ANALYTISCHER FORSCHUNGSBERICHT · PHILOSOPHENSTUDIO

Beweise der russischen Hybridkriegsfuehrung

Einzelfallanalyse, Quellendokumentation und Einordnung nach Beweiskategorien

Erstellt von: Christer Häberli

Datum: 8. Oktober 2026

Aktenzeichen: CHH-2026-BEW-001

Status: Analytisches Arbeitsdokument

ANALYTISCHES DOKUMENT · KEIN AMTLICHER SCHRIFTSATZ

BEWEISE RUSSISCHER HYBRIDKRIEGSFÜHRUNG GEGEN DEUTSCHLAND UND DIE NATO: DOKUMENTATION, ATTRIBUTION UND BEWEISGRENZEN

Christer Häberli October 08, 2026

BEFUNDZUSAMMENFASSUNG

Die öffentlich zugängliche Evidenz für russische, staatlich gesteuerte oder staatlich gebilligte Operationen gegen Deutschland ist weder einheitlich noch pauschal. Sie reicht von rechtskräftigen Verurteilungen wegen geheimdienstlicher Agententätigkeit über Anklagen und Haftbefehle bis zu administrativen Sanktionen, technischen Zuordnungen und nicht öffentlich belegten Nachrichtendienstbewertungen. Der Begriff „Hybridkriegsführung“ bezeichnet dabei keine eigene strafrechtliche Kategorie. Er bündelt politisch und sicherheitspolitisch unterschiedliche Phänomene wie Cyberoperationen, Spionage, Sabotagevorbereitung, Desinformation und verdeckte Einflussnahme. Für jeden Einzelfall muss deshalb getrennt geprüft werden, ob die Tat selbst, ihre technische Urheberschaft, die organisatorische Anbindung an einen russischen Dienst und die Identität individueller Täter jeweils belegt sind.

Am stärksten dokumentiert sind folgende Komplexe:

1. **Der Cyberangriff auf den Deutschen Bundestag 2015** ist als Angriff und Datendiebstahl substanziell belegt. Deutsche Behörden ordneten ihn offiziell APT28 beziehungsweise dem russischen Militärnachrichtendienst GRU und dessen Einheit 26165 zu. Gegen Dmitry Sergeyevich Badin wurde ein deutscher Haftbefehl erlassen. Die Europäische Union belegte Badin, GRU-Chef Igor Kostyukov und die Einheit 26165 mit Sanktionen. Diese Kombination aus technischer Analyse, strafprozessuellem Tatverdacht, politisch-behördlicher Attribution und personenbezogenen Sanktionen ergibt eine starke öffentliche Beweislage. Ein deutsches Strafurteil gegen Badin liegt in den ausgewerteten Quellen jedoch nicht vor. Der Fall ist daher hinsichtlich der Dienst- und Individualzuordnung **Klasse B**, ergänzt um technische Belege der **Klasse C**, nicht Klasse A.

2. **Gerichtlich festgestellte Spionage- und Agententätigkeit zugunsten russischer Stellen** ist in mehreren deutschen Verfahren nachgewiesen. Dazu gehören ein über Jahre in Deutschland operierendes „Illegalen“-Paar, ein Bundeswehroffizier, der Russland militärische Unterlagen anbot, ein Mitarbeiter mit Zugang zu Bundestagsgrundrissen sowie Dieter S., der wegen Spionage und geplanter Brandanschläge verurteilt wurde. In einem 2026 entschiedenen Paket- beziehungsweise Sabotagefall wurde ein Angeklagter verurteilt, während zwei Mitangeklagte freigesprochen wurden. Diese Urteile sind die belastbarste Evidenzklasse, soweit der russische Auftrag oder Dienstbezug Bestandteil der gerichtlichen Tatsachenfeststellung war.

3. **Der Fall Carsten L./Arthur E.** belegt dagegen zunächst nur eine formelle Anklage. Die Bundesanwaltschaft wirft dem BND-Mitarbeiter und seinem mutmaßlichen Mittäter besonders schweren Landesverrat zugunsten des russischen FSB vor. Nach der Anklage wurden neun BND-Dokumente weitergegeben und insgesamt mindestens 850.000 Euro gezahlt. Solange kein Urteil zugrunde gelegt werden kann, gilt die Unschuldsvermutung; der Fall gehört in Klasse B.

4. **Russische Desinformations- und Einflussnetzwerke** wie „Doppelgänger“ sind durch EU-Institutionen, technische Untersuchungen und Sanktionen vergleichsweise konkret dokumentiert. Die EU beschreibt geklonte Medienseiten, inauthentische Konten und eine Verbindung zur Social Design Agency sowie zur russischen Präsidialadministration. Sanktionen gegen Beteiligte sind jedoch administrative Maßnahmen und kein Strafurteil. Bei „Ghostwriter“ und insbesondere „Storm-1516“ ist die öffentliche Attribution heterogener. Für Storm-1516 enthält das Material sekundäre und technische Zuordnungen bis zur GRU-Einheit 29155, aber keine deutsche Anklage oder gerichtliche Feststellung.

5. **Nord Stream ist nach dem öffentlichen Stand nicht Russland zuzurechnen.** Die deutsche Strafverfolgung verfolgt vielmehr konkrete ukrainische Tatverdächtige. Der Bundesgerichtshof bestätigte im Dezember 2025 den dringenden Tatverdacht gegen einen mutmaßlichen Koordinator und verneinte Immunität sowie ein Kombattantenprivileg; über die endgültige Schuld entschied er damit nicht. Eine rechtskräftige Attribution der Anschläge an Russland liegt nicht vor.

6. **Unterseekabel- und Ostseevorfälle dürfen nicht pauschal Russland zugeschrieben werden.** Beim Balticconnector führte die finnische Untersuchung die physische Beschädigung auf den Anker der unter Hongkong-Flagge fahrenden *Newnew Polar Bear* zurück; ob vorsätzlich gehandelt wurde, blieb Gegenstand der Untersuchung. Nationalität, Flagge, Route oder mögliche Verbindungen eines Schiffes ersetzen keinen Nachweis staatlicher Steuerung.

7. **Pauschale Behauptungen über eine russische Finanzierung der AfD sind durch das vorliegende Material nicht tragfähig belegt.** Das Quellenkorpus enthält weder ein einschlägiges rechtskräftiges Urteil noch eine deutsche Anklage, einen veröffentlichten Zahlungsnachweis oder eine hinreichend konkrete offizielle Tatsachenfeststellung. Das schließt unbekannte oder nicht veröffentlichte Erkenntnisse nicht aus; es erlaubt aber keine Tatsachenbehauptung, die Partei werde als solche vom russischen Staat finanziert.

Der Gesamtbefund lautet deshalb: Stark belegt sind bestimmte Spionagefälle, die Existenz des Bundestag-Angriffs, die technische Kontinuität von APT28 und die offizielle Zuordnung zur GRU-Einheit 26165. Offiziell, aber ohne Strafurteil zugeschrieben sind weitere Cyber-, Desinformations- und Sabotagekomplexe. Offen oder umstritten bleiben Nord Stream, pauschale Russland-Zurechnungen bei Ostsee-Infrastruktur, weitreichende

Behauptungen zur Parteienfinanzierung sowie alle Schuldzuweisungen, deren Beweiskette ausschließlich auf nicht veröffentlichten Nachrichtendienstinformationen beruht.

MASSSTAB, BEGRIFFE UND EVIDENZKLASSEN

Keine einheitliche Bedeutung von „Hybridkriegsführung“

„Hybridkriegsführung“ ist im vorliegenden Bericht ein analytischer Oberbegriff. Er bedeutet nicht, dass jeder Cyberangriff, jede Falschmeldung, jede Spionagehandlung oder jeder Infrastrukturdefekt Teil eines einheitlich befohlenen russischen Operationsplans sein muss. Ebenso wenig folgt aus mehreren russischen Bezügen automatisch eine zentrale Steuerung durch dieselbe staatliche Stelle.

Zu unterscheiden sind mindestens:

- eine tatsächlich eingetretene Schädigung oder Ausspähung;
- die unmittelbaren technischen beziehungsweise operativen Verursacher;
- die Zugehörigkeit dieser Personen zu einer Organisation;
- die Anbindung dieser Organisation an GRU, FSB, SWR, die Präsidialadministration oder eine andere staatliche Stelle;
- ein staatlicher Auftrag für den konkreten Einzelfall;
- individuelle strafrechtliche Verantwortlichkeit;
- eine weitergehende politische Deutung als Bestandteil einer umfassenden Strategie.

Diese Ebenen können unterschiedlich stark belegt sein. Der Nachweis eines Angriffs beweist nicht automatisch dessen russische Urheberschaft. Wiederverwendete Schadsoftware beweist nicht ohne Weiteres die Identität eines Operators. Eine Dienstzugehörigkeit beweist noch nicht jede dem Dienst zugerechnete Einzeltat. Umgekehrt ist das Fehlen veröffentlichter Geheimdienstquellen kein Gegenbeweis; es begrenzt aber die unabhängige Kontrolle.

Vierstufige Evidenzskala

Klasse	Definition	Typische Quellen	Aussagegrenze
A gerichtlich festgestellt	Rechtskräftige Verurteilung oder belastbare gerichtliche Tatsachenfeststellung. Soweit die Rechtskraft aus dem Material nicht hervorgeht, wird dies ausdrücklich vermerkt.	Urteil, Beschluss eines Oberlandesgerichts oder des Bundesgerichtshofs	Belegt nur das, was das Gericht tatsächlich festgestellt hat. Ein Haftbeschluss ist noch kein Schuldurteil.
B formelle oder offizielle Attribution	Anklage, Haftbefehl, dringender Tatverdacht oder konkret benannte behördlich-offizielle Zuordnung; ferner förmliche EU-, NATO- oder staatliche Attribution.	Bundesanwaltschaft, BGH-Haftentscheidung, Bundesregierung, EU-Rat, ausländische Regierung	Eine Anklage ist keine Verurteilung. Eine behördliche Attribution kann auf geheimen Erkenntnissen beruhen und ist nicht mit gerichtlicher Beweisführung gleichzusetzen.
C substanzielle öffentlich prüfbare Indizien	Technische Forensik, Infrastrukturmerkmale, nachvollziehbare Open-Source-Recherche, dokumentierte Kampagnennetze oder mehrere konsistente seriöse Berichte.	CERT-Berichte, technische Unternehmen, OSINT, investigative Medien	Kann eine Attribution erheblich stützen, erreicht aber nicht automatisch den strafprozessualen Beweismaßstab.
D Behauptung oder unvollständige Beweiskette	Politische oder nachrichtendienstliche Bewertung ohne öffentlich zugängliche tragfähige Beweiskette; einzelne Medienberichte oder interessengeleitete Selbstdarstellungen.	politische Rede, nicht belegte Geheimdienstbehauptung, Einzelbericht, Propaganda	Darf nicht als bewiesene Tatsache dargestellt werden.

