ANALYTISCHER FORSCHUNGSBERICHT · PHILOSOPHENSTUDIO

Das Attributionsproblem und der westliche Doppelstandard

Methodische Analyse der Zurechenbarkeit und asymmetrischer Beweismassstabe

Erstellt von: Christer Häberli

Datum: 8. Oktober 2026

Aktenzeichen: CHH-2026-ATT-001

Status: Analytisches Arbeitsdokument

ANALYTISCHES DOKUMENT · KEIN AMTLICHER SCHRIFTSATZ

ATTRIBUTION, GEGENAKTIVITÄTEN UND DOPPELSTANDARDS IM CYBER- UND SICHERHEITSKONFLIKT ZWISCHEN RUSSLAND UND DEM WESTEN

Christer Häberli October 08, 2026

KURZFAZIT

1. **Cyberattribution ist kein einzelner Beweis, sondern eine Beweiskette.** Ein Schadprogramm, eine IP-Adresse oder eine russischsprachige Zeichenfolge beweisen weder eine bestimmte Organisation noch staatliche Steuerung. Belastbare Attribution verbindet technische Forensik, wiederkehrende Taktiken, Techniken und Verfahren (TTPs), Infrastruktur- und Metadaten, operative Fehler, nachrichtendienstliche Erkenntnisse und soweit vorhanden personenbezogene Ermittlungsdaten.

2. **Vier Ebenen müssen getrennt werden:**

   - technische Urheberschaft oder operative Kontrolle,
   - Zuordnung zu einer Organisation,
   - Zurechnung zu einem Staat,
   - persönliche Befehlskette bis zum Präsidenten.
     Öffentliche Belege können in Fällen wie NotPetya eine Zuordnung zu namentlich genannten GRU-Offizieren und zur Einheit 74455 stützen. Eine persönliche Anordnung Wladimir Putins ist damit nicht öffentlich bewiesen. Für die meisten öffentlich diskutierten Cyberoperationen ist eine direkte Kreml- oder Putin-Befehlskette nicht nachweisbar.

3. **Für russische staatliche Cyberaktivitäten existieren mehr als bloße politische Behauptungen.** Besonders im Fall der GRU-Einheit 74455 („Sandworm“) liegen technische Behördenberichte, gemeinsame internationale Warnungen, eine detaillierte US-Anklage und personenbezogene Zuordnungen vor. Die US-Anklage von 2020 wirft sechs GRU-Offizieren eine Kampagne destruktiver Operationen vor, darunter NotPetya; sie ist jedoch eine Anklage und keine rechtskräftige Verurteilung der Beschuldigten [ref773, ref774, ref824]. Gemeinsame Warnungen von CISA, FBI, NSA und internationalen Partnern ordnen Sandworm dem Hauptzentrum für Spezialtechnologien des GRU zu [ref803, ref804, ref809].

4. **Alternativerklärungen müssen geprüft, aber nicht automatisch gleich gewichtet werden.** Unabhängige Kriminelle, Dissidenten, patriotische Hacker, staatlich geduldete Gruppen oder False Flags sind real mögliche Modelle. Ihre bloße Möglichkeit widerlegt jedoch keine konkrete Attribution. Umgekehrt darf ein Angriff nicht allein deshalb einem Staat zugerechnet werden, weil er dessen Interessen dient oder bekannte Werkzeuge eines staatlichen Akteurs enthält.

5. **False Flags sind praktisch belegt.** Beim Angriff „Olympic Destroyer“ wurden technische Merkmale manipuliert, um unter anderem eine Verbindung zur nordkoreanischen Lazarus-Gruppe zu suggerieren. Die forensische Prüfung zeigte, dass vermeintlich eindeutige Codeartefakte gefälscht waren [ref793, ref843, ref847, ref849]. Auch die US-Anklage gegen GRU-Offiziere beschreibt den Einsatz falscher Identitäten und die Nachahmung anderer Akteure [ref775, ref777, ref780]. Daraus folgt die Notwendigkeit tieferer Prüfung nicht die Vermutung, jeder Russland zugeschriebene Vorfall sei ein False Flag.

6. **Westliche Spionage ist dokumentiert und für einen symmetrischen Maßstab unverzichtbar.** Die Snowden-Unterlagen belegten weitreichende amerikanische und britische Überwachung. Das Mobiltelefon Angela Merkels galt als NSA-Ziel; die politische Reaktion war erheblich. Ein deutsches strafrechtliches Verfahren wurde allerdings eingestellt, weil der konkrete Abhörvorgang nicht gerichtsfest bewiesen werden konnte [ref876, ref878]. Die US-Regierung erklärte 2013 nur, Merkels Kommunikation werde gegenwärtig nicht überwacht und künftig nicht überwacht werden; eine ausdrückliche Verneinung früherer Überwachung enthielt diese Erklärung nicht [ref922].

7. **Die BND-NSA-Kooperation ist stärker institutionell dokumentiert als der konkrete Merkel-Fall.** Der NSA-Untersuchungsausschuss und der Graulich-Bericht zeigten erhebliche Kontrollmängel bei Selektoren. Von 39.082 Mitte 2015 identifizierten problematischen Selektoren richteten sich ungefähr 68,7 Prozent gegen Regierungsstellen in der Europäischen Union [ref909, ref912]. Dies belegt nicht nur amerikanische Überwachungsinteressen, sondern auch deutsche Mitwirkung und unzureichende Kontrolle.

8. **Stuxnet ist ein starker Kontrastfall westlicher Cyber-Sabotage, aber kein offiziell eingestandenes Beispiel.** Die Operation verursachte physische Wirkungen an iranischen Industrieanlagen und wird in hochrangiger journalistischer Berichterstattung den USA und Israel zugeschrieben. Eine förmliche öffentliche Verantwortungsübernahme beider Regierungen liegt nach der dokumentierten Quellenlage nicht vor [ref949, ref950, ref951, ref953].

9. **Öffentlich bestätigte US-Cyberdoktrin ist nicht dasselbe wie ein bestätigter Angriff auf Russland.** US Cyber Command bestätigt „persistent engagement“, „defend forward“ und auf Einladung durchgeführte „Hunt Forward“-Einsätze in Partnerstaaten [ref958, ref959, ref987, ref990]. Berichte über offensive US-Operationen gegen russische Infrastruktur sind teilweise journalistisch oder beruhen auf russischen Behauptungen. Die öffentlich dokumentierte

Entscheidung, 2025 bestimmte offensive Operationen gegen Russland auszusetzen, spricht dafür, dass solche Operationen bestanden; sie legt aber weder alle Ziele noch Methoden oder Wirkungen offen [ref1000]. NATO und USA dürfen dabei nicht gleichgesetzt werden: Die NATO verfügt nach eigener Darstellung nicht über ein eigenes offensives Cyberarsenal, sondern kann freiwillig bereitgestellte nationale Fähigkeiten integrieren [ref1014, ref1017, ref1020].

10. **Merkels Überwachung widerlegt russlandbezogene Vorwürfe nicht.** Sie widerlegt vielmehr die Vorstellung, westliche Staaten betrieben keine rechts- und politisch problematische Spionage. Konsistent ist deshalb nur ein Standard, der dieselben Beleganforderungen und Rechtsmaßstäbe auf alle Staaten anwendet. Zugleich dürfen Spionage, Datenveröffentlichung, Sabotage, physische Zerstörung und bewaffnete Gewalt nicht begrifflich gleichgesetzt werden.

11. **Zur NATO-Erweiterung ist die historische und rechtliche Lage zweigeteilt.** Archivunterlagen dokumentieren wiederholte mündliche Zusicherungen westlicher Politiker 1990/91, die sowjetische Sicherheitsbedenken beschwichtigen sollten [ref1022, ref1076, ref1080, ref1083]. Ein rechtsverbindlicher allgemeiner Vertrag, der spätere NATO-Beitritte osteuropäischer Staaten verbot, wurde jedoch nicht geschlossen. Der Zwei-plus-Vier-Vertrag regelte insbesondere das Gebiet der früheren DDR und enthielt keine allgemeine Erweiterungssperre [ref1066, ref1067, ref1068].

12. **Westlicher Einfluss in der Ukraine ist belegt; eine westliche Gesamtsteuerung des Machtwechsels ist es nicht.** Das Nuland-Pyatt-Gespräch zeigt amerikanische Präferenzen für die personelle Zusammensetzung einer künftigen Regierung [ref1104, ref1110, ref1144]. NED und USAID finanzierten langjährig Zivilgesellschaft, Medien, Wahl-, Parlaments- und Antikorruptionsprogramme [ref1113, ref1120, ref1123, ref1125]. Diese Tatsachen belegen Einflussnahme und politische Interessen, aber für sich genommen weder die operative Kontrolle der Proteste noch einen vollständig von außen gesteuerten Regimewechsel. Ukrainische Akteure, gesellschaftliche Mobilisierung, innerstaatliche Konflikte und spätere Wahlen besitzen eigenständiges Erklärungsgewicht.

13. **Sanktionen sind Zwangsinstrumente, aber nicht automatisch Kriegshandlungen.** EU- und US-Sanktionen beruhen auf innerstaatlichen beziehungsweise unionsrechtlichen Rechtsakten und verfolgen ausdrücklich wirtschaftlichen und politischen Druck [ref1176, ref1183, ref1184, ref1220]. Ihre Wirkungen können gravierend sein und als „Wirtschaftskrieg“ bezeichnet werden; rechtlich sind sie jedoch nicht ohne Weiteres mit bewaffneter Gewalt oder einem „armed attack“ gleichzusetzen.

AUFTRAG, BEGRIFFE UND METHODE

Untersuchungsauftrag

Der Bericht beantwortet drei miteinander verbundene Fragen:

1. Wie belastbar sind öffentliche Zuschreibungen mutmaßlich russischer Cyberangriffe, Sabotage- und Spionageoperationen?
2. Welche westlichen Aktivitäten gegen Russland, Deutschland oder Drittstaaten sind öffentlich nachweisbar?
3. Werden auf russische und westliche Aktivitäten unterschiedliche Beweis- und Bewertungsmaßstäbe angewandt, und welche symmetrischen Standards wären sachgerecht?

Im Mittelpunkt steht nicht die Frage, welche geopolitische Erzählung politisch attraktiver ist. Entscheidend ist, was durch öffentlich zugängliche technische Berichte, amtliche Dokumente, parlamentarische Untersuchungen, gerichtliche Unterlagen, hochwertige Forschung oder nachvollziehbare journalistische Recherchen gestützt wird.

Statuskennzeichnungen

Der Bericht verwendet drei sichtbare Kategorien:

- **Dokumentiert/belegt:** durch Primärdokumente, technische Daten, parlamentarische Untersuchungen, unstrittige Originalaufnahmen oder mehrere voneinander unabhängige hochwertige Quellen gestützt.
- **Offiziell behauptet/nicht abschließend bewiesen:** Attribution einer Regierung, Behörde, Anklage oder Sanktion, deren vollständige Beweisgrundlage geheim bleibt oder noch nicht gerichtlich geprüft wurde.
- **Spekulativ/strittig:** plausible, aber öffentlich nicht hinreichend belegte Erklärung; umstrittene Interpretation; Einzelaussage ohne ausreichende unabhängige Bestätigung.

Diese Kategorien dürfen nicht mit strafprozessualen Beweismaßen verwechselt werden. Eine Regierungsattribution kann nachrichtendienstlich hochwahrscheinlich sein, ohne öffentlich einen gerichtlichen Vollbeweis zu liefern. Umgekehrt kann ein eingestelltes Strafverfahren bedeuten, dass eine Tat strafrechtlich nicht beweisbar ist, obwohl die politische oder nachrichtendienstliche Einschätzung weiterhin für ihre tatsächliche Begehung spricht.

