt werden können oder dass Russland für bestimmte Handlungen international verantwortlich ist.

Aber selbst ein solcher Befund hätte Grenzen:

- Kontrolle über eine bewaffnete Gruppe beweist nicht notwendig den Einzelbefehl zu jeder Handlung;
- staatliche Verantwortlichkeit ist nicht identisch mit individueller Strafschuld;
- die Lieferung oder Verfügbarkeit eines Waffensystems ist nicht identisch mit dem Nachweis, wer den konkreten Einsatz befahl;
- Verantwortung im Konfliktgebiet der Ukraine beweist keine operative Steuerung eines Brandanschlags, Cyberangriffs oder Kabelschadens in Deutschland.

10.4 Warum MH17 kein Universalschlüssel ist

Ein starker Beweis für russische Einbindung in einen bewaffneten Konflikt kann die generelle Fähigkeit und Bereitschaft zu verdeckter Unterstützung, Abstreitbarkeit und hybrider Operationsführung belegen. Er kann außerdem abstrakte Gegenhypothesen schwächen, Russland nutze grundsätzlich keine nichtstaatlichen oder scheinbar lokalen Akteure.

Er ersetzt aber nicht die fallbezogene Attribution in Deutschland. Der Schluss

> Russland trug Verantwortung im MH17-Komplex, also steckt Russland hinter Nord Stream, Telegram-Bränden oder Ostsee-Kabelschäden

wäre logisch unzulässig. Frühere oder anderswo festgestellte Taten können Kontext und Musterbeleg sein aber keine automatische Täterschaftsvermutung.

10.5 Teilurteil

MH17 kann, abhängig vom genauen Inhalt der niederländischen und internationalen Entscheidungen, ein sehr starkes Argument für russische Einbindung und Verantwortung im Krieg in der Ukraine sein. Auf Grundlage des hier vorliegenden Materials kann jedoch nicht behauptet werden, ein Gericht habe einen konkreten russischen Staatsauftrag in einer Form festgestellt, die die strenge Kategorie A für die gesamte Staatsebene erfüllt.

Für die Leitfrage nach einer koordinierten russischen Strategie gegen Deutschland bleibt MH17 deshalb Kategorie C: stark als Kontext- und Musterargument, nicht als Tatnachweis für deutsche Fälle.

11. EINZELPRÜFUNG 9: NATO-OSTERWEITERUNG UND ZUSICHERUNGEN VON 1990

Hauptkategorie: C, kein Täterschaftsnachweis sondern historischer Kontext

11.1 Dokumentierte Zusicherungen

Archivunterlagen dokumentieren, dass westliche Politiker 1990 und 1991 Formulierungen verwendeten, die sowjetische Sicherheitsbedenken hinsichtlich einer Ostverschiebung der NATO beruhigen sollten. US-Außenminister James Baker erklärte Michail Gorbatschow am 9. Februar 1990, die NATO-Jurisdiktion werde sich „not one inch eastward“ ausdehnen. Helmut Kohl sagte am

folgenden Tag, die NATO solle den Bereich ihrer Tätigkeit nicht erweitern. Hans-Dietrich Genscher hatte ebenfalls erklärt, die deutsche Einheit dürfe sowjetische Sicherheitsinteressen nicht beeinträchtigen und die NATO solle sich territorial nicht nach Osten ausdehnen.

Damit ist die Behauptung „Es gab keinerlei Zusicherungen“ historisch nicht haltbar.

11.2 Räumlicher und politischer Kontext

Umstritten ist, worauf sich diese Aussagen bezogen:

- ausschließlich auf das Gebiet der früheren DDR;
- auf die Stationierung bestimmter Truppen und Waffen;
- auf die NATO-Jurisdiktion;
- oder auf eine weiter reichende politische Nichtausdehnung nach Osteuropa.

Die Archivdokumente stützen, dass der Gesprächshorizont zeitweise über rein technische Stationierungsfragen hinausging. Zugleich fanden die Gespräche im Kontext der deutschen Einheit und einer damals noch bestehenden Sowjetunion statt.