Diese Skala ergänzt die vom Auftraggeber verlangte Dreiteilung: Gerichtliche Fakten entsprechen Klasse A; offiziell zugeschriebene Vorfälle ohne Urteil Klasse B; nicht öffentlich belegte Geheimdienstbehauptungen Klasse D. Klasse C wird zusätzlich benötigt, um technische und offene Belege sichtbar von bloßen Behauptungen zu trennen.

Rechtsfolgen sind keine Schuldurteile

Sanktionen, Einreiseverbote, Kontensperren und Diplomatenausweisungen sind politische oder administrative Maßnahmen. Ihre Begründungen können konkrete Tatsachen enthalten, sie ersetzen aber kein Strafverfahren. Ebenso ist ein internationaler Haftbefehl Ausdruck eines gerichtlich geprüften Tatverdachts, nicht der Nachweis endgültiger Schuld. Bei Angeklagten und Beschuldigten gilt die Unschuldsvermutung.

Stichtag und Quellengrenzen

Stichtag ist der 8. Oktober 2026. Wo das Material lediglich „Oktober 2026“ nennt, ohne zu zeigen, dass ein Ereignis spätestens an diesem Datum stattfand, wird es nicht als gesicherter Stichtagsbefund verwendet. Das betrifft insbesondere Berichte über eine Festnahme des früheren BND-Präsidenten August Hanning, deren genaues Datum im Material nicht verlässlich bestimmbar ist. Zudem ist die Domain „bundesanwalt.de“ keine Behördenquelle, sondern eine zum Verkauf stehende private Domain. Amtliche Mitteilungen stammen von „generalbundesanwalt.de“.

Die beiden Valdai-Transkripte dokumentieren russische Selbstbeschreibung, strategische Narrative und öffentliche Kommunikation. Sie belegen, dass die russische Führung westlichen Staaten Aggression vorwirft, eine multipolare Ordnung propagiert und Gegenschritte in maritimen Auseinandersetzungen ankündigt. Sie belegen keine konkrete verdeckte Operation gegen Deutschland und werden deshalb nicht zur Attribution einzelner Angriffe herangezogen.

TABELLARISCHE FALLÜBERSICHT

Datum/Zeitraum	Ereignis	Akteur/Zuordnung	Offizielle Stelle	Klasse	Verfahrensstatus	Durch Quellen gedeckte Aussage
April Mai 2015	Cyberangriff auf den Bundestag	APT28/Fancy Bear; GRU-Einheit 26165; Dmitry Badin als Beschuldigter	Bundesregierung/Auswärtiges Amt, deutsche Strafverfolgung, EU-Rat	**B/C**	Haftbefehl; kein Urteil im Material	Angriff Datendiebstahl dokumentiert; Deutschland ordnete Operation dem GRU gegen Badin bestand Haftbefehl.
22. Oktober 2020	EU-Sanktionen wegen Bundestag-Hack	Badin, Igor Kostyukov, Einheit 26165	Rat der EU	**B**	Administrative Sanktionen	Vermögenssperren Reisebeschränkunge keine strafgerichtl Verurteilung.
2013	Verurteilung eines russischen „Illegalen“-Paars	Tätigkeit für den russischen SWR	OLG Stuttgart	**A**	Verurteilung	Ehemann zu Ehefrau zu 5½ Ja Haft verurteilt.
2021/2022 berichtet	Bundestagsgrundrisse an GRU-Kontakt	Mitarbeiter einer Bundestags-Dienstleistungsfirma	deutsches Gericht; ergänzende Berichte	**A**	Zwei Jahre auf Bewährung	Übermittlung Grundrissen an e GRU-Kontakt in russischen Botsc wurde mit e Bewährungsstrafe geahndet.
November 2022	Reserveoffizier	Informationsweitergabe an GRU	deutsches Gericht; Medienberichte	**A**	Ein Jahr und neun Monate auf Bewährung	Verurteilung we Weitergabe Informationen über Reservistenwesen.
2022 2023	Carsten L. und Arthur E.	mutmaßliche Weitergabe von BND-Geheimnissen an FSB	Generalbundesanwalt	**B**	Anklage, Untersuchungshaft	Anklage we besonders schw Landesverrats; r Dokumente mindestens 850 Euro behauptet.
Mai 2024	Thomas H., Bundeswehrhauptmann	Angebot militärischer Informationen an Russland	OLG Düsseldorf; Medienbericht	**A**	Drei Jahre und sechs Monate Haft	Verurteilung we geheimdienstlicher Agententätigkeit.
April 2024 ff.	Dieter S. und Mitbeschuldigte	Spionage und Sabotageplanung zugunsten Russlands	deutsche Strafverfolgung/Gericht	**A**	Urteil Oktober 2025	Dieter S. zu sechs Ja Haft; z Mitangeklagte erhie Bewährungsstrafen.
Januar/September 2026	Ilona W.	mutmaßliche Tätigkeit für russischen Dienst/GRU	Generalbundesanwalt	**B**	Festnahme und Anklage	Vorwurf Informationsbeschaf und Kontaktvermitt in Politik, Verteidig und Rüstungsindus kein Urteil.

Datum/Zeitraum	Ereignis	Akteur/Zuordnung	Offizielle Stelle	Klasse	Verfahrensstatus	Durch Quellen gedeckte Aussage
Januar August 2026	Paket-/Sabotagekomplex	mutmaßlicher russischer Nachrichtendienstauftrag	Generalbundesanwalt, OLG Stuttgart	**A/B**	Ein Angeklagter verurteilt, zwei freigesprochen	Ein 30-jähriger Ukra erhielt ein Jahr und Monate Haft; z Mitangeklagte wu mangels Vorsatznachweises freigesprochen.
September 2022 2025	Nord-Stream-Sprengungen	konkrete ukrainische Verdächtige; keine gerichtliche Russland-Zuordnung	Generalbundesanwalt, BGH	**B**	Haftbefehle und Haftprüfung; kein Endurteil	BGH bejahte dringer Tatverdacht ge mutmaßlichen Koordinator; k Zurechnung Russland.
8. Oktober 2023	Balticconnector beschädigt	Anker der *Newnew Polar Bear*	finnische Ermittlungsbehörden	**B/C**	Untersuchung jedenfalls bis Mai 2025 aktiv	Physische Ursache Anker zugeord Vorsatz und staatl Steuerung r abschließend belegt.
Dezember 2024	Estlink 2 beschädigt	offen	finnische Stellen	**D** hinsichtlich Russland	Ermittlungen im Material nicht ausreichend dokumentiert	Das Ereignis erwähnt; eine belast Russland-Attribution ergibt sich nicht.
ab 2022/2023	„Doppelgänger“	Social Design Agency, Structura, russische Präsidialadministration	EEAS, EU-Rat	**B/C**	EU-Sanktionen	Geklonte Mediense und koordin Verbreitung; EU lis beteiligte Personen Einrichtungen.
längerfristig	„Ghostwriter“	russische und belarussische Akteure	Europäische Kommission	**B/C**	keine deutsche Verurteilung im Material	Kombination Cyberzugriffen Einflussoperationen gegen NATO-Sta und Ukraine.
2025 2026	„Storm-1516“	russisch ausgerichtetes Netzwerk; behauptete Verbindung zu GRU 29155	technische/sekundäre Quellen; einzelne Behördenbewertungen	**C**, teils **D**	keine deutsche Anklage im Material	Einsatz gefälsc Medienmarken, Vi und KI-Inh Dienstzuordnung r gerichtlich bestätigt.
2024 2026	AfD-Finanzierungsbehauptungen	unterschiedliche, nicht hinreichend belegte Behauptungen	keine tragfähige offizielle Fallquelle im Material	**D**	kein einschlägiges Urteil/keine einschlägige Anklage belegt	Eine pauschale staatl russische Finanzie der Partei ist aus Material r nachweisbar.

1. BUNDESTAG-HACK, APT28 UND GRU-EINHEIT 26165

1.1 Was als Angriff belegt ist

Im April und Mai 2015 wurde die IT-Infrastruktur des Deutschen Bundestages kompromittiert. Der Initialzugriff erfolgte nach den ausgewerteten technischen und investigativen Darstellungen über Spear-Phishing-Nachrichten, die als Mitteilungen der Vereinten Nationen getarnt waren. Als Köder wurde unter anderem ein Text zum Konflikt zwischen Russland und der Ukraine verwendet. Nach dem Anklicken eines Links wurde Schadsoftware installiert. Die Angreifer erlangten Zugang zu internen Systemen und entwendeten ungefähr 16 Gigabyte Daten, darunter E-Mail-Bestände.

Damit sind vier Punkte relativ stark belegt:

- Es gab einen tatsächlichen unbefugten Zugriff.
- Der Angriff begann mit präparierten Nachrichten beziehungsweise Links.
- Schadsoftware und Werkzeuge zur Gewinnung von Zugangsdaten wurden eingesetzt.
- Ein erheblicher Datenbestand wurde exfiltriert.

Diese Feststellungen betreffen zunächst nur **Schaden und Angriffsmethode**, nicht die staatliche Urheberschaft.

Evidenzklasse: C für technische und offen nachvollziehbare Angriffsfeststellungen; soweit die Strafverfolgung diese Tatsachen einem Haftbefehl zugrunde legte, **B**.

1.2 Technische Zuordnung zu APT28

APT28 ist kein gerichtlicher Vereinsname, sondern eine von Sicherheitsunternehmen und Behörden verwendete Clusterbezeichnung. Weitere Bezeichnungen sind Fancy Bear, Sofacy, Pawn Storm und Strontium. Ein Cluster fasst Aktivitäten anhand wiederkehrender Infrastruktur, Malware, Arbeitsmuster, Ziele und operativer Überschneidungen zusammen.

Für den Bundestag-Angriff werden Übereinstimmungen mit der „Scaramouche“-Malwarefamilie, APT28-typischen Werkzeugen und bekannten Vorgehensweisen genannt. Breitere Analysen zu APT28 verweisen auf Spear-Phishing, kundenspezifische Backdoors wie X-Agent, verschlüsselte Exfiltration und Arbeitszeiten, die mit Moskauer Zeit vereinbar seien.

