Martin-Luther-Universität Halle-Wittenberg
Naturwissenschaftliche Fakultät III
Institut für Informatik

Seminar

Informatik und Gesellschaft

Sommersemester 2023

geleitet durch Prof. Dr. Paul Molitor

Mit Hacks und Desinformation Wahlen beeinflussen

Nicolas Marx & Frederik Rösner

Inhaltsverzeichnis

Gender-Hinweis: Die männliche Form ist der weiblichen Form in dieser Arbeit gleichgestellt; lediglich aus Gründen der Vereinfachung wurde die weiblich Form gewählt.

Überarbeitung durch den Dozenten: Der vorliegende Text entspricht im Wesentlichen dem ursprünglichen durch Herrn Marx und Herrn Rösner erstellten Bericht. Der Dozent hat lediglich kleinere Schreibfehler entfernt und einige wenige Umformulierungen bzw. Umformatierungen durchgeführt.

1 Einleitung

Im Zeitalter der Digitalisierung, bieten sich in vielen Bereichen des Lebens immer mehr Möglichkeiten. Die Integrität und Fairness von Wahlen sind Grundpfeiler demokratischer Gesellschaften. Doch in einer zunehmend digitalisierten Welt, in der Technologie eine immer größere Rolle spielt, eröffnen sich auch neue Möglichkeiten, eine Wahl zu manipulieren. Eine besonders beunruhigende Entwicklung stellt dabei die wachsende Bedrohung durch Hacking und Desinformationen dar. Der Missbrauch von Technologie zur Wahlmanipulation ist heute nicht mehr nur eine theoretische Gefahr. In der vorliegenden Arbeit sollen diese Themen genauer analysiert und mit Beispielen untermauert werden. Unser Ziel ist es, die Folgen der Digitalisierung und Technisierung mit Blick auf den Erhalt der Demokratie aufzuzeigen und so ein Bewusstsein für reale Gefahren für die Gesellschaft zu schaffen. Außerdem soll die Frage beantwortet werden, wie Wahlen durch technologische Mittel manipuliert werden können und wie dies die Gesellschaft beeinflusst.

Um dies zu realisieren, folgt zunächst eine Erklärung des Begriffs der Wahlfälschung und der rechtlichen Konsequenzen. Danach werden die Grundlagen des Bereiches Hacking erläutert. Dafür erfolgt eine Erklärung der grundlegenden Begriffe und Verfahren zur Manipulation von Netzwerken und Computern. Wichtig ist dabei zu betonen, dass das Spektrum an Möglichkeiten enorm ist und sich im stetigen Wandel befindet, sodass es nicht möglich ist, alle Ansätze und Methoden in dieser Arbeit zu erläutern. Aus diesem Grund beschränkt sich die vorliegende Arbeit auf die bekanntesten und wichtigsten Methoden.

Nachdem die theoretischen Aspekte betrachtet wurden, werden dann die Situationen bei den US-Wahlen und in Deutschland beleuchtet. Dadurch können die Zusammenhänge von Hacking und Desinformationen, sowie deren Wirkungen beschrieben werden. Außerdem werden die Auswirkungen des digitalen Wandels, im Speziellen auf Deutschland, aber auch auf der ganzen Welt, aufgezeichnet.

Insgesamt hoffen wir, einen umfassenden Beitrag im Sinne der Demokratie und eines selbstbestimmten und kritischen Denkens eines jeden Menschen zu leisten, das auf der freien und fairen Willensbildung der Bürgerinnen beruht. Wenn diese Willensbildung durch technologische Eingriffe gestört oder verfälscht wird, kann dies schwerwiegende Folgen für die Legitimität und Stabilität unserer politischen Systeme haben. Aus diesem Grund ist es wichtig, sich mit diesem Thema auseinanderzusetzen und sich der Gefahren und Herausforderungen bewusst zu werden. Nur so können größere Katastro-

phen verhindert und unsere Demokratie geschützt und gestärkt werden.
So ist die Weisheit des bekannten Philosophen Immanuel Kant: “Habe Mut, dich deines eigenen Verstandes zu bedienen!” auch in solch besonderen Zeiten, in denen unser Verstand durch Hacking und Desinformationen manipuliert werden kann, immer noch aktuell.

2 Was versteht man unter einer Wahlfälschung?

In einer Demokratie bildet die freie und faire Ausübung des Wahlrechts das Fundament für legitime politische Entscheidungen. Die Integrität von Wahlen ist daher von entscheidender Bedeutung für das Funktionieren demokratischer Gesellschaften.
Zunächst soll eine präzise Definition des Begriffes der Wahlfälschung erarbeitet werden. Damit ist es anschließend möglich, verschiedene technische Möglichkeiten zu beschreiben, mit welchen Einfluss auf eine Wahl ausgeübt werden kann. Außerdem wird beleuchtet, welche rechtlichen Konsequenzen in solchen Fällen in Deutschland drohen.

2.1 Begriffserklärung

Gemäß dem deutschen Wahlrecht umfasst der Begriff Wahlfälschung sämtliche Maßnahmen, welche ergriffen werden, um das Ergebnis einer Wahl, entgegen der demokratischen Prinzipien, zu Gunsten oder Ungunsten einer Partei beziehungsweise eines Kandidaten zu beeinflussen (vgl. [1]). Im eigentlichen Sinne werden bei einer Wahlfälschung bestehende Vorschriften missachtet, um das gewünschte Ergebnis zu erreichen. Kandidaten oder Parteien, die zur Wahl stehen, können für Manipulationsversuche verantwortlich sein. Es ist jedoch auch eine signifikante Zunahme von Einflussnahme-Versuchen durch externe Dritte, wie ausländische Staaten und interessierte Unternehmen, zu beobachten (vgl. [2]). Wahlfälschungen treten systematisch in diktatorischen Systemen auf, welche versuchen durch Wahlen ihre Legitimation zu steigern. Ebenso können Betrugsversuche erschwert auch in demokratischen Systemen auftreten. Hier wird jedoch durch größtmögliche Transparenz, sowie Sicherheits- und Kontrollsysteme versucht, gezielte Manipulation zu verhindern. Indirekte Einflussnahmen durch u.a. Desinformationskampagnen sind dem hingegen schwierig identifizierbar und erfordern neue Richtlinien und entsprechende Maßnahmen. Da in einer zunehmend digitalen Gesellschaft der Informationskonsum der Menschen stetig wächst, stellen Desinformationen in Demokratien ein bislang unkontrollierbares Sicherheitsrisiko dar, wie den

folgenden Kapiteln noch näher verdeutlicht werden soll.

