GLOBAL NETWORK & INTELLIGENCE

CII WHITE PAPER

Wahlbeeinflussung: Gefahren und Lösungen für Unternehmen

Dr. Christopher Nehring

CYBER|INTELLIGENCE
.Institute

Inhalt

Key Take-aways

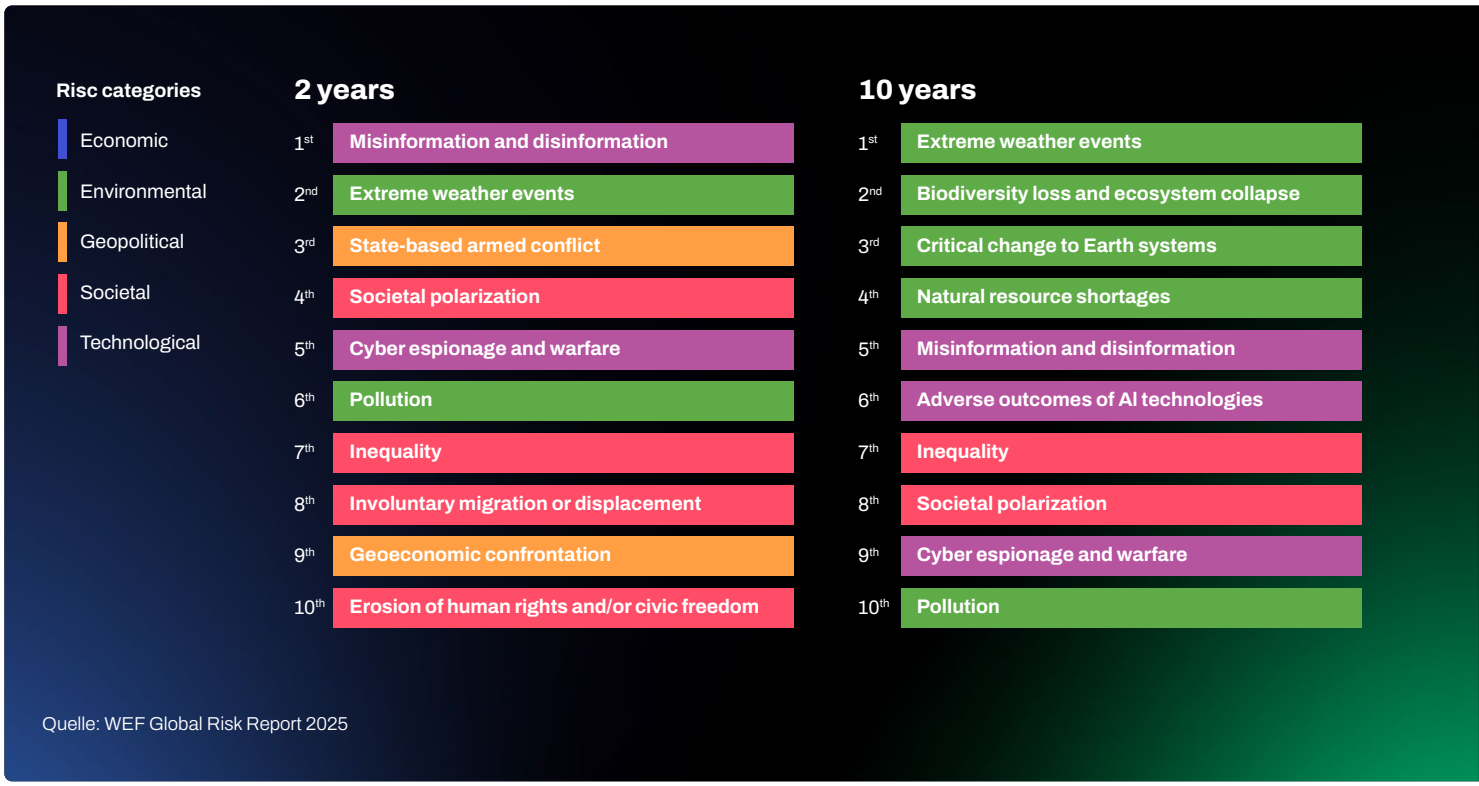
- Wahlbeeinflussung ist eine allgegenwärtige Erscheinung bei über 90 Prozent aller Wahlen weltweit und sorgt für teils erhebliche Verwerfungen.
- Wahlbeeinflussung ist kein rein politisches Phänomen, sondern birgt zahlreiche Risiken für Unternehmen, Verbände, Führungskräfte und Mitarbeiter.
- Die Anzahl gezielter Informations- und Einflussangriffe auf Unternehmen und Organisationen steigt rapide an.
- Gesetzgeberische und regulatorische Maßnahmen (z.B. DSA) haben Probleme und Lücken bei Umsetzung und Durchsetzung und bieten Unternehmen nur bedingt Schutz.
- Unternehmen müssen Wahlbeeinflussung (auch entlang globaler Lieferketten) in ihre Risikoanalysen einbeziehen und in strategische Sicherheitskonzepte übersetzen.

Über den Autor

Dr. Christopher Nehring, Intelligence Director des cyberintelligence.institute in Frankfurt am Main. Er ist Forscher, Analyst und Experte für verschiedene Medien in Deutschland und Europa. Sein Themengebiet umfasst die Arbeit von Geheimdiensten, Desinformation, Hybride Kriegsführung und KI-Cyberrisken (insbesondere Deepfakes und Manipulationen). Er war Gastdozent und Experte für Desinformation des Medienprogramms der Konrad-Adenauer-Stiftung, wissenschaftlicher Leiter des Spionagemuseums Berlin sowie Senior Analyst des Institute for Global Analysis. Dr. Nehring ist regelmäßiger Gastautor und Experte für zahlreiche Medien (z.B. ARD, Tagesspiegel, Spiegel, NZZ, Welt etc.), als Speaker, Trainer, Kursleiter und Berater ist er für verschiedene Unternehmen, IHKs, Stiftungen und Medienorganisationen tätig.

Kontakt: christopher.nehring@cyberintelligence.institute

Einleitung:
Warum Wahlbeeinflussung ein Problem für Unternehmen ist



Quelle: WEF Global Risk Report 2025

Zweimal hintereinander – 2024 und 2025 – wählte das Weltwirtschaftsforum WEF Desinformation in Kombination mit künstlicher Intelligenz (KI) und Wahlen zum globalen Risiko Nr. 1![1] Doch Wahlbeeinflussung und Desinformation sind nicht nur politische Phänomene, sondern betreffen auch Unternehmen und Wirtschaftsakteure direkt. Wahlbeeinflussung ist vor allem in den vergangenen zehn Jahren zu einem immer größeren Problem für Unternehmen geworden. Dabei geht es weniger bzw. nicht nur darum, ob der Ausgang einer Wahl durch innere oder äußere Akteure effektiv gestört und manipuliert werden kann und welche Folgen dies für das (wirtschafts-)politische Umfeld und das Agieren von Unternehmen hat. Vielmehr geraten Unternehmen immer öfter selbst direkt in die Schusslinie und werden zum Opfer von Image- und Reputationsangriffen, wahlbezogenen Cyberattacken, inszenierten oder gekauften Protestaktionen, Sabotage etc. Im Zeitalter der „Multi-Krisen“ und gesellschaftlicher Polarisierung werden auch Unternehmen zu politischen Akteuren und Zielscheiben politisch motivierter Angriffe – auch entlang globaler Lieferketten!

Mit dieser Studie richtet sich das cyberintelligence.institute deshalb direkt an Unternehmen, Wirtschaftsverbände und andere private Organisationen, um über die Gefahren von Wahlbeeinflussung aufzuklären. Dazu werden hier anhand realer Fallbeispiele die direkten und indirekten Risiken und Gefahren (z.B. Reputationsschäden, Produktionsausfälle, Datenausfälle, oder rechtliche Anforderungen) von Wahlbeeinflussung für Unternehmen aufgezeigt. Darüber hinaus gibt die Studie einen Überblick über Formen, Taktiken, Strategien und Urheber hinter Wahlbeeinflussung sowie hinsichtlich benutzter Technologien. Darauf aufbauend gibt die Studie konkrete Handlungsempfehlungen und skizziert Lösungs- und Abwehrstrategien.

1 Siehe: https://www.weforum.org/publications/global-risks-report-2025/.

Teil 1:
Das Einmaleins der Wahlbeeinflussung

Was ist Wahlbeeinflussung?

Wahlbeeinflussung (engl. „**election interference**“) kann definiert werden als Versuche, das Ergebnis von Wahlen durch unfaire bzw. illegitime Maßnahmen absichtsvoll zu beeinflussen, die gegen die Grundsätze demokratischer Wahlen (z.B. Freiheit, Gleichheit und Allgemeinheit) verstoßen. Wahlbeeinflussung unterscheidet sich damit von legitimem, ebenfalls interessengeleitetem Wahlkampf mit den legitimen politischen Organisationen, die um Einfluss, Stimmen und Macht werben. Im Gegensatz zum demokratischen Wahlkampf verletzt Wahlbeeinflussung demokratische Prinzipien und Wahlrechtsgrundsätze, benutzt Methoden wie Desinformation oder Cyberangriffe, die über legale politische Werbung und Argumentation hinausgehen, zielt auf die Manipulation von Medien, Organisationen und Wählern, beruht auf Drohungen, Täuschungen und Falschinformationen und wird zumeist von Akteuren (z.B. ausländischen Staaten oder Firmen) durchgeführt, die keine Legitimation für wahlbezogene Aktivitäten haben.

Wie werden Wahlen beeinflusst? Formen, Taktiken und Technologien der Wahlbeeinflussung

Wahlbeeinflussung – aus dem **In- oder Ausland** – kann **offen** (d.h. mit einem öffentlichen Absender und Ursprung) oder **verdeckt** (d.h. hinter „Stellvertretern“, anonym oder getarnt und mit verwischten Spuren) stattfinden. Häufige Formen und Instrumente sind dabei:

- **Cyberattacken**,
- **Desinformation**, Informationskrieg und Cyber-Influence-Angriffe,
- offene oder verdeckte **Stellvertreter**,
- offene oder verdeckte **finanzielle Unterstützung**,
- inszenierte oder angestachelte **Offline-Aktionen**.

Online- und Offline-Aktivitäten sind dabei oft eng miteinander verbunden. **Cyberattacken** werden z.B. häufig strategisch eingesetzt, um Auswirkungen in der physischen Realität zu haben (z.B. die Störung bestimmter Services). **Hacking und Leaking**-Angriffe verbinden Cyberattacken mit Informationsangriffen durch die gezielte Veröffentlichung bestimmter Informationen, die ihre Wirkung „offline“ entfalten sollen.

