

Risikoanalyse vulnerabler Betriebsmittel im elektrischen Übertragungs- und Verteilnetz am Beispiel Hamburg

Philipp Wagner¹, Kevin Alexander Winterfeld², Detlef Schulz
Professur für Elektrische Energiesysteme
Helmut-Schmidt-Universität / Universität der Bundeswehr Hamburg
Hamburg, Deutschland
¹philipp.wagner@hsu-hh.de, ²kevin.winterfeld@hsu-hh.de

Kurzfassung – Elektrische Übertragungs- und Verteilnetze zählen zur kritischen Infrastruktur (KRITIS). Ausfälle in diesen Netzen können, je nach betroffener Region, Schweregrad und Ausfalldauer, zu langanhaltenden Versorgungsunterbrechungen, massiven Störungen der öffentlichen Ordnung und erheblichen wirtschaftlichen sowie gesellschaftlichen Schäden führen. Vor dem Hintergrund zunehmender hybrider Bedrohungen ist ein wirksamer Schutz dieser Infrastrukturen ein zentrales Element staatlichen Risiko- und Krisenmanagements. Die vorliegende Studie führt eine Risikoanalyse für den Großraum Hamburg durch, um Betriebsmittel zu identifizieren, die durch gezielte physische Angriffe mit geringem technischen Aufwand – etwa Brandanschläge, Vandalismus oder mechanische Beschädigungen – erheblich gestört oder außer Betrieb gesetzt werden können. Die Analyse zeigt, dass öffentlich zugängliche Quellen (Open-Source Intelligence, OSINT) ausreichen, um kritische Schwachstellen zu lokalisieren und potenzielle Ziele zu identifizieren. Zur Bewertung der Bedrohungslage wurde eine Matrix entwickelt, welche den erforderlichen Aufwand sowie die potenziellen Auswirkungen verschiedener Angriffsszenarien systematisch gegenüberstellt. Darauf aufbauend werden Schutzmaßnahmen vorgeschlagen, die in Feldversuchen validiert wurden. Besonders exponiert und angreifbar zeigen sich dabei Freileitungen sowie Umspann- und Umschaltwerke als zentrale Knotenpunkte der Netzinfrastruktur.

Stichworte – Risikomanagement, Risikoanalyse, Hybride Bedrohung, Terrorismus, Sabotage, Übertragungsnetz, Verteilnetz, Umspannwerke, Freileitungen, Open-Source, Bevölkerungsschutz

NOMENKLATUR

ATP	Army Techniques Publication
BSI	Bundesamt für Sicherheit in der Informationstechnik
CaaS	Crime as a Service
CCaaS	Cyber Crime as a Service
IEC	International Electrotechnical Commission
IT	Informationstechnologie
KRITIS	Kritische Infrastrukturen
MDCOA	Most Dangerous Course of Action
MLCOA	Most Likely Course of Action

n-1	Netzsicherheitskriterium „n minus 1“ (Ausfall eines Betriebsmittels ohne Versorgungsverlust)
OSINT	Open Source Intelligence
PSA	Persönliche Schutzausrüstung
THD	Total Harmonic Distortion (Gesamte harmonische Verzerrung)
UBA	Umweltbundesamt
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e. V.
VIK	Verband der Industriellen Energie- und Kraftwirtschaft e. V.

I. EINLEITUNG

Elektrische Übertragungs- und Verteilnetze (ÜN bzw. VN) sind elementare Bestandteile der kritischen Infrastruktur (KRITIS)[1]. Die Funktionsfähigkeit ist grundlegend für die Versorgungssicherheit, die öffentliche Ordnung sowie das wirtschaftliche und gesellschaftliche Leben. Ausfälle – ob technisch bedingt oder vorsätzlich herbeigeführt – können Versorgungsengpässe, Panik Beeinträchtigungen sicherheitsrelevanter Systeme und langfristige Folgewirkungen für das Gemeinwesen bedingen [2].

Zahlreiche Studien und politische Initiativen betonen inzwischen die Bedeutung resilienter Energiesysteme. So formuliert etwa die Deutsche Akademie der Technikwissenschaften (acatech) in ihrer Stellungnahme übergeordnete Maßnahmen zur Erhöhung der Systemresilienz, wie Monitoring, Redundanz und Dezentralität [3]. Diese bleiben jedoch häufig auf einer abstrakten oder systemweiten Ebene – spezifische Verwundbarkeiten einzelner Betriebsmittel auf regionaler Ebene werden dort nur am Rande betrachtet. Die vorliegende Studie adressiert diese Lücke und fokussiert sich explizit auf die gezielte Gefährdung elektrischer Infrastruktur durch mutwillige physische Eingriffe im Raum Hamburg. Frühere Untersuchungen – wie etwa das Forschungsprojekt KritisKat (TH Köln) oder die regionalen KRITIS-Analysen des LfV Hamburg – konzentrierten sich vorrangig auf sektorübergreifende Schutzbedarfe oder übergeordnete Risikoszenarien. Eine systematische Bewertung verwundbarer Betriebsmittel (wie Freileitungen oder Umspannwerke) im Kontext lokaler Angriffsszenarien mit

geringen Einstiegshürden blieb bislang weitgehend aus. Ziel dieser Arbeit ist daher die Entwicklung eines praxistauglichen Ansatzes zur Identifikation besonders vulnerabler Elemente der elektrischen Energieversorgung im urbanen Raum. Darüber hinaus wird eine strukturierte Bewertung der Bedrohungslage vorgenommen, indem dokumentierte Anschläge auf elektrische Infrastrukturen seit den 1960er Jahren systematisch ausgewertet und typologisiert werden. Diese Rückschau ermöglicht es, reale Angriffsmuster, Motivlagen und technische Vorgehensweisen einzuordnen sowie typische Zielobjekte zu identifizieren. Die Analyse bildet die Grundlage, um realistische Szenarien für urbane Räume wie Hamburg zu entwickeln und deren potenzielle Gefährdung sachgerecht abzuschätzen. Im Fokus stehen dabei gezielte physische Eingriffe wie Brandstiftung, Vandalismus oder mechanische Sabotageakte, die mit geringem Aufwand erhebliche Folgen auslösen können. Derartige niedrigschwellige Angriffsformen lassen sich mit einfachsten Mitteln realisieren, erfordern keine besondere Expertise und können dennoch großflächige Versorgungsausfälle verursachen. Dabei wird aufgezeigt, dass selbst öffentlich verfügbare Informationen (OSINT) genügen, um potenzielle Schwachstellen zu identifizieren und anzugreifen. Eine zentrale methodische Komponente der Untersuchung stellt die Entwicklung einer Risiko-Matrix dar. Aufbauend auf der Identifikation konkreter Bedrohungsszenarien werden Aufwand, Eintrittswahrscheinlichkeit und Auswirkungen möglicher physischer Angriffe auf unterschiedliche Betriebsmittel systematisch bewertet. Die Kriterienauswahl, Skalierung und Gewichtung orientieren sich dabei an einschlägigen Sicherheitsanalysen sowie an Experteneinschätzungen. Die Matrix dient nicht nur der Risikoquantifizierung, sondern auch der vergleichenden Bewertung typischer Angriffsformen und Zielobjekte. Sie verknüpft damit erstmals in konsistenter Weise die strukturellen Schwächen mit realen Gefährdungslagen. Auf Basis dieser Bewertung werden konkrete technische und organisatorische Schutzmaßnahmen abgeleitet und hinsichtlich ihrer Wirksamkeit analysiert. Die daraus abgeleiteten Schutzmaßnahmen werden sowohl technisch als auch organisatorisch differenziert dargestellt. Neben allgemeinen Ansätzen zur Risikominderung – etwa in den Bereichen Überwachung, Redundanz oder Zugangssicherung – werden auch objektspezifische Maßnahmen für besonders exponierte Betriebsmittel erarbeitet. Dabei erfolgt eine strukturierte Ableitung entlang der zuvor definierten Angriffsvektoren, um die Wirksamkeit der Maßnahmen im jeweiligen Szenariokontext nachvollziehbar bewerten zu können. Durch die exemplarische Analyse des Hamburger Netzes können nicht nur lokale Schwachstellen aufgezeigt, sondern auch übertragbare Handlungsempfehlungen für vergleichbare urbane Versorgungsräume formuliert werden. Die Studie gliedert sich wie folgt: Zunächst werden grundlegende Definitionen, rechtliche Rahmenbedingungen und Anforderungen an die Energieinfrastruktur erörtert (Kapitel II). Danach werden typische Fehlerursachen, Schwachstellen sowie Zielbetriebsmittel identifiziert (Kapitel III und IV). Im Anschluss erfolgt die Bewertung mittels Risiko-Matrix (Kapitel V). Abschließend werden mögliche Gegenmaßnahmen abgeleitet und zusammenfassend diskutiert (Kapitel VI). Letztlich wird Kapitel VII ein Ausblick gegeben.

II. KRITISCHE INFRASTRUKTUR – RAHMEN UND RELEVANZ FÜR DIE ENERGIEVERSORGUNG

Kritische Infrastrukturen (KRITIS) sind Einrichtungen, deren Ausfall gravierende Auswirkungen auf die öffentliche Sicherheit, das Gemeinwesen und die Wirtschaft hätte. Die Stromversorgung gehört dabei zu den zentralen Sektoren – sowohl auf nationaler als auch internationaler Ebene. Entsprechende Definitionen und Anforderungen finden sich unter anderem im BSI-Gesetz (§ 2 Abs. 10), der EU-Richtlinie 2022/2557 zur Resilienz kritischer Einrichtungen sowie im NATO Strategic Concept 2022. Gemeinsam ist diesen Regelwerken der Fokus auf systemische Risiken, die sich aus Naturkatastrophen, Cyberbedrohungen oder hybriden Angriffen ergeben können. Diese Arbeit fokussiert sich jedoch nicht auf die allgemeine Systemresilienz, sondern auf die gezielte Gefährdung technischer Betriebsmittel innerhalb der elektrischen Energieinfrastruktur im urbanen Raum – insbesondere durch physische, mutwillige Eingriffe mit niedrigem Aufwand. Ziel ist es, technische Schwachstellen auf der Ebene konkreter Komponenten zu identifizieren und geeignete Schutzmaßnahmen für besonders gefährdete Elemente zu entwickeln.

A. Struktur und Schutzbedarf der Strominfrastruktur

Das elektrische Energieversorgungssystem in Deutschland basiert auf einer mehrstufigen Netzstruktur, die sich aus Übertragungsnetzen (Spannungsebene > 110 kV) und Verteilnetzen (≤ 110 kV) zusammensetzt. Die Übertragungsnetzbetreiber (ÜNB) – darunter TenneT, 50Hertz, Amprion und TransnetBW – sind für die großräumige Netzstabilität, den Netzwiederaufbau sowie den internationalen Energieaustausch verantwortlich. Verteilnetzbetreiber (VNB) gewährleisten hingegen die flächendeckende Versorgung von Industrie, Gewerbe und Privathaushalten. Diese Unterscheidung ist essenziell für die Bewertung kritischer Schwachstellen, da die Angriffsflächen, Redundanzkonzepte und bauliche Schutzmaßnahmen je nach Netzebene stark variieren. In beiden Ebenen finden sich jedoch kritische Betriebsmittel, deren Ausfall unmittelbare Auswirkungen auf die Versorgungssicherheit haben kann. Besonders verwundbar sind Freileitungsmasten, Umspannwerke, Schaltanlagen, Transformatorenstationen sowie Kabeltrassen, da sie meist oberirdisch verlaufen, weitflächig verteilt sind und häufig ohne physische Abschirmung betrieben werden. Die Gefährdung dieser essentiellen Infrastrukturelemente beschränkt sich dabei nicht auf klassische Risiken wie Extremwetter oder Materialermüdung. In zunehmendem Maße sind auch gezielte physische Eingriffe wie Brandstiftung, Vandalismus, Metalldiebstahl oder Sabotage zu verzeichnen. Diese Angriffe erfordern oft nur geringe Mittel und lassen sich – insbesondere bei fehlender Redundanz – mit hoher Wirkung auf die Versorgung ausüben. Die damit verbundenen Risiken betreffen nicht nur die technische Funktionalität der Netze, sondern auch die öffentliche Sicherheit und Ordnung, insbesondere im städtischen Kontext. Vor diesem Hintergrund gewinnt die systematische Identifikation kritischer Schwachstellen auf Netz- und Betriebsmittelniveau an Bedeutung. Sie bildet die Grundlage für präventive Schutzmaßnahmen sowie für eine risikobasierte Auslegung zukünftiger Netzstrukturen.

B. Rechtliche und technische Anforderungen

Ein zentrales technisches Prinzip zur Sicherung der Stromversorgung ist das sogenannte n-1-Kriterium: Es verlangt, dass der Ausfall einer einzelnen Systemkomponente (z. B. Leitung, Transformator) nicht zur Netzinstabilität führen darf [4]. Dieses Prinzip ist in der VDE-Anwendungsregel VDE-AR-N 4121 sowie im Transmission Code verankert und bildet die Grundlage für die Netzplanung im Übertragungsnetz. Ergänzend fordert das Energiewirtschaftsgesetz (EnWG) (§ 19) von Netzbetreibern [5] den Nachweis geeigneter Maßnahmen zur Sicherstellung der Netzstabilität. Doch selbst bei Einhaltung technischer Kriterien und regulatorischer Standards bleibt die Frage offen, inwieweit die physische Sicherheit einzelner Betriebsmittel gewährleistet ist – insbesondere im urbanen Raum, wo dichte Bebauung, eingeschränkter Zugang und eine Vielzahl potenzieller Angriffsflächen zusammentreffen.