2.2 Rechtliche Konsequenzen

Nach Artikel 38 Absatz 1 des Grundgesetzes sind freie und unabhängige Wahlen ein wichtiger Bestandteil der Demokratie. Aus diesem Grund stellt in Deutschland Wahlfälschung gemäß §§ 107 ff des Strafgesetzbuchs (StGB) eine Straftat dar. Zur Straftat Wahlfälschung heißt es unter § 107a StGB [3]:

> [1] *Wer unbefugt wählt oder sonst ein unrichtiges Ergebnis einer Wahl herbeiführt oder das Ergebnis verfälscht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.*
>
> [2] *Unbefugt wählt auch, wer im Rahmen zulässiger Assistenz entgegen der Wahlentscheidung des Wahlberechtigten oder ohne eine geäußerte Wahlentscheidung des Wahlberechtigten eine Stimme abgibt*

Außerdem können Personen, die das Wahlergebnis falsch bekannt geben oder dies initiieren, mit einer Geldstrafe oder Freiheitsstrafe von bis zu fünf Jahren belegt werden (vgl. [3, § 107a, Absatz 2]). Zudem ist auch der Versuch der Wahlfälschung bereits strafbar.

3 Technische Möglichkeiten, Wahlen zu beeinflussen

Denkt man an Wahlbetrug, hat man zunächst das klassische Bild vor Augen, in dem die Stimmzettel gefälscht werden. Allerdings ist diese Methoden mittlerweile weit überholt und es gibt ein neues großes Spektrum an Möglichkeiten eine Wahl zu beeinflussen. Statt auf die alten, aufwendigen und „nutzlosen“ Methoden zu setzen, wird in der heutigen digitalisierten und technischen Zeit auf kreative und einfachere Möglichkeiten gebaut. Das Spektrum ist enorm und reicht von verzerrten Hochrechnungen, über Daten-Lecks, bis hin zur Verbreitung von Falschnachrichten in den sozialen Medien [11]. In der Zeit von Facebook, Instagram und TikTok ist es leicht, Nachrichten und Informationen zu verbreiten. Hier kommen die „Social Bots“ in Einsatz. Social Bots sind Computerprogramme, welche in den sozialen Netzwerken arbeiten. Oft werden sie als „gute“ Bots eingesetzt und können so als kleine Helfer, beispielsweise in der Umwandlung von Tweets in Facebook-Posts, arbeiten. Jedoch werden sie vermehrt auch in

der Verbreitung von Falschnachrichten und Fehlinformationen eingesetzt. Sie arbeiten meist von Fake-Accounts und verbreiten ihre Informationen rasend schnell [12]. Weitere Möglichkeiten sind zum Beispiel die Strategie des Chaos, welche beispielsweise beim Brexit in Großbritannien angewendet wurde und „Deep-Fakes“. Als Deep-Fakes werden KI generierte Fälschungen bezeichnet, welche häufig mithilfe des Internets verbreitet werden. Die künstliche Intelligenz kann ohne großen Aufwand Gesichter, Stimmen, Informationen und Texte verändern. Somit wird es Hackerinnen erleichtert, Desinformationskampagnen zu starten. Die KI kann beispielsweise auf Grundlage eines Videos, die darin gezeigte Person etwas sagen lassen, was diese in der realen Welt niemals gesagt hat. Im Zusammenhang der Wahl können diese Desinformationskampagnen gefährlich werden, da die Nutzerin nicht in der Lage ist, zu unterscheiden, ob sie die Realität oder eine Fälschung sieht [13]. In Abbildung 1 sieht man ein Beispiel für Deepfakes. Dieses KI-generierte Bild zeigt die Verhaftung von Donald Trump, welche in der Realität niemals stattgefunden hat.

Abbildung 1: Deepfake (Trump bei einer Verhaftung) [14]

4 Desinformationskampagnen

Von Pharao Ramses bis Trump: Fake News gibt es schon lange. Gezielt verbreitet dienen sie seit Jahrtausenden in Krisen und Kriegen als unterschätzte Waffe. Durch die zunehmende Digitalisierung eröffnen sich allerdings beispiellos neue, wirksamere Möglichkeiten, demokratische Prozesse wie Wahlen gezielt zu beeinflussen. Besonders autoritären Regimen bieten sich somit eine Vielzahl an Möglichkeiten, um öffentliche Meinungen im In- und Ausland zu manipulieren und ihre Machtposition nachhaltig zu stärken.

Der Umgang mit Desinformationen gestaltet sich sowohl für politische Institutionen als auch für die Bevölkerung schwierig. Wie unterscheidet man Fake News von vertrauenswürdigen Informationen? Wie ist es möglich, dessen Verbreitung einzudämmen, wenn Empfehlungsalgorithmen die Fehlinformationen immer weiterverbreiten? Eine konkrete Beantwortung dieser Fragen erscheint aufgrund der Komplexität der Problematik als schwierig, ist wahrscheinlich sogar unmöglich. Trotzdem soll nachfolgend versucht werden, die wichtige Thematik schrittweise, anhand von Beispielen zu erörtern, um anschließend mögliche Handlungsmaßnahmen zu dessen Bekämpfung vorzuschlagen.
Angesichts der Neuartigkeit und Komplexität der Thematik ist es zunächst erforderlich, eine eindeutige Begriffserklärung zu erarbeiten. Es folgt die Erklärung zentraler Begrifflichkeiten, Konzepte, sowie der Funktionsweise von Desinformationen im digitalen Raum. Hierbei wird besonders die Rolle der sozialen Medien genauer betrachtet und untersucht, welche psychologischen und technischen Mechanismen die Verbreitung von Desinformationen verstärken. Kapitel 4.3 „Ausgewählte Desinformationskampagnen“ richtet daraufhin den Blick auf den organisierten Einsatz digitaler Desinformation zur außenpolitischen Einflussnahme. Dabei werden zwei Bespiele beleuchtet, welche die Dimension der Problematik exemplarisch verdeutlichen sollen. Daraufhin können auf Grundlage mehrerer Studien des ISD (Institute for Strategic Dialogue) Aussagen darüber getroffen werden, welche verschiedenen Maßnahmen zur nachhaltigen Bekämpfung von Desinformationen in den sozialen Netzwerken existieren und wie diese sinnvoll in Deutschland und der Europäischen Union eingesetzt werden könnten. Es folgt abschließend eine Betrachtung der aktuellen Konzepte zur Bekämpfung digitaler Desinformationen in Deutschland.