Quellentypen und ihr Gewicht

Zentrale Quellen werden nach ihrer Funktion unterschieden:

- **Technische Behördenberichte:** stark für Schadprogramm, Infrastruktur, Schwachstellen und TTPs; weniger stark für nicht offengelegte politische Befehlsketten.
- **Anklageschriften:** detaillierte staatliche Vorwürfe, häufig mit personenbezogenen und operativen Angaben; keine Verurteilung.
- **Parlaments- und Untersuchungsberichte:** stark für institutionelle Abläufe, Aufsicht und amtlich zugängliche Dokumentation; durch Geheimschutz begrenzt.
- **Regierungserklärungen und Sanktionen:** Beleg für die offizielle Position und Rechtsfolge, nicht automatisch für die Richtigkeit aller Tatsachenbehauptungen.
- **Nachrichtendienstliche Einschätzungen:** potenziell auf besonders aussagekräftigen Quellen beruhend, öffentlich aber oft nicht reproduzierbar.
- **Journalistische Untersuchungen:** können geheime Vorgänge erschließen, hängen aber von Quellenschutz und nicht vollständig überprüfbaren Informanten ab.
- **Wissenschaftliche Forschung:** besonders nützlich für Methoden, Fehlerrisiken und historische Einordnung; bei geheimen Einzeloperationen meist auf öffentlich verfügbare Daten angewiesen.
- **Politische Selbstdarstellungen:** belegen, was ein Akteur behauptet, nicht, dass die Behauptung zutrifft. Dies gilt gleichermaßen für westliche und russische Regierungsäußerungen.

Wesentliche Erkenntnisgrenzen

- Öffentliche Daten sind systematisch unvollständig.
- Geheimdienste schützen Quellen, Zugänge und Methoden.
- Technische Indikatoren können kopiert, gestohlen, verkauft oder absichtlich platziert werden.
- Infrastruktur kann kompromittiert oder angemietet sein.
- Zeitstempel, Spracheinstellungen und Metadaten sind manipulierbar.
- Gruppenbezeichnungen privater Sicherheitsfirmen sind nicht immer deckungsgleich.
- Eine Anklage ist ein Vorwurf und keine Verurteilung.
- Eine Sanktionierung ist eine administrative oder politische Maßnahme, kein gerichtlicher Schuldspruch.
- Organisationszugehörigkeit beweist nicht automatisch einen konkreten politischen Einzelbefehl.
- Der Nutzen einer Operation für einen Staat beweist nicht dessen Urheberschaft.
- Das Fehlen öffentlich zugänglicher Beweise beweist weder Unschuld noch Verantwortung.

TEIL I: ATTRIBUTION MUTMASSLICH RUSSISCHER CYBERANGRIFFE, SABOTAGE UND SPIONAGE

1. Beweisstufen-Typologie

Stufe	Zu beantwortende Frage	Typische Belege	Was damit noch nicht bewiesen ist
A: Technische Urheberschaft/Operationskontrolle	Wer entwickelte, bediente oder kontrollierte Schadsoftware und Infrastruktur?	Malwarecode, Serverlogs, C2-Verbindungen, Zugangsdaten, Build-Umgebungen, operative Fehler, Geräteforensik	Zugehörigkeit zu einer bestimmten Behörde oder staatlicher Auftrag
B: Organisationszuordnung	Gehören die Operatoren zu einer bekannten Gruppe oder Einheit?	stabile TTP-Muster, Infrastrukturüberschneidungen, gemeinsame Schlüssel, Konten, Personal- und Reisebezüge, interne Dokumente	dass die Organisation als Staatsorgan handelte oder dieser konkrete Angriff autorisiert war
C: Staatliche Zurechenbarkeit	Ist die Operation einem Staat rechtlich oder politisch zurechenbar?	Dienstzugehörigkeit, staatliche Ressourcen, Befehls- oder Kontrollbelege, amtliche Unterlagen, HUMINT/SIGINT, gerichtliche Ermittlungen	persönliche Kenntnis oder Anordnung des Staatsoberhaupts
D: Persönliche Kreml-/Putin-Befehlskette	Hat Putin den konkreten Vorgang angeordnet, gebilligt oder nachträglich bestätigt?	authentische Befehle, Protokolle, glaubwürdige Insideraussagen, abgefangene Kommunikation, Geständnisse	

Die öffentliche Debatte überspringt diese Stufen häufig. Aus „Malware ähnelt früheren Sandworm-Werkzeugen“ wird dann unmittelbar „Putin hat den Angriff befohlen“. Das ist analytisch unzulässig. Umgekehrt ist es ebenfalls unzulässig, eine starke Stufe-B- oder Stufe-C-Attribution allein deshalb zu verwerfen, weil Stufe D nicht öffentlich belegt ist.

Das Recht der Staatenverantwortlichkeit unterscheidet insbesondere zwischen Handlungen staatlicher Organe und Handlungen nichtstaatlicher Akteure unter staatlicher Weisung, Leitung oder Kontrolle. Technische Herkunft und rechtliche Zurechnung sind daher verschiedene Fragen [ref1194, ref1199, ref1200].

2. Technische Instrumente der Attribution

2.1 TTPs

TTPs sind **Tactics, Techniques and Procedures**: wiederkehrende Verhaltensweisen, mit denen ein Akteur Ziele auswählt, Zugänge gewinnt, Privilegien erweitert, sich im Netz bewegt, Daten exfiltriert, Spuren beseitigt oder Systeme zerstört. Dazu gehören etwa:

- Spearphishing und die Gestaltung von Köderdokumenten,
- Auswahl und Verkettung bestimmter Schwachstellen,
- Passwortdiebstahl und laterale Bewegung,
- Verwendung bestimmter Administrationswerkzeuge,
- Kommandostrukturen und Arbeitszeiten,
- Art der Persistenz,
- Exfiltrationswege,
- Zeitpunkt und Form einer Veröffentlichung,
- spezifische Zerstörungs- oder Verschleierungsmethoden.

TTPs sind meist belastbarer als ein einzelner Dateiname oder eine einzelne IP-Adresse, weil konsistentes Arbeitsverhalten schwerer vollständig zu imitieren ist. Sie sind aber nicht unveränderlich. Akteure lernen, nutzen allgemein verfügbare Werkzeuge oder kopieren bekannte Vorgehensweisen. Das britische NCSC weist ausdrücklich darauf hin, dass Akteure TTPs verändern und legitime Werkzeuge einsetzen, um sich im normalen Netzwerkverkehr zu verbergen [ref813, ref815, ref817].

2.2 IOCs

Indicators of Compromise (IOCs) sind beobachtbare technische Spuren, darunter:

- Hashwerte von Schadprogrammen,
- IP-Adressen und Domains,
- Zertifikate,
- Dateipfade und Registry-Einträge,
- E-Mail-Adressen und Phishing-Domains,
- Mutex-Namen,

- Befehlsfolgen,
- charakteristische Netzwerkpakete.

IOCs sind für Erkennung und Gefahrenabwehr unverzichtbar, für Attribution aber begrenzt. Server können gehackt, Domains unter falscher Identität registriert und Malwarebausteine wiederverwendet werden. Gerade leicht sichtbare IOCs eignen sich als Täuschungsmittel. Das NCSC trennt deshalb technische Malwareberichte ausdrücklich von Attribution: Seine Malware Analysis Reports enthalten IOCs und TTPs, vermeiden aber wegen Malwarewiederverwendung und möglicher Desinformation Aussagen über den Täter [ref817].

2.3 Infrastruktur- und Metadatenanalyse

Untersucht werden Registrierungsdaten, Hostinganbieter, Serverkonfigurationen, TLS-Zertifikate, Domainmuster, Bezahlwege, Wiederverwendung von Konten und Verbindungen zwischen Command-and-Control-Infrastruktur. Besonders aussagekräftig sind langfristige Überschneidungen: beispielsweise dieselben administrativen Zugänge, kryptografischen Schlüssel oder seltene Konfigurationsfehler in mehreren Operationen.

Fehlerquellen sind:

- kompromittierte Server als Zwischenstationen,
- kommerziell angemietete Infrastruktur,
- falsche Registrierungsangaben,
- VPNs, Tor und Proxyketten,
- gemeinsam genutzte oder verkaufte Malware,
- absichtlich wiederverwendete fremde Indikatoren,
- Überinterpretation zufälliger Überschneidungen.

Metadaten wie Zeitzonen, Tastaturlayout, Kompilierungszeiten und Spracheinstellungen können Hinweise liefern. Sie können aber bewusst verändert werden und dürfen nie allein tragend sein.

2.4 Personenbezogene Ermittlungen

Eine Attribution wird wesentlich stärker, wenn technische Daten mit realen Personen verbunden werden: E-Mail-Konten, Reisebewegungen, Passdaten, Geräte, Zahlungsinformationen, Arbeitgeber, militärische Einheiten oder operative Konten. Die US-Anklage von 2020 geht über eine abstrakte Gruppenbezeichnung hinaus, indem sie sechs mutmaßliche GRU-Offiziere benennt und einzelnen Beschuldigten Entwicklungs- und Operationsrollen zuschreibt [ref773, ref774, ref775].

Auch hier gilt: Die Angaben stammen aus einer Anklage. Ohne Verfahren mit Verteidigung, Beweisaufnahme und Urteil sind sie keine rechtskräftig festgestellten Tatsachen.

2.5 Nachrichtendienstliche Erkenntnisse

SIGINT kann Kommunikation, Infrastrukturverwaltung und Befehlsketten sichtbar machen; HUMINT kann organisatorische oder politische Zusammenhänge erklären. Satelliten-, Finanz- oder Reisedaten können technische Befunde ergänzen. Solche Erkenntnisse können die staatliche Zuordnung entscheidend stärken.

Ihre öffentliche Prüfbarkeit ist jedoch gering. Behörden veröffentlichen häufig nur die Schlussfolgerung oder „high confidence“, nicht aber Rohdaten. Dafür gibt es legitime Gründe: Offenlegung kann Quellen gefährden und Zugänge verbrennen. Das erzeugt zugleich ein demokratisches Problem, weil Öffentlichkeit, Wissenschaft und Gerichte die Schlussfolgerung nicht vollständig reproduzieren können. Kollektive Attributionen mehrerer Staaten erhöhen das politische Gewicht, ersetzen aber keine Offenlegung der Beweise [ref1195, ref1197, ref1200].

3. Öffentliche Fälle

3.1 NotPetya und GRU-Einheit 74455/Sandworm

Status: offiziell detailliert zugeschrieben; starke öffentliche Indizien; keine rechtskräftige Verurteilung der Angeklagten; keine öffentliche Putin-Befehlskette.

Im Oktober 2020 erhob das US-Justizministerium Anklage gegen sechs Offiziere des russischen Militärnachrichtendienstes GRU, die der Militäreinheit 74455 zugeordnet wurden. Vorgeworfen wurde ihnen eine weltweite Kampagne destruktiver Cyberoperationen [ref773, ref824]. Die Anklage ordnet die Entwicklung von NotPetya-Komponenten konkret Yuriy Andrienko, Sergey Detistov, Pavel Frolov und Petr Pliskin zu [ref775, ref777].

NotPetya wurde im Juni 2017 eingesetzt, traf zunächst stark ukrainische Systeme und verursachte anschließend internationale Schäden, darunter bei einem Gesundheitssystem in Pennsylvania [ref775]. Gemeinsame technische Warnungen amerikanischer und britischer Behörden führen NotPetya ebenso wie BlackEnergy, KillDisk, Industroyer, Olympic Destroyer und VPNFilter im Aktivitätsspektrum von Sandworm [ref804, ref809, ref810].