Solche Merkmale sind relevant, aber nicht einzeln beweiskräftig:

- Schadsoftware kann kopiert oder weitergegeben werden.
- Zeitzonenindizien lassen sich manipulieren.
- Phishing ist keine exklusive Methode eines bestimmten Dienstes.
- gemeinsame Infrastruktur kann auf denselben Betreiber, auf Dienstleister oder auf bewusste Täuschung hindeuten.

Aussagekräftiger wird die technische Zuordnung durch die Kombination mehrerer Merkmale über verschiedene Operationen hinweg. Im Bundestag-Fall kommt hinzu, dass deutsche Ermittlungen, ausländische Partnerinformationen und personenbezogene Erkenntnisse zusammengeführt wurden.

Evidenzklasse: C für die technische Clusterzuordnung zu APT28.

1.3 Dienstzuordnung zur GRU-Einheit 26165

Die Bundesregierung und das Auswärtige Amt ordneten den Angriff dem russischen Militärnachrichtendienst GRU 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.

Die Einheit 26165 wird als 85. Hauptzentrum für Spezialdienste beziehungsweise GTsSS bezeichnet. Die EU behandelte sie im Sanktionsbeschluss als die für den Bundestag-Angriff verantwortliche Organisation.

Diese Dienstzuordnung geht über eine bloße technische Clusteranalyse hinaus. Öffentlich nachvollziehbar stützt sie sich auf:

- die Kontinuität der APT28-Infrastruktur und -Werkzeuge;
- internationale Ermittlungs- und Nachrichtendienstkooperation;
- Erkenntnisse aus dem Vorgehen niederländischer Behörden gegen GRU-Bedienstete;
- offene Recherchen zu Registrierungs- und Identitätsdaten;
- die Identifizierung Badins als Angehörigen der Einheit 26165.

Nicht vollständig öffentlich ist hingegen die deutsche behördliche Beweiskette. Weder sämtliche forensischen Rohdaten noch die geheimdienstlichen Ausgangsinformationen sind publiziert. Die offizielle Attribution ist deshalb belastbar, aber extern nicht in allen Teilen reproduzierbar.

Evidenzklasse: B, gestützt durch **C**.

1.4 Dmitry Badin: Identifizierung und Haftbefehl

Gegen Dmitry Sergeyevich Badin wurde am 29. April 2020 ein Haftbefehl erlassen. Ihm wurde geheimdienstliche Agententätigkeit und Datenausspähung im Zusammenhang mit dem Bundestag-Angriff vorgeworfen. Deutsche Stellen gingen davon aus, dass Badin während der Tat der Einheit 26165 angehörte.

Die offene Recherche von Bellingcat verband Registrierungsdaten Badins mit der offiziellen Anschrift der GRU-Einheit. Dies ist ein relevantes Identitäts- und Organisationsindiz, ersetzt aber nicht die strafprozessuale Hauptverhandlung.

Zu trennen sind:

- **Individuelle Identität:** Badin ist namentlich bezeichnet.
- **Dienstzugehörigkeit:** offiziell und durch offene Indizien gestützt.
- **Tatbeteiligung:** Gegenstand des Haftbefehls.
- **Schuld:** mangels deutschen Urteils nicht rechtskräftig festgestellt.

Evidenzklasse: B. Der Haftbefehl ist stärker als ein Medienverdacht, aber schwächer als ein Urteil.

1.5 EU-Sanktionen

Am 22. Oktober 2020 verhängte die EU restriktive Maßnahmen gegen Badin, Igor Kostyukov und die Einheit 26165. Die Maßnahmen umfassten Einreisebeschränkungen und Vermögenssperren.

Der Sanktionsbeschluss ist ein förmlicher Akt und enthält eine politische beziehungsweise administrative Verantwortungszuweisung. Er ist deshalb wichtige offizielle Attribution. Er beweist jedoch weder nach deutschem noch nach europäischem Strafprozessrecht die individuelle Schuld.

Evidenzklasse: B.

1.6 Gesamtbewertung des Cyberfalls

Zuordnungsebene	Befund	Klasse
Angriff und Schaden	Eindringen, Malwareeinsatz und Datenabfluss sind substanziell dokumentiert.	C/B
Technischer Akteur	Muster und Werkzeuge werden APT28 zugeordnet.	C
Dienst	Bundesregierung und EU ordnen APT28 beziehungsweise Einheit 26165 dem GRU zu.	B
Individuum	Haftbefehl gegen Badin; offene Indizien zur Dienstzugehörigkeit.	B
Strafrechtliche Schuld	Kein Urteil im Material.	nicht A

Der Bundestag-Hack ist damit einer der am stärksten öffentlich belegten russischen Cyberfälle gegen Deutschland. Präzise formuliert ist er aber **offiziell dem GRU zugeschrieben und strafprozessual einem Beschuldigten zugeordnet**, nicht „rechtskräftig von einem GRU-Offizier begangen“.

2. SPIONAGE, AGENTENTÄTIGKEIT UND SABOTAGEVORBEREITUNG

2.1 Das russische „Illegalen“-Paar

Das OLG 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 ist besonders belastbar, weil nicht nur ein russischer Bezug politisch behauptet, sondern eine langfristige Agententätigkeit gerichtlich festgestellt wurde.

Evidenzklasse: A.

Die Aussagegrenze bleibt gleichwohl wichtig: Das Urteil belegt die Tätigkeit dieses Paars. Es ist kein pauschaler Nachweis über Umfang oder Struktur aller SWR-Aktivitäten in Deutschland.

2.2 Bundestagsgrundrisse

Ein Mitarbeiter einer Firma mit Tätigkeit für den Bundestag übermittelte Grundrisse von Parlamentsliegenschaften an einen GRU-Kontakt in der russischen Botschaft. Er wurde zu zwei Jahren Freiheitsstrafe auf Bewährung verurteilt. Der Verfassungsschutz fing die Nachricht nach den Berichten ab.

Evidenzklasse: A, soweit Übermittlung und Dienstbezug Gegenstand des Urteils waren.

Die offene Darstellung lässt jedoch nicht erkennen, ob konkrete Anschlagspläne bestanden. Das Weitergeben von Gebäudeplänen ist sicherheitsrelevant; daraus darf ohne zusätzliche Belege keine konkrete Sabotageabsicht abgeleitet werden.

2.3 Reserveoffizier Ralph G.

Die Bundesanwaltschaft erhob 2022 Anklage gegen den Reserveoffizier Ralph G. Ihm wurde vorgeworfen, Informationen über das Reservistenwesen, die zivil-militärische Zusammenarbeit, Waffensysteme und Nord Stream 2 an einen russischen Nachrichtendienst geliefert zu haben. Ergänzende Berichte nennen eine Verurteilung im November 2022 zu einem Jahr und neun Monaten auf Bewährung.

Für die Anklage gilt **Klasse B**; für die im Urteil festgestellte Agententätigkeit **Klasse A**. Soweit einzelne Informationskomplexe nur aus der Anklageschrift hervorgehen, sind sie nicht automatisch gerichtlich bestätigt.

Der Fall zeigt zudem, dass ein Agent weder hauptamtlicher Geheimdienstmitarbeiter noch klassisch angeworbener „Maulwurf“ sein muss. Die Quellen beschreiben teilweise Eigeninitiative und ideologische Sympathie. Das Motiv ist aber nur dann als festgestellt zu behandeln, wenn es im Urteil ausdrücklich festgestellt wurde.

2.4 Bundeswehrhauptmann Thomas H.

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

Evidenzklasse: A.

Der Fall belegt eine konkrete Agententätigkeit zugunsten Russlands. Er belegt nicht zwingend eine vorangegangene russische Rekrutierung; nach den Berichten ging die Initiative wesentlich von Thomas H. aus. Für die Bewertung staatlicher Verantwortung ist relevant, ob russische Stellen das Angebot annahmen oder steuerten. Die Verurteilung wegen Agententätigkeit zeigt einen hinreichenden Auslandsdienstbezug, erlaubt aber ohne Urteilsgründe keine weitergehende Rekonstruktion.

2.5 Carsten L. und Arthur E.

Die Bundesanwaltschaft erhob am 8. September 2023 Anklage gegen den BND-Beschäftigten Carsten L. und den Geschäftsmann Arthur E. wegen besonders schweren Landesverrats. Nach der Anklage entnahm Carsten L. neun Dokumente aus BND-Systemen. Arthur E. soll das Material bei Reisen nach Moskau dem FSB übergeben und Fragen des Dienstes zurückgebracht haben. Carsten L. soll weitere Informationen geliefert haben. Die Bundesanwaltschaft bezifferte die Zahlungen auf 450.000 Euro an Carsten L. und mindestens 400.000 Euro an Arthur E.

Die öffentlich zugängliche Qualität der Quelle ist hoch: Es handelt sich um eine konkrete Anklage mit benanntem Dienst, Tatzeit, Übermittlungsweg, Dokumentenzahl und Zahlungssummen. Dennoch bleibt sie eine Anklage.

Evidenzklasse: B.

Was bekannt ist:

- zwei namentlich bezeichnete deutsche Angeschuldigte;
- ein konkret benannter Empfänger, der russische FSB;
- beschriebene Reisen und Übergabewege;
- konkrete Dokumente und Zahlungen laut Anklage;
- Haftbefehle und Untersuchungshaft.

Was nicht als bewiesen gelten darf:

- die endgültige Täterschaft;
- sämtliche Einzelheiten der Anklage;
- ein rechtskräftig festgestellter Schaden;
- weitergehende Aussagen über eine umfassende Unterwanderung des BND.

2.6 Dieter S.

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, mit dem Ziel, die deutsche Unterstützung der Ukraine zu stören. Zwei Mitangeklagte erhielten Bewährungsstrafen.

Evidenzklasse: A.

Dieser Fall liegt an der Schnittstelle zwischen Spionage und Sabotagevorbereitung. Wichtig ist die Unterscheidung zwischen:

- ausgeführten Sabotageakten;
- konkreter Anschlagsplanung;
- Ausspähung möglicher Ziele;
- bloß allgemeinen Gesprächen oder Absichten.

Die Quelle stützt Spionage und geplante Brandanschläge, nicht zwangsläufig die erfolgreiche Durchführung dieser Anschläge.

2.7 Paket- und Brandsatzkomplex 2026

Die Bundesanwaltschaft erhob im Januar 2026 Anklage gegen Daniil B. und Vladyslav T.; Yevhen B. wurde anderweitig verfolgt. Der Vorwurf lautete auf Agententätigkeit zu Sabotagezwecken im Auftrag eines russischen Dienstes. Nach der Darstellung sollten Paketwege ausgespäht beziehungsweise Brandsätze über Logistiksysteme transportiert werden.