C. Verwundbarkeit als Forschungsschwerpunkt

Die vorliegende Untersuchung konzentriert sich auf die physische Verwundbarkeit ausgewählter Betriebsmittel im elektrischen Übertragungs- und Verteilnetz – mit dem Ziel, konkrete Bedrohungsszenarien systematisch zu analysieren und deren Auswirkungen qualitativ zu bewerten. Im Zentrum steht dabei nicht das Stromsystem als Ganzes, sondern die gezielte Betrachtung operativer Schwachstellen einzelner technischer Komponenten wie Freileitungsmasten, Kabelübergängen und Umspannwerken. Diese Fokussierung stellt ein methodisches Alleinstellungsmerkmal dar: Während sich bestehende KRITIS-Analysen und nationale Strategien wie die acatech-Stellungnahme „Das Energiesystem resilient gestalten“ primär mit übergreifenden Resilienzstrategien, Digitalisierung oder Dezentralisierung befassen, bleiben konkrete Untersuchungen zur physischen Verwundbarkeit netztechnischer Infrastruktur bislang unterrepräsentiert [1, 3].

Ziel dieses Beitrags ist es daher, physisch angreifbare Betriebsmittel systematisch hinsichtlich ihrer Anfälligkeit für niederschwellige Sabotageakte zu untersuchen – insbesondere solche, die mit einfachen Mitteln, geringem Aufwand und ohne Spezialwissen durchführbar sind. Dabei werden exemplarisch realitätsnahe Szenarien entwickelt und im städtischen Raum Hamburg verortet. Die Analyse berücksichtigt nicht nur technische und örtliche Merkmale der Betriebsmittel, sondern auch deren mögliche systemische Relevanz im Netzverbund. Zur Identifikation potenziell verwundbarer Infrastrukturelemente greift die Untersuchung auf Open-Source-Informationsquellen (OSINT) zurück.

Fokus der Untersuchung

Die vorliegende Untersuchung analysiert die physische Verwundbarkeit technischer Betriebsmittel im elektrischen Übertragungs- und Verteilnetz – exemplarisch am Beispiel Hamburg. Im Mittelpunkt stehen reale, niederschwellige Angriffsszenarien auf Freileitungsmasten, Kabelübergänge und Umspannwerke, wie sie mit einfachen Mitteln durchführbar wären. Die Identifikation verwundbarer Infrastrukturelemente erfolgt systematisch auf Basis öffentlich zugänglicher Datenquellen (OSINT). Ziel ist eine praxisnahe Risikoabschätzung, die bestehende KRITIS-Strategien um operative Perspektiven ergänzt und konkrete Schutzmaßnahmen ableitbar macht.

Dazu zählen öffentlich zugängliche Kartenportale, Luftbild- und Satellitendaten, Bauausschreibungen, Planfeststellungsunterlagen, technische Berichte von Netzbetreibern, Unternehmensdatenbanken sowie Umwelt- und Genehmigungsdokumente.

Diese methodisch systematisierte OSINT-Nutzung erlaubt es, technische Eigenschaften, Zugänglichkeit und Netzrelevanz einzelner Komponenten mit vertretbarem Aufwand zu erfassen und bewertbar zu machen. Der vorliegende Beitrag evaluiert diese Methodik exemplarisch am Fallbeispiel Hamburg und überprüft die Aussagekraft öffentlich verfügbarer Datenquellen hinsichtlich der Erkennung infrastruktureller Schwachstellen. Insgesamt zielt dieser Abschnitt darauf ab, den methodischen Kern der Untersuchung zu definieren: die gezielte Identifikation operativ verwundbarer Betriebsmittel unter Verwendung frei verfügbarer Informationen – als Beitrag zur praxisnahen Sicherheitsanalyse kritischer Infrastruktur auf lokaler Ebene. Die normative und strategische Bedeutung dieser Betrachtung, insbesondere mit Blick auf mögliche Kaskadeneffekte in urbanen Verdichtungsräumen, wird in der Einleitung eingeordnet.

III. ANFÄLLIGKEITEN ELEKTRISCHER BETRIEBSMITTEL UND RELEVANTE FEHLERURSACHEN

Elektrische Betriebsmittel im Übertragungs- und Verteilnetz – insbesondere Freileitungsmasten, Kabelübergänge und Umspannstationen – sind technischen, organisatorischen und zunehmend sicherheitsrelevanten Risiken ausgesetzt. Die Ursachen für Fehlfunktionen oder Ausfälle lassen sich dabei in zwei grundlegende Kategorien einteilen: unbeabsichtigte Störungen (z. B. durch Defekte, Bedienfehler oder Umwelteinflüsse) und vorsätzliche schädigende Eingriffe (z. B. durch Sabotage oder kriminelle Akte). Diese Fehlerquellen wirken sich auf unterschiedliche Weise auf die Verwundbarkeit einzelner Betriebsmittel aus – sei es durch schleichenden Verschleiß, plötzliche Überlastung oder gezielte physische Angriffe. Um diese Verwundbarkeiten systematisch zu analysieren, werden im Folgenden die häufigsten Fehlerursachen beschrieben und durch eine Auswertung dokumentierter Anschläge auf europäische Energieinfrastruktur ergänzt. Ziel ist es, typisierte Bedrohungsmuster zu erkennen und ihre Relevanz für konkrete Betriebsmittel im Stromnetz zu identifizieren.

A. Technische Fehler/ Fehlbedienung

Unbeabsichtigte Ausfälle entstehen häufig durch technische Defekte (z. B. Materialermüdung, Fertigungsfehler, Alterung) oder durch menschliches Fehlverhalten (z. B. Fehlbedienung, Zeitdruck, unklare Zuständigkeiten). Besonders anfällig sind dabei komplexe, stark vernetzte Systeme wie Umspannstationen oder zentrale Schaltanlagen. Ein vermeintlich lokales Problem – etwa eine falsch gesetzte Schaltfolge – kann dabei kaskadierende Effekte bis in übergeordnete Netzebenen auslösen. Diese Art von Verwundbarkeit wird unter anderem von Charles Perrow in seiner Theorie „Normal Accidents“ beschrieben [6]. In hochkomplexen Systemen seien Fehler letztlich unvermeidbar, da Wechselwirkungen nicht vollständig antizipierbar seien. Diese strukturelle Systemanfälligkeit stellt jedoch nicht den Hauptfokus dieser Arbeit dar. Die folgenden Abschnitte konzentrieren sich daher auf gezielte Eingriffe mit Schadensabsicht.

B. Mutwilliger schädigender Eingriff

Mutwillige Eingriffe stellen eine eigenständige Gefährdungskategorie dar. Im Gegensatz zu zufälligen Ausfällen zielen sie bewusst auf die Beeinträchtigung oder Zerstörung einzelner Betriebsmittel ab [7]. Diese Form der Verwundbarkeit ist insbesondere für exponierte Netzkomponenten wie Freileitungsmasten, Übergabepunkte oder unbewachte Stationen hoch relevant. Die Motivation hinter diesen Angriffen lässt sich dabei in zwei Hauptgruppen einteilen:

a) Politisch motivierte Angriffe

Politisch motivierter Kriminalität werden Straftaten zugeordnet, welche den demokratischen Willensbildungsprozess beeinflussen, dem Erreichen politische Ziele dienen oder diese verhindern sollen, sich gegen Wesensmerkmale der demokratischen Grundordnung richten oder auswärtige Belange der Bundesrepublik Deutschland gefährden beziehungsweise darauf abzielen [8]. Die öffentliche Sicherheit und damit einhergehend KRITIS ist in Deutschland insbesondere aufgrund von Terrorismus und organisierter Kriminalität gefährdet [9]. Politisch oder ideologisch motivierte Straftaten stellen für KRITIS unter dem Gefahrenkomplex „mutwilliger schädigender Eingriff“ die größte Gefährdung dar [9].

b) Wirtschaftlich motivierte Angriffe – Crime-as-a-Service (CaaS)

CaaS bezeichnet das Anbieten von kriminellen Handlungen als erwerbbarer Dienstleistung im Sinne eines Geschäftsmodells innerhalb der organisierten Kriminalität [10]. Insbesondere im Bereich Cyberkriminalität, bezeichnet als Cyber-Crime-as-a-Service (CCaaS), ist das Auslagern von einzelnen Schritten oder Bestandteilen eines Cyberangriffs an darauf spezialisierte Gruppierungen gegen Bezahlung etabliert [10]. Crime-as-a-service wird besonders durch darauf spezialisierte Plattformen im Dark-Net verbreitet, wodurch die jeweilige Dienstleistung einer Vielzahl an Gruppierungen zugänglich ist und auf Fähigkeiten und Ressourcen zurückgegriffen werden kann, welche zuvor oftmals nicht verfügbar waren [11]. Gemäß Europol erhöht dies das Risiko der Verschmelzung von organisiertem Verbrechen und Terrorismus erheblich [11].

C. Rückblick: Dokumentierte physische Anschläge auf Energieinfrastruktur

Um Ableitungen für vulnerable Punkte im Hamburger Stromnetz treffen zu können, wurden bekanntgewordene beziehungsweise durch Medien veröffentlichte Angriffe auf Stromnetze und damit verbundene Infrastruktur in Europa rückblickend bis 1961 analysiert. Betrachtet wurden ausschließlich „erfolgreiche“ Angriffe, welche zu einem realen Schadensbild durch Versorgungsausfälle oder Schäden an Stromnetzen führten und eine Instandsetzung erforderten. Nicht medial veröffentlichte, jedoch den Autoren bekannte Vorfälle wurden nicht in die Analyse einbezogen. Die Anschläge wurden unterteilt in Cyberangriffe sowie physische Angriffe und weiter untergliedert nach staatlichen Akteuren sowie nicht staatlichen Akteuren. Cyberangriffe, welche zu keiner physischen Beeinträchtigung der Stromnetze führten, wurden als nicht-„erfolgreich“ bewertet und nicht weiter betrachtet, wenngleich von einem wirtschaftlichen Schaden ausgegangen werden muss. Besonders herauszustellen sind 13

in TABELLE 1 aufgeführte Anschläge und Anschlagsserien im Zeitraum 1961 – 2024 in Europa.

TABELLE 1 ANSCHLÄGE AUF STROMNETZE IN EUROPA

2024	Russischer Öltanker zerstört mittels Anker EstLink2 HGÜ Seekabel zwischen Finnland und Estland [12]
2024	Linksextreme Gruppierung Vulkangruppe verübt Brandanschlag auf 110kV Kabelendmast bei Tesla Werk nahe Berlin [13]
2023	Unbekannte Täter zerstören 110 kV Freileitungsmast durch Sägen, welcher Tagebau und Wasserwerk bei Grevenbroich versorgt [14]
2021	Linksextremisten verüben Brandanschlag auf durch Bauarbeiten geöffneten Mittelspannungskabelkanal, gerichtet gegen Rüstungsindustrie in München [15]
2020	Unbekannte Täter zerstören Hochspannungsmast durch Sägen bei Gland (Schweiz) [16]
2016	Unbekannte Täter zerstören 110 kV Freileitungsmast durch Sägen, welcher den Tagebau Inden versorgt [17]
2016	Identifizierter Einzeltäter zerstört 10 Freileitungsmasten durch Sägen in der Steiermark (Österreich) [18]
2015	Mutmaßlich staatliche russische Hacker sabotieren Stromnetz der Ukraine und verursachen Stromausfälle und teilweise Stromausfälle in fast 200 Städten [19]
1995	Unbekannte Täter zerstören 380 kV und 110 kV Freileitungsmasten durch Sägen in Brandenburg [20]
1986	Kernkraftgegner verüben bundesweit über 80 Anschläge durch Zerstörung von Hochspannungsmasten mittels Sägen oder Sprengstoff [21]
1982	Kernkraftgegner feuert 5 Gefechtsköpfe mittels Panzerabwehrhandwaffe RPG-7 auf im Bau befindliches Kernkraftwerk in Frankreich ab [22]
1979	Kernkraftgegner sprengt Meteomast für meteorologische Kontrollmessung, sodass dieser 400 kV Umspann- und -schaltwerk bei AKW Gösgen (Schweiz) beschädigt [23]
1961	Separatisten zerstören 37 Strommasten durch Sprengen in Südtirol (Italien) [24]

Mutmaßlich staatlichen Akteuren sind 2 der 13 Anschläge oder Anschlagsserien, darunter der einzige Cyberangriff, zuzuschreiben. Die Sabotage von EstLink2 wurde durch einen physischen Eingriff durchgeführt. 11 der 13 Anschläge wurden durch nicht-staatliche Akteure begangen. Hiervon sind 7 von 11 Anschlägen dem linksextremistischen Spektrum oder militanten Umweltaktivisten zuzuordnen. 1 der 11 Anschläge ist Separatisten und 3 von 11 Anschlägen Unbekannt zuzuordnen. Während staatliche Akteure aus dem Ausland oder im Grenzraum auf See agieren, wurden die Anschläge nicht staatlicher Akteure im Inland vor Ort ausgeführt. Die absolute Mehrheit der Anschläge richtete sich hierbei gegen Freileitungsmasten. Ausgeführt wurden die meisten Anschläge durch Vorgehensweisen, welche mit

einem sehr niedrigen Aufwand verbunden sind, wie Sägen, zum Beispiel mittels Akku-Flex, und Brandanschlägen. Zur besseren Einordnung wurden die beobachteten Angriffsmuster nach Art der Durchführung, Motivation und Wirkmechanismus strukturiert. Die betrachteten Maßnahmen lassen sich dabei drei übergeordneten Angriffsformen zuordnen:

1. **Physisch-direkte Eingriffe vor Ort:** Dazu zählen u. a. das Sägen von Freileitungsmasten, Brandanschläge auf ungeschützte Betriebsmittel sowie Vandalismus an exponierten Einrichtungen. Diese Methoden sind technisch niedrigschwellig, erfordern kaum spezielles Know-how oder Ressourcen und zielen auf die Zerstörung von Trag- und Übertragungskomponenten. Ihre Häufigkeit und Erfolgsquote – wie die Fallzahlen in Tabelle 1 zeigen – unterstreichen ihre praktische Relevanz.
2. **Fern- oder indirekt gesteuerte Angriffe:** Diese Kategorie umfasst Cyberangriffe sowie operationelle Angriffe mit technischer Unterstützung, etwa durch Drohnen oder manipulierte Steuerkomponenten. Während Cyberangriffe eher auf Steuerungssysteme und Dateninfrastruktur zielen, ermöglichen Drohnen erstmals einen physischen Zugang zu geschützten Anlagen, ohne räumliche Präsenz des Täters.
3. **Staatlich oder organisatorisch koordinierte Angriffe:** Diese Angriffsform ist seltener, aber potenziell weitreichender. Sie umfasst gezielte Sabotage durch spezialisierte Einheiten oder nachrichtendienstliche Operationen, etwa durch Störungen in Seekabeln oder Verdeckte Operationen im Grenzbereich.