Eine mündliche politische Zusicherung kann Erwartungen und Vertrauen erzeugen, ohne ein allgemeiner rechtsverbindlicher Vertrag zu sein. Politische Verlässlichkeit und juristische Bindung sind verschiedene Kategorien.

11.3 Der Zwei-plus-Vier-Vertrag

Der Zwei-plus-Vier-Vertrag vom 12. September 1990 ermöglichte die deutsche Einheit, bestätigte die NATO-Mitgliedschaft des vereinten Deutschlands und enthielt besondere Beschränkungen für ausländische Truppen und Kernwaffen auf dem Gebiet der früheren DDR. Er enthielt keine allgemeine Klausel, die die spätere Aufnahme Polens, Ungarns oder anderer osteuropäischer Staaten verbot.

Daraus folgen zwei gleichzeitig zutreffende Aussagen:

- Es gab dokumentierte politische Zusicherungen und Beschwichtigungen, aus denen sowjetische beziehungsweise spätere russische Entscheidungsträger Erwartungen westlicher Zurückhaltung ableiten konnten.
- Es gab keinen allgemein verbindlichen schriftlichen Vertrag, der jede spätere NATO-Erweiterung untersagte.

Die Aussage „eindeutiger Vertragsbruch“ ist deshalb zu weitgehend. Die Aussage „vollständig erfundener russischer Beschwerdegrund“ ist ebenfalls zu weitgehend.

11.4 Begründete Wahrnehmung eines Vertrauensbruchs

Wenn eine Seite im entscheidenden Verhandlungsmoment weitreichende politische Formeln verwendet, später aber auf deren fehlende Vertragsform verweist, kann die andere Seite dies nachvollziehbar als Vertrauensbruch wahrnehmen. Eine solche Wahrnehmung kann außenpolitisches Verhalten erklären und Sicherheitsdilemmata verschärfen.

Die Valdai-Transkripte zeigen, wie die russische Führung diese Geschichte heute deutet: Sie beschreibt sowjetisches Vertrauen als naiv, behauptet, der Westen habe Zusagen über eine Nichtausdehnung missachtet und stellt spätere Erweiterungen als Teil einer langfristigen Isolierung Russlands dar. Das belegt die russische Selbstbeschreibung, nicht automatisch ihre historische oder rechtliche Vollständigkeit.

11.5 Handlungsmacht der Beitrittsstaaten

Eine ausschließlich großmachtzentrierte Erzählung unterschätzt die Interessen der osteuropäischen Staaten. Spätere Beitritte sind nicht nur als amerikanische Expansion sondern auch als Entscheidungen beitrittswilliger Staaten zu betrachten. Im Material wird dies am Beispiel Finnlands und Schwedens sichtbar: Beide beantragten 2022 nach dem russischen Großangriff auf die Ukraine die Mitgliedschaft; Finnland trat 2023 und Schweden 2024 bei.

Die Sicherheitswahrnehmung Russlands und die Sicherheitswahrnehmung osteuropäischer Staaten können gleichzeitig real sein. Keine von beiden löscht die andere aus.

11.6 Kontext ist keine Rechtfertigung

Selbst ein politischer Vertrauensbruch rechtfertigt keine Spionage, Brandstiftung, Sabotage oder Desinformation. Er beweist auch nicht, dass Russland einen bestimmten Angriff durchgeführt hat. Historischer Kontext kann Motive, Eskalationsdynamik und gegenseitiges Misstrauen erklären. Er ersetzt weder strafrechtliche Täterschaft noch staatliche Zurechnung.

11.7 Teilurteil

Die NATO-Erweiterung ist als Kontext relevant, weil dokumentierte Zusicherungen und spätere Erweiterungen eine begründete russische Wahrnehmung westlicher Unzuverlässigkeit erzeugen konnten. Eine allgemein verbindliche Nicht-Erweiterungsverpflichtung wurde jedoch nicht kodifiziert. Der Komplex gehört hinsichtlich der Hybridkriegsfrage in Kategorie C: Er erklärt mögliche Motive und Narrative, beweist aber keine einzige konkrete Operation.