4.1 Terminologie: Schlagwörter im Überfluss

Der Einfluss von Desinformationen auf die öffentliche Meinungsbildung im Netz steht spätestens seit der US-Präsidentschaftswahl 2016 im Blickpunkt von Wahlkämpfen demokratischer Systeme. Aufgrund des zunehmenden politischen und öffentlichen Diskurses nimmt auch das Interesse innerhalb der Wissenschaft stetig zu. Es folgt eine steigende Vielfalt an Begrifflichkeiten, welche versuchen das Phänomen zu beschreiben, zu analysieren und zu erklären. Dies erschwert eine spezifische Betrachtung der Thematik, da sich zwischen den einzelnen Erklärungsansätzen einige Abweichungen und Widersprüche ergeben.
Zunächst wird nun der Begriff der Desinformation nach Don Fallis definiert. Fallis

charakterisiert eine Desinformation anhand von drei Merkmalen [15, S.404-406]:

1. *Desinformation Is Information*
2. *Disinformation Is Misleading Information*
3. *Disinformation Is Nonaccidentally Misleading Information*

Das bedeutet, eine Information kann als Desinformation aufgefasst werden, wenn sie falsche oder irreführende Informationen enthält und zudem die Funktion besitzt, den Leser vorsätzlich in die Irre zu führen. Dies deckt sich mit der Auffassung verschiedener politischer Institutionen. So bezeichnet die Bundesregierung eine Desinformation als „[. . .] nachweislich falsche oder irreführende Information, die mit Ziel der vorsätzlichen Beeinflussung oder Täuschung der Öffentlichkeit verbreitet werden“ (vgl. [16, S.2]).
Allgemein wird in vielen wissenschaftlichen Studien und Büchern eine Desinformation in Abgrenzung zu einer „misinformation“ definiert. Dabei beschreiben beide Begriffe eine Information welche falsch, fehlerhaft oder irreführend ist (vgl. [17]). Der Unterschied besteht allerdings darin, dass eine Desinformation vorsätzlich fehlerhaft bzw. irreführend ist, während eine Missinformation diese Mängel unabsichtlich aufweist. Desinformationen werden zudem oft mit der Absicht verbreitet, in die Irre zu führen und Schaden anzurichten, wohingegen Missinformationen aus einem ehrlichen Fehler, Nachlässigkeit oder unbewusster Verzerrung resultieren kann.
Der Begriff der Desinformation wird im politischen und wissenschaftlichen Kontext oft dem englischen Begriff „Fake News“ gleichgesetzt. Dabei beziehen sich „Fake News“ meistens auf Desinformationen im digitalen Umfeld (vgl. [18]). Genauer charakterisiert Gelfert „Fake News“ als Form von Berichterstattungen (vgl. [19]). Damit umfasst eine Desinformation ein um einiges größeres Spektrum an Inhalten, die nicht ausschließlich auf Berichterstattungen beschränkt sein müssen. Man kann daher Fake News als Unterkategorie von Desinformationen betrachten, welche überwiegend in den Sozialen Medien kursieren. Ferner werden unter Desinformationskampagnen verschiedene Praktiken und Verhaltensmuster gefasst, welche zur Vorbereitung von Fake News und Fehlinformationen im digitalen Raum und in den sozialen Netzwerken dienen. Beispiele hierfür sind social bots, astroturfing, computational propaganda und targeted advertising (vgl. [20]).
Die Motivation hinter der Verbreitung von Desinformationen und Fake News sind vielfältig. Wardle und Derakhshan kategorisieren als mögliche Motivationen finanzielle, politische, soziale und psychologische Aspekte (vgl. [21]). Besonders im Fokus sind

dabei problematische Inhalte, die dem Zweck dienen, politischen Einfluss zu nehmen, um so ein vermeintlich funktionierendes System zu stören. Ähnlich vielfältig, wie die Motivationen hinter Desinformationen sind auch die Urheberinnen und am Verbreitungsprozess beteiligten Personen. Diese können „sowohl von individueller als auch von kollektiver Ebene ausgehen sowie private, nicht-staatliche oder staatliche Akteure involvieren“ [22]. Die korrekte Zuordnung der Urheberin stellt dabei oft einen sehr schweren und aufwendigen Prozess dar. Auf den meisten Informationswegen agieren eine Vielzahl von involvierten Akteuren, weshalb eine unmittelbare Urheberschaft nur mit hohem Aufwand nachzuweisen ist. Außerdem sind die meisten Urheberinnen bemüht ihre Identität zu verschleiern und dem Prinzip der plausiblen Abstreitbarkeit möglichst zu folgen. Wie Desinformationskampagnen im Detail eingesetzt werden, soll in Kapitel 4.3 an verschiedenen Beispielen erläutert werden.
Zusammenfassend konnte nun der Begriff der Desinformation aus verschiedenen Blickpunkten beleuchtet werden. Dabei wurde klar, dass im Bereich der digitalen Desinformation eine Vielzahl sich überschneidender, unscharfer Begriffe und Konzepte existieren, welche die wissenschaftliche Auseinandersetzung mit der Problematik erschweren. Im Rahmen dieser Arbeit soll nachfolgend die Desinformationen im digitalen Raum genauer betrachtet und die zunehmende Problematik der Sozialen Medien beschrieben werden.