Online-**Desinformationskampagnen** greifen gleichzeitig Offline-Aktionen (z.B. inszenierte und angestachelte Proteste oder Sabotagen) auf und vervielfältigen den Effekt, um Reaktionen in der physischen Welt zu gene-

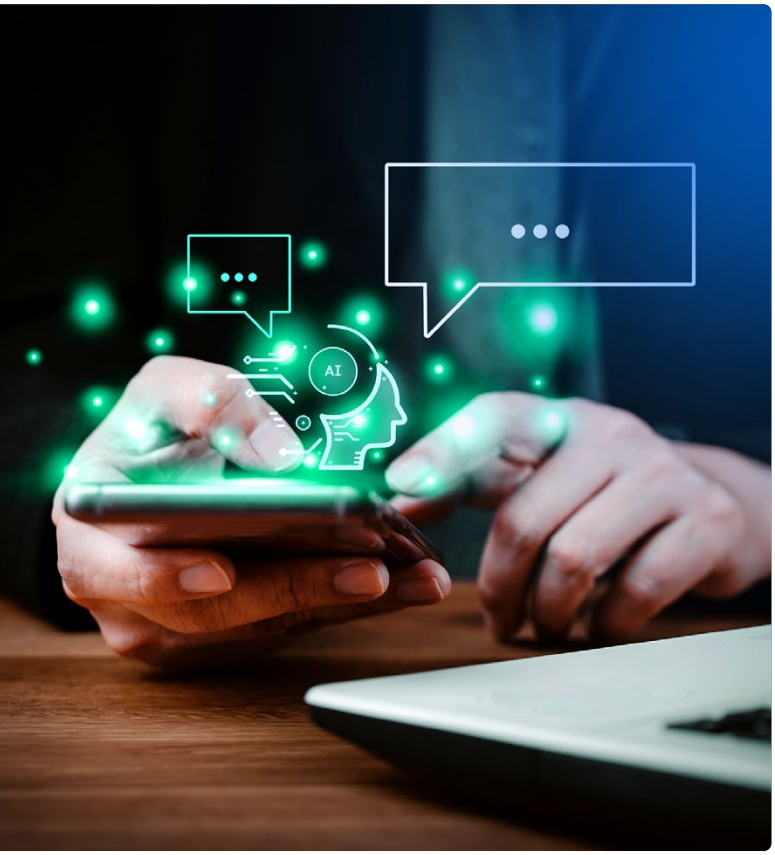
> **On- und Offline-Aktivitäten sind dabei oft eng miteinander verbunden.**

rieren. So werden z.B. Protestaktionen einerseits durch Online-Kampagnen angestachelt und andererseits durch einen Kreislauf aus ständigen Falschinformationen anschließend vervielfältig und weitergetrieben. Ein Beispiel in Deutschland dafür war zum Beispiel der „Fall Lisa“ um die vorgetäuschte Vergewaltigung eines russlanddeutschen Mädchens in Berlin im Jahr 2016;[2] oder 2023 in UK der Audio-Deepfake des Londoner Bürgermeisters Sadiq Khan, der zu Ausschreitungen von über 1.000 Personen aus meist rechtsradikalen Gruppen führte.[3]

Für den Angegriffenen erscheinen diese verschiedenen Online- und Offline-Angriffe oftmals getrennt und unverbunden abzulaufen. Der Angreifer jedoch, der eine Wahl beeinflussen will, denkt sie zusammen, organisiert sie strategisch aus einer Hand und multipliziert ihre Effekte.

2 Siehe: https://www.bpb.de/themen/migration-integration/russlanddeutsche/271945/der-fall-lisa/.
3 Siehe: https://www.bbc.com/news/uk-68146053.

Bei den benutzten **Technologien** zur Wahlbeeinflussung im Online-Raum kommt die gesamte Bandbreite zur Verfügung stehender Instrumente zum Einsatz. Dies reicht vom Einsatz von Schadsoftware für Computer-Netzwerk (CNE)- und Penetrations-Angriffe, DDoS-Malware sowie Ransomware bis hin zu „Hacking & Leaking"-Taktiken, bei denen in IT-Systeme zum Diebstahl vertraulicher Informationen (E-Mails, Dokumente o.Ä.) eingedrungen wird und anschließend die Informationen über eigens geschaffene Websites, Leak-Plattformen oder Social Media veröffentlicht werden. Im Bereich der Cyber-Influence-Aktivitäten und Desinformation kommen z.B. automatisierte Social-Media-Profile („bots") und menschliche „Trolle" zum Einsatz, die untereinander auch Netzwerke bilden, um bestimmte Meldungen und Botschaften zu verstärken. Durch dieses massive, sog. „unauthentische (sprich: nichtmenschliche) Verhalten" sollen nicht nur bestimmte Narrative gepusht werden, sondern auch die Ausspielungsalgorithmen von Online-Plattformen (also die Programme, die festlegen, welche Nachrichten, Informationen und Profile anderen Nutzern automatisch angezeigt werden) manipuliert werden. Dadurch wird Botschaften mehr Aufmerksamkeit verliehen und Themen, Inhalte, Debatten, Personen und Profile erscheinen größer und wichtiger, als sie eigentlich sind („astroturfing" und eine „herbeigeführte kollektive Mobilisierung"[4]). Die neueste Technologie bei Online-Cyber-Influence-Attacken ist generative KI (genAI). Mithilfe verschiedener genAI-Applikationen können nahezu auf Knopfdruck Texte, Artikel, Posts, Kommentare, Bilder, Videos und Tondateien erstellt werden. Zahlreiche Akteure – insbesondere rechtspopulistische Parteien und Gruppierungen sowie Russland zugeschriebene Firmen und Hackergruppen – haben diese Tools erwiesenermaßen seit 2022 massiv zur Erstellung von wahlbezogener Falschinformation genutzt.



Wer beeinflusst Wahlen? Die Angreifer

Die **Auftraggeber und Hintermänner** von Wahlbeeinflussung können im Inland oder im Ausland sitzen und staatliche oder privat organisierte Akteure sein. Die Bandbreite der Auftraggeber von Wahlbeeinflussung ist heterogen und umfasst z.B. extremistische und undemokratische Parteien und ausländische Regierungen. Bei **Parteien** greifen besonders oft (links- und rechts-)extreme „Anti-System-Parteien" auf unlautere Mittel der Wahlbeeinflussung zurück. Bei ausländischen **Staaten und Regierungen** hingegen sind autoritäre wie Staaten Russland, China, Iran, Nordkorea oder die Golfstaaten besonders aktiv. In demokratischen Staaten (USA, teilweise auch Israel, früher auch UK und Frankreich) ist das Phänomen der illegitimen Wahlbeeinflussung zwar nicht gänzlich unbekannt, tritt jedoch wesentlich seltener und beschränkter auf, ist moralisch und rechtlich geächtet und gehört nicht zu den normalen Handlungsweisen.

> **Die Bandbreite der Auftraggeber von Wahlbeeinflussung ist heterogen und umfasst z.B. extremistische und undemokratische Parteien und ausländische Regierungen.**

4 Siehe hierzu: Katja Muñoz: Influencers and Their Ability to Engineer Collective Online Behavior, DGAP Policy Brief 23, hg.: German Council on Foreign Relations, 2024, https://doi.org/10.60823/DGAP-24-41340-en.

Private Organisationen (z.B. ausländische Unternehmen, Oligarchen) sind in der Vergangenheit ebenfalls bereits mit Aktionen zur Wahlbeeinflussung in Erscheinung getreten. Dies stellt für Unternehmen vor allem dann eine Gefahr dar, wenn direkte wirtschaftliche Interessen damit verbunden sind.

Zur Durchführung und Umsetzung von Wahlbeeinflussung greifen diese Auftraggeber (allen voran autoritäre Staaten) auf verschiedene Instrumente, Handlanger und Stellvertreter zurück:

- Geheimdienste,
- Stellvertreter-Parteien in anderen Ländern,
- gekaufte Medien, gekaufte oder angeworbene Journalisten und Influencer sowie gekaufte oder angeworbene öffentliche Personen („Einflussagenten"),
- private Hackergruppen,
- private PR-Firmen (beispielsweise als Auftragnehmer von ausländischen Regierungen oder Geheimdiensten fremder Mächte).

Gerade in den vergangen zehn Jahren hat sich gezeigt, dass in- und ausländische Akteure (gerade im Cyberraum) immer schwerer voneinander zu unterscheiden sind. So unterstützt Russland z.B. sowohl kommunistische als auch rechtspopulistische Parteien und Strömungen in anderen Staaten offen als auch

> **Gerade in den vergangen zehn Jahren hat sich gezeigt, dass in- und ausländische Akteure (gerade im Cyberraum) immer schwerer voneinander zu unterscheiden sind.**

verdeckt. Und auch die Grenze zwischen privaten und staatlichen Akteuren verschwimmt immer weiter. Waren z.B. im Kalten Krieg Geheimdienste das Hauptinstrument für staatlich gesponserte verdeckte Wahlbeeinflussung, vergeben heute Regierungen (z.B. Russland oder Golfstaaten) Aufträge an private PR-Firmen, die Cyber-Influence-Operationen im Online-Raum durchführen.[5] Auch die Verbindung zwischen Staat, Geheimdiensten und einzelnen bekannten Hackgruppen, z.B. in Russland, China oder Nordkorea, ist oftmals nicht im Detail nachzuvollziehen. Manchmal treten diese Gruppen vordergründig als kriminelle Organisation (z.B. zur Erpressung von Lösegeld) und manchmal als Angreifer im staatlichen Auftrag auf. Einzelne Aktionen und Angriffe auseinanderzuhalten und korrekt zu attribuieren, ist oftmals, wenn überhaupt, nur mit großem Aufwand und entsprechenden Ressourcen möglich.

Ziele und Strategien der Angreifer

Das **Ziel** von Versuchen der Wahlbeeinflussung (aus dem In- oder Ausland) ist in der Regel, eine bestimmte Partei und/oder einen bestimmten Kandidaten zu stärken. Ausländische Akteure erhoffen sich davon, ihre außen-, sicherheits- und wirtschaftspolitischen Interessen durchsetzen und stärken zu können; inländische Akteure hingegen wollen politische und wirtschaftliche Macht erreichen. Im Gegensatz zum legitimen Wahlkampf, der politische Programme, Positionen und Personen bewirbt und „positiv" überzeugen möchte, zielen die meisten Wahlbeeinflussungsversuche auf „negative" Effekte und Manipulation. In vielen Fällen – gerade bei ausländischer Wahlbeeinflussung – geht es dabei mangels Erfolgschancen nicht immer um einen Wahlgewinn, sondern um gezielte **Destabilisierung**. Je polarisierter eine Gesellschaft und je blockierter das politische System, desto geschwächter ist ein Staat (so z.B. das Kalkül hinter vielen russischen Einflussversuchen). Hier geht es dann oft darum, einen größtmöglichen Schaden zu erzeugen, Ängste zu schüren, gesellschaftliche Gräben zu vertiefen und zu spalten. Für den Wahlkampf in Deutschland, zum Beispiel, setzte eine von der russischen Präsidialverwaltung beauftragte PR-Firma gezielt darauf, „Angst" in der deutschen Gesellschaft zu verstärken.[6] Dies sollte nicht nur der präferierten Partei, sondern eben auch der Lähmung und Schwächung des Landes dienen. Zur Steigerung von „Angst", Lähmung, Spaltung und

5 Vgl. z.B. zur russischen PR-Firma „SDA": https://www.tagesschau.de/investigativ/ndr-wdr/russland-propaganda-fakenews-sda-deutschland-100.html; zu einer israelischen Einflusskampagne: https://www.nytimes.com/2024/06/05/technology/israel-campaign-gaza-social-media.html; zur israelischen Firma „Percepto", die Wahlbeeinflussung in Afrika als Geschäftsmodell anbot: https://disinfo.africa/robot-wars-how-to-build-a-bot-to-subvert-elections-9f739411aa39.

6 Siehe den Bericht des US-Justizministeriums inkl. der detaillierten FBI-Berichte: https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence; und: https://www.tagesschau.de/investigativ/ndr-wdr/russland-propaganda-fakenews-sda-deutschland-100.html.

Blockaden kommt dann das gesamte Arsenal hybrider Bedrohungen (Cyberattacken, Sabotage, inszenierte Proteste, Desinformation etc.) zum Einsatz.

In den vergangenen Jahren besonders oft identifizierte **Themen von Wahlbeeinflussungskampagnen** sind:

- Angriffe auf Wahlintegrität (gestohlene oder manipulierte Wahlen),
- Schmieren- und Diffamierungskampagnen gegen einzelne Personen (insbesondere falsche strafrechtliche Vorwürfe, sexuelle Belästigungen, Zuschreibung falscher bzw. übertriebener politische Auffassungen etc.),
- russischer Angriffskrieg gegen die Ukraine und westliche Unterstützung für die Ukraine,
- Nahost-Konflikt,
- Rüstung und Frieden,
- Migration, Asyl und Einwanderung,
- LGTBQ- und andere Minderheitenrechte,
- soziale Ängste,
- wirtschaftlicher Abstieg/Ängste,
- Versorgungsengpässe.

Zum **Ziel von Wahl-Beeinflussungsangriffen** werden dabei insbesondere:

- Organisationen, Institutionen und Unternehmen der Wahlinfrastruktur,
- Medien, Journalisten, Influencer,
- Parteien, politische Organisationen und Politiker,
- gesellschaftlich und öffentlich exponierte Persönlichkeiten,
- Social-Media-Diskurse und -Plattformen,
- Verbände und Interessensvertretungen,
- Unternehmen.