Die Attribution stützt sich öffentlich auf mehrere Schichten:

- technische Verknüpfungen zu länger beobachteten Sandworm-Operationen,
- identifizierte militärische Einheit,
- namentlich genannte mutmaßliche Operatoren,
- gemeinsame Behördeneinschätzungen mehrerer Staaten,
- Zuordnung verwandter Infrastruktur und Operationen,
- detaillierte Anklagebehauptungen.

Das reicht über eine bloße Behauptung „Russland war es“ hinaus. Gleichwohl bleiben Grenzen:

- Die Angeklagten wurden in den vorliegenden Unterlagen nicht rechtskräftig verurteilt.
- Ein erheblicher Teil nachrichtendienstlicher Belege ist nicht öffentlich.
- Die Zuordnung zur GRU-Einheit beweist keine persönliche Anweisung Putins.
- Der politische Entscheidungsweg für den konkreten Einsatz von NotPetya ist öffentlich nicht vollständig dokumentiert.

Die präzise Schlussfolgerung lautet deshalb: **Die öffentliche Zuordnung von NotPetya zu Sandworm beziehungsweise GRU-Einheit 74455 ist stark gestützt; eine persönliche Putin-Befehlskette ist öffentlich nicht nachweisbar.**

3.2 Ukrainische Energieinfrastruktur und weitere Sandworm-Aktivitäten

Status: gemeinsame staatliche Attribution mit technischen Begleitberichten; nicht in jedem Fall gerichtlich geprüft.

CISA und Partner schreiben Sandworm Angriffe auf ukrainische Energieunternehmen 2015 mit BlackEnergy und KillDisk sowie 2016 mit Industroyer zu. Hinzu kommen der Angriff auf die Olympischen Winterspiele 2018, VPNFilter und Operationen gegen georgische Websites 2019 [ref804, ref810].

2023 veröffentlichten CISA, FBI, NSA und Partner einen Bericht über „Infamous Chisel“, eine Sammlung von Android-Komponenten, die Geräte des ukrainischen Militärs ausgespäht haben soll. Dokumentiert wurden Dateiexfiltration, Netzwerküberwachung, Tor- und SSH-Zugänge sowie Persistenz durch Ersetzung einer Systemdatei. Die Behörden ordneten das Werkzeug Sandworm und damit dem GRU-Hauptzentrum für Spezialtechnologien zu [ref803, ref851].

Die technischen Fähigkeiten des Werkzeugs sind durch den Analysebericht stärker öffentlich nachvollziehbar als die gesamte organisatorische Zurechnung. Diese beruht zusätzlich auf behördlichem Wissen, das nur teilweise offengelegt ist. Wiederum fehlt ein öffentlicher Nachweis einer persönlichen Kreml- oder Putin-Anordnung.

3.3 Fancy Bear/APT28 und Abgrenzung zu Sandworm

Gruppennamen werden häufig unscharf verwendet. Das US-Justizministerium unterscheidet GRU-Einheit 26165, die unter anderem als Fancy Bear, APT28, Sofacy oder Sednit bezeichnet wird, von Einheit 74455/Sandworm [ref779]. Bei Operationen um die US-Wahl 2016 werden Einheit 26165 Hackingaktivitäten und Einheit 74455 unter anderem die strategische Verbreitung entwendeter Informationen zugeschrieben [ref826, ref828].

Diese Unterscheidung ist wichtig: „Russischer Hacker“, „Fancy Bear“, „Sandworm“ und „GRU“ sind keine austauschbaren Begriffe. Private Sicherheitsunternehmen können denselben Akteur

unterschiedlich benennen oder verwandte Aktivitätscluster unterschiedlich abgrenzen.

3.4 Bundestag und Deutschland

Der Cyberangriff auf den Deutschen Bundestag von 2015 wird in der deutschen Debatte russischen beziehungsweise GRU-nahen Akteuren zugeschrieben; parlamentarische Dokumente behandeln ihn getrennt von der NSA-Affäre und ordnen russische Fälle teilweise als „Hack-and-Leak“-Operationen mit Einflusskomponente ein [ref1254]. Die hier ausgewertete öffentliche Datenlage enthält jedoch nicht dieselbe technische und personenbezogene Detailtiefe wie die US-Anklage zu NotPetya. Deshalb ist Zurückhaltung bei weitergehenden Aussagen geboten.

Insbesondere lässt sich aus der vorliegenden Dokumentation keine öffentliche persönliche Befehlskette bis Putin ableiten. Eine solche Behauptung wäre eine zusätzliche, eigenständig zu belegende Stufe.

4. Gegenhypothesen

4.1 Unabhängige Kriminelle

Cyberkriminelle können dieselben Schwachstellen, Malwarefamilien und Infrastrukturdienste wie staatliche Akteure verwenden. Staatliche Stellen können kriminelle Gruppen zudem tolerieren, rekrutieren oder punktuell einsetzen. Der Fall Evil Corp illustriert die mögliche Überschneidung von Finanzkriminalität und behaupteten Staatsbeziehungen; das US-Finanzministerium sanktionierte Mitglieder und Unterstützer wegen massiver finanzieller Diebstähle und Verbindungen zum russischen Staat [ref791].

Die Hypothese unabhängiger Kriminalität gewinnt an Gewicht, wenn:

- das Ziel primär finanziell ist,
- Opferauswahl opportunistisch wirkt,
- Lösegeldzahlungen und Geldwäscheketten dominieren,
- politische Zielauswahl oder militärische Synchronisierung fehlen,
- Werkzeuge breit auf kriminellen Märkten verfügbar sind.

Sie verliert an Gewicht, wenn:

- wirtschaftlicher Gewinn erkennbar nachrangig ist,
- Schadsoftware gezielt industrielle Prozesse zerstört,
- Operationen mit militärischen oder geheimdienstlichen Interessen korrespondieren,
- personenbezogene Ermittlungen Operatoren einer staatlichen Einheit zuordnen,
- Infrastruktur und Konten langfristig mit dieser Einheit verbunden sind.

Bei NotPetya ist die Erklärung eines rein unabhängigen, profitorientierten kriminellen Angriffs insbesondere deshalb schwach, weil die Operation destruktive Wirkungen hatte und die US-Anklage konkrete GRU-Offiziere benennt. Das ist dennoch eine staatliche Anklagebehauptung, keine abgeschlossene gerichtliche Beweisaufnahme.

4.2 Dissidenten

Russische oder russischsprachige Dissidenten könnten aus politischen Motiven handeln. Sprache, regionale Arbeitszeiten oder russische Infrastruktur würden dann keine staatliche Verantwortlichkeit beweisen. Die Hypothese ist besonders dann ernst zu nehmen, wenn ein Akteur glaubwürdig eigene Motive, technische Zugänge und unabhängige Organisationsstrukturen nachweisen kann.

Für die öffentlich dokumentierten Sandworm-Fälle erklärt die Dissidentenhypothese jedoch weder die wiederholte Zuordnung zu militärischen Einheiten noch die in Anklagen beschriebenen Personalbezüge. Ohne positive Belege bleibt sie eine abstrakte Möglichkeit.

4.3 Patriotische Hacker

„Patriotische Hacker“ können eigeninitiativ handeln, lose staatlich geduldet, informell ermutigt oder tatsächlich gelenkt sein. Die Bezeichnung beschreibt daher keinen einheitlichen Verantwortungsgrad. Vier Modelle sind auseinanderzuhalten:

1. vollständig selbstständige Aktivisten,
2. Akteure, die staatliche Interessen antizipieren,
3. staatlich tolerierte Gruppen mit informellen Kontakten,
4. staatlich gesteuerte Gruppen unter scheinbar privater Identität.

Das britische NCSC weist darauf hin, dass Staaten patriotische oder hacktivistische Fassaden zur plausiblen Abstreitbarkeit nutzen können [ref837]. Für rechtliche Zurechnung genügt jedoch nicht, dass ein Staat profitiert oder einen Täter nicht verfolgt. Erforderlich sind je nach Rechtsansatz Belege für Organeigenschaft, Anweisung, Leitung oder Kontrolle [ref1194, ref1199, ref1200].

4.4 False Flags

False Flags sind absichtlich platzierte Hinweise, die einen anderen Täter suggerieren. Mögliche Techniken sind:

- fremdsprachige Codekommentare,
- gefälschte Kompilierungszeiten,
- nachgeahmte Malwarefragmente,
- Verwendung öffentlich bekannter fremder Werkzeuge,
- kompromittierte Infrastruktur im Zielstaat,
- falsche Hacktivisten-Personas,

- bewusst gewählte Opfer- oder Veröffentlichungsmuster,
- manipulierte Metadaten und „zu perfekte“ Signaturen.

Die Existenz solcher Techniken begründet drei Regeln:

1. Einzelne IOCs dürfen nie allein tragen.
2. Widersprüche zwischen leicht sichtbaren Artefakten und tieferen Verhaltensmustern müssen aktiv gesucht werden.
3. Aus der abstrakten Möglichkeit eines False Flags darf nicht auf sein tatsächliches Vorliegen geschlossen werden.

5. Olympic Destroyer als dokumentierter False-Flag-Fall

Beim Angriff auf die Olympischen Winterspiele 2018 fanden Ermittler zunächst einen vollständigen Gleichlauf eines sogenannten Rich Headers mit Schadsoftware der nordkoreanisch zugeschriebenen Lazarus-Gruppe. Eine manuelle Prüfung zeigte, dass dieser Fingerabdruck manipuliert worden war [ref843, ref847, ref849]. Weitere Inkonsistenzen bei Passwörtern und TTPs passten nicht zum erwarteten Lazarus-Verhalten [ref843, ref847].

Der Fall ist methodisch bedeutsam:

- Ein scheinbar eindeutiger technischer Treffer kann gerade deshalb verdächtig sein.
- Oberflächenmerkmale sind leichter zu imitieren als eine konsistente Gesamtheit langfristiger TTPs.
- Frühzeitige öffentliche Zuschreibungen können sich gegenseitig verstärken, obwohl sie auf demselben irreführenden Indikator beruhen.
- Attribution sollte konkurrierende Hypothesen ausdrücklich prüfen.

US-Unterlagen werfen GRU-Akteuren darüber hinaus vor, falsche Personas und nachgeahmte Merkmale anderer Gruppen eingesetzt zu haben [ref775, ref777, ref780]. Diese amtliche Darstellung erhöht die Plausibilität, dass russische Dienste Täuschungstechniken einsetzen. Sie ist aber kein Freibrief, jeden strittigen Fall Russland zuzuschreiben.

6. Typische Wege zur Fehlattribution

Fehlerquelle	Fehlerschluss	Korrektiv
Russische Sprache im Code	„Der Täter ist russisch“	Prüfen, ob Spracheinstellung oder Kommentar manipulierbar ist
Russische IP-Adresse	„Angriff kam aus Russland“	Eigentum, Kompromittierung und Administrationszugänge untersuchen

Fehlerquelle	Fehlerschluss	Korrektiv
Bekannte Malware	„Bekannte Gruppe war es“	Malwarewiederverwendung und Quellcodezugang prüfen
Ziel passt zu russischem Interesse	„Russischer Staat hat befohlen“	Alternativmotive und unabhängige Akteure prüfen
Übereinstimmende TTPs	„Identischer Täter“	Seltenheit, Dauer und Kombination der Merkmale bewerten
Regierungsattribution	„Gerichtlich bewiesen“	Offenlegung, Beweisstandard und Verfahrensstand benennen
Keine Offenlegung	„Behauptung ist erfunden“	Geheimschutz berücksichtigen, aber Unsicherheit sichtbar lassen
False Flags existieren	„Jede Zuschreibung kann verworfen werden“	Positive Belege für konkrete Täuschung verlangen

TEIL II: NACHWEISBARE WESTLICHE AKTIVITÄTEN UND POLITISCHE KONTEXTE

1. NSA-ÜBERWACHUNG ANGELA MERKELS

1.1 Was dokumentiert ist

2013 wurden auf Grundlage von Snowden-Material Vorwürfe bekannt, die NSA habe das Mobiltelefon von Bundeskanzlerin Angela Merkel überwacht. Merkel erklärte öffentlich, „Abhören unter Freunden“ gehe nicht, und sprach das Thema gegenüber Präsident Barack Obama an [ref854, ref879, ref881].

