VSW
Bundesverband

complexium

Desinformationsangriffe gegen Unternehmen

Aktuelle Fallbeispiele, Einschätzungen und ein Rahmenmodell Hybrid

Prof. Dr. Martin Grothe
Dr. Christopher Nehring
VSW-Bundesverband

Executive Summary

Eine erneute Analyse von Complexium, Dr. Christopher Nehring und VSW-Bundesverband rund zehn Jahre nach der ersten gemeinsamen Studie zu Desinformationsangriffen zeigt: Der Angriffsvektor ist heute deutlich bekannter, wird jedoch weiterhin nicht ausreichend berücksichtigt.

Dr. Nehring stellt anhand von aktuellen Beispielen dar, dass der „neue Cyberangriff" schnell, billig und wirksam ist und auf die Vorstandsagenda gehört:

- **Desinformation ist „der neue Cyberangriff" mit direktem Business-Impact:** Globale Experten und Organisationen wie das Weltwirtschaftsforum, Bitkom, Gartner oder der ehem. Chef des britischen Geheimdienstes ranken Desinformation unter die dringendsten globalen Gefahren für Sicherheit, Stabilität, Umsatz, Reputation, Talent, Lieferketten und Vertrauen. Der finanzielle Schaden liegt im zweistelligen Milliardenbereich. Deutsche Unternehmen beurteilen das Thema jedoch überwiegend als geringes bis mittleres Risiko und nehmen es nur zögerlich in Aktionspläne auf.
- **Desinformation ist billig, schnell, facettenreich, wirksam und schwer zu fassen:** Geopolitische Krisen, gesellschaftliche Polarisierung und technologische Entwicklungen (KI) begünstigen Angreifer. Beispiele reichen von russischen Einflussoperationen, chinesische Kampagnen, Cyber-Kriminellen und politischen Aktivisten. Besonders betroffene Branchen in Deutschland sind die Automobilindustrie, der Energiesektor, Rüstung und Zulieferer sowie Unternehmen mit klarer politischer Positionierung.
- **Desinformation gehört wie Cybersecurity auf die C-Level-Agenda: Governance, Lagebild, Playbooks, Übungen:** Klarer Owner/SPoC (Task Force), 360° Monitoring/OSINT & Threat Intelligence, Incident-Response für Informationsangriffe, vorgefertigte Kommunikationsbausteine, realistische Legal/Takedown-Strategie, Simulationen/Red-Teaming und Kooperation mit Plattformen/Behörden.

Aus der Erhebung des VSW-Bundesverbandes lassen sich drei Forderungen an unterschiedliche Adressaten ableiten:

- **Awareness zur Desinformation muss sowohl in Unternehmen als auch in der breiten Öffentlichkeit viel intensiver angegangen werden.** Eine breit angelegte Kampagne ist nötig um die Mitarbeiter/Bevölkerung zu sensibilisieren und die Gefahr für alle Akteure zu minimieren.
- **Zusammenarbeit ist auch hier der Schlüssel zum Erfolg.** Sei es im Unternehmen durch gemeinsame Task-Forces der involvierten Abteilungen oder zwischen staatlichen und wirtschaftlichen Stakeholdern. Desinformation ist eine Querschnitts-Gefahr und muss als solche auch behandelt werden.
- **Plattformenbetreiber müssen Verantwortung tragen und schnelle sowie einfache Gegenmaßnahmen bereitstellen.** Die sich rasch entwickelnden Technologien dürfen nicht nur von Vorteil für den Angreifer sein. Rechtliche Rahmenbedingungen sowie technologische Lösungen müssen zum Kampf gegen Desinformation weiterentwickelt werden.

Ausgehend von der Vermutung, dass die bisherige Reaktionszurückhaltung von einem Gegner durchaus gewollt sein kann, skizziert Prof. Dr. Martin Grothe ein Rahmenmodell für ein Lagebild „Hybride Angriffe“ mit einer grundlegenden Struktur dieser Angriffe sowie KI-Szenarien mit konkreten Mitigationsmaßnahmen:

- **Unternehmen als strategische Angriffsziele:** Desinformationsangriffe gegen Unternehmen sind oftmals keine isolierten Phänomene, sondern dienen als erste Stufe in einem hybriden Gesamtrahmen. Entlang von vier strategischen Stufen ist es Ziel,
  - durch die Schwächung von Unternehmen ein Grundmisstrauen aufzubauen,
  - dann eigene, d.h. gegnerische Positionen zu verfestigen,
  - um dies in politischer Beeinflussung von Wahlkämpfen und
  - später Regierungshandeln zu kapitalisieren.
- **Vierstufige Eskalationslogik (TEAM):** Systematische Kampagnen folgen oftmals einer operativen Skala:
  - Thematisierung (Schaffung von Narrativen),
  - Emotionalisierung (Appell an Angst/Wut),
  - Aktivierung (Aufruf zur Interaktion) und schließlich
  - Mobilisierung, bei der die Kampagne in reale Aktionen wie Boykotte, Proteste oder Wahlentscheidungen übergeht.

Angriffsstufen und Eskalationsskala können Dimensionen in einem Lagebild „Hybride Angriffe“ aufspannen.

- **Herausforderung der Detektion:** Da Angriffe oft dekontextualisierte, aber faktisch korrekte Informationen nutzen, ist eine Erkennung schwierig. Sie gelingt nur auf einer höheren Ebene durch die laufende Analyse großer Datenmengen auf Auffälligkeiten, atypische Muster, Themenpeaks, besondere Akteursfunktionen sowie Qualifizierung durch Analysten.
- **KI-gestützte Früherkennung (PrediCX):** Mithilfe eines prädiktiven Systems können aus einer breiten Datenbasis (Social Media, Telegram, News sowie verdichteten Sicherheitsberichten und Factbooks) frühzeitig spezifische Bedrohungsszenarien generiert werden. Dies ermöglicht es Unternehmen, im Rahmen von Digital Listening „vor die Lage“ zu kommen und Angriffe mitunter in der Entstehungsphase zu erkennen.
- **Mitarbeitende als „intelligente Sensoren“:** Eine entscheidende Maßnahme zur Stärkung der Resilienz ist neben vorbereitenden Wargames und einem laufenden Monitoring die Einbindung der Belegschaft. Sensibilisierte Mitarbeitende fungieren als Sensoren, die Angriffe frühzeitig erkennen und so nicht nur die Reputation des Unternehmens schützen, sondern auch die gesellschaftliche Widerstandskraft stärken.

Wir laufen Gefahr, diese Bedrohung nicht ernst genug zu nehmen.

Desinformationsangriffe zielen auf mehr als die Reputation. Auch Destabilisierung ist kein finales Ziel. Schwierigkeiten der Detektion und der Schadensmessung dürfen die aktive Auseinandersetzung nicht verhindern.

Inhalt

Kapitel 1

Fallbeispiele, Analysen, Gegenmaßnahmen

Von: Dr. Christopher Nehring

1.1 Einführung

Desinformation ist – gerade im Kontext hybrider Bedrohungen – von einem Randphänomen zu einer strategischen Bedrohung geworden. Dies gilt schon lange nicht mehr nur für Staaten und Gesellschaften, sondern insbesondere auch für Unternehmen und die Wirtschaft als Ganzes. Zahlreiche internationale Experten, Organisationen und Beobachter bestätigen dies: Der Global Risk Report des Weltwirtschaftsforums wählte sie 2024 und 2025 auf Platz eins der größten globalen Risiken, 2026 folgt sie unmittelbar auf Platz zwei.[1] Dabei ist nicht nur die Zahl staatlicher Akteure gewachsen, auch privatwirtschaftliche Dienstleister wie PR-Agenturen und Cybersecurity-Firmen sind heute als operative Akteure beteiligt. Gleichzeitig geraten zunehmend Unternehmen ins Fadenkreuz, insbesondere solche mit kritischer Infrastruktur, Rüstungsnähe oder wirtschaftlicher Schlüsselrolle. Laut dem Branchenverband Bitkom betrugen die wirtschaftlichen Schäden durch hybride Angriffe allein in Deutschland im Jahr 2024 rund 267 Milliarden Euro.[2] Desinformation ist dabei nicht nur ein Reputationsproblem, sondern entwickelt sich zum strategischen Angriffswerkzeug; der ehemalige Chef des britischen Geheimdienstes MI6 John Sawers schätze deshalb ein: “The dangers you have of a disinformation campaign against your company have gone up in the same way that cyber threats have gone up”[3]. Oder anders: Desinformation ist der neue Cyberangriff!

Diese Studie ordnet deshalb die Bedrohung von Desinformation für Unternehmen ein. Dazu werden in diesem Kapitel Fallbeispiele unterschiedlicher Desinformationsangriffe gegen Unternehmen vorgestellt. Im Anschluss werden darauf aufbauend die verschiedenen Formen und Angriffsvektoren definiert, besonders betroffene Branchen und Sektoren sowie wiederkehrende Narrative und Botschaften und erkannte Urheber und Angreifer identifiziert. Besonderer Raum wird gleichfalls der Frage gewidmet, wie sich die Kosten und Schäden von Desinformation für Unternehmen berechnen lassen und warum Desinformation und Cyber Influence-Angriffe gegen Unternehmen rapide zunehmen. Abschließend geht diese Analyse auf Gegenmaßnahmen, Abwehr- und Schutzkonzepte ein und stellt eine kurze Checkliste für Unternehmen vor, um sich konkret gegen Desinformationskampagnen zu wappnen.

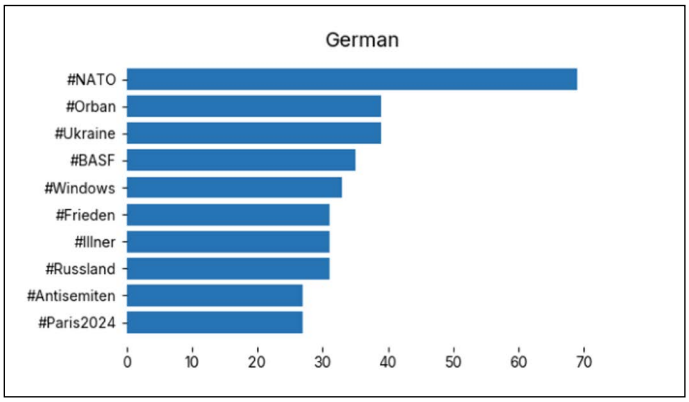
1 Siehe: https://www.weforum.org/publications/global-risks-report-2024/; https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf; https://www.weforum.org/publications/series/global-risks-report/.
2 Siehe: https://www.bitkom.org/sites/main/files/2025-09/bitkom-pressekonferenz-wirtschaftsschutz-cybercrime.pdf.
3 Siehe: https://www.linkedin.com/posts/oliver-hayes-_sir-john-sawers-the-former-chief-of-mi6-activity-7383396080245325825-46ck.

1.2 Desinformationangriffe gegen Unternehmen – Beispiele aus der Praxis

Bislang gibt es nur rudimentäre Untersuchungen zu Desinformationsangriffen gegen Unternehmen und Wirtschaft. Fehlende quantitative Datenerhebungen (sprich: die gezielte Analyse von online Räumen zur Aufklärung von Angriffen) erschwert grundsätzlich die Analyse. Beispielhafte Fälle sind deshalb oft Zufallsfunde und Mosaiksteinchen, die z.B. im Zuge von Analysen oder Datenlecks im Kontext politischer Desinformation öffentlich wurden.

1.2.1 Russland

Dies gilt z.B. für globale **russische Desinformationskampagnen,** die seit Beginn des russischen Krieges gegen die Ukraine 2022 verstärkt deutsche Unternehmen ins Visier nehmen. Ein Beispiel hier sind die Kampagnen der Moskauer PR-Agentur „Social Design Agency" (SDA), die als direkter Auftragnehmer der russischen Präsidialverwaltung globale Einflusskampagnen im online Raum durchführt. 2023 „leakten" mehrere Gigabyte interne Daten der SDA und wurden seitdem sowohl von US-Behörden, als auch von Medien und Forschung detailliert ausgewertet.[4] Hieraus ersichtlich war in Bezug auf Deutschland der klare Plan der SDA und des Kremls, das gesellschaftliche und politische Klima in Deutschland durch die Verbreitung und das Anstacheln von Angst, Unsicherheit und Chaos zu beeinflussen. Hierzu dienten gerade auch Wirtschaftsthemen wie die Auswirkungen der Post-Covid-Krise und die Auswirkungen von Wirtschaftssanktionen gegen Russland. Im Vordergrund stand dabei vor allem 2022 und 2023 eine mögliche Energiekrise sowie deren Auswirkungen auf die Wirtschaft und Einzelunternehmen. Energie- und Rohstoffintensive Branchen und Unternehmen wurden hier in Kampagnen der SDA besonders oft mit erfundenen oder übertriebenen Negativmeldungen wie Werksschließungen, Pleiten u.a. angegriffen. Der Chemieriese BASF war so z.B. zeitweise auf Platz 4 der von der SDA in ihren online Kampagnen benutzten Hashtags, besonders häufig in Kombination mit Falschmeldungen über Werksschließungen, Produktionsstops und Entlassungen.[5]



Besonders häufig tauchen deutsche DAX-Unternehmen und Vertreter von Schlüsselsektoren auch in Telegram- und anderen Kanälen auf, die im Auftrag der SDA und des Kremls Memes und Cartoons (sog. „memetische Kriegsführung") erstellen und global in Umlauf bringen. Hier geht es insbesondere um den Niedergang deutscher Traditionsmarken (insb. die Automobilindustrie) und eine Wirtschaftskrise, die die Regierungen Scholz und Merz durch ihre Unterstützung der Ukraine verursacht hätten:

4 Siehe ausführlich: https://cemas.io/blog/sda-dokumente-russlands-desinformationsstrategie/; https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence; und: https://www.psychologicaldefence.lu.se/article/beyond-operation-doppelganger-capability-assessment-social-design-agency.

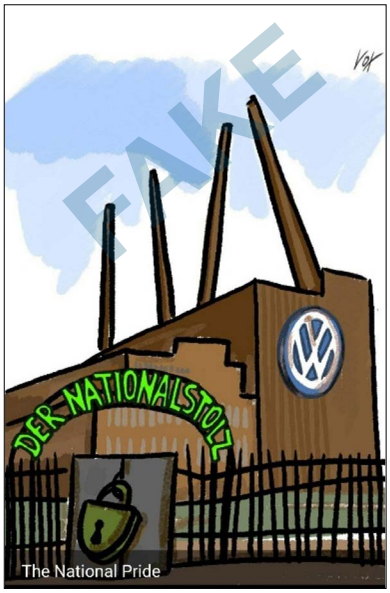
5 Siehe: https://correctiv.org/faktencheck/2022/12/15/bezahlte-falschinformation-das-volkswagen-werk-wolfsburg-wird-nicht-geschlossen/.

6

7

8

9



10

6 https://correctiv.org/faktencheck/2022/12/15/bezahlte-falschinformation-das-volkswagen-werk-wolfsburg-wird-nicht-geschlossen/.
7 Siehe: https://t.me/VoxCartoons.
8 Siehe: https://t.me/VoxCartoons
9 Siehe: https://t.me/VoxCartoons
10 Siehe: https://t.me/VoxCartoons

Mit „VoxCartoons“ schuf die SDA dabei ein spezielles Outlet für diese Form der Desinformation, von wo aus die Bilder narrativbildend und cross-medial verbreitet werden und wirken sollen. Hier geht es um simple Botschaften, die sowohl Politik und Wirtschaft in Deutschland angreifen und durch die Strahlkraft starker und globaler Marken verstärkt werden sollen.

Ein anderes verbreitetes Narrativ sind NS-Vergleiche und Andeutungen, die sich zumeist aus den Plänen der Automobilindustrie für eine engere Kooperation mit militärischer Rüstung:

11

12

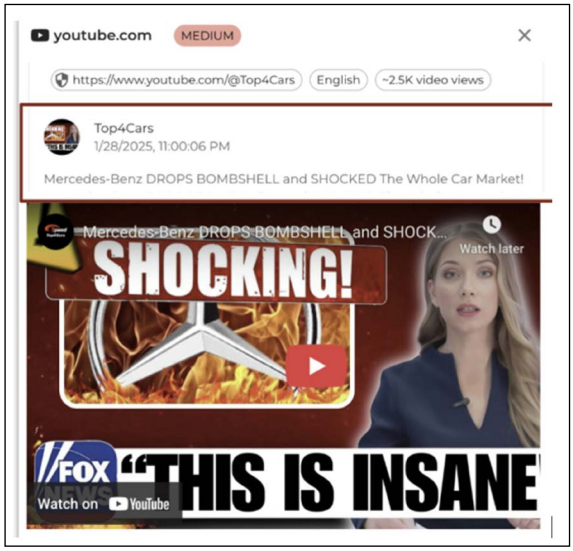
Insbesondere der Themenkomplex einer engeren Verzahnung zwischen Automobil- und Zuliefererindustrie und der Rüstung wird seit Anfang 2025 sowohl von einschlägigen russischen Medien und Kampagnen, als auch von links- und rechtsgerichteten Seiten und Accounts besonders häufig aufgegriffen. „Vom Passat zum Panzer“ oder „Porsche-Panzer“ waren dabei Motive, die unisono von der russischen „Pravda News“[13], Indymedia, Apollo News, den Grauen Panthern sowie einzelnen Aktivisten verbreitet werden. Einen Höhepunkt erreichten diese Veröffentlichungen im Vorfeld der Jahres-Hauptversammlungen 2025.

1.2.2 China

Die Automobilindustrie, sowohl in der EU als auch den USA, stand 2025 auch im Fokus anderer gesteuerter Kampagnen. Eine mehrmonatige Stichprobenanalyse von ca. 800 Videos in 14 Auto-zentrierten Youtube-Kanälen zeigte so z.B. deutliche Spuren von koordiniertem online Verhalten und in Bild und Text identischem Messaging. Die Botschaften hierbei waren u.a.: Koordinierte Negativität gegenüber US- und europäischen Automarken, Preisverfall und Absatzprobleme dieser Marken sowie die Existenzkrise der westlichen Automobilindustrie kontrastiert mit der Stärke der chinesischen Automobilindustrie. Die Urheber dieser konkreten Kampagne blieben jedoch im Dunkeln, eine direkte Verbindung zu chinesischen Akteuren war vordergründig nicht ersichtlich.

Andere Studien belegten auf Basis metrischer Netzwerkanalysen gezielte und massiv staatlich unterstützte chinesische Kampagnen, um chinesische Elektromobilität und ihre Vertreter im Konkurrenzkampf mit US- und europäischen Marken zu pushen. Botschaften waren dabei insb. die Wirkungslosigkeit von Zöllen, die minderwertige Qualität nicht-chinesischer Produkte sowie die Überlegenheit chinesischer Elektromobilität.[14] Diese wurden durch identische Textbausteine, Memes und andere Bilder sowohl durch offizielle Accounts chinesischer Vertreter (z.B. Diplomaten), Influencer, unauthentische Accounts („bots“) und staatsnahe Medien verbreitet.

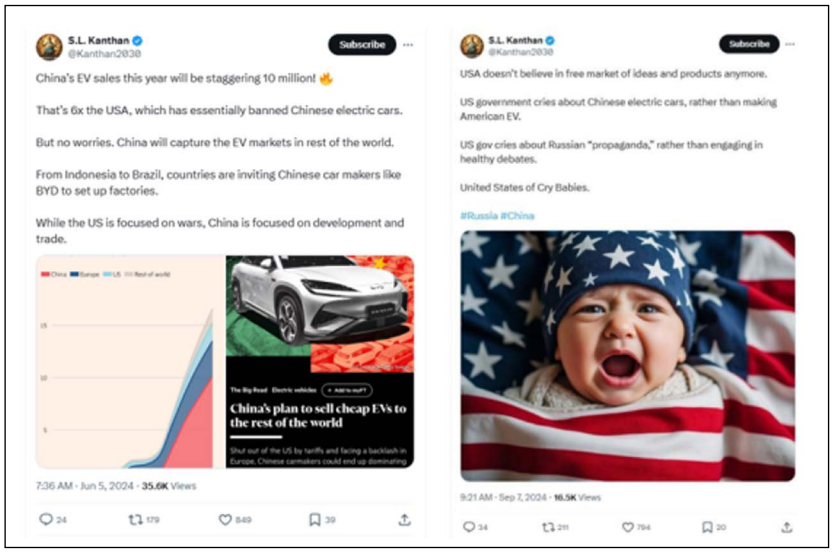
11 Siehe: https://x.com/MartinDemirow/status/1910296514401804780
12 Siehe: https://x.com/MyLordBebo/status/1907751296976777518
13 Siehe ausführlich zu „Pravda“: https://dfrlab.org/the-pravda-network/
14 Siehe ausführlich: https://www.cyfluence-research.org/post/china-s-influence-war-on-the-ev-market

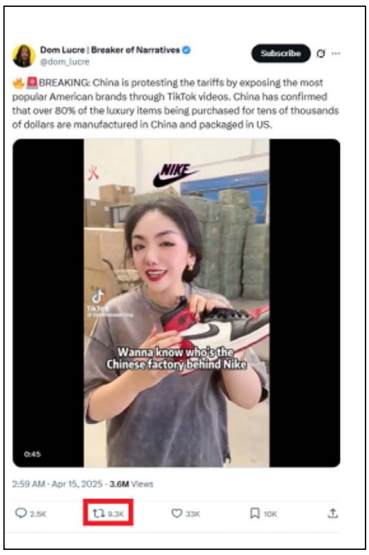


Ein anderes, besonders aufsehenerregendes Beispiel für gezielte Desinformationsangriffe gegen Unternehmen und Marken ereignete sich Anfang April 2025. Hier verbreiteten chinesische „sourcing agents" in einer koordinierten Kampagne sowohl inhaltlich, als auch bildlich gleichlautende Messages gegen den französischen Luxus-Riesen LVMH Moët Hennessy Louis Vuitton.[15] Das Narrativ hierbei lautete, dass Louis Vuitton-Handtaschen in China für ca. 50 $ produziert würden. Die koordinierte Verbreitung erfolgte über unauthentische online Accounts und Influencer über die Plattformen X und TikTok mit exakt gleichen Text- und Bildbausteinen. Diese Kampagne dauerte ca. 8 Tage und erreichte – nicht zuletzt dank künstlicher, gezielter Verstärkung – ein Millionenpublikum.

16

Medien verbreitet:

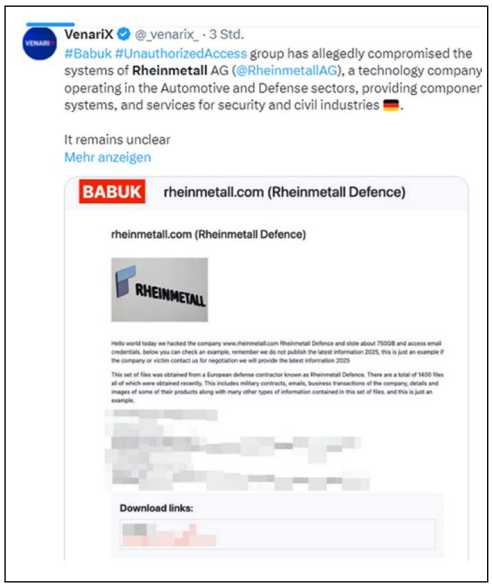




15 Siehe ausführlich: https://www.cyfluence-research.org/post/the-attack-on-luxury-brands-a-case-study-of-the-weaponization-of-the-online-ecosystem-by-china
16 Siehe ausführlich: https://www.cyfluence-research.org/post/cib-operation-targeting-western-automotive-brands

1.2.3 Cyber-Influence Angriffe

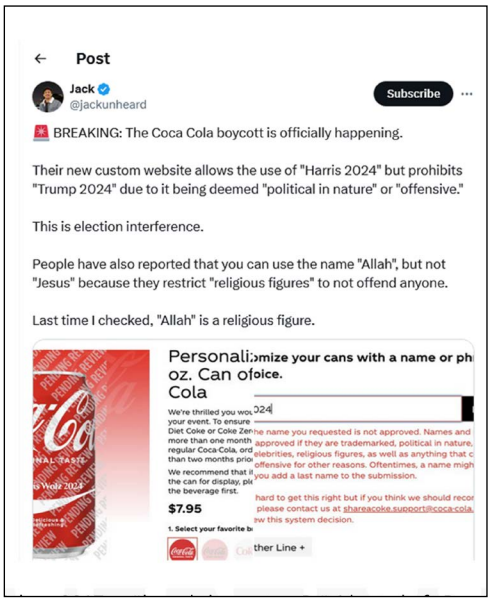
Cyber influence-Angriffe sind koordinierte Bemühungen von Angreifern, um mittels digitaler Kanäle (social media, fake websites, doxing und cyberangriffen) falsche oder irreführende Informationen zu verbreiten und Denken und Handeln zu beeinflussen.[17] Solche Angriffe unterscheiden sich in ihren Mitteln und Vorgehensweisen teilweise von traditioneller Desinformation. Ein Beispiel erlebte zum Beispiel der Rüstungskonzern Rheinmetall im April 2025 als die russische Cyber Crime-Gruppe „Babuk2“ über ihre Social Media und Darknet-Kanäle verbreitete, sie habe das Unternehmen gehackt und leake nun riesige Datensätze. Der Konzern wiederum kommunizierte, dass es sich nicht wie verbreitet um einen neuen Vorfall handele, sondern um einen bereits mehrere Jahre zurückliegenden Angriff.[18] Nichtsdestoweniger handelte es sich dabei um einen sensiblen Vorfall, da interne Daten (wenn auch veraltet) austraten; der Kontext dabei wurde mutmaßlich im hybriden Krieg Russlands verortet, da es anscheinend kein Versuch war, Geld zu erbeuten, sondern darum ging, dem Rüstungskonzern in der öffentlichen Wahrnehmung zu schaden und seine Geschäftsprozesse zu beeinflussen.