Teil 2:
Risiken und Gefahren von Wahlbeeinflussung für Unternehmen

Unternehmen geraten in der Regel auf **zwei Arten** ins Kreuzfeuer politischer Wahlbeeinflussung: Entweder sie werden, erstens, zur **direkten Zielscheibe** vor allem von Desinformationsattacken. Oder sie werden, zweitens, zu einem **Kollateralschaden**, werden also mehr oder weniger zufällig Opfer solcher Angriffe.

A) Direkte Gefahren

1. Direkte Reputationsangriffe

Unternehmen, aber auch exponierte und gesellschaftlich bekannte Führungskräfte können zum Ziel direkter Kampagnen und von Cyber-Influence-Operationen werden. Nicht immer müssen Unternehmen oder Personen auch politisch aktiv sein, um zur Zielscheibe zu werden. Solche Schmierenkampagnen ähneln jenen aus dem politischen Bereich und finden heutzutage vor allem in sozialen Medien und auf Online-Plattformen statt (erreichen jedoch einen „Spillover"-Effekt, wenn sie groß genug werden). Hier werden v.a. Falschinformationen und Angriffe durch Bots und Trolle eingesetzt, um Unternehmen, Marken, Firmen und Personen schlechtzumachen und das öffentliche Vertrauen in sie zu erschüttern. Anders als bei „normalen Reputationsangriffen", haben diese Angriffe mit Falschinformationen aber einen politischen Hintergrund und ein entsprechendes Ziel (und die Urheber sind zumeist politischen Akteure, nicht konkurrierende Unternehmen).

Beispiel A: Politische Agitation durch die AfD in Thüringen

2024 engagierte sich der Verband der Familienunternehmer im Zuge der Landtagswahlen in Thüringen aktiv gegen die AfD, ihre Wirtschafts- und Einwanderungspolitik. Daraufhin griff der Vorsitzende der AfD Thüringen, Björn Höcke, den Verband sowie die beteiligen Unternehmen öffentlich an mit den Worten: „Ich hoffe, dass diese Unternehmen in schwere, schwere wirtschaftliche Turbulenzen kommen", und Unternehmer sollten „die Klappe halten", wenn es um Politik gehe.[7]

Beispiel B: Trump-Attentat und BlackRock-Verschwörung

Während des US-Präsidentschaftswahlkampfs 2024 kam es zu zwei Attentatsversuchen auf Donald Trump. Der erste Attentäter, Thomas Crooks, spielte als Student in einem Werbevideo des globalen Vermögensverwalters „BlackRock" mit. Schon dies sorgte für massenhafte Social-Media-Posts und Kommentare über eine angebliche Verschwörung und Urheberschaft von BlackRock hinter dem Attentat. Nach dem zweiten Attentatsversuch tauchten dann noch mehr Posts, Videos etc. auf, die den zweiten Attentäter, Ryan Routh, ebenfalls als ehemaligen BlackRock-Mitarbeiter darstellten. Dies waren jedoch Fälschungen. Nichtsdestoweniger hatte die Firma mit Anfeindungen, Beschuldigungen und Reputationsangriffen zu tun, vor allem vonseiten von Verschwörungstheoretikern und organisierten Trump-Unterstützern.[8]

Beispiel C: Kostenloser Starbucks-Kaffee für illegale Migranten

Migrationspolitik spaltet westliche Gesellschaften seit Jahren. In den USA kam das zum Beispiel die Kaffeeshop-Kette „Starbucks" zu spüren. Nachdem Präsident Trump 2017 ein Dekret zum Einreise-Stopp von Migranten erlassen hatte, kündigte das Unternehmen öffentlich an, 10.000 Migranten einstellen zu wollen. Rechte Aktivisten und Anhänger von Donald Trump griffen das Unternehmen deswegen gezielt mit Störaktionen an. Über das in rechten Kreisen beliebte Netzwerk „4chan" wurden gefälschte Gutscheine verbreitet, mit denen angeblich jeder illegale Migrant in den USA 40 Prozent

7 Siehe: https://www.familienunternehmer.eu/vor-ort/lb-thueringen/presse/pressemitteilungen-thueringen/detail/die-familienunternehmer-in-thueringen-zu-hoeckes-hetze-gegen-unternehmen.html.

8 Siehe z.B.: https://www.newstatesman.com/business/2024/07/why-the-internet-blames-blackrock.

Rabatt auf alle Starbucks-Artikel in jedem Starbucks-Laden bekäme.[9] Ein Jahr später, nach einer Verhaftung von zwei Afroamerikanern in einem Starbucks-Laden, zirkulierten erneut gefälschte Gutscheine für Gratis-Kaffee „nur für people of colour".[10] Die Aktionen waren gekennzeichnet von koordiniertem Vorgehen in der Online-Welt und der physischen Realität und zeichneten sich durch ein gewisses Maß an Professionalität aus (Deckname „Operation Mermaid").

Beispiel D: Hersteller elektronischer Wahlmaschinen in Venezuela und Bulgarien

Die Firma „Smartmatik" ist einer der weltweit führenden Hersteller von Maschinen zur elektronischen Stimmabgabe. Sie steht besonders oft im Mittelpunkt politisierter Informationsangriffe. Hintergrund: reale Wahlmanipulation oder Verschwörungstheorien über angebliche Wahlmanipulation. Letzteres ist seit rund zehn Jahren ein Dauermotiv rechtspopulistischer Gruppierungen weltweit und besagt, dass solche Wahlmaschinen vorprogrammiert seien, links-liberale Parteien und Kandidaten zu begünstigen. Deshalb plädieren diese Akteure nicht nur für die Stimmabgabe per Zettel, sondern versuchen auch, die Technologie an sich mit allen Mitteln zu diskreditieren. Smartmatik wurde etwa 2024 im Zuge der Wahlen in Venezuela wieder gezielt angegriffen. Die offensichtliche Wahlmanipulation von Präsident Maduro färbte hier ab und wurde teilweise auch offen der Herstellerfirma zugeschrieben (obgleich Beobachter der Wahl zeigten, dass bei der Stimmabgabe die Opposition eine Mehrheit erhielt und die Maschinen diesen Input korrekt verarbeiteten, die Manipulation also später stattgefunden haben muss).[11]

Smartmatik und der Fall Venezuela hatten Auswirkungen auch in der EU. Im Zuge der sieben Parlamentswahlen in Bulgarien seit 2020 geriet die Firma „Siela Norma", die die Maschinen von Smartmatik in dem Balkanland vertreibt und einsetzt, immer wieder ins Kreuzfeuer öffentlicher Debatten und Angriffe. Wie in vielen westlichen Ländern, war der Einsatz elektronischer Geräte zur Stimmabgabe auch in Bulgarien hochgradig umstritten und polarisierte. Realer Hintergrund war neben den globalen Verschwörungstheorien, dass ältere Wähler Stimmzettel und jüngere Wähler elektronische Geräte bevorzugten, sodass Parteien mit älterer Stammwählerschaft z.B. ein höheres Interesse daran hatten, keine elektronischen Geräte einzusetzen. Im Fall Bulgariens ging es 2021 (und nochmal 2023) sogar so weit, dass der Inlandsgeheimdienst kurz vor der Wahl öffentlich Stellung gegen Wahlmaschinen bezog bzw. Razzien durchführte, bei denen große Mengen solcher Maschinen angeblich in Lagerhäusern gefunden wurden. Als Resultat wurde die elektronische Stimmabgabe teilweise nur zwei Tage vor der Wahl verboten. Die Firma Siela Norma geriet (auch aufgrund ihrer Beziehungen zur langjährigen Regierungspartei und eines Quasi-Monopols) dabei immer wieder direkt ins Zentrum hochpolitisierter Auseinandersetzungen.[12] Ein langfristiger Imageverlust (und potenziell auch ein Auftragsverlust) war die Folge.

> **Eine weitere direkte Gefahr für Unternehmen ist es, durch wahlbezogene Imageangriffe, Cyberattacken oder sogar Sabotage direkte finanzielle Schäden zu erleiden.**

2. Finanzielle Schäden

Eine weitere direkte Gefahr für Unternehmen ist es, durch wahlbezogene Imageangriffe, Cyberattacken oder sogar Sabotage direkte finanzielle Schäden zu erleiden. Diese können durch Boykott-Aufrufe, einbrechende Verkäufe und Nachfrage, aber auch Produktionsausfälle zustande kommen. Gerade in polarisierten Gesellschaften und politischen Räumen besteht fernerhin die konkrete Gefahr, dass sich andere Unternehmen von Werbung, Kooperationen und Aufträgen aufgrund politischer Positionierung von Unternehmen zurückziehen.

9 Siehe: https://www.businessinsider.com/fake-news-starbucks-free-coffee-to-undocumented-immigrants-2017-8.

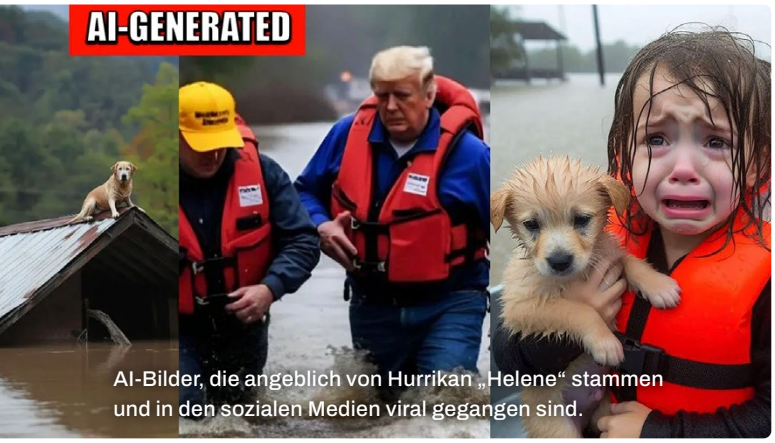
10 Siehe: https://www.nbcnews.com/business/business-news/trolls-spread-hateful-fake-starbucks-coupon-n867501.

11 Siehe ausführlich: Javier Corrales, Dorothy Kronick: How Maduro Stole Venezuela's Vote. Journal of Democracy, vol. 36 no. 1, 2025, p. 36–49. Project MUSE, https://dx.doi.org/10.1353/jod.2025.a947882; und: https://www.ceps.eu/venezuelas-election-shows-that-technology-can-be-democracys-ally-and-not-only-an-enemy/.

12 Siehe: https://www.mediapool.bg/oshte-199-mashini-za-glasuvane-byaha-otkriti-v-sklad-v-sofiya-rashkov-razporedi-proverka-news328692.html; https://www.mediapool.bg/istoriyata-na-mashinniya-vot-u-nas-kato-tuka-ima--tuka-nema-news342174.html; und: https://www.mediapool.bg/edno-kam-edno-kak-dans-udari-mashinnoto-glasuvane-news352776.html.

Beispiel A: Coca-Cola-Boykott US-Wahl 2024

In den USA bietet Coca-Cola über ihre Website den Service an, sich Cola-Dosen nach Wunsch mit persönlichen Slogans und Botschaften bedrucken zu lassen. Während der heißen Phase der US-Wahl im Herbst 2024 verbreiteten Anhänger von Donald Trump auf einmal wütende Proteste und Boykottaufrufe gegen Coca-Cola. Der Grund: Angeblich bevorzuge die Firma Trumps Konkurrentin, US-Vizepräsidentin Kamala Harris, wohingegen ein persönlicher Aufdruck mit Trump und seinen Slogans nicht möglich sei. Dazu wurden offensichtlich gefälscht Snapshots als „Beweis" geteilt. Alleine der Original-Post verbreitete sich über zwei Millionen Mal.[13] Für Coca-Cola bedeutete dieser – unwahre – Vorwurf einen enormen Schaden: Erstens erlitten Verkäufe kurzzeitig einen Einbruch durch den Boykott von Trump-Anhängern; zweitens erlitt die Marke einen (zumindest kurzzeitigen) Imageschaden; und drittens band der Vorfall enorme interne Ressourcen (PR, Kommunikation, Krisenmanagement). Insofern interne Überprüfungen der Produktionsanlangen und -prozesse notwendig waren, entstanden gleichfalls Schäden durch kurzeitigen Ausfall von Produktionskapazitäten.