4.2 Desinformationen im digitalen Raum

Durch die zunehmende Digitalisierung hat sich Art und Weise, mit welcher Informationen produziert, kommuniziert und verbreitet werden nachhaltig verändert. In den Sozialen Medien ist es heute für jede registrierte Person möglich, Informationsbeiträge kostenlos, anonym, sowie mit hoher Geschwindigkeit zu erstellen. Mittels Algorithmen kann der Beitrag dann weltweit verbreitet werden und so mehrere Millionen Nutzerinnen erreichen. Desinformationen bieten somit eine nie dagewesene Ausgangssituation. In kürzester Zeit können Falschinformationen koordiniert unzählige Personen erreichen, während die vermeintlichen Verfasserinnen anonym bleiben und von einem beliebigen Standpunkt in der Welt agieren.
In den folgenden Kapiteln soll nun näher erörtert werden, weshalb der digitale Raum für die Verbreitung von Desinformationen prädestiniert ist. Dabei wird beleuchtet, welche besondere Stellung die sozialen Medien bei Desinformationskampagnen einnehmen. Außerdem ist es daraufhin möglich, verschiedene psychologische und technische Aspek-

te herauszustellen, die dem Phänomen der digitalen Desinformation zugrunde liegen oder diese zumindest begünstigen. Der Schwerpunkt liegt dabei überwiegend auf Desinformationen, welche im Kontext mit Wahlmanipulation und politischer Einflussnahme stehen.

4.2.1 Soziale Medien

Im Zuge der fortschreitenden Globalisierung und Digitalisierung generieren die sozialen Medien eine immer größere gesellschaftliche Bedeutung. Sie zählen bei einer Vielzahl von Menschen zu den festen Bestandteilen des Alltags. Spezifisch können die sozialen Medien dabei als Internet-Plattformen charakterisiert werden, „die auf Web 2.0 -Basis arbeiten, den Austausch von user-generated content ermöglichen sowie die Erstellung und Vernetzung individueller Profile erlauben“ (vgl. [23]). Bemerkenswert ist dabei, dass sich die aktiven Nutzer überwiegend auf eine begrenzte Anzahl an Plattformen verteilen. Betrachtet man die Marktanteile von Social-Media-Seiten nach Seitenabrufen fällt auf, dass im Oktober 2023 die Plattformen Facebook (65,58%), Instagram (11,9%), Twitter (8,63%) und Pinterest (8,38%) alleine 94,49% der internationalen Marktanteile besitzen (s. Kapitel 8.1 (1), [24]). Dies entspricht in etwa der Größenordnung von 6 Milliarden aktiven Accounts.
Angesichts der enormen Reichweite sind die sozialen Medien eine optimale Umgebung für die Verbreitung von Desinformationen. Es kann eine hohe Anzahl an Menschen erreicht werden, welche sich durch den oft individuellen Aufbau eines Posts persönlichen angesprochen fühlen. Dies ist auch die Grundlage für die Geschäftsmodelle verschiedener sozialer Medien. Die Erfassung von Metadaten der Nutzerinnen ermöglicht es, Rückschlüsse auf das digitale Verhalten, persönliche Informationen, Vorlieben und Interessen, sowie die politischen Einstellungen zu ziehen und somit individualisierte Werbeanzeigen zu schalten. Zudem wird die Verbreitung von Inhalten von plattformspezifischen Algorithmen und Automatismen unterstützt, die beeinflussen, welche Themen und Inhalte von den Nutzerinnen wahrgenommen werden und somit an Aufmerksamkeit und Bedeutung gewinnen (vgl. [22]). Der zusätzliche weitläufige Verzicht von einer inhaltlichen Überprüfung der verbreiteten Inhalte durch die Plattformen bildet die besten Voraussetzungen dafür, die Wahrnehmungen, das Verhalten oder die Meinungen der Nutzerinnen gezielt durch geplante Kampagnen von Dritten zu manipulieren und somit politischen Einfluss zu nehmen.
Das Verhältnis von politischen Institutionen zu sozialen Medien ist oft widersprüchlich. Zum Einen werden digitale Plattformen zur politischen Kommunikation und teil-

weise zur Verbreitung von Propaganda genutzt, zum Anderen werden sie wegen dem Verbreiten von Falschnachrichten und der Möglichkeit, Opposition und Protest großflächig zu organisieren, kritisiert. In autoritären Staaten werden soziale Plattformen überwiegend als Instrument benutzt, mit welchem soziale Kontrolle ausgeübt werden kann. Die Benutzerinnen in demokratischen Systemen wiederum werden meist in ihrer Meinungsbildung gezielt beeinflusst. Dabei vereinfachen soziale Plattformen die praktische Koordination politischer Proteste, indem sie den Austausch von Informationen, sowie emotionaler und motivierender Inhalte ermöglichen (vgl, [25]), welche wiederum Proteste und die Entstehung sozialer Bewegungen unterstützen können (vgl. [22]).
Ein großer Vorteil des digitalen Raumes stellt die weitreichende Anonymität der handelnden Akteure dar. Diese profitieren von der schnellen, kostengünstigen Erstellung und Verbreitung von Inhalten in den einzelnen Netzwerken. Dieses Merkmal bedingt allerdings ein weiteres zentrales Problem, welches die Unterscheidung von Wahrheit und Lüge zunehmend erschwert. Immer häufiger gibt es Fälle, bei denen traditionelle Medienseiten originalgetreu imitiert und anschließend mittels Fake Accounts hundertfach in den Sozialen Medien geteilt werden. Das Teilen und Austauschen der Inhalte trägt dabei dazu bei, dass das Konzept der Quellenzuordnung verwässert wird (vgl. [26]), indem eindeutige, visuelle Kennzeichen des traditionellen Journalismus wegfallen (vgl. [19]). Zur Verdeutlichung dieses Verfahrens betrachtet man dazu ein aktuelles Beispiel, welches auf der Grundlage des Ukraine-Konflikts beruht.