Im weiteren Verlauf der Arbeit werden diese Angriffsformen exemplarisch auf relevante Betriebsmittel projiziert, um typische Angriffsvektoren in ihrer Kombination aus Aufwand, Zugang, Zerstörungspotenzial und Auswirkung auf das Gesamtsystem zu bewerten. Damit erfolgt eine sachlich fundierte Abgrenzung, welche Maßnahmen im Kontext dieser Studie betrachtet werden – und welche bewusst ausgeschlossen bleiben.

IV. SCHWACHSTELLEN IDENTIFIZIEREN BSP HH ENERGIEVERSORGUNG

Für die weitere Analyse wird zunächst der Standort Hamburg charakterisiert und herausgestellt, weshalb sich die Freie und Hansestadt Hamburg als besonders vulnerables Ziel von staatlichen und nicht staatlichen Akteuren darstellt. Im Weiteren werden historische Anschläge auf Strominfrastruktur und deren Vorgehen beleuchtet, um diese dann mittels Open-Source Informationsquellen auf das Hamburger Stromnetz zu übertragen.

A. Hamburg als kritischer urbaner Standort mit systemischer Relevanz für die Stromversorgung

Die Auswahl der Freien und Hansestadt Hamburg als Untersuchungsregion erfolgt nicht willkürlich, sondern basiert auf einer Kombination aus wirtschaftlicher Bedeutung, netztechnischer Relevanz und der Verfügbarkeit offen zugänglicher Informationen. Hamburg weist als Stadtstaat mit industriellem und logistischem Schwerpunkt, dichter Infrastrukturanbindung und hohem Anteil kritischer Einrichtungen eine überdurchschnittliche Vulnerabilität gegenüber gezielten Eingriffen in die Stromversorgung auf.

Zugleich erlaubt die klare Abgrenzung des Stadtraums und die hohe Datenverfügbarkeit eine modellhafte Fallstudie, deren Ergebnisse methodisch auf andere urbane Versorgungsräume

in Deutschland übertragbar sind. Die nachfolgende Analyse dient somit der exemplarischen Identifikation von Schwachstellen in elektrischen Verteil- und Übertragungsnetzen im urbanen Kontext und liefert übertragbare Erkenntnisse zur Gefährdungsabschätzung und Schutzplanung.

Das Stromnetz der Freien und Hansestadt Hamburg als Stadtstaat stellt sowohl für staatliche als auch nicht-staatliche Akteure innerhalb der Bundesrepublik ein mögliches Ziel dar, um deutschlandweit Schaden anzurichten. Dies begründet sich durch die geographische Lage und die daraus abgeleitete Infrastruktur wie den Hafen sowie Binnengewässerschifffahrt, die wirtschaftliche Struktur und den hohen Grad an Verflechtung aufgrund des Status als Im- und Export-Drehscheibe.

Hamburg verfügt über eine Ost-West sowie Nord-Süd-Ausdehnung von jeweils rund 40 km gelegen an der Unterelbe in Norddeutschland. Die Elbe ermöglicht den Zugang zur Nordsee sowie den Gütertransport über die Binnenschifffahrt und verbindet damit die jeweiligen Wirtschaftszentren von Tschechien, Sachsen, Sachsen-Anhalt, Niedersachsen, Brandenburg und Berlin Richtung Norden zum Hamburger Hafen [25]. Durch Anbindung an das Binnenwasserstraßennetz auf Höhe Lauenburg und Magdeburg ist auch ein weiterer Transport nach Westen möglich [25]. Der Hafen Hamburg ist Deutschlands größter Universalhafen und drittgrößte Hafen nach Containerumschlag in der Europäischen Union mit einem Seegüterumschlag von 114,3Mio t und 7,7Mio TEU im Jahr 2023 [26]. Über die Binnenschifffahrt wurden am Hafen Hamburg 2023 123000 TEU Güter transportiert [26]. Importiert werden am Hafen Hamburg als Universalhafen alle Güter der Erzeugungskette. Dies umfasst sowohl Energieträger und Rohstoffe als auch Halbzeug, Maschinen, Chemikalien, pharmazeutische Produkte, Konsumgüter und Lebensmittel. Durch Art und Menge der Güter ist das Hafen Hamburg auf Bundesebene mit seinem Terminal Tollerart als KRITIS eingestuft [27].

Hamburg ist Produktions- und/oder Entwicklungsstandort für eine Vielzahl an Rüstungsunternehmen und Unternehmen, welche anteilig Rüstungsunternehmen beliefern oder Dual-Use-Produkte herstellen sowie durch den Hafen selbst Umschlagplatz für Rüstungsgüter [28–30].

Darüber hinaus ist Hamburg neben München, Berlin und Frankfurt ein zentraler Standort für Rechenzentren gem. ABBILDUNG 1 und verfügt über eine chemische Industrie, welche 9,1 % des Umsatzes der chemischen Industrie Deutschlands erwirtschaftet [31]. Weitere Cluster umfassen die Luftfahrtbranche, Lebensmittelchemie und Pharmaunternehmen, Maschinenbau sowie die im Zusammenhang mit dem Hafen bestehende Logistikbranche, welche den Transport von Gütern aber auch deren Lagerung durch Lebensmittelkühlhäuser umfasst und inländischer Ausgangspunkte für zahlreiche Logistikketten ist [31]. Hamburg ist mangels ausreichender eigener Stromerzeugung auf Stromimporte über die drei 380 kV Netzanschlusspunkte Hamburg-Nord, Hamburg-Ost und Hamburg-Süd angewiesen

da der Leistungsbedarf nicht allein in Hamurg bereitgestellt werden kann, gem. ABBILDUNG 2.

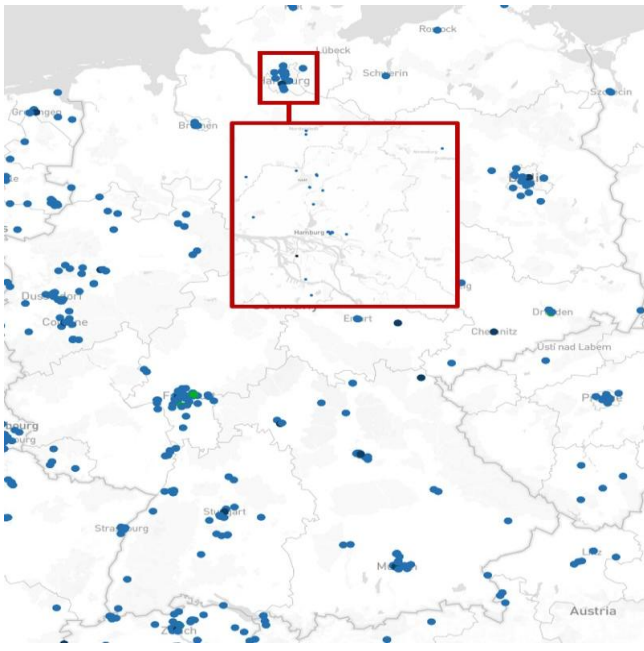


ABBILDUNG 1: RECHENZENTREN IN DEUTSCHLAND. VERGRÖßERTER AUSSCHNITT: HAMBURG [32]

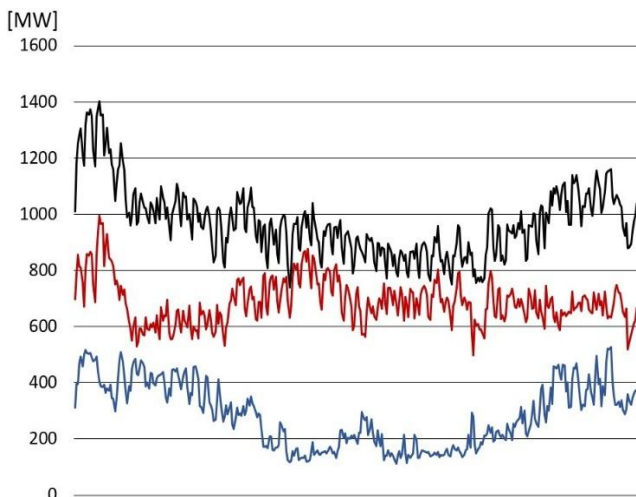


ABBILDUNG 2: TÄGLICHE STROMBILANZ HAMBURG 2024, BLAU: STROM ERZEUGT IN HAMBURG, ROT: STROMIMPORTE NACH HAMBURG, SCHWARZ: LAST IN HAMBURG [33]

Die weitere Distribution erfolgt über das städtisch geprägte Verteilnetz der Hamburger Energienetze GmbH. Um die Resilienz im Falle eines Stromausfalles zu erhöhen, wurde mit dem Bau des schwarzstartfähigen Gas- und Turbinenkraftwerks (GuD) Dradenau mit einer elektrischen Leistung von 180 MW begonnen, mit dessen Fertigstellung Ende 2025 gerechnet wird [34, 35]. Die wichtigsten Betriebsmittel werden in ABBILDUNG 4 geografisch eingeordnet.

B. Identifizierung von Zielbetriebsmitteln des Stromnetzes in Hamburg

Ziel dieses Kapitels ist es, im Kontext der für Hamburg dokumentierten KRITIS-Strukturen jene elektrischen

Betriebsmittel zu identifizieren, die im Fall eines gezielten Angriffs besonders relevant wären. Grundlage ist eine systematische Ableitung aus öffentlich zugänglichen Quellen (OSINT) sowie eine räumliche und funktionale Verknüpfung zu kritischen Abnehmern und Systemen. Die anschließende Szenarienbildung erfolgt in Anlehnung an militärische Methoden der Gefahrenprognose und dient der Bewertung potenzieller Angriffsformen und -folgen.

1) Methodisches Vorgehen zur Identifikation möglicher Zielbetriebsmittel

1. Auswahl elektrischer Betriebsmittel mit hohem Angriffspotenzial

Mithilfe öffentlich zugänglicher Plattformen wie flosm.org und Google Maps wurden zunächst alle relevanten Betriebsmittel im Raum Hamburg identifiziert, die aufgrund ihrer physischen Exponiertheit, Zugänglichkeit und energietechnischen Bedeutung potenzielle Angriffspunkte darstellen. Dazu zählen:

- Umspannwerke
- Umschaltwerke
- Kabelendmasten (110 kV)

Freileitungsmasten wurden – in Ergänzung zu Abschnitt III.C – als besonders kritisch berücksichtigt, da ihre Zerstörung direkt zur Unterbrechung mehrerer Leitersysteme führen kann. Insgesamt wurden **37 relevante Betriebsmittel** identifiziert (vgl. ABBILDUNG 4).

2. Kartierung kritischer Abnehmerstrukturen im Stadtgebiet

In einem zweiten Schritt wurden bekannte Standorte kritischer Infrastrukturen (KRITIS) in Hamburg kartiert – darunter Krankenhäuser, Wasserwerke, Rechenzentren, Verkehrsknotenpunkte, Lebensmittelversorger, industrielle Großverbraucher sowie der Flughafen und das Hafenterminal (vgl. ABBILDUNG 3.). Ziel war es, mögliche Angriffswirkungen auf diese Strukturen durch Netzkomponenten in räumlicher Nähe abzuleiten.