AI-Bilder, die angeblich von Hurrikan „Helene" stammen und in den sozialen Medien viral gegangen sind.

Beispiel B: Desinformation und Verschwörungstheorien über Hurrikan „Milton" und die Waldbrände in Los Angeles 2025

Nicht nur politische Aktivitäten, sondern auch jede Art von Großereignissen (z.B. Sportveranstaltungen wie Olympia) und vor allem Naturkatastrophen werden heutzutage zum Gegenstand politisierter Desinformation. Diese politisch motivierten Falschinformationen können jedoch auch Unternehmen, ihre Interessen und Geschäftsprozesse massiv stören. Hintergrund ist zumeist, dass populistische und extreme politische Akteure versuchen, Staat und Regierung Versagen und Korruption bei der Bekämpfung und der Versorgung von und nach Naturkatastrophen nachzuweisen. Beispiele waren zum Beispiel die Flut im Ahrtal 2021, Hurrikan „Milton" im Oktober 2024 oder die Waldbrände in Los Angeles 2025. Gerade kurzfristig kann es so zu massiver Verwirrung von Bürgern, aber auch betroffenen Unternehmen kommen, wenn es zum Beispiel um Zuständigkeiten, Ansprechpartner, Versicherungsgewährleistungen, kurzfristige finanzielle Hilfen, Untersuchungen oder Notversorgung geht.

Beispiel C: X/Twitter vs. Bluesky und Tesla nach US-Wahl 2024

Die Social-Media-Plattform X (ehemals Twitter) geriet im Zuge der US-Präsidentschaftswahlen 2024 aufgrund der Nähe und Agitation ihres Eigentümers Elon Musk zu Donald Trump in den Fokus vieler Auseinandersetzungen. Für die Firma und ihr Geschäft hat dies mitunter weitreichende Folgen: So kündigten zum Beispiel einige namhafte globale Unternehmen wie z.B. IBM ihre Werbung auf X, weil die Plattform Hassrede befördere statt bekämpfe.[14] Schon damals etablierte sich die Plattform Bluesky als Alternative. Nach der Wahl vom November 2024 kam es nicht nur zum Rückzug von Werbeanzeigen und Kunden, sondern auch zur massiven, millionenfachen Verbreitung von Falschnachrichten darüber, dass sich bestimmte Marken und Firmen von X zurückzögen und zu Bluesky wechselten.[15] In Deutschland kündigten zum Beispiel Mercedes und BASF an, keine Werbung mehr auf X kaufen zu wollen. Nachdem Musk seine politischen Aktivitäten bei der Unterstützung rechtspopulistischer Parteien auch im Hinblick auf die Bundestagswahl 2025 in Deutschland ausgeweitet hatte, gingen einige Unternehmen (z.B. der Freiburger Energieversorge badenova, der niedersächsische Massivhausbauer Viebrockhaus und die Handelskette Rossmann) dazu über, auf Tesla-Fahrzeuge als Dienstwagen zu verzichten und Verträge zu kündigen.[16]

13 Siehe ausführlich zu dem Fall: https://www.newsguardrealitycheck.com/p/calls-to-boycott-coke-for-false-claim.

14 Siehe z.B.: https://www.washingtonpost.com/technology/2023/11/17/elon-musk-x-companies-pulling-ads-anti-semitism/.

15 Siehe z.B.: https://substackcdn.com/image/fetch/f_auto,q_auto:good,fl_progressive:steep/https%3A%2F%2Fsubstack-post-media.s3.amazonaws.com%2Fpublic%2Fimages%2F65848e14-4d1b-4db0-93d7-f8ff15195bc7_1206x890.png.

16 Siehe auch: https://www.tagesschau.de/wirtschaft/unternehmen/musk-imageschaden-firmen-100.html.

3. Politische Oligarchisierung von Wirtschaftsprozessen

Vor allem seit der US-Präsidentschaftswahl von 2024 tritt (auch im globalen Westen) ein neues Phänomen zutage, das vorher zumeist nur aus dem ehemaligen sozialistischen Osten bekannt war: der Einfluss sog. Oligarchen auf politische Prozesse bzw. direkte Formen der Wahlbeeinflussung durch Oligarchen im In- und Ausland. Diese haben dabei vor allem auch wirtschaftliche Interessen. Niemand verkörpert dieses Phänomen so gut wie Elon Musk, der sich seit 2024 als exponierter „Polit-Influencer" betätigt und dabei die gesamte Macht seiner Online-Plattform X, seiner persönlichen Reichweite und seines Reichtums einsetzt. Wahlbeeinflussung findet hier z.B. durch monetäre Wahlgeschenke, persönliches Werben sowie vor allem über eigene Messages als auch die Bevorzugung einiger politischer Ansichten oder Kandidaten auf seiner Plattform statt.[17]

Beispiel: Elon Musk

Für Unternehmen ergeben sich daraus vielfache Risiken und Konsequenzen: Dieser neue Typus von Großunternehmern als „Polit-Influencer und Polit-Oligarchen" ist gepaart mit enormen Risiken und Herausforderungen für Unternehmen. Einerseits besteht dies in einer zunehmenden Politisierung von Wirtschafts-

> **Niemand verkörpert dieses Phänomen so gut wie Elon Musk, der sich seit 2024 als exponierter „Polit-Influencer" betätigt und dabei die gesamte Macht seiner Online-Plattform X, seiner persönlichen Reichweite und seines Reichtums einsetzt.**

beziehungen, von Marken und auch von der Zurverfügungstellung von Produkten, Rohstoffen und Services. Zudem wird oft verkannt, dass dieser Typus des Polit-Oligarchen finanzielle und unternehmerische Absichten mit politischem Interesse verknüpft. Sowohl bei Elon Musk als auch z.B. bei dem traditionellen Typus, beispielsweise russische Oligarchen, geht es auch um die Gewinnung staatlicher Ausschreibungen und ein „Ausschalten" der Konkurrenz. Gleichzeitig ermöglicht die enorme Marktmacht, gepaart mit politischer Macht und Zugang zu politischen Entscheidungsträgern, den neuen Oligarchen auch, konkurrierende Unternehmen unter vorgeblich politischen Gesichtspunkten von Services, Produkten oder Rohstoffen abzuschneiden und diese stattdessen nur in Einklang mit politischen „Werten" und Beziehungen zur Verfügung zu stellen. Vor allem bei monopolartigen Stellungen auf dem globalen Markt (Raumfahrt, Rüstung, KI, Kommunikation) bedeutet dies weitreichende Risiken und negative Konsequenzen für Unternehmen, die als „politische Gegner" angesehen werden.[18] Da dieser Typus des Polit-Oligarchen sehr oft über enorme Ressourcen im Bereich globaler Kommunikation (eigene Social-Media-Plattformen, traditionelle Medienunternehmen mit Zeitungen und TV und/oder riesige PR-Firmen inklusive eigener Troll-Armeen wie Jewgeni Prigoschin) verfügt, besteht ebenfalls das Risiko, dass Werbeanzeigen oder Inhalte von konkurrierenden oder politisch missliebigen Unternehmen dort demobilisiert, zurückgestuft oder abgeschaltet werden. Schließlich besteht ein weiteres Risiko darin, dass dieses – in Deutschland und Europa bislang weniger verbreitete – Phänomen schnell Nachahmer (wenn auch in kleinerem Maßstab) finden wird.

4. Cyberangriffe und Datenabfluss

Cyberangriffe sind ein weit verbreitetes Mittel zur Wahlbeeinflussung vor allem von staatlichen ausländischen Akteuren. Sie haben mehrere Ziele, z.B. **Wahlinfrastruktur** während der heißen Wahlphase mittels DDoS-Angriffen **lahmzulegen und zu blockieren** (z.B. Websites von Parteien, Wahlbüros, Kandidaten, Behörden etc.), **Wahlservices unbrauchbar zu machen oder zu manipulieren** (z.B. elektronische Wahlmaschinen, Verbindungen und Kommunikation von Wahlbüros, Umfragen und Medien) oder mittels sogenannter **„Hacking & Leaking"-Cyberangriffe** sensible Informationen aus politischen oder anderen Organisationen zu erbeuten und zu veröffentlichen, um das **Wahlergebnis zu beeinflussen**.[19] In Rumänien zum Beispiel erklärte das Verfassungsgericht die erste Runde der Präsidentschaftswahlen 2024 für ungültig, nicht nur wegen massiver Online-Desinformation, sondern auch wegen über 10.000 detektierter gezielter Cyberangriffe gegen

17 Siehe z.B.: https://www.independent.co.uk/tech/elon-musk-trump-x-algorithm-bias-b2640976.html.

18 Siehe z.B.: https://www.spiegel.de/wirtschaft/tesla-starlink-spacex-wie-elon-musk-geschaeftliche-und-politische-interessen-verquickt-a-45c862fb-50ab-4194-8316-0ff6682ff581.

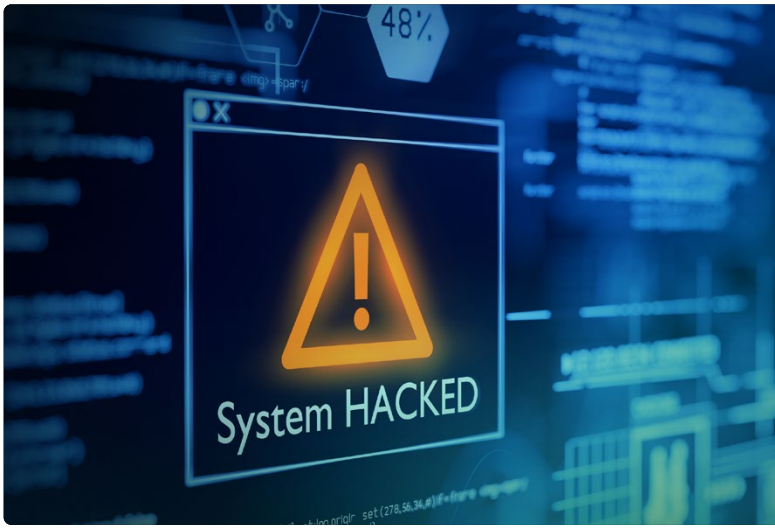
19 Siehe z.B.: https://www.resecurity.com/blog/article/global-malicious-activity-targeting-elections-is-skyrocketing.

Wahlinfrastruktur, politische Organisationen, Behörden und verbundene Organisationen und Unternehmen.[20]

Für Unternehmen bedeuten solche Angriffe sowohl mittelbare als auch unmittelbare Gefahren: Unternehmen, die entweder direkt oder über eine Lieferkette (z.B. Papier für Stimmzettel, technische oder physische Ausstattung von Wahlbüros und anderen Institutionen) mit kritischer Wahlinfrastruktur verbunden sind, können ein direktes Ziel solcher Angriffe werden.[21] Ebenso können Unternehmen der allgemeinen kritischen Infrastruktur KRITIS (z.B. Verkehr, Energie- und Wasserversorgung oder Gesundheitswesen) zum Ziel werden, um durch Ausfälle Angst und Panik zu erzeugen und so das Wahlergebnis zu beeinflussen. Sind Unternehmen – über Spenden, persönliche Verbindungen, politisches Engagement und offene Unterstützung – mit Parteien und Kandidaten direkt verbunden, können auch sie zum Ziel von Hacking-Angriffen werden, um Daten zu erbeuten oder Services abzuschalten. Während der Wahl in Südafrika 2024 kam es etwa zu gezielten DDoS-Attacken gegen Medien- und Kommunikationsunternehmen, um ihre Dienste (und vermeintliche Unterstützung für eine der Parteien) vorübergehend unerreichbar zu machen.[22] Ebenfalls können gezielte (vor allem Spear-)Phishing-Angriffe, die eigentlich politischen Organisationen oder der Wahlinfrastruktur gelten, Unternehmen angreifen, wenn diese mit den Angriffszielen direkte und hochrangige Verbindungen unterhalten. Das Problem bei solchen wahlbezogenen Cyberangriffen gegen Unternehmen ist, dass der politische Kontext des Angriffs (und damit verbundene Schäden) überhaupt nicht erkannt wird.[23]

> **In Rumänien zum Beispiel erklärte das Verfassungsgericht die erste Runde der Präsidentschaftswahlen 2024 für ungültig, nicht nur wegen massiver Online-Desinformation, sondern auch wegen über 10.000 detektierter gezielter Cyberangriffe gegen Wahlinfrastruktur, politische Organisationen, Behörden und verbundene Organisationen und Unternehmen.**

Der **Abfluss von Daten aus Unternehmen** durch solche wahlbezogenen Cyberangriffe stellt schließlich einen weiteren Angriffsvektor dar. Angreifer versuchen z.B., Wählerdaten, Informationen zu Partei- und Kandidatenspenden oder andere sensible Daten zu erbeuten und zu veröffentlichen.[24] Auch hier gilt: Sind Unternehmen auch nur potenziell in der „Lieferkette" solcher Daten, können sie zum Ziel werden. Und: Neben Image- und Vertrauensverlust zieht Datenabfluss generell immer eine lange Kette an Folgeschäden (Untersuchungen, verpflichtende Informierung der Betroffenen, mögliche Audits oder Strafen nach DSGVO) nach sich.