Abbildung 2: Imitierte Webseite der Bildzeitung [27]

Der abgebildete Webseitenausschnitt stammt aus dem September des vergangenen Jahres und proklamiert den Tod eines Teenagers aufgrund von Einsparungen in der Stadt Berlin. Die Webseite besitzt dabei das typische Layout der Online-Nachrichtenseite von

„Bild-Deutschland“, der auflagenstärksten Tageszeitung in Deutschland. Die Berichterstattung von Bild ist bekanntlich kontrovers und von öffentlichen Diskussionen geprägt, weshalb ein solcher Beitragstitel als authentisch wahrgenommen werden kann. Zusätzlich zu der Webseite war auf den sozialen Plattformen Facebook und Twitter (heute X) ein Video im Umlauf, welches einen Polizeieinsatz mit Rettungshubschrauber, untermalt von melancholischer Musik zeigt. Es war außerdem der Untertitel eingeblendet: „Der 16-jährige Marius fuhr spätabends mit dem Fahrrad nach Hause. Der Junge sah das Loch in der Dunkelheit nicht und fiel hin. Er ist verblutet, da Passanten ihn im Dunkeln nicht gefunden haben“ [28]. In der Postbeschreibung findet man auch eine Verlinkung zu der oben genannten Webseite. Untersucht man allerdings den Beitrag genauer stellt sich heraus, dass an dieser Meldung alles falsch ist. Es gab in dem Zeitraum weder einen tödlichen Sturz, noch ist ein vergleichbarer Unfall der Berliner Polizei bekannt. Auch stammt das zehntausendfach geteilte Video nicht von der Bild-Zeitung. Die angebliche Nachrichtenseite ist ein neuer, sehr professionell gemachter Fake, einer von Unzähligen. Schon mehrere Dutzend solcher pro-russischer Fake-Seiten wurden im vergangenen Jahr in Deutschland enttarnt, betroffen waren unter anderem die Onlineauftritte von ARD, Spiegel Online, Zeit und t-online. Das Ziel etwaiger Kampagnen ist klar erkennbar: Die Bevölkerung verunsichern und Stimmung gegen die Sanktionen machen, welche im Rahmen des Ukraine-Konflikts Russland auferlegt wurden. Bewusst wurden solche Kampagnen auch im Wahlkampf der Landesparlamente eingesetzt, um Einfluss auf die Entscheidungsfindung der Bürgerinnen zu verüben. So fielen mehrere Berichte im t-online-Design auf, welche berichten „Baerbock bereitet einen Atomkrieg vor“ oder „Bundeskanzler Scholz hat mit den wirtschaftlichen Sanktionen gegen Russland das Todesurteil für Deutschland unterschrieben“ [28]. Das Problem bei diesen Webseiten ist, dass auch wenn die Seiten enttarnt und gelöscht wurden, Screenshots und Videos weiter in den Sozialen Medien im Umlauf sind und durch eine „Armee von Fake-Profilen“ weiterverbreitet werden. Eine effektive Selektion der immensen Menge an Desinformationen in den sozialen Medien erscheint im Moment nahezu unmöglich. Eine Verbesserung ist diesbezüglich auch nicht in Aussicht, da die Plattformen Änderungen nur durchsetzen, wenn sie mittels Gesetze dazu gezwungen werden. Der vermeintliche Grund, warum Plattformen das Problem nicht selbstständig wirksam angehen, ist vermeintlich einfach: Sie erweitern ihre Reichweite und verdienen Geld mit den Falschnachrichten [28].

Bezüglich der Verbreitung von Desinformationsnarrativen müssen besonders die Plattformen Facebook und Twitter (heute X) hervorgehoben werden. Facebook stand in den

vergangenen Jahren gehäuft im Mittelpunkt breit angelegter Desinformationskampagnen und kann nachträglich als Auslöser der weltweiten Debatten über Nutzen und Funktion der sozialen Medien angesehen werden. Besonderer Beachtung gilt in diesem Zusammenhang dem US-Wahlkampf 2016, welchem auf Grund seiner Prominenz in dieser Thematik ein eigenes Kapitel in der vorliegenden Arbeit zugeschrieben wird.
Für die digitale Verbreitung und den Austausch von Informationen gewinnen die sogenannten Sofortnachrichtendienste wie WhatsApp, Telegram, Signal oder Discord in den letzten Jahren stetig an Bedeutung. Aufgrund dieser Entwicklung werden die sozialen Medien und Sofortnachrichtendienste zu einem Grundbaustein der modernen politischen Kommunikation, insbesondere in demokratischen Prozessen und bei Wahlkämpfen. Dementsprechend häufen sich auch die Fälle von Desinformationskampagnen, die über die eben genannten Kanäle verbreitet werden (vgl. [29]).
Zusammenfassend kann festgehalten werden, dass die sozialen Medien ein hervorragendes Umfeld für politische Desinformationskampagnen sind. Es ist daher davon auszugehen, dass in den kommenden Jahren die Bedeutung der sozialen Medien für die Verbreitung von Desinformation weiter zunehmen wird. Die Anfälligkeit sozialer Plattformen für Desinformationskampagnen ist erschreckend, weshalb eine koordinierte Regulierung durch staatliche Institutionen unabdingbar erscheint.

4.2.2 Psychologische und technische Aspekte

Im vorherigen Kapitel wurde festgestellt, dass sich Desinformationen ausgezeichnet in den sozialen Netzwerken verbreiten können. Nachfolgend soll nun schrittweise erörtert werden, welche Prozesse den Konsum und die Verarbeitung der Informationen aus psychologischer und technischer Sicht in den sozialen Netzwerken begünstigen. Dabei wird sich auf die Erkenntnisse des Fachbuches „Kollektive Strategien zur Abwehr digitaler Desinformation“ von Karl Moritz Heil bezogen [22].
Innerhalb der bestehenden Informationsflut müssen die Inhalte um die begrenzte Aufmerksamkeit der Nutzerinnen konkurrieren. Besonders wirksam zeigen sich dabei Inhalte, welche bei dem Leser starke Gefühle hervorrufen. In dieser Verbindung steht ein prominenter Effekt, welcher in der Fachliteratur unter Negativitätsbias aufgeführt wird. Dieser besagt, dass Informationen eine hohe Aufmerksamkeit generieren, wenn sie bei den Nutzerinnen negative Emotionen wecken. Im politischen Kontext sind dies etwa Ängste und Sorgen (z.B Existenzängste) und überwiegend Empörung (z.B. politische Entscheidungen). Dieser Effekt kann zusätzlich durch den „confirmation bias“ verstärkt werden, welcher besagt, dass „Informationen wahr- und ernst genommen [werden, wenn