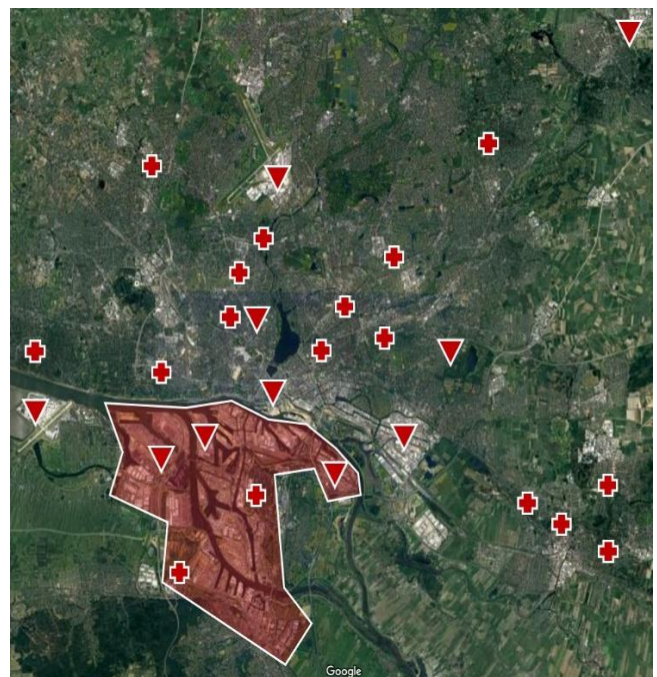


ABBILDUNG 3: STANDORTE KRITISCHER INFRASTRUKTUR HAMBURG

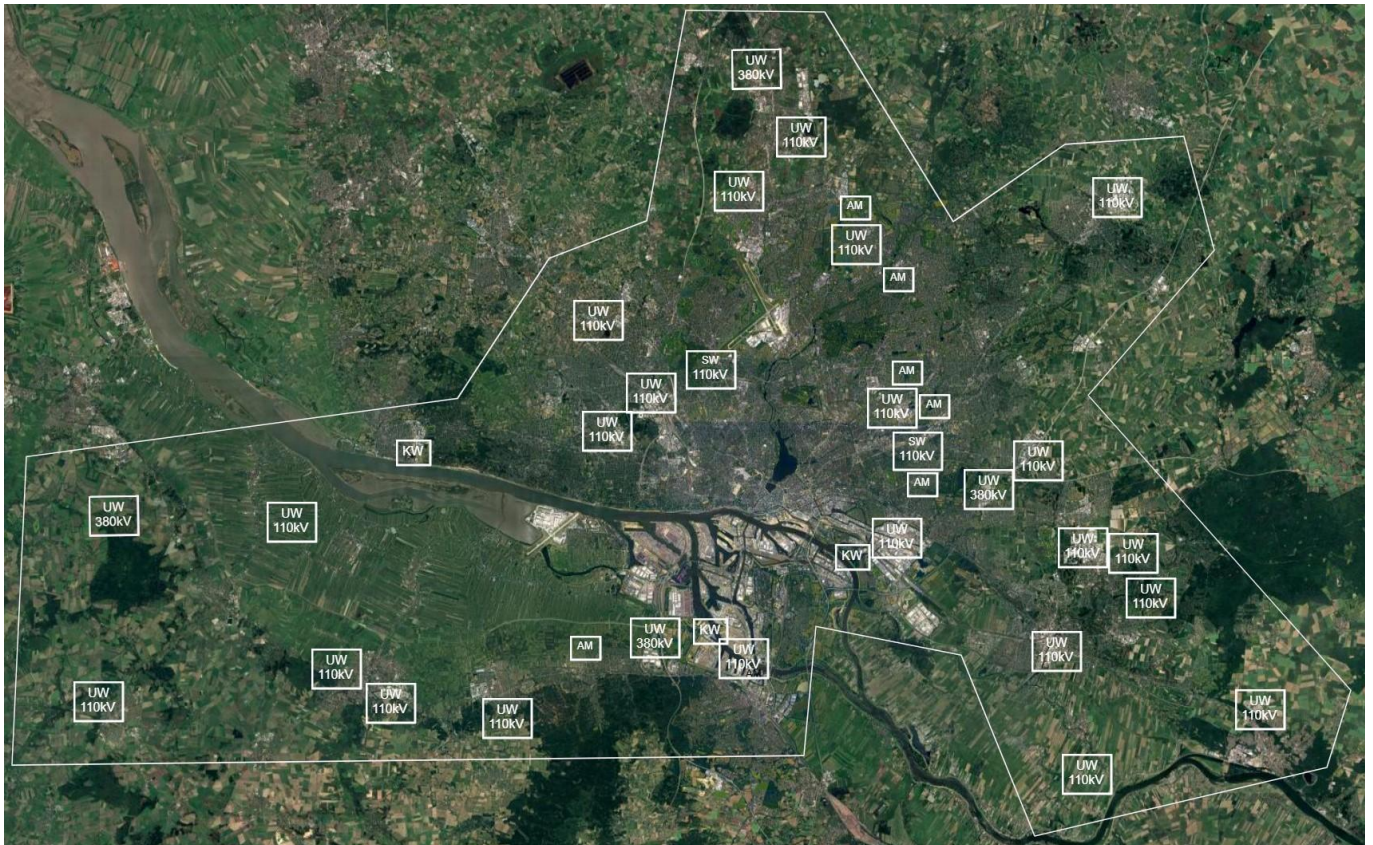


ABBILDUNG 4: BETRIEBSMITTEL ZIELE RAUM HAMBURG

3. Zuordnung betrieblicher Knotenpunkte zu denkbaren Angriffsszenarien

Auf Basis der räumlich-funktionalen Zuordnung erfolgte eine qualitative Risikoabschätzung nach dem Modell der Intelligence Preparation of the Battlefield (IPB). Hierbei werden zwei Szenariotypen unterschieden:

- MLCOA (Most Likely Course of Action): Szenarien mit hoher Eintrittswahrscheinlichkeit, aber begrenzten Folgen.
- MDCOA (Most Dangerous Course of Action): Szenarien mit geringerer Eintrittswahrscheinlichkeit, aber gravierenden Folgen für Versorgungssicherheit und öffentliche Ordnung

Der MDCOA stellt nicht das unwahrscheinlichste Szenario dar, sondern ein wenig wahrscheinliches mit sehr weitreichenden Folgen, wohingegen der MLCOA ein sehr wahrscheinliches Szenario mit Folgen geringer Schwere darlegt. Durch den MDCOA und den MLCOA wird eine Ebene realistischer Ereignisvektoren aufgespannt.

2) Entwicklung realistischer Angriffsszenarien (MLCOA / MDCOA)

Die im Folgenden dargestellten Fallbeispiele dienen der realitätsnahen Modellierung möglicher Bedrohungslagen im Hamburger Stromnetz. Sie basieren ausschließlich auf OSINT-Quellen, beschränken sich auf hypothetische Annahmen und dienen ausschließlich der wissenschaftlichen Gefahreneinschätzung.

Most Likely Course of Action (MLCOA)

Der MLCOA lässt sich wie folgt charakterisieren:

- Ziel ist ein einzelnes Betriebsmittel
- niedrige Wahrscheinlichkeit der Überführung für Täter von hoher Priorität
- nicht-staatlicher Akteur
- extremistischer Beweggrund
- Auswirkungen lokal begrenzt
- einfache Ausführbarkeit von Nöten
- Einzeltäter oder kleine Gruppierung

Mögliche MLCOA:

1. Brandanschlag auf 110 kV Kabelendmast durch Linksextremisten oder extremistische Umweltaktivisten bei Finkenwerder gerichtet gegen Airbus SE.



ABBILDUNG 5: MLCOA FINKENWERDER

Airbus SE als Flugzeugbauer, unter anderem von Militärmaschinen wie dem A400M oder dem Eurofighter sowie einem vollumfänglichen Geschäftsbereich Defense, stellt aufgrund seiner Geschäftsfelder sowohl ein mögliches Ziel für Linksextremisten als auch militante Umweltaktivisten dar. Das Werk wird durch eine 110 kV- Freileitung versorgt, deren zwei n-1 Systeme durch 110 kV- Kabelendmasten unterbrochen werden. Mittels Brandanschlags können die Masten in der Durchführung sehr niederschwellig zerstört und die Stromversorgung unterbrochen werden. Durch die ländliche und außerstädtische Lage sind gedeckte An- und Abmarschwege sichergestellt und die Wahrscheinlichkeit der unmittelbaren Überführung als gering zu bewerten. Ortlichkeiten und Auswirkungen sind in ABBILDUNG 5 dargestellt.

- Zerstören durch Sägen eines 110 kV-Freileitungsmastes durch Linksextremisten bei Steinwerder gerichtet gegen Blohm+Voss B.V. & Co. KG, Marinetechnik Zulieferer SKF Marine und Bundeswehr Standort.

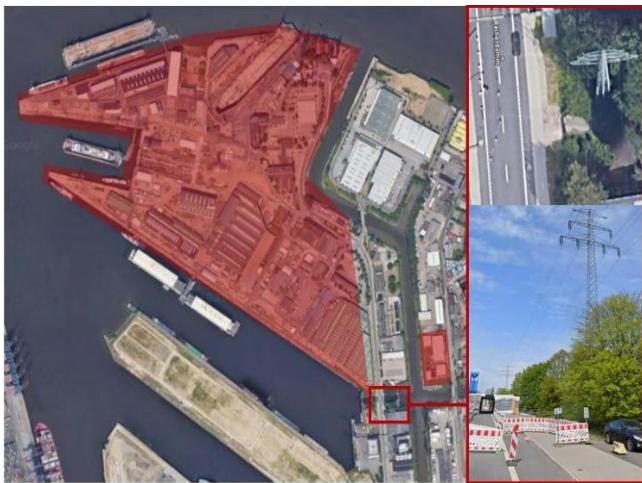


ABBILDUNG 6: MLCOA STEINWERDER

Blohm+Voss B.V. & Co. KG, der Marinetechnik Zulieferer SKF Marine sowie ein Bundeswehrstandort bilden einen Komplex im Stadtteil Steinwerder und stellen durch den Schwerpunkt in der Rüstungsindustrie sowie den medial verkündeten Bau der neuen Fregatte F126 durch Blohm+Voss B.V. & Co. KG am Standort Hamburg ein mögliches Ziel für linksextremistische Gruppierungen dar. Durch Zerstörung eines 110 kV- Freileitungsmastes, welcher beide n-1 Systeme trägt, ist ein gezielter Anschlag auf die versorgende Infrastruktur der Werke möglich. Die gedeckte Aufstellung ermöglicht eine unbeobachtete Vorgehensweise, welche auch durch Überwachungssysteme umliegender Betriebe nicht erfasst wird. Wenngleich bedingt durch das städtische Straßennetz aufgrund von Verkehrsüberwachungssystemen von einer Nachverfolgung auszugehen ist, bieten die gute Anbindung und Zugänglichkeit als sicher zu bewertende An- und Abmarschwege und eine damit einhergehende geringe Wahrscheinlichkeit der unmittelbaren Überführung. Ortlichkeiten und Auswirkungen sind in ABBILDUNG 6 dargestellt.

Most Dangerous Course of Action (MDCOA)

Der MDCOA lässt sich wie folgt charakterisieren:

- Ziel sind mehrere Betriebsmittel
- Wahrscheinlichkeit der Überführung wird in Kauf genommen

- Schadensmaximierung wird angestrebt
- staatlicher Akteur oder im Auftrag eines staatlichen Akteurs
- Auswirkungen nicht lokal begrenzt
- koordinierte Vorgehensweise durch mehrere Trupps

Möglicher MDCOA:

Zerstören von 380 kV Freileitungsmasten bei den drei 380 kV- Umspannwerken Hamburg Nord, Süd und Ost durch staatlichen Akteur mittels koordinierter Trupps (i.S.v. CaaS) gegen Bundesrepublik Deutschland.

Die Sabotage der drei 380 kV- Umspannwerke Nord, Süd und Ost (ABBILDUNG 7) würde zu einem hamburgweiten Stromausfall mit weitreichenden Folgen für Logistikketten in der Bundesrepublik Deutschland sowie Europa und erheblichen Beeinträchtigungen sowie Risiken für die öffentliche Sicherheit in Hamburg führen. Durch die leicht zugänglichen und ungeschützten 380 kV- Freileitungsmasten stellt sich ein koordinierter Anschlag durch drei Trupps als niederschwellig und einfach durchführbar dar. Weitere Schadmöglichkeiten wie die zusätzliche Beschädigung der Umspannwerke mittels Drohnen wurden nicht weiter betrachtet, würden jedoch das Schadbild insofern verstärken, als dass eine zügige Wiederherstellung der Übertragungsleistung verzögert wird.

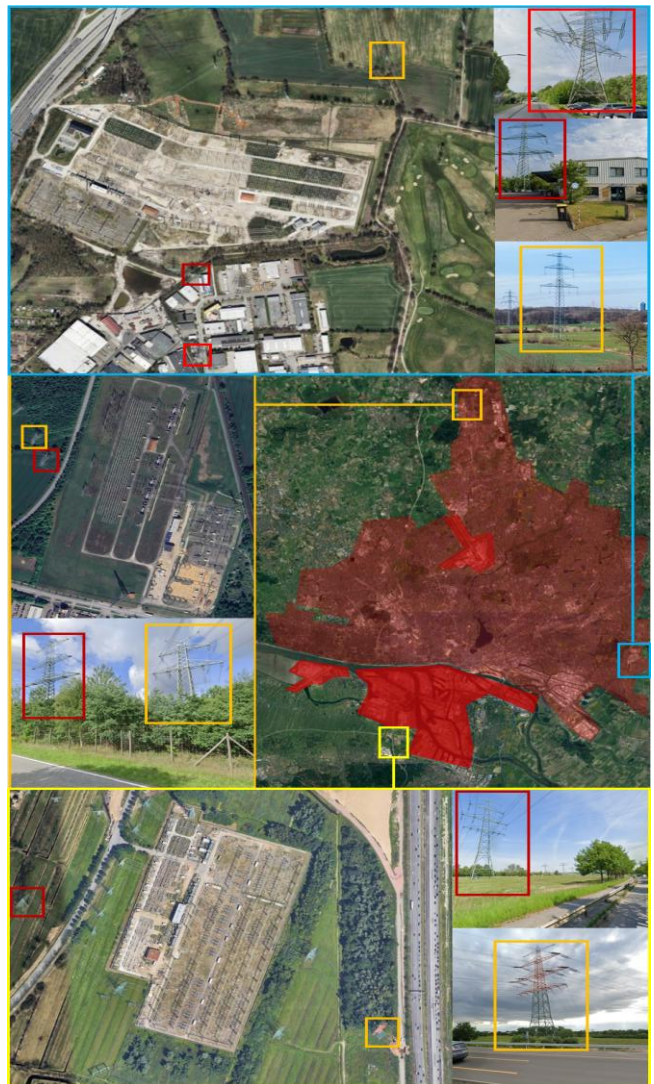


ABBILDUNG 7: MDCOA 380 kV UMSPANNWERK NORD, OST UND SÜD

C. Beobachtungen aus der Szenarienanalyse

Wenngleich sich die unmittelbaren und mittelbaren Auswirkungen der MLCOA und des MDCOA erheblich unterscheiden, zeichnen sich sowohl der MLCOA als auch der MDCOA durch eine sehr niedrige Hemmschwelle, Schwierigkeitsgrad als auch geringen notwendigen Aufwand aus. In der Folge müssen insbesondere zur Vermeidung des MDCOA Maßnahmen ergriffen werden, welche genannte Kriterien auf ein zu diskutierendes Mindestmaß anheben. Besonders die Verletzung des n-1 Kriteriums mangels physischer Trennung der redundanten Systeme muss in der Folge dazu führen, dass für Betriebsmittel, Systeme und Netze das n-1 Kriterium um KRITIS Betrachtungen erweitert wird. Die Redundanz wird allerdings dadurch eingeschränkt, dass in der Regel nur ein Mast diese Leitersysteme trägt. Wenn ganze Masten ausfallen, nutzt die redundante Auslegung der Leitersysteme nichts. [3]