Im August 2026 wurde ein 30-jähriger ukrainischer Staatsangehöriger zu einem Jahr und drei Monaten Haft wegen geheimdienstlicher Agententätigkeit verurteilt. Zwei Mitangeklagte wurden freigesprochen, weil ihnen vorsätzliches Handeln nicht nachgewiesen werden konnte.

Der Fall ist ein Beispiel dafür, warum differenziert werden muss:

- Für den Verurteilten besteht **Klasse A**.
- Die Freisprüche sind ebenfalls gerichtliche Tatsachen mit hoher Relevanz: Sie widerlegen die pauschale Annahme, alle Beteiligten hätten wissentlich im russischen Auftrag gehandelt.
- Für darüber hinausgehende Hintermänner oder Dienststrukturen bleibt es bei **Klasse B**, soweit nur die Anklage vorliegt.

Freisprüche sind keine Randnotiz, sondern Teil der Beweisbilanz. Sie zeigen die Grenze zwischen objektiver Mitwirkung und nachweisbarem Vorsatz.

2.8 Ilona W.

Ilona W., eine deutsch-ukrainische PR-Unternehmerin beziehungsweise Lobbyistin, wurde im Januar 2026 festgenommen. Die Bundesanwaltschaft wirft ihr vor, seit November 2023 für einen russischen Nachrichtendienst Informationen über Rüstungsindustrie, Drohnentests und politische Veranstaltungen gesammelt sowie einem als Diplomaten auftretenden russischen Nachrichtendienstmitarbeiter Zugänge zu politischen und militärischen Netzwerken verschafft zu haben. Im September 2026 wurde Anklage erhoben.

Evidenzklasse: B.

Die Quellenlage erlaubt folgende Formulierung: Ilona W. ist angeklagt, nicht verurteilt. Die behauptete GRU-Verbindung und die Funktion des russischen Vizeattachés sind Gegenstand des Vorwurfs. Ihre gesellschaftlichen Kontakte beweisen für sich genommen keine Agententätigkeit.

2.9 Markus R. als Abgrenzungsfall

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

Dieser Fall darf nicht verkürzt als „für Russland verurteilter BND-Spion“ geführt werden. Die Verurteilung belegt Landesverrat, aber der zentrale Empfänger war nach der Quellenlage ein US-Dienst. Der russische Bezug besteht im zusätzlichen Angebot und ist für die hier untersuchte Fragestellung nur eingeschränkt aussagekräftig.

3. UNTERSEEKABEL, NORD STREAM UND KRITISCHE INFRASTRUKTUR

3.1 Nord Stream: gesicherte Tatsachen und Ermittlungsrichtung

Im September 2022 wurden Nord Stream 1 und 2 durch Explosionen beschädigt. Vier Lecks entstanden an drei der vier Leitungsstränge. Deutsche Ermittlungen konzentrierten sich auf die Segelyacht *Andromeda* und mehrere ukrainische Staatsangehörige.

Die Ermittlungen führten zu Haftbefehlen. Ein Verdächtiger, Wolodymyr Z., soll sich 2024 der Festnahme in Polen entzogen haben. Im August 2025 wurde Serhij K. in Italien festgenommen; ihm wird eine koordinierende Rolle zugeschrieben. Ein weiterer ukrainischer Tatverdächtiger und Berufstaucher wurde 2025 in Polen festgenommen.

Diese Angaben haben unterschiedliche Qualität. Die Existenz von Haftbefehlen und Festnahmen ist formelle Strafverfolgung, also **Klasse B**. Einzelne Rollenbeschreibungen bleiben Anklage- beziehungsweise Verdachtsstoff.

3.2 BGH-Entscheidung vom 10. Dezember 2025

Der Bundesgerichtshof verwarf am 10. Dezember 2025 die Haftbeschwerde eines Beschuldigten. Er bejahte deutschen Strafanspruch und dringenden Tatverdacht wegen verfassungsfeindlicher Sabotage in Tateinheit mit dem Herbeiführen einer Sprengstoffexplosion. Der Beschuldigte soll als Offizier einer ukrainischen Spezialeinheit eine koordinierende Rolle gespielt haben.

Der BGH entschied außerdem, der Beschuldigte könne sich bei einem verdeckten Gewaltakt gegen zivile Infrastruktur nicht auf funktionelle Immunität oder ein Kombattantenprivileg berufen.

Dabei handelt es sich um eine gerichtliche Feststellung im Haftverfahren, nicht um ein rechtskräftiges Schuldurteil nach Hauptverhandlung. Der dringende Tatverdacht ist daher **Klasse B**, die rechtliche Aussage zur Immunität eine gerichtliche Tatsachen- und Rechtsbewertung, aber kein endgültiger Schuldspruch.

3.3 Keine belastbare Russland-Zurechnung

Aus den ausgewerteten Quellen folgt ausdrücklich nicht, dass Russland die Nord-Stream-Leitungen sprengte. Die konkreteste öffentlich bekannte deutsche Ermittlungsrichtung betrifft ukrainische Tatverdächtige. Auch daraus folgt noch keine rechtskräftige staatliche Attribution an die Ukraine: Die Nationalität von Tatverdächtigen, eine behauptete frühere Dienststellung oder ein möglicher staatlicher Auftrag müssen getrennt bewiesen werden.

Für Nord Stream gilt deshalb:

Frage	Öffentlicher Stand
Wurden die Leitungen vorsätzlich gesprengt?	Durch Explosions- und Ermittlungsbefunde stark gestützt.

Frage	Öffentlicher Stand
Gibt es konkrete Tatverdächtige?	Ja, mehrere ukrainische Staatsangehörige; Haftbefehle und Festnahmen.
Gibt es ein Endurteil?	Im Material nein.
Hat der BGH dringenden Tatverdacht bestätigt?	Ja, gegen einen mutmaßlichen Koordinator.
Ist Russland rechtskräftig verantwortlich?	Nein.
Ist der ukrainische Staat rechtskräftig verantwortlich?	Ebenfalls nein.

Pauschale Behauptungen, Nord Stream sei ein bewiesener russischer Sabotageakt, sind mit der öffentlichen deutschen Verfahrenslage unvereinbar.

3.4 Balticconnector

Am 8. Oktober 2023 kam es an der Gasleitung Balticconnector zwischen Finnland und Estland zu einem Druckabfall. Die Leckstelle lag in der finnischen ausschließlichen Wirtschaftszone. Finnische Ermittler kamen zu dem Ergebnis, dass der Anker des unter Hongkong-Flagge fahrenden Schiffes *Newnew Polar Bear* die Leitung beschädigte. Die Untersuchung lief jedenfalls im Mai 2025 weiter; finnische Behörden kooperierten mit chinesischen und Hongkonger Stellen.

Hier sind drei Ebenen zu trennen:

1. **Physische Verursachung:** Der Anker des Schiffes wird offiziell als Ursache genannt.
2. **Vorsatz:** Die Untersuchung sollte weiterhin klären, ob absichtlich gehandelt wurde.
3. **Staatliche Attribution:** Eine russische Steuerung ergibt sich aus den vorliegenden offiziellen Befunden nicht.

Evidenzklasse: B/C für die physische Ursache, **D** für eine darüber hinausgehende pauschale Russland-Zuordnung.

3.5 Estlink 2 und andere Ostseevorfälle

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

Bei Unterseekabeln sind außerdem alternative Erklärungen einzubeziehen:

- Ankerziehen durch Navigationsfehler;
- technische Defekte;
- wetter- oder materialbedingte Schäden;
- fahrlässige Schiffsführung;
- privatwirtschaftliche oder kriminelle Handlungen;
- vorsätzliche Sabotage ohne staatlichen Auftrag;
- staatlich gesteuerte Sabotage.

Die bloße Gleichzeitigkeit mehrerer Schäden, die Lage in der Ostsee oder eine Verbindung eines Schiffes mit russischen Häfen reichen nicht für eine staatliche Attribution.

3.6 Deutsche Regierungseinschätzungen zur Infrastrukturgefahr

Die Bundesregierung beschreibt Spionage, Sabotage, Cyberangriffe, Drohnenaktivitäten und Desinformation als Teile einer verschärften hybriden Bedrohungslage. Sie benennt Russland in allgemeinen Bewertungen als wichtigen Urheber solcher Aktivitäten und begründet damit Maßnahmen zum Schutz kritischer Infrastruktur, NIS-2-Umsetzung und das KRITIS-Dachgesetz.

Diese Aussagen sind für die **allgemeine Lagebewertung Klasse B oder D**, je nach Konkretisierungsgrad. Sie ersetzen bei einzelnen Kabel-, Pipeline- oder Drohnenvorfällen keine tatbezogene Attribution.

4. BFV, BSI, BND UND BUNDESREGIERUNG: WAS WURDE TATSÄCHLICH VERÖFFENTLICHT?

4.1 Bundesamt für Verfassungsschutz

Das bereitgestellte Material enthält allgemeine Hinweise, wonach das BfV russische Nachrichtendienste als Akteure klassischer Spionage, der Ausspähung kritischer Infrastruktur, der Sabotagevorbereitung und von Einflussoperationen bewertet.

Die öffentliche Aussagekraft solcher Bewertungen hängt davon ab, was publiziert wird:

- Benennt das BfV nur eine Gefahrenkategorie, liegt eine Lageeinschätzung vor.
- Benennt es eine Operation, Infrastruktur und konkrete Indikatoren, steigt die Überprüfbarkeit.

- Benennt es Einzelpersonen ohne offengelegte Belege, bleibt die externe Prüfung begrenzt.
- Wird ein Fall an die Strafverfolgung übergeben und führt zu Anklage oder Urteil, entsteht eine unabhängige zweite Beweisebene.

Für Storm-1516 enthält das Material keine belastbare BfV-Primärquelle. Die Suchergebnisse unter „bfv.de“ betrafen irrtümlich den Bayerischen Fußball-Verband und sind für Verfassungsschutzfragen unbrauchbar. Eine behauptete BfV-Zuschreibung darf daher nicht allein auf diese Fundstellen gestützt werden.

4.2 Bundesamt für Sicherheit in der Informationstechnik

Im bereitgestellten Quellenmaterial findet sich keine hinreichend konkrete BSI-Primärveröffentlichung zu den hier untersuchten Einzelfällen russischer Aktivitäten. Deshalb kann nicht seriös behauptet werden, das BSI habe bestimmte Gruppen, Personen oder Dienste in einem bestimmten Fall mit eigener öffentlich dargelegter Forensik identifiziert.