12. QUERSCHNITTSANALYSE: GIBT ES EINE KOORDINIERTE RUSSISCHE STAATSSTRATEGIE?

12.1 Was für Koordination spricht

Mehrere Befunde weisen über isolierte Zufallstaten hinaus:

- gerichtlich bewiesene Agententätigkeit für SWR- oder GRU-bezogene Stellen;
- wiederholte Beschaffung militärischer, parlamentarischer und sicherheitsrelevanter Informationen;
- Sabotageplanung mit dem Ziel, deutsche Unterstützung für die Ukraine zu stören;
- amtliche Zuordnung des Bundestag-Hacks zu einer konkreten GRU-Einheit;
- EU-attribuierte Informationskampagnen mit identifizierten russischen Organisationen;
- Kombination aus Cyberzugriff, Veröffentlichung und narrativer Verstärkung;
- russische staatliche Kommunikation, die Gegenseitigkeit und „spiegelbildliche“ Reaktionen ausdrücklich betont.

Diese Befunde machen es unplausibel, sämtliche Fälle als rein private, zufällige oder erfundene Vorgänge abzutun. Russische Staatsorgane betreiben nachweislich Nachrichtendiensttätigkeit und werden von deutschen und europäischen Behörden mit hoher Konkretion Cyber- und Einflussoperationen zugerechnet.

12.2 Was für eine einheitliche Gesamtstrategie fehlt

Für die stärkere These eines zentral koordinierten hybriden Krieges gegen Deutschland fehlen öffentlich:

- ein authentisches Strategiedokument, das die untersuchten Operationen zusammenführt;
- eine nachgewiesene gemeinsame Befehlsstelle;
- eine gerichtlich festgestellte Koordination zwischen SWR, GRU, FSB, Präsidialadministration und privaten Akteuren;
- durchgehende Zahlungs- und Kommunikationsketten;
- eine belastbare Attribution der spektakulärsten Infrastrukturvorfälle;
- der Nachweis, dass autonome Sympathisanten, Kriminelle und opportunistische Täter zentral gesteuert wurden;
- eine quantitative Wirkungsmessung für Wahl- und Desinformationsoperationen.

Es ist möglich, dass eingestufte Informationen ein klareres Bild ergeben. Öffentlich kann diese Möglichkeit nicht die fehlende Beweiskette ersetzen.

12.3 Strategie kann dezentral sein

Ein Gegenargument lautet, moderne hybride Operationen seien gerade deshalb schwer zu beweisen, weil sie dezentral, arbeitsteilig und mit weitgehender operativer Autonomie durchgeführt würden. Das ist plausibel. Ein Staat kann strategische Ziele setzen während Dienste, Auftragnehmer und Hilfspersonen eigenständig Mittel wählen. Eine zentrale Unterschrift unter jedem Einzelauftrag wäre dann nicht zu erwarten.

Doch auch eine dezentrale Strategie muss positiv belegt werden. Wiederkehrende Ziele, institutionelle Kontinuität, Ressourcen, Personalüberschneidungen und abgestimmte Zeitabläufe können dafür sprechen. Die öffentliche Evidenz erreicht diesen Grad bei einzelnen Diensten und Kampagnen, nicht aber für die Gesamtheit aller politisch als „hybrid“ bezeichneten Vorfälle.

12.4 Unterschied zwischen „gegen Deutschland“ und „gegen den Westen“

Auch das Zielobjekt muss präzisiert werden. Der Bundestag-Hack und deutsche Spionagefälle betreffen Deutschland unmittelbar. MH17 und Operationen in der Ukraine betreffen Deutschland nur mittelbar. Globale russische Informationskampagnen können mehrere Staaten gleichzeitig adressieren. Der Ausdruck „gegen den Westen“ kann daher sehr verschiedene regionale und funktionale Ziele zusammenziehen.

Ein Staat kann westliche Bündniskohäsion schwächen wollen, ohne jeden Mitgliedstaat identisch zu behandeln. Er kann Deutschland wegen seiner politischen, wirtschaftlichen oder militärischen Rolle gezielt bearbeiten. Diese strategische Plausibilität ist aber nicht mit dem Beweis jeder Einzeltat gleichzusetzen.