Die US-Regierung erklärte am 23. Oktober 2013, Obama habe Merkel zugesichert, die Vereinigten Staaten überwachten ihre Kommunikation gegenwärtig nicht und würden dies künftig nicht tun [ref922]. Die Formulierung beantwortete die Frage früherer Überwachung nicht ausdrücklich. Ein US-Senator bezeichnete später das Abhören von Merkels Telefon als einen Fehler der Vergangenheit, der sich nicht wiederholen dürfe [ref921].

Die Snowden-Enthüllungen dokumentierten daneben ein wesentlich breiteres Überwachungssystem. Betroffen waren europäische Einrichtungen, Regierungsnetze, Diplomaten, internationale Organisationen und Unternehmen [ref884, ref885, ref887]. Das Europäische Parlament untersuchte

die Programme in 16 Anhörungen und verabschiedete 2014 mit 544 zu 78 Stimmen eine Resolution [ref940].

1.2 Was strafrechtlich nicht bewiesen wurde

Die deutsche Bundesanwaltschaft leitete Ermittlungen wegen des Verdachts der Ausspähung von Merkels Mobiltelefon ein. Sie konnte jedoch kein originales NSA-Dokument erhalten, das den konkreten Abhörvorgang gerichtsfest belegte. Ein öffentlich als Beleg behandeltes Dokument erwies sich nach Angaben deutscher Ermittler nicht als authentischer Überwachungsauftrag aus einer NSA-Datenbank [ref876, ref878].

Am 12. Juni 2015 wurde das Verfahren eingestellt, weil sich der Vorwurf strafrechtlich nicht rechtssicher beweisen ließ [ref878]. Diese Einstellung ist weder ein Beweis, dass keine Überwachung stattgefunden hat, noch eine Bestätigung jedes veröffentlichten Dokuments. Sie zeigt die Differenz zwischen:

- politisch und journalistisch überzeugender Indizienlage,
- nachrichtendienstlicher Plausibilität,
- strafprozessual verwertbarem Beweis gegen identifizierbare Täter.

Merkel erklärte 2017 im Untersuchungsausschuss, aus den Vorwürfen sei „nichts Beweisbares“ hervorgegangen [ref854, ref858]. Die präzise Einstufung lautet daher:

- **Breite NSA-Überwachung und Zielinteresse an europäischen Spitzenpolitikern: dokumentiert.**
- **Merkels Telefon als mutmaßliches Ziel: stark indiziert und politisch behandelt.**
- **Konkreter individueller Abhörvorgang in einem deutschen Strafverfahren: nicht gerichtsfest bewiesen.**
- **Verantwortung einzelner NSA-Mitarbeiter oder persönliche Anordnung Obamas: öffentlich nicht nachgewiesen.**

1.3 Politische Reaktion und Konsequenzgrenzen

Der Bundestag setzte am 20. März 2014 einstimmig den NSA-Untersuchungsausschuss ein [ref904, ref911]. Dieser arbeitete über drei Jahre, hielt 581 Sitzungsstunden ab, hörte 89 Zeugen und legte 2017 einen etwa 1.800 Seiten umfassenden Abschlussbericht vor [ref903, ref910].

Ein angestrebtes „No-Spy-Abkommen“ kam nicht zustande [ref854, ref861]. Forderungen nach einer Vernehmung Snowdens in Deutschland oder nach Asyl wurden nicht umgesetzt [ref854, ref859, ref862]. Ende 2016 trat ein neues BND-Gesetz in Kraft, das Rechtsgrundlagen und Kontrolle reformieren sollte [ref856, ref861].

Die Konsequenzen blieben begrenzt:

- keine gerichtliche Feststellung des Merkel-Abhörens,
- keine personenbezogene strafrechtliche Verantwortlichkeit,
- kein No-Spy-Abkommen,
- weiterhin enge nachrichtendienstliche Kooperation,
- Reformen der deutschen Rechts- und Kontrollstruktur,
- erheblicher diplomatischer, aber begrenzter materieller Preis für die USA.

Diese Asymmetrie ist für die Doppelstandardfrage relevant: Ein Verbündeter konnte politisch scharf kritisiert werden, ohne Sanktionen oder vergleichbare Strafmaßnahmen wie gegen russische Akteure zu erfahren.

2. BND-NSA-KOOPERATION UND SELEKTOREN

2.1 Kooperationsstruktur

Die Zusammenarbeit in Bad Aibling beruhte auf einem Memorandum of Agreement von 2002. Der BND filterte Kommunikationsdaten anhand von Selektoren der NSA etwa E-Mail-Adressen, Telefonnummern und Internetkennungen [ref865, ref868]. Die Kooperation wurde unter anderem mit Terrorismusbekämpfung begründet, erfasste aber auch europäische Regierungsstellen, Diplomaten und Unternehmen [ref855, ref868, ref870].

2.2 Befunde des Graulich-Berichts

Der ehemalige Bundesverwaltungsrichter Kurt Graulich wurde als Vertrauensperson eingesetzt, weil die vollständigen Selektorenlisten dem Untersuchungsausschuss nicht unmittelbar überlassen wurden. Mitte Mai 2015 umfasste die untersuchte Liste exakt 39.082 Selektoren, darunter 2.918 Telefonnummern und 36.164 Internetadressen. Rund 68,7 Prozent richteten sich gegen Regierungsstellen innerhalb der EU [ref909, ref912].

Graulich kam zu dem Ergebnis, dass die NSA das Kooperationsabkommen systematisch missachtet hatte. Beanstandete Selektoren wurden teilweise erneut eingereicht; zugleich fehlte im BND eine klare Definition „deutscher Interessen“, und Beschäftigte waren nicht hinreichend über die Kooperationsregeln informiert [ref909, ref912].

2.3 Deutsche Mitverantwortung

Die Selektorenaffäre ist kein ausschließlich amerikanischer Fall. Sie zeigt:

- Die NSA definierte problematische Ziele.

- Der BND betrieb technische Filter- und Erfassungsinfrastruktur.
- Kontrollmechanismen funktionierten unzureichend.
- Informationen erreichten Leitung und Kanzleramt verspätet oder unvollständig.
- Der BND überwachte selbst Ziele in EU- und NATO-Staaten.

Der frühere BND-Präsident Gerhard Schindler erklärte, Merkels Aussage über das Abhören unter Freunden habe eine interne Überprüfung ausgelöst; anschließend seien eigene Überwachungsaktivitäten gegen EU- und NATO-Ziele beendet und das Kanzleramt informiert worden [ref1259, ref1260].

Merkel sagte 2017 aus, den Begriff „Selektor“ erst im März 2015 kennengelernt zu haben [ref854, ref858, ref908]. Dies kann ihre persönliche Kenntnis begrenzen, beseitigt aber nicht die institutionelle Verantwortung von BND und Kanzleramt.

2.4 Geheimhaltung und parlamentarische Kontrolle

Die Bundesregierung verweigerte dem Untersuchungsausschuss die vollständige Liste mit Hinweis auf US-Eigentumsrechte, Geheimschutz und internationale Kooperationsfähigkeit. Das Bundesverfassungsgericht ließ diese Verweigerung 2016 im Ergebnis bestehen, weil Geheimhaltungsinteressen und völkerrechtliche Verpflichtungen das parlamentarische Informationsinteresse unter den konkreten Umständen überwogen [ref865, ref869].

Dieser Vorgang illustriert ein strukturelles Dilemma: Nachrichtendienstliche Kooperation kann Sicherheit erhöhen, zugleich aber effektive demokratische Kontrolle beschränken. Wenn Regierungen bei Attributionen gegen Gegner auf geheime Erkenntnisse verweisen, müssen sie akzeptieren, dass dieselbe Geheimhaltung bei eigenen oder verbündeten Operationen Misstrauen erzeugt.

3. STUXNET

3.1 Technisch dokumentierte Sabotage

Stuxnet wurde 2010 entdeckt und war darauf ausgelegt, Siemens-SPS in der iranischen Urananreicherungsanlage Natanz zu manipulieren. Die Schadsoftware beeinflusste die Drehzahlen von Zentrifugen und unterdrückte zugleich Warnanzeigen, sodass physische Degradation und Zerstörung eintreten konnten [ref949, ref951].

Stuxnet unterscheidet sich qualitativ von gewöhnlicher Spionage:

- Eingriff in industrielle Steuerung,
- beabsichtigte physische Wirkung,
- hohe Ziel- und Anlagenkenntnis,

- Sabotage einer strategischen Infrastruktur.

3.2 Attribution und Beleggrenzen

Journalistische Untersuchungen, insbesondere zur „Operation Olympic Games“, schreiben Stuxnet einer gemeinsamen US-israelischen Operation zu, die unter George W. Bush begonnen und unter Barack Obama fortgesetzt worden sei [ref950, ref953]. Hinzu kommen indirekte Aussagen und israelische Hinweise [ref948].

Gleichwohl fehlt eine förmliche öffentliche Verantwortungsübernahme der US- oder israelischen Regierung. Offizielle US-Reden zur Cybersicherheit und technische CISA-Dokumente bestätigen die Urheberschaft nicht [ref1007, ref1008, ref1009, ref1010, ref1012].

Daher ist zu unterscheiden:

- **Funktion und Sabotagewirkung: dokumentiert.**
- **US-israelische Urheberschaft: durch hochwertige journalistische Recherchen und Indizien stark gestützt.**
- **Offizielle staatliche Bestätigung: nicht vorhanden.**
- **Gerichtliche Feststellung und veröffentlichte Befehlskette: nicht vorhanden.**

Stuxnet ist somit ein legitimer Kontrast zu westlichen Vorwürfen gegen russische Cyber-Sabotage. Er rechtfertigt Kritik an selektiver Empörung, widerlegt aber nicht die Belege für einzelne russische Operationen.

4. PEGASUS UND DAS BKA: WENN DIE BEDROHUNG VON INNEN KOMMT

4.1 Erwerb und Einsatz

Das Bundeskriminalamt erwarb die Spionagesoftware Pegasus des israelischen Unternehmens NSO Group spätestens 2020. Der operative Einsatz in Strafverfolgungsverfahren ist ab März 2021 durch Berichte von Süddeutscher Zeitung, Die Zeit und Der Spiegel dokumentiert. Pegasus ermöglicht vollständige Smartphone-Übernahme ohne Nutzerinteraktion: Zugriff auf verschlüsselte Nachrichten, Gesprächsmitschnitt, Kamera- und Mikrofonaktivierung, Echtzeit-Standortdaten und Bewegungsprofile, ohne Spuren, ohne Erkennungsmöglichkeit durch Antiviren-Software, ohne wirksame Abwehrmöglichkeit. Dokumentiert durch forensische Berichte von Amnesty International und dem Citizen Lab der Universität Toronto.