sie] in das eigene Weltbild passen“ [30]. Desinformationskampagnen im Vorfeld einer Wahl sind also umso erfolgreicher, je mehr negative Emotionen sie bei den Leserinnen hervorrufen und desto authentischer bestehende Überzeugungen und Vorteile bedient werden. Authentische Beispiele für diesen Effekt stellen Fehlinformationen über Politikerinnen dar (s. Kapitel 8.1 (5)). Diese können vermeintliche Vorurteile bestätigen und damit die politische Wahrnehmung der Nutzerinnen beeinflussen.
Ein weiterer wichtiger psychologischer Effekt stammt aus dem Gebiet der Sozialforschung. Dieser besagt, dass der interaktive Charakter der sozialen Medien die Herausbildung von Zugehörigkeitsgefühlen und Identitäten vereinfacht. Das bedeutet, innerhalb eines Netzwerkes kommt es oft zur Interessengruppenbildung. Die Anhängerinnen dieser Gruppen beeinflussen sich dann gegenseitig, welchen Informationen man Glauben schenkt und weiterverbreitet und welchen nicht. Für diesen Effekt könnte man als Beispiel diverse Telegramm Gruppen aufführen. Innerhalb diesen werden oft Desinformationen über bestimmte Parteien oder politische Einstellungen an „Gleichgesinnte“ verbreitet. Ähnlich kann die Idee der „Filterblase“ aufgeführt werden, welche besagt, „dass die Algorithmen, mit denen die Anzeige von Inhalten auf die [Nutzerinnen] personalisiert wird, dazu beitragen können, eine homogene Informationsblase aufzubauen, in der Desinformation multipliziert wird" [22].
Die beschriebenen Effekte können durch die technischen Möglichkeiten des digitalen Raumes noch weiter verstärkt werden. So können etwa personalisierte Metadaten zum Verhalten der Nutzerinnen dazu genutzt werden, um Desinformationsinhalte auf das Zielpublikum zugeschnitten auszurichten. Unterstützt wird dieses Vorgehen zusätzlich durch das werbebasierte Geschäftsmodell der sozialen Plattformen. Mittels diesem erhalten interessierte Käufer Zugang zu ausgewählten Verhaltensdaten der Nutzerinnen, anhand derer sich anschließend Desinformationskampagnen effektiver gestalten lassen (vgl. [31]).
Desinformationen können zudem durch den organisierten Einsatz von social bots verstärkt werden. Mithilfe halb-automatischer Prozesse ist es so möglich, Desinformationen großflächig im Netz zu verbreiten, ohne auf die Interaktion realer Accounts angewiesen zu sein. Die Bots bauen hierzu ein strategisches Netzwerk auf, mit welchem sie versuchen, die Algorithmen und oben beschriebene Effekte der sozialen Medien auszunutzen, um so Einfluss auf den Diskurs der Leserinnen auszuüben. Zusätzlich können hybride Accounts, die teilweise menschlich gesteuert werden, systematisch Desinformationsinhalte und Desinformationsnarrative in den sozialen Medien verbreiten und auf äußere Umstände reagieren, um den Effekt der Authentizität aufrecht zu erhalten.

Das Potenzial von Künstlicher Intelligenz und maschinellen Lernen gewinnt zunehmend auch im digitalen Raum zur Verbreitung von Falschinformationen an Bedeutung. Es ermöglicht, menschliches Verhalten glaubwürdig zu simulieren und somit die Enttarnung von Desinformationen zu erschweren. Damit können unter anderem wirkungsvolle Deepfakes erstellt werden, auf welche in der Arbeit bereits genauer eingegangen wurde. Der technologische Fortschritt ermöglicht es außerdem, immer realistischere Desinformationen mittels digitaler Werkzeuge zu erstellen. Die Manipulation von Text-, Bild-, Video- und Audiomaterial ist mittels moderner Bearbeitungsapps wahrscheinlich einfacher wie je zuvor. Die zusätzliche Steigerung der Qualität der Bearbeitungswerkzeuge führt fortlaufend dazu, dass das ursprüngliche Original nur sehr schwierig von der Fälschung unterschieden werden kann.
Insgesamt lässt sich feststellen, dass die Verbreitung von Desinformationen durch den Aufbau von sozialen Plattformen mittels psychologischer und technischer Faktoren verstärkt werden kann. Dabei schließen sich die einzelnen psychologischen und technischen Effekte/ Möglichkeiten nicht aus, sondern unterstützen sich gegenseitig. Das Erkennen einer fehlerhaften Information wird immer schwieriger und erfordert ein umfassendes Verständnis von Technologie, Medien und menschlichen Verhalten.

4.3 Ausgewählte Desinformationskampagnen

Die zu untersuchende Problematik wurde bis jetzt überwiegend theoretisch betrachtet. Um den Einfluss von Desinformationskampagnen exemplarisch herauszustellen sollen nun zwei konkrete Beispiele aus der Realität vorgestellt werden. Dabei handelt es sich lediglich um einen selbstgewählten Ausschnitt einer Kampagne, weshalb die nachfolgenden Ausführungen nicht auf Vollständigkeit beruhen.

4.3.1 Der Fall „Team Jorge “

Team Jorge ist der Name einer israelischen Arbeitsgruppe, welche nachweislich mittels social bots Desinformationskampagnen in den Sozialen Medien betreibt, um so die Ergebnisse von Wahlen gezielt zu manipulieren. Die wichtigsten Akteure bei Team Jorge sind dabei ehemalige Sicherheits- und Geheimdienstmitarbeiter. Aufgeflogen ist das Unternehmen im Februar 2023 durch eine Undercover-Operation verschiedener Journalisten aus dem Netzwerk „Forbidden Stories“. Diese gaben sich als ein potenzieller Käufer aus, welche Einfluss auf eine Wahl in Afrika verüben möchte. Dabei wurde herausgefunden, dass die israelische Arbeitsgruppe seit 2015 aktiv ist und mindestens