Ein anderes (mutmaßliches) Beispiel ereignete sich im Vorfeld der Bundestagswahl 2025. Hier schafften es Unbekannte, die Anzeige eines ICEs mit pro-AfD-Botschaften zu übernehmen und so den Konzern und seine Produkte ungewollt zum Träger von Wahlwerbung zu machen. Bilder der Anzeige verbreiteten sich rasch über Social Media, wobei unklar blieb, ob es sich um einen Cybervorfall handelte oder Urheber physisch die Anzeige im Zug manipulieren konnten.[19]

1.2.4 Boykott und gesellschaftliche Polarisierung

Die zunehmende Polarisierung westlicher Gesellschaften entlang bestimmter Themen (z.B. Migration, LGTBQ, Russland/Ukraine, Umwelt, Rüstung, Kriminalität, „Wokeismus“) führt zu einer starken Zunahme koordinierter Informationsangriffe und Kampagnen gegen Unternehmen und Marken. Immer öfter (wenn auch nicht immer) beruhen diese auf falschen oder gezielt dekontextualisierten Informationen, Grundlagen, Aussagen oder Ereignissen.



Eine besonders häufig auftretende Form solcher Angriffe sind online koordinierte Boykott-Kampagnen mit Übergriff in die physische Welt (z.B. durch Proteste, Rückgaben, Plakate etc.). Im US-Wahlkampf 2024 traf eine solche koordinierte Aktion z.B. den Konzern Coca-Cola.[20] In organisierten Kampagnen riefen Trump-Anhänger zum Boykott auf, weil das Personalisierungsprogramm des Konzerns, mit dem man Namen und Botschaften auf Cola-Dosen drucken kann, die demokratische Kandidaten Kamela Harris vor Donald Trump bevorzugte (bzw. letzteren nicht drucken würde). Die Anschuldigungen entbehrten dabei jeder faktischen Grundlage, erreichten jedoch ein Millionenpublikum und führte zu direkten Umsatzeinbußen.

Schon 2017, während der ersten Präsidentschaft Donald Trumps, wurde Starbucks

17 Siehe: https://www.cyfluence-research.org/post/cyfluence-the-latest-frontier-of-cognitive-warfare.
18 Siehe z.B.: https://www.tagesschau.de/wirtschaft/digitales/cybersecurity-deutsche-unternehmen-gehackt-100.html.
19 Siehe: https://www1.wdr.de/nachrichten/afd-werbung-ice-koeln-100.html
20 Siehe z.B.: https://www.newsguardrealitycheck.com/p/calls-to-boycott-coke-for-false-claim; und: https://cbsaustin.com/news/nation-world/why-boycottcocacola-was-trending-on-social-media-wednesday-coca-cola-coke-soda-12-ounce-custom-can-creator-donald-trump-kamala-harris.

ebenfalls Opfer einer koordinierten Kampagne der „far right“.[21] Nachdem sich der Konzern gegen die Migrationspolitik der Regierung ausgesprochen hatte, verabredeten sich Unterstützergruppen online zur Verbreitung gefälschter Gutscheine für Migranten, die kostenlosen Kaffee in Starbucks-Filialen versprachen. Diese Kampagne wiederholte sich mit weiteren Gutscheinen noch mehrmals.

Andere gezielt verbreitete Falschmeldungen betrafen die New Yorker Bürgermeisterwahl 2025 Zohran Mamdanis. Nach seinem Wahlsieg verbreiteten rechtsgerichtete online Accounts immer wieder gezielte Falschmeldungen über angebliche Standortschließungen, Boykotts und Wegzug verschiedener Unternehmen aus New York wegen der „kommunistischen Politik“ des neuen Bürgermeisters.[22] Auch diese Meldungen entbehrten faktischer Grundlagen.

Auch von der anderen Seite des politischen Spektrums werden ähnliche Methoden eingesetzt. Eine online Kampagne mit Boykott-Aufrufen durch Anti-Trump-Anhänger rief zum Beispiel 2025 und 2026 zum Boykott des Home Security Systems „Ring“ von Amazon auf, da es angeblich Daten an die Einwanderungsbehörde ICE weitergebe.[23]

Elon Musks Firmenimperium war ebenfalls bereits kurz nach dem Wahlsieg Donald Trumps im Fokus zahlreicher Boykott- und Negativ-Kampagnen, die auf gezielt verbreiteten Falschmeldungen beruhten. Ein Beispiel dafür waren die immer wieder koordinierten verbreiteten Falschmeldungen, große Geschäftskunden hätten nach der Wahl 2024 ihre Accounts und Werbung auf der Plattform „X“ gestoppt bzw. gekündigt und seien zur Konkurrenz „Bluesky“ gewechselt.[24]

Boykott-Aufrufe und Kampagnen entlang politischer und gesellschaftlicher Konflikte und Polarisierung gibt es nicht nur in den USA; auch in Deutschland hat dieses Vorgehen Einzug gehalten und gewinnt an Momentum. Im Fokus dabei stehen vor allem pro- oder anti-Haltungen zur AfD. Im Unterschied zu den oben vorgestellten Beispielen aus den USA variiert die Faktenlage bzw. Anteil und Ausmaß von Falschinformationen oder Verzerrungen jedoch. Ein besonders einprägsames Beispiel war die heftige Negativ- und Boykott-Kampagne gegen die Drogeriemarkt-Kette DM 2025. Die maßgeblich von Campact organisierte und im online Raum weit verbreitete Boykott-Kampagne bezog sich auf die Öffnung des Verbandes der Familienunternehmer hin zu Gesprächen mit AfD-Politikern. Sie richtete sich vor allem gegen DM, obgleich das Unternehmen bereits vorher aus dem Verband ausgetreten war.[25] Hier handelte es sich also nicht um Desinformation im klassischen Sinne, jedoch spielten verkürzte und dekontextualisierte Informationen eine große Rolle.

Bereits 2024 ereigneten sich pro- und contra Aufrufe, nachdem der Lebensmittelhänd-

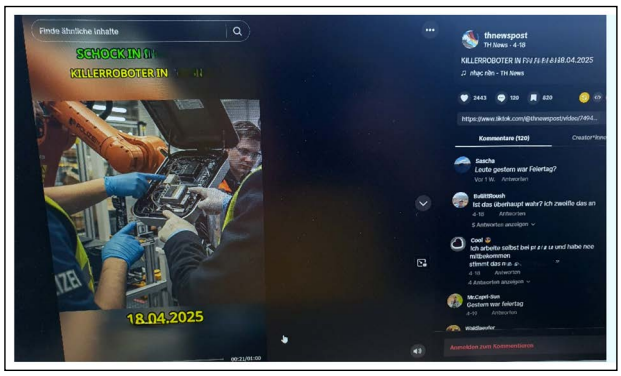
21 Siehe z.B.: https://www.businessinsider.com/fake-news-starbucks-free-coffee-to-undocumented-immigrants-2017-8.
22 Siehe z.B.: https://x.com/NewsGuardRating/status/1988023246143271326.
23 Siehe z.B.: https://www.newsguardrealitycheck.com/p/amazons-ring-faces-boycott-over-misrepresented.
24 Siehe z.B.: https://www.wsj.com/business/media/musks-x-adds-nestle-colgate-shell-other-brands-to-ad-boycott-suit-3e1c8715.
25 Siehe z.B.: https://www1.wdr.de/nachrichten/wirtschaft/verband-familienunternehmer-afd-diskussion-100.html.

ler Edeka eine mehr oder minder offene Positionierung gegen die AfD bei Landtagswahlen beworben hatte. Einerseits boykottierten einige Filialen die Aktion, andererseits riefen AfD-Anhänger zum Boykott von Edeka auf.[26]

Ein anderes, laufendes Beispiel ist die (ebenfalls von Campact mitgetragene) Kampagne gegen Theo Müller. Auch hier geht es sowohl um Boykott-Aufrufe als auch Negativ-Kampagne, die die persönliche Nähe von Konzerngründer Theo Müller zu AfD-Politikerin Alice Weidel.[27] Diese Nähe und persönliche Beziehung ist zwar faktisch belegt, nicht belegt sind hingegen finanzielle oder andere Unterstützung des Konzerns und der dazugehörigen Marken für die Partei an sich. Auch hier handelt es sich also inhaltlich nicht um eine klassische Desinformationskampagne.

Noch größere Wellen schlugen die Auseinandersetzungen um die Böttcher AG. Nachdem ein Aufsichtsratsmitglied des Bürobedarf-Großhändlers rund 1 Million Euro an die AfD gespendet hatte, kam es zu koordinierten Boykott-Aufrufen von AfD-Gegnern.[28] Dabei wurde die Spende oft fälschlich als Spende des Konzerns, und nicht einer mit dem Konzern verbundenen und in der Folge abberufenen Privatperson dargestellt. Die Firma wiederum versuchte ihrerseits den Boykottaufrufen durch koordiniertes online Verhalten ihrer Mitarbeiter zu begegnen.[29] Auch hier galt also: Noch arbeiten politisch motivierte Boykott-Kampagnen nicht komplett ohne jede Grundlage in der Realität (wie z.B. in den USA). Fakten und Informationen werden jedoch verkürzt, aus dem Kontext gerissen und die Organisation und koordinierte Verbreitung im online Raum folgt bereits den aus den USA beschriebenen Beispielen.

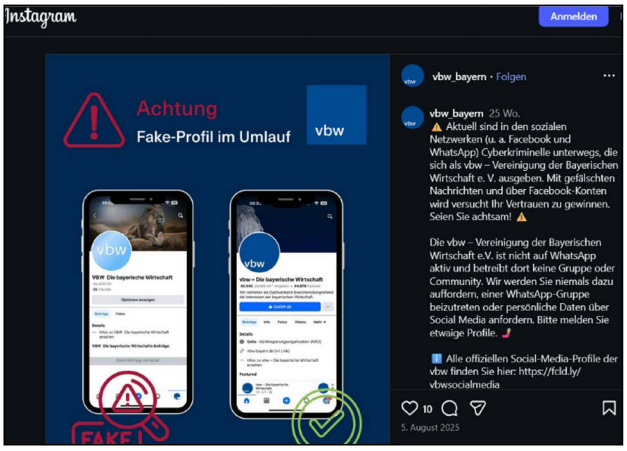
1.2.5 KI-Müll, Fake News und Verschwörungs-Kanäle

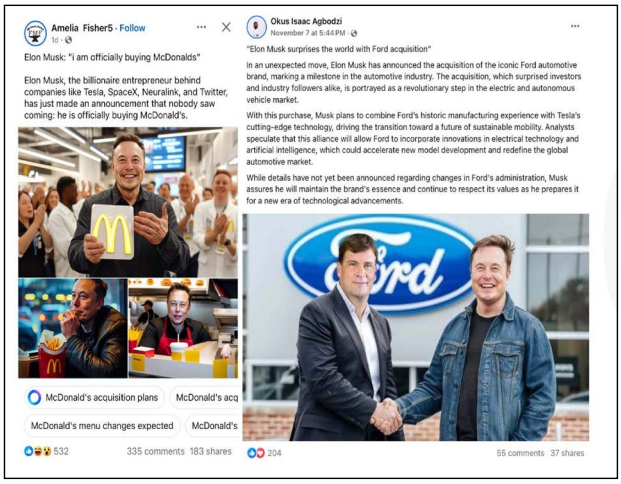


Studien belegen, dass seit dem Aufkommen von Tools zur automatisierten Erstellung von multimedialem Social Media-Content Plattformen wie TikTok, Instagram und Youtube einen enormen Anstieg von anonymisierten „Nachrichten-Kanälen“ erleben. Diese Kanäle (die es mittlerweile in fast allen Sprachen gibt) kopieren oder imitieren die Logos und den Auftritt echter Medien oder geben vor, Nachrichtenmedien zu sein. Die ausschließlich KI-generierten Inhalte hingegen sind nahezu ausschließlich frei erfunden und bespielen stark emotionalisierte und kontroverse Themen mit populistischen Botschaften.[30] Dabei gerade Unternehmen und Marken immer öfter mit den Fokus, sei es durch erfundene Anschläge auf und Unfälle in Unternehmensstandorte, erfundene Entführungen von CEOs, Pleiten und Bankrotte, Katastrophen oder dyfunktionale Technik wie kaputte Bankautomaten oder „Killer-Roboter in der Produktion“. Ob es sich dabei um politische oder politisierende Angriffe und Hintergründe, finanzielle Motive oder einfach nur Benutzung der Strahlkraft großer Marken und ihrer Bedeutung handelt, ist nur durch Untersuchungen im Einzelfall herauszufinden.

26 Siehe z.B.: https://t3n.de/news/edeka-afd-vielfalt-heidelbeer-werbung-boykott-aufrufe-1643967/.
27 Siehe: https://www.campact.de/blog/2025/09/mueller-backwerk-red-bull-unternehmer-unterstuetzen-rechtsextreme/.
28 Siehe z.B.: https://www.absatzwirtschaft.de/afd-spende-der-fall-boettcher-ag-und-was-marken-daraus-lernen-koennen-266372/.
29 Siehe z.B.: https://www.spiegel.de/panorama/mitarbeitende-sollen-boettcher-ag-im-netz-verteidigen-a-ae2bdc99-a35d-463a-9f0c-13a2eb3cbb36.
30 Siehe z.B.: https://www.tagesschau.de/faktenfinder/kontext/ki-fake-videos-100.html.

1.2.6 Betrug, Aktienkursmanipulation und Mal-Advertising





Gezielte Falschinformationen werden auch von Cyber-Kriminellen, insbesondere für Betrugsmaschen, benutzt. Ein Beispiel hierfür ist z.B. der Versuch von Betrügern, über ein dem Original der Vereinigung der Bayerischen Wirtschaft (VBW) nachempfundenes, gleichnamiges Fake-Profil gefälschte Nachrichten an Follower des Original-Accounts zu versenden, um sie zum Übertritt in eine WhatsApp-Gruppe und der Bereitgabe persönlicher Daten zu locken.[31]

Das Kopieren von Webseiten oder online Profilen und Accounts durch Angreifer ist eine Methode, die Cyber-Kriminelle und professionelle Desinformationsangreifer gerne und oft anwenden. Nicht immer ist dabei zwischen finanziell motivierten, kriminellen Handlungen und Informations- oder Cyber Influence Angriff klar zu unterscheiden. Für Unternehmen bedeutet dies jedoch eine Vielzahl von Risiken: 2022 beispielsweise verbreiteten Angreifer über ein gefälschtes Twitter-Profil des Pharmaherstellers „Eli Lilly" Falschnachrichten über angebliche kostenfreie Abgabe von Insulin, was den Aktienkurs des Unternehmens kurzeitig erheblich unter Druck setzte.[32] Noch raffinierte gingen Cyber-Kriminelle in den USA 2024 vor, als sie das Twitter-Profil der Börsenaufsicht SEC hackten und dort Falschnachrichten über Krypto-Produkte verbreiteten, was kurzzeitig zu enormen Gewinnen führte.[33] Ein anderes Beispiel waren KI-generierte Bilder und Texte, die nach dem Wahlsieg Donal Trumps 2024 die Übernahme zahlreicher Großkonzerne durch Elon Musks verkündetet und ebenfalls kurzeitig Aktienkurse beeinflussten.[34]

Besonders häufig benutzen Angreifer KI-Technologie, um sog. Deepfake-Videos von CEOs und anderen hochrangigen Vertretern von Unternehmen und Marken. Dabei wird KI eingesetzt, um prominente Personen fremde oder zweifelhafte Produkte und Services bewerben zu lassen. Der CEO des Pharmaunternehmens Bayer, Bill Anderson, war z.B. Anfang 2025 in einem solchen Video zu sehen, in dem er angeblich ein Abnehmpräparat bewarb.[35] Anfang 2026 entdeckten Journalisten gleichfalls eine Werbekampagne für ein angebliches Wundermittel, die dank verschiedener Deepfakes realer Ärzte hunderttausende Zuschauer auf TikTok fand.[36]

Obgleich nicht vergleichbar mit der Wucht staatlich gesteuerter Desinformationskampagnen, bedeuten auch solche, mittlerweile nahezu von jedermann herstellbare Fakes, ein signifikantes Risiko für Reputation, Vertrauen und Aktienkurse von Marken, Unternehmen und Führungskräften.

31 Siehe: https://www.instagram.com/p/DM94t9gNOTD/.
32 Siehe z.B.: https://www.spiegel.de/wirtschaft/unternehmen/twitter-chaos-aktienkurs-von-insulinhersteller-faellt-nach-fake-tweet-a-cd2eebad-54aa-4c33-81d9-6b37c78dd733
33 Siehe z.B.: https://www.theguardian.com/technology/2024/jan/09/sec-twitter-account-hacked-bitcoin-etf-not-approved.
34 Siehe: https://www.newsguardrealitycheck.com/p/fake-claims-of-elon-musks-latest.
35 Siehe z.B.: https://www.capital.de/wirtschaft-politik/ki-betrug--bayer-chef-bill-anderson-wurde-deepfake-opfer-35486154.html.
36 Siehe: https://correctiv.org/faktencheck/hintergrund/2026/02/13/rote-bete-kapseln-tiktok-ignoriert-deepfake-werbung-mit-aerzten/.

1.3. Formen und Angriffsvektoren von Desinformations- und Informationsangriffen auf Unternehmen

Desinformations- und Informationsangriffe können auf vielfältige Weise erfolgen. Sie nutzen dabei gezielt digitale Kommunikationskanäle, soziale Medien und manipulative Inhalte, um wirtschaftlichen, politischen oder Reputationsschaden zu verursachen. Auf Basis der vorgestellten Beispiele sowie ausführlicher Literatur- und Fallrecherchen können folgende Hauptformen und Angriffsvektoren von Informationsangriffen gegen Unternehmen identifiziert werden:

1. **Aktienkursmanipulationen**
   Falschmeldungen über Geschäftszahlen, Übernahmen oder Unternehmenskrisen können erhebliche Kursbewegungen auslösen. Besonders börsennotierte Großkonzerne sind anfällig für gezielte Fake News-Angriffe, die Investoren verunsichern und innerhalb kürzester Zeit massive Marktverluste verursachen.

2. **Image- und Reputationsangriffe**
   Unternehmen werden bewusst durch falsche Narrative diskreditiert – etwa durch Gerüchte über Fehlverhalten von Führungskräften, angebliche Skandale oder verfälschte Unternehmensentscheidungen. Solche Angriffe zielen auf das Vertrauen von Kunden, Investoren und Mitarbeitern.

3. **Durch Falschinformation herbeigeführte Boykott-Aufrufe**
   Insbesondere gesellschaftliche und politische Polarisierung entlang bestimmter Streitthemen (wie z.B. Migration oder Umwelt) führte in der jüngsten Vergangenheit zu koordinierten Boykott-Aufrufen, die mit gezielten Falschmeldungen begründet und verbreitet wurde. Aufrufe, Produkte oder Dienstleistungen nicht mehr zu kaufen, verursachen unmittelbare Umsatzverluste und wirken sich zugleich langfristig negativ auf die Marke aus.

4. **Fake-Bewertungen und manipulierte Reviews**
   Über Plattformen wie Google, Amazon oder TripAdvisor werden gezielt und koordiniert gefälschte Kundenbewertungen verbreitet, die das Image von Produkten und Unternehmen schädigen oder Wettbewerber begünstigen. Diese Form des Angriffs ist besonders schwer kontrollierbar, da sie mit relativ geringem Aufwand in großer Zahl durchgeführt werden kann, durch KI sehr leicht automatisierbar ist und als kommerzielle Dienstleistung breit angeboten wird.

5. **„Malvertising“ und Fake-Werbung**
   Angriffe erfolgen auch über manipulierte Anzeigenkampagnen, in denen Deepfake-Videos oder gefälschte Werbematerialien verbreitet werden. Dabei erscheinen z.B. Unternehmensvertreter scheinbar als Unterstützer fremder Produkte oder fragwürdiger Botschaften, was zu einem erheblichen Vertrauensverlust führt.

6. **Produktivitätsverluste durch Gesundheitsdesinformation**
   Falschinformationen zu Gesundheitsthemen – etwa Impfungen oder Medikamenten – können dazu führen, dass Mitarbeiter verunsichert werden, häufiger erkranken oder durch Angst und Misstrauen weniger leistungsfähig sind. Unternehmen tragen in der Folge höhere Kosten durch Krankenstände und sinkende Produktivität.

7. **Politisierung und Polarisierung im Unternehmen**
   Angriffe können gezielt den Betriebsfrieden stören, indem gesellschaftliche oder politische Streitthemen (z.B. Russland oder Gaza) durch Desinformationskampagnen in die Belegschaft getragen werden. Interne Konflikte und Misstrauen beeinträchtigen dann das Arbeitsklima und können zu Effizienzverlusten führen.

8. Angriffe auf Vertrags- und Auftragsvergaben

In Ausschreibungsprozessen können gezielte Falschinformationen genutzt werden, um Konkurrenten auszuschalten oder ein Unternehmen in Misskredit zu bringen. Dies führt zu direkten wirtschaftlichen Schäden durch verlorene Aufträge und untergräbt die Wettbewerbsfähigkeit.

9. Betrug durch Informationsangriffe

Informationsmanipulation wird auch eingesetzt, um Unternehmen finanziell direkt zu schädigen – etwa durch CEO-Fraud, manipulierte Zahlungsanweisungen oder den Einsatz gefälschter Dokumente.

Solche Angriffe können dann in verschiedenen Formen auftreten. In der Praxis lassen sich in der jüngsten Vergangenheit verschiedene Arten beobachten: Zum einen stehen großflächige, koordinierte Kampagnen, die oft von politischen Akteuren wie z.B. staatlichen russischen Angreifern durchgeführt werden. Hier können Unternehmen und Marken gezielt ins Visier genommen werden, wie beispielsweise die oben beschriebenen chinesischen Kampagnen über Elektromobilität (staatlich unterstützt) oder der koordinierte Angriff gegen Luxusartikelhersteller (kein Beweis für staatliche Unterstützung) zeigen. Wie die ausgeführten Beispiele der russischen „SDA“ oder des „Pravda-Netzwerks“ zeigen, werden Unternehmen zur Zielscheibe, weil sie gesellschaftlich und politisch herausgehobene Bedeutung haben und im Kontext dieser Narrative zur Zielscheibe werden. Hierbei geht es, wie z.B. bei den russischen Angriffen dieser Akteure gegen die deutsche Energie- oder Automobilbranche, vor allem um die Erzeugung gesellschaftlicher Angst und Krisen, die wiederum politische Ziele und Kampagnen unterstützen sollen.

Auf Desinformation und politisch motivierten Informationsangriffen basierte Boykott-Aufrufe müssen ebenfalls als gezielte Kampagnen betrachtet werden. Diese gehen oft von organisierten Unterstützern politischer Parteien und Kandidaten aus, beginnen zumeist im online-Raum und sollen nach Möglichkeit zu Aktionen in der physischen Realität führen. Solche Aufrufe und Aktionen sind zumeist kurzfristiger als lang angelegte staatlich organisierte Kampagnen.

Eine andere Form sind Fake News Seiten und Kanäle, die Verschwörungs- und Sensationsmeldungen teils über vollautomatisierte Social-Media-Kanäle verbreiten. Informationsangriffe auf Unternehmen und ihre Vertreter gehören zu einem neuen Geschäftsmodell, bei dem über Falschmeldungen z.B. über angebliche Terroranschläge, Insolvenzen oder Entführungen die Bekanntheit von Marken und Personen nutzen, um Reichweite und Viralität zu erzeugen.

1.4. Besonders betroffene Branchen, Sektoren und Unternehmen in Deutschland

Eine genaue Bestimmung der größten und häufigsten Opfer von Desinformationsattacken ist aus vielen Gründen schwierig: Einerseits gibt es aufgrund eines fehlenden Dauer-Monitorings wenig empirisch belastbare Daten über Desinformationsangriffe, sondern oft nur Einzelfälle, Stichproben und Mosaiksteinchen. Darüber hinaus nehmen unterschiedliche Angreifer unterschiedliche Unternehmen zu unterschiedlichen Zeitpunkten ins Visier. Geopolitische Faktoren (z.B. die Rolle bestimmter Unternehmen in lokalen oder regionalen Konflikten) beeinflussen die Anzahl und Auswahl besonders betroffener Branchen und Unternehmen dabei ebenso, wie innenpolitische und gesellschaftliche Konflikte (und die Positionierung von Unternehmen in demselben). Und schließlich erschwert auch die Vielfalt der Angriffsarten zwischen klassischen Cyber Influence Attacks auf die Reputation von Marken bis hin zu Boykott-Aufrufen innländischer politischer Aktivisten die Frage, welche Unternehmen besonders betroffen sind.