4.2 Die BSI-Warnung und das Klassifizierungsparadox

Am 27. Juli 2021 neun Tage nach dem internationalen Pegasus-Projekt gab das Bundesamt für Sicherheit in der Informationstechnik die Cyber-Sicherheitswarnung CSW 2021-234348-1032 heraus. Das Dokument enthält einen internen Widerspruch, der für die Doppelstandard-Frage zentral ist.

Kopfzeile: IT-Bedrohungslage 2/Gelb (“verstärkte Beobachtung von Auffälligkeiten, temporäre Beeinträchtigung des Regelbetriebs”).

Bewertungstext im selben Dokument: “Das Bedrohungspotenzial ist als hoch zu bewerten.” Schutzmaßnahmen seien “aufgrund der Professionalität der Angreifer sehr schwierig” umzusetzen; “auch aktuelle Versionen von iOS und Android gelten immer noch als verwundbar”; avisierte Ziele könnten “kurzfristig über andere Wege infiziert werden”.

Die Begründung für die niedrige amtliche Einstufung liefert das BSI selbst: Es handele sich nicht um eine Massenverbreitungskampagne. Das ist formal korrekt. Es ist analytisch irrelevant. Pegasus zielt nicht auf Masse, sondern auf Präzision: Staatschefs, Oppositionspolitiker, Journalisten, Menschenrechtsanwälte. Genau die Personengruppe, die politische Entscheidungsprozesse trägt und kontrolliert. Eine auf diese Zielgruppe präzise konzentrierte Vollzugriffswaffe als 2/Gelb einzustufen, beschreibt keine technische Bewertung. Es beschreibt eine politische Deutungsentscheidung.

4.3 Parlamentarische Kontrolle: verweigert

NSO Group ist ein israelisches Unternehmen. Die Exportgenehmigung für Pegasus an ausländische Behörden liegt beim israelischen Verteidigungsministerium, nicht bei NSO. Der Kauf durch das BKA ist damit ein bilateraler Staatsbeschaffungsvorgang.

Das Pegasus-Projekt (Washington Post, Guardian, Le Monde und 13 weitere Medien) belegte Juli 2021: 50.000 Zielnummern, darunter der französische Staatspräsident Macron. Trotz dieses weltweiten Skandals ergriffen die betroffenen europäischen Staaten nach Feststellung einer ARTE-Dokumentation von 2022 keinerlei Maßnahmen.

Bundesinnenminister Alexander Dobrindt reiste am 29. Juni 2025 nach Jerusalem und traf Netanyahu, Außenminister Gideon Sa’ar und Verteidigungsminister Israel Katz (Bundestag-Drucksache 21/4306, 23.02.2026). Am 12. Januar 2026 unterzeichneten Dobrindt und Netanyahu in Jerusalem einen Cyber- und Sicherheitspakt. Das Bundesministerium des Innern verkündete dies auf seiner Website. Als beteiligte deutsche Behörden nennt die Bundesregierung das BKA, die Bundespolizei, das BSI und ZITiS (Drucksache 21/4306, S. 5). Israelische Partner: Israel National Cyber Directorate und Israel National Police.

Der Pakttext ist nicht veröffentlicht. Parlamentarische Anfragen zu gemeinsamen Datenzugriffen zwischen dem Bundesamt für Verfassungsschutz und israelischen Nachrichtendiensten beantwortete

die Bundesregierung mit der Begründung: “aus Gründen des Staatswohls” (Drucksache 21/4306, S. 4).

4.4 Einordnung in die Doppelstandard-Frage

Wenn russische Geheimdienste verdächtigt werden, Personen zu rekrutieren, die Daten aus deutschen Institutionen abziehen, bezeichnet die Bundesregierung das als Hybridkrieg. Wenn das BKA Vollzugriffs-Spyware kauft, israelischer Provenienz, mit staatlicher Exportgenehmigung, auf Smartphones aller Zielpersonen, und diese Aktivität als Verschlusssache gegen parlamentarische Kontrolle abschirmt: Kein Bundesminister nennt das vergleichbar.

Das ist kein Argument dafür, dass beides gleich schlimm ist. Es ist ein Argument dafür, dass der Begriff Hybridkrieg nicht symmetrisch angewendet wird. Aktivitäten, die bei einem westlich verbündeten Staat mit Schweigen und Paktunterzeichnung beantwortet werden, lösen bei Russland für funktional Vergleichbares Kriegsrhetorik aus. Das ist eine dokumentierbare Asymmetrie, kein moralisches Urteil.

5. US-CYBEROPERATIONEN GEGEN RUSSLAND

5.1 Offiziell bestätigte Doktrin und Operationstypen

US Cyber Command beschreibt „persistent engagement“ und „defend forward“ als kontinuierliches Handeln im Cyberraum, um gegnerische Aktivitäten möglichst nahe an ihrem Ursprung zu erkennen und zu stören [ref958, ref999]. „Hunt Forward“-Teams werden auf Einladung von Partnerstaaten in deren Netzen eingesetzt. Bis Mai 2022 waren 28 Einsätze in 16 Staaten öffentlich genannt, darunter Estland, Litauen, Montenegro, Nordmazedonien und die Ukraine [ref987, ref990].

Diese Einsätze sind offiziell als defensiv beschrieben. Sie liefern jedoch zugleich:

- Einblick in gegnerische Werkzeuge,
- Malwareproben,
- Informationen über Infrastruktur und TTPs,
- operative Erfahrung in Netzen nahe an einem Gegner.

Aus „defend forward“ folgt grundsätzlich die Bereitschaft, außerhalb eigener Netze tätig zu werden. Daraus folgt aber nicht automatisch, dass jeder Einsatz in fremde staatliche Infrastruktur eindringt oder destruktive Wirkungen erzeugt.

4.2 Öffentlich berichtete offensive Operationen

Russland erklärte 2019, amerikanische Angriffe auf Kontrollsysteme russischer Infrastruktur abgewehrt zu haben [ref973]. Diese russische Behauptung ist kein unabhängiger Beleg.

Stärker ist die Reuters-Meldung vom März 2025, wonach die USA eine Pause offensiver Cyberoperationen gegen Russland angeordnet hätten; die Entscheidung sei mit diplomatischen Bemühungen zur Ukraine verbunden gewesen [ref1000]. Eine Anordnung, Operationen zu pausieren, ist ein relevantes Indiz dafür, dass offensive Aktivitäten bestanden. Sie beweist aber nicht öffentlich:

- welche Systeme angegriffen wurden,
- ob es sich um Spionage, Vorbereitung, Störung oder Zerstörung handelte,
- welche Wirkungen eintraten,
- auf welcher Rechtsgrundlage einzelne Operationen beruhten.

Die symmetrische Einordnung lautet daher: **Offensive US-Cyberaktivität gegen Russland ist als allgemeine Praxis und politische Kategorie plausibel und teilweise journalistisch bestätigt; konkrete destruktive Operationen gegen russische kritische Infrastruktur sind in der vorliegenden öffentlichen Dokumentation nicht in derselben Detailtiefe belegt wie NotPetya.**

6. NATO IST NICHT MIT DEN USA GLEICHZUSETZEN

Die NATO erkannte den Cyberraum 2016 als Operationsdomäne an [ref1014, ref1017]. Sie schützt eigene Netze und kann bei schwerwiegenden Cyberangriffen auf Einzelfallbasis Artikel 5 in Betracht ziehen [ref1015, ref1017, ref1019].

Nach NATO-Dokumenten verfügt die Organisation jedoch nicht über eigene offensive Cyberkräfte. Sie kann „Sovereign Cyber Effects Provided Voluntarily by Allies“ integrieren; Eigentum und Kontrolle verbleiben grundsätzlich bei den Mitgliedstaaten [ref1014, ref1017, ref1020].

Folglich sind drei Ebenen zu unterscheiden:

1. nationale US-Operation,
2. nationale Operation eines anderen NATO-Mitglieds,
3. in eine NATO-Mission eingebrachter nationaler Cyber-Effekt.

Ohne konkreten Nachweis darf eine US-Operation nicht als „NATO-Angriff“ bezeichnet werden. Umgekehrt kann die NATO politisch oder operativ eingebunden sein, wenn ein Mitglied eine nationale Fähigkeit freiwillig für eine gemeinsame Mission bereitstellt.

7. NATO-OSTERWEITERUNG UND ZUSAGEN VON 1990/91

6.1 Dokumentierte Zusicherungen

Archivunterlagen dokumentieren, dass westliche Politiker im Kontext der deutschen Einheit mehrfach Formulierungen verwendeten, die sowjetische Sorgen vor einer Ostverschiebung der NATO

beruhigen sollten. James Baker erklärte 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 [ref1022, ref1076, ref1080, ref1083].

Hans-Dietrich Genscher hatte zuvor gefordert, die deutsche Einheit dürfe sowjetische Sicherheitsinteressen nicht beeinträchtigen und die NATO solle eine territoriale Ausdehnung nach Osten ausschließen [ref1022]. Archivforscher sprechen deshalb von einer „Kaskade“ politischer Zusicherungen.

6.2 Räumliche und rechtliche Begrenzung

Umstritten ist, ob diese Äußerungen:

- nur das Gebiet der früheren DDR,
- die militärische NATO-Jurisdiktion,
- oder eine allgemeine Nichtaufnahme osteuropäischer Staaten betrafen.

Die Dokumente stützen, dass der Gesprächshorizont zeitweise über rein technische Stationierungsfragen in Ostdeutschland hinausging [ref1022, ref1077]. Gleichzeitig entstand daraus kein unterschriebener allgemeiner Nichtausweitungsvertrag.

Der Zwei-plus-Vier-Vertrag vom 12. September 1990 ermöglichte die deutsche Einheit, bestätigte die NATO-Mitgliedschaft des vereinten Deutschlands und regelte besondere Beschränkungen für ausländische Truppen und Kernwaffen auf dem Gebiet der früheren DDR [ref1066, ref1067, ref1068]. Er verbot nicht generell die spätere Aufnahme Polens, Ungarns oder anderer Staaten.

Daher sind zwei Aussagen zugleich zutreffend:

- **Politisch-historisch:** Sowjetische Entscheidungsträger erhielten wiederholte Zusicherungen, die eine Erwartung westlicher Zurückhaltung erzeugen konnten.
- **Rechtlich:** Eine allgemeine, dauerhaft bindende Nichtausweitungsverpflichtung wurde nicht kodifiziert.

Die Aussage „Es gab keinerlei Zusage“ ist zu kategorisch. Ebenso zu kategorisch ist die Aussage „Die NATO brach einen eindeutigen schriftlichen Vertrag“.

6.3 Spätere Erweiterung und Handlungsmacht der Beitrittsstaaten

Die Erweiterung war nicht ausschließlich ein amerikanischer Vorgang; beitrittswillige Staaten handelten aus eigenen Sicherheitsinteressen. Spätere Beitritte Finnlands und Schwedens zeigen diese Handlungsmacht besonders deutlich: Beide beantragten nach dem russischen Großangriff auf die Ukraine am 18. Mai 2022 die Mitgliedschaft; Finnland trat am 4. April 2023, Schweden am 7. März 2024 bei [ref1051, ref1057, ref1059, ref1063].

Das erklärt nicht rückwirkend alle früheren Erweiterungen und hebt russische Sicherheitswahrnehmungen nicht auf. Es widerspricht aber einer Darstellung, osteuropäische Staaten seien lediglich passive Objekte amerikanischer Expansion.