Das ist ein Negativbefund über die verfügbare Dokumentation, nicht über das Wissen des BSI. Möglich ist, dass technische Informationen vertraulich mit Betroffenen oder Partnerbehörden geteilt wurden. Für eine öffentliche Beweiswürdigung gilt jedoch: Ohne zugängliche technische Indikatoren, Malwareanalysen oder Attributionsbegründungen kann keine eigenständige BSI-Beweiskette rekonstruiert werden.

Demgegenüber liegt für einen nicht-russischen Fall eine BSI-Primärquelle vor, die analytisch relevant ist: Die Cyber-Sicherheitswarnung CSW 2021-234348-1032 vom 27. Juli 2021 betrifft die israelische Spionagesoftware Pegasus (NSO Group). Das BSI beschreibt darin das Bedrohungspotenzial als “hoch”, räumt ein, dass Schutzmaßnahmen “aufgrund der Professionalität der Angreifer sehr schwierig” seien, und bestätigt, dass aktuelle iOS- und Android-Versionen weiterhin verwundbar sind. Die amtliche Gefahreneinstufung auf der Kopfzeile desselben Dokuments lautet 2/Gelb. Das BKA nutzte dieselbe Software seit März 2021 (vier Monate vor dieser Warnung). Dieser Befund ist für die Beurteilung der BSI-Klassifizierungspraxis relevant: Die Einstufung einer Bedrohung hängt offensichtlich nicht ausschließlich vom technischen Schadpotenzial ab.

4.3 Bundesnachrichtendienst

Öffentlich nachvollziehbare BND-Bezüge bestehen vor allem über Strafverfahren:

- Der Fall Carsten L./Arthur E. betrifft den mutmaßlichen Abfluss von BND-Staatsgeheimnissen an den FSB. Die veröffentlichte Quelle ist die Anklage der Bundesanwaltschaft, nicht ein technischer BND-Bericht.
- Der BND kann Erkenntnisse zu ausländischen Akteuren beigetragen haben; die entsprechenden Quellen und Methoden sind regelmäßig nicht öffentlich.
- Nicht veröffentlichte Nachrichtendienstinformationen können eine behördliche Attribution tragen, sind aber extern nicht überprüfbar.

Die zurückhaltende Formulierung lautet daher nicht: „Der BND hat öffentlich bewiesen“, sondern: „Deutsche Behörden haben unter Einbeziehung nachrichtendienstlicher Erkenntnisse offiziell zugeschrieben“, soweit dies die konkrete Quelle trägt.

4.4 Bundesregierung und Auswärtiges Amt

Beim Bundestag-Hack ging die Bundesregierung über eine allgemeine Bedrohungsbewertung hinaus. Das Auswärtige Amt bestellte den russischen Botschafter ein, bezeichnete Badin und den GRU als Verantwortliche und unterstützte EU-Sanktionen.

Bei kritischer Infrastruktur sind die Aussagen breiter. Die Bundesregierung spricht von systematischen hybriden Bedrohungen und benennt Russland als maßgeblichen Akteur. Solche Erklärungen publizieren jedoch regelmäßig:

- eine politische Lagebewertung;
- teilweise eine Täter- oder Staatenzuordnung;
- selten vollständige technische Indikatoren;
- keine gerichtliche Beweisaufnahme;
- häufig keine Offenlegung nachrichtendienstlicher Quellen.

Ihre Evidenzklasse ist deshalb fallabhängig. Für eine allgemeine Gefahreneinschätzung kann eine offizielle Stellungnahme genügen; für individuelle strafrechtliche Schuld nicht.

5. DESINFORMATION UND STAATLICH RUSSISCHER BEZUG

5.1 RT und Sputnik

Die EU behandelt russische staatliche beziehungsweise staatlich kontrollierte Medien als Bestandteile eines breiteren Informationsökosystems, das Narrative gegen die Ukraine, die EU und die NATO verbreitet. Das Material beschreibt wiederkehrende Darstellungen von NATO und EU als aggressive Bedrohungen und verknüpft diese mit staatlich kontrollierter russischer Kommunikation.

Hier muss zwischen verschiedenen Kategorien unterschieden werden:

- nachweislich falsche Tatsachenbehauptung;

- einseitige oder propagandistische Auswahl wahrer Tatsachen;
- politische Meinung;
- staatliche Finanzierung oder Kontrolle;
- verdeckte Identitätstäuschung;
- koordinierte Plattformmanipulation.

Die staatliche Verbindung eines Mediums macht nicht jede einzelne Veröffentlichung falsch. Umgekehrt kann eine nachweislich falsche Veröffentlichung unabhängig von der Trägerschaft untersucht werden. Im vorliegenden Material fehlt eine hinreichend detaillierte, einzelfallbezogene Analyse bestimmter RT- oder Sputnik-Beiträge zu Deutschland. Deshalb ist nur die allgemeine Einordnung als Teil eines staatlich russischen Kommunikationssystems belastbar, nicht eine pauschale Bewertung sämtlicher Inhalte.

5.2 „Doppelgänger“

„Doppelgänger“ ist im öffentlichen Quellenmaterial die am besten dokumentierte Desinformationskampagne. Kennzeichnend sind:

- täuschend nachgebildete Internetseiten etablierter Medien und staatlicher Institutionen;
- gefälschte Artikel;
- koordinierte inauthentische Social-Media-Konten;
- Bot- und Verstärkernetzwerke;
- pro-kremlfreundliche Narrative;
- Zielgruppen in Deutschland, Frankreich, der Ukraine, den USA und anderen Staaten.

Der EEAS ordnet „Doppelgänger“ russischen Akteuren zu und nennt die Kampagne als prominentes Beispiel für Foreign Information Manipulation and Interference. Der EU-Rat verhängte Sanktionen gegen Personen und Einrichtungen, die mit der Kampagne verbunden wurden. Dazu gehören Nikolai Tupikin, die Social Design Agency und Struktura; Sofia Zakharova wurde als Funktionsträgerin im Umfeld der russischen Präsidialadministration bezeichnet.

Die Beweisstruktur ist mehrschichtig:

Ebene	Öffentliche Evidenz
Existenz gefälschter Websites	Direkt prüfbar; Klasse C
koordinierte Verbreitung	Technische Netzwerk- und Plattformanalyse; Klasse C
organisatorische Verbindung zu SDA/Struktura	EU-Attribution und offene Analyse; Klasse B/C
Verbindung zur Präsidialadministration	EU-Sanktionsbegründung; Klasse B
individuelle Strafschuld	Kein einschlägiges Urteil im Material

Sanktionen erhöhen das offizielle Gewicht, bleiben aber Verwaltungsmaßnahmen. „Doppelgänger“ ist daher **offiziell zugeschrieben und technisch substanziell belegt**, nicht gerichtlich abschließend bewiesen.

5.3 „Ghostwriter“

Die Europäische Kommission beschreibt „Ghostwriter“ als längerfristige, aus Russland und Belarus stammende Operation, die Cyberzugriffe mit Einflussmaßnahmen verbindet und insbesondere NATO-Staaten sowie die Ukraine adressiert.

Die Kombination aus kompromittierten Konten und anschließender Veröffentlichung manipulierter Inhalte ist analytisch bedeutsam: Cyberzugriff und Informationsoperation können Teil derselben Kette sein. Gleichwohl enthält das Material keine deutsche Anklage und kein Urteil gegen konkrete Operatoren.

Evidenzklasse: B/C, je nach konkretem Teilbefund. Die politische oder dienstliche Gesamtzuordnung bleibt ohne Veröffentlichung der vollständigen Forensik extern nur teilweise überprüfbar.

5.4 „Storm-1516“

Storm-1516 wird als russisch ausgerichtetes Netzwerk beschrieben, das gefälschte „Whistleblower“-Videos, KI-generierte Personen, manipulierte Dokumente und nachgeahmte Medienmarken verwendet. Inhalte werden über „Pravda“-Seiten, Bots und reichweitenstarke Multiplikatoren verbreitet.

Einige Quellen bringen das Netzwerk mit der GRU-Einheit 29155 und dem Center for Geopolitical Expertise in Verbindung. John Mark Dougan wird als wichtiger Betreiber oder Verstärker beschrieben; die EU sanktionierte ihn nach den Berichten im Dezember 2025 wegen seiner Rolle in einem Netzwerk gefälschter Websites.

Die öffentliche Beweislage ist schwächer als beim Bundestag-Hack:

- Kampagneninhalte und gefälschte Webseiten sind sichtbar.
- technische und semantische Gemeinsamkeiten können untersucht werden;
- einzelne Betreiber und Infrastrukturverbindungen werden in offenen Quellen genannt;
- die unmittelbare GRU-Steuerung ist im Material nicht durch deutsche Strafverfolgung oder ein Urteil festgestellt.

Evidenzklasse: C für das Netzwerk und seine Methoden; **B oder D** für die Dienstzuordnung, abhängig davon, ob eine konkrete Behörde mit nachvollziehbarer Begründung zitiert wird. Eine pauschale Formulierung „Storm-1516 ist gerichtlich erwiesen GRU“ wäre unzutreffend.

5.5 Ursula von der Leyen als Ziel

Das Material dokumentiert mehrere gegen Ursula von der Leyen gerichtete Narrativtypen:

- ein synthetisches beziehungsweise als Deepfake bezeichnetes russischsprachiges „Interview“ in einer russischen Fernsehsendung;
- manipulierte Genealogie- und „Nazi-Vorfahren“-Behauptungen;
- nachgeahmte Medienauftritte und Bildmontagen.

Die wiederkehrende Behauptung einer genealogischen Verbindung zu NS-Funktionären wurde von Faktenprüfern als falsch bewertet. Bei dem 2025 ausgestrahlten synthetischen Interview soll ein KI-Hinweis enthalten gewesen sein. Das ist für die Täuschungsbewertung relevant: Satire oder gekennzeichnete Synthese unterscheidet sich von verdeckt als echt verbreitetem Material. Entscheidend ist daher nicht nur die Produktion, sondern auch, wie das Material anschließend ausgespielt und kontextualisiert wurde.

Evidenzklasse: C für die Existenz konkreter manipulierter Inhalte; die staatliche Steuerung ist je nach Verbreitungskanal **B/C**. Nicht jeder von russischsprachigen Accounts verbreitete Angriff auf von der Leyen ist damit automatisch eine staatliche Operation.