5. Ausfall von Services und Infrastruktur

Gezielte Cyberangriffe, Desinformationsoperationen und physische Angriffe, wie Sabotage gegen Services und Infrastruktur, während einer Wahl betreffen Unternehmen, auch wenn sie kein direktes Ziel sind. Fallen zum Beispiel staatliche Services und Dienstleistungen aus, hat das direkte Auswirkungen auf Unternehmen. Einmal können Services nicht in Anspruch genommen werden, Gesprächspartner fallen aus, Kommunikation steht still; kommt es zu einem Angriff und dem Ausfall von KRITIS, sind Unternehmen ebenfalls massiv

20 Siehe z.B.: https://www.kas.de/de/laenderberichte/detail/-/content/praesidentenwahlen-annulliert-nach-hybriden-angriffen.
21 Interview mit einem Mitarbeiter einer deutschen Sicherheitsbehörde.
22 Siehe: https://radar.cloudflare.com/reports/elections-2024#id-88-attacks-news-under-attack.
23 Interview mit einem Mitarbeiter einer deutschen Sicherheitsbehörde.
24 Siehe z.B.: https://www.resecurity.com/blog/article/global-malicious-activity-targeting-elections-is-skyrocketing.

direkt betroffen. Gleichzeitig können solche Angriffe direkte Auswirkungen auf Unternehmen haben, die über Aufträge oder Zulieferung mit betroffenen staatlichen Einrichtungen (z.B. Ministerien und Behörden) oder KRITIS-Unternehmen verbunden sind.[25] Lieferketten müssen hier in ihrer gesamten Breite berücksichtigt und mitbedacht werden.

Beispiel: Paketbomben-Angriffe auf DHL

Ein anschauliches Beispiel gibt es aus der Reihe der Vorfälle vermeintlicher russischer Sabotage im Zuge des Ukraine-Krieges (da hier nicht nur militärische Ziele verfolgt werden, sondern vor allem die Stimmung gegen weitere Unterstützung der Ukraine gekippt werden soll, kann dies auch in den breiteren Kontext der Wahlbeeinflussung eingeordnet werden): Hier wurden Pakete, die Sprengladungen enthielten, als DHL-Pakete zwischen dem Baltikum und Deutschland versendet, mutmaßlich von einem russischen Agentenring. Diese Pakete explodierten zum Teil, zum Teil konnten sie abgefangen und untersucht werden. Ungeachtet ihrer politischen Wirkungen, bedeuteten diese Angriffe natürlich auch eine massive Disruption der Geschäftsprozesse eines der größten Logistik-Dienstleister der Welt. Davon war

nicht nur das Unternehmen selbst betroffen, sondern natürlich Kunden und Lieferketten des Unternehmens. Lieferungen kamen zu spät, Aufträge konnten nicht oder nur verzögert bearbeitet und durchgeführt werden, Kunden mussten kurzfristig Alternativen finden oder Einbußen in Kauf nehmen. Die Gesamtschäden entlang aller Lieferketten sind hier realiter kaum zu ermessen.

6. Planungsunsicherheit

Wahlbeeinflussung, Desinformations- und Cyberangriffe bringen für Unternehmen das grundlegende Risiko von Planungsunsicherheit. Das meint nicht so sehr Unsicherheit bezüglich des Wahlausgangs, sondern Unsicherheit über Arten, Dauer und Intensität von Angriffen und Störungs- und Beeinflussungsversuchen, Unsicherheit über die Möglichkeit zur ordnungsgemäßen Durchführung von Wahlen und schließlich auch die Unsicherheit darüber, ob Wahlergebnisse von Parteien und Bewerbern überhaupt anerkannt werden oder auch, ob

> **Wahlbeeinflussung, Desinformations- und Cyberangriffe bringen für Unternehmen das grundlegende Risiko von Planungsunsicherheit.**

Wahlen von Gerichten wegen Beeinflussungsversuchen für ungültig erklärt werden. Dies war bei der Präsidentschaftswahl 2024 in Rumänien (also innerhalb der EU!) der Fall, bei der die erste Wahlrunde wegen massiver Einflussoperationen für ungültig erklärt wurde.[26]

Mögliche Folgen dieser Unsicherheit sind:

- Instabilität,
- wirtschaftliche Unsicherheit,
- kürzere Planungszyklen bzw. Notwendigkeit von Anpassungen,
- kurzfristige Disruptionen,
- Ausfall von Aufträgen,
- spontane, aber anhaltende gravierende Veränderung von Marktbedingungen und Standortattraktivität.

7. Lieferketten

Lieferketten sind ein sog. „Querschnittsthema“ bei den Folgen und Gefahren von Wahlbeeinflussung für Unternehmen. Lieferketten können direkt und kurzfristig von solchen Angriffen betroffen sein (z.B. wenn das eigene oder ein zulieferndes Unternehmen Opfer eines direkten Angriffs inkl. Service- oder Produktausfall wird); andererseits können die Folgen von Wahlbeeinflussung aber auch mittel- und langfristig entlang der „langen Lieferketten“ spürbar werden (z.B. wenn ein zuliefern-

25 Interview mit einem Mitarbeiter einer deutschen Sicherheitsbehörde.

26 Siehe z.B.: https://www.kas.de/de/laenderberichte/detail/-/content/praesidentenwahlen-annulliert-nach-hybriden-angriffen.

des Unternehmen im Ausland aufgrund von Wahlbeeinflussung Aufträge, Lieferungen oder Produktionsweisen ändern muss).[27] Viele der oben ausgeführten Bedrohungen (wie z.B. Reputationsangriffe, Cyberattacken oder Serviceausfälle) müssen deshalb unbedingt entlang der gesamten globalen Lieferketten gedacht werden.

B) Indirekte Gefahren

1. Langzeitauswirkungen auf Marken und Märkte

Wahlbeeinflussung – egal ob durch Desinformation oder Cyberattacken – hat viele Langzeitfolgen für Unternehmen, die unabhängig vom Wahlausgang sind. Störungen, Ausfälle, Proteste, Gewalt, gesellschaftliche Polarisierung, Hass und Angst haben langfristig einen Einfluss auf Standortattraktivität, Konsumklima, Mitarbeitergewinnung und das generelle Marktumfeld.

> **Störungen, Ausfälle, Proteste, Gewalt, gesellschaftliche Polarisierung, Hass und Angst haben langfristig einen Einfluss auf Standortattraktivität, Konsumklima, Mitarbeitergewinnung und das generelle Marktumfeld.**

Dasselbe gilt auch für die Faktoren Vertrauen und Reputation (von Marken, Firmen, aber auch Personen wie Führungskräften), denen ein schleichender Ansehens- und Vertrauensverlust droht. Ebenso gibt es negative Auswirkungen von Wahlbeeinflussung auf die generelle Planungssicherheit von Unternehmen (siehe oben) und ihr Marktumfeld entlang globaler Lieferketten.

Beispiel A: Russische „Angst"-Kampagne zur Wahlbeeinflussung in Deutschland 2024/25

Die russische Präsidialverwaltung im Kreml erteilte spätestens ab 2024 verschiedene Aufträge zur Wahlbeeinflussung durch Online-Desinformationskampagnen in den USA und Deutschland. Datenleaks aus einer der beauftragten PR-Firmen („SDA") geben tiefe Einblicke in die Details dieser Operationen. Für die Bundestagswahl 2025 in Deutschland will die Firma mittels Maßnahmen zur Online-Desinformation (Fake-News-Seiten, Trolle und Bots, die Artikel und Botschaften teilen und kommentieren) die Wahl beeinflussen. Oberstes Ziel ist es, russlandfreundliche Parteien zu stärken (als solche wurde die AfD ausdrücklich genannt). Ein Hauptmittel dabei ist, Angst in der deutschen Gesellschaft zu verbreiten, zu schüren und zu befeuern.[28] Ängste vor wirtschaftlichem Abstieg, Engpässen bei Konsumgütern und Ausfällen der Energieversorgung wurden dabei konkret als Beispiele genannt (neben Krieg, Migration und organisierter Kriminalität). Das Schüren und Anheizen von Angst hat dabei nicht nur Auswirkungen auf Konsumenten- und Kundenentscheidungen, sondern natürlich auch auf Standort- und Marktstimmung sowie Vertrauen.

Beispiel B: Russische Kampagne über Energiekrise und Werksschließungen von Siemens und BASF 2022

Bereits aus dem Jahr 2022, im unmittelbaren Kontext der russischen Invasion in der Ukraine, stammen mehrere konkrete Beispiele dafür, wie solche Desinformations-Operationen deutsche Unternehmen direkt angreifen.[29] In einer gezielten Aktion verbreiteten gefälschte Facebook-Seiten (die auch als gekaufte Werbung angezeigt wurden) Falschmeldungen über angebliche Werksschließungen und drohenden Konkurs namhafter deutscher Großkonzerne. Betroffen waren u.a. BASF, Siemens, VW und die Salzgitter AG. Angeblich, so die Fake-Kampagne, müssten Werke und Einrichtungen in Deutschland wegen Energieknappheit schließen. Hintergrund der höchstwahrscheinlich aus Russland gesteuerten Kampagne war, Ängste und Debatten im Zuge der ausfallenden Energielieferungen aus Russland anzuheizen. Hierbei ging es jedoch keineswegs nur darum, politische Stimmung gegen die Unterstützung der Ukraine zu machen, sondern auch, Unternehmen, die den EU-Sanktionen folgend ihr Russland-Geschäft eingestellt hatten, zu diskreditieren und zu schwächen. Diese Aktion war ein Paradebeispiel dafür, wie politische Desinformation und Angriffe gegen Unternehmen Hand in Hand gehen.

27 Interview mit einem leitenden Mitarbeiter einer deutschen Sicherheitsbehörde.

28 Siehe den Bericht des US-Justizministeriums inkl. der detaillierten Angaben des FBI: https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence; und: https://www.tagesschau.de/investigativ/ndr-wdr/russland-propaganda-fakenews-sda-deutschland-100.html.

29 Siehe: https://correctiv.org/faktencheck/2022/12/08/fake-kampagne-werke-von-basf-siemens-oder-vw-werden-nicht-wegen-energiekrise-geschlossen/?utm_source=substack&utm_medium=email.

2. Haftungsrisiken, Compliance und neue Vorschriften

Für Unternehmen bestehen im Themenumfeld der Wahlbeeinflussung breit gestreute Haftungsrisiken, die direkte (finanzielle oder Image-)Schäden, zumindest jedoch erheblichen Mehraufwand bedeuten können. Verbreiten oder beteiligen sich Mitarbeiter (und auch Führungskräfte) zum Beispiel an Online-Desinformation und Wahlbeeinflussung (ggf. auch während der Arbeitszeit unter Einsatz von Diensthandy oder PC), kann das nicht nur Imageschäden, sondern ggf. auch rechtliche Folgen haben. Wird Technologie des Unternehmens (auch IT-Infrastruktur) entweder entfremdet (z.B. für Bot-Netzwerke) oder direkt oder indirekt zur Verfügung gestellt (z.B. als Teil eines DDoS-Netzwerks), kann dies ebenfalls Konsequenzen und Haftungsrisiken bergen.