Aus den oben behandelten Fallbeispielen lassen sich deshalb zwar durchaus einige Aussagen darüber ableiten, welche Branchen und Unternehmen in Deutschland in der jüngsten Vergangenheit besonders betroffen waren; zur Verallgemeinerung dieser Aussagen sind jedoch ressourcenintensive, repräsentative Daten- und semantische Analysen notwendig. Wie die oben ausgewerteten Beispiele russischer Desinformationskampagnen seit der Invasion der Ukraine 2022 zeigen, standen 2022 und 2023 **Energieunternehmen sowie und Rohstoff-basierte Branchen und Sektoren** im Fokus. Auffällig war hier zum Beispiel die Häufigkeit, mit der der Chemie-Riese BASF in den Desinformationskampagnen der „Social Design Agency“ figurierte. Dies erklärte sich offenbar auf den damals gesellschaftlich virulenten und heftig debattierten Fragen, wie sich die Sanktionen und das Embargo von Gas und Öl auf die Wirtschaft und eine potentielle Energieknappheit auswirken würde. 2024 und 2025 hingegen, so legt z.B. eine Key-Word-Search des russischen „Pravda-Netzwerks“ da, steht die deutsche Automobilindustrie besonders im Fokus russischer Narrative. Die Gründe hierfür sind einmal die strategische (und damit auch politische) Bedeutung der Automobilindustrie für die deutsche Wirtschaft insgesamt; weiterhin zielt russische Desinformation auf die Verschärfung bzw. Ausschlachtung der Krise des Automobilsektors ab, um politische und gesellschaftliche Unzufriedenheit und Spaltung zu erzeugen und zu verstärken; und schließlich stehen die Kooperation zwischen **Automobilindustrie** und Rüstungsindustrie, wie sie seit Anfang 2025 öffentlich besprochen und bekannt wurde, im Fokus russischer Angreifer. Die **Rüstungsindustrie** und ihre Zulieferer sind ohnehin ein Dauer-Ziel für russische Kampagnen, wobei es einmal um direkte Waffenlieferungen an die Ukraine geht und andererseits um die Schwächung von Verteidigungskapazitäten der NATO in einem potentiellen Konflikt mit Russland.

Unternehmen und Marken der **Finanzindustrie** (insbesondere Banken) hingegen tauchen regelmäßig in Fake News-Kanälen auf TikTok, Instagram und Youtube auf, von denen manche dank digitaler Spuren nach Asien zurückzuverfolgen sind. Hintergrund ist hier, dass über Schock-Videos und Horror-News wie Finanzkrisen, Bankenpleiten oder manipulierten Geldautomaten einerseits gesellschaftliche Panik und Angst und andererseits Klickzahlen und Viralität erzeugt werden soll.

Nicht branchenspezifisch, aber generell zunehmend, sind Vorfälle von Boykott-Aufrufen und Reputationsattacken gegen Unternehmen und Marken, die sich in aktuellen politischen und gesellschaftlichen Auseinandersetzungen in Deutschland öffentlich positionierten. Bekannte Fälle, wie zum Beispiel Boykott-Aufrufe und Auseinandersetzungen um DM, Müller Milch, Böttcher oder den Verband der Familienunternehmer. Da es hierbei nicht vordergründig um Unternehmen geht, sondern vor allem um die Verbreitung politischer und gesellschaftlicher Botschaften, sind Großunternehmen und Marken mit Strahlkraft – auch aus dem Ausland –besonders betroffen.

1.5 Narrative und Botschaften

Desinformationsangriffe laufen nicht immer gleich ab und die verbreiteten Botschaften und Narrative variieren; nichtsdestoweniger kann sowohl aus den oben beschriebenen **Fallbeispielen,** als auch der Umfrage im Zuge dieser Studie eine Reihe von wiederkehrenden Narrativen der vergangenen Jahre identifiziert werden:

- Wirtschaftlicher Niedergang, Abschwung, Krise, Standortschließungen, Produktionsverlagerung und Entlassungen
- Chaos & Angst in Deutschland, z.B. durch (falsche) Angriffe, Attacken, Anschläge, Unfälle in Unternehmen
- Kooperation ziviler Unternehmen mit Rüstung (insb bei Verbindung in die Ukraine): Militarismus, NS-Vergangenheit, Kriegsgefahr, Kosten
- Energie-Unterversorgung und Energieknappheit
- „Kulturkämpfe“ um die Themen Migration, Gender, Umwelt
- Anti-Kapitalistische Narrative
  (z.B. Korruption, Verschwendung, Ausbeutung der Mitarbeiter)
- Boykott-Aufrufe wegen pro- oder anti-AfD-Haltung
- Überlegenheit chinesischer Produkte

1.6 Urheber, Angreifer und Akteure

Die Urheber hinter Desinformationsangriffen und Kampagnen zu identifizieren, erfordert kleinteilige und aufwendige Untersuchungen mittels OSINT (Open Source Intelligence) sowie Netzwerk- und semantischer und narrativer Analysen durch hochspezialisierte Software. Dies war im Kontext dieser Studie nicht möglich. Nichtsdestoweniger verweisen insbesondere die hier beschriebenen Fallbeispiele sowie die geführten Interviews (siehe die Umfrage dieser Studie) auf eine erkennbare Gruppe von Akteuren:

- Feindliche Staaten: insb. Russland und China, aber auch Iran, Nordkorea (global auch Türkei sowie einige arabische Staaten bekannt)
- Extremistische Parteien, Politiker und Unterstützer: hier insbesondere die extreme Rechte mit großem digitalen Mobilisierungspotential, digitaler Infrastruktur wie Bots, deepfake-personas, Influencern sowie koordiniertem online Verhalten etc. In Deutschland treten jedoch AfD-Gegner ebenfalls sehr aktiv im online Raum mit Boykott-Aufrufen und koordiniertem Verhalten auf (ohne dabei immer auf Faktengrundlage zu agieren)
- Private Desinformations-Service-Dienstleister: Private PR- & Cybersecurity-Dienstleister sowie privat organisierte Bot-, Betrugs- und Content-Farmen priv. Dienstleister, die Desinformation als Dienstleistung für Staaten, Organisationen und Unternehmen anbieten und durchführen
- (Cyber-)Kriminelle: Kriminelle Netzwerke, die für Betrug und Manipulation massenhaft falsche Webseiten, Emails, Produkte, Stellenanzeigen etc. erstellen und verbreiten
- Mitarbeiter: Mitunter treten unzufriedene ehemalige oder aktuelle Mitarbeiter als Ursprung und Verbreiter gezielter Falschinformationen über Marken, Unternehmen, Produkte und andere Mitarbeiter auf
- (Einzel- oder lose organisierte) Aktivisten: diese treten in Deutschland öfter im linken Spektrum auf und können lokal und zeitlich begrenzt wirkungsmächtig sein.

1.7 Die Gründe: Warum nehmen Desinformation gegen Unternehmen zu?

Die Zunahme von Desinformationskampagnen auf Unternehmen ist Ausdruck eines sich verändernden geopolitischen, gesellschaftlichen und technologischen Umfelds, in dem Informationen und Deutungshoheit zu einem zentralen Macht- und Einflussfaktor geworden sind. Mehrere Entwicklungen wirken hier zusammen und verstärken sich gegenseitig:

1. Ein wesentlicher Treiber für Desinformation sind **sich verstärkende geopolitischen Spannungen.** Der russische Angriffskrieg gegen die Ukraine, der strategische Wettbewerb zwischen den USA und China sowie z.B. Konflikte im Nahen Osten haben Desinformation einen enormen Auftrieb gegeben. Staaten, aber auch staatsnahe Akteure, nutzen gezielt Informationsoperationen, um politische, wirtschaftliche oder gesellschaftliche Ziele zu verfolgen. Unternehmen geraten dabei zunehmend in den Fokus, sei es als Symbol westlicher Werte, als wirtschaftliche Stellvertreter oder als Hebel zur Destabilisierung von Machträumen, Gesellschaften und Märkten.

2. Hinzu kommt eine zunehmende **gesellschaftliche Polarisierung**, vor allem entlang von links-rechts bzw. liberal-anti-liberaler Konfliktlinien. Die Trennlinien zwischen politischen Lagern verlaufen heute schärfer, und viele gesellschaftliche Debatten werden nicht nur hochemotional und aggressiv, sondern auch durch gezielte online Kampagnen mit Desinformation geführt. Marken und Unternehmen werden dabei immer häufiger zum Schauplatz ideologischer Auseinandersetzungen. Durch tatsächliche oder angebliche Positionierungen oder auch nur Zuschreibungen von Unternehmen bei Genderfragen, Klimaschutz, Migration oder Haltung zu internationalen Konflikten, werden Unternehmen und Marken rasch in politische Lager eingeordnet und dadurch Teil der Auseinandersetzung. Desinformation wird in diesem Kontext gezielt eingesetzt, um Vertrauen zu untergraben, Empörung zu erzeugen oder Konsumenten gegeneinander aufzubringen. Oftmals wird jedoch auch die Strahlkraft globaler Marken von politischen Aktivisten genutzt, um ihren Aktionen und Botschaften größere Reichweite zu verleihen. Mitunter verbinden sich hier auch politische mit handfesten finanziellen Interessen.

3. Ein dritter Faktor ist die **rasante Entwicklung digitaler Technologien,** insbesondere die Auswirkungen Künstlicher Intelligenz (KI). Wie auch z.B. ChatGPT-Mutterfirma OpenAI in ihren Threat Intelligence Reports beschreibt, wirken diese Tools als „booster“ und „supercharger“ für Desinformations- und Cyber Influence Operationen.[37] Digitale Technologien haben eine Vielzahl von verstärkenden Effekten sowohl für die Erstellung von Desinformationsinhalten (also z.B. Bilder, Videos und Texte), als auch für deren Ausspielung und damit die digitale Infrastruktur von professioneller Desinformation (z.B. automatisierte Seiten, Profile und Accounts) mit sich gebracht. Wo früher erheblicher Aufwand nötig war, genügen heute frei verfügbare Tools, um täuschend echte Inhalte zu produzieren. Deepfakes, automatisierte Social-Media-Profile oder KI-Agenten können in kürzester Zeit glaubwürdige, emotional aufgeladene Falschinformationen generieren und verbreiten. Dies hat zur Folge, dass Eintrittsbarrieren, Hemmungen, aber auch Kosten und Risiken für professionelle Desinformationskampagnen radikal gesunken sind. Dies führt dazu, dass private Desinformationsdienstleister mit enormen Gewinnspannen arbeiten können.

4. Angreifer bekommen jedoch nicht nur immer bessere Tools, sondern werden auch unterstützt durch den **Wandel der Medien- und Informationslandschaft.** Klassische, redaktionell verantwortete Medien verlieren an Reichweite und Vertrauen, während algorithmisch gesteuerte Plattformen und soziale Netzwerke zum Hauptmedium werden. Inhalte werden nicht mehr aufgrund journalistischer Relevanz verbreitet, sondern nach ihrer Fähigkeit, Aufmerksamkeit und Interaktion zu erzeugen. So entstehen Filter-

37 Siehe: OpenAI (hg.): Disrupting malicious uses of AI: an update, Oktober 2025 (https://openai.com/global-affairs/disrupting-malicious-uses-of-ai-october-2025/).

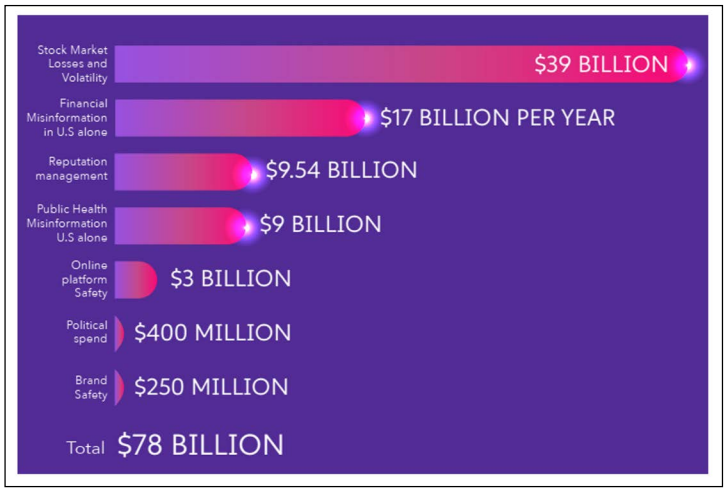
blasen und Echokammern, in denen sich bestimmte Narrative nahezu ungestört verbreiten und gegenseitig verstärken können. Dieser Wandel sorgt dafür, dass Desinformations-Angreifer ihre Inhalte leicht veröffentlichen, amplifizieren und monetarisieren können.

Die Kombination aus geopolitischer Unsicherheit, gesellschaftlicher Polarisierung, technologischem Fortschritt und einer fragmentierten Informationslandschaft schafft ein Umfeld, in dem Desinformation gegen Unternehmen zunehmend wirksam und attraktiv werden. Sie sind Ausdruck einer neuen Form des Wettbewerbs um Deutungshoheit, Vertrauen und Glaubwürdigkeit.

1.8 Was kostet das? Finanzielle Schäden durch Informationsangriffe & Desinformation

Das Weltwirtschaftsforum (WEF) spricht in einem aktuellen Beitrag von 2025 von einem wachsenden Risiko für Unternehmen weltweit, das durch gezielte Desinformationskampagnen entsteht. Die Relevanz für Investoren, Kunden und die Unternehmensführung selbst nehmen dabei stetig zu.[38] Die finanziellen Auswirkungen und eine wirtschaftliche Bewertung von Desinformation auf Unternehmen genau zu berechnen, sind jedoch herausfordernd. Der wirtschaftliche Schaden durch Desinformationsangriffe lässt sich oft schwer in Zahlen fassen, da vor allem langfristige Folgen von Desinformation wie Imageverluste, Umsatzrückgänge oder ein Ausschluss von Aufträgen oft nur sehr schwer zu messen sind.

Trotz dieser Unsicherheiten liefern Studien der Universität Baltimore und CHEQ („The Economic Cost of Fake News“) aus dem Jahr 2019 erste belastbare Schätzungen: Demnach belaufen sich die durch Desinformation verursachten Schäden weltweit auf rund 78 Milliarden US-Dollar jährlich. Laut dieser Studie setzen sich diese Schäden wie folgt zusammen:



- 39 Milliarden USD durch Kursschwankungen und Verluste an den Kapitalmärkten
- 17 Milliarden USD durch Finanzdesinformation (z. B. fehlerhafte Anlageberatung)
- 9 Milliarden USD durch Gesundheits-Desinformation (z. B. Anti-Impfkampagnen)
- 9,54 Milliarden USD an Kosten für Social Media- und Reputationsmanagement
- 3 Milliarden USD durch Desinformationsinhalte auf Onlineplattformen
- 250 Millionen USD durch Markensicherheit sowie
- 400 Millionen USD an globalen Wahlkampf-Ausgaben für gezielte Fake-News-Verbreitung.[39]

In einem anderen Beispiel ebenfalls aus dem Jahr 2019 demonstrierte der Think Tank „Recorded Future“ auf der Mikroebene wie leicht und billig Informationsangriffe gegen Unternehmen schon damals zu haben waren.[40] In einem **praktischen Selbstversuch** gründeten sie eine (fiktive) Firma in UK und beauftragten anschließend zwei private russischer Dienstleister über das Darknet. Beide Dienstleister stellten ausführliche

38 Siehe: https://www.weforum.org/stories/2025/07/financial-impact-of-disinformation-on-corporations/.
39 Siehe: https://s3.amazonaws.com/media.mediapost.com/uploads/EconomicCostOfFakeNews.pdf, S. 13.
40 Siehe: https://www.recordedfuture.com/research/disinformation-service-campaigns.

Preis- und Arbeitsmodelle vor, die von selbst betriebenen Webseiten, Pressekontakten und gekauften Presseartikeln sowie online bots und Trolle bereit. Die in Rechnung gestellten Kosten für die beiden 6–8-wöchigen Desinformations-Kampagnen beliefen sich auf gerade einmal 6.000 US-Dollar.

Während die Kosten auf der Angreifer-Seite also gering sind und aufgrund technologischer Entwicklungen weiter sinken, sind die Kosten und Schäden auf der Opfer-Seite hoch. Die obige Aufschlüsslung zeigt, dass die Studie von 2019 einige kostenintensive Formen von Informationsangriffen auf Unternehmen, wie z.B. durch Falschinformationen herbeigeführte Boykott-Aufrufe, Werbe-Schwindel, Deepfake-Betrug, gefälschte Bewertungen sowie interne Konflikte und Produktivitätsverluste durch demotivierte, polarisierte oder fehlinformierte und verunsicherte Mitarbeiter, (noch) gar nicht berücksichtigt. Ebenfalls aufgrund des Zeitpunkts der Studie nicht miteinbezogen wurden die Auswirkungen der KI-Revolution im Bereich Informationsangriffe, die Kosten, Hemmschwellen und Eintrittsbarrieren für Angreifer senken und gleichzeitig Angriffe skalieren. Die errechneten 78 Milliarden US-Dollar können daher als Richt- und Orientierungswert genommen werden. Der KI-Entwickler Anthropic, zum Beispiel dokumentierte 2025 den Fall einer PR-Firma aus Südostasien, die mithilfe des Chatbots „Claude“ automatisierte Desinformationskampagnen durchführte.[41] Und auch das US-Heimatschutzministerium warnt in einem Bericht 2025 eindringlich vor dem Einsatz autonomer KI-Agenten, die Desinformationsangriffe – etwa durch CEO-Fraud, Deepfakes oder Fake-Bewertungen – in großem Stil automatisieren und skalieren könnten.[42] Darüber hinaus muss natürlich auch immer mitbedacht werden, dass nicht nur direkte Schäden (z.B. Imageschaden oder Auftragsverlust) entstehen, sondern auch indirekte wie z.B. die Kosten für Krisenmanagement oder rechtliche Maßnahmen. Das IT-Beratungsunternehmen Gartner schätzt deshalb, dass Unternehmen alleine in den USA bis zum Jahr 2028 jährlich mehr als 30 Milliarden US-$ ausgeben werden müssen, um mit Desinformationsangriffen umzugehen.[43]

Demgegenüber weicht die Einschätzung der Auswirkung von Desinformation durch die deutschen Unternehmen, die an der Umfrage dieser Studie teilnahmen, deutlich ab: 30% gaben an, keine Erfahrung zu haben, 27% sahen nur geringe Auswirkungen, 26% mittel schwere Auswirkungen und nur 17% sahen starke Auswirkungen (siehe die Umfrage dieser Studie).

1.9 Gegenmaßnahmen, Abwehr- und Schutzkonzepte

Desinformation ist ein komplexes, multidimensionales Phänomen, das ebenso vielschichtige Lösungen, Abwehr- und Schutzmaßnahmen auf mehreren Ebenen bedingt. Für Staaten und Gesellschaften als Ganzes haben Experten in den vergangenen Jahren über 20 Einzelmaßnahmen identifiziert, die z.B. politische, wirtschaftliche, rechtlichen, kommunikative oder Cyber-Maßnahmen umfassen.[44] Unternehmen und Einzel-Organisationen können und müssen jedoch anders vorgehen als Staaten. Der folgende kurze Überblick bezieht sich daher also nicht auf das Phänomen Desinformation als Ganzes, sondern spezifisch auf Unternehmen und andere wirtschaftliche Organisationen:

Wichtig ist hierbei, das am Anfang eines Schutzkonzeptes eine klare Zielstrategie stehen sollte. Klar ist, dass Desinformation nicht verschwinden wird bzw. komplett gestoppt werden kann, deshalb ist wichtig zu definieren, was durch Schutzmaßnahmen erreicht werden soll: Sollen Narrative und Angriffe möglichst klein gehalten werden?

41 Siehe: Anthropic (hg.): Operating Multi-Client Influence Networks Across Platforms, April 2024 (https://www.anthropic.com/news/detecting-and-countering-malicious-uses-of-claude-march-2025).

42 Siehe: US Department of Homeland Security, Science & Technology Department: Impacts of Adversarial Use of Generative AI on Homeland Security, in: January 2025 Preparedness Series, S. 63 (https://www.dhs.gov/archive/science-and-technology/publication/impacts-adversarial-use-generative-ai-homeland-security).

43 Siehe: https://www.gartner.com/en/newsroom/press-releases/2025-10-21-gartner-predicts-enterprise-spending-on-battling-misinformation-and-disinformation-will-surpass-30-billion-dollars-by-2028.

44 Siehe z.B.: https://globalanalytics-bg.org/2023/12/06/briefing-paper-countering-disinformation-an-evaluation-of-the-institutional-approach-of-governments/.

Sollen Angreifer identifiziert und gestoppt werden? Sollen Mitarbeiter, Führungskräfte, Kunden und Öffentlichkeit möglichst resilient gegen Desinformation gemacht werden? Sollen Angreifer abgeschreckt werden? Soll der betreffende Informationsraum dominiert werden?

In Abhängigkeit der Zielstrategie können Tools und Kompetenzen aufgebaut werden. Wichtig ist, dass Desinformation heute zumeist cyber enabled information threats sind, die cyber enabled information responses brauchen. Dafür brauchen Organisationen einen Werkzeugkasten, aus dem sie verschiedenen Maßnahmen und Tools wählen und angepasst an Eskalationsgrad von Maßnahmen, Ressourcen, Zielen und Angriffsformen umsetzen können. Dazu empfiehlt es sich ähnlich wie bei traditionellen Cyberangriffen einen Incident Response Plan zu erarbeiteten, zu proben und ständige anzupassen.

Auf dieser Grundlage lassen sich konkrete, multidimensionale Gegenmaßnahmen ableiten, die – je nach Zielstrategie – modular eingesetzt und kombiniert werden können. Wichtig ist dabei, dass Unternehmen und Organisationen frühzeitig und bewusst in ihre Fähigkeit investieren, Desinformationsangriffe zu erkennen, einzuordnen und zu begegnen:

Zunächst empfiehlt es sich, das Thema zentral in einer Einheit bzw. Ansprechpartner als single point of contact (SPoC) zu bündeln und „ownership" für das Thema zu haben. Dies kann ein Beauftragter, eine Arbeitsgruppe oder Task Force sein. Im angelsächsischen Wirtschaftsraum etabliert sich im letzten Jahr z.B. auch die Position des „Chief Trust Officers" (dessen Aufgaben oft im Zusammenhang mit KI-Implementierung und Vertrauensmaßnahmen stehen). Da Desinformation ein Querschnittsthema ist, das sowohl Corporate Security, Cybersecurity, PR & Kommunikation, Legal, HR & Personal und natürlich die C-Suite betrifft, bietet ein SPoC den Vorteil, stehende Abstimmungs- und Austauschkanäle, Meldeketten, Informationsfluss sowie klare Entscheidungswege zu etablieren. Als ein best practice-Beispiel kann hier z.B. die „Deepfake-Task Force" der Bayer AG genannt werden.[45]

Bei den Maßnahmen stehen proaktive Awareness und Sensibilisierung am Anfang. Mitarbeitende, Führungskräfte und externe Stakeholder müssen über die Gefahren, Funktionsweisen, Angriffsformen, Ziele und Folgen von Desinformation im Bilde sein, um resilienter zu werden und adäquat reagieren zu können. Zur Umsetzung bieten sich hier Schulungen, Vorträge, Workshops, Simulationen und interaktive „War Games" an. Wie die Umfrage dieser Studie ergab, ist die Notwendigkeit solcher Schulungen – insbesondere für Mitarbeiter – bereits in den Unternehmen angekommen und 73% der Befragten gab an, solche Schulungen bereits durchzuführen.

Ebenfalls essenziell ist ein solides Lagebild: Unternehmen müssen in der Lage sein, Bedrohungen und Entwicklungen frühzeitig zu erkennen, einzuordnen und auf dieser Basis abzuwehren. Dazu gehören Maßnahmen wie Social Listening, Monitoring von Plattformen und Kanälen, Threat Awareness, Threat Intelligence und gezielte OSINT-Recherche (Open Source Intelligence). Diese Fähigkeiten sind besonders wichtig, um gezielte Desinformationsangriffe, Deepfakes, Narrative und Angreifer frühzeitig zu identifizieren und richtig einzuordnen. Die Notwendigkeit dieser Maßnahmen wird auch durch die im Zuge der Umfrage dieser Studie geäußerten Wünsche und Forderungen unterstützt: Ein Lagebild und der strukturierte Austausch zwischen Unternehmen wurde hier besonders hervorgehoben (siehe die Umfrage dieser Studie).