6. POLITISCHE EINFLUSSNAHME UND WAHLBEEINFLUSSUNG

6.1 Begriffliche Trennung

Politische Einflussnahme kann legal, illegitim oder strafbar sein. Zu unterscheiden sind:

- offene Diplomatie;
- staatliche Auslandsmedien;
- Parteikontakte und öffentliche Sympathiebekundungen;
- Lobbyismus;
- verdeckte Sach- oder Geldleistungen;
- illegale Parteienfinanzierung;
- kompromittierende Informationsbeschaffung;
- verdeckte Desinformation;
- Cyberangriffe auf Parteien und Politiker;
- operative Unterstützung einzelner Kandidaten.

Eine ideologische Übereinstimmung mit russischen Positionen ist kein Beweis russischer Steuerung. Ebenso beweist ein Kontakt zu russischen Amtsträgern keine Zahlung.

6.2 Dokumentierte Einflussinstrumente

Öffentlich besser belegt als direkte Parteienfinanzierung sind digitale Einflusskampagnen. „Doppelgänger“ zielte nach EU-Darstellungen auf demokratische Prozesse und die Europawahl 2024. Die „Portal Kombat“- beziehungsweise „Pravda“-Netzwerke verbreiteten mehrsprachige Inhalte, darunter auf Deutsch. Ghostwriter verband Cyberzugriffe mit manipulativen Veröffentlichungen.

Diese Befunde belegen das Vorhandensein von Einflussinstrumenten. Ob sie das Verhalten einer relevanten Zahl von Wählern tatsächlich veränderten, ist eine andere Frage. Reichweite, Interaktion und messbarer Wahleffekt dürfen nicht gleichgesetzt werden.

6.3 AfD-Finanzierungsbehauptungen

Für eine pauschale Behauptung, die AfD werde vom russischen Staat finanziert, fehlen im vorliegenden Material die erforderlichen Belege. Es liegt keine dokumentierte Kombination aus folgenden Elementen vor:

- identifizierter russischer Zahler;
- konkreter Empfänger innerhalb der Partei;
- Betrag und Datum;
- Bank- oder Vertragsunterlagen;

- Gegenleistung;
- Anklage oder Urteil;
- förmliche Feststellung einer zuständigen deutschen Kontrollinstanz.

Daher ist die pauschale Behauptung **Klasse D**.

Auch EU-Sanktionen gegen einzelne Akteure wegen russischer Einflussoperationen wären getrennt von deutschem Parteienfinanzierungsrecht zu behandeln. Eine Sanktionslistung beweist nicht automatisch, dass eine Partei als Organisation Geld erhielt. Umgekehrt würde eine konkrete rechtswidrige Zahlung nicht ohne Weiteres beweisen, dass sämtliche politischen Positionen der Empfänger fremdgesteuert sind.

Die korrekte Aussage lautet: Das vorliegende Quellenmaterial erlaubt keine verlässliche Feststellung einer systematischen russischen Finanzierung der AfD. Es erlaubt ebenso wenig den Schluss, mögliche Einzelkontakte oder Unterstützungsleistungen seien ausgeschlossen. Der öffentliche Belegstatus bleibt offen.

6.4 Wahlbeeinflussung als Wirkungsbehauptung

Eine Kampagne kann auf Wahlbeeinflussung zielen, ohne nachweisbar den Wahlausgang beeinflusst zu haben. Vier Ebenen sind zu unterscheiden:

1. Veröffentlichung manipulativer Inhalte;
2. gezielte Ausrichtung auf Wähler oder Kandidaten;
3. messbare Rezeption;
4. kausale Veränderung von Wahlentscheidung oder Wahlergebnis.

Die vorliegenden EU-Quellen tragen vor allem die ersten beiden Ebenen. Für eine kausale Änderung deutscher Wahlergebnisse enthalten sie keine belastbare Quantifizierung.

7. EU-, NATO-, US- UND PARTNERATTRIBUTIONEN

7.1 Europäische Union

Die EU hat in den untersuchten Fällen zwei besonders konkrete Instrumente eingesetzt:

- Cyber-Sanktionen gegen Badin, Kostyukov und die GRU-Einheit 26165 wegen des Bundestag-Angriffs;
- Sanktionen nach dem 2024 geschaffenen Regime gegen russische hybride Aktivitäten und FIMI, unter anderem gegen Beteiligte an „Doppelgänger“.

Der EEAS veröffentlicht darüber hinaus Lageberichte, Kampagnenanalysen und methodische Leitlinien. Für 2024 wurden mehr als 500 FIMI-Vorfälle in 90 Ländern erfasst; diese Zahl beschreibt dokumentierte Vorfälle, nicht 500 gerichtlich bewiesene russische Straftaten.

Die institutionelle Quellengüte ist differenziert:

EU-Quelle	Publizierter Inhalt	Beweiswert
EU-Rat, Sanktionsrechtsakt	Namen, Organisationen, politische Verantwortungsgründe, Rechtsfolgen	Offizielle Attribution, Klasse B
EEAS-FIMI-Bericht	Kampagnenmuster, Infrastruktur, Ziele, Fallbeispiele	B/C
CERT-EU	technische Warnungen und Indikatoren, soweit publiziert	C
Europäische Kommission	regulatorische und politische Lagebewertung	B/D
EU-Sanktionsliste	administrative Listung	kein Strafurteil

7.2 NATO

Das Material enthält keine ausreichend detaillierte NATO-Primärdarstellung, aus der eine eigenständige, technisch begründete NATO-Attribution jedes behandelten Einzelfalls rekonstruiert werden könnte. NATO-Partner werden im Zusammenhang mit koordinierter Reaktion auf russische Cyber- und Informationsaktivitäten genannt, doch die konkretesten öffentlich nachvollziehbaren Attributionen im Bundestag-Fall stammen von Deutschland, der EU und dem Vereinigten Königreich.

Eine gemeinsame politische Verurteilung durch NATO-Staaten erhöht das diplomatische Gewicht einer Attribution. Sie ist dennoch weder eine internationale gerichtliche Entscheidung noch ein Ersatz für veröffentlichte technische Beweise.

7.3 Vereinigte Staaten

US-Behörden suchten Dmitry Badin auch wegen anderer Cyberoperationen, darunter Eingriffe im Umfeld der US-Wahl 2016 und Angriffe auf WADA. Dies stützt die Identifizierung Badins als wiederholt beschuldigten Operator der Einheit 26165, ist aber kein deutsches Urteil zum Bundestag-Hack.

US-amerikanische technische und strafrechtliche Erkenntnisse können deutsche Ermittlungen gestützt haben. Die öffentliche deutsche Zurechnung darf jedoch nicht mit amerikanischen Vorwürfen zu anderen Taten vermengt werden. Für jeden Tatkomplex gelten eigene Tatbestands-, Zuständigkeits- und Beweisfragen.

7.4 Vereinigtes Königreich und weitere Partner

Das Vereinigte Königreich verhängte im Zusammenhang mit dem Bundestag-Hack Maßnahmen gegen die Einheit 26165 und russische Offiziere. Niederländische Erkenntnisse aus der Aufdeckung eines GRU-Einsatzes gegen die Organisation für das Verbot chemischer Waffen wurden nach den Berichten für weitere Ermittlungen bedeutsam.

Partnerinformationen können eine Attribution stark verdichten. Ihre externe Überprüfbarkeit hängt aber davon ab, ob Geräte, Registrierungsdaten, Reisebewegungen oder technische Protokolle veröffentlicht wurden oder lediglich das Ergebnis mitgeteilt wird.

8. QUELLENKRITISCHE BEWERTUNG DER INSTITUTIONEN

8.1 Gerichte

Gerichte bieten den stärksten öffentlichen Beweiswert, wenn sie nach Hauptverhandlung urteilen. Aber auch gerichtliche Dokumente unterscheiden sich:

- Ein Haftbefehl bestätigt dringenden Tatverdacht, nicht Schuld.
- Eine Haftbeschwerdeentscheidung prüft vorläufige Beweislage und Rechtsfragen.
- Ein erstinstanzliches Urteil kann angefochten sein.
- Ein rechtskräftiges Urteil hat den höchsten Status.
- Selbst ein Urteil bindet nur hinsichtlich des entschiedenen Falls.

Beim Nord-Stream-Komplex ist der BGH-Beschluss deshalb nicht als endgültige Täterfeststellung zu lesen. Bei den verurteilten Agenten ist die gerichtliche Beweisqualität höher, soweit die Urteile rechtskräftig wurden.

8.2 Generalbundesanwalt

Mitteilungen der Bundesanwaltschaft publizieren häufig:

- Identität oder Initialen von Beschuldigten;
- Staatsangehörigkeit;
- vorgeworfene Straftatbestände;
- Tatzeit und mutmaßlichen Auftraggeber;
- Grundzüge der Beweislage;
- Haft- und Verfahrensstatus.

Die Mitteilung zu Carsten L. und Arthur E. ist wegen ihrer Detailtiefe besonders aussagekräftig. Sie bleibt gleichwohl die Darstellung der Anklagebehörde.

8.3 Bundesregierung und Auswärtiges Amt

Diese Stellen veröffentlichen politische Attributionen, diplomatische Maßnahmen und Lageeinschätzungen. Beim Bundestag-Hack wurde ein konkreter Beschuldigter und Dienst genannt. Bei allgemeinen Aussagen über hybride Bedrohungen werden häufig keine technischen Details offengelegt.

Die Quellen sind autoritativ dafür, **dass** die Bundesregierung eine bestimmte Bewertung vertritt. Sie sind nicht automatisch vollständiger Beweis dafür, **warum** diese Bewertung zutrifft.

8.4 EU-Rat und EEAS

Der EU-Rat benennt in Sanktionsakten Personen, Organisationen und Gründe. Der EEAS veröffentlicht analytische FIMI-Berichte. Beide sind Primärquellen für die EU-Position; die zugrunde liegenden technischen und nachrichtendienstlichen Daten sind nur teilweise öffentlich.

Bei „Doppelgänger“ ist die Kombination aus offen sichtbaren Kopien legitimer Medien, technischer Netzwerkanalyse und EU-Listungen vergleichsweise stark.

8.5 Technische Unternehmen und OSINT

Technische Firmen können hochauflösende Daten zu Malware, Servern, Zertifikaten, Domains und Operatorverhalten liefern. Ihre Clusterbezeichnungen und Schwellenwerte unterscheiden sich jedoch. Ein kommerzieller Bericht ist keine neutrale Gerichtsentscheidung.

OSINT kann Identitäten und institutionelle Verbindungen überzeugend stützen, wie bei Badins Registrierungsdaten. Es ist besonders wertvoll, wenn:

- Rohdaten benannt werden;
- der Untersuchungspfad reproduzierbar ist;
- mehrere unabhängige Quellen übereinstimmen;
- Alternativerklärungen geprüft werden.