6.4 NATO-Russland-Grundakte

Die spätere NATO-Russland-Grundakte gehört politisch zur Entwicklung der Beziehungen nach den frühen Zusicherungen. Die vorliegenden Forschungsdaten enthalten jedoch keine hinreichend detaillierte Primärquellenauswertung ihrer einzelnen Bestimmungen. Sie kann deshalb hier nur als späterer institutioneller Rahmen genannt, nicht aber als Beleg für eine umfassende russische Zustimmung zu jeder künftigen Erweiterung oder für eine westliche Aufgabe aller früheren politischen Zusicherungen verwendet werden.

8. WESTLICHER EINFLUSS IN DER UKRAINE

7.1 Das Nuland-Pyatt-Gespräch

Das Anfang Februar 2014 veröffentlichte Gespräch zwischen Victoria Nuland und US-Botschafter Geoffrey Pyatt ist als Aufnahme und diplomatischer Vorgang dokumentiert. Beide diskutierten bevorzugte Rollen ukrainischer Oppositionspolitiker. Nuland hielt Arsenij Jazenjuk für die geeignete Person für eine führende Regierungsrolle, während Vitali Klitschko zunächst außerhalb der Regierung bleiben sollte [ref1104, ref1105, ref1110]. Das US-Außenministerium bestritt die inhaltliche Richtigkeit nicht ausdrücklich; Nuland entschuldigte sich für ihre Äußerung über die EU [ref1144, ref1151].

Das Gespräch belegt:

- intensive amerikanische Einmischung in die politische Krisenbearbeitung,
- klare personelle Präferenzen,
- den Versuch, internationale Vermittlung und ukrainische Regierungsbildung zu beeinflussen.

Es belegt nicht allein:

- operative US-Kontrolle über die Protestbewegung,
- einen amerikanischen Befehl zur Absetzung Wiktor Janukowytschs,
- Kontrolle über sämtliche ukrainischen Parteien, Sicherheitskräfte oder Parlamentsentscheidungen,
- Planung jedes Gewaltereignisses,
- einen vollständig fremdgesteuerten Staatsstreich.

Die korrekte Einordnung liegt zwischen den Polen „bloße normale Diplomatie ohne Einflussabsicht“ und „lückenlos bewiesener amerikanischer Regimewechsel“.

7.2 NED- und USAID-Förderung

NED unterstützte in der Ukraine Zivilgesellschaft, unabhängige Medien, Menschenrechtsgruppen, Parteienentwicklung und Antikorruptionsarbeit [ref1113, ref1114, ref1154, ref1156]. USAID finanzierte Programme zu Wahlen, Parlament, Dezentralisierung, Zivilgesellschaft, Medienkompetenz und Korruptionsbekämpfung [ref1120, ref1123, ref1124, ref1126].

Diese Finanzierung ist politische Einflussnahme im weiten Sinn: Geld, Ausbildung, Netzwerke und institutionelle Beratung verändern Handlungsmöglichkeiten. NED wird weitgehend aus Mitteln des US-Kongresses finanziert, auch wenn es formal als private gemeinnützige Organisation auftritt. Kritik an der geopolitischen Funktion solcher Förderung ist daher grundsätzlich legitim.

Nicht belegt ist dagegen der automatische Schluss:

> westliche Finanzierung einzelner Organisationen → westliche Kontrolle der gesamten ukrainischen Gesellschaft → vollständig gesteuerter Machtwechsel.

Dazwischen liegen mehrere ungeklärte Kausalstufen. Förderempfänger können eigene Interessen verfolgen, Geldgeber enttäuschen oder miteinander konkurrieren. Wissenschaftliche Untersuchungen beschreiben zudem „NGO-cracy“, Geberabhängigkeit und Distanz mancher Organisationen zur breiten Bevölkerung, aber auch erhebliche eigenständige ukrainische Mobilisierung und informelle Netzwerke [ref1169, ref1171, ref1173, ref1174].

7.3 Ukrainische Handlungsmacht und Wahlen

Die OSZE/ODIHR bewertete die Präsidentschaftswahl vom 25. Mai 2014 trotz Gewalt und Einschränkungen als Ausdruck des Willens, demokratische Freiheiten zu schützen [ref1161, ref1163, ref1165]. Die Parlamentswahl vom 26. Oktober 2014 galt als wichtiger Schritt demokratischer Konsolidierung, wenngleich Stimmenkauf, administrative Ressourcen, Kommissionsprobleme und Sicherheitsbeschränkungen festgestellt wurden [ref1129, ref1166].

Auch die Wahlen von 2019 wurden als wettbewerblich beschrieben, allerdings mit Problemen wie Stimmenkauf, Amtsbonus und rechtlichen Schlupflöchern [ref1130, ref1132, ref1133].

Diese Befunde beweisen keine makellose Verfassungs- oder Revolutionsgeschichte. Sie zeigen jedoch, dass die weitere ukrainische Entwicklung nicht überzeugend als bloße Marionettensteuerung beschrieben werden kann. Ukrainische Wähler, Parteien, Oligarchen, Aktivisten, regionale Interessen und staatliche Institutionen besaßen eigene Handlungsmacht.

7.4 Gesamtbewertung

- **Belegt:** westliche Finanzierung, politische Beratung, personelle Präferenzen und Einflussversuche.
- **Plausibel und diskussionswürdig:** westliche Programme trugen zur langfristigen prowestlichen Orientierung bestimmter Eliten und Organisationen bei.
- **Nicht durch die vorliegenden Belege nachgewiesen:** vollständige operative Steuerung des Maidan oder ein lückenlos von Washington befohlener Regimewechsel.
- **Ebenfalls unzureichend:** eine Darstellung, nach der externe Einflüsse keinerlei Bedeutung hatten.

9. SANKTIONEN: ZWANG, RECHT UND KRIEGSBEGRIFF

8.1 Rechtsgrundlagen

EU-Sanktionen werden im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik beschlossen und insbesondere über Artikel 215 AEUV sowie Verordnungen wie 833/2014 und 269/2014 umgesetzt [ref1219, ref1220]. Ziele sind wirtschaftlicher Druck, Einschränkung russischer Kriegsfinanzierung und Verweigerung kritischer Technologie [ref1176, ref1177, ref1183].

US-Sanktionen beruhen unter anderem auf dem International Emergency Economic Powers Act, präsidentiellen Executive Orders wie E.O. 14024 und Gesetzen wie CAATSA [ref1184, ref1193, ref1227]. OFAC kann Vermögen blockieren und Transaktionen untersagen [ref1227, ref1229].

8.2 Wirkungen und Bewertung

Sanktionen treffen Finanzen, Energie, Technologie, Transport, Einzelpersonen und Unternehmen. Sie können Vermögenswerte einfrieren, Handel verhindern, Kosten erhöhen und mittelbar auch unbeteiligte Bevölkerungsteile oder Drittstaaten belasten [ref1176, ref1177, ref1183].

Ihre Wirksamkeit bleibt umstritten. Ein US-GAO-Bericht kritisierte fehlende klare und messbare Ziele, die eine belastbare Erfolgskontrolle erschweren [ref1187, ref1191]. Umgehung, Drittstaatenhandel und begrenzte internationale Beteiligung reduzieren die Wirkung [ref1184, ref1187].

8.3 Sind Sanktionen Kriegshandlungen?

Politisch können umfassende Sanktionen als „Wirtschaftskrieg“ bezeichnet werden. Dieser Ausdruck beschreibt Intensität und Zweck, ist aber keine automatische völkerrechtliche Klassifikation. Die Schwelle zur Gewaltanwendung oder zum bewaffneten Angriff wird im Cyber- und allgemeinen

Völkerrecht regelmäßig an Wirkungen wie Tod, Verletzung oder physische Zerstörung angeknüpft [ref1194, ref1201, ref1203].

Deshalb gilt:

- Sanktionen sind coercive, also Zwangsmittel.
- Sie können rechtswidrig, unverhältnismäßig oder humanitär schädlich sein.
- Sie sind nicht allein wegen ihrer Schwere automatisch militärische Angriffe.
- Ihre Rechtmäßigkeit ist anhand der jeweiligen Rechtsgrundlage, Zuständigkeit, Verhältnismäßigkeit und menschenrechtlichen Folgen zu beurteilen.
- Der politische Begriff „Wirtschaftskrieg“ darf nicht unbesehen in „bewaffneter Angriff“ übersetzt werden.

TEIL III: SYMMETRISCHER VERGLEICH UND DOPPELSTANDARDFRAGE

1. VERGLEICHSMATRIX

Kriterium	Russland zugeschriebene Fälle	Westliche Fälle	Symmetrischer Maßstab
Spionage	GRU-, SVR- oder FSB-Aktivitäten werden politisch und technisch attribuiert	NSA/GCHQ-Überwachung, Merkel-Ziel, BND-NSA-Selektoren sind dokumentiert	Spionage aller Staaten kritisch prüfen; nicht automatisch mit Sabotage gleichsetzen
Cyber-Sabotage	NotPetya, Industroyer und Olympic Destroyer werden Sandworm zugeschrieben [ref804, ref810]	Stuxnet wird USA/Israel stark zugeschrieben, aber nicht offiziell eingestanden [ref949, ref950]	Physische und destruktive Wirkung bei allen Akteuren höher gewichten als bloße Ausspähung
Öffentliche Beweise	technische Advisories, Sanktionen, Anklagen, teils namentliche Beschuldigte	Snowden-Dokumente, Untersuchungsausschüsse, journalistische Recherchen, offizielle Doktrin	Quellentyp und Offenlegungsgrad sichtbar machen

Kriterium	Russland zugeschriebene Fälle	Westliche Fälle	Symmetrischer Maßstab
Gerichtlicher Status	US-Anklagen, meist keine Verurteilung der russischen Beschuldigten	Merkel-Verfahren eingestellt; keine Stuxnet-Verurteilung	Anklage, Ermittlung, Einstellung und Urteil nicht vermischen
Staatliche Zurechnung	bei GRU-Offizieren und Einheiten teilweise stark	NSA und BND institutionell eindeutig; Stuxnet nur indirekt	Organisationszugehörigkeit und staatliche Zurechnung gleich prüfen
Persönliche Befehlskette	Putin-Befehl öffentlich regelmäßig nicht bewiesen	Obama-Befehl zu Merkel oder Stuxnet öffentlich nicht bewiesen	Kein Staatsoberhaupt ohne spezifische Belege persönlich verantwortlich erklären
Geheimhaltung	westliche Dienste legen Quellen nicht vollständig offen	westliche Dienste verweigern auch bei eigenen Operationen Akten oder Bestätigung	Geheimhaltung als reale Grenze, aber nicht als Beweisersatz behandeln
Institutionelle Kontrolle	öffentliche Einsicht in russische Kontrolle begrenzt	Bundestagsausschuss und Gerichte existieren, waren aber durch Geheimschutz beschränkt	Nicht nur Existenz, sondern tatsächliche Wirksamkeit der Kontrolle bewerten
Rechtsfolgen	Sanktionen, Anklagen, Ausweisungen, diplomatische Maßnahmen	bei NSA-Affäre überwiegend politische Kritik und Rechtsreformen	Unterschiede müssen sachlich begründet werden, etwa Bündnisstatus oder Schadensart; bloße Nähe genügt nicht
False Flags	in GRU-Anklagen und Olympic Destroyer beschrieben	westliche Akteure könnten technisch ebenfalls täuschen; konkreter Beleg erforderlich	Möglichkeit anerkennen, konkrete Behauptung nur mit positiven Belegen
Proxy- und Hacktivistenmodell	patriotische Hacker oder kriminelle Gruppen möglich	private Auftragnehmer und nationale Beiträge ebenfalls möglich	Kontrolle, Finanzierung und Weisung bei allen Seiten untersuchen
Sanktionen	Russland bezeichnet sie als Krieg oder Aggression	EU/USA behandeln sie als Rechts- und Politikinstrument	politische Härte von juristischer Gewaltanwendung trennen

2. SPIONAGE IST NICHT GLEICH SABOTAGE

Spionage kann nationale Gesetze, Datenschutz, diplomatisches Vertrauen und möglicherweise Souveränitätsrechte verletzen. Das Völkerrecht enthält jedoch kein umfassendes, unstreitiges Verbot jeder Spionage in Friedenszeiten; umstritten ist, wann Cyberausspähung zusätzlich Souveränität oder das Interventionsverbot verletzt [ref1204, ref1206, ref1211].