Gleichzeitig können steigende Polarisierung und Wahlbeeinflussung auch dazu führen, dass Unternehmen intern neue Compliance-Richtlinien für die Nutzung von Social Media oder für politisches Engagement erlassen, die umgesetzt und überwacht werden müssen. Dies verursacht Mehraufwand und Kosten.

3. Radikalisierung und Polarisierung von Mitarbeitern und Störung des Betriebsfriedens

Desinformation, politische Grabenkämpfe, Verschwörungstheorien und politischer Extremismus finden nicht nur im privaten Umfeld, sondern auch am Arbeitsplatz statt. Dies kann für Unternehmen vielfältige Auswirkungen haben:

- Konflikte, die den Betriebsfrieden stören und auch zu Betriebsausfällen führen können,
- politisch beeinflusstes Verhalten von Mitarbeitern zum Schaden des Unternehmens (z.B. bei Einstellung oder Kündigung von Mitarbeitern oder bei Auftragsvergaben),
- Sabotage- oder Blockadeaktionen von Mitarbeitern aus politischen Gründen,
- steigende Abwesenheits- und Krankheitszeiten,
- Imageverlust nach außen inkl. Auswirkungen auf Aufträge oder auch auf Anwerbung neuer Fachkräfte.

Beispiel: Impfgegner und Verschwörungstheoretiker

Besonders die Corona-Pandemie hat die Folgen von Verschwörungsglauben und gezielten Falschmeldungen zu Gesundheitsthemen für Großorganisationen und Unternehmen aufgezeigt: Einerseits waren dies z.B. direkte Gesundheitsrisiken nicht nur für den Einzelnen, sondern vor allem die Gefahr der Massenverbreitung am Arbeitsplatz. Dies hatte direkte Auswirkungen auf den Krankenstand und damit auf Arbeitsleistung und Produktivität. Andererseits führten Falschmeldungen und Verschwörungsglauben zu politischer Polarisierung und den damit verbundenen Konflikten am Arbeitsplatz. Dies wiederum hatte Auswirkungen auf Betriebsklima, Betriebsfrieden sowie Produktivität.

4. Negative Auswirkung bei Gewinnung von Mitarbeitern und Fachkräften im In- und Ausland

Wahlbeeinflussung kann sich für Unternehmen negativ auf die Rekrutierung von Mitarbeitern auswirken: Betätigen sich Mitarbeiter oder Führungskräfte zum Beispiel an Wahlbeeinflussung für extremistische Parteien oder ausländische Regierungen, kann dies das Unternehmen unattraktiv für potenzielle Mitarbeiter im In- und Ausland machen. Gleichzeitig können durch Wahlbeeinflussung befeuerte gesellschaftliche Polarisierung, Hass und ein Klima der Angst sowohl das Image des Markt- und Unternehmensstandorts als auch das Unternehmen an sich diskreditieren (gerade für ausländische Fachkräfte).

> **Betätigen sich Mitarbeiter oder Führungskräfte zum Beispiel an Wahlbeeinflussung für extremistische Parteien oder ausländische Regierungen, kann dies das Unternehmen unattraktiv für potenzielle Mitarbeiter im In- und Ausland machen.**

Beispiel: Russische Kampagne gegen deutsche Anwerbung von Fachkräften in Afrika

Das Thema Migration und Einwanderung von Arbeitskräften ist weltweit ein Kampfthema der Neu-Rechten, wird aber auch von Russlands Desinformations-Maschinerie immer wieder instrumentalisiert, um westliche Gesellschaften zu spalten. Ein Beispiel ist das Netzwerk von Desinformations-Websites von John Dougan, einem ehemaligen Sheriff, der vor Strafverfolgung nach Russland flüchtete. Während der US-Wahl 2024 unterhielt er laut Recherchen ein Netzwerk von über 170 solcher Seiten; Ende 2024/Anfang 2025 baute er

ein ähnliches Netzwerk an deutschsprachigen Fake-News-Seiten auf. Diese versuchen z.B., durch Falschnachrichten über von der Regierung Scholz massenhaft angeworbene Arbeitskräfte politische Stimmung zu machen (so z.B. in Fake-Artikeln über die angebliche Anwerbung von 1,8 Millionen kenianischen Arbeitern).[30]

5. Werbung auf Websites, Kanälen und Profilen der Desinformation und Wahlbeeinflussung

Das automatische Schalten von Werbung im Online-Raum birgt für Unternehmen u.a. die Gefahr, auf Online-Portalen, -Seiten oder Social-Media-Kanälen und -Profilen von in- und ausländischen Akteuren der Desinformation und Wahlbeeinflussung Werbung zu positionieren. Dies muss keine absichtliche Platzierung sein, sondern kann durch die Automatisierung von Werbeanzeigen zustande kommen. Für Unternehmen bedeutet das nicht nur ein Reputationsrisiko und einen Imageverlust, sondern auch Verstöße gegen Compliance-Richtlinien sowie internationale Sanktionen.

> **Für Unternehmen bedeutet das nicht nur ein Reputationsrisiko und einen Imageverlust, sondern auch Verstöße gegen Compliance-Richtlinien sowie internationale Sanktionen.**

Beispiel: Werbung deutscher Großkonzerne auf pro-russischen Desinformationsseiten

Mehrere deutsche Großkonzerne schalteten in den vergangenen Jahren immer wieder automatische Werbung im europäischen Online-Raum. In Bulgarien zum Beispiel fanden Forscher automatische Werbeanzeigen deutscher Großunternehmen auf Websites eines riesigen pro-russischen Netzwerks von über 500 Fake-News-Seiten, die Falschnachrichten über den russischen Krieg gegen die Ukraine verbreiten.[31] *In Serbien wiederum wurden deutsche Großunternehmen dabei beobachtet, wie Werbeanzeigen automatisiert in notorischen Desinformations-Medien geschaltet wurden.*[32] *Diese Aktivitäten wurden nicht nur in der deutschen Presse bekannt, sondern werden mittlerweile auch von Organisationen wie dem „Global Disinformation Index" gezielt überwacht, was das Risiko eines Imageschadens erhöht.*[33]

C) Warum werden Unternehmen bei Wahlbeeinflussung zur Zielscheibe?

Für Unternehmen erscheint Wahlbeeinflussung oft als ein rein politisches (und damit nicht als wirtschaftliches oder unternehmerisches) Problem. Für Angreifer jedoch, die Wahlen beeinflussen wollen, sind Unternehmen – wie ausführlich gezeigt – ein wichtiges Ziel. Das gilt umso mehr in Ländern, die vor allem wegen ihrer wirtschaftlichen Bedeutung und nicht z.B. aufgrund ihrer sicherheitspolitischen oder strategischen Bedeutung eine globale oder regionale Vormachtstellung haben. Deutschland („Wirtschaftsmacht Deutschland") ist dafür ein Paradebeispiel. Mit Angriffen gegen Unternehmen solcher Länder können Angreifer daher sowohl direkt als auch indirekt politisch agieren und Wahlen und politische Prozesse beeinflussen.

Im engeren Fokus haben **direkte Angriffe** auf Unternehmen oft folgende **Gründe**:

- Unternehmen haben sich in einem Wahlkampf **klar politisch positioniert** (z.B. gegen rechtsextreme Parteien und Gruppen) und politisch engagiert (z.B. für Minderheitenrechte).
- Unternehmen gehören zu einem **Teil der technischen Lieferkette für kritische Wahlinfrastruktur** (z.B. Software, Papier, Services etc.).
- Unternehmen haben aufgrund von Größe, Umsatz oder Produkten und Leistungen **eine systemrelevante Funktion** und **Stellung**.
- Unternehmen sind **Teil der Lieferkette von Produkten** (z.B. Rüstung, Logistik, Software, Automobilbranche), die von **Sanktionen** betroffen sind bzw. in **globalen militärischen Konflikten** eine Bedeutung haben.

30 Siehe: https://correctiv.org/faktencheck/2025/01/23/russische-einflussoperation-verbreitet-fake-artikel-zu-migrationsabkommen-mit-kenia/.

31 Siehe: https://hssfoundation.org/wp-content/uploads/2024/03/%D0%B1%D0%B3-%D0%B1%D1%8E%D0%BB%D0%B5%D1%82%D0%B8%D0%BD-%D0%B1%D1%804.pdf; und: https://csd.eu/fileadmin/user_upload/events_library/files/2023_12/Prezentacija_Todor_Galev.pdf.

32 Siehe: https://www.tagesschau.de/faktenfinder/serbien-medien-finanzierung-101.html.

33 Siehe: https://www.disinformationindex.org/.

- Unternehmen befinden sich in **Konkurrenz zu staatsnahen oder systemrelevanten Unternehmen** in einem anderen Land.
- Unternehmen befinden sich oder geraten in **Konkurrenz zu Unternehmen von Oligarchen oder dem neuen Typus der „Polit-Oligarchen“**.

Indirekte Gefahren der Wahlbeeinflussung für Unternehmen sind deutlich komplexer und schwieriger vorherzusehen. Die **Gründe** dafür, dass Unternehmen davon betroffen sind, erweisen sich als äußerst vielfältig; einige davon sind:

- Unternehmen sind **von staatlichen oder privaten Services und Produkten abhängig**, die zur Zielscheibe von Angriffen wurden und ausfallen.
- Unternehmen **kooperieren** mit, engagieren sich für oder erhalten Aufträge bzw. leisten Services **für politische Organisationen, Gruppen, Personen oder Teile der kritischen Wahlinfrastruktur**.
- Unternehmen leiden indirekt durch **Angriffe auf den Marktstandort** (z.B. durch ein Klima der Angst und Verunsicherung, das sich auf die Nachfrage auswirkt).
- Durch Desinformation befeuerte gesellschaftliche **Polarisierung** wirkt sich negativ auf **Betriebsklima, Betriebsfrieden** und die Gewinnung von Mitarbeitern aus.
- Unternehmen **werben** (unabsichtlich) in **Medien** (z.B. Websites, Channels, Profilen, Gruppen, TV oder Radio-Stationen), die **Wahl-Desinformation verbreiten**.
- **Gesetze und Compliance-Regeln**, die als Reaktion auf oder zum Schutz vor Wahlbeeinflussung erlassen wurden, bringen **neue Belastungen** für Unternehmen.

Teil 3:

Die Gesetzeslage: Helfen Recht und Gesetz den Unternehmen?

Die Gesetzeslage hinsichtlich Wahlbeeinflussung ist unübersichtlich und kompliziert. Zum einen kommt es auf die Form der Angriffe an: Direkte Cyberangriffe sind zum Beispiel strafbar, die Umsetzung bzw. Verfolgung jedoch oftmals unmöglich, da kein Täter ermittelt werden kann oder der Täter im Ausland sitzt. Bei Desinformation und Informationsangriffen ist die Lage noch deutlich komplizierter: Desinformation als solche ist kein Straftatbestand, hier kommt es sehr genau auf den Einzelfall (z.B. Art von Manipulationen, Beleidigungen oder Verletzung von Persönlichkeitsrechten durch einzelne Falschmeldungen) an. Grundsätzlich haben im Bereich von Falschinformationen das Netzwerkdurchsetzungsgesetz (NetzDG) sowie vor allem der EU Digital Services Act (DSA) eine Bedeutung. Diese machen es jedoch zur Pflicht von Social-Media-Plattformen, Maßnahmen gegen bösartige und schädliche Inhalte zu ergreifen, jene Inhalte zu überprüfen und ggf. auch zu löschen.[34] Die großen – und für Unternehmen im Notfall mitunter entscheidenden – Hindernisse sind jedoch die Um- und die Durchsetzung dieser Regeln. Zum einen laufen bei der EU-Kommission derzeit gegen

> **Dementsprechend lange kann es dauern, bis – wenn überhaupt – einzelne Beiträge, Posts, Seiten und Bilder gelöscht werden.**

verschiedene Social-Media-Plattform Verfahren wegen der Nicht-Einhaltung dieser Regelungen; zum anderen ist die Umsetzung der Bekämpfung von z.B. wahlbezogener, schädlicher Falschinformation immer an einen zeitintensiven Kreislauf von Meldungen, Überprüfungen und Aktionen geknüpft. Dementsprechend lange kann es dauern, bis – wenn überhaupt – einzelne Beiträge, Posts, Seiten und Bilder gelöscht werden. Im Falle eines Reputationsangriffes zum Beispiel zählt jedoch jede Minute. Die Durch- und Umsetzung der hier bestehenden Rechtslage ist also für betroffene Unternehmen in der Regel eher schwierig.