Erst auf Basis eines fundierten Lagebildes können (reaktive) Maßnahmen ergriffen werden. Besonders häufig gehören dazu rechtliche Schritte, insb. sog „Takedown-Anfragen", bei denen Plattformen, Provider, Hosts etc. auf juristischem Wege (Anwalt, Staatsanwalt, Gerichte) aufgefordert werden, bestimmte Inhalte (Profile, Posts, Webseiten etc.) zu löschen. Im deutschen Rechtsraum ist dies wahrscheinlich das Standard-Vorgehen, dessen Wirkung nach Expertenmeinung jedoch begrenzt ist: Einerseits können Takedowns im globalen Maßstab nur schwer erzwungen werden, insbeson-

45 Siehe: https://prmagazin.de/mai-ausgabe-2025/ und: https://www.capital.de/geld-versicherungen/bayer--aktie-zwischen-krisenmodus-und-comeback-hoffnung-35521028.html.

dere dann, wenn professionelle Angreifer ihre digitale Infrastruktur sehr gut tarnen und im Nicht-EU-Ausland unterhalten. Gleichzeitig können solche Prozeduren viel Zeit in Anspruch nehmen, was dafür sorgt, dass die betreffenden Inhalte noch lange Zeit abrufbar sind. Ein weiteres Problem ergibt sich daraus, dass Takedowns in der Regel nur für einzelne Seiten, Posts, Shares und Re-Posts, Videos etc. gelten, professionelle Desinformationskampagnen aber aus vielen kleinen Bausteinen besteht, die einzeln „gelöscht" werden müssten. Ebenso gilt es als Grundregel, dass online Inhalte nicht einfach so „verschwinden", sondern über archivierte Versionen, Re-Posts etc. auch weiterhin sichtbar bleiben. Der Kosten-Nutzen-Faktor von Takedowns ist deshalb oft negativ, umso mehr, da Angreifer wesentlich schneller und kostengünstiger neue digitale Infrastruktur aufbauen als sie mittels Takedowns gelöscht werden kann. Die Herausforderungen und negativen Seiten von Takedowns spiegeln sich auch in den Umfrageergebnissen dieser Studie wider: Hier wird die Kooperation von online Plattformen sowie die Reaktion und Redaktionsdauer auf Meldungen gefährlicher Inhalte als schwierig eingestuft (siehe die Umfrage dieser Studie). Nichtsdestoweniger scheinen rechtliche Schritte, Löschungen und Takedowns die häufigste Reaktion deutscher Unternehmen auf Desinformationsangriffe zu sein.

Zentraler Baustein für eine wirksame Verteidigung ist daher eine gut vorbereitete, Desinformation-spezifische strategische Kommunikation: Dazu gehört nicht nur das schnelle, inhaltlich professionell gestaltete und strategisch ausgespielte Debunking falscher Informationen, sondern auch proaktives Messaging, das zentrale Narrative aufgreift, kontert oder bewusst umlenkt. Zu dieser Art der strategischen Kommunikation gehört auch, dass auf Basis eines Lagebildes (mögliche) Narrative und Botschaften von Angreifern proaktiv identifiziert werden; darauf aufbauend können strategische und an entsprechenden Zielgruppen und Ausspielungskanäle angepasste Botschaften ausgearbeitet werden. Unternehmen sollten in der Lage sein, auf Knopfdruck vorgefertigte Medienformate (Posts, Videos, Memes) für verschiedene Zielgruppen und Plattformen bereitzuhalten. Ebenso wichtig ist die Mobilisierung von Unterstützern, ob intern, in der Zivilgesellschaft oder unter Stakeholdern, sowie der gezielte Outreach zu Multiplikatoren. Eine konzeptionell ausgestaltete strategische Kommunikation ermöglicht es Organisationen, narrative Angriffe wie Desinformation auch als Gelegenheit wahrzunehmen, die eigene Story zu erzählen, Markenwahrnehmung zu stärken, Vertrauen aufzubauen und Angreifer kommunikativ zu entwaffnen.

Im digitalen Raum stehen außerdem gezielte Cybermaßnahmen zur Verfügung. Diese reichen von offensiven Eingriffen in die Infrastruktur der Angreifer (in enger Abstimmung mit Rechts- und Sicherheitsvorgaben), über den Einsatz von Honeypots zur Täuschung und Ablenkung, bis hin zu Spoofing- und Obfuscation-Operationen, bei denen gegnerische Narrative gezielt verwässert oder unterwandert werden. Auch Hashtag-Hijacking, koordinierte Bot-Strategien oder das gezielte „public exposure" von Angreifern und deren Netzwerken können Teil einer solchen aktiven Verteidigung sein.

Und schließlich gilt: Verteidigung, Reaktion, Maßnahmen und Abläufe müssen geprobt werden. Simulationen, Red Teaming-Übungen und strukturierte Krisenplanspiele helfen deshalb, Abläufe zu automatisieren, Lücken in Prozessen zu erkennen, Zuständigkeiten zu klären und Kommunikationsketten zu festigen.

Wichtig: Auch diese Liste ist keine vollständige Anleitung oder einfache Blaupause. Die Auswahl und Umsetzung der Maßnahmen hängt stets ab von der individuellen Risikobewertung, den verfügbaren Ressourcen, der angestrebten Zielstrategie und der konkreten Angriffsform ab. Ein durchdachtes, anpassungsfähiges und regelmäßig überprüftes Schutzkonzept ist daher die wichtigste Grundlage jeder erfolgreichen Verteidigung gegen Desinformation.

1.10 Fazit & Zusammenfassung

Desinformation, Info-Angriffe und Cyber Influence-Attacken gegen Unternehmen, Wirtschaft und private Organisationen nehmen rapide zu. Obgleich das tatsächliche Ausmaß oftmals im Dunkeln bleibt, deuten die zunehmende Anzahl und Qualität von Angriffen einen umfassenden Informationskrieg verschiedener staatlicher und privater Akteure gegen Wirtschaft und Unternehmen hin. Dies ist ein globaler Trend, der sich auch und gerade in Deutschland manifestiert. Geopolitische Konflikte, gesellschaftliche Polarisierung und Kulturkämpfe, die gezielt in und über Unternehmen und Marken ausgetragen werden, sowie rasante technologische Entwicklungen sind hierfür die Hauptgründe. Insbesondere die Entwicklung im Bereich Künstlicher Intelligenz in Verbindung mit der Evolution von online Informationsräumen als Informationsquellen haben dazu beigetragen, dass Desinformation ein Multi-Milliarden-Geschäftszweig geworden ist.

Wie die Ergebnisse der Umfrage und Interviews (siehe die Umfrage dieser Studie) zeigen, klafft eine Lücke zwischen der Gefahren-Einschätzung und Gefahren-Bewertung internationaler Experten und Organisationen und der befragten deutsche Unternehmen. Letztere bewerteten die Bedeutung und vor allem die Effekte und Folgen von Desinformation als mittel bis gering (siehe die Umfrage dieser Studie), wohingegen Weltwirtschaftsforum, Gartner und Sicherheitsprofis ein Milliardenrisiko einschätzen. Die Ursachen dafür können vielfältig sein: Einerseits ergab die Umfrage, dass das Bewusstsein für die Gefahr von Desinformation für Unternehmen unter den befragten Unternehmen immer noch ausbaufähig ist: Nur 13% der Befragten sahen ein starkes Gefahren-Bewusstsein bei Mitarbeitern, immerhin 36% bei den Leitungsebenen (wobei die Mehrheit der Befragten letzterer zuzuordnen sind).

Ein anderer Grund für die im internationalen Vergleich eher geringere Bewertung der Gefahr mag sein, dass Unternehmen in Deutschland Desinformation vor allem als gesamtgesellschaftliches, politisches Phänomen sehen. Dies legt z.B. die starke Fokussierung befragter Unternehmen auf den Faktor Mitarbeiter nahe. Hier werden sowohl ein geringes Gefahrenbewusstsein, als auch die meisten Gegenmaßnahmen verortet (z.B. Schulungen, aber auch die Forderung nach gesamtgesellschaftlichen Aufklärungskampagnen). Hier geht es also z.B. um Krankheitsausfällen aufgrund von Gesundheitsdesinformation oder innerbetrieblichen Konflikten aufgrund extremistischer Agitation und Propaganda. Dass Desinformation, wie in den Fallstudien gezeigt, im globalen Maßstab sowohl von Staaten zur Durchsetzung geopolitischer Interessen als auch durch konkurrierende Unternehmen eingesetzt wird, spielte unter den Befragten kaum eine Rolle. In Interviews wurde teilweise stattdessen explizit angemerkt, dass Desinformation von Konkurrenten keine Rolle spielen würde. Das bedeutet: Entweder werden deutsche Unternehmen im internationalen Vergleich seltener zum Ziel von Desinformations-Angriffen oder aber die Angriffe werden nicht entsprechend zugeordnet und bewertet. Für letzteres spricht auch, dass ein einheitliches behördliches Lagebild zu Desinformationsangriffen sowie ein strategischer Austausch zwischen Unternehmen untereinander als Desiderat genannt wird. Das bedeutet, dass sowohl threat assessment als auch threat intelligence – ähnlich wie sie in Unternehmen bereits für traditionelle Cyberangriffe betrieben werden - in Bezug auf Desinformation noch schwach ausgeprägt sind.

Auch bei den Gegen- und Sicherheitsmaßnahmen zeigt die Umfrage dieser Studie, dass die befragten deutsche Unternehmen vor allem auf traditionelle Maßnahmen wie Mitarbeiterschulungen, Medienbildung und Löschungen bzw. Kennzeichnung von online Inhalten setzen. Wie oben bereits diskutiert, gehören diese Maßnahmen zwar sämtlich in den Werkzeugkasten einer Anti-Desinformationsstrategie, sind jedoch für sich nicht ausreichend. Präventive und reaktive strategische Kommunikation, die Desinformationsangriffe entwaffnen kann, setzen z.B. nur 42% der Befragten ein, Cybermaßnahmen wurden überhaupt nicht genannt. Und auch bei der Zuständigkeit für das Thema verwiesen die Befragten auf mehrere Arbeitseinheiten, zentrale Ansprechpersonen

oder Arbeitseinheiten nannten nur wenige. Bei diesen Maßnahmen, insbesondere der cyber-unterstützen kommunikativen Abwehr und der Etablierung von Strukturen, Prozessen und Zuständigkeiten, besteht also weiterhin Handlungsbedarf. Abschließend sei dabei auch auf ein best practice-Beispiel verwiesen, dem „Leitfaden: Sicherer Umgang mit Desinformation“ der Vereinigung der Bayerischen Wirtschaft und der Bayern-Allianz gegen Desinformation.[46]

1.11 Checkliste für Unternehmen

- Regelmäßige **Risiko-Analysen**
- 360° **online Monitoring und Threat Intelligence** für Informationsangriffe
- Teilnahme an branchenübergreifenden **Austausch-Systemen und Plattformen**
- **Incident Response Pläne** für Informationsangriffe
- **Tool-Stack für Technologien und Programme** (OSINT, Monitioring, Analyse, Cybersecurity, KI-basierte Vorhersage-Systeme, Daten-Analysen, Dash Boards, Threat Intelligence)
- **Trainings, Sensibilisierungen und Awareness-Kampagnen**
- **Red Teaming** (Angriffs- und Krisen-Simulationen)
- Strategien, Tools und Expertise zum **Takedown von online-Inhalten**
- Desinformations-spezifische **strategische Kommunikation & Kommunikationsstrategien**
- **Strategische Resilienz** (intern und für Marken)
- **Anleitungen, Beispiele und Aufklärungskampagnen für politische Kommunikation und politisches Engagement** von Mitarbeiter und Führungskräften
- **Kooperation mit Behörden, Experten und Fachwelt**
- **Feedback- und Lernschleife**

1.12 An wen wenden?

Im Ernstfall ist es gut, Unternehmen haben eine vorbereitete und ständig gepflegte Liste mit verschiedenen Kontakten, an die sie sich wenden können. Wie auch die Umfrage dieser Studie ergab, wünschten sich 79% der befragten Unternehmen mehr Unterstützung vonseiten der Behörden und des Staates. Daher hier eine kurze Liste möglicher Ansprechpartner:

- Wirtschaftsschutz der Verfassungsschutz-Behörden (Land)
- Landeskriminalämter
- Zentrale Ansprechstelle Cybercrime (ZAC) der Bundesländer
- OSINT-Analysten und -dienstleister
- Priv. Sicherheitsdienstleister mit Desinformations- und Cyber-Kompetenz
- Spezialisierte Kommunikations- und Krisenberater
- Kanzleien mit Spezialisierung auf Online- und Medien-Recht
- Branchenverbände und IHKs
- Service- und Meldestellen von Online Plattformen

46 Siehe: https://www.vbw-bayern.de/vbw/Themen-und-Services/Services-fuer-Verbaende/Kommunikation-und-Oeffentlichkeitsarbeit/Leitfaden-Sicherer-Umgang-mit-Desinformation.jsp

Wichtig dabei zu beachten sind jedoch die Möglichkeiten und Grenzen von Behörden und Ansprechpartnern: Polizei- und Strafverfolgungsbehörden zum Beispiel dürfen nur reaktiv bei Vorliegen von Straftatbeständen (bzw. Gefahr in Verzug) reagieren. Desinformationsangriffe erfüllen diese Anforderungen jedoch oft nicht; Verfassungsschutzbehörden hingegen können Desinformationsangriffe zwar analysieren und verzeichnen, sind jedoch beschränkt bei den Möglichkeiten zur Informationsweitergabe an Unternehmen und haben (noch) keinen Auftrag zur aktiven Abwehr solcher Angriffe auf Unternehmen. Stattdessen können hier die Wirtschaftsschutz-Bereiche vor allem bei Schulungen und Sensibilisierungen unterstützen. Wie auch bei politischer Desinformation, tun sich staatliche Stellen aufgrund uneindeutiger bzw. vom Einzelfall abhängiger Rechtslagen oft schwer mit der gezielten Bekämpfung von Desinformation und Informationsangriffen. Dies gilt umso mehr, wenn die Angreifer und ihre digitale Infrastruktur im Ausland (insb. außerhalb der EU) angesiedelt sind. Die große Hoffnung von Unternehmen auf behördliche Hilfe, wie sie in den Umfrageergebnissen dieser Studie zum Ausdruck kam, sollte daher gedämpft werden. Stattdessen sollten Unternehmen eigenverantwortlich Schutzmaßnahmen ergreifen.

Kapitel 2

Eine Lageerfassung

Von: Lisa Acker & Günther Schotten, VSW-Bundesverband

2.1. Hintergrund & Methodik

Im Jahr 2017 wurde bereits eine Studie zur Desinformation durch den VSW-Bundesverband (damals ASW Bundesverband), Complexium und weiteren Autoren erstellt. Neun Jahre später erscheint eine erneute Erfassung der Lage angebracht. Seit der ersten Studie hat sich das Phänomen weiterentwickelt, wurde im politischen Umfeld bei mehreren Wahlkämpfen und im Kontext politischer Auseinandersetzungen angewandt. Desinformation wird als Teil hybrider Kriegsführung verstärkt genutzt und auch Unternehmen sind Opfer von Desinformationsangriffen geworden. Wie weit diese Bedrohung für Unternehmen geht, möchte diese vorliegende Studie aufzeigen. In Kapitel 1 dieser Studie findet sich eine ausführliche Analyse internationaler Fallstudien im Hinblick auf Bedrohungsart, Akteure, Narrative, Mittel und Gegenmaßnahmen. Kapitel 3 wird Desinformationsangriffe methodisch aufschlüsseln und eine Risiko-Modellierung vorstellen. Dieses Kapitel wird Ergebnisse einer aktuellen Umfrage und einzelner Interviews vorstellen und somit die Bedrohungswahrnehmung unter deutschen Unternehmen analysieren.

Von Oktober bis Dezember 2025 führte der VSW-Bundesverband eine Online-Umfrage durch, bei der 109 Unternehmensvertreter[47] 12 Fragen zur Betroffenheit und Einschätzung von Desinformationsangriffen in Bezug auf ihre Unternehmen ausfüllten. 46% der Befragten waren dabei Unternehmen mit weniger als 1.000 Mitarbeitern weltweit. Industrievertreter waren mit 30% die stärkste Branche in dieser Umfrage, wobei Dienstleistungen mit 19%, Energie & Wasser mit 15% und Informations- und Telekommunikationstechnik mit 14% ebenfalls im zweistelligen Bereich lagen. Ergänzend wurden zwölf qualitative Interviews mit Unternehmensvertretern verschiedener Konzerne (ebenfalls branchenübergreifend) durchgeführt.[48] Diese gaben noch einmal einen detaillierteren Einblick in die Strukturen und bisherigen Schutzmaßnahmen in den Unternehmen sowie auch die Einschätzung zu zukünftigen Entwicklungen, notwendigen Schritten und der Zusammenarbeit der Stakeholder.

Um ein gemeinsames Verständnis von Desinformation zu haben, wurde der Umfrage eine Definition[49] vorausgestellt, die wie folgt lautete:

> Desinformation ist die gezielte Verbreitung falscher oder irreführender Informationen, um die öffentliche Meinung, Gruppen oder Einzelpersonen zu beeinflussen – mit politischen oder wirtschaftlichen Zielsetzungen. Akteure können privat oder staatlich sein.

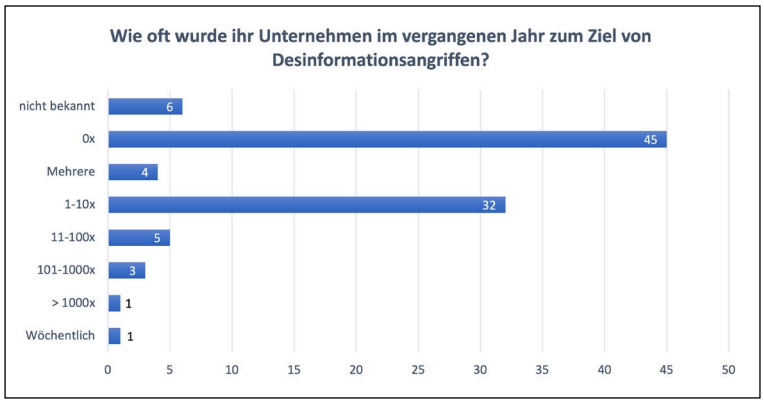
47 215 Beantwortungen hatte die Umfrage insgesamt erfasst, doch waren es nur 109 Teilnehmer, die zwar vereinzelt Fragen übersprangen, den Fragebogen jedoch vollständig bearbeitet hatten.

48 Diese wurden im November und Dezember 2025 in digitalen Gesprächen durchgeführt.

49 Diese Definition ist an die Definition der EU-Kommission angelehnt.

2.2. Die Hälfte der Befragten waren bereits Opfer von Desinformationsangriffen

Auf die Frage wie oft das Unternehmen im vergangenen Jahr nach Eigenwahrnehmung Ziel von Desinformationsangriffen war, haben 47,5% der Umfrage-Befragten angegeben im vergangenen Jahr Opfer geworden zu sein, davon einige mehr als einmal, wie die Abbildung 1 zeigt. 46,5% waren im vergangenen Jahr nicht betroffen. 6% der Befragten konnten keine Angaben zur Betroffenheit geben.



Auch in den Interviews zeigte sich, dass fast alle der interviewten Unternehmen bereits von Desinformationsangriffen betroffen war. Dabei variierten die Angriffe von kleineren Sachverhalten durch Einzelpersonen (persönliche Rache, unzufriedene Mitarbeiter, unbeliebte Projekte) bis hin zu größeren Kampagnen mit Hilfe von Deep Fakes und vermutlich staatlich gelenkter Vorhaben.

Abbildung 1: Wie oft wurde ihr Unternehmen im vergangenen Jahr nach Eigenwahrnehmung zum Ziel von Desinformationsangriffen? N=97

2.3. Im Unternehmensalltag wird Desinformation als mittlere Bedrohung wahrgenommen

Bei einer Skala von 1-10 auf die Fragen, wie groß die Bedrohung Desinformation für das eigene Unternehmen wahrgenommen wird und welche Bedeutung es im täglichen Arbeitsumfeld hat, wurde bei beiden Fragen ein Durchschnittswert von 5 angegeben. Unternehmen müssen sich mit sehr vielen Bedrohungen auseinandersetzen und Desinformation ist dabei eine von vielen.

Bei der Einschätzung des Bewusstseins für das Thema auf Leitungs- und Mitarbeiterebene bewerteten die Befragten beide mit einem mehrheitlich mittleren Bewusstsein fürs Thema. Der Leitungsebene wird aber von mehr Unternehmen ein stärkeres Bewusstsein zugeschrieben (34%) als den Mitarbeitern (12%)[50]. Auf Mitarbeiterebene sehen 43% der Befragten wenig Bewusstsein fürs Thema.

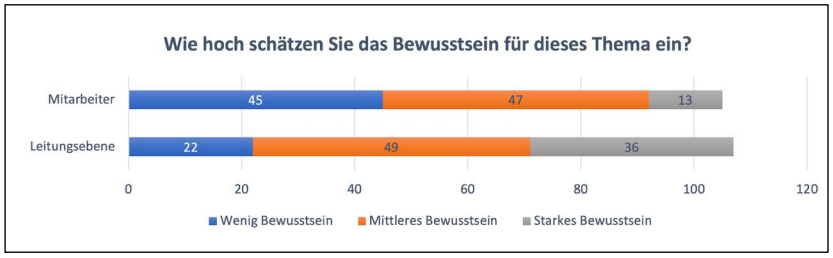
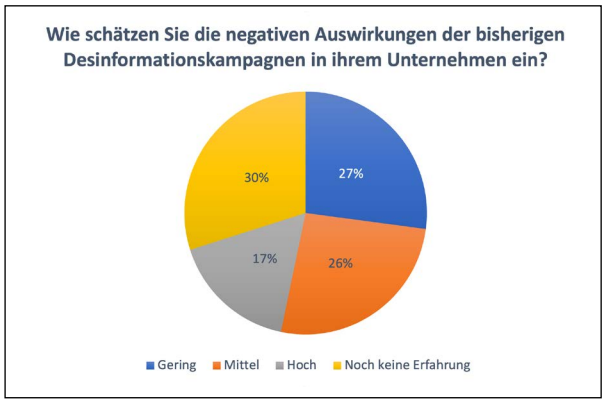


Abbildung 2: Wie hoch schätzen Sie das Bewusstsein für dieses Thema auf der Leitungsebene (und auch unter Mitarbeitern) ein? N=107 (Bewertung Leitungsebene) N=105 (Bewertung Mitarbeiter)

50 Hier muss beachtet werden, dass die Leitungsebene von zwei Befragten bewertet wurde, welche keine Bewertung der Mitarbeiter abgaben. Am Ergebnis ändert dieser Unterschied aber nichts.

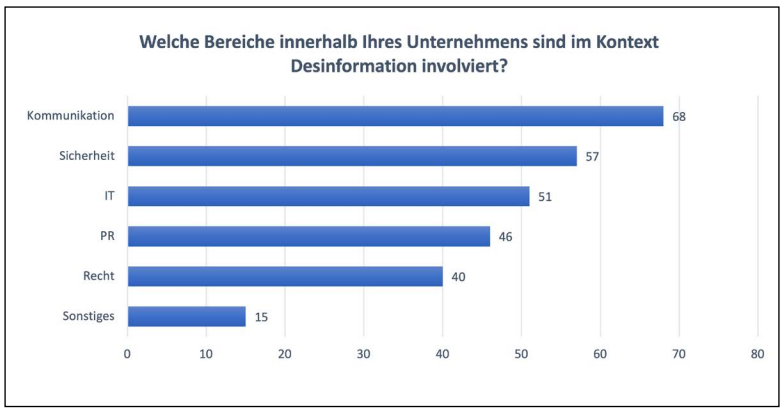
2.4. Bisherige Desinformationsangriffe zeigten mehrheitlich geringe bis mittlere Auswirklungen



Es ist natürlich nicht einfach Auswirkungen von Desinformationskampagnen genau zu messen. Siehe dazu auch den Teil „Was kostet das?“ in Kapitel 1. Jedoch zeigte die Umfrage, dass die Unternehmensvertreter – die bisher von Desinformationsangriffen betroffen waren – mehrheitlich die Auswirkungen als gering einschätzten. Hohe negative Auswirkungen gaben knapp 17% der Befragten an.

Abbildung 3: Wie schätzen sie die negativen Auswirkungen von Desinformationskampagnen ein, die ihr Unternehmen betroffen haben? N=107

2.5. Fach- & Abteilungsübergreifende Zusammenarbeit beim Monitoring und Aufklärung von Angriffen



In Unternehmen liegt das Thema Desinformation in Händen vieler, da dieses Phänomen nicht nur die Kommunikation und Sicherheit eines Unternehmens tangiert, sondern auch Abteilungen wie Recht und PR.