13. DOPPELSTANDARDS UND DIE GEFAHR WESTLICHER ÜBERINTERPRETATION

13.1 Dokumentierte westliche Aktivitäten

Westliche Staaten betreiben ihrerseits Spionage, Cyberoperationen und politische Einflussnahme. Die NSA- und BND-Affären sind institutionell dokumentiert. Stuxnet verursachte physische Wirkungen an iranischen Industrieanlagen und wird durch hochwertige journalistische Berichte den USA und Israel zugeschrieben, obwohl eine förmliche öffentliche Verantwortungsübernahme fehlt.

US Cyber Command bestätigt Doktrinen wie „persistent engagement“ und „defend forward“ sowie auf Einladung durchgeführte Hunt-Forward-Einsätze. Dies belegt eine aktive Cyberstrategie aber nicht automatisch jeden behaupteten Angriff auf russische Infrastruktur.

Besonders aufschlussreich für die Doppelstandard-Frage ist der Pegasus-Komplex. Das Bundeskriminalamt erwarb spätestens 2020 die israelische Spionagesoftware Pegasus (NSO Group) und setzte sie ab März 2021 in Strafverfolgungsverfahren ein (Süddeutsche Zeitung, Die Zeit, Der Spiegel). Pegasus ermöglicht vollständige Smartphone-Übernahme ohne Nutzerinteraktion, ohne Spuren, ohne wirksame Abwehr. Das BSI gab am 27. Juli 2021 die interne Cyber-Sicherheitswarnung CSW 2021-234348-1032 heraus: Das Bedrohungspotenzial von Pegasus sei “als hoch zu bewerten”. Die amtliche Gefahreinstufung in der Kopfzeile desselben Dokuments: 2/Gelb. Das BKA nutzte dieselbe Software seit März 2021. Die Reaktion auf den weltweiten Pegasus-Skandal (Pegasus-Projekt, Juli 2021): keine Maßnahmen. Stattdessen unterzeichnete Bundesinnenminister Dobrindt am 12. Januar 2026 in Jerusalem einen Cyber- und Sicherheitspakt mit Netanyahu; beteiligte Behörden laut Bundesregierung: BKA, Bundespolizei, BSI, ZITiS (Bundestag-Drucksache 21/4306). Parlamentarische Anfragen zu gemeinsamen Dateizugriffen von BfV und israelischen Diensten: verweigert, “aus Gründen des Staatswohls” (Drucksache 21/4306, S. 4).

Russland wird für vergleichbare Fähigkeiten als Führung eines Hybridkriegs bezeichnet. Das Klassifizierungssystem des BSI stuft russische und westlich-verbündete Werkzeuge mit denselben Fähigkeiten unterschiedlich ein. Das ist eine dokumentierte Asymmetrie.

Diese Tatsachen relativieren nicht russische Taten. Sie verlangen jedoch eine Sprache, die vergleichbare Handlungen vergleichbar bezeichnet. Physische Cyber-Sabotage bleibt Sabotage, auch wenn sie von einem westlichen Staat ausgeht. Spionage bleibt Spionage, auch unter Verbündeten.

13.2 Wo Überinterpretation entsteht

Westliche Überinterpretation beginnt typischerweise an vier Stellen:

1. Eine allgemeine Bedrohungsbewertung wird zur konkreten Täterschaftsaussage.
2. Eine technische Clusterzuordnung wird zur staatlichen Befehlskette.
3. Mehrere russlandbezogene Einzelfälle werden ohne Koordinationsnachweis zu einem Masterplan verbunden.
4. Politische Nähe oder die Verbreitung ähnlicher Narrative wird als Agentenstatus behandelt.

Besonders problematisch ist die selektive Einbeziehung von Ereignissen. Wenn Nord Stream trotz gegenteiliger Ermittlungsrichtung weiterhin als russischer Hybridangriff geführt wird, schwächt dies die Glaubwürdigkeit stärkerer Fälle. Dasselbe gilt für pauschale Russland-Zurechnungen jedes Ostsee-Kabelschadens oder unbelegte Parteienfinanzierungsvorwürfe.

13.3 Wo russische Gegenargumente zu weit gehen

Die umgekehrte Überinterpretation besteht darin, westliche Spionage, NATO-Erweiterung oder Ukrainepolitik als Widerlegung aller russlandbezogenen Vorwürfe zu behandeln. Das ist logisch falsch. Ein NSA-Verstoß macht den Bundestag-Hack nicht ungeschehen.