Gleichzeitig gilt für rechtliche Maßnahmen, dass regelmäßig ein Verstoß vorliegen muss, bevor gehandelt werden kann. Dies bedeutet im Falle eines Angriffs, dass mit zeitaufwendigen Prozeduren (deren Umsetzung derzeit bestenfalls holprig ist) zu rechnen ist. In der Zwischenzeit bestehen die Risiken, Gefahren und negativen Wirkungen des Angriffs jedoch weiter. Ebenso gibt es bei Informationsangriffen im Online-Raum die Herausforderung, dass Recht und Gesetz in der Regel national bzw. in der EU Geltung besitzen, Angriffe jedoch oftmals aus dem Nicht-EU-Ausland kommen oder Infrastruktur nutzen, die nicht in der EU sitzt. Die strafrechtliche Verfolgung ist in diesem Fall schwierig.

Diesem eher trägen und lückenhaften Schutz, den Recht und Gesetz deutschen Unternehmen hier bieten, stehen gleichzeitig aber entschlossene, tatkräftige Täter mit großen Ressourcen und entsprechender Expertise, oftmals staatlicher und politischer Unterstützung sowie ausgeprägten Verschleierungstaktiken gegenüber.

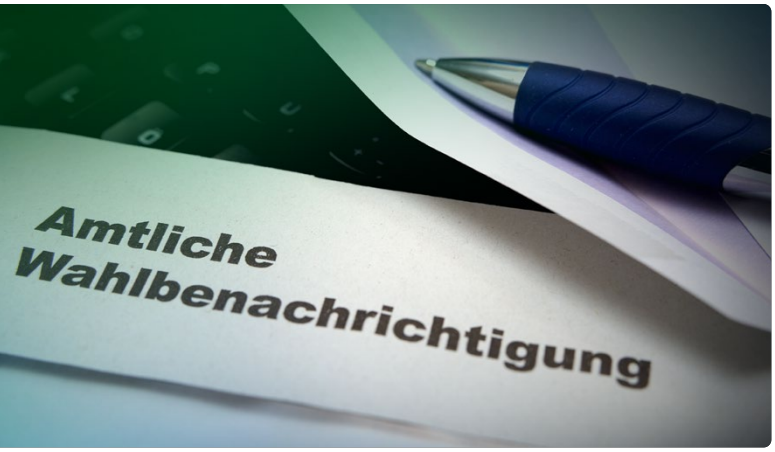
In Kürze: *Recht und Gesetz bieten Unternehmen nur wenig unmittelbaren Schutz und Hilfe vor den Risiken durch Wahlbeeinflussung!*

34 Bitkom (Hg.): Policy Brief: Maßnahmen gegen Desinformation und Deepfakes im Superwahljahr 2024: https://www.bitkom.org/Bitkom/Publikationen/Massnahmen-gegen-Desinformation-und-Deepfakes.

Teil 4:

Lessons Learned aus dem globalen Superwahljahr 2024

2024 fanden weltweit 76 Wahlen statt, an denen rund 3,6 Milliarden Menschen teilnahmen (u.a. in den USA, der EU, Indien, Südafrika oder Indonesien). Aus den vorliegenden Erkenntnissen zum Thema Wahlbeeinflussung 2024[35] können deshalb wertvolle „Lessons Learned“ gewonnen werden:



- Laut der Bertelsmann Stiftung kam es 2024 bei über 90 Prozent der Wahlen zur Beeinflussung durch Desinformation;[36] dies unterstreicht sowohl die globale Relevanz als auch das disruptive Potenzial des Themas für eine globale Wirtschaft, die auf Informationen beruht.
- Angriffe sind zunehmend hochgradig technisiert; neben Desinformation sind Cyber-Influence-Operationen und Cyberangriffe (auf Wahlinfrastruktur, auf politische Organisationen und auf Unternehmen) die häufigsten Formen der Wahlbeeinflussung.
- Polit-Influencer und Polit-Oligrachen, die große mediale Macht haben und oftmals politische mit wirtschaftlichen Eigeninteressen verbinden, sind weltweit auf dem Vormarsch.
- Die Nutzung von KI für Angriffe und Wahlbeeinflussung (z.B. Deepfakes) nimmt rapide zu, hat aber bisher nur in Ausnahmefällen einen bedeutenden Unterschied gemacht.
- Desinformation, KI und Wahlbeeinflussung haben kurzfristige und langfristige Folgen, die Unternehmen direkt betreffen.
- Gesetze, Normen, und Social-Media-Standards haben – auch innerhalb der EU – bislang nur begrenzte Wirkung (bzw. Umsetzung) und bieten Unternehmen und Organisationen nur begrenzten Schutz.
- Wahlbeeinflussung trifft Unternehmen entlang globaler Lieferketten und muss entsprechend gedacht werden.
- Unternehmen und private Organisationen brauchen ganzheitliche Sicherheits- und Risikominimierungsstrategien für Probleme wie Desinformation und Wahlbeeinflussung.

> **Unternehmen und private Organisationen brauchen ganzheitliche Sicherheits- und Risikominimierungsstrategien für Probleme wie Desinformation und Wahlbeeinflussung.**

35 Siehe: Karen Allen, Christopher Nehring: AI Disinformation in Europe and Africa. Use Cases, solutions and transnational learning, hg. Medienprogramm Subsahara Africa Konrad-Adenauer-Stiftung, Johannesburg, 2025; siehe die Ergebnisse des „Upgrade Democracy“-Programms der Bertelsmann Stiftung zur Desinformation weltweit: https://upgradedemocracy.de/en/superwahljahr-2024-superjahr-desinformation/.

36 Siehe: https://upgradedemocracy.de/en/superwahljahr-2024-superjahr-desinformation/.

Teil 5:

Was tun? Gegenmaßnahmen, Sicherheitsstrategien und Handlungsempfehlungen

Wahlbeeinflussung ist in ihrer Brandbreite ein hochgradig komplexes Thema mit zahlreichen Angriffsvektoren. Aufgrund der politischen Bedeutung des Themas besteht bei vielen Akteuren und Betroffenen die Erwartungshaltung, Staat und Regierung seien für die Lösung des Problems und für die Gefahrenabwehr zuständig. Gerade in Deutschland jedoch entwickelt sich die strategische Ab- und Gegenwehr von Wahlbeeinflussung, Desinformation und Cyberattacken nur sehr holprig. Wie zudem in Teil 3 ausgeführt wurde, dürfen staatliche Sicherheitsbehörden oft nur reaktiv und nicht bzw. nur sehr eingeschränkt vorbeugend aktiv werden. Unternehmen und Organisationen tun deshalb gut daran, eigene Sicherheitskonzepte zu entwickeln und umzusetzen.

Grundsätzliche Empfehlungen

- **Awareness:** Unternehmen müssen sich auf allen Ebenen der Bedeutung des Themas bewusst werden und dieses Bewusstsein nach innen und außen kommunizieren.
- **Mindset:** Sicherheit gelingt, wenn sie von Anfang an mitgedacht wird, selbstverständlich ist (security by default) und entsprechende Kosten in Kauf genommen werden.
- **Risikoanalysen:** Wahlen und langfristige Wahlbeeinflussungsversuche müssen als Risikosituation eingeplant und in entsprechenden Strategien berücksichtigt werden.
- **Proaktives Handeln:** Unternehmen sollten nicht warten, bis sie angegriffen werden, sondern vorab Sicherheitsstrategien und konkrete Maßnahmen installieren.
- **Ganzheitliche Sicherheitsstrategie:** Sicherheit, auch hinsichtlich der Folgen von Wahlbeeinflussung, darf nicht für einzelne Abteilungen, Standorte oder Angriffsarten gedacht werden, sondern muss auf allen Ebenen ansetzen.
- **Technologie und Mensch:** Cybersicherheit, genau wie die Abwehr von Einflussoperationen, betrifft Menschen und Mitarbeiter genauso wie IT-Infrastruktur und Technologien. Sicherheitskonzepte müssen Stärken und Schwächen von Menschen genauso berücksichtigen wie die von Hard- und Software.
- **Sicherheit beginnt im Inneren (und endet außen):** Mitarbeiter, aber auch die breite Öffentlichkeit müssen mitgedacht und mitgenommen werden, wenn Sicherheitsstrategien aufgehen sollen.

Ganzheitliche Sicherheit

Sicherheitskonzepte, Strategien, Planungen und Maßnahmen müssen individuell auf die Bedürfnisse von Unternehmen zugeschnitten werden. Dabei können Unternehmen von Erfolgen und Schwächen staatlicher, politischer und militärischer Akteure lernen:[37] Der Schlüssel dabei ist die **ganzheitliche Ausrichtung** eines Sicherheits- und Abwehrkonzepts.

37 Siehe u.a.: Christopher Nehring: Countering Disinformation. An Evaluation of the Institutional Approach of Governments, in: Briefing Paper 4, Institute for Global Analytics, Sofia, 2023 (https://globalanalytics-bg.org/2023/12/06/briefing-paper-countering-disinformation-an-evaluation-of-the-institutional-approach-of-governments/); ders.: Not One but Many Silver Bullets. Towards a Classification of Responses to Disinformation, in: Briefing Paper 5, Institute for Global Analytics, Sofia, 2023 (https://globalanalytics-bg.org/2023/12/06/briefing-paper-5-not-one-but-many-silver-bullets-towards-a-classification-of-responses-to-disinformation/); ders.: Effective Strategic Communications for Resilient State and Society, in: Briefing Paper 2, Institute for Global Analytics, Sofia, 2023 (https://globalanalytics-bg.org/2023/10/19/new-briefing-paper-effective-strategic-communications-for-resilient-state-and-society/); James Pamment: A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence, and Foreign Interference. Riga: NATO Strategic Communications Centre of Excellence (https://stratcomcoe.org/publications/a-capability-definition-and-assessment-framework-for-countering-disinformation-information-influence-and-foreign-interference/255); Björn Palmertz u.a.: Building Resilience and Psychological Defence. An analytical framework for countering hybrid threats and foreign influence and interference, hg.: Lund University Psychological Defence Research Institute, 2024 (https://mpf.se/download/18.49d76a6a18e5a91c7581ce99/1712658679908/buidling-resilience-and-psychological-defence.pdf); Jean-Baptiste Jeangène Vilmer: Hybrid CoE Research Report 2: Effective state practices against disinformation: Four country case studies, hg.: Hybrid CoE, 2021 (https://www.hybridcoe.fi/publications/hybrid-coe-research-report-2-effective-state-practices-against-disinformation-four-country-case-studies/).

Ganzheitlich meint:

- → ein Konzept entlang der gesamten Zeitachse (proaktiv – ad hoc/incident management – follow-up und Nachsorge),
- → ein umfassendes Mapping von Gefahren, Risiken, Angriffsvektoren und Angreifern (es gibt kommunikative Angriffe und Gegenmaßnahmen, physische Angriffe und Gegenmaßnahmen, genauso wie Cyberangriffe und Gegenmaßnahmen),
- → ein integratives Konzept: alle internen und externen Stakeholder mitdenken und mitnehmen (kein übertrieben enger Fokus auf Eigeninteressen, sondern Mitarbeiter, Führungskräfte, andere Unternehmen, Gesellschaft, Medien, Politik, Behörden und andere Stakeholder mit ins Boot holen),
- → ein strategisches Konzept: vorausschauend und präemptiv, anpassungsfähig, in übergeordneten Zusammenhängen denken, alle Angriffsvektoren und Ebenen in ein gesamtes Konzept eingliedern (z.B. nicht Cyberangriffe, Kommunikation und physische Gefahren voneinander isoliert betrachten),
- → ein Konzept, das auch auf langfristige Resilienz ausgerichtet ist,
- → das Nutzen und Poolen von Ressourcen,
- → einen steten Kreislauf von Tests/Übungen, Feedback, Verbesserungen und Anpassungen,
- → den Aufbau und die Nutzung (internationaler) Kooperationen.