33 Präsidentschaftswahlen manipuliert hat, nach Angaben der Firma in 27 Fällen mit dem gewünschten Erfolg.
Im Zentrum der durchgeführten Desinformationskampagnen steht das Software Programm AIMS (Advanced Impact Media Solutions). Mit AIMS ist es möglich, eine große Anzahl von gefälschten Social-Media- Profilen (z.B. auf X und Facebook) zu erstellen und automatisch zu steuern (vgl. [32]). Diese Accounts sind dabei authentisch mit KI generierten Profilbildern gestaltet und teilweise mit Amazon, Kreditkarten und Bitcoin Konten verbunden. Es ist so kaum möglich, ein Fake-Profil zu enttarnen, weshalb diese wirkungsvolle Falschnachrichten verbreiten können. Neben KI generierten Bildern nutzt die Firma offenbar auch Bilder von Social-Media-Profilen wie TikTok, ohne dass die Betroffenen dies mitbekommen. Diese Tatsache bestätige beispielsweise eine Frau aus Großbritannien, bei welcher ohne Erlaubnis Fotos aus dem Jahr 2018 entwendet wurden.
Als Demonstration des AIMS-Systems wurde im Juli 2022 unter dem Hashtag „#RIP_Emmanuel“ eine Desinformationskampagne auf Twitter gestartet. Emmanuel ist dabei ein Emu, der auf der Plattform TikTok eine tierische Berühmtheit ist. Tatsächlich verbreiteten zahlreiche Twitter-Konten den Hashtag und die Falschnachricht vom Tod des Emus Emmanuel. In einigen Ländern landete die vermeintliche Falschinformation sogar in den nationalen Trends. Anhand der inszenierten Kampagne war es zusätzlich möglich, rund 20 Social-Media-Kampagnen zu identifizieren, bei denen Avatare eingesetzt wurden, die in der AIMS-Software von Team Jorge auftauchen. Es waren Kampagnen in den USA, Großbritannien, Frankreich und Panama (vgl. [33]).
Zusätzlich zu der automatischen Steuerung von gefälschten Profilen verschafft sich Team Jorge Zugang zu anvisierten Konten durch direktes/brute-force Hacken (vgl. [34]). So ist es möglich, Social-Media-Kanäle nichtsahnender Dritter zu kontrollieren. Innerhalb einer Live-Präsentation präsentierte ein Mitarbeiter der Arbeitsgruppe dieses Vorgehen. Dabei wurden die Chats und Mailpostfächer eines afrikanischen Politikers gehackt und kurze Beispielnachrichten verschickt. Ein Reporter des „Spiegels“ suchte daraufhin den Geschädigten in Afrika auf, welcher den Angriff bestätigen konnte. Tatsächlich tauchte die Demo-Nachricht mit richtigem Datum und Uhrzeit in dessen Postfach auf.
Schon 2014 nahmen Mitarbeiter der Arbeitsgruppe nachweislich an Besprechungen mit Cambridge Analytica teil (vgl. [35]), einer Datenanalysefirma, welche in einer Vielzahl von Fällen in Verbindung mit Wahlbeeinflussung steht (s. Kapitel 4.3.2) Zusätzlich beweisen E-Mails, welche der Zeitung The Guardian zugänglich gemacht wurden, dass

Team Jorge auch in 2015 und 2017 mit Cambridge Analytica in Kontakt stand, bezüglich politischer Kampagnen in Afrika und Südamerika. Die beiden Gruppen arbeiteten zusammen an der Manipulation der nigerianischen Wahlen. Dabei wurde versucht, dem amtierenden Präsidenten Goodluck Jonathan zur Wiederwahl zu verhelfen, indem sein Gegenkandidat Muhammadu Buhari durch eine Verleumdungskampagne geschwächt werden sollte.

4.3.2 Cambridge-Analytica-Datenskandal

Der Skandal um die Datenanalysefirma CA (Cambridge Analytica) offenbart im Jahr 2018 eines der größten Datenlecks aller Zeiten und gilt heute als prominentestes Beispiel in der Causa breit angelegter Desinformationskampagnen. Noch immer sind nicht alle Untersuchungen zu diesem komplexen Fall abgeschlossen, weshalb in regelmäßigen Zeitintervallen neue Erkenntnisse ans Licht kommen.
Nachfolgend sollen nun die Ziele und Methoden von CA betrachtet werden. Zunächst kann als Hauptgeschäft von CA die Verbraucherforschung aufgeführt werden. Mithilfe von Datensätzen wurden Persönlichkeitsprofile erstellt, welche es ermöglichten, Werbung sehr genau auf die Menschen zuzuschneiden und eine personalisierte, passende Ansprache zu finden (vgl. [36]). Das Angebot richtete sich dabei sowohl an Firmenkunden, als auch Politiker im Wahlkampf. Passend war auch das Firmenmotto formuliert: „Wir finden Ihre Wähler[innen] und mobilisieren sie“. Sie kombinieren dazu die Datenanalyse mit der Verhaltensforschung, um jede Einzelperson verstehen und somit persönlich erreichen zu können. Dabei orientierte sich CA an dem Fünf-Faktoren-Modell aus der Psychologie (s. Kapitel 8.2 (1)).
Im Zentrum des aufgedeckten Skandals im Jahr 2018 steht der mittlerweile bewiesene Vorwurf, dass CA Daten von Facebook-Profilen gesammelt hat, um diesen gezielt politische Werbung zu schalten. Facebook geht dabei von mindestens 87 Millionen betroffenen Accounts aus. Dabei liegt der Schwerpunkt auf den US-Amerikanischen Markt, welcher nach einer Statistik mit 70,63 Millionen Accounts eindeutig am stärksten von dem Skandal betroffen ist (s. Kapitel 8.1 (2), [37]). Aber wie kam CA an die Daten der Nutzerinnen? Dies ist ein längerer Prozess, welcher bereits im Jahr 2014 begann. Damals programmierte Aleksandr Kogan eine Facebook-App namens „thisisyourdigitallife“ welches sich das System des „Microtargeting“ zu Nutzen machte. Mit der App konnten Facebook-Nutzerinnen einen Persönlichkeitstest machen, bei welchem jedoch nicht nur Informationen über die eigentlichen Nutzerinnen, sondern auch über deren Facebook-Kontakte gesammelt wurden. Kogans Firma GSR (Global Science Research)