Stuxnet entlastet keinen russischen Agenten. Dokumentierte Zusicherungen von 1990 beweisen nicht, wer 2015 in das Bundestagsnetz eindrang.

Auch der Hinweis auf mögliche False Flags reicht nicht aus. Für eine konkrete Täuschungsoperation braucht es konkrete Belege. Skepsis ist eine Methode, keine alternative Täterfeststellung.

13.4 Die Valdai-Transkripte als Quellenart

Die Valdai-Texte dokumentieren russische Selbstbeschreibung: Der Westen wird als aggressiv und vertragsbrüchig dargestellt; Russland beschreibt sein Handeln als Reaktion, Verteidigung oder Spiegelung. Die Führung betont eine multipolare Ordnung, „unteilbare Sicherheit“ und Gegenschritte bei maritimen Eingriffen.

Diese Texte sind relevant, weil sie Ziele, Rechtfertigungen und strategische Narrative sichtbar machen. Sie sind für verdeckte Operationen jedoch keine Geständnisse. Ebenso wenig sind westliche Regierungsreden neutrale Beweise eigener Rechtmäßigkeit. Politische Selbstdarstellungen belegen zunächst nur, was eine Regierung öffentlich behauptet.

14. ABGESTUFTES SCHLUSSURTEIL

14.1 Was gerichtlich bewiesen ist

Gerichtlich bewiesen sind mehrere konkrete Fälle russlandbezogener Agententätigkeit in Deutschland:

- langfristige Tätigkeit eines „Illegalen“-Paars für den SWR;
- Übermittlung von Bundestagsgrundrissen an einen GRU-Kontakt;
- Agententätigkeit eines Reserveoffiziers;
- Tätigkeit eines Bundeswehrhauptmanns zugunsten Russlands;
- Spionage und Sabotageplanung durch Dieter S.;
- die wissentlich begangene Agententätigkeit eines Beteiligten im Paketkomplex, bei gleichzeitigen Freisprüchen anderer Beteiligter.

Diese Fälle erfüllen Kategorie A, soweit Täter, Tat und russischer Dienst- oder Auftraggeberbezug vom Gericht festgestellt wurden. Sie beweisen reale russische Nachrichtendienstoperationen in Deutschland. Sie sind kein bloßes NATO-Narrativ.

14.2 Was stark aber nicht gerichtlich bewiesen ist

Der Bundestag-Hack erfüllt Kategorie B. Angriff und Datenabfluss sind dokumentiert; die technische Zuordnung zu APT28 ist erheblich gestützt; Bundesregierung und EU nennen den GRU und die Einheit 26165; gegen Dmitry Badin besteht ein Haftbefehl. Das fehlende Strafurteil verhindert Kategorie A.

Auch „Doppelgänger“ gehört in Kategorie B. Die Täuschungsinfrastruktur ist sichtbar, EU-Stellen benennen Organisationen und Verbindungen zur russischen Präsidialadministration und Sanktionen wurden verhängt. Die individuelle strafrechtliche Verantwortlichkeit ist nicht gerichtlich festgestellt.

Carsten L./Arthur E., Ilona W. und weitere laufende Verfahren sind ebenfalls Kategorie B. Ihre Vorwürfe sind konkret aber nicht mit Urteilen gleichzusetzen.

14.3 Was offen oder spekulativ bleibt

Kategorie C umfasst:

- eine russische Täterschaft bei Nord Stream;
- pauschale Russland-Zurechnungen von Balticconnector, Estlink 2 und anderen Kabelschäden;
- die Behauptung eines einheitlichen Telegram-Agentennetzes, soweit die Befehlskette zum russischen Staat fehlt;
- die pauschale staatlich russische Finanzierung der AfD;
- einen messbaren russischen Einfluss auf deutsche Wahlergebnisse;
- die unmittelbare GRU-Steuerung jeder unter Storm-1516 oder ähnlichen Bezeichnungen geführten Aktivität;
- die Übertragung von MH17-Befunden auf Operationen in Deutschland;

- die Behauptung, sämtliche untersuchten Vorgänge seien Teile eines zentral befohlenen Gesamtplans.