Cyber-Sabotage zielt dagegen auf Funktionsbeeinträchtigung oder Zerstörung. NotPetya und Stuxnet sind deshalb anders zu bewerten als das Abhören eines Telefons, auch wenn alle Vorgänge rechts- und politisch problematisch sein können.

Eine konsistente Skala unterscheidet:

1. passive Informationsgewinnung,
2. Eindringen und dauerhafte Präsenz,
3. Datendiebstahl und Veröffentlichung,
4. Manipulation von Daten oder Abläufen,
5. Betriebsunterbrechung,
6. physische Zerstörung,
7. Verletzung oder Tod,
8. Wirkungen auf dem Niveau bewaffneter Gewalt.

Der Akteur darf die Kategorie nicht bestimmen. Wenn Stuxnet westliche Sabotage war, muss es als solche bezeichnet werden. Wenn NotPetya russische destruktive Staatshandlung war, darf es nicht als bloße Spionage verharmlost werden.

3. ÖFFENTLICHES BEWEISNIVEAU

Ein symmetrischer Maßstab verlangt für jede Attribution:

- mehrere voneinander unabhängige Belegklassen,
- Offenlegung technischer Befunde, soweit sicher möglich,
- klare Trennung technischer von politischer Attribution,
- Benennung des Vertrauensgrades,
- Prüfung von Alternativerklärungen,
- Korrekturmöglichkeit bei neuen Erkenntnissen,
- keine persönliche Zuschreibung an Staatsoberhäupter ohne gesonderte Beweise.

Unter diesem Maßstab ist die NotPetya-Attribution stärker als viele pauschale Behauptungen über „russische Hacker“, weil sie technische, organisatorische und personenbezogene Elemente verbindet.

Die Merkel-Affäre ist institutionell und politisch stark belegt, blieb hinsichtlich des individuellen strafrechtlichen Vorgangs aber unterhalb gerichtsfester Gewissheit. Stuxnet ist technisch eindeutig Sabotage, während die staatliche Urheberschaft journalistisch stark, aber amtlich nicht bestätigt ist.

4. GEHEIMHALTUNGSPROBLEM

Staaten verlangen häufig Vertrauen in geheime Beweise, wenn sie Gegner beschuldigen. Dieselben Staaten berufen sich auf Geheimschutz, wenn eigene Tätigkeiten untersucht werden. Der NSA-Ausschuss zeigt dieses Spannungsverhältnis deutlich: Das Parlament erhielt keinen vollständigen Zugriff auf Selektoren; Geheimhaltungs- und Kooperationsinteressen setzten der Kontrolle Grenzen [ref865, ref869].

Daraus folgt kein genereller Schluss, Regierungsattributionen seien wertlos. Es folgt aber:

- Regierungsaussagen dürfen nicht als gerichtlicher Vollbeweis ausgegeben werden.
- Wo Offenlegung unmöglich ist, muss der verbleibende Unsicherheitsgrad benannt werden.
- Gemeinsame Attributionen mehrerer verbündeter Dienste sind nicht vollständig unabhängig, wenn sie dieselben geheimen Informationen teilen.
- Technische Berichte sollten möglichst reproduzierbare Daten enthalten.
- Parlamente und Gerichte benötigen privilegierten Zugang, auch wenn die Öffentlichkeit ihn nicht erhält.

5. INSTITUTIONELLE KONTROLLE

Westliche Demokratien verfügen über Untersuchungsausschüsse, Gerichte, Datenschutzbehörden und freie Medien. Der NSA-Ausschuss, der Graulich-Bericht und die öffentliche Debatte sind reale Kontrollleistungen. Sie brachten umfangreiche Missstände ans Licht.

Diese Institutionen sind jedoch kein automatischer Beweis effektiver Verantwortlichkeit:

- Snowden wurde nicht vor dem Ausschuss in Deutschland vernommen.
- Selektorenlisten blieben geheim.
- Das Merkel-Verfahren endete ohne Verantwortlichen.
- Ein No-Spy-Abkommen scheiterte.
- Die Zusammenarbeit mit der NSA wurde nicht grundsätzlich beendet.

Eine symmetrische Bewertung darf daher weder behaupten, es habe keine Kontrolle gegeben, noch Kontrolle mit vollständiger Aufklärung gleichsetzen.

6. RECHTSFOLGEN UND BÜNDNISPOLITIK

Russische Akteure wurden mit Sanktionen, Anklagen und öffentlicher Attribution belegt. Auf die NSA-Affäre folgten hauptsächlich diplomatische Kritik, parlamentarische Untersuchung und deutsche Gesetzesreform. Diese unterschiedliche Behandlung kann teilweise erklärt werden durch:

- Bündnisbeziehungen,
- unterschiedliche Rechtszuständigkeit,
- Schadensart,
- Beweislage,
- politische Abhängigkeiten,
- erwartete Wirksamkeit von Maßnahmen.

Sie kann zugleich als Doppelstandard wirken, wenn identische Handlungen bei Gegnern als grundsätzlich illegitim und bei Verbündeten als bloßer Ausrutscher behandelt werden. Konsistenz verlangt zumindest, verbündete Spionage klar zu benennen, ihre Opfer anzuerkennen und wirksame Kontrolle zu verlangen.

7. WIDERLEGT MERKELS ÜBERWACHUNG VORWÜRFE GEGEN RUSSLAND?

Nein. Die Überwachung Merkels widerlegt weder die technische Attribution von NotPetya noch die organisatorische Zuordnung von Sandworm zum GRU. Ein Fehlverhalten der USA macht eine unabhängige russische Operation weder unmöglich noch rechtmäßig.

Sie widerlegt jedoch drei weitergehende Behauptungen:

1. dass westliche Staaten keine aggressive oder rechtsproblematische Cyber- und Nachrichtendiensttätigkeit betrieben;
2. dass enge Bündnispartner grundsätzlich nicht gegeneinander spionierten;
3. dass westliche Regierungserklärungen allein wegen ihrer Herkunft einen höheren Beweiswert hätten.

Die angemessene Folgerung lautet:

- gleiche Beweisstandards,
- gleiche begriffliche Kategorien,
- gleiche Anforderungen an staatliche Zurechnung,
- gleiche Zurückhaltung bei persönlichen Befehlsketten,
- gleiche menschenrechtliche und rechtsstaatliche Kontrolle,

- unterschiedliche Bewertung nur bei nachweislich unterschiedlichen Wirkungen und Rechtslagen.

„Die NSA hat Merkel überwacht, also ist jede Russland-Attribution falsch“ ist ein Fehlschluss. Ebenso fehlerhaft wäre: „Russland betreibt Cyberoperationen, also ist die NSA-Überwachung unerheblich.“

8. LIEGT EIN DOPPELSTANDARD VOR?

Eine pauschale Ja-oder-Nein-Antwort wäre unzureichend.

Bereiche mit erkennbarer Asymmetrie

- Westliche Spionage gegen Verbündete hatte begrenztere außenpolitische Folgen.
- Bei Russland werden staatliche und persönliche Verantwortlichkeit in öffentlicher Sprache häufig verkürzt.
- Westliche Cyberaktivitäten werden eher als „defensiv“, „forward defense“ oder „intelligence“ beschrieben, russische eher als „hybrid warfare“, auch wenn operative Methoden sich überschneiden können.
- Stuxnet wird trotz destruktiver Wirkung seltener im selben normativen Rahmen wie russische Sabotage behandelt.
- Sanktionen und Cyberoperationen westlicher Staaten werden häufiger aus ihrem erklärten Zweck heraus bewertet, gegnerische Operationen stärker nach ihren Wirkungen.

Bereiche, in denen Unterschiede sachlich begründet sein können

- Nicht jede Operation hat dieselbe Wirkung.
- NotPetya verursachte breite Kollateralschäden; gewöhnliche Spionage tut dies nicht.
- Eine detaillierte Anklage gegen identifizierte Offiziere besitzt mehr öffentliches Gewicht als eine allgemeine Verdächtigung.
- Ein transparentes Untersuchungsverfahren ist institutionell relevant, auch wenn es unvollständig bleibt.
- Staatliche Organe, unabhängige Kriminelle und lose Hacktivisten sind rechtlich verschieden.
- NATO, USA, EU und einzelne Mitgliedstaaten sind keine identischen Akteure.

Das Ergebnis ist daher: **In politischer Reaktion, Sprache und Rechtsfolgen existieren Anzeichen selektiver Maßstäbe. Daraus folgt aber nicht, dass sämtliche westlichen Vorwürfe gegen Russland unbegründet oder sämtliche Handlungen moralisch und rechtlich gleichwertig wären.**

ABSCHLIESSENDE ANTWORTEN AUF DIE LEITFRAGEN

Leitfrage 1: Wie belastbar sind Attributionen mutmaßlich russischer Cyberangriffe, Sabotage und Spionage?

Sie reichen von spekulativ bis stark gestützt. Pauschale Aussagen über „russische Hacker“ sind häufig zu ungenau. Im Fall von Sandworm und NotPetya besteht dagegen eine vergleichsweise starke öffentliche Beweiskette aus technischen Analysen, gemeinsamen Behördenwarnungen, Organisationszuordnung und namentlicher Anklage gegen GRU-Offiziere [ref773, ref775, ref803, ref804].

Diese Beweiskette stützt die Zuordnung zur GRU-Einheit 74455. Sie ist kein rechtskräftiges Urteil gegen die Beschuldigten und kein öffentlicher Beweis, dass Putin den konkreten Angriff persönlich angeordnet hat. Eine direkte Putin-Befehlskette ist öffentlich nicht nachweisbar.

Unabhängige Kriminelle, Dissidenten, False Flags und patriotische Hacker sind grundsätzlich mögliche Erklärungen. Sie müssen anhand positiver Belege geprüft werden. Ihre bloße Möglichkeit reicht weder zur Entkräftung einer starken Attribution noch zur Begründung einer alternativen Schuldzuweisung.

Leitfrage 2: Welche westlichen Aktivitäten sind nachweisbar?

Am klarsten dokumentiert sind:

- globale NSA- und GCHQ-Überwachung,
- die mutmaßliche Zielerfassung Angela Merkels,
- die BND-NSA-Kooperation und problematische Selektoren gegen europäische und deutsche Interessen,
- offiziell bestätigte US-Cyberdoktrinen wie „persistent engagement“ und „defend forward“,
- auf Einladung durchgeführte Hunt-Forward-Einsätze,
- politisch und rechtlich kodifizierte Sanktionen,
- umfangreiche NED- und USAID-Förderung in der Ukraine,
- amerikanische Präferenzen im Nuland-Pyatt-Gespräch.

Stuxnet ist als Sabotage technisch dokumentiert und wird den USA und Israel durch hochwertige Recherchen stark zugeschrieben, ist aber nicht offiziell eingestanden. Konkrete destruktive US-Angriffe auf russische Infrastruktur sind öffentlich weniger detailliert dokumentiert. Die gemeldete Aussetzung offensiver Operationen 2025 ist ein relevantes Indiz, aber keine vollständige Offenlegung [ref1000].