Abbildung 4: Welche Bereiche innerhalb ihres Unternehmens sind im Kontext Desinformation involviert bzw. besonders gefordert? N=101

In den meisten Unternehmen, welche an der Umfrage teilgenommen haben, sind die Kommunikationsabteilungen im Kontext Desinformation involviert. Knapp dahinter liegt die Sicherheitsabteilung. Aber auch IT, PR und Recht nehmen bei einigen der Unternehmen noch eine Rolle im Kontext Desinformation ein. Wie die Interviews ergaben, haben ein paar der Konzerne diese relevanten Abteilungen in unterschiedlicher Form vernetzt, um einen kontinuierlichen Informationsfluss zu gewährleisten. Ob Task-Force oder auch Social-Media-Intelligence-Network, die Vernetzung der Bereiche ermöglicht es schnell Informationen zu teilen und alle relevanten Perspektiven an einen Tisch zu holen. Diese Unternehmen gehen mit gutem Beispiel voran und zeigen, dass eine Vernetzung und ein Ownership für dieses Thema ein wichtiges Element in der Bekämpfung der Desinformation ist.

Aber nicht nur im Angriffsfall ist die Zusammenarbeit essenziell, sondern auch beim Monitoring. Viele der interviewten Unternehmen setzen auf Social-Media-Monitoring Tools, die oft bei der Kommunikationsabteilung angewendet werden. Aber auch die Abteilungen der Unternehmenssicherheiten setzen vereinzelt Monitoring-Tools ein oder greifen auf Dienstleister in diesem Bereich zurück.

Best Practice: Krisenunterstützungsteam bei Desinformationsangriffen

Vor allem kleinere Unternehmen werden das Problem kennen, dass der Normalbetrieb mit einem Personalstamm zwar sehr gut abzudecken ist, in eine Krisensituation dieser jedoch nicht mehr ausreichend ist. Bei einer größeren Desinformationskampagne gegen ein Unternehmen kann das Personal der Kommunikationsabteilung schnell an ihre Grenzen kommen. Dies erkannte auch eines der befragten Unternehmen und errichtete kurzerhand ein „Krisenunterstützungsteam" für die Kommunikationsabteilung. In einer Alarmierungsmatrix eingebettete Mitarbeiter, die ebenfalls Pressemitteilungen schreiben und Social-Media-Kanäle bedienen können, werden im Krisenfall herangezogen, um bei Desinformationsangriffen zu unterstützen.

Bei der Frage nach konkreten Schutzmaßnahmen und Frühwarnsystemen waren es die Mitarbeiterschulungen, welche die meisten Unternehmen (74%) als die in ihrem Unternehmen etablierten Maßnahmen angaben. Die Interviews ergaben, dass die befragten Konzerne das Thema Desinformation meist jedoch nicht alleine schulen, sondern dieses gemeinsam mit anderen Themen als Teil einer allgemeinen Sensibilisierung oder Sicherheitsschulung thematisieren, die einmalig oder auch regelmäßig im Unternehmen durchgeführt wird.

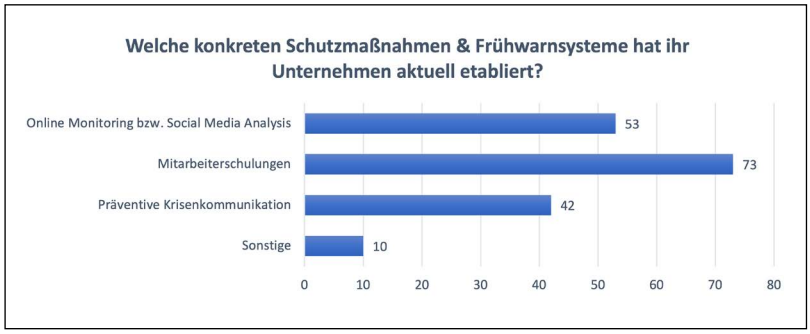


Abbildung 5: Welche konkreten Schutzmaßnahmen und Frühwarnsysteme hat ihr Unternehmen aktuell etabliert? N= 98

Zwei Interviewpartner gaben an – auch im Kontext der geopolitischen Lage und hybriden Kriegsführung – bereits Krisenübungen durchgeführt zu haben, die auch das Element Desinformationsangriffe verwendeten.

Die Mehrheit der in den Interviews befragten Unternehmen äußerten sich jedoch kritisch darüber, ob die bisherigen Maßnahmen in den Unternehmen die Mitarbeiter wirklich genügend auf große Desinformationskampagnen vorbereitet haben.

Online-Monitoring bzw. Social-Media-Analysis wird bei mehr als der Hälfte der befragten Unternehmen bereits eingesetzt. Der Aufklärung wird eine etwas wichtigere Rolle als dem Monitoring in der Umfrage zugesprochen. In 81% der Unternehmen spielt die Aufklärung eine mittlere und hohe Rolle. Das Monitoring erhielt in diesen beiden Kategorien nur von 71% der Unternehmen diese Bewertung.

2.6. Social-Media-Plattformen und die Herausforderung der Regulierung

Auf die Frage, welche Faktoren die Verbreitung von Desinformation fördern, war es der Begriff „Soziale Medien“, der von jedem Unternehmensvertreter ohne Ausnahme unverzüglich in den Interviews genannt wurde. Facebook ist in der Umfrage das Tool, das von den meisten Unternehmen als Plattform mit Desinformationsinhalten über das Unternehmen benannt wurde. Danach folgt die Plattform LinkedIn, die jedoch in den qualitativen Interviews gar nicht als Plattform benannt wurde. Auf der Plattform X begegneten 34 Unternehmen bereits Desinformationen über ihr Unternehmen.

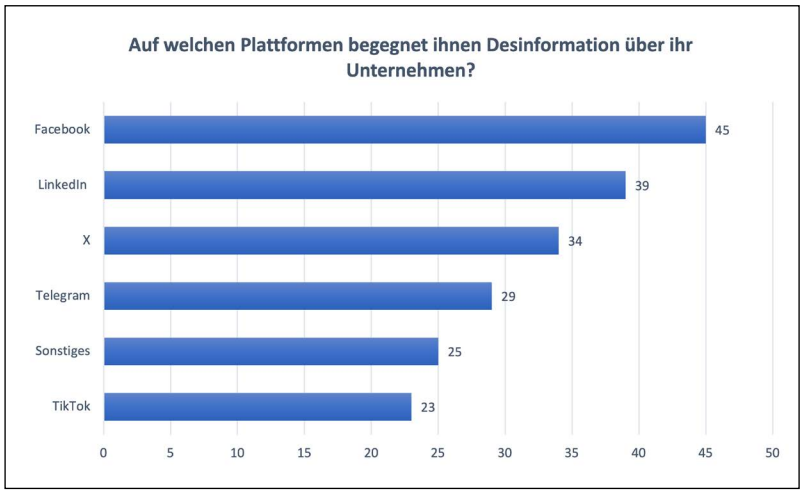
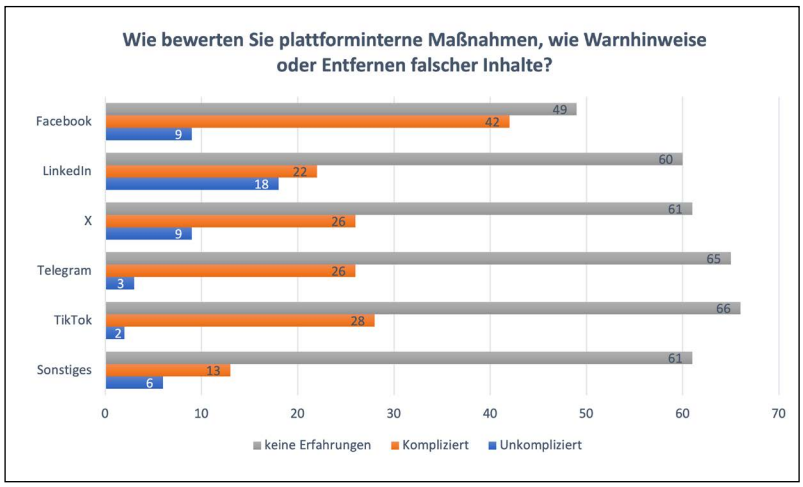


Abbildung 6: Auf welchen Plattformen begegnet Ihnen Desinformation in Bezug auf ihr Unternehmen? N=84[51]

Unter der Kategorie Sonstiges benannten die Unternehmen in einem Frei-Feld noch die folgenden Plattformen: Instagram, Xing, Bewertungsportale, YouTube, Printmedien und vereinzelt auch Mastodon, Signal oder generell Foren, Blogs und Websites.



Die Zusammenarbeit mit den Plattformen wurde sowohl in der Umfrage, als auch in den Interviews als eher schwierig bewertet. Falsche Inhalte, die von Unternehmen gemeldet wurden, wurden oftmals nicht schnelle genug gelöscht, so dass die Weiterverbreitung in dieser Zeit weiter fortgesetzt werden konnte. Die Umfrage ergab, dass die internen Maßnahmen – Warnhinweise oder das Entfernen falscher Inhalte – bei allen Plattformen als überwiegend kompliziert bewertet werden.

Abbildung 7: Wie bewerten Sie plattforminterne Maßnahmen wie Warnhinweise oder das Entfernen falscher Inhalte? N=101

In den qualitativen Interviews wurde die fehlende Regulierung von Social-Media-Plattformen durch die Mehrheit der Befragten beklagt und sowohl ein schnellerer Prozess der Löschung als auch eine Kennzeichnungspflicht für potenziell falsche Inhalte / KI-generierte Inhalte gefordert. Das Problem der fehlenden Identitätsprüfung bei der Eröffnung von Accounts und die damit verursachte Anonymität sowie die vermehrte Verbreitung von polarisierenden Nachrichten durch die Algorithmen wurde ebenfalls kritisch diskutiert.

KI-gestützte Fälschungen oder Social-Bots als Gefahr für Unternehmen wird von den Umfrageteilnehmern kritisch wahrgenommen: 50% der Unternehmen bewerteten die Gefahr als hoch, 36% als mittel und lediglich 14% als niedrig – wobei sich ein Unternehmen bei dieser Frage enthielt.

51 Hier ist auffällig, dass 84 Befragte die Frage zu den Plattformen beantworten, es aber nur 46 Befragte gab, welche die Frage zu Desinformationsangriffe gegen Unternehmen im letzten Jahr bejaht haben. Dies kann zum einen damit erklärt werden, dass weiter zurückliegende Angriffe hier herangezogen werden oder die „individuelle“ Wahrnehmung und Bewertung von Plattformen hier Einfluss nimmt.

2.7. Aufklärungsarbeit und Zusammenarbeit auf allen Ebenen

Neben der Zusammenarbeit mit Plattformen, war auch die Zusammenarbeit zwischen Unternehmen und Behörden ein wichtiger Teil, den nicht nur die Umfrage mit einer Frage abfragte, sondern auch in den Interview-Gesprächen Berücksichtigung fand.

79% der Umfrageteilnehmer wünschen sich mehr Unterstützung von behördlicher Seite oder durch rechtliche Rahmenbedingungen zum Thema Desinformation. 21% der Unternehmen wiederum verneinten dies. Auch die Interviewpartner der Unternehmen waren sich in diesem Punkt nicht wirklich einig. Einige der Gesprächspartner äußerten sich kritisch darüber, dass zusätzliche rechtliche Rahmenbedingungen keine Hilfe darstellten, da es an der Sanktionierung und Durchsetzungskompetenz scheitere. Ein Unternehmensvertreter sagte dazu „Es gibt keine Regularien, die Unternehmen besonders helfen oder Angreifer besonders stören". Fest steht, dass die Desinformationsabwehr im Sinne von Ermittlungen, Aufklärung, Belangen und Abschalten etc. keine rechtliche Grundlage hat, solange kein Straftatbestand erfüllt ist.

Des Weiteren sahen die interviewten Unternehmensvertreter ebenfalls die Grenzen in einer Zusammenarbeit mit Behördenvertretern in diesem Thema, da der Informationsaustausch immer noch durch rechtliche Hürden erschwert wird. Als Wunsch wurde mehrfach ein gemeinsames Lagebild formuliert und das Potenzial gesehen gemeinsame Lösungsansätze zu erarbeiten.

Auf die Interviewfragen zum Handlungsbedarf und Wünschen wurde auch von den interviewten Firmenvertretern die gesamtgesellschaftliche Verantwortung hervorgehoben. Aufklärungsarbeit und Sensibilisierung müsse in allen Bereichen der Gesellschaft, Unternehmen, Schulen, am besten durch eine vom Staat angelegte übergeordnete Kampagne umgesetzt werden.

2.8. Fazit

Das Potenzial großen Schaden durch Desinformationskampagnen anzurichten ist gegeben und wird sich durch die rasant technologischen Entwicklungen in der Zukunft noch zuspitzen. Unsere Umfrage und die qualitativen Interviews haben jedoch ergeben, dass die befragten Unternehmen glücklicherweise noch nicht permanent von großen Kampagnen betroffen sind und hohe negative Auswirkungen durch Desinformationsangriffe nur wenige Unternehmen verzeichnen mussten.

Die Aufmerksamkeit für dieses Thema ist bei den Sicherheits- und Kommunikationsabteilungen der Unternehmen oft angekommen. Jedoch fehlt bei vielen Mitarbeitern noch die Sensibilität für dieses Thema, das dringend – gerade auf dieser Ebene – vorhanden sein sollte. Gerade das Potenzial von Mitarbeitern als eine Schwarm-Sensorik für ihr Unternehmen zu fungieren, sollte nicht unterschätzt werden.

Obwohl Mitarbeiterschulungen als eines der zentralen Maßnahmen im Unternehmen angegeben werden, bezweifelt viele der befragten Interviewpartner, dass ihre Mitarbeiter auf große Desinformationskampagnen genügend vorbereitet seien.

Eine engere Zusammenarbeit zwischen allen gesellschaftlichen Stakeholdern zu diesem gesamtgesellschaftlichen Problem wünscht sich die Mehrheit der Unternehmen.

Kapitel 3

Hybride Bedrohungen im Digitalraum – Desinformationsangriffe und Einflusskampagnen

Prof. Dr. Martin Grothe, complexium GmbH, Berlin

3.1. Einführung

3.1.1. Vorrede und Einordnung

Betrachten wir Desinformationsangriffe gegen insbesondere deutsche Unternehmen als isoliertes Phänomen, dann kommen eine aktuelle Umfrage, die Suche nach hiesigen Beispielen wie auch die Eindrücke aus regelmäßigen, Monitoring-basierten Sicherheitsgesprächen zu einem bemerkenswerten Schluss:

Diese Bedrohung ist bekannt,
aber nicht sonderlich relevant.

Das Bewusstsein ist grundsätzlich vorhanden, eine Handlungsorientierung aber im jeweils eigenen Fall zumeist sehr unausgeprägt. Möglicherweise ist dies so, weil die Bedrohung eher politisch verortet und unternehmensbezogen nicht wirklich belastbar messbar ist. Der aktuelle Kostendruck mag auch dazu verleiten, eine Zuständigkeit überwiegend im Bereich der Unternehmenskommunikation zu sehen, da Reputationsaspekte tangiert werden.

Mit dem wohlmeinenden Hinweis, dass man sicherlich mehr machen müsse, wäre das Thema damit aus Sicht der Unternehmenssicherheit abgehakt. Bevor wir uns aber folglich anderen Aufgaben zuwenden, sei noch eine Frage aufgeworfen:

Warum ist das so?
Warum passiert nicht mehr?

Aus Sicht eines Angreifers kann dies, selbst wenn wir den sicherlich relevanten Aspekt des Dunkelfeldes außer Betracht lassen, nur zwei Gründe haben:

1. Mehr geht nicht.

Hier müssen wir uns aber in Erinnerung rufen, dass Deutschland als noch immer drittgrößte Volkswirtschaft der Erde ein Top-Target für imperial motivierte Staaten ist. Und auch ein Regime im demographischen und ökonomischen Niedergang wie die Russische Föderation sollte bei diesem Ziel nicht an Kapazitätsgrenzen stoßen. Einige weitere Hundertschaften sollten sich für die Bürofluchten der Desinformationsfabriken mobilisieren lassen. Diese erste Antwortalternative erscheint also unplausibel.

2. Mehr soll nicht.

Dies ist womöglich der springende, aber rein spekulative Punkt. Eine deutliche Steigerung des bisherigen Angriffsdrucks könnte dazu führen, dass sich nicht nur direkt betroffene Unternehmen zu Maßnahmen veranlasst sehen, sondern auch allgemein besser vorgesorgt werden würde, was nicht nur den Erfolg der aufgesetzten Kampagnen reduzieren, sondern womöglich auch umfassendere Zielsetzungen gefährden könnte.

Denken wir diesen zweiten Punkt einen Schritt weiter: Was wären geeignete Maßnahmen, die Unternehmen umsetzen könnten?

- Zunächst erscheint es sinnvoll, sich in Planspielen präventiv auf konkrete Desinformationskampagnen vorzubereiten und entsprechende Prozesse zu etablieren.

Weiterhin sollte die Früherkennung durch ein regelmäßiges Digital Listening gestärkt werden, idealerweise so, dass entsprechende Kampagnen erkannt werden, bevor der eigene Unternehmensname genannt wird.

Von entscheidender Bedeutung ist aber die Mitarbeiterschaft: Über eine sporadische Sensibilisierung hinaus können Mitarbeitende als **„intelligente Sensoren“** fungieren, die durch eigene Beobachtung oder über ihr Umfeld mögliche Angriffe bereits frühzeitig erkennen und ihre Einschätzung unternehmensintern zusteuern.

Ein solches, sehr facettenreiches Sensorium als gelebte Praxis würde zu einer intensiveren, möglicherweise sogar um sich greifenden Auseinandersetzung mit dieser Bedrohung führen, die vermutlich nicht nur auf die unternehmensbezogene Sphäre beschränkt bliebe.

So könnte entsprechendes Hintergrundwissen beispielsweise auch vorschnelles Weiterleiten von effektheischenden Botschaften in politischen Wahlkämpfen eingrenzen: Mitarbeitende sind zumeist auch Wähler.

Ein deutlich höheres Niveau an Desinformationsangriffen gegen Unternehmen würde vermutlich indirekt die Beeinflussbarkeit von politischen Wahlkämpfen reduzieren.

Folglich wollen wir hier Desinformationskampagnen gegen Unternehmen nicht, wie eingangs formuliert, als isoliertes Phänomen betrachten: Mit ihnen wird ein Grundmisstrauen aufgebaut, das sich in politischer Beeinflussung weiter kapitalisieren lässt, um dann bei entsprechender Regierungsbildung möglicherweise willfährige Entscheidungen zu erreichen.

So ist vermutlich der Reputations- oder Umsatzverlust einzelner Unternehmen kein finales Ziel gegnerischer Akteure, sondern eine erste Stufe in einem hybriden Gesamtrahmen zur nichtmilitärischen Durchsetzung eigener Interessen. Hierbei besteht die Klaviatur des Angreifers natürlich nicht nur aus gezielten Desinformationskampagnen: Auch etwa andere Einflussoperationen, Cyberangriffe, Drohnenüberflüge (oder zumindest vorgetäuschte Sichtungen) und Sabotageaktionen gehören dazu.

Mit solchen **kinetischen Operationen** können jedoch lediglich Grundüberzeugungen, etwa die der gesellschaftlichen Sicherheit, gelockert, aber nicht gezielt in eine bestimmte Richtung gelenkt werden: Hierzu sind **kognitive Operationen,** insbesondere Desinformationskampagnen notwendig.

Mit dieser Einordnung, die hier natürlich als Hypothese zu verstehen ist, kann ausgeführt werden, dass Desinformationskampagnen gegen Unternehmen trotz der derzeit als gering erachteten Relevanz als eine wichtige Operationsstufe gegen die Widerstandskraft unseres Gemeinwesens verstanden werden können: Eine deutlich aktivere und koordinierte Gegenstrategie erscheint als überaus wünschenswert.

Mit den folgenden Ausführungen wird zunächst der Grundaufbau solcher Kampagnen beschrieben, um dies am Beispiel einer Branche weiter zu konkretisieren und mit Mitigationsmaßnahmen zu unterlegen. Auf dieser Basis wird ein Gesamtrahmen für ein Lagebild „Hybride Angriffe“ skizziert.

3.1.2. Zusammenfassung

Wenn wir also anerkennen, dass Desinformationsangriffe und Einflusskampagnen stattfinden, dann macht es Sinn, ihre Deskription in ein allgemeines Schema zu überführen (Dekonstruktion). Mit dieser Grundlage lassen sich Szenarien für einzelne künftige Operationen skizzieren (Konstruktion) und insgesamt ein deduktives Modell für ein Lagebild „Hybride Angriffe“ entwerfen.

So kann eine vierstufige **Eskalationslogik** den schematischen Ablauf dieser Operationen darstellen. Die Stufen geben zum einen Auskunft über den Entfaltungsgrad der Kampagne und bieten zum anderen Ansatzpunkte für unterschiedliche Detektionsverfahren:

1. Thematisierung
2. Emotionalisierung
3. Aktivierung
4. Mobilisierung

Dieses Konstruktionsmodell dient – zusammen mit einer umfassenden Daten- und Dokumentenbasis – als Rahmen, um durch ein elaboriertes KI-basiertes **„Multi-Agent Predictive Corporate Security Intelligence System** (PrediCX-System)“ Bedrohungsszenarien für verschiedene Entitäten zu generieren.

Kernaufgabe des PrediCX-Systems ist die Generierung von Bedrohungsszenarien für konkrete Unternehmen bzw. Entitäten. Diese Szenarien werden üblicherweise durch Analysten validiert und fließen in das regelmäßige Sicherheitsberichtswesen ein. Auf diese Weise wird der Blick nach vorn gestärkt: Es wird sichtbar, ob aktuelle Ereignisse ein Szenario stützen, abschwächen oder entkräften. Statt einer reinen Rückschau leistet diese Perspektive einen Beitrag, um „vor die Lage“ zu kommen.

Ein aktuelles Szenarienbündel für „Deutschland“ umreißt verschiedene Bedrohungsvektoren, darunter auch einen Angriffsvektor Desinformation gegen den Automobil-Sektor. Dieses Feld wird beispielhaft herangezogen, um zunächst aufzuzeigen, wie narrative Stränge aus einer Faktenbasis heraus entwickelt werden können. Im weiteren Verlauf werden die vier Eskalationsstufen konkreter ausgeführt und mit möglichen Mitigationsmaßnahmen unterlegt.

Das Prinzip solcher Angriffe wird deutlich, ebenso die Möglichkeit, an den unterschiedenen Stufen sowohl mit Früherkennung als auch mit Maßnahmen einzugreifen.

Diese Eskalationsfolge gibt einem modellhaft dargestellten Lagebild „Hybride Angriffe“ eine erste Strukturdimension. In der zweiten Dimension wird eine initiale Angriffskategorie der Destabilisierung um drei weitere, darauf aufbauende Kategorien ergänzt: Unterstützung von (fremden) Überzeugungen, Wahlkampfbeeinflussung, Beeinflussung von Regierungshandeln. Die letzte Hochwertkategorie ist mit militärischen Mitteln nur sehr aufwändig und risikobehaftet zu erreichen.

In diesem so aufgespannten Gesamtrahmen sollten sich sowohl kognitive wie auch kinetische Operationen, wie Cyberangriffe, Drohnenüberflüge und Sabotagen einordnen lassen. Kriterium ist dabei die Zielsetzung aus Angreiferperspektive.

Damit kommt dem Umgang mit entsprechenden Angriffen auf Unternehmensebene eine fast staatstragende Bedeutung zu: Resilienz entsteht emergent. Hier steht in der Praxis zumeist die Schwierigkeit der operativen Schadensmessung einer tatkräftigen Auseinandersetzung bzw. Mittelallokation im Weg.

Wenn nun auf Unternehmensebene entsprechenden Angriffen wenig entgegengesetzt wird, dann wird dadurch eine Zielsetzung begünstigt, die weit über die Unternehmensreputation hinausgeht. So wäre zu begrüßen, dass trotz des schwer messbaren Schadens hier eine deutlich höhere Reaktionskraft eingesetzt wird, als aktuell feststellbar ist.

3.2. Digitalraum als Gefechtsfeld

3.2.1. Desinformation als Modus Operandi hybrider Angriffe

In einer offenen Konfrontation, sei es zwischen Staaten oder Unternehmen, prallen grundsätzlich gleichartige Fähigkeiten aufeinander. Der Ausgang solcher Operationen unterliegt jedoch zumeist hohen Risiken. Hybride Aktivitäten versuchen, dies zu umgehen: Angriffsziele sind Führungsfähigkeit und Stabilität des Zielobjekts. Gleichzeitig wird die Zurechenbarkeit der Maßnahmen verschleiert.

Das Kalkül ist, hierbei einen solchen **Einfluss auf das Denken und Handeln** der angegriffenen Struktur auszuüben, der durch offene Konfrontation nicht möglich oder zu kostspielig zu sein scheint. Direkte physische Operationen, etwa Sabotagen oder Drohnenüberflüge, sind in diesem Kontext einzuordnen, da sie insbesondere die Verwundbarkeit der Infrastruktur zeigen bzw. Zweifel an der Verteidigungsfähigkeit nähren.