14.4 Führt Russland „hybriden Krieg“?

Die Antwort hängt von der behaupteten Reichweite ab.

Im weiten sicherheitspolitischen Sinn: ja, mit hoher Wahrscheinlichkeit und teilweise nachweislich. Russische Dienste betreiben gerichtlich bewiesene Spionage. Einzelne Sabotageplanungen sind bewiesen. Cyber- und Informationsoperationen werden von deutschen und europäischen Stellen konkret und teilweise technisch stark gestützt russischen Staatsorganen zugeschrieben.

Im strengen Beweissinn einer einheitlichen, zentral koordinierten Gesamtstrategie gegen Deutschland: nein, nicht öffentlich nachgewiesen. Die Fälle ergeben ein belastbares Muster russischer Aktivität aber keinen durchgehenden Beweis einer gemeinsamen Befehls- und Koordinationsstruktur. Einige der politisch am stärksten ausgeschlachteten Fälle passen nicht in die Russland-These oder bleiben offen.

Im Sinn eines persönlichen Kreml- oder Putin-Befehls für jeden Vorgang: nicht bewiesen. Dienstzugehörigkeit, staatliche Zurechnung und persönlicher Einzelbefehl sind verschiedene Ebenen. Die öffentliche Debatte überspringt diese Trennung häufig.

14.5 Was bleibt übrig, wenn man den politischen Überbau wegnimmt?

Es bleiben erstens mehrere rechtskräftig oder gerichtlich festgestellte Fälle von Spionage und Agententätigkeit zugunsten russischer Stellen in Deutschland. Das ist der härteste Befund.

Es bleibt zweitens ein schwerer Cyberangriff auf den Bundestag, den deutsche und europäische Stellen nach technischen, strafprozessualen und nachrichtendienstlichen Ermittlungen dem GRU zuschreiben. Die Attribution ist stark aber nicht durch ein Strafurteil abgeschlossen.

Es bleiben drittens technisch sichtbare und offiziell russisch zugeschriebene Informationsoperationen, vor allem „Doppelgänger“. Sie zeigen Täuschung, Klonseiten und koordinierte Verstärkung. Ihre tatsächliche politische Wirkung ist nicht zuverlässig quantifiziert.

Es bleiben viertens einzelne gerichtlich bewiesene Sabotageplanungen und ein Modell niedrigschwelliger Rekrutierung, bei dem die Befehlskette durch Telegram-Konten, Mittelsmänner und unwissende Hilfspersonen strukturell gekappt werden kann. Die Einzelhandlung kann beweisbar sein während der staatliche Hintermann verborgen bleibt.

Es bleiben fünftens erhebliche Lücken: Nord Stream ist Russland nicht zurechenbar; bei Ostsee-Kabelschäden fehlen Vorsatz- und Auftragsnachweise; eine pauschale AfD-Finanzierung ist nicht belegt; MH17 beweist keine Tat in Deutschland; allgemeine Regierungseinschätzungen ersetzen keine Einzelfallermittlung.

Und es bleibt sechstens ein historischer Sicherheitskonflikt. Die Zusicherungen von 1990 sind dokumentiert, eine allgemeine rechtlich bindende Erweiterungssperre war es nicht. Eine russische Wahrnehmung des Vertrauensbruchs ist nachvollziehbar aber weder Rechtfertigung für Straftaten noch Beweis ihrer Täterschaft.

14.6 Endformel

Die nüchternste Antwort lautet:

> Russland führt nachweislich einzelne staatliche oder staatlich angebundene Geheimdienst-, Cyber- und Einflussoperationen gegen Deutschland und andere westliche Staaten durch. Mehrere dieser Operationen sind gerichtlich bewiesen, andere stark amtlich attribuiert. Nicht nachgewiesen ist, dass alle als „hybrid“ bezeichneten Vorfälle Bestandteil eines einheitlichen, zentral koordinierten russischen Kriegsplans sind.