Ein ganzheitliches Sicherheitskonzept zur Abwehr der Gefahren von Wahlbeeinflussung denkt also alle beschriebenen Angriffsvektoren und Ebenen von Anfang mit. Es nimmt in den Blick, dass:

- ✓ **Online- und Offline-Angriffe** als zusammenhängendes Ökosystem gedacht und behandelt werden müssen, die Cyber- und die physische Welt zwar von unterschiedlichen Angriffsarten betroffen sind, die Absichten, Ziele und Strategien der Angreifer jedoch dieselben sind.
- ✓ **Mensch und Technologie** unbedingt in Einklang miteinander gebracht werden müssen. Dies gilt sowohl bei Angriffsvektoren (z.B. Mensch als Innentäter oder Opfer von Phishing-Angriffen) als auch bei Abwehrstrategien (z.B. Zusammenspiel von Software und Mitarbeitern bei der Erkennung und Abwehr von Angriffen oder bei der Mitarbeiterschulung).
- ✓ Wahlbeeinflussung global **entlang von Lieferketten, Kreisläufen und Märkten** wirkt und abgewehrt werden muss.
- ✓ **interne und externe Kommunikation** mit allen Stakeholdern essentiell ist.

Ein integratives, ganzheitliches Sicherheitskonzept verbindet alle diese Ebenen und sorgt für kohärente Maßnahmen, die Angriffe auf jeder Ebene abwehren können. Dies erfordert die enge Verzahnung von verschiedenen Abteilungen (z.B. Security, IT, PR, Compliance, Risikomanagement und strategische Planung) und deren strategisches Zusammenspiel. Wichtige Elemente und Maßnahmen sind dabei:

- **Technologische Sicherheit:** Schutz von IT-Infrastruktur und Daten vor Cyberangriffen (z.B. DDoS, Phishing, Hacking & Leaking) ebenso wie Schwachstellentests, Monitoring und Incident Response.
- **Strategische Vorausschau und Risikoanalyse:** Implementierung von Monitoring- und Frühwarnsystemen, die potenzielle Bedrohungen rechtzeitig erkennen.
- **Lieferkettensicherheit:** Analyse und Absicherung globaler Wertschöpfungs- und Lieferketten.
- **Strategische Kommunikation:** proaktive Multi-Channel-Kommunikation von entwaffnenden Narrativen und Botschaften.
- **Krisenkommunikation:** Aufbau und Schulung von Expertise und Kapazitäten zur schnellen und effektiven Abwehr von Informationsangriffen.
- **Mitarbeiter-Resilienz:** Schulung von Mitarbeitern, um sie vor gezielten Manipulationsversuchen oder unbewusster Verbreitung von Falschinformationen zu schützen.

Zur erfolgreichen Umsetzung gehört dabei auch ein breiter Stack an Tools, Software und Instrumenten, regelmäßige Schulungen, Übungen und Tests, Feedbackschleifen sowie konstante Verbesserung und Anpassung.

Konkrete Maßnahmen: Eine Check-Liste

- ✓ Sind ein **360°-Monitoring, Beobachtungsmechanismen** sowie **Vorhersagen (Forecasting)** implementiert, um Gefahren zu erkennen?
- ✓ Sind **Blaupausen und Ablaufpläne für Incident-Response-Mechanismen** für die verschiedenen Angriffen und Gefahren implementiert?
- ✓ **Gibt es einen Tool-Stack für Technologien und Programme?** (Z.B. OSINT, Monitoring, Analyse, Cybersecurity, KI-basierte Vorhersage-Systeme und Daten-Analysen.)
- ✓ Gibt es regelmäßig interne und externe **Trainings, Sensibilisierungen und Awareness-Kampagnen?**
- ✓ Ist ein regelmäßiges **Red Teaming** (regelmäßige Angriffssimulationen verschiedener Szenarien) implementiert?
- ✓ Sind Strategien, Tools und Expertisen zum **Takedown von Online-Inhalten** implementiert?
- ✓ Ist eine dauerhafte **strategische Kommunikation** (z.B. nach militärischem Vorbild) implementiert?
- ✓ Kann mein Kommunikationsteam Informationsangriffe **richtig widerlegen?**
- ✓ Gibt es **Kommunikationsstrategien** (für Reputationsangriffe genau wie für Cyberangriffe)?
- ✓ Gibt es regelmäßige **Risikoanalysen**, die diese Angriffe (z.B. bzgl. Russland, Ukraine, China, Nordkorea, Iran, aber auch aus dem extrem rechten Spektrum) in ihrer globalen Bedeutung berücksichtigen?
- ✓ Zielen meine Maßnahmen nicht nur auf die Abwehr von Angriffen, sondern auch auf die **Bildung strategischer Resilienz?**
- ✓ Gibt es **Anleitungen, Beispiele und Aufklärungskampagnen für politische Kommunikation und politisches Engagement** für Mitarbeiter und Führungskräfte?
- ✓ Ist eine regelmäßige **Kooperation mit Behörden, Experten und der Fachwelt** zur Prävention und Gefahrenerkennung implementiert?
- ✓ Ist eine regelmäßige **Feedback- und Lernschleife** eingerichtet?

Anmerkung zur Methodologie

Die Untersuchung zur Wahlbeeinflussung im vorliegenden White Paper basiert auf einer systematischen, mehrdimensionalen Analyse, die qualitative und quantitative Forschungsansätze kombiniert. Primär erfolgt eine explorative Fallstudienanalyse, bei der reale Wahlbeeinflussung und ihre Folgen für Unternehmen anhand dokumentierter Vorfälle und forensischer Cyber-Untersuchungen analysiert werden. Dabei werden sowohl öffentlich zugängliche Datenquellen (z.B. Social-Media-Analysen, OSINT-Methoden) als auch vertrauliche Expertenberichte und sicherheitsrelevante Informationsquellen sowie qualitative Interviews herangezogen.

Zur Identifikation und Kategorisierung der Wahlbeeinflussung wurde ein taxonomischer Ansatz verfolgt, der verschiedene Einflussvektoren – etwa Desinformationskampagnen, Cyberangriffe, wirtschaftliche Druckmechanismen und hybride Bedrohungen – systematisch unterscheidet und klassifiziert. Dabei wird insbesondere der Einfluss externer Akteure auf politische und wirtschaftliche Organisationen durch strategische Narrativsetzung und gezielte Einflussmaßnahmen untersucht.

Aufbauend darauf erfolgte eine Risikoanalyse für Unternehmen, die potenzielle Bedrohungen durch Wahlbeeinflussung in strategische Bedrohungsmodelle überführt. Dies geschieht unter Anwendung von Bedrohungsszenarien, die auf historischen Präzedenzfällen basieren. Schließlich fließen politische, rechtliche und technologische Kontextfaktoren in die Analyse ein, um die regulatorischen Rahmenbedingungen und institutionellen Gegenmaßnahmen zu bewerten. Im Anschluss an diese Risikoanalyse erarbeitet das White Paper die Konturen eines ganzheitlichen Sicherheits- und Schutzkonzepts für Unternehmen, das maßgeblich auf einer flexiblen Adaption von Sicherheitsmaßnahmen aus dem politischen und militärischen Bereich beruht. Hierzu erfolgte eine qualitative Auswertung von Expertenanalysen, Forschungsliteratur sowie Policy- und Strategiepapieren.

Literatur (Auswahl)

- Bitkom (Hg.): Policy Brief: Maßnahmen gegen Desinformation und Deepfakes im Superwahljahr 2024, 2024 (https://www.bitkom.org/Bitkom/Publikationen/Massnahmen-gegen-Desinformation-und-Deepfakes)
- European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE): Countering hybrid threats to elections: From updating legislation to establishing collaboration networks, 2024, (https://www.hybrid-coe.fi/wp-content/uploads/2024/03/20240319-Hybrid-CoE-Research-Report-12-Countering-hybrid-threats-to-elections-WEB.pdf)
- Christopher Nehring: Countering Disinformation. An Evaluation of the Institutional Approach of Governments, in: Briefing Paper 4, Institute for Global Analytics, Sofia, 2023 (https://globalanalytics-bg.org/2023/12/06/briefing-paper-countering-disinformation-an-evaluation-of-the-institutional-approach-of-governments/)
- Ders.: Not One but Many Silver Bullets. Towards a Classification of Responses to Disinformation, in: Briefing Paper 5, Institute for Global Analytics, Sofia, 2023 (https://globalanalytics-bg.org/2023/12/06/briefing-paper-5-not-one-but-many-silver-bullets-towards-a-classification-of-responses-to-disinformation/)
- Ders./Rumena Filipova: Effective Strategic Communications for Resilient State and Society, in: Briefing Paper 2, Institute for Global Analytics, Sofia, 2023 (https://globalanalytics-bg.org/2023/10/19/new-briefing-paper-effective-strategic-communications-for-resilient-state-and-society/)
- James Pamment: A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence, and Foreign Interference. Riga: NATO Strategic Communications Centre of Excellence (https://stratcomcoe.org/publications/a-capability-definition-and-assessment-framework-for-countering-disinformation-information-influence-and-foreign-interference/255)
- Björn Palmertz u.a.: Building Resilience and Psychological Defence. An analytical framework for countering hybrid threats and foreign

influence and interference, hg.: Lund University Psychological Defence Research Institute, 2024 (https://mpf.se/download/18.49d76a6a-18e5a91c7581ce99/1712658679908/buidling-resilience-and-psychological-defence.pdf)

- Jean-Baptiste Jeangène Vilmer: Hybrid CoE Research Report 2: Effective state practices against disinformation: Four country case studies, hg.: Hybrid CoE, 2021 (https://www.hybridcoe.fi/publications/hybrid-coe-research-report-2-effective-state-practices-against-disinformation-four-country-case-studies/)
- Daria Azariev North/David Levine/Krystyna Sikora/Nikoleta Diossy: Building Resilience Against Election Influence Operations: Preparing for the European Elections in 2024 and Beyond, hg.: GMF, 2024 (https://www.gmfus.org/sites/default/files/2024-04/Building-Resilience-Against-Election-Influence-Operations.pdf)
- Miles Kahler: Foreign Influence and Democratic Governance. Defining and Countering Malign Influence, hg.: CFR, 2024 (https://www.cfr.org/report/foreign-influence-and-democratic-governance)
- Center for Monitoring, Analysis and Strategy (CEMAS) (Hg.): Welche Art von falschen und irreführenden Informationen werden rund um Wahlen verbreitet?, 2025 (https://btw2025.cemas.io/artikel/falschinformation-rund-um-wahlen)
- European External Action Service (EEAS): 2nd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats, 2024 (https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf)

Über das CII

Neue Zeiten brauchen eine neue Form der Forschung: das cyberintelligence.institute (CII) – ein Ort, an dem sich Innovation, Technologie, Strategie und Resilienz treffen. An der Schnittstelle von Wirtschaft und Wissenschaft, NGO und Start-up entwickelt das CII in Frankfurt am Main neue Lösungen für eine sichere digitale Zukunft. Kerngedanken sind die Kooperation, der Dialog und der interdisziplinäre und globale Informations- und Wissensaustausch, um Staat, Wirtschaft und Gesellschaft resilienter zu machen. Gefragt sind dabei ganzheitliche Konzepte, die Cybersicherheit nicht nur als abstrakte technisch-organisatorische Gewährleistungsverantwortung, sondern als gesamtgesellschaftliche Aufgabe zum Schutz gemeinsamer europäischer Werte verstehen. Damit tritt das cyberintelligence.institute aktiv für mehr digitale Sicherheit in einem Zeitalter neuer digitaler Herausforderungen ein.

Weitere Informationen gibt es auf der Website des CII unter www.cyberintelligence.institute.

cyberintelligence.institute
MesseTurm
Friedrich-Ebert-Anlage 49
D-60308 Frankfurt am Main

www.cyberintelligence.institute
info@cyberintelligence.institute

+49 69 505034602