Verstärkt werden solche Einflüsse durch Informationsoperationen, die über eine Emotionalisierung ihre Zielgruppen im digitalen Raum erreichen. Dies können die breite Öffentlichkeit, aber auch engere Zielgruppen oder Entscheidungsgremien sein. Aufgabe ist die **Aktivierung von Einstellungen und Mobilisierung zu Handlungen, die ohne die Kampagne nicht getroffen bzw. erfolgt wären.** Dies kann eine politische Abstimmungs- oder Wahlentscheidung, die Teilnahme an einer Protestdemonstration, einem Produktboykott oder die Weitergabe von Aufrufen oder internen Informationen betreffen.

Damit sind Desinformationsangriffe und Einflusskampagnen ein zentraler Baustein hybrider Angriffe. Durch die Effekte der Operationen soll eine strategisch motivierte Einflussnahme oder Destabilisierung ohne offene Konfrontation erreicht werden. Es werden systemische Schwächen oder selbstgeschaffene Grauzonen genutzt, um auf eine systemische Überforderung hinzuwirken.

Um einen solchen Einfluss auszuüben, müssen bestehende Wahrheitselemente aufgenommen und anschlussfähige Botschaften formuliert werden. Auch ein scheinbarer Drohnenüberflug, ein glaubhafter Produktfehler oder festgehaltenes Managerzitat können inszenierte Wahrheitselemente sein, um gewünschte Narrative zu stützen. Die Erfolgswahrscheinlichkeit steigt, wenn solche Maßnahmen an bestehenden Konfliktlinien, Unklarheiten oder Polarisierungen ansetzen.

Für die Erkundung solcher Diskussions- und Entscheidungsräume bietet der Digitalraum eine einzigartige Basis. Passgenau und unerkannt können Narrative eingebracht, Wahrnehmung gestaltet und Akteure delegitimiert werden.

Während die klassische Propaganda grundsätzlich einen klaren Absender, ein nachvollziehbares Ziel und das Mittel der (eigenen und gegnerischen) Emotionalisierung aufweist, erscheinen Desinformationsangriffe und Einflusskampagnen als zentraler Modus Operandi in einem hybriden Gesamtangriff, der auch weitere kognitive und kinetische Facetten umfassen kann, der jedoch unter dem Radar insbesondere auf die Entscheidungsbildung einwirken soll.

3.2.2. Möglichkeiten der Detektion: Forschungsergebnisse Mobi diG und HybriD

Desinformationskampagnen lassen sich auch mit sachlich völlig korrekten Inhalten umsetzen: Darum ist ihre Detektion so schwierig.

Fiktives Beispiel: In einer Großstadt vermeldet ein Radiosender Verkehrsunfälle, aber ausschließlich solche, die von Fahrzeugen mit bayerischen Kennzeichen verursacht wurden. **„Schon wieder ein hat bayerischer Fahrer die Vorfahrt genommen, … Schon wieder … diesmal aus Franken …"** Vermutlich bekäme schon nach wenigen Tagen ein Aufruf ersten Zulauf, entsprechende Fahrzeuge aus dem Stadtgebiet zu verbannen. Zumal wenn vermeintliche Opfer zu Wort oder Kinder zu Schaden kommen.

Dekontextualisierung nennt sich dieses Vorgehen, das die Untersuchung von Einzelbeiträgen ins Leere laufen lässt. Wenn nun aber eine Einzelanalyse nicht zum Detektionsziel führt, dann müssen auf höherer Ebene große Datenmengen nach Mustern untersucht werden. So bringen ausgeprägte Kampagnen atypische Strukturen mit sich:

- Es werden bestimmte Themen oder Themenkombinationen herausgehoben.
- Einzelne Akteure bzw. deren Profile übernehmen zentrale Verbreitungsaufgaben.

Beide Aspekte können durch Ergebnisse aus Forschungsprojekten plastisch dargestellt werden.

Was? Unknown Unknowns systematisch erkennen (Mobi diG)

Im Verbundprojekt Mobi diG (Monitoring biologischer Gefahrenlagen in der digitalen Gesellschaft), das von 2012 bis 2014 vom BMBF im Programm **„KMU-innovativ: Forschung für die zivile Sicherheit"** gefördert wurde, haben die Verbundpartner Robert Koch-Institut RKI und complexium GmbH Lösungen entwickelt, um große digitale Beitragsmengen ohne Vorgabe nach ansetzenden Auffälligkeiten zu untersuchen: Schwache Signale.

Diese Möglichkeit zur Früherkennung ist für die Detektion von Desinformationsangriffen und Einflusskampagnen relevant, da initial nicht vorhergesehen werden kann, auf welche Aspekte und Themen die eingesetzten Narrative zielen. Folglich gilt es, systematisch die **unknown Unknowns** zu finden.

Dies gelingt mit Methoden der Computerlinguistik und Netzwerkanalyse: In einem solchen System, hier GALAXY von complexium, werden die Beitragsmengen in ihre Terme zerlegt, die in einem linguistischen Korpus jeweils eine übliche Häufigkeit aufweisen. Wird diese Häufigkeit plötzlich deutlich überschritten, dann steigt die sogenannte Signifikanz des Terms. Ungewöhnliche Peaks können in einem Ranking deutlich gemacht, inhaltliche Cluster und Begriffszusammenhänge in Netzwerken dargestellt werden.

Folglich gelingt noch keine automatische Detektion, allerdings erhalten Analysten sehr frühzeitige Hinweise auf eine verstärkte Verbreitung von im Vorhinein unspezifizierten Begrifflichkeiten, die gezielt weiter untersucht werden können. Nadeln im Heuhaufen der digitalen Beitragsflut werden angezeigt.

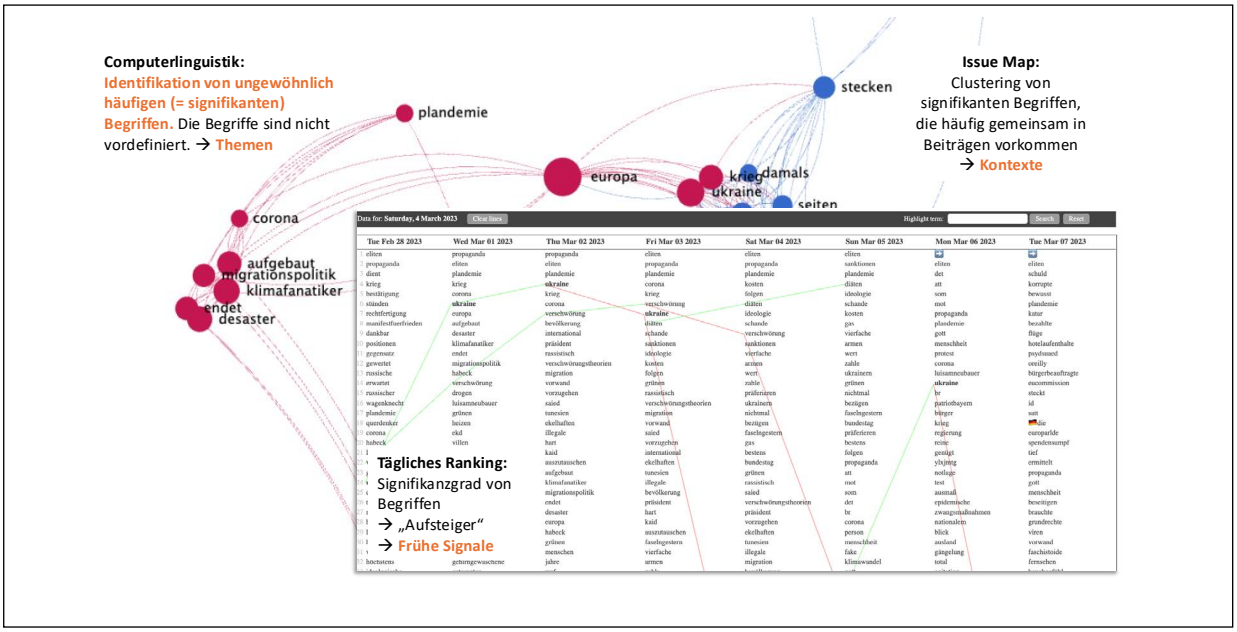


Abbildung 8: Detektion von „Unknown Unknowns“, Quelle: complexium.

Wer? Datensammlung, Akteure und Muster (HybriD)

Im Verbundprojekt HybriD stand die Echtzeiterkennung von Desinformationskampagnen in Online-Medien im Fokus. Die Zusammenarbeit von complexium mit mehreren universitären Partnern wurde von 2021 bis 2025 vom BMBF gefördert.

„Die Forschenden kombinieren dabei die maschinelle Analyse mit menschlicher Expertise, um Desinformationskampagnen zu erkennen. Das Analysewerkzeug soll ermöglichen, große Datenmengen aus Onlinemedien und sozialen Netzwerken in Echtzeit auszuwerten und zeitliche Muster zu erfassen. Auf dieser Datenbasis können Expertinnen und Experten Desinformationskampagnen und ihre Auswirkungen umfassend beurteilen.“ https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/hybrid

Auch hier war keine direkte Detektion möglich, allerdings wurde ein großer Datenraum erschlossen, der die Möglichkeit bot, **taktische Funktionen in Akteursnetzwerken** zu erkennen. Durch die Aufnahme von über 10.000 Telegram-Kanälen sowie weiterer Bereiche auf BlueSky, Mastodon, X und anderen Plattformen konnten übergreifende Flüsse erfasst und auch rückverfolgt werden.

In der Einschätzung von Desinformations- oder anderen Kampagnen ist es hilfreich, die interagierenden Accounts funktional einzuordnen. Sind wir noch in der Filterblase? Hat das Narrative bereits die relevanten Influencer erreicht? In welche Regionen wird die Botschaft geleitet?

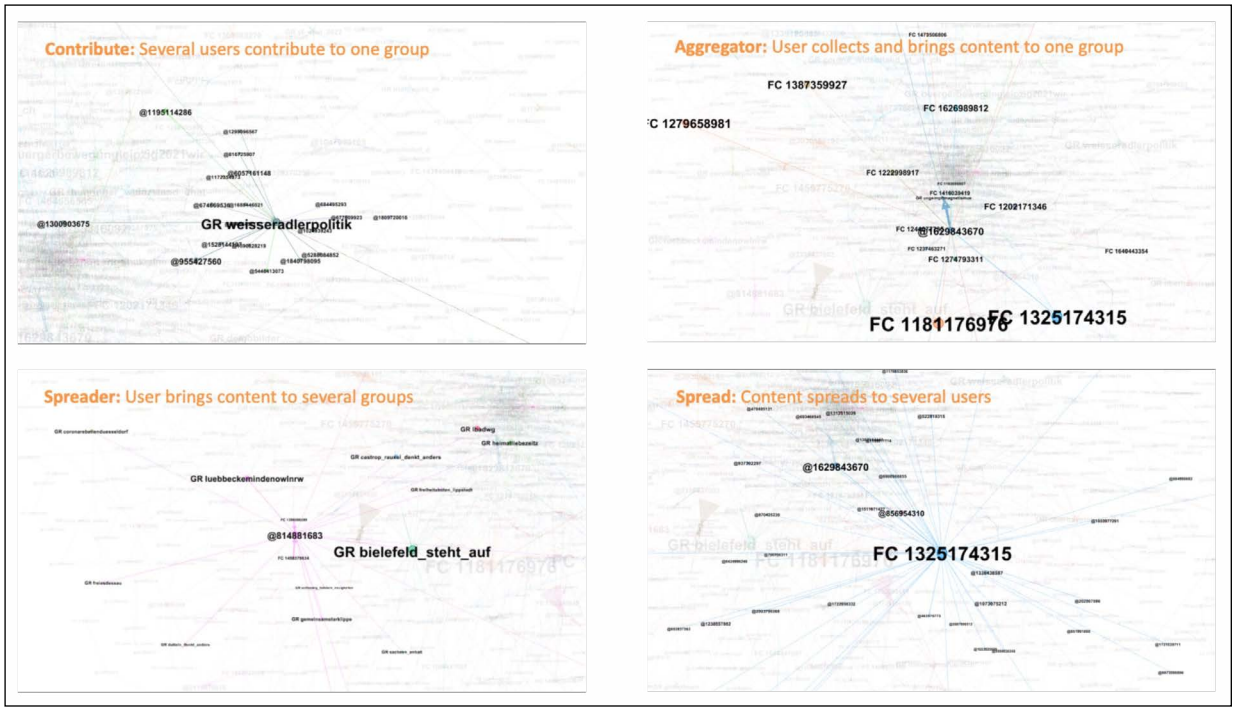


Abbildung 9: Akeursfunktionen in Netzwerken, Quelle: complexium.

Es wird deutlich, dass eine unmittelbare, idealerweise automatisierte Detektion von Desinformationskampagnen nicht möglich ist. Folglich erscheint es sinnvoll, sich mit der Struktur solcher Operationen zu beschäftigen, um hier nach Ansatzpunkten zu suchen. Es wird darüber hinaus aber auch deutlich, dass die Bedeutung sowohl von Analysten wie auch von Mitarbeitenden als Sensorium nicht unterschätzt werden darf.

3.3. Dekonstruktion: Vierstufige Eskalationslogik von Desinformationsangriffen und Einflusskampagnen

Aus einer Vielzahl von Beschreibungen von einzelnen Desinformationsangriffen kann ein allgemeines Schema abgeleitet werden. Ein solcher Orientierungsrahmen ist hilfreich, um auf der einen Seite etwa Szenarien für einzelne künftige Operationen strukturiert zu skizzieren. Auf der anderen Seite kann eine solche Eskalationslogik als eine erste Dimension für ein umfassendes Lagebild „hybride Angriffe“ herangezogen werden.

So kann eine übersichtliche Stufenfolge als **Eskalationslogik** grundsätzlich den schematischen Ablauf dieser Operationen darstellen. Die Stufen geben zum einen Auskunft über den Entfaltungsgrad der Kampagne und bieten zum anderen Ansatzpunkte für unterschiedliche Detektionsverfahren:

1. Thematisierung
2. Emotionalisierung
3. Aktivierung
4. Mobilisierung

Inhaltlich natürlich irreführend, ist die Merkhilfe **TEAM** für die Stufenfolge recht praktisch.

3.3.1. Stufe 1: Thematisierung: Planung und Vorbereitung > Schaffung von Narrativen und Framing > Erstverbreitung

Die erste Stufe wird in drei Aufgaben gegliedert:

Planung und Vorbereitung

- Bestimmung der Ziele, die mit der Desinformation erreicht werden sollen (z.B. Polarisierung, Delegitimierung von Institutionen, Beeinflussung von Wahlen, Verwirrung stiften, Unterstützung für bestimmte politische Agenden generieren).
- Identifizierung der relevanten Zielgruppen, ihrer Überzeugungen, Werte, Schwachstellen und Informationskonsumgewohnheiten.
- Identifikation von bestehenden gesellschaftlichen Bruchlinien, Ängsten oder Unzufriedenheiten (z.B. Migration, Energiepolitik, soziale Ungleichheit, Pandemie-Maßnahmen).
- Auswahl eines Themas, das Polarisierungspotenzial besitzt und an vorhandene Vorurteile oder Unsicherheiten anknüpfen kann.
- Kreation von überzeugenden, emotional ansprechenden und oft spaltenden Narrativen, die auf die Schwachstellen der Zielgruppen abzielen. Dies kann auch die Entwicklung von empörenden Geschichten umfassen.

Schaffung von Narrativen und Framing

- Entwicklung einfacher, prägnanter und wiederholbarer Botschaften (Narrative), die eine bestimmte Sichtweise auf das Thema etablieren sollen. Verwendung von Framing-Techniken, um das Thema in einem gewünschten Licht darzustellen (z.B. „Flüchtlingskrise“ statt „Fluchtbewegung“, „Klima-Hysterie“ statt „Klimawandel“).
- Oftmals werden Halbwahrheiten, aus dem Kontext gerissene Zitate oder bewusst falsch interpretierte Daten verwendet.
- Erstellung von Inhalten: Texten, Bildern, Videos, Memes, Audioinhalten, die die Desinformation transportieren sollen. Dies kann Deepfakes oder manipulierte andere „Belege“ beinhalten.

Erstverbreitung (Seeding)

- Verbreitung der Narrative über zunächst weniger offensichtliche, aber bereits kontrollierte oder „freundliche“ Kanäle (z.B. bestimmte Nischen-Websites, Blogs, Telegram-Gruppen, private Social-Media-Accounts, Foren).
- Ziel ist es, die Inhalte zunächst unauffällig in Umlauf zu bringen und eine erste Basis für die Verbreitung zu legen und das Thema in bestimmten Kreisen bekannt zu machen. Auf diese Weise finden Nutzer, die auf das Narrativ stoßen, bereits erste „Belege“.

3.3.2. Stufe 2: Emotionalisierung: Etablierung von Echokammern und Filterblasen > Appell an Emotionen > Multiplikation

Die zweite Stufe wird in drei Aufgabe gegliedert:

Etablierung von Echokammern und Filterblasen

- Stärkung von bereits bestehenden Meinungen innerhalb geschlossener Gruppen, indem nur bestätigende Informationen präsentiert werden.
- Reduzierung des Zugangs zu Gegenargumenten oder differenzierten Informationen, um die eigene Sicht zu zementieren.
- Die Desinformation wird damit innerhalb spezifischer Gruppen verstärkt und dort als „Fakt" etabliert, während abweichende Informationen ausgeblendet werden.

Appell an Emotionen

- Verwendung von emotional aufgeladenen Inhalten (z.B. Angst, Wut, Empörung, Neid, Misstrauen), um eine starke emotionale Reaktion hervorzurufen.
- Einsatz von Bildern, Videos und Überschriften, die schockieren, provozieren oder Empörung auslösen sollen.
- Häufig werden Sündenböcke oder **Opferrollen** konstruiert und Verschwörungserzählungen gestreut.

Multiplikation

- Anreize zur Interaktion (Likes, Shares, Kommentare) durch provokative oder polarisierende Inhalte. Ausnutzung von Plattform-Algorithmen, die emotionalisierende Inhalte bevorzugen, um die Reichweite zu maximieren.
- Gezielte Streuung der emotionalisierten Inhalte über soziale Medien (Facebook, X, TikTok, Instagram) durch automatisierte Bots, Fake-Accounts und organisierte Netzwerke. Einsatz von Bot-Netzwerken, Troll-Farmen und kompromittierten Accounts, um die Inhalte schnell und massiv zu verbreiten. Dies erhöht die Sichtbarkeit und simuliert eine organische Reichweite.
- Einsatz von menschlichen Influencern, bezahlten Akteuren oder bereits etablierten Meinungsführern in sozialen Medien, die die Narrative aufgreifen und weiterverbreiten. Diese Personen verleihen den Desinformationen höhere Glaubwürdigkeit und verschaffen ihr ein breiteres Publikum. Angestrebt wird der Sprung über die Filterblasen hinaus.

3.3.3. Stufe 3: Aktivierung: Aufruf zur Interaktion > Verbreitung und Verstärkung > Schaffung von digitalen Bezugsorten

Die dritte Stufe wird in drei Aufgaben gegliedert:

Aufruf zur Interaktion

- Explizite oder implizite Aufforderungen an eine breitere Nutzerschaft, sich zu beteiligen (z.B. durch Kommentare, Teilen, das Erstellen eigener Inhalte, die Teilnahme an Umfragen oder Petitionen).
- Formulierung von Fragen oder Situationen, die zur Stellungnahme anregen.

Verbreitung und Verstärkung

- Wenn der Kampagnenstart erfolgreich ist, wird die Desinformation von echten Nutzern, die sie für wahr halten oder mit ihr übereinstimmen, weiterverbreitet. Die organische Verbreitung setzt den Anfangsimpuls fort.
- Die Desinformation erreicht die Mainstream-Medien und die öffentliche Debatte. Dies kann durch wiederholtes Zitieren der ursprünglichen Desinformation oder durch Kontroversen darüber geschehen. Die Glaubwürdigkeit der primären Quellen wird dabei oft verschleiert.
- Aktives Glaubwürdigkeitsmanagement kann eine Kampagne begleiten. Die Akteure hinter der Kampagne versuchen, Kritik oder Dementi zu untergraben, indem sie die Kritiker diskreditieren („Fake News“-Vorwürfe, Verschwörungstheorien über Dementi).

Schaffung von digitalen Bezugsorten

- Bildung von Online-Gruppen, Foren oder Kanälen, in denen sich Gleichgesinnte austauschen und gegenseitig in ihren Meinungen bestärken können.
- Förderung des Gefühls der Zugehörigkeit und des gemeinsamen Kampfes gegen einen vermeintlichen „Feind“ oder eine „Bedrohung“.
- Die ursprünglichen Filterblasen wachsen.

3.3.4. Stufe 4: Mobilisierung: Transition ins Reale > Konsolidierung und Normalisierung > Erosion von Vertrauen und gesellschaftliche Spaltung

Die vierte Stufe wird in drei Aufgaben gegliedert:

Transition ins Reale

- Mit der Etablierung des Narrativs ist ein Einfluss auf das Denken und Handeln bestimmter Gruppen wahrscheinlich. Es kann zu einer Umwandlung der Online-Aktivitäten in reale Aktionen kommen: z.B. Wahlentscheidungen, Aufrufe zu Demonstrationen, Protesten, Boykotten oder zivilem Ungehorsam.
- Die Desinformation hat ihre beabsichtigte, mitunter nachhaltige Wirkung erzielt, sei es Polarisierung, Vertrauensverlust oder die Beeinflussung von Entscheidungen. Auch wenn die ursprüngliche Quelle der Desinformation aufgedeckt wird, kann der Schaden irreparabel sein.
- Die Etablierung eines Narrativs kann Gruppen mobilisieren, um Druck (z.B. auf Politiker, Medien, Unternehmen, Institutionen) auszuüben oder öffentliche Diskurse oder Veranstaltungen durch gezielte Störaktionen oder Verbreitung von Desinformationen zu untergraben.

Konsolidierung und Normalisierung

- Das desinformierende Narrativ wird von einem Teil der Zielgruppe als wahr akzeptiert und in ihr Weltbild integriert. Es wird als Teil des „common sense“ in bestimmten Kreisen etabliert.
- Eine Organisation von digitalen oder physischen Treffen oder Veranstaltungen, die auf den online verbreiteten Narrativen basieren, verstärkt das Zusammengehörigkeitsgefühl.
- Der Eindruck, im Besitz des Wissens um die „wahren Zusammenhänge“ zu sein, stärkt ein elitäres Gruppengefühl und die Abgrenzung zur nichtsahnenden Masse. Das Gruppengefühl kann durch eine Opferrolle weiter verstärkt werden.

Erosion von Vertrauen und gesellschaftliche Spaltung

- Langfristige Ziele sind die Aushöhlung des Vertrauens in etablierte Institutionen (Unternehmen, Medien, Wissenschaft, Politik) sowie die Vertiefung von Spaltungen und Polarisierung durch die Verfestigung von Gegenpositionen und Misstrauen.
- Auf mittlere Sicht wird die Schaffung eines Klimas der Unsicherheit und Instabilität, das die Akzeptanz von extremistischen Ansichten erleichtern kann, erreicht.
- Durch entsprechende Kampagnen kann die systemische Überforderung des Angriffsziels angestrebt werden, seien es politische Institutionen oder Unternehmen. Eine solche Überforderung setzt nicht eine einzige, besonders große Kampagne voraus, sondern wird viel passgenauer durch Kampagnenbündel, die auch unabhängig voneinander über einen längeren Zeitraum umgesetzt werden, erreicht.

Dieser schematische Ablauf zeigt, wie Desinformations- und Einflusskampagnen systematisch aufgebaut sind, um von der stillen Verbreitung von Narrativen bis zur aktiven Einflussnahme auf die öffentliche Meinung und das gesellschaftliche Handeln zu reichen.

3.4 Konstruktion: KI-gestützte Bedrohungsszenarien

3.4.1 Grundlage: Intelligence Cycle mit Predictive Intelligence: PrediCX

Neben einem strukturellen Verständnis von gegnerischen Vorgehensweisen ist für die Detektion, wie bereits geschildert, eine valide und kontinuierlich aktualisierte Datenbasis essenziell. Dies gilt umso mehr für die Generierung von Szenarien zu bereits entstehenden oder erst möglichen Angriffen und Bedrohungen.

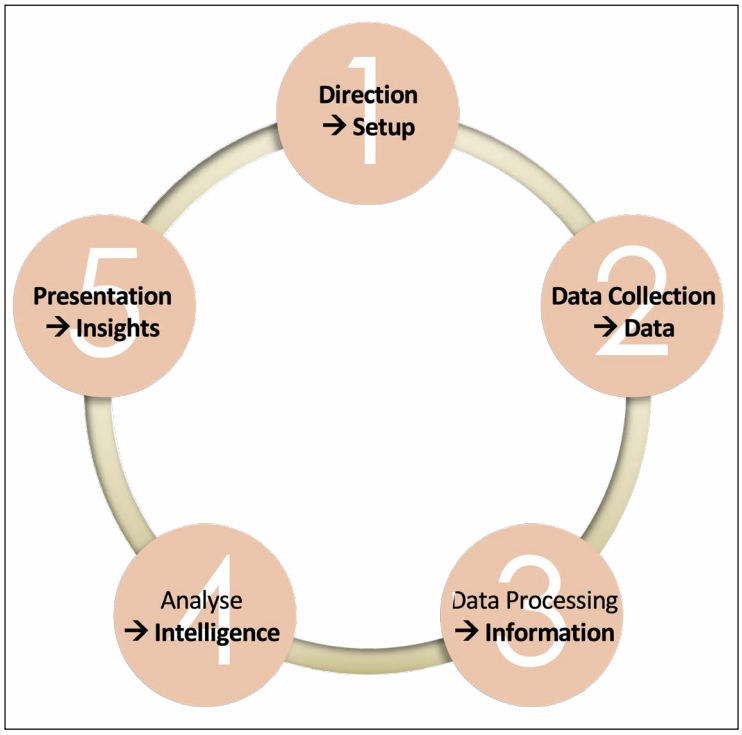


Abbildung 10: Intelligence Cycle.