Wer jede Russland-Zuschreibung als Propaganda verwirft, ignoriert rechtskräftige Urteile und konkrete amtliche Beweisketten. Wer dagegen Cyberangriffe, Nord Stream, Kabelschäden, Telegram-Täter, Medieninhalte, AfD-Vorwürfe und MH17 zu einem bereits bewiesenen Gesamtkrieg verschmilzt, behauptet mehr, als die öffentliche Evidenz trägt.

Das ehrliche Urteil ist deshalb abgestuft und unbequem: Die russische Bedrohung ist real aber ihre politische Gesamterzählung ist breiter als ihr öffentlich beweisbarer Kern. Gerade die strikte Trennung von Urteil, Anklage, Attribution, Indiz und Spekulation schützt vor zwei Fehlern zugleich, vor der Verharmlosung nachgewiesener russischer Operationen und vor ihrer Überdehnung zu einer allumfassenden, angeblich schon bewiesenen Kriegserzählung.

SOURCES

1. Beweise_Russische_Hybridkriegsfuehrung.md (uploaded document)
2. Attributionsproblem_und_Doppelstandard.md (uploaded document)
3. https://www.businessinsider.com/der-spiegel-and-nsa-phone-tapping-story-2014-12
4. https://www.bbc.com/news/world-europe-33106044
5. https://www.bundestag.de/webarchiv/presse/hib/2015-11/394386-394386
6. https://www.bundestag.de/dokumente/textarchiv/2015/kw45-pa-1ua/393230
7. https://www.tandfonline.com/doi/full/10.1080/1369118X.2025.2604662
8. https://www.techtarget.com/searchsecurity/news/252436661/Olympic-Destroyer-was-a-false-flag-cyberattack-research-claims
9. https://securelist.com/olympic-destroyer-is-still-alive/86169/
10. https://www.kaspersky.com/about/press-releases/the-olympic-false-flag
11. Putin Valdai 2026 ru.txt (uploaded document)
12. Putin Valdai 2026 Frage und Antwort en.txt (uploaded document)
13. https://www.bbc.com/news/world-europe-26079957
14. https://www.pbs.org/newshour/world/leaked-u-s-phone-call-ukraine-draws-anger-russia-eu
15. https://www.ned.org/impact-report-strengthening-ukraines-democratic-resilience-and-countering-russias-aggression/
16. https://www.state.gov/wp-content/uploads/2021/08/Ukraine_FY-2020-Country-Assistance-Fact-Sheet.pdf
17. https://2012-2017.usaid.gov/news-information/fact-sheets/political-process-and-governance
18. https://oig.usaid.gov/sites/default/files/2018-06/9-121-14-002-p.pdf
19. https://nsarchive.gwu.edu/briefing-book/russia-programs/2017-12-12/nato-expansion-what-gorbachev-heard-western-leaders-early
20. https://nsarchive.gwu.edu/document/16116-document-05-memorandum-conversation-between
21. https://nsarchive.gwu.edu/document/16117-document-06-record-conversation-between
22. https://nsarchive.gwu.edu/document/16120-document-09-memorandum-conversation-between
23. https://nsarchive.gwu.edu/briefing-book/russia-programs/2018-03-16/nato-expansion-what-yeltsin-heard
24. https://blogs.loc.gov/law/2025/11/falqs-35-years-of-german-reunification/
25. https://history.state.gov/countries/german-democratic-republic
26. https://2001-2009.state.gov/r/pa/ho/time/pcw/108224.htm
27. https://www.nato.int/en/what-we-do/partnerships-and-cooperation/enlargement-and-article-10
28. https://www.nato.int/en/what-we-do/partnerships-and-cooperation/relations-with-finland
29. https://www.nato.int/cps/en/natohq/news_213448.htm
30. https://www.nato.int/cps/en/natohq/news_223446.htm
31. https://homeland.house.gov/wp-content/uploads/2025/07/2025-07-22-CIP-Testimony.pdf
32. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html
33. https://spectrum.ieee.org/the-real-story-of-stuxnet
34. https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/
35. https://modeldiplomat.com/learn/glossary/persistent-engagement
36. https://www.cybercom.mil/Media/News/Article/3218642/
37. https://www.cybercom.mil/Media/News/Article/3505610/us-conducts-first-hunt-forward-operation-in-lithuania/
38. https://www.cybercom.mil/