8.6 Medien

Seriöse Medien sind unverzichtbar, wenn Urteile oder laufende Verfahren nicht vollständig veröffentlicht werden. Sie bleiben gegenüber Gerichten und Behörden sekundär. Einzelne Berichte sollten nicht zur Grundlage weitreichender Staatsattributionen werden, insbesondere wenn sie anonyme Nachrichtendienstquellen wiedergeben.

8.7 Russische Selbstdarstellung

Die Valdai-Transkripte zeigen, wie die russische Führung die internationale Lage rahmt: Sie bezeichnet westliche Politik als aggressiv, betont Gegenseitigkeit und kündigt spiegelbildliche Maßnahmen bei maritimen Eingriffen an. Das ist relevanter Kommunikationskontext. Es beweist weder den Bundestag-Hack noch Kabelsabotage, Spionage oder Desinformationskampagnen. Keine verdeckte Operation darf allein aus strategischer Rhetorik abgeleitet werden.

9. WAS DIE ÖFFENTLICHE EVIDENZ NICHT HERGIBT

9.1 Keine Russland-Zurechnung von Nord Stream

Die öffentliche deutsche Strafverfolgungslage trägt keine Behauptung, Russland habe Nord Stream gesprengt. Der BGH befasste sich mit einem ukrainischen Tatverdächtigen und einem möglichen fremdstaatlichen Auftrag, ohne ein Endurteil zu fällen.

Ebenso voreilig wäre die gegenteilige Behauptung, der ukrainische Staat sei rechtskräftig überführt. Festnahme, militärischer Hintergrund und ukrainische Staatsangehörigkeit beweisen keinen staatlichen Befehl.

9.2 Keine pauschale Russland-Zurechnung aller Ostsee-Kabelschäden

Die Balticconnector-Ermittlung identifiziert einen Anker als physische Ursache, lässt aber Fragen des Vorsatzes und staatlicher Steuerung offen. Zu Estlink 2 fehlt im Material eine hinreichend konkrete Attribution.

Daraus folgt: Eine Serie von Vorfällen kann Anlass für erhöhte Aufmerksamkeit sein, aber nicht Ersatz für fallbezogene Ermittlungen.

9.3 Keine pauschale russische Finanzierung der AfD

Das Quellenmaterial enthält keinen ausreichenden Beleg für eine systematische Finanzierung der AfD durch den russischen Staat. Ohne Zahlungsnachweis, Anklage, Urteil oder konkrete behördliche Tatsachenfeststellung bleibt die Behauptung ungesichert.

Auch politische Nähe, Reisen, Interviews in russischen Medien oder die Übernahme russischer Narrative wären für sich genommen kein Finanzierungsnachweis.

9.4 Keine Kollektivzurechnung

Verurteilte russische Agenten, einzelne russische Staatsbedienstete oder staatlich kontrollierte Medien repräsentieren nicht „die Russen“ oder die russische Bevölkerung. Der Bericht bewertet individuelle, organisatorische und staatliche Verantwortung, nicht ethnische oder nationale Kollektivschuld.

9.5 Keine automatische Gleichsetzung von Attribution und Urteil

Wenn Bundesregierung, EU oder NATO einen Akteur benennen, ist die korrekte Formulierung „offiziell zugeschrieben“. „Gerichtlich bewiesen“ ist nur zulässig, wenn ein Gericht den betreffenden Sachverhalt festgestellt hat.

9.6 Keine weitreichende Schuldbehauptung allein aus Geheimdienstinformationen

Nachrichtendienste können über Quellen verfügen, die aus Schutzgründen nicht veröffentlicht werden. Das ist kein Beleg dafür, dass die Bewertung falsch ist. Für eine öffentliche Beweiswürdigung entsteht jedoch ein strukturelles Defizit:

- Quellen können nicht auf Zuverlässigkeit geprüft werden;

- technische Alternativerklärungen bleiben unbekannt;
- mögliche politische Auswahlentscheidungen sind schwer kontrollierbar;
- Betroffene können die Beweise öffentlich nicht widerlegen.

Daher gehören nicht offengelegte Nachrichtendienstbehauptungen ohne ergänzende Justiz- oder Forensikbelege in Klasse D, selbst wenn sie politisch plausibel erscheinen.

9.7 Kein sicherer Nachweis messbarer Wahlausgänge

Die Existenz russisch zugeschriebener Desinformationskampagnen beweist weder eine bestimmte Zahl beeinflusster Stimmen noch eine Veränderung des Wahlergebnisses. Ziel, Reichweite und Wirkung sind getrennte Kategorien.

9.8 Keine vollständige BSI-Beweiskette

Aus dem bereitgestellten Material lässt sich keine eigenständige öffentliche BSI-Attribution mit technischen Indikatoren für die zentralen Fälle rekonstruieren. Es wäre deshalb irreführend, eine solche Analyse zu behaupten.

10. VERGLEICHENDE GESAMTBEWERTUNG

Stark belegt

Gerichtlich am stärksten belegt sind konkrete Agententätigkeiten:

- das russische „Illegalen“-Paar und seine Tätigkeit für den SWR;
- die Weitergabe von Bundestagsgrundrissen an einen GRU-Kontakt;
- Agententätigkeit eines Bundeswehrhauptmanns;
- Spionage und Sabotageplanung durch Dieter S.;
- der 2026 verurteilte Beteiligte im Paket- beziehungsweise Sabotagekomplex, bei gleichzeitigen Freisprüchen zweier Mitangeklagter.

Diese Fälle zeigen, dass russische Dienste oder russische Auftraggeber in Deutschland Informationen beschaffen und teilweise Sabotageziele verfolgen ließen. Sie beweisen jedoch keinen allumfassenden, zentral gesteuerten „Masterplan“.

Offiziell zugeschrieben und technisch gut gestützt

Der Bundestag-Hack gehört in diese Kategorie. Angriff, Datendiebstahl, APT28-Muster, Einheit 26165, Badins Identität, deutscher Haftbefehl und EU-Sanktionen bilden eine konsistente Beweiskette. Die fehlende Hauptverhandlung verhindert die Einstufung der individuellen Schuld als Klasse A.

„Doppelgänger“ ist ebenfalls stark dokumentiert: Die Täuschungsinfrastruktur ist offen sichtbar, EU-Stellen haben Organisationen und Personen benannt und Sanktionen erlassen. Die strafrechtliche Individualverantwortung ist gleichwohl nicht gerichtlich festgestellt.

Formell verfolgt, aber nicht entschieden

Dazu gehören:

- Carsten L. und Arthur E. mit dem Vorwurf der Weitergabe von BND-Staatsgeheimnissen an den FSB;
- Ilona W. mit dem Vorwurf geheimdienstlicher Tätigkeit und Kontaktvermittlung;
- einzelne Hintermänner und Mitwirkende von Sabotage- oder Desinformationsnetzwerken.

Bei diesen Fällen ist die Quellenlage konkreter als ein bloßes Gerücht. Die Unschuldsvermutung bleibt uneingeschränkt bestehen.

Technisch oder analytisch plausibel, aber nicht gerichtlich bestätigt

Hierzu gehören Teile der Zuordnung von Ghostwriter und Storm-1516. Die Kampagnenmuster sind dokumentiert; die genaue Befehlskette zu russischen Diensten ist öffentlich nicht immer vollständig nachvollziehbar.

Offen oder umstritten

Offen bleiben insbesondere:

- die endgültige Täterschaft und staatliche Auftragsebene bei Nord Stream;
- Vorsatz und staatliche Steuerung bei mehreren Ostsee-Infrastrukturvorfällen;
- pauschale Russland-Zurechnungen sämtlicher Kabelschäden;
- pauschale AfD-Finanzierungsbehauptungen;
- die konkrete Wirkung russischer Desinformation auf deutsche Wahlergebnisse;
- weitreichende Schuldbehauptungen, die nur auf nicht veröffentlichten Nachrichtendienstinformationen beruhen.

SCHLUSSBEFUND

Die öffentliche Evidenz belegt nicht „Russlands Hybridkrieg“ als einheitlichen, in allen Teilen gerichtlich erwiesenen Gesamtkomplex. Sie belegt vielmehr eine Reihe unterschiedlich gut dokumentierter Einzeloperationen und Strukturen.

Am belastbarsten sind rechtskräftige oder jedenfalls gerichtlich festgestellte Agentenfälle. Sie zeigen tatsächliche geheimdienstliche Tätigkeit für russische Dienste und in einzelnen Fällen die Ausspähung militärischer, parlamentarischer oder infrastruktureller Informationen. Ebenfalls stark ist die öffentliche Beweislage beim Bundestag-Hack: Der Angriff selbst und seine Zuordnung zu APT28 sind technisch gut dokumentiert; Deutschland und die EU ordneten ihn dem GRU und der Einheit 26165 zu; gegen Dmitry Badin besteht ein Haftbefehl. Ein Strafurteil fehlt, weshalb die präzise Kategorie „offiziell attribuiert und strafprozessual verfolgt“ lautet.

Bei Desinformation ist „Doppelgänger“ durch sichtbare Täuschungsinfrastruktur, EU-Analysen und Sanktionen substanziell belegt. Ghostwriter und Storm-1516 zeigen vergleichbare Muster, doch sind einzelne Dienstzuordnungen weniger transparent und nicht gerichtlich bestätigt. RT und Sputnik sind als staatliche beziehungsweise staatlich kontrollierte Kommunikationsakteure einzuordnen; daraus folgt nicht, dass jede einzelne Veröffentlichung falsch oder Teil einer verdeckten Operation ist.

Für kritische Infrastruktur ist besondere Zurückhaltung erforderlich. Nord Stream ist öffentlich nicht Russland zugerechnet; die deutsche Ermittlung richtet sich gegen konkrete ukrainische Verdächtige, ohne dass eine staatliche Verantwortlichkeit rechtskräftig festgestellt wäre. Beim Balticconnector ist die physische Verursachung durch einen Schiffsanker amtlich beschrieben, nicht aber eine russische Befehlskette. Andere Ostsee-Kabelvorfälle müssen einzeln untersucht werden.

Schließlich gibt das Material keine tragfähige Grundlage für die pauschale Behauptung, die AfD werde vom russischen Staat finanziert. Politische Nähe, kommunikative Verstärkung und verdeckte Finanzierung sind verschiedene Sachverhalte und dürfen nicht vermengt werden.