Eine solche Datenbasis wird in frei verfügbaren KI-Modellen nicht herangezogen: Dort dominieren öffentlich verfügbare Dokumente und Beiträge als Grundlage: Reddit, LinkedIn und Wikipedia kommt hier eine große Bedeutung zu.

Durch den Intelligence Cycle, der die Analyseinfrastruktur von complexium auszeichnet, werden täglich große Mengen, teilweise bis zu 0,5 Millionen digitaler Beiträge aufgenommen, durch diverse Werkzeuge kontextualisiert, durch Analysten validiert und als Intelligence mit Einordnungen und Ableitungen in Sicherheitsberichten dargestellt.

Die Logik dahinter: Da sich Gegnerschaften im digitalen Raum austauschen und koordinieren, können Analysten viele Bedrohungen durch Digital Listening frühzeitig erkennen. Mit dem Intelligence Cycle als Prozess kann ein OSINT-Lagezentrum für Konzernsicherheiten umgesetzt werden.

Mit diesem Ablauf wird sichergestellt, dass über die Detektion hinaus auch belastbare Bedrohungsszenarien aus aktuellen Daten und bewerteter Intelligence generiert werden können.

Im Einzelnen:

- **Breite Data Collection:**
  Durch eigene Technologie werden täglich bis zu 0,5 Mio. potenziell kritische Beiträge unmittelbar gesichtet. Quellen: Aktivistenseiten, Blogs, BlueSky, Discord, Foren, 4Chan, Gettr, Instagram, Mastodon, Reddit, Social Media, ca. 10.000 Telegram-Kanäle/Gruppen, TikTok, X, …
- **Durch Data Processing vor der Lage:**
  Die Analyseinfrastruktur verbindet insbesondere Crawler, Computerlinguistik, Netzwerkanalyse/SNA und Künstliche Intelligenz: Das Analyseteam kann schwache Signale/unknown Unknowns, herannahende Themen, Zusammenhänge, Hintergründe und andere Muster effektiv erschließen.
- **Analyse und Intelligence:**
  Im Lagezentrum findet ein stetiger Austausch zu Operationsformen und Akteuren statt. Erkannte Bedrohungen werden qualifiziert bewertet. In akuten Lagen oder bei Ad-hoc-Fragen können stets Analysten hinzugezogen werden, um zeitnahe Ergebnisse zu generieren.

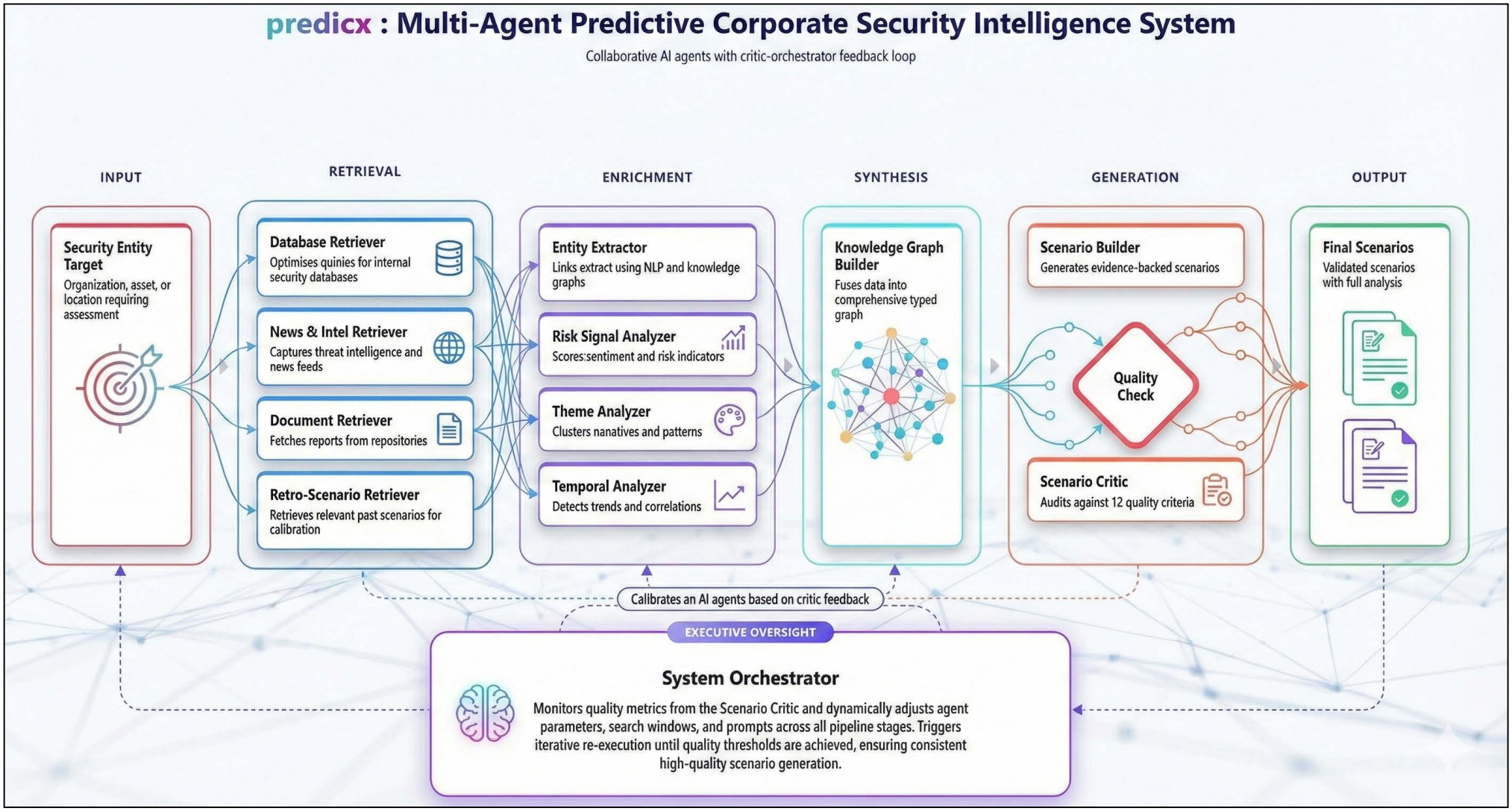


Abbildung 11: Multi-Agent Predictive Corporate Security Intelligence System, Quelle: complexium.

Diese Datenbasis ist grundlegend, um durch das KI-System „PrediCX“ Bedrohungsszenarien für verschiedene Entitäten generieren zu können. Hierzu wird wiederum ein standardisierter Ablaufprozess genutzt, der dem Intelligence Cycle entspricht:

- **Retrieval:** Für die jeweilige Anfrage wird eine evidenzbasierte **Datenbasis** zusammengestellt. Je nach Entität umfasst diese
  - ▷ Analystenberichte zu Aktivistengruppen und Vorgehensweisen,
  - ▷ behördliche Dokumente/Verlautbarungen,
  - ▷ Nachrichtenartikel,
  - ▷ Social-Media-Beiträge (insbesondere von Organisationsaccounts) sowie
  - ▷ bereits erstellte Szenarien und Validierungen.
- **Enrichment:**
  Die Rohdaten werden strukturiert und inhaltlich angereichert. Dabei identifiziert das System u. a. wiederkehrende **Akteurs- und Themenmuster, Ereignisabfolgen, Auslöser/Trigger, Indikatoren und Frühwarnsignale**.
  Beispiel: Aus mehreren Quellen wird erkennbar, dass eine Mobilisierung nicht nur thematisch, sondern auch zeitlich auf ein konkretes Ereignis (Konferenz, Firmenentscheidung, politischer Beschluss) zuläuft - inklusive typischer Eskalationslogik (Thematisierung → Emotionalisierung → Aktivierung → Mobilisierung).
- **Generation & Qualitätskontrolle:**
  Auf Basis dieser strukturierten Evidenz erzeugt PrediCX Szenario-Entwürfe und prüft sie gegen mehrere Kriterien, um das bekannte Halluzinieren generativer KI weitgehend zu unterbinden. Dazu gehören u. a.
  - ▷ ein **Evidenz-Gate** (Szenarien werden nur erstellt, wenn ausreichende, unabhängige Belege vorliegen),
  - ▷ **Konsistenz-Checks** (Zeitlinie, Plausibilität, Widersprüche) sowie
  - ▷ eine **Plausibilitätsbewertung** und
  - ▷ ein **Evidence-Strength-Score** pro Szenario.

Ein wesentlicher Erfolgsfaktor ist damit die herangezogene Datenbasis und deren Gewichtung: Hochwertige Quellen (z. B. Behördenmaterial, belastbare Medienberichte, primäre Veröffentlichungen, Analyseberichte) werden als entscheidend priorisiert; niedrigere Qualität kann ergänzend genutzt werden, wird aber klar gekennzeichnet und nicht als alleinige Grundlage für zentrale Annahmen verwendet.

Transparenz & Nachvollziehbarkeit: Neben dem finalen Report werden auch alle wesentlichen Zwischenergebnisse als Artefakte ausgegeben (z. B. Rohdaten-Extrakte, strukturierte Muster/Indikatoren, Claims-Listen, Validierungsfeedback). Zudem ist jede wesentliche Aussage im Output auf **konkret referenzierte Quellen** zurückgeführt (inkl. URL, Datum) - der Report ist somit auditierbar und für Analysten schnell prüfbar.

Kernaufgabe des Systems ist die Generierung von Bedrohungsszenarien für konkrete Unternehmen bzw. Entitäten. Diese Szenarien werden durch Analysten validiert und fließen in das regelmäßige Sicherheitsberichtswesen ein. Auf diese Weise wird der Blick nach vorn gestärkt: Es wird sichtbar, ob aktuelle Ereignisse ein Szenario stützen, abschwächen oder entkräften. Statt einer reinen Rückschau leistet diese Perspektive einen Beitrag, um „vor die Lage“ zu kommen.

Im Folgenden wird zunächst überblicksartig dargestellt, welche kurzfristigen Szenarien sich für die Entität „Deutschland“ ergeben, um dann eines dieser Szenarien mit einer

Branchenvertiefung weiter zu spezifizieren. Es wird deutlich, wie Desinformationskampagnen der Automobilindustrie zusetzen können.

3.4.2 Deutschland: Bedrohungsszenarien, kurze Frist

In kurzer Frist sehen wir für Deutschland mehrere Szenarien (Stand 26. Januar 2026):

Scenario	Threat Hypothesis
SCENARIO 1: Coordinated Anti-Militarization Protests Targeting Munich Security Conference (MSC)	Activists will leverage the upcoming Munich Security Conference to launch coordinated blockades and direct actions against defense contractors and their financial backers. The operational intent is to disrupt logistics and "mark" sponsors as complicit in war crimes, fueled by the convergence of anti-fascist, climate, and pro-Palestine networks.
SCENARIO 2: Disinformation & Economic Espionage Targeting German Automotive Sector	State-affiliated actors (likely Chinese or Russian) will execute a pre-planned disinformation campaign framed around the "Industrial Decline of Germany." This campaign will exploit the Feb 1st US tariff implementation to amplify narratives of "Ausverkauf" (sell-out) and technological obsolescence compared to Chinese EV competitors, aiming to depress stock prices and incite workforce unrest.
SCENARIO 3: Water Activism & Sabotage Targeting Chemical Infrastructure	The release of the „Karte Rheinisches Revier" on Jan 27 will serve as a targeting grid for environmental activists. Groups like „Wasserbündnis" will escalate from digital campaigns (PFAS videos) to physical disruptions (blockades, pipeline sabotage) at identified „toxic" sites like Chempark Leverkusen, framed as defense of drinking water.
SCENARIO 4: Critical Supply Chain Compromise via Gogs/Git Vulnerability	Threat actors (Ransomware groups or State-sponsored) will exploit the unpatched CVE-2025-8110 in self-hosted Gogs instances to achieve Remote Code Execution (RCE). This will lead to supply chain attacks where malicious code is injected into German industrial software or widespread ransomware deployment (e.g., Black Basta) within corporate networks.
SCENARIO 5: Direct Action against Insurance Sector over "Genocide" Complicity	Following the Jan 21 attack on AXA Berlin, activist groups (Palestine Action Germany, BDS) will broaden targets to include insurance offices in major German cities. Tactics will shift from peaceful protest to vandalism (red paint, glass breaking) and "office occupations" demanding divestment from Elbit and other defense firms, driven by the narrative of "financing genocide."
SCENARIO 6: Russian Hybrid Sabotage Operations on Energy/ Logistics	Russian intelligence (GRU) will utilize recruited proxies (e.g., via Telegram) or radicalized local groups (like "Volcan") to conduct low-level physical sabotage against rail logistics (Deutsche Bahn) or energy substations. The goal is to disrupt NATO logistics ("Steadfast Dart") and erode German public sense of security, framed as "anti-imperialist resistance."

Den Angriffsvektor Desinformation (Szenario 2) führen wir im Folgenden näher aus, wenngleich in einem umfassenden Lagebild „Hybride Angriffe" auch zumindest Aspekte weiterer Szenarien eine Rolle spielen.

3.4.3 Automobil (Szenario 2): Disinformation & Economic Espionage Targeting German Automotive Sector

Narrative Stränge und Abgrenzung: Legitimer Diskurs vs. Desinformation/Manipulation

„Narrativen Stränge“ sind wiederkehrende thematische Muster, die in mehreren Phasen auftreten können. Sie stellen potenzielle Storylines dar, die zur Desinformation genutzt werden könnten.

1. Verlust der technologischen Führungsrolle („Made in Germany“ vs. „Made in China“)
2. Systemische Inkompetenz bei der Digitalisierung und Softwareentwicklung
3. Abhängigkeit von geopolitischen Akteuren (USA, China) als existenzielle Bedrohung

Die Thematik des Einstiegs in die Rüstungsproduktion bzw. des Engagements durch entsprechende Investments wird hier nicht weiter ausgeführt, da die Bezüge in diesem Kontext sehr unternehmensspezifisch sind. Gleichwohl weitet sich dieses Narrativ kontinuierlich aus.

Die folgenden Ausführungen zeigen exemplarisch, wie legitime Diskussionen zu irreführenden Narrativen umfunktioniert werden können.

1. Verlust der technologischen Führungsrolle (‘Made in Germany’ vs. ‘Made in China’)

Kern der Wahrheit (faktische Grundlage):

Deutsche Automobilhersteller haben den Übergang zur Elektromobilität im Vergleich zu „First-Movern“ wie Tesla oder chinesischen Unternehmen (z.B. BYD) verzögert. China kontrolliert weite Teile der Lieferkette für Batterietechnologie. Deutsche Marktanteile im wichtigen chinesischen Absatzmarkt sind rückläufig.

Manipulationsvektoren
(Wie legitime Themen verzerrt werden):

Rosinenpicken (Cherry-Picking):

Gezielte Auswahl einzelner Quartalszahlen oder Segmente, in denen deutsche Hersteller schwächeln, unter Ausblendung globaler Gewinne oder erfolgreicher Verbrenner-Sparten.

Falsche Äquivalenz:

Vergleich von subventionierten chinesischen Kleinwagenpreisen mit deutschen Premium-Limousinen, um ein verzerrtes Bild von „Wucher“„ und mangelnder Wettbewerbsfähigkeit zu erzeugen.

Emotionales Framing:

Umdeutung notwendiger technischer Anpassungsprozesse als irreversibler „Untergang der deutschen Ingenieurskunst“ und Vorbote einer totalen Deindustrialisierung.

Warnsignale
(Monitoring-Indikatoren für Manipulation):

- Plötzlicher Anstieg von „RIP“-Memes oder Hashtags wie #Deindustrialisierung in Verbindung mit Quartalsberichten.
- Koordinierte Verbreitung von Videos, die singuläre Features chinesischer Autos (z.B. Karaoke-Funktionen) als Beweis für die technische Obsoleszenz des gesamten deutschen Antriebsstrangs darstellen.
- Verwendung von Superlativen in Überschriften („Endgültiges Aus“, „Totale Vernichtung“), die nicht durch den Artikelinhalt gedeckt sind.

2. Systemische Inkompetenz bei der Digitalisierung und Softwareentwicklung

Kern der Wahrheit (faktische Grundlage):

Deutsche Konzerne hatten in der Vergangenheit Probleme bei der Software-Integration (z.B. Verzögerungen bei Cariad/VW). Die Benutzeroberflächen (UX) gelten im Vergleich zu Tech-Giganten oft als weniger intuitiv. Die „Legacy"-Hardwarearchitektur erschwert schnelle Over-the-Air-Updates.

Manipulationsvektoren
(Wie legitime Themen verzerrt werden):

Kontext-Stripping:
Ein isolierter Software-Bug (z.B. im Infotainment) wird aus dem Kontext gerissen und als Beweis für die Unsicherheit sicherheitskritischer Systeme (Bremsen, Lenkung) dargestellt.

Falsche Kausalität:
Technische Probleme werden nicht auf Komplexität, sondern auf kulturelle Kampfbegriffe („Wokeness", „Quote statt Kompetenz") zurückgeführt.

Verallgemeinerung:

Vereinzelte Rückrufaktionen werden als Beweis für den kompletten Kontrollverlust des Managements über die Produktqualität dargestellt.

Warnsignale
(Monitoring-Indikatoren für Manipulation):

- Narrative Muster, die „Spaltmaße" (alte Welt) gegen „Software" (neue Welt) ausspielen, um deutsche Ingenieure als ewiggestrig darzustellen.
- Gezielte Verbreitung von „Glitch"-Videos in Social Media durch Accounts, die sonst politische Inhalte posten.
- Vermischung von legitimer Kritik an der Bedienoberfläche mit unbegründeter Angstmacherei vor Hackerangriffen auf das Fahrzeug.

3. Abhängigkeit von geopolitischen Akteuren (USA, China) als existenzielle Bedrohung

Kern der Wahrheit (faktische Grundlage):

Deutsche Automobilkonzerne erwirtschaften einen signifikanten Teil ihres Gewinns in China und sind auf globale Lieferketten angewiesen. Gleichzeitig können protektionistische Maßnahmen der USA oder Handelskonflikte (Zölle) das Geschäftsmodell empfindlich treffen.

Manipulationsvektoren
(Wie legitime Themen verzerrt werden):

Falsches Dilemma:

Darstellung der Situation, als müssten sich Konzerne entweder vollständig unterwerfen oder sofort bankrottgehen, unter Ausblendung von Diversifizierungsstrategien.

Verschwörungsnarrative:

Behauptung, Vorstände seien „Marionetten" fremder Mächte (BlackRock, KP China), die die deutsche Wirtschaft absichtlich sabotieren („Ausverkauf").
Zudem treiben vermeintliche „woke"/"links-grüne" nationale Eliten den Ausverkauf ideologisch absichtlich voran, sind aber ihren internationalen Gegenspielern mutmaßlich unterlegen.

Angstmacherei:

Szenarien eines plötzlichen Lieferstopps oder einer Enteignung werden als unmittelbar bevorstehende Realität dargestellt, um Aktienkurse zu beeinflussen oder politisches Misstrauen zu säen.

Warnsignale
(Monitoring-Indikatoren für Manipulation):

- Häufung von emotional aufgeladenen Begriffen wie „Vasallen", „Knechtschaft" oder „Verrat" in Kommentarspalten zu Unternehmensnachrichten.
- Synchronisiertes Auftauchen von Artikeln in Randmedien, die normale Investitionsentscheidungen im Ausland als „Kapitalflucht" und „Landesverrat" framen.
- Bot-Aktivitäten, die geopolitische Ereignisse (z.B. Taiwan-Spannungen) sofort mit dem Aktienkurs deutscher Autobauer verknüpfen.

Dies zeigt, wie legitime Themen zu irreführenden Narrativen umfunktioniert werden können. Der folgende Abschnitt analysiert die vier Eskalationsstufen einer möglichen Desinformationskampagne.

- Stufe Thematisierung: Technologische Führung, Inkompetenz, Abhängigkeit
- Stufe Emotionalisierung: Angst, Wut, Zweifel
- Stufe Aktivierung: Aufrufe zu internen Missständen und politischen Abkommen
- Stufe Mobilisierung: Aktiver Widerstand, Ablehnung, Boykott von Produkten/Unternehmen

Stufe Thematisierung: Technologische Führung, Inkompetenz, Abhängigkeit

Narrative Frames

- Verlust der technologischen Führungsrolle („Made in Germany“vs. „Made in China“)
- Systemische Inkompetenz bei der Digitalisierung und Softwareentwicklung
- Abhängigkeit von geopolitischen Akteuren (USA, China) als existenzielle Bedrohung

Beobachtete Manifestationen

- Verbreitung von Berichten über Software-Verzögerungen und gescheiterte Kooperationen
- Gegenüberstellung sinkender Absatzzahlen deutscher Hersteller mit dem Wachstum chinesischer Konkurrenten
- Fokussierung auf externe Einflussfaktoren wie Zölle oder politische Entscheidungen, die Investitionen verhindern

Early Indicators (Digital Listening)

- Anstieg von Keywords wie „Software-Debakel“, „Abstieg“, „Chinavorherrschaft“ in Verbindung mit Markennamen
- Vermehrte Erwähnung von historischen Vergleichen im Kontext von „Vergangenheit vs. Zukunft“
- Teilen von Artikeln über Werksverlagerungen oder gestoppte Investitionen

Mitigationsmaßnahmen:

1. Implementierung eines spezialisierten Digital-Listening-Systems, das gezielt nach Narrativ-Mustern wie „Made in China vs. Germany“ und „Software-Verzögerungen“, aber auch unvorhersehbaren Signifikanzzunahmen sucht, um koordinierte Kampagnen bereits in der Thematisierungsphase zu identifizieren.
2. Durchführung von präventiven „Pre-bunking“-Maßnahmen in der internen Kommunikation, um Mitarbeiter und Investoren mit faktenbasierten Informationen zur Digitalstrategie und technologischen Wettbewerbsfähigkeit gegen das Narrativ der „systemischen Inkompetenz“ zu immunisieren.
3. Vorbereitung von validierten Fakten-Hubs und Dark Sites, die differenzierte Daten zu globalen Absatzzahlen und F&E-Fortschritten bereithalten, um verzerrten Vergleichen mit chinesischen Wettbewerbern im Ernstfall sofort begegnen zu können.
4. Etablierung eines Netzwerks unabhängiger Technologie-Analysten und Branchenexperten, die bereitstehen, um bei aufkommenden Falschbehauptungen die technologische Substanz und Innovationskraft des eigenen Konzerns objektiv zu validieren.
5. Juristische Vorprüfung und Vorbereitung standardisierter Meldeverfahren (Notice-and-Takedown) bei Social-Media-Plattformen gegen nicht authentische Akteure, die gezielt Desinformationen verstärken.
6. Verschärfung der Informationssicherheits- und Compliance-Richtlinien für strategische Partnerschaften, um das Risiko von Informationslecks zu minimieren, die böswillig als „gescheiterte Kooperationen“ umgedeutet werden könnten.
7. Erstellung einer transparenten Resilienz-Dokumentation bezüglich der Lieferketten-Diversifizierung, um dem Narrativ der „existenziellen geopolitischen Abhängigkeit“ von den USA oder China proaktiv die faktische Grundlage zu entziehen.