konnte so ohne größere Schwierigkeiten auf die Profile von rund 87 Millionen Personen zugreifen und aus diesen Daten umfangreiche Persönlichkeitsprofile erstellen. Das Verrückte daran, Facebook hat sich zunächst nicht für den vermeintlichen Datenleck interessiert. Stattdessen wurden von GSR Millionen von Nutzerprofilen und persönlichen Daten systematisch von Facebook-Servern abgezogen. Die betroffenen Personen erfuhren nie davon (vgl. [36]).
Unwissend wurden die Daten im Folgenden an das Unternehmen CA verkauft. Dieses benutzte es anschließend, um Wahlen in der USA zu beeinflussen. Zusätzlich wurden die Daten durch die Erkenntnisse des Fragebogens zur Persönlichkeitsanalyse, die die eigentlichen Nutzerinnen der App ausgefüllt hatten, ergänzt. Dadurch ergab sich eine Masse an psychologischen Profilen, die groß genug war, um auch über die Millionen von Nutzerinnen, die den Fragebogen gar nicht ausgefüllt hatten, psychologische Profile anlegen zu können (vgl. [36]).
Basierend auf aktuellen Erkenntnissen wurden die Daten von Cambridge Analytica während der US-Präsidentschaftswahl 2016, sowie bei der intensiveren Brexit-Kampagne "leave.eu" durch Microtargeting-Methoden genutzt, bei denen Wähler auf Grundlage ihrer psychologischen Profile angesprochen wurden. Dabei vermehrt auch mit Informationen, welche sich als fehlerhaft herausstellen. Es gibt unterschiedliche Ansichten darüber, inwieweit diese Strategien den Wahlausgang beeinflusst haben könnten. Selbst wenn sie einen Einfluss gehabt hätten, könnte man argumentieren, dass dies nicht unbedingt als Wahlmanipulation betrachtet werden sollte. Vielmehr handelte es sich um die gezielte Ansprache von Einzelpersonen mit spezifischen, auf sie abgestimmten Botschaften. Dennoch wurden diese Strategien auf der Grundlage von unrechtmäßig erworbenen Persönlichkeitsprofilen durchgeführt (vgl. [36]).
Obwohl der Skandal schon vor einigen Jahren aufgedeckt wurde, hat sich bis heute noch nicht viel bezüglich Datenschutz verändert. Die Firmen CA und GSR sind zwar im Zuge der Affäre verschwunden, werden aber bestimmt bereits durch neue Konstrukte ersetzt. Es ist daher an der Zeit, neue verschärfte Regeln zum Datenschutz und damit auch zum Schutz demokratischer Systeme aufzustellen. Die Politik ist in dieser Hinsicht gefordert, da Plattformen wie Facebook selbst bei starkem Druck von außen, ihre Verfahren nur bedingt anpassen. Zu profitabel ist das Geschäft mit persönlichen Daten und zu verlockend das Streben nach Macht und Einflussnahme in einem System.

4.4 Maßnahmen: Bekämpfung von Desinformation im Internet

Angesichts der Gefahren, die von Desinformationskampagnen für die Grundwerte einer demokratischen Gesellschaft ausgehen, ist es dringend erforderlich, Maßnahmen zu dessen Bekämpfung im Internet zu ergreifen. Dabei müssen gezielt die Betreiberinnen von sozialen Plattformen in die Pflicht genommen werden. Entgegen der häufigen Selbstdarstellung als neutrale Kommunikationskanäle verkörpern soziale Plattformen wie Facebook, X und Instagram große Medienunternehmen, die mutmaßlich selbst darüber entscheiden, welche Inhalte gezielt verbreitet werden sollen (vgl. [38]). Verschiedene Algorithmen dienen dazu, einen personalisierten Newsfeed bei den Nutzerinnen zu erzeugen. Daher ist es für die Betreiberinnen möglich, den Informationsfluss aktiv zu kontrollieren und zu steuern. Hier sollten rechtliche Vorgaben ansetzen, die darauf abzielen, digitale Desinformationen einzuschränken. Dabei muss gewährleistet werden, dass das in einer Demokratie verankerte Recht auf Meinungsfreiheit nicht systematisch eingeschränkt wird. Die Sozialen Medien sollten ein Ort des offenen Austausches sein, welcher weder von anderen Staaten noch von dem eigenen politischen System beeinflusst wird. Letzterer Fall ist vor allem in autoritären Systemen wie China und Iran verstärkt vorzufinden. Es ist daher schwierig Lösungsansätze zu entwickeln, die verschiedene anhaltende systemische Herausforderungen berücksichtigen und gleichzeitig keine Gefahr eines Machtvakuums zu Gunsten einer politischen Richtung darstellen.
Es sollen nun zunächst die aktuellen Maßnahmen der deutschen Bundesregierung und der Europäischen Union gegen Desinformationskampagnen beleuchtet werden. Anschließend erfolgt die Vorstellung weiterführender Maßnahmen entsprechend der Empfehlungen des ISD.
Laut dem Staatssekretär Dr. Helmut Teichmann verfolgen die Maßnahmen der Bundesrepublik Deutschland das übergeordnete Ziel, die sachgerechte Durchführung der anstehenden Europa- und Bundestagswahlen zu gewährleisten (vgl. [39]). Die Europäische Kommission gibt dazu konkrete Initiativen zur Bekämpfung von Desinformation an (s. Kapitel 8.2 (2)). Auf Grundlage dieser Initiativen wurden in Deutschland eine Reihe von Maßnahmen umgesetzt. Diese umfassen 5 Schwerpunkte, welche nun kurz vorgestellt werden [40]:

1. *Desinformationen aufdecken und analysieren*

   Die einzelnen Ministerien und Behörden analysieren fortlaufend die Nachrichtenlage. Das Auswärtige Amt (AA) fokussiert sich auf Desinformationen als gezieltes Mittel fremder Staaten (z.B. Desinformationen über den russischen Angriffskrieg). Dabei erfolgt ein regelmäßiger Austausch mit internationalen Partnern

wie der EU. Das Bundesinnenministerium koordiniert den Umgang mit hybriden Bedrohungen. Hybride Bedrohungen umfassen in diesem