Der angemessene Gesamtbefund lautet daher:

- **Gerichtlich bewiesen:** mehrere konkrete Fälle russlandbezogener Agententätigkeit und Sabotagevorbereitung.
- **Offiziell attribuiert und erheblich technisch gestützt:** Bundestag-Hack durch APT28/GRU-Einheit 26165 sowie „Doppelgänger“ als russisch gesteuerte Informationsoperation.
- **Formell angeklagt, aber nicht entschieden:** insbesondere Carsten L./Arthur E. und Ilona W.
- **Plausibel oder behördlich bewertet, aber öffentlich nur teilweise überprüfbar:** Teile weiterer Cyber- und Desinformationszuordnungen.
- **Offen oder nicht belegt:** russische Täterschaft bei Nord Stream, pauschale Russland-Zurechnung von Ostsee-Kabelschäden, pauschale russische AfD-Finanzierung und konkrete kausale Veränderungen deutscher Wahlergebnisse.

Gerade diese Differenzierung stärkt den Befund. Sie verhindert, dass gut belegte russische Geheimdienst-, Cyber- und Einflussoperationen durch überzogene oder unbelegte Pauschalbehauptungen entwertet werden.

SOURCES

1. https://www.bellingcat.com/news/2020/05/05/who-is-dmitry-badin-the-gru-hacker-indicted-by-germany-over-the-bundestag-hacks/
2. https://www.auswaertiges-amt.de/en/newsroom/news/hacker-attack-bundestag-2345580
3. https://www.consilium.europa.eu/en/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/
4. https://www.reuters.com/world/german-courts-convict-russian-spy-start-trial-three-other-suspects-2025-10-30/
5. https://www.sueddeutsche.de/politik/spione-russland-urteil-staatsschutz-li.3533112
6. https://oberlandesgericht-stuttgart.justiz-bw.de/pb/,Lde_DE/8975554/?LISTPAGE=8975446
7. https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/2023/Pressemitteilung-vom-08-09-2023.html
8. https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf
9. https://www.eeas.europa.eu/eeas/inside-infrastructure-foreign-information-manipulation-and-interference-fimi-operations_en
10. https://data.consilium.europa.eu/doc/document/ST-15796-2024-INIT/en/pdf
11. https://www.consilium.europa.eu/en/press/press-releases/2024/12/16/russian-hybrid-threats-eu-agrees-first-listings-in-response-to-destabilising-activities-against-the-eu-its-member-states-and-partners/
12. https://ukrainianweek.com/storm-1516-russian-disinformation/
13. https://edmo.eu/publications/storm-1516-the-pro-russian-disinformation-operation-threatening-the-public-debate/
14. https://www.techtimes.com/articles/323611/20260807/storm-1516-hits-merz-stolen-deutsche-welle-logo-european-leader-blitz.htm
15. https://www.bundesgerichtshof.de/SharedDocs/Entscheidungen/DE/Strafsenate/3_StS/2025/StB__60-25.pdf?__blob=publicationFile&v=5
16. https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2026/2026012.html

17. https://valtioneuvosto.fi/en/-/25235045/cooperation-in-balticconnector-case-to-continue
18. https://valtioneuvosto.fi/en/-/25235045/national-bureau-of-investigation-launched-investigation-into-the-incident-in-the-gulf-of-finland
19. https://bundesanwalt.de/ru/index.php?id=24&mainm=24
20. http://www.bundesanwalt.de/ru/index.php?id=28&mainm=9
21. Putin Valdai 2026 ru.txt (uploaded document)
22. Putin Valdai 2026 Frage und Antwort en.txt (uploaded document)
23. https://www.consilium.europa.eu/en/policies/sanctions-against-cyber-attacks/timeline-sanctions-cyber-attacks/
24. https://www.derstandard.de/consent/tcf/story/2000124471871/anklage-in-deutschland-wegen-spionage-fuer-russland-erhoben
25. https://www.t-online.de/nachrichten/panorama/kriminalitaet/id_91049180/56-jaehriger-kooperierte-mit-russischem-geheimdienst-gru-bewaehrungsstrafe.html
26. https://www.mz.de/deutschland-und-welt/deutschland/spionage-fur-russland-bundeswehroffizier-muss-in-haft-3851592
27. https://www.reuters.com/world/europe/suspected-spy-russia-arrested-germany-prosecutors-2023-08-09/
28. https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/2026/Pressemitteilung-vom-21-01-2026-2.html
29. https://www.tagesschau.de/inland/innenpolitik/anklage-spionin-russland-100.html
30. https://www.lto.de/recht/nachrichten/n/bundesanwaltschaft-kammergericht-berlin-russland-spionin-lobbyistin-anklage
31. https://www.spiegel.de/panorama/justiz/stuttgart-freiheitsstrafe-im-prozess-gegen-agenten-russlands-a-0bde92a2-a99a-4ddd-a5b5-0f7e676a3669
32. https://www.handelsblatt.com/politik/deutschland/spionage-haftstrafe-im-prozess-gegen-mutmasslichen-agenten-russlands/100247960.html
33. https://valtioneuvosto.fi/en/-/44957406/estlink-2-electricity-transmission-cable-damaged-in-the-baltic-sea-on-25-dec-2024
34. https://ec.europa.eu/commission/presscorner/api/files/attachment/879707/Mem
35. https://cyberlaw.ccdcoe.org/wiki/Bundestag_Hack_(2015
36. https://www.sueddeutsche.de/politik/hack-bundestag-angriff-russland-1.4891668
37. https://attack.mitre.org/groups/G0007/
38. https://eurepoc.eu/wp-content/uploads/2023/07/APT28-EN.pdf
39. https://www.bankinfosecurity.com/eu-sanctions-2-russians-for-german-parliament-hack-a-15237
40. https://www.bankinfosecurity.com/russian-suspected-german-parliament-hack-report-a-14236
41. https://www.govinfosecurity.com/russian-suspect-in-german-parliament-hack-report-a-14236
42. https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/2022/Pressemitteilung-vom-01-04-2022.html
43. https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/2022/Pressemitteilung-vom-22-12-2022.html
44. https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/2026/Pressemitteilung-vom-13-01-2026.html
45. https://www.spiegel.de/politik/deutschland/spionage-ex-bnd-mitarbeiter-zu-acht-jahren-haft-verurteilt-a-1082796.html
46. https://www.spiegel.de/politik/deutschland/bnd-spion-markus-r-wegen-landesverrats-angeklagt-a-1049010.html
47. https://www.stimme.de/politik/welt/politik/ausland/berichte-haftbefehl-nach-nord-stream-anschlaegen-erwirkt-art-4954586
48. https://www.bluewin.ch/de/news/international/berichte-haftbefehl-nach-nord-stream-anschlaegen-erwirkt-2325733.html
49. https://www.deutschlandfunk.de/bundesanwaltschaft-bestaetigt-weitere-festnahme-in-zusammenhang-mit-nord-stream-sabotage-104.html
50. https://www.sueddeutsche.de/politik/nord-stream-festgenommener-ukrainer-sabotage-team-li.3302375
51. https://valtioneuvosto.fi/en/-//1410877/minister-mykkanen-on-balticconnector-disruption-gas-system-is-stable-but-the-disruption-highlights-importance-of-preparedness-by-gas-using-businesses
52. https://www.bundesregierung.de/breg-de/aktuelles/nis-2-richtlinie-deutschland-2373174
53. https://www.bundesregierung.de/breg-de/suche/bundesinnenminister-kritis-2392826
54. https://www.bundesregierung.de/breg-de/service/newsletter-und-abos/bundesregierung-aktuell/ausgabe-29-2026-september-04-2451054?view=renderNewsletterHtml
55. https://www.bundesregierung.de/breg-de/service/newsletter-und-abos/bulletin/bmi-kritische-infrastruktur-2405068
56. https://www.dw.com/de/m%C3%BCnchen-drei-m%C3%A4nner-wegen-spionage-f%C3%BCr-russland-verurteilt/a-74554316
57. https://www.bfv.de/binaries/content/assets/inhalt/spielbetrieb-verbandsleben/schiedsrichter/gruppen/oberbayern/inn-salzach/8132-chiem/formulare/lehrwesen/lehrbriefe/vsa-lehrbrief-01---die-zeitstrafe-im-bfv.pdf
58. https://www.bfv.de/binaries/content/assets/inhalt/spielbetrieb-verbandsleben/schiedsrichter/gruppen/schwaben/donau/8313-westschwaben/austausch-wfv/wfv-merkblatt_2023-2024.pdf
59. https://www.bfv.de/mspw/regionalliga-bayern/2022-23/regionalliga-bayern-der-11.-spieltag
60. https://enlargement.ec.europa.eu/news/disinformation-about-current-russia-ukraine-conflict-seven-myths-debunked-2022-01-24_en
61. https://cert.europa.eu/publications/threat-intelligence/cb23-07/markdown

62. https://www.eeas.europa.eu/sites/default/files/2025/documents/2024%20Report%20on%20EEAS%20Activities%20to%20Counter%20FIMI.pdf
63. https://www.iss.europa.eu/publications/briefs/smoke-and-mirrors-building-eu-resilience-against-manipulation-through-cognitive
64. https://www.eeas.europa.eu/eeas/fighting-foreign-interference-protect-our-democracy_en
65. https://euromaidanpress.com/2025/12/23/russia-disinformation-storm-1516-overtakes-rt-sputnik/
66. https://blog.gdeltproject.org/a-deepfake-first-russian-television-interviews-deepfake-donald-trump-ursula-von-der-leyen-about-us-eu-policy-on-ukraine/
67. https://unn.ua/en/news/russia-revives-fake-news-about-ursula-von-der-leyens-nazi-ancestors-the-center-for-countering-disinformation-reveals-the-campaigns-goal
68. https://www.dw.com/en/fact-check-how-to-spot-fake-news-ahead-of-eu-elections/a-69046888
69. https://ec.europa.eu/newsroom/edmo/newsletter-archives/52424
70. https://www.consilium.europa.eu/en/policies/sanctions-against-russia/timeline-sanctions-against-russia/
71. https://www.gov.uk/government/news/uk-enforces-new-sanctions-against-russia-for-cyber-attack-on-german-parliament
72. https://www.zdnet.com/article/german-authorities-charge-russian-hacker-for-2015-bundestag-hack/
73. https://www.cfr.org/articles/bundestag-hack-redux-more-smoke-mirrors
74. https://www.zeit.de/digital/datenschutz/2020-05/angriff-bundestag-hacker-geheimdienst-russland
75. https://www.focus.de/politik/deutschland/auch-das-fbi-fahndet-bundesanwaltschaft-erwirkt-haftbefehl-hacker-aus-russischem-militaergeheimdienst-fuer-bundestag-cyberangriff-2015-verantwortlich_id_11956008.html