Stufe Emotionalisierung: Angst, Wut, Zweifel

Narrative Frames

- Angst vor Arbeitsplatzverlust und Deindustrialisierung
- Wut über Fahrverbote und regulatorische Einschränkungen (Diesel-Thematik)
- Zweifel an der ethischen Integrität der Unternehmensführung (historische Verantwortung vs. Profit)
- Zweifel an etablierten Strukturen und Akteuren der Mitbestimmung
- Vermeintliche Unfähigkeit insbesondere weiblicher Führungskräfte

Beobachtete Manifestationen	Early Indicators (Digital Listening)
▶ Sentiment-Verschiebung hin zu Angst und Wut bei Themen wie Sparmaßnahmen und Vorstandsumbau ▶ Polarisierende Diskussionen im Kontext von Holocaust-Gedenktagen vs. aktuellem Geschäftsgebaren ▶ Emotional aufgeladene Kommentare zu Fahrverboten in deutschen Innenstädten	▶ Hohes Aufkommen negativer Emojis (Wut, Angst) bei Finanzberichten und Sparankündigungen ▶ Verbindung von Begriffen wie „Verrat“, „Untergang“ oder „Versagen“ mit Vorstandsnamen ▶ Virale Verbreitung von Inhalten, die individuelle Mobilitätseinschränkungen dramatisieren

Mitigationsmaßnahmen:

1. Implementierung eines Echtzeit-Sentiment-Monitorings (idealerweise entlang der TEAM-Eskalationsskala), das spezifisch auf emotionale Triggerwörter wie „Deindustrialisierung“, „Verrat“ oder „Enteignung“ kalibriert ist, um künstlich verstärkte Empörungswellen frühzeitig zu identifizieren.
2. Entwicklung und Bereitstellung von internen Pre-bunking-Materialien für Führungskräfte und Betriebsräte, die Ängsten vor Arbeitsplatzverlust durch transparente Fakten zur Standortstrategie präventiv entgegenwirken.
3. Erstellung spezialisierter Deeskalations-Leitfäden für das Community-Management, um bei polarisierenden Themen wie Fahrverboten sachlich und empathisch zu moderieren, ohne die emotionale Spirale weiter zu füttern.
4. Etablierung einer forensischen Analyse von Kommentarmustern in sozialen Medien, um koordinierte Bot-Netzwerke oder Troll-Fabriken zu erkennen, die gezielt historische Vergleiche nutzen, um die Unternehmensreputation zu beschädigen.
5. Proaktive Einbindung unabhängiger Historiker und Ethikbeiräte in die Kommunikation zu Gedenktagen, um die Glaubwürdigkeit der historischen Verantwortung zu validieren und Desinformations-Narrativen die Angriffsfläche zu nehmen.
6. Definition klarer juristischer Eskalationsprozesse (Takedown-Requests, Unterlassungserklärungen) für den Fall, dass Desinformationskampagnen die Schwelle zur Verleumdung oder Volksverhetzung, insbesondere bei NS-Vergleichen, überschreiten.

Stufe Aktivierung: Aufrufe zu internen Missständen und politischen Abkommen

Narrative Frames

- Aufruf zur Aufdeckung interner Missstände und Sicherheitslücken
- Aktivierung gegen politische Handelsabkommen (Mercosur, Indien) unter dem Vorwand des Verbraucherschutzes oder Protektionismus

Beobachtete Manifestationen	Early Indicators (Digital Listening)
▶ Verbreitung von Leaks oder Schwachstellenberichten (z.B. Shadow-IT, GitHub Leaks)	▶ Zunahme von Referenzen auf technische Sicherheitsreports oder 'Hacks'
▶ Gezielte Ansprache von Stakeholdern bezüglich der Risiken von Freihandelsabkommen	▶ Steigendes Suchvolumen nach spezifischen Sicherheitslücken oder internen Dokumenten
▶ Diskussionen über die technische Unsicherheit von Fahrzeugdaten und autonomen Systemen	▶ Koordinierte Kommentarspalten-Aktivität unter Artikeln zu Handelsabkommen

Mitigationsmaßnahmen:

1. Intensivierung des digitalen Monitorings durch spezialisierte Tools, um proaktiv nach geleakten Repositories (z. B. auf GitHub), Shadow-IT-Infrastrukturen und aufkommenden Narrativen gegen Handelsabkommen (Mercosur/Indien) in sozialen Netzwerken und Foren zu scannen.
2. Erstellung und vorabgestimmte Freigabe von „Holding Statements" und technischen Q&A-Dokumenten, die spezifisch auf potenzielle Vorwürfe zur Unsicherheit von Fahrzeugdaten und autonomen Systemen eingehen, um die Reaktionszeit bei Veröffentlichungen drastisch zu verkürzen.
3. Durchführung von proaktiven Pre-bunking-Briefings für politische Stakeholder, Investoren und Branchenverbände, um über die tatsächliche Position des Konzerns zu den Handelsabkommen aufzuklären und vor Desinformationskampagnen zu warnen, die Verbraucherschutz als Vorwand nutzen.
4. Stärkung und interne Bewerbung legitimer, anonymer Whistleblower-Kanäle, um interner Unzufriedenheit ein sicheres Ventil zu bieten und Mitarbeitern eine konstruktive Alternative zum externen Leaken von angeblichen Missständen aufzuzeigen.
5. Etablierung einer technischen Taskforce, die bereitsteht, um die Authentizität und den Schweregrad von behaupteten Sicherheitslücken oder Datenlecks innerhalb weniger Stunden technisch fundiert zu bewerten.
6. Vorbereitung rechtlicher Notfallpläne und Takedown-Templates (z. B. auf Basis des Geschäftsgeheimnisgesetzes), um bei tatsächlicher Veröffentlichung von geschütztem Source-Code oder vertraulichen Strategiepapieren auf Plattformen unverzüglich Löschungen beantragen zu können.

Stufe Mobilisierung: Aktiver Widerstand, Ablehnung, Boykott von Produkten/Unternehmen

Narrative Frames

- Aktiver Widerstand gegen unternehmerische Restrukturierungsmaßnahmen
- Ablehnung von Produkten aufgrund politischer oder ideologischer Gründe („Kaufstreik“)

Beobachtete Manifestationen	Early Indicators (Digital Listening)
▶ Aufrufe zu Protesten gegen Werkschließungen oder Personalabbau ▶ Boykottaufrufe im Kontext von geopolitischen Spannungen ▶ Forderungen nach staatlicher Intervention oder Protektionismus	▶ Verwendung von Hashtags, die zu konkreten Aktionen aufrufen (z.B. #Boykott, #Protest) ▶ Organisierte Petitionen gegen spezifische Unternehmensentscheidungen oder politische Rahmenbedingungen ▶ Verlinkung von Offline-Ereignissen (Demos) in Online-Foren

Mitigationsmaßnahmen

1. Implementierung eines eng getakteten Monitorings von Social-Media-Plattformen und Messenger-Diensten (insb. Telegram) zur frühzeitigen Identifikation organisierter Protestaufrufe und Boykott-Hashtags.
2. Proaktive und transparente Kommunikation mit dem Betriebsrat und der Belegschaft über interne Kanäle (Intranet, Townhalls), um Gerüchten über Werksschließungen mit verifizierten Fakten und Zeitplänen zuvorzukommen.
3. Erstellung und Bereithaltung von „Dark Sites“ und Argumentationsleitfäden (Q&As), die spezifische ideologische Vorwürfe und Falschbehauptungen zu Produkten oder politischen Positionierungen faktisch widerlegen.
4. Durchführung von präventiven Hintergrundgesprächen mit politischen Entscheidungsträgern und lokalen Behörden, um die wirtschaftliche Notwendigkeit von Restrukturierungsmaßnahmen darzulegen und populistischen Forderungen nach staatlicher Intervention entgegenzuwirken.
5. Schulung des Community-Management-Teams in Deeskalationsstrategien, um auf den eigenen Kanälen sachlich auf Kritik zu reagieren und gleichzeitig Verstöße gegen die Netiquette konsequent zu moderieren.
6. Juristische Prüfung von rufschädigenden Falschbehauptungen oder gewaltverherrlichenden Aufrufen im Rahmen von Protesten und konsequente Meldung rechtswidriger Inhalte gemäß Netzwerkdurchsetzungsgesetz (NetzDG).

Dieses prototypische Szenariobündel wurde durch das KI-gestützte PrediCX-System auf Basis von über eintausend Quelldokumenten generiert. Es zeigt einen möglichen Eskalationsprozess und bietet Ansatzpunkte der aktiven Auseinandersetzung mit möglichen Abläufen auf der Branchenebene. In einer weiteren Konkretion können Szenarien für einzelne Unternehmen dargestellt werden.

3.5 Ausblick und Modell Lagebild „Hybride Angriffe“

Die vorstehend ausgeführten Strukturierungen sind hilfreich, um das Modell eines Lagebildes „Hybride Angriffe“ zu skizzieren.

So wird hier vorgeschlagen, ein solches Unterfangen nicht induktiv aus der unscharf abgegrenzten Menge an Einzelvorkommnissen zu versuchen, sondern deduktiv aus den wahrscheinlichen Zielsetzungen entsprechender Akteure abzuleiten.

Eine zu starke Fokussierung auf festgestellte „Incidents“ verhindert zum einen das Erkennen der übergeordneten Einflussoperationen und legt zum anderen nur sehr partielle Maßnahmen nahe.

Mit dem deduktiven Ansatz können vier strategische Stränge als Angriffskategorien unterschieden werden.

1. Operationen zur Lockerung von Grundüberzeugungen/Destabilisierung
2. Operationen zur Unterstützung eigener Positionen
3. Operationen zur Beeinflussung der Zusammensetzung von Landes-/Bundesparlamenten (Wahlkampfbeeinflussung)
4. Operationen in Bezug auf Entscheidungen von Landes-/Bundesparlamenten (Regierungshandeln)

Es scheint naheliegend, dass diese Stränge in logischer Sequenz durchlaufen werden, um in letzter Konsequenz Regierungshandeln im eigenen Sinne zu beeinflussen, ohne militärische Mittel einsetzen zu müssen. So ist die Hochwert-Kategorie des Einflusses auf Regierungshandeln mit militärischen Mitteln unverhältnismäßig aufwändiger zu erreichen.

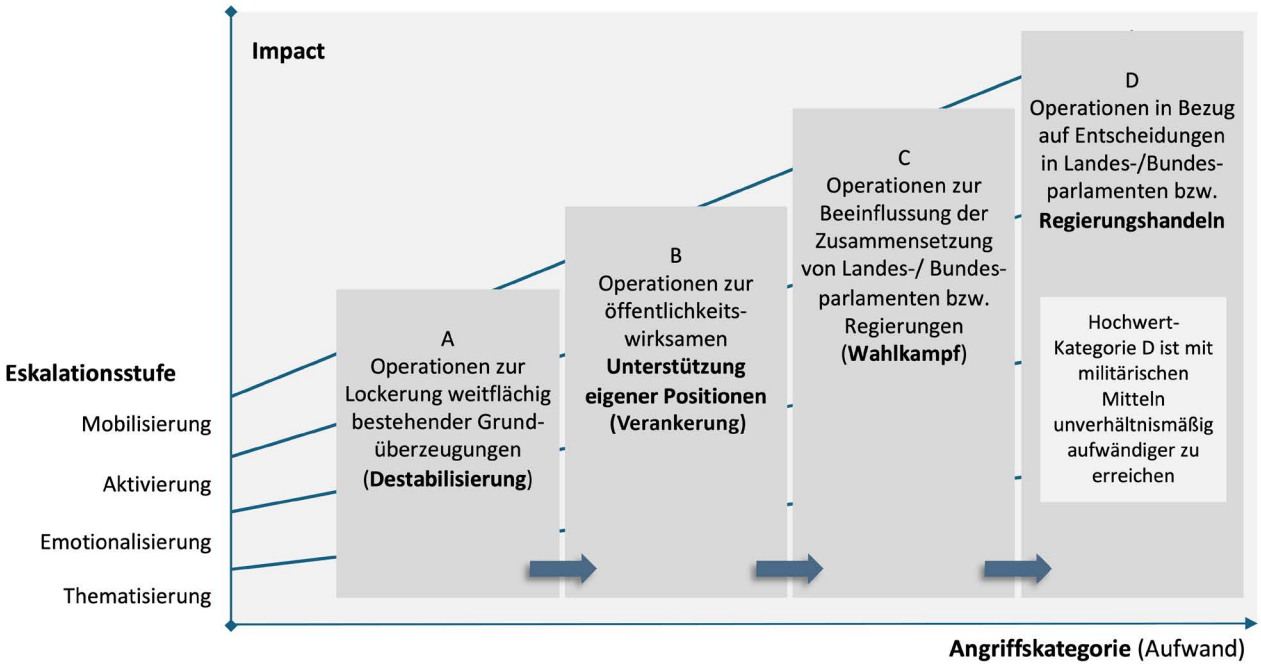


Abbildung 12: Schema Lagebild „Hybride Angriffe“, Quelle: Grothe/complexium.

Der modellhafte Überblick setzt damit die beiden hier ausgeführten Dimensionen in Beziehung:

- **Vier Eskalationsstufen:**
  Thematisierung > Emotionalisierung > Aktivierung > Mobilisierung
- **Vier Angriffskategorien:**
  Destabilisierung > Unterstützung eigener Positionen > Wahlkampfbeeinflussung > Beeinflussung Regierungshandeln

Kognitive sowie kinetische Operationen lassen sich in diesem Rahmen verorten. Damit ist es wichtig, herauszustellen, dass Desinformations- oder Einflusskampagnen nicht final der Destabilisierung dienen sollen, sondern Baustein einer deutlich umfassenderen Zielsetzung sind. Plastisch ausgedrückt: **Niemand geht in die Küche, nur um Wasser zum Kochen zu bringen.**

Es wird aber auch deutlich, dass die angegriffenen Unternehmen, sofern dies nicht aus rein kriminellen Motiven geschieht, primär als indirekte Vehikel eingesetzt werden, um die Dysfunktionalität, De-Industrialisierung und den Niedergang des gesamten Gemeinwesens zu unterlegen. Mit diesem Schluss werden die Ziele der nächsten Kategorie, insbesondere der Wunsch nach einem grundlegenden politischen Wechsel gefördert.

Im Gesamtmodell hybrider Angriffe unterstützen kognitive Einflusskampagnen gegen Unternehmen damit die Beeinflussung von Wahlkämpfen/Wahlausgängen auf Bundes- und Landesebene. Bei einer gewünschten Veränderung der Mehrheitsanteile kann ein Einfluss auf die Regierungsbildung und später Regierungshandeln als Endziel hybrider Angriffe die Folge sein.

Damit kommt dem Umgang mit entsprechenden Angriffen auf Unternehmensebene eine fast staatstragende Bedeutung zu. Hier steht in der Praxis zumeist die Schwierigkeit der operativen Schadensmessung einer tatkräftigen Auseinandersetzung bzw. Mittelallokation im Weg.

Wenn nun auf Unternehmensebene entsprechenden Angriffen wenig entgegengesetzt wird, dann wird dadurch eine Zielsetzung begünstigt, die weit über die Unternehmensreputation hinausgeht. So wäre zu begrüßen, dass trotz des schwer messbaren Schadens, hier eine deutlich höhere Reaktionskraft eingesetzt wird als aktuell feststellbar ist.

Abbildungsverzeichnis

Anhang

Online-Fragebogen

Zu welcher Branche gehört ihr Unternehmen? Bank & Versicherung

Energie & Wasser
Handel
Industrie
ITK
Medien
Dienstleistungen
Sonstige

Welche Mitarbeiterzahl (weltweit) hat ihr Unternehmen?

1 - 1.000
1.001 – 10.000
10.001 – 50.000
50.001 – 100.000
Mehr als 100.000

Wie groß nehmen sie die Bedrohung für ihr Unternehmen durch Desinformation wahr?

Auf einer Skala von 1-10

Welche Bedeutung hat das Thema Desinformation in Ihrem täglichen Arbeitsumfeld?

Auf einer Skala von 1-10

Wie oft wurde ihr Unternehmen im vergangenen Jahr nach Eigenwahrnehmung zum Ziel von Desinformationsangriffen?

ANZAHL: _____

Auf welchen Plattformen begegnet Ihnen Desinformation in Bezug auf ihr Unternehmen?

(Mehrfachauswahl)

Facebook
X
TikTok
Telegram
LinkedIn
Sonstige: _____

Wie bewerten Sie plattforminterne Maßnahmen wie Warnhinweise oder das Entfernen falscher Inhalte?

Facebook	unkompliziert	kompliziert	Keine Erfahrung
X	unkompliziert	kompliziert	Keine Erfahrung
TikTok	unkompliziert	kompliziert	Keine Erfahrung
Telegram	unkompliziert	kompliziert	Keine Erfahrung
LinkedIn	unkompliziert	kompliziert	Keine Erfahrung
Sonstige	unkompliziert	kompliziert	Keine Erfahrung

Wie bewerten Sie die Gefahren von KI-gestützten Fälschungen oder Social Bots für Ihr Unternehmen?

Gering

Mittel

Hoch

K.A.

Wie schätzen sie die negativen Auswirkungen von Desinformationskampagnen ein, die ihr Unternehmen betroffen haben?

Gering

Mittel

Hoch

Noch keine Erfahrungen gemacht

Welche Bereiche innerhalb Ihres Unternehmens sind im Kontext Desinformation involviert bzw. besonders gefordert?

(Mehrfachauswahl)

IT

PR

Kommunikation

Sicherheit

Recht

Sonstige: _____

Welche konkreten Schutzmaßnahmen und Frühwarnsysteme hat ihr Unternehmen aktuell etabliert?

(Mehrfachauswahl)

Online-Monitoring bzw. Social Media Analysis

Mitarbeiterschulungen

Präventive Krisenkommunikation

Sonstige: _____

Welche Rolle spielen Monitoring und Aufklärung in diesem Zusammenhang in Ihrem Unternehmen?

Monitoring	Geringe	Mittlere	Hohe
Aufklärung	Geringe	Mittlere	Hohe

Wie hoch schätzen Sie das Bewusstsein für dieses Thema auf der Leitungsebene (und auch unter Mitarbeitern) ein?

Leitungsebene	Starkes Bewusstsein	Mittleres Bewusstsein	Wenig Bewusstsein
Mitarbeiter	Starkes Bewusstsein	Mittleres Bewusstsein	Wenig Bewusstsein

Würden Sie sich mehr Unterstützung zu diesem Thema von behördlicher Seite / durch rechtliche Rahmenbedingungen wünschen?

JA

NEIN

Kommentar:

Fragebogen für die Interviews

0. Gab es schon Desinformationsangriffe gegen ihr Unternehmen?

Stellen Sie sich vor:

Sie sind Hersteller eines Produktes. Ein Mitarbeiter kommt Freitag nachmittags in ihr Büro: Er habe auf einem X-Account ein Bild gesehen, dass das Produkt in einem Kriegsgebiet zeigt. Inzwischen wird der Post von antimilitaristischen und rechten friedensaktivistischen Accounts empört geteilt. Natürlich ist Ihnen bewusst, dass es sich um eine Fälschung handeln muss, da die Ausschreibung noch gar nicht entschieden ist.

1. Sind Ihre Mitarbeitende auf diesen Fall vorbereitet? Gibt es in Ihrem Unternehmen Schulungen zu den Risiken und zum Umgang mit Desinformation?
2. Setzen Sie Tools zur Erkennung von Desinformation in Ihrem Unternehmen ein?
3. Welche Desinformationsnarrative begegnen Ihnen am häufigsten?
4. Wo sehen Sie mit Blick auf Ihr Unternehmen die größten Schwachstellen/Angriffspunkte für Desinformationskampagnen?
5. Wie verbreitet sich Desinformation Ihrer Meinung nach am häufigsten? Welche Faktoren fördern Ihrer Meinung nach die Verbreitung (z.B. Emotionalität, etc.)?
6. Wen sehen Sie als Hauptakteur/Gefahr/Urheber?
7. Können Sie an Ihren Unternehmensstandorten regionale Unterschiede feststellen?
8. Welche gesetzlichen Regelungen halten Sie für sinnvoll und wirksam? Haben Sie den Eindruck, dass der rechtliche Rahmen Ihren Handlungsspielraum erweitert oder eingrenzt im Umgang mit Desinformation?
9. Wie wichtig ist die Zusammenarbeit zwischen Unternehmen, Behörden, Plattformen und Zivilgesellschaft?
10. Wo sehen Sie den größten Handlungsbedarf? Welche Lücken müssen unbedingt geschlossen werden? Und wer ist dafür jeweils zuständig?
11. Gibt es noch etwas, was Sie im Kontext Desinformationen schon immer mal sagen wollten?
12. Sehen Sie bezüglich dieses Thema Handlungs- oder Unterstützungsbedarf durch die Politik? Wenn ja: welchen?

Autoren

Dr. Christopher Nehring ist Sicherheitsforscher, Analyst und Medienexperte. Er ist Experte für Desinformation und Cyber-Einflussnahme, Cybersicherheit, KI und Deepfakes, OSINT und Nachrichtendienste. Promotion in osteuropäischer Geschichte mit einer Dissertation zur Geheimdienstgeschichte (Zusammenarbeit des KGB mit der ostdeutschen Stasi und dem bulgarischen Geheimdienst) und schreibt regelmäßig für führende deutsche Medien (z. B. Deutsche Welle, Tagesspiegel, NZZ, SpiegelOnline, Welt) zu Sicherheitsthemen. Zu seinen früheren Positionen gehören:

- Intelligence Director am Cyberintelligence Institute in Frankfurt am Main (leitender Forscher für Nachrichtendienste, hybride Bedrohungen und Desinformation/Informationsmanipulation)
- Gastdozent für Desinformation, KI, Nachrichtendienste und Medien am Medienprogramm Südosteuropa der Konrad-Adenauer-Stiftung und an der Fakultät für Journalismus und Massenkommunikation der Universität Sofia
- Senior Analyst am Institute for Global Analysis in Sofia
- Wissenschaftlicher Leiter am Deutschen Spionagemuseum in Berlin (2015–2020).

Für weitere Informationen zu seiner Arbeit und seinem Fachwissen besuchen Sie sein LinkedIn-Profil: https://www.linkedin.com/in/christopher-n-423b06257/

Prof. Dr. Martin Grothe ist Experte für die Früherkennung von aktivistischen und hybriden Bedrohungen im Digitalraum und Geschäftsführer der complexium GmbH in Berlin. Als Pionier auf dem Gebiet des „Digital Listening“ befasst er sich intensiv mit der systematischen Detektion von „Unknown Unknowns“ sowie der Analyse kognitiver Einflussoperationen.

Unter seiner Leitung agiert complexium als spezialisiertes OSINT-Lagezentrum für Konzernsicherheiten. Das Analystenteam des Unternehmens nutzt eine eigenentwickelte Analyseinfrastruktur, die durch den Einsatz des KI-gestützten PrediCX-Systems („Multi-Agent Predictive Corporate Security Intelligence System“) einen signifikanten technologischen Vorsprung erzielt. Durch die tägliche Verarbeitung von bis zu 0,5 Millionen Beiträgen aus diversen digitalen Quellen ermöglicht dieser Ansatz Unternehmen, Bedrohungsszenarien bereits in der Entstehungsphase zu identifizieren und proaktiv „vor die Lage“ zu kommen.

Prof. Dr. Grothe begleitete maßgebliche, vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Verbundprojekte zur zivilen Sicherheit, darunter:

- Mobi diG: Monitoring biologischer Gefahrenlagen in der digitalisierten Gesellschaft durch computerlinguistische Analyse schwacher Signale.
- HybriD: Echtzeiterkennung von Desinformationskampagnen in Online-Medien durch die Kombination maschineller Analyse und menschlicher Expertise.

Seine aktuelle Arbeit konzentriert sich auf die Etablierung von Austauschrunden wie AktiMo (Corporate Security), AktiMEx (Exponierte) und der LageRunde, um die aufgebauten Konzeptionen, Technologien und erkannten Insights kontinuierlich für aufgeschlossene Unternehmenssicherheiten zu nutzen. Die Konstruktion KI-gestützter Lagebilder kann zusammen mit laufendem Digital Listening Beiträge leisten, um die kognitive Resilienz von Unternehmen, Wirtschaft und Gesellschaft nachhaltig zu stärken.

Kontakt: grothe@complexium.de

Der **Verband für Sicherheit in der Wirtschaft, Bundesverband e.V.** (kurz: **VSW-Bundesverband**), vertritt die Sicherheitsinteressen der deutschen Wirtschaft auf Bundesebene und engagiert sich in der Initiative Wirtschaftsschutz. Er stärkt das Bewusstsein für Wirtschaftsschutz in Unternehmen, Politik und Medien und fördert den kontinuierlichen sowie anlassbezogenen Informationsaustausch zwischen Unternehmen und Sicherheitsbehörden.

Darüber hinaus unterstützt der Verband seine Mitglieder durch Schulungen und Qualifizierungsangebote. Die Kompetenz-Center zu den Themen Sabotage- & Spionageabwehr, Lage & Reisesicherheit, Krisenmanagement, Aus- & Weiterbildung, Cyber-Security sowie Wirtschaftskriminalität dienen zudem als Plattformen für Best-Practice-Sharing, fachliche Vernetzung und den Austausch bewährter Standards.

Mitglieder des VSW-Bundesverbandes sind sieben regionale Verbände für Sicherheit in der Wirtschaft sowie vier Fachverbände. Ergänzend bestehen Partnerschaften mit Hochschulen und weiteren Institutionen.

Impressum

Herausgeber:

VSW-Bundesverband
Verband für Sicherheit in der Wirtschaft, Bundesverband e.V.
Bayerischer Platz 6, 10779 Berlin

Telefon: +49 (0)30 24 63 71 73
info@vsw-bundesverband.de
www.vsw-bundesverband.de

complexium GmbH
Oranienburger Str. 50, 10117 Berlin

grothe@complexium.de
www.complexium.de

Stand:

März 2026

Gestaltung:

LÜCKEN-DESIGN
www.luecken-design.de

Haftungsausschuss

Die an der Erstellung der Studie beteiligten Projektpartner, VSW-Bundesverband, complexium und Dr. Christopher Nehring übernehmen keine Haftung für Inhalte oder aus Analysen resultierende Aktivitäten.