V. AUSWERTUNG MITTELS RISIKO-MATRIX

A. Entwicklung der Risiko-Matrix

Die Entwicklung der Risiko-Matrix bildet einen zentralen Schritt zur systematischen Bewertung potenzieller Bedrohungen für kritische Betriebsmittel im elektrischen Übertragungs- und Verteilnetz. Ziel ist es, auf strukturierter Grundlage Maßnahmen priorisieren und die Resilienz der Infrastruktur gezielt erhöhen zu können. Die Matrix basiert auf sechs Kriterien, die sowohl die Wahrscheinlichkeit eines Angriffs als auch dessen technische und systemische Auswirkungen abbilden: Hemmschwelle, Schwierigkeitsgrad, Aufwand, unmittelbare Auswirkungen, sowie Auswirkungen auf das angrenzende Netz im Sinne des wahrscheinlichsten (MLCOA) und des gefährlichsten Szenarios (MDCOA).

Die Kriterien wurden auf Grundlage sicherheitsanalytischer Literatur [6–9, 36–38] und Experteneinschätzungen [2, 3, 7, 9] ausgewählt und sind bewusst so gestaltet, dass sie relevante Merkmale realer Angriffsszenarien differenziert und vergleichbar beschreiben. Dabei wurde auf eine gemeinsame Skalierung von 1 (niedrig) bis 10 (hoch) geachtet, ohne eine rechnerische Gewichtung vorzunehmen – zugunsten einer qualitativen Bewertung, die Klarheit schafft, aber keine scheinexakten Risikosummen suggeriert. Um Überlappungen zwischen den Kriterien (etwa zwischen Aufwand und Schwierigkeitsgrad) methodisch einzuordnen, erfolgt in den Folgeabschnitten eine Einzeldarstellung jeder Bewertungsdimension. Die nachfolgende Übersichtstabelle (Tabelle II) bietet ergänzend eine komprimierte Darstellung der Kriterien und ihrer typischen Ausprägungen in Form konkreter Beispiele.

1) Bewertungsdimensionen der Risiko-Matrix

Die Risiko-Matrix in TABELLE II basiert auf sechs Bewertungsdimensionen, die auf sicherheitsanalytischen Prinzipien und einschlägiger Fachliteratur beruhen [36–38]. Die Kriterien wurden so gewählt, dass sie typische Angriffsmerkmale auf physisch angreifbare Betriebsmittel im elektrischen Versorgungsnetz abbilden und zugleich eine praxisnahe, qualitative Einordnung erlauben. Eine vollständige Disjunktheit der Kriterien ist dabei nicht gegeben; insbesondere zwischen Aufwand und Schwierigkeitsgrad bestehen inhaltliche Überschneidungen, die im Bewertungsprozess jedoch bewusst getrennt berücksichtigt werden.

Hemmschwelle

Dieses Kriterium beschreibt psychologische oder physische Barrieren, die potenzielle Angreifer von einem Angriff abhalten können. Dazu zählen Zäune, Videoüberwachung, Zugangskontrollen oder soziale Hemmungen aufgrund von Standortnähe zur Öffentlichkeit. Eine geringe Hemmschwelle liegt beispielsweise bei ungeschützten Freileitungen in unbewohnten Gelände vor, eine hohe Hemmschwelle bei Umspannwerken mit Alarm- und Detektionssystemen. Das Kriterium unterscheidet sich vom Schwierigkeitsgrad dadurch, dass es nicht die technische Machbarkeit, sondern den subjektiven Abschreckungseffekt bewertet.

Schwierigkeitsgrad

Bewertet wird die technische oder logistische Komplexität der Durchführung eines Angriffs – etwa, ob Spezialwerkzeuge, elektrotechnisches Fachwissen oder risikoreiche Zugänge erforderlich sind. Brandstiftung an einem Mastfuß stellt einen Angriff mit niedrigem Schwierigkeitsgrad dar, während die Manipulation von Steuerungseinheiten oder Transformatoren als hochkomplex gilt. Im Gegensatz zum Aufwand bezieht sich dieses Kriterium primär auf Fähigkeiten und nicht auf Ressourcen.

Aufwand

Der Aufwand beschreibt die Ressourcen, die zur Durchführung des Angriffs notwendig sind, insbesondere Zeit, Material, Geld und Personal. Dieses Kriterium bewertet somit die praktische Hürde, nicht die technische Komplexität. Ein einfacher Diebstahl von Kupferdraht fällt bei niedrigem Aufwand an, während das präzise zeitkoordinierte Ausschalten mehrerer Systeme mit hohem logistischem Aufwand verbunden ist.

Unmittelbare Auswirkung

Dieses Kriterium bewertet den direkten Schaden am angegriffenen Betriebsmittel. Dazu zählen Zerstörung, Funktionsverlust oder Reparaturbedarf. Oberflächliche Schäden an Isolatoren gelten als geringfügig, ein Totalschaden an einem Transformator hingegen als hoch.

Auswirkung auf das angrenzende Netz – MLCOA

Bewertet werden die systemischen Folgewirkungen eines realistisch erwartbaren Angriffsszenarios (Most Likely Course of Action). Hierzu zählen etwa lokale Spannungseinbrüche, notwendige Umschaltungen oder temporäre Überlastsituationen. Eine Abgrenzung zur unmittelbar betroffenen Komponente erfolgt über den Netzkontext.

Auswirkung auf das angrenzende Netz – MDCOA

Dieses Kriterium bewertet die theoretisch schwerwiegendsten denkbaren Folgen (Most Dangerous Course of Action). Dazu zählen beispielsweise kaskadierende Ausfälle, regionale Blackouts oder Systeminstabilitäten durch das Wegbrechen zentraler Netzkomponenten. Die Einordnung erfolgt dabei unabhängig von der tatsächlichen Eintrittswahrscheinlichkeit.

2) Skalierung und Anwendung der Kriterien

Die oben beschriebenen Kriterien werden auf einer einheitlichen Skala von 1 bis 10 bewertet. Dabei steht 1 für

TABELLE II: ÜBERSICHT KRITERIEN FÜR RISIKO-MATRIX

Kriterium	Erklärung	Niedrig 1	Mittel 5	Hoch 10
Hemmschwelle	psychologische oder physische Barrieren, die Angreifer von der Durchführung eines Angriffs abhalten	freier Zugang, keine Überwachung, Angreifer werden nicht abgeschreckt, z. B. offene Freileitungen oder Kabelübergänge in ländlichen Gebieten	Sicherheitsmaßnahmen wie Zäune oder Überwachungskameras erschweren den Zugang, erfordern jedoch keine umfassende Planung zur Überwindung	stark gesicherte Anlagen, z. B. Umspannwerke mit Alarm- und Überwachungssystemen, die nur mit komplexen Mitteln und hohem Risiko zugänglich sind
Schwierigkeitsgrad	technische oder logistische Komplexität eines Angriffs	einfache Angriffe ohne technisches Wissen oder spezielle Werkzeuge, z. B. Brandstiftung an Mastfüßen.	Angriffe erfordern grundlegende technische Fähigkeiten oder Werkzeuge, wie die Manipulation von Transformatoren oder Isolatoren mit moderatem Aufwand	hochkomplexe Angriffe wie Cyberinfiltration oder gezielte Sabotage an zentralen Steuerungssystemen, die Expertenwissen und ausgeklügelte Vorbereitung verlangen
Aufwand	Ressourcen (Zeit, Kosten, Werkzeuge), die zur Durchführung eines Angriffs benötigt werden	minimaler Ressourceneinsatz, kein signifikanter Planungsaufwand, Durchführung in wenigen Minuten, z. B. Vandalismus.	moderater Ressourceneinsatz, z. B. Werkzeuge oder längere Planungszeit notwendig, Angriffe können bis zu mehrere Stunden Vorbereitungszeit erfordern	hoher Aufwand mit speziellem Equipment, erhebliche logistische Planung, zeit- und kostenintensive Durchführung, z. B. Sabotage eines Umspannwerks
Auswirkung unmittelbar	direkte Schäden oder Funktionsverluste am Betriebsmittel infolge eines Angriffs	leichte Beschädigungen, Betriebsmittel bleibt größtenteils funktional, z. B. Kratzer oder oberflächliche Schäden am Kabelmantel.	temporäre Einschränkungen, z. B. Funktionsverluste an einzelnen Komponenten wie Isolatoren oder beschädigten Freileitungen, Reparaturen erforderlich	Komplettausfall des Betriebsmittels, z. B. Zerstörung eines Transformators oder Brandschäden an einem Mast, die einen Austausch oder Neubau erfordern
Auswirkung auf das angrenzende Netz MLCOA	Folgen des Angriffs auf das Netz, das mit dem beschädigten Betriebsmittel verbunden ist	lokale, kurzzeitige Störungen ohne Beeinträchtigung des übergeordneten Netzes, z. B. Unterbrechung einer Leitung mit redundanter Versorgung	regionale Ausfälle, Umschaltungen notwendig, zeitlich begrenzte Netzstörungen in angrenzenden Gebieten, z. B. Ausfall eines Kabelübergangs mit Lastverlagerung.	keine
Auswirkung auf das angrenzende Netz MDCA	Folgen des gefährlichsten Angriffs auf das Netz, das mit dem beschädigten Betriebsmittel verbunden ist	keine	regionale Ausfälle, Umschaltungen notwendig, zeitlich begrenzte Netzstörungen in angrenzenden Gebieten, z. B. durch Ausfall eines Übergangsknotens	weitreichende Auswirkungen wie großflächige Blackouts, Netzstörungen oder Instabilität, z. B. durch den Ausfall eines zentralen Umspannwerks oder digitalen Steuerungssystems

eine geringe Ausprägung des jeweiligen Merkmals (z. B. minimaler Aufwand, keine Auswirkung) und 10 für eine sehr hohe (z. B. vollständiger Ausfall, komplexe Sabotage). Die Einordnung erfolgt ordinal und dient der strukturierten qualitativen Vergleichbarkeit zwischen verschiedenen Betriebsmitteln. Die Skala umfasst dabei exemplarische Schwellenwerte für die Ausprägungsstufen niedrig (1), mittel (5) und hoch (10), um die Bewertung konsistent und nachvollziehbar zu gestalten. Eine numerische Verrechnung oder Gewichtung dieser Werte findet nicht statt, um vermeintlicher Genauigkeit in der Risikoaggregation vorzubeugen. Ziel der Analyse: Die Risiko-Matrix bewertet die Anfälligkeit eines 110-kV-Freileitungsmastes anhand der Kriterien Hemmschwelle, Schwierigkeitsgrad, Aufwand sowie unmittelbare und netzweite Auswirkungen.

B. Freileitungsmast 110 kV

Freileitungsmasten stellen eine der exponiertesten Komponenten im Übertragungsnetz dar. Ihre Lage in offenen und oft abgelegenen Bereichen macht sie besonders anfällig für physische Angriffe wie Vandalismus, Brandstiftung oder Sabotage.

1) Mögliche Bedrohungsszenarien für einen Freileitungsmast

Freileitungsmasten sind zentrale und exponierte Bestandteile des Übertragungsnetzes und damit anfällig für verschiedene Angriffsarten. Zu den möglichen Bedrohungsszenarien gehören:

1. LKW-Anschlag: Durch gezieltes Rammen mit einem schweren Fahrzeug können die Tragstrukturen eines Freileitungsmastes erheblich beschädigt oder zum Einsturz gebracht werden. Dies führt unmittelbar zur Unterbrechung der Stromleitung.
2. Drohne mit Stahlseil: Angreifer könnten eine Drohne verwenden, um ein Stahlseil über die Leitungen zu werfen. Das Seil könnte einen Kurzschluss verursachen oder die Leitung mechanisch beschädigen.
3. Sägen am Mast: Durch manuelles oder maschinelles Sägen an der Tragstruktur eines Mastes wird dessen Stabilität geschwächt. Dies kann zu einem vollständigen Kollaps führen, insbesondere bei Windbelastung oder anderen Umwelteinflüssen.