Leitfrage 3: Werden unterschiedliche Beweisstandards angewandt?

Teilweise ja. In politischer Kommunikation werden Regierungsattributionen gegen Gegner oft wie feststehende Tatsachen behandelt, während vergleichbare Vorwürfe gegen Verbündete als unbewiesen oder als normale Geheimdienstpraxis relativiert werden. Die Merkel- und Selektorenaffäre zeigt, dass auch westliche Staaten systematisch Partner ausspähten und Kontrollregeln verletzten.

Ein konsistenter Standard darf jedoch nicht jede Handlung gleichsetzen. Spionage, Sabotage, Datenveröffentlichung und physische Gewalt unterscheiden sich in Wirkung und Rechtslage. Symmetrie bedeutet gleiche Prüfkriterien, nicht identische Urteile unabhängig vom Sachverhalt.

Leitfrage 4: Widerlegt die NSA-Überwachung Merkels westliche Russland-Kritik?

Nein. Sie widerlegt keine unabhängig belegte russische Operation. Sie verpflichtet westliche Regierungen jedoch zu Selbstanwendung ihrer Standards:

- keine persönliche Schuldzuweisung ohne Beweis,
- transparente Kennzeichnung von Unsicherheit,
- wirksame parlamentarische und gerichtliche Kontrolle,
- klare Kritik auch an verbündeter Spionage,
- keine Verharmlosung westlicher Sabotage,
- keine Gleichsetzung politischer Attribution mit gerichtlichem Beweis.

Leitfrage 5: Waren NATO-Erweiterung und Ukrainepolitik westliche Aggressionen?

Die Dokumentenlage zur NATO zeigt reale politische Zusicherungen 1990/91, aber keinen allgemeinen rechtsverbindlichen Nichtausweitungsvertrag. Die Behauptung eines völlig erfundenen russischen Beschwerdegrundes ist historisch zu grob; die Behauptung eines eindeutig gebrochenen schriftlichen Vertrags ist rechtlich falsch.

In der Ukraine sind westlicher Einfluss, Finanzierung und politische Einmischung belegt. Nicht belegt ist eine vollständige westliche Steuerung sämtlicher Ereignisse. Eine sachgerechte Analyse muss externe Einflussnahme und ukrainische Handlungsmacht gleichzeitig anerkennen.

Leitfrage 6: Sind Sanktionen Krieg?

Sanktionen sind machtpolitische und rechtliche Zwangsinstrumente mit teils schweren wirtschaftlichen und humanitären Folgen. Sie können politisch als Wirtschaftskrieg bezeichnet werden. Rechtlich sind sie jedoch nicht automatisch Gewaltanwendung oder bewaffneter Angriff. Für eine solche Einstufung müssten Rechtsgrundlage, Wirkungen und anwendbare völkerrechtliche Schwellen im Einzelfall geprüft werden.

ANHANG A: ZEITACHSE ZENTRALER EREIGNISSE

Jahr/Datum	Ereignis	Belegstatus
9. 10. Februar 1990	Baker und Kohl verwenden gegenüber Gorbatschow Formulierungen gegen eine Ostverschiebung der NATO-Aktivität [ref1022, ref1076, ref1080, ref1083]	Dokumentierte diplomatische Zusicherungen; keine allgemeine Vertragsklausel
12. September 1990	Unterzeichnung des Zwei-plus-Vier-Vertrags [ref1066, ref1067]	Rechtsverbindlicher Vertrag mit besonderen Regeln für frühere DDR
15. März 1991	Inkrafttreten des Zwei-plus-Vier-Vertrags [ref1066, ref1067]	Dokumentiert
2002	Memorandum zur BND-NSA-Kooperation in Bad Aibling [ref865, ref868]	Institutionell dokumentiert
2010	Entdeckung von Stuxnet [ref949, ref951]	Sabotagefunktion dokumentiert; Urheberschaft nicht offiziell eingestanden
Juni 2013	Beginn der Snowden-Veröffentlichungen [ref855, ref861]	Dokumentiert
23. Oktober 2013	Obama erklärt, Merkels Kommunikation werde gegenwärtig nicht und künftig nicht überwacht [ref922]	Offizielle Erklärung; Vergangenheit offengelassen
2013/14	Maidan-Proteste; westliche diplomatische und zivilgesellschaftliche Einflussnahme	Finanzierung und Diplomatie belegt; Gesamtsteuerung nicht belegt
Februar 2014	Veröffentlichung des Nuland-Pyatt-Gesprächs [ref1104, ref1144]	Aufnahme und politische Präferenzen dokumentiert
20. März 2014	Bundestag setzt NSA-Untersuchungsausschuss ein [ref904, ref911]	Dokumentiert

Jahr/Datum	Ereignis	Belegstatus
25. Mai 2014	Ukrainische Präsidentschaftswahl unter OSZE-Beobachtung [ref1161, ref1163]	Dokumentiert
26. Oktober 2014	Ukrainische Parlamentswahl [ref1129]	Dokumentiert; Mängel und Sicherheitsbeschränkungen
2015	Angriff auf den Deutschen Bundestag	Offiziell russischen Akteuren zugeschrieben; hier begrenzte technische Detailbasis
12. Juni 2015	Einstellung des Ermittlungsverfahrens zum Merkel-Handy [ref878]	Strafrechtlicher Beweis nicht erbracht
Mitte Mai 2015	39.082 problematische NSA-Selektoren; rund 68,7 Prozent gegen EU-Regierungsstellen [ref909, ref912]	Parlamentarisch/amtlich dokumentiert
2015/16	Cyberangriffe auf ukrainische Energieinfrastruktur [ref804, ref810]	Sandworm offiziell zugeschrieben
2016	NATO erkennt Cyberraum als Operationsdomäne an [ref1014, ref1017]	Offizielle NATO-Politik
Ende 2016	Reform des BND-Rechts [ref856, ref861]	Dokumentiert
16. Februar 2017	Merkel sagt vor dem NSA-Untersuchungsausschuss aus [ref858, ref908]	Dokumentiert
Juni 2017	NotPetya [ref775, ref804]	Destruktive Wirkung dokumentiert; GRU-Zuordnung stark gestützt
28. Juni 2017	Vorlage des Abschlussberichts des NSA-Ausschusses [ref910]	Dokumentiert
Februar 2018	Olympic Destroyer mit gefälschten technischen Artefakten [ref793, ref843, ref849]	Dokumentierter False-Flag-Mechanismus
2018	US-Doktrin „persistent engagement“/„defend forward“	Offiziell dokumentiert [ref958, ref999]

Jahr/Datum	Ereignis	Belegstatus
Oktober 2020	US-Anklage gegen sechs GRU-Offiziere der Einheit 74455 [ref773, ref824]	Anklage, keine Verurteilung
18. Mai 2022	Finnland und Schweden beantragen NATO-Mitgliedschaft [ref1051, ref1057]	Dokumentiert
August 2023	Gemeinsamer Bericht zu Infamous Chisel [ref803, ref851]	Technischer Bericht und staatliche Attribution
4. April 2023	Finnland wird NATO-Mitglied [ref1051, ref1059]	Dokumentiert
7. März 2024	Schweden wird NATO-Mitglied [ref1062, ref1063]	Dokumentiert
März 2025	Bericht über Pause offensiver US-Cyberoperationen gegen Russland [ref1000]	Journalistisch berichtet; operative Details nicht öffentlich

ANHANG B: CHECKLISTE FÜR BELASTBARE KÜNFTIGE ATTRIBUTIONEN

Technische Ebene

- Wurden Schadprogramm und Angriffspfad forensisch gesichert?
- Sind Hashwerte, Netzwerkspuren und Zeitabläufe reproduzierbar dokumentiert?
- Beruht die Attribution auf mehreren IOCs oder auf einem einzelnen auffälligen Merkmal?
- Wurde geprüft, ob Infrastruktur kompromittiert, angemietet oder gemeinsam genutzt war?
- Wurden Manipulationen von Zeitstempeln, Spracheinstellungen und Metadaten erwogen?
- Sind die TTP-Übereinstimmungen selten und langfristig stabil oder allgemein verbreitet?
- Gibt es operative Fehler, die virtuelle Identitäten mit realen Personen verbinden?

Organisationszuordnung

- Sind Gruppennamen verschiedener Anbieter sauber abgeglichen?
- Bestehen langfristige Infrastruktur-, Konten- oder Schlüsselüberschneidungen?
- Gibt es personenbezogene Verbindungen zu einer Organisation?
- Sind alternative Gruppen mit denselben Werkzeugen geprüft worden?

- Wird zwischen Entwickler, Infrastrukturbetreiber und eigentlichem Operator unterschieden?

Staatliche Zurechenbarkeit

- Handelte ein identifiziertes Staatsorgan?
- Gibt es Belege für Weisung, Leitung oder Kontrolle nichtstaatlicher Akteure?
- Reicht die Beweislage über bloßes staatliches Interesse oder Duldung hinaus?
- Werden kriminelle, dissidente und patriotische Akteure als getrennte Hypothesen behandelt?
- Ist klar, ob die Attribution technisch, politisch oder rechtlich gemeint ist?

Persönliche Befehlskette

- Gibt es spezifische Belege für Kenntnis, Billigung oder Anordnung durch politische Spitzen?
- Wird aus Organisationszugehörigkeit unzulässig auf einen Präsidentenbefehl geschlossen?
- Sind Behauptungen über Putin, den Kreml, Obama oder andere Regierungschefs als eigenständige Beweisstufe gekennzeichnet?
- Wird offen gesagt, wenn eine persönliche Befehlskette nicht öffentlich nachweisbar ist?

False-Flag-Prüfung

- Sind besonders offensichtliche „Fingerabdrücke“ unabhängig validiert?
- Weichen oberflächliche IOCs von tieferen TTPs ab?
- Gibt es Hinweise auf gefälschte Header, Sprachspuren oder Personas?
- Wird aus der Möglichkeit eines False Flags fälschlich auf sein Vorliegen geschlossen?
- Wurden Täuschungshypothesen mit positiven Belegen statt bloßem Misstrauen begründet?

Quellen- und Verfahrensqualität

- Handelt es sich um technische Rohdaten, eine Regierungsbehauptung, Anklage, Sanktion, journalistische Recherche oder ein Urteil?
- Ist eine Anklage ausdrücklich als Vorwurf gekennzeichnet?
- Sind staatliche Quellen durch unabhängige technische Forschung ergänzt?
- Teilen mehrere zitierte Stellen möglicherweise dieselbe geheime Ausgangsquelle?
- Wurden widersprechende Befunde veröffentlicht und behandelt?
- Gibt es einen Mechanismus zur Korrektur oder Revision der Attribution?

Rechts- und Folgenprüfung

- Handelt es sich um Spionage, Datenmanipulation, Sabotage oder physische Zerstörung?
- Welche tatsächlichen Wirkungen sind nachgewiesen?

- Wird politische Verurteilung von völkerrechtlicher Qualifikation getrennt?
- Sind Sanktionen, Strafverfolgung und Gegenmaßnahmen verhältnismäßig zur Beweislage?
- Werden für Verbündete und Gegner dieselben Kategorien und Beweisanforderungen verwendet?

Eine belastbare Attribution endet nicht mit der Feststellung, dass ein bestimmter Staat „wahrscheinlich“ verantwortlich sei. Sie benennt, **welche Stufe bewiesen oder plausibel ist, welche Quellen diesen Schluss tragen, welche Alternativen geprüft wurden und welche Lücken verbleiben**. Nur ein solcher abgestufter Ansatz kann zugleich Fehlattributionen begrenzen, staatliche Täuschung erschweren und Doppelstandards sichtbar machen.