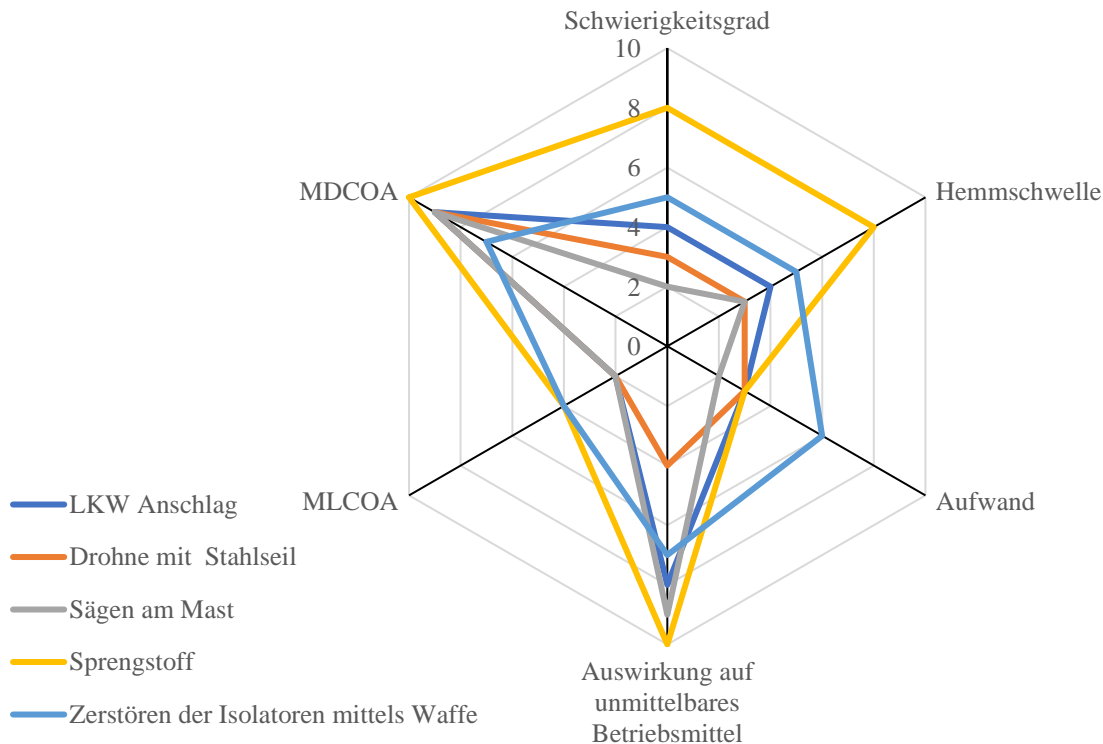


ABBILDUNG 8: RISIKOBEWERTUNG FREILEITUNGSMAST

4. Sprengstoff: Der Einsatz von Sprengstoff ist eine der effektivsten Methoden, um die Struktur eines Freileitungsmastes sofort zu zerstören. Die Folgen wären weitreichend, einschließlich großflächiger Stromausfälle.
5. Zerstören der Isolatoren mittels Waffe: Der gezielte Beschuss oder die mechanische Zerstörung der Isolatoren führt zu Kurzschlüssen oder Lichtbögen, die den Betrieb der Leitung erheblich stören oder unterbrechen können.

2) Bewertung

Die ABBILDUNG 8 zeigt eine Radar-Chart zur Risiko-Analyse eines Freileitungsmastes, wobei verschiedene Bedrohungsszenarien anhand von Kriterien wie Hemmschwelle, Schwierigkeitsgrad, Aufwand, Auswirkung auf unmittelbares Betriebsmittel, MLCOA (Most Likely Course of Action) und MDCOA (Most Dangerous Course of Action) bewertet werden.

1. LKW-Anschlag

- Schwierigkeitsgrad: relativ niedrig, da keine technische Expertise benötigt wird
- Hemmschwelle: moderat, da das Risiko der Entdeckung besteht
- Aufwand: gering bis mittel, abhängig von der Verfügbarkeit des Fahrzeugs
- Auswirkung: mittel bis hoch, da der Mast direkt beschädigt oder zerstört werden kann

2. Drohne mit Stahlseil

- Schwierigkeitsgrad: mittel bis hoch, da der Einsatz technischer Geräte und präzises Arbeiten erforderlich sind
- Hemmschwelle: relativ niedrig, da Drohnen leicht zugänglich und einsetzbar sind
- Aufwand: mittel, da die Vorbereitung und der Einsatz einer Drohne Ressourcen benötigen
- Auswirkung: hoch, da ein Kurzschluss oder physischer Schaden an den Leitungen weitreichende Folgen haben kann

3. Sägen am Mast

- Schwierigkeitsgrad: niedrig bis mittel, da keine spezifischen technischen Fähigkeiten erforderlich sind
- Hemmschwelle: niedrig, wenn der Mast in einem abgelegenen Bereich steht
- Aufwand: mittel bis hoch, abhängig vom Material des Mastes und der Dauer des Sägens
- Auswirkung: hoch, da ein Kollaps des Mastes großflächige Stromausfälle verursachen kann

4. Sprengstoff

- Schwierigkeitsgrad: hoch, da der Einsatz von Sprengstoff spezielle Kenntnisse und Zugang zu Materialien erfordert
- Hemmschwelle: hoch, da Sprengstoff schwer zu beschaffen ist und das Risiko der Entdeckung groß ist

- Aufwand: hoch, sowohl in der Planung als auch in der Durchführung
- Auswirkung: sehr hoch, da Sprengstoff die Struktur des Mastes vollständig zerstören kann, was zu großflächigen Netzstörungen führt

5. Zerstören der Isolatoren mittels Waffe

- Schwierigkeitsgrad: mittel bis hoch, da Zielgenauigkeit und Zugang zu Waffen erforderlich sind
- Hemmschwelle: niedrig bis mittel, abhängig von der Umgebung und der Überwachung
- Aufwand: gering bis mittel, da Schusswaffen oder ähnliche Geräte relativ leicht zugänglich sind
- Auswirkung: mittel, da beschädigte Isolatoren Störungen oder Kurzschlüsse verursachen können, jedoch weniger katastrophal als ein Mastkollaps

Fazit

- Sprengstoff und Drohne mit Stahlseil stellen die gravierendsten Bedrohungen dar, da sie sowohl hohe Auswirkungen als auch technisches Potenzial haben.
- Sägen am Mast ist hinsichtlich Aufwand und Hemmschwelle ein einfach umsetzbares Szenario, jedoch mit erheblichen Folgen.
- LKW-Anschlag ist leicht auszuführen, jedoch stärker standortabhängig.
- Zerstören der Isolatoren hat begrenzte Auswirkungen, bleibt jedoch eine reale Bedrohung, da der Aufwand gering ist.
- Das Radar-Diagramm zeigt deutlich, wie die Szenarien in ihrer Risikointensität variieren, und bietet eine Grundlage, um gezielte Schutzmaßnahmen zu entwickeln.

C. Kabel-Endmast – Übergang der Freileitung auf Kabelstrecke

Kabelendmasten sind kritische Knotenpunkte im Netz, da sie den Übergang von Freileitungen zu Erdkabeln ermöglichen. Dieser Bereich ist aufgrund seiner mechanischen und elektrischen Komplexität sowie seiner zentralen Bedeutung besonders schützenswert. Ziel der Analyse: Die Risiko-Matrix zeigt, wie dieser Übergang durch Angriffe auf mechanische oder elektrische Komponenten beeinträchtigt werden könnte. Faktoren wie die Erreichbarkeit des Kabelendmastes und die möglichen Folgen eines Ausfalls für das Netz werden dabei detailliert betrachtet.

1) Neue Bedrohungsszenarien

1. Brandanschlag

- Schwierigkeitsgrad: niedrig bis mittel, da nur leicht zugängliche brennbare Materialien benötigt werden
- Hemmschwelle: niedrig, insbesondere in abgelegenen Bereichen
- Auswirkung: hoch, da die Kabelisolierung durch einen Brand stark beschädigt werden kann, was zu Kurzschlüssen oder Totalausfällen führt

2. Zerschneiden der Kabelbahn

- Schwierigkeitsgrad: mittel, da das Zerschneiden der Kabelschienen präzises Werkzeug und physischen Zugang erfordert
- Hemmschwelle: mittel, da ein direkter Zugang zur Kabelbahn notwendig ist, der oft durch Schutzmaßnahmen erschwert wird
- Auswirkung: sehr hoch, da das Durchtrennen einer Kabelbahn die Energieübertragung vollständig unterbrechen kann

2) Bewertung

Die ABBILDUNG 9 stellt alle Bedrohungsszenarien, einschließlich der neuen Szenarien Brandanschlag (rot) und Zerschneiden der Kabelbahn (blau), grafisch dar.

Der Kabelendmast ist besonders anfällig für physische Eingriffe wie Brandanschläge und Zerschneiden der Kabelbahn, die sowohl eine niedrige Hemmschwelle als auch erhebliche Auswirkungen auf das Betriebsmittel und das Netz haben können. Präventive Maßnahmen sollten sich auf die physische Sicherung und Überwachung dieser Komponenten konzentrieren.

1. Brandanschlag

- Schwierigkeitsgrad: niedrig bis mittel, da brennbare Materialien einfach verfügbar sind
- Hemmschwelle: niedrig, besonders in unbewachten Bereichen
- Aufwand: niedrig bis mittel, da die Durchführung einfach ist
- Auswirkung: hoch, da ein Brand die Isolierung der Kabel beschädigen und Kurzschlüsse oder Betriebsausfälle verursachen kann

2. Zerschneiden der Kabelbahn

- Schwierigkeitsgrad: mittel bis hoch, da spezielles Werkzeug benötigt wird
- Hemmschwelle: mittel, da direkter Zugang notwendig ist
- Aufwand: mittel, da die Kabelschienen robust sind und das Zerschneiden Zeit und Präzision erfordert
- Auswirkung: sehr hoch, da ein Durchtrennen der Kabelbahn den Energiefluss vollständig unterbrechen kann, was weitreichende Störungen nach sich zieht

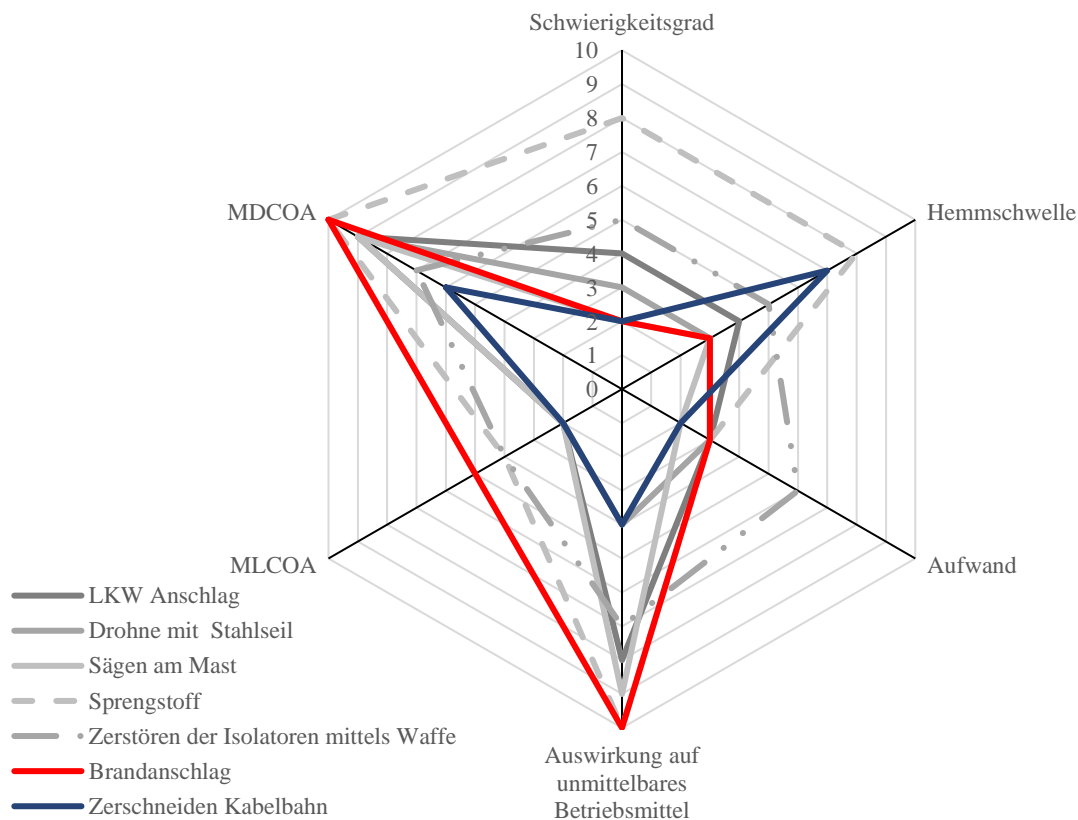


ABBILDUNG 9: RISIKOBEWERTUNG KABEL-ENDMAST

D. Umspannstationen oder Schaltwerke

Umspannstationen und Schaltwerke gehören zu den zentralen Elementen der Energieversorgung, da sie Spannungen transformieren und Energieflüsse steuern. Sie sind oft durch äußere Umzäunungen, feste Wände und Zugangssperren geschützt. Dennoch stellen sie aufgrund ihrer strategischen Bedeutung ein attraktives Ziel für Sabotageakte dar.

Ziel der Analyse: Die Risiko-Matrix untersucht die Schutzmechanismen und Schwachstellen von Umspannstationen. Insbesondere wird bewertet, wenn die Anforderungen der DIN EN IEC 61936-1 (VDE 0101-1:2023-02) an Zutrittsbeschränkung erfüllt wird.

1) Mögliche Bedrohungsszenarien für Umspannstationen oder Schaltwerke

Nur neue Szenarien, andere entsprechend verändert

1. Zerstören der Transformatoren mittels Waffe:

- Angriffe mit Schusswaffen oder anderen Fernkampfaffen auf die Gehäuse von Transformatoren können das Kühllöl freisetzen, was zu Überhitzung und schwerwiegenden Ausfällen führen kann.

2. Drohne mit Termitschweißtiegel auf Transformator:

- Der Einsatz einer Drohne, die einen Termitschweißtiegel auf einem Transformator abwirft, könnte gezielt Materialien erhitzen und Bauteile zerstören. Dies ist besonders gefährlich, da

die hohen Temperaturen des Thermits selbst massive metallische Strukturen beschädigen können.

2) Bewertung

Das Radar-Diagramm in ABBILDUNG 10 bietet eine Übersicht über die Bewertung der möglichen Bedrohungsszenarien für Umspannwerke und Schaltwerke.

1. Brandanschlag

- Hemmschwelle: niedrig, da leicht zugängliche brennbare Materialien genutzt werden können
- Schwierigkeitsgrad: mittel, da die Durchführung keine speziellen technischen Kenntnisse erfordert
- Aufwand: gering bis mittel, da einfache Mittel wie Benzin oder andere Brandstoffe ausreichen
- Auswirkung: hoch, da Brandschäden Isolierungen und Transformatoren beschädigen können, was zu Stromausfällen führen könnte
- MLCOA: hoch, da Brandanschläge häufig eine leicht umsetzbare Sabotageoption darstellen
- MDCOA: sehr hoch, wenn der Brand großflächig außer Kontrolle gerät und kritische Komponenten zerstört

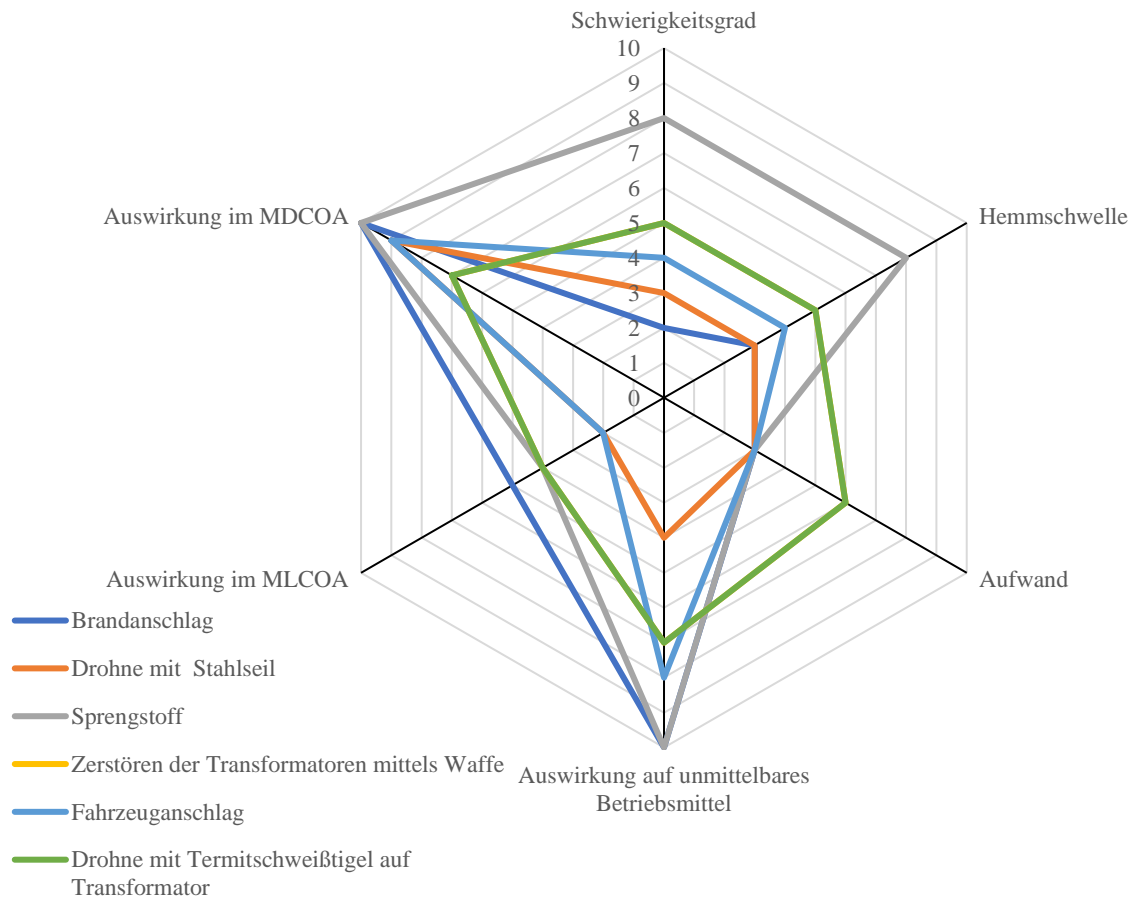


ABBILDUNG 10: RISIKOBEWERTUNG UMSPANNWERKE/ SCHALTWERKE

2. LKW-Anschlag

- Hemmschwelle: mittel, da Zugang und schweres Gerät erforderlich sind
- Schwierigkeitsgrad: niedrig bis mittel, da die Durchführung technisch einfach ist
- Aufwand: hoch, da ein LKW organisiert und die Umzäunung durchbrochen werden muss
- Auswirkung: hoch, da mechanische Beschädigungen an Transformatoren oder anderen wichtigen Komponenten schwerwiegende Folgen haben können
- MLCOA: mittel bis hoch, abhängig von der Durchführbarkeit
- MDCOA: sehr hoch, wenn mehrere Komponenten oder Transformatoren zerstört werden

3. Drohne mit Stahlseil

- Hemmschwelle: mittel, da Drohnen leicht zugänglich, aber der Einsatz auffällig ist
- Schwierigkeitsgrad: hoch, da die präzise Steuerung einer Drohne und das Platzieren des Stahlseils technisches Geschick erfordern
- Aufwand: mittel bis hoch, da Vorbereitung und geeignete Drohnen notwendig sind
- Auswirkung: hoch, da Kurzschlüsse oder Schäden an Leitungen die Funktion erheblich stören können

- MLCOA: hoch, da solche Angriffe gezielt und effektiv eingesetzt werden können
- MDCOA: Sehr hoch, wenn die Drohne zentrale Stromleitungen oder Transformatoren beschädigt

4. Sägen am Mast

- Hemmschwelle: niedrig, besonders bei abgelegenen Standorten
- Schwierigkeitsgrad: niedrig, da keine fortgeschrittenen Fähigkeiten erforderlich sind
- Aufwand: mittel, da Werkzeuge und Zeit erforderlich sind
- Auswirkung: mittel bis hoch, da der Mast instabil werden oder sogar einstürzen könnte
- MLCOA: mittel, da diese Methode eher in abgelegenen Bereichen realistisch ist
- MDCOA: hoch, wenn die Stabilität von Schaltwerken oder Umspannstationen beeinträchtigt wird

5. Sprengstoff

- Hemmschwelle: hoch, da der Zugang zu Sprengstoff kontrolliert ist
- Schwierigkeitsgrad: hoch, da der Einsatz Planung und technisches Wissen erfordert
- Aufwand: sehr hoch, da die Beschaffung und Platzierung von Sprengstoff komplex sind

- Auswirkung: sehr hoch, da Transformatoren oder andere zentrale Komponenten vollständig zerstört werden könnten
- MLCOA: mittel bis hoch, da der Einsatz von Sprengstoff aufwendig ist
- MDCOA: sehr hoch, da massive Netzstörungen oder Blackouts möglich sind

6. Zerstören der Transformatoren mittels Waffe

- Hemmschwelle: niedrig bis mittel, da Waffen relativ leicht zugänglich sind
- Schwierigkeitsgrad: mittel, da Zielgenauigkeit erforderlich ist
- Aufwand: gering bis mittel, da nur die richtige Positionierung notwendig ist
- Auswirkung: hoch, da beschädigte Transformatoren schwerwiegende Netzprobleme verursachen können
- MLCOA: mittel, da dieser Angriff schnell durchführbar ist
- MDCOA: hoch, wenn mehrere Transformatoren gleichzeitig angegriffen werden

Fazit

Die Bewertung zeigt, dass besonders Sprengstoffanschläge, Brandanschläge sowie der Einsatz von Drohnen mit Stahlseil im Hinblick auf die potenzielle Schadenshöhe (MDCOA) als besonders kritisch einzustufen sind. Sie können – bei erfolgreicher Durchführung – zentrale Betriebsmittel wie Transformatoren vollständig zerstören und damit großflächige Versorgungsunterbrechungen oder Dominoeffekte im Netz auslösen. Diese Szenarien erfordern jedoch meist hohen Aufwand, spezielles technisches Wissen oder schwer zugängliche Mittel (z. B. Sprengstoff), was ihre Eintrittswahrscheinlichkeit senkt. Demgegenüber sind Brandanschläge und das Zerstören von Transformatoren mittels Schusswaffen Szenarien mit vergleichsweise niedriger Hemmschwelle und höherer Eintrittswahrscheinlichkeit (MLCOA). Sie können ohne hochspezialisierte Mittel durchgeführt werden und haben sich in der Vergangenheit als umsetzbare Angriffsmethoden mit teilweise gravierenden Folgen gezeigt. Besondere Aufmerksamkeit verdienen daher Szenarien, die sowohl bei MLCOA als auch MDCOA hohe Bewertungen erzielen, wie etwa Brandanschläge oder gezielte Drohnenangriffe, da sie nicht nur plausibel durchführbar, sondern im Ernstfall auch besonders schädlich sein können.

VI. MÖGLICHE GEGENMAßNAHMEN UND DISKUSSION

Der Schutz kritischer Betriebsmittel im elektrischen Übertragungs- und Verteilnetz erfordert einen ganzheitlichen Ansatz, der auf systematisch bewerteten Bedrohungsszenarien basiert. Aufbauend auf der Risikoanalyse (Kap. V) werden in diesem Kapitel technische, organisatorische und präventive Maßnahmen abgeleitet, die auf die spezifischen Schwächen und Angriffsmuster reagieren. Die Maßnahmenentwicklung folgt dabei einem induktiven Vorgehen:

Die Ableitung erfolgt aus:

- dokumentierten realen Angriffen (vgl. Kap. III.3),
- der typisierten Bewertung ausgewählter Betriebsmittel (Kap. V),

- sicherheitsanalytischen Standards [[1, 39, 40]],
- und praxisnahen Handlungsempfehlungen aus Fachliteratur und Expertengesprächen.

Der Fokus liegt auf physisch umsetzbaren Schutzmaßnahmen für Freileitungen, Umspannwerke und Kabelübergänge. Die Maßnahmen adressieren dabei explizit jene Risikoindikatoren, die sich in der Analyse als kritisch erwiesen haben: geringe Hemmschwelle, einfacher Zugang, hoher Schaden im MLCOA- oder MDCOA-Szenario. Die vorgeschlagenen Maßnahmen sind entlang dieser Dimensionen strukturiert und werden hinsichtlich ihrer Wirksamkeit diskutiert.

A. Systematische Ableitung von Schutzmaßnahmen

Auf Grundlage der Risikoanalyse aus Kapitel V wurden gezielt Maßnahmen entwickelt, die den erkannten Schwachstellen einzelner Betriebsmittel und typischer Angriffsmuster begegnen. Die Struktur folgt den dort eingeführten Bewertungskriterien – Hemmschwelle, Schwierigkeitsgrad, Aufwand, unmittelbare Auswirkung sowie systemische Wirkung im MLCOA- und MDCOA-Szenario. Diese Systematik erlaubt eine differenzierte Maßnahmenentwicklung mit nachvollziehbarem Bezug zur Gefährdungslogik.

1) Maßnahmen zur Erhöhung der Hemmschwelle

Diese Maßnahmen sind insbesondere für Betriebsmittel mit offenem Zugang und fehlender Überwachung geeignet. Sichtbare Kameras, Zäune, Warnhinweise und Zugangskontrollen schaffen physische und psychologische Barrieren.

Bewertung: Kostengünstig, flächig einsetzbar, hohe Abschreckungswirkung – insbesondere bei opportunistischen Tätern.

Folgerung: Niedrigschwellige Maßnahmen mit hohem Wirkungspotenzial im ländlichen Raum.

2) Maßnahmen zur Erhöhung des Schwierigkeitsgrads

Hier geht es um die technische Härtung der Betriebsmittel: isolierte Leitungen, geschützte Anschlüsse, manipulationssichere Isolatoren.

Bewertung: Technisch wirksam, aber teilweise kostenintensiv und schwer nachrüstbar.

Folgerung: Besonders relevant für Neubauprojekte oder kritische Knotenpunkte mit hoher MDCOA-Wirkung.

3) Maßnahmen zur Erhöhung des Aufwands

Beispiele sind verriegelte Zugänge, dokumentierter Personaleintritt oder Nachtsperren.

Bewertung: Wirksam gegen spontane Eingriffe; personell/organisatorisch anspruchsvoll im Dauerbetrieb.

Folgerung: In Verbindung mit organisatorischen Maßnahmen gut integrierbar; nicht isoliert wirksam.

4) Maßnahmen zur Begrenzung unmittelbarer Schäden

Dazu zählen Segmentierung, Feuerhemmung und automatische Schutzfunktionen.

Bewertung: Begrenzen technische Folgeschäden, mindern Reparaturkosten.

Folgerung: Besonders geeignet bei Betriebsmitteln mit langer Wiederherstellungsdauer (z. B. Trafos).

5) Maßnahmen zur Reduzierung systemischer Netzwirkungen

Redundante Netzstrukturen, Inselbetriebskonzepte, Speichersysteme oder schwarzfallfeste Kommunikation stärken die Resilienz gegen Eskalationen. schwarzfallfeste Kommunikation (z. B. 450-MHz-Notfunk oder LoRaWAN-Systeme)

Die Hamburger Energienetze setzen bereits LoRaWAN-basiertes Monitoring ein, das dafür genutzt werden könnte [41].

Bewertung: Hoher Wirkungsgrad, aber oft nur mittel- bis langfristig umsetzbar.

Folgerung: Erforderlich für kritische Infrastrukturen mit nationaler Bedeutung; Umsetzungszeitpunkt und Ressourcenbedarf sind begrenzende Faktoren.

B. Diskussion der Wirksamkeit und Grenzen

Die Analyse zeigt, dass viele effektive Maßnahmen bereits bekannt oder verfügbar sind, ihre gezielte Anwendung jedoch stark vom jeweiligen Betriebsmittel, Standort und Bedrohungsszenario abhängt. Maßnahmen zur Erhöhung der Hemmschwelle und des Aufwands lassen sich oft kurzfristig realisieren und wirken besonders bei MLCOA-Szenarien. Technische Maßnahmen mit Fokus auf Schadensbegrenzung oder Erhöhung des Schwierigkeitsgrads sind v. a. bei zentralen Netzelementen (z. B. Umspannwerke) unverzichtbar, aber investitionsintensiv. Systemisch wirksame Maßnahmen wie Notfallregelungen, Dezentralisierung oder digitale Monitoringlösungen sind langfristig entscheidend, aber auch komplex in der Umsetzung. Besonders relevant ist dabei die Erkenntnis, dass viele reale Anschläge mit einfachen Mitteln bei gleichzeitig großer Wirkung durchgeführt wurden – ein starkes Argument für priorisierte Abschreckung und Früherkennung.

Schlussfolgerung: Ein wirkungsvoller Schutz kritischer Betriebsmittel ergibt sich nicht aus Einzelmaßnahmen, sondern aus einer Kombination technischer, organisatorischer und strategischer Ansätze entlang der Risikoindikatoren. Die vorgestellte Kategorisierung bietet ein robustes Raster zur strukturierten Maßnahmenentwicklung und ermöglicht eine praxisnahe Priorisierung.

VII. AUSBLICK

Die vorliegende Untersuchung zeigt exemplarisch, wie sich systematisch hergeleitete Risikoindikatoren nutzen lassen, um verwundbare Betriebsmittel im elektrischen Versorgungsnetz zu identifizieren und gezielt mit Schutzmaßnahmen zu adressieren. Insbesondere wurde deutlich, dass vergleichsweise einfache Angriffe auf physisch exponierte Komponenten wie Freileitungsmasten oder Kabelübergänge zu erheblichen Funktionsstörungen bis hin zu systemischen Netzstörungen führen können. Die Kombination aus geringer Hemmschwelle, minimalem Aufwand und potenziell hoher Wirkung macht diese Betriebsmittel besonders sicherheitskritisch. Für die zukünftige Ausgestaltung von Schutzkonzepten ergibt sich daraus ein klarer Handlungsauftrag: Es bedarf integrierter Sicherheitsstrategien, die technische Härtung, organisatorische Schutzmaßnahmen und intelligente Überwachungslösungen miteinander verbinden. Während bauliche und organisatorische Maßnahmen punktuell bereits wirksam eingesetzt werden, offenbart sich ein wachsender Bedarf an adaptiver, echtzeitfähiger Sensorik – insbesondere

an schwer einsehbaren oder abgelegenen Freileitungsmasten. Flächendeckende, kosteneffiziente Detektionssysteme könnten nicht nur Angriffe frühzeitig erkennen, sondern auch gezielte Reaktionen und Netzanpassungen ermöglichen. Zugleich ist eine verstärkte Zusammenarbeit zwischen Netzbetreibern, staatlichen Stellen und Forschungseinrichtungen erforderlich, um vorhandene Erkenntnisse systematisch zusammenzuführen und in normativen Vorgaben zu verankern. Nur durch ein gemeinsames Verständnis von Bedrohungslagen und eine abgestimmte Priorisierung von Schutzmaßnahmen lässt sich die Resilienz elektrischer Infrastrukturen gegenüber physischen Angriffen nachhaltig steigern.

Fazit: Die Risikoanalyse und Maßnahmensystematik bieten eine tragfähige Grundlage, um die Verletzlichkeit zentraler Netzkomponenten zu bewerten und gezielte Schutzstrategien zu entwickeln. Künftige Arbeiten sollten sich verstärkt der praktischen Erprobung und Skalierung sensorbasierter Überwachungsansätze widmen – als Schlüssel zu einem proaktiven, lageangepassten Sicherheitsmanagement im Stromnetz der Zukunft.

LITERATUR

- [1] *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz*, 2022. Zugriff am: 8. November 2024. [Online]. Verfügbar unter: <https://www.gesetze-im-internet.de/bsi-kritisch/>
- [2] *Forschung für den Bevölkerungsschutz*, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2023. Zugriff am: 20. November 2024. [Online]. Verfügbar unter: https://www.bbk.bund.de/DE/Themen/Forschung/Fachkongress/fachkongress_node.html
- [3] S. Byfield, Hg. *Das Energiesystem resilient gestalten: Maßnahmen für eine gesicherte Versorgung* (Schriftenreihe zur wissenschaftsbasierten Politikberatung). München, Mainz: acatech - Deutsche Akademie der Technikwissenschaften; Union der Deutschen Akademien der Wissenschaften, 2017. [Online]. Verfügbar unter: http://web.archive.org/web/20181115010653/http://www.acatech.de/wp-content/uploads/2018/03/ESYS_Stellungnahme_Das_Energiesystem_resilient_gestalten.pdf
- [4] *Resilienz bei Kritischen Infrastrukturen in der EU*, 2022/2557, EUROPÄISCHEN PARLAMENT UND RAT, Brüssel, Dez. 2022. [Online]. Verfügbar unter: <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2557>
- [5] Bundesamt für Justiz, *Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz - EnWG)*: EnWG (2024), 2024. Zugriff am: 20. November 2024. [Online]. Verfügbar unter: https://www.gesetze-im-internet.de/enwg_2005/
- [6] C. Perrow, *Normale Katastrophen: Die unvermeidbaren Risiken der Großtechnik* (Reihe Campus 1028). Frankfurt/Main, New York: Campus-Verl., 1989.
- [7] Bundesministerium des Innern und für Heimat, Hg. *Umsetzungsplan der Deutschen Strategie zur Stärkung der Resilienz gegenüber Katastrophen* (2024). Berlin, 2024. Zugriff am: 20. November 2024. [Online]. Verfügbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/BMI24017-umsetzungsplan-resilienz.pdf?__blob=publicationFile&v=3
- [8] Hein-Adalbert Krebs und Patricia Hagenweiler, *Energieresilienz und Klimaschutz-Energiesysteme, kritische Infrastrukturen und Nachhaltigkeitsziele*. Springer, 2021.
- [9] J. Birkmann, C. Bach, S. Guhl, M. Witting, T. Welle und M. Schmude, *State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom/Stromausfall*. Forschungsforum Öffentliche Sicherheit.
- [10] Bundesamt für Sicherheit und Informationstechnik. "Active Crime Gruppen." [Online.] Verfügbar: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive-Crime-Gruppen/aktive-crime-gruppen_node.html
- [11] Europol, *Exploring tomorrow's organised crime*, 2015.

- [12] *EU warnt vor russischer Schattenflotte*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: <https://www.zdf.de/nachrichten/politik/ausland/russland-eu-schattenflotte-sabotage-100.html>
- [13] *Drei Monate nach Tesla Anschlag noch kein Ende der Ermittlungen absehbar*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: <https://www.tagesspiegel.de/potsdam/brandenburg/drei-monate-nach-tesla-anschlag-noch-kein-ende-der-ermittlungen-absehbar-11768735.html>
- [14] *Attacke auf kritische Infrastruktur in Grevenbroich*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: <https://www.zeit.de/news/2021-05/21/feuer-an-stromtrasse-sorgt-fuer-stromausfall-in-muenchen>
- [15] *Stromausfall in München*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: https://www.bkk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/PiB/PiB-16-risikoanalyse-bevoelkerungsschutz.pdf?__blob=publicationFile
- [16] *Strommast Sabotage*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: <https://polizei.news/2020/10/20/gland-vd-strommast-sabotage-vom-26-6-20-nicht-mit-sprengstoff/>
- [17] *Sabotage-Akt am Tagebau*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: <https://www.aachener-zeitung.de/region-nrw/sabotage-akt-am-tagebau-strommast-angesagt/3516341.html>
- [18] *Öffentliche Sicherheit 5-6/17, Sabotage, Drohungen, Angriffe*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: https://www.bmi.gv.at/magazinfiles/2017/05_06/files/schutz%20kritischer%20infrastruktur_ii.pdf
- [19] *Bundesamt geht von Hackerangriff auf ukrainisches Stromnetz aus*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: <https://www.sueddeutsche.de/wirtschaft/ukraine-bundesamt-geht-von-hackerangriff-auf-ukrainisches-stromnetz-aus-1.2830197>
- [20] *Millionen-Schaden / Energieversorgung normal: Täter sägten an einem Strommast*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: <https://www.berliner-zeitung.de/millionen-schaden-energieversorgung-normal-anschlag-taeter-saegten-an-einem-strommast-li.44569>
- [21] *Abschallen mit Säge*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: <https://www.spiegel.de/politik/abschallen-mit-saege-a-d61b59b1-0002-0001-0000-000013521610>
- [22] Frank J. Prial, "Antitank Rockets Are Fired at French Nuclear Reactor," *The New York Times*, 1982.
- [23] *Sprengstoffanschlag gegen Kernkraftwerk Gösgen*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: <https://www.nzz.ch/>
- [24] *Als zwischen Bozen und Brenner die Bomben explodierten*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: <https://www.welt.de/geschichte/article231759543/Suedtirol-Die-Extremisten-attackierten-die-Stromversorgung-um-Verhandlungen-zu-torpedieren.html>
- [25] *Die Elbe – wichtiger Verkehrsweg für See- und Binnenschiffe*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: https://www.gdws.wsv.bund.de/SharedDocs/Kurzmeldungen/DE/20220616_Elbschiffahrtstag.html
- [26] *Statistiken Hafen Hamburg*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: https://www.hafen-hamburg.de/de/aktuelles/statistiken/?utm_source=chatgpt.com#in-page-gesamtumschlag
- [27] *Hamburg: Hafenterminal als kritische Infrastruktur registriert*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: <https://www.schiffahrtundtechnik.de/nachrichten/binnenschiffahrt/hamburg-hafenterminal-als-kritische-infrastruktur-registriert-3360874>
- [28] *Hamburg als Umschlagplatz für Waffen in alle Welt*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: <https://ziviler-hafen.de/hamburg-als-umschlagplatz>
- [29] *Hamburg militaria, Panzer, Kanonen und die Fregatten*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: <https://www.hamburg-global.de/v1.0/maps/8-hamburg-militaria#map>
- [30] Jan van Aken, Eva Grotenhuis, Katarzyna Kubiak, Annette Sawatzki, *Made in Hamburg – tödlich weltweit, Rüstungsindustrie in Hamburg*. Hamburg.
- [31] *Die wichtigsten Branchen der Metropolregion Hamburg im Überblick*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: <https://metropolregion.hamburg.de/wirtschaft-wissenschaft/branchen>
- [32] *DataCenterMap*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: <https://www.datacentermap.com/>
- [33] *Energieportal Hamburg*. Zugriff am: 12. Januar 2025. [Online]. Verfügbar unter: <https://www.energieportal-hamburg.de/>
- [34] *Hamburger Abendblatt*. "Warum das Kraftwerk Wedel jetzt doch länger am Netz bleibt." [Online.] Verfügbar: <https://www.abendblatt.de/schleswig-holstein/pinneberg/article407141613/waermewende-hamburg-warum-kraftwerk-wedel-laenger-am-netz-bleibt.html>
- [35] Frankfurter Allgemeine. "Neues Gaskraftwerk am Hamburger Hafen kann bei Stromausfall einspringen." [Online.] Verfügbar: <https://www.faz.net/aktuell/wirtschaft/hamburg-neues-gaskraftwerk-soll-stromversorgung-sicherer-machen-18098461.html>
- [36] G. Andersson *et al.*, "Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance," *IEEE Trans. Power Syst.*, Jg. 20, Nr. 4, S. 1922–1928, 2005, doi: 10.1109/TPWRS.2005.857942.
- [37] CIGRÉ Study Committee C4, *Risk Assessment and Ranking of Power System Disturbances Based on Probability and Consequences: Technical Brochure 627*, 2015.
- [38] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, "Risikoanalyse im Bevölkerungsschutz: Ein Stresstest für die Allgemeine Gefahrenabwehr und den Katastrophenschutz," Nr. 16, 2015. [Online]. Verfügbar unter: https://www.bkk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/PiB/PiB-16-risikoanalyse-bevoelkerungsschutz.pdf?__blob=publicationFile
- [39] Nationale Kontaktstelle für das Sendai Rahmenwerk beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), Hg. *Sendai Rahmenwerk für Katastrophenvorsorge 2015-2030* (2019). Bonn: Nationale Kontaktstelle für das Sendai Rahmenwerk beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), 2019. Zugriff am: 25. November 2024. [Online]. Verfügbar unter: https://www.bkk.bund.de/SharedDocs/Downloads/DE/Fremd-Publikationen/SENDAI/sendai-raahmenwerk-2015-2030.pdf?__blob=publicationFile&v=4
- [40] *BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)*, Bundesamt für Sicherheit in der Informationstechnik, 2017. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.pdf?__blob=publicationFile&v=2
- [41] Hamburger Energienetze GmbH. "LoRaWAN: Long Range Wide Area Network." [Online.] Verfügbar: <https://www.hamburger-energienetze.de/energie-der-zukunft/fortschritt-innovation/digitalisierung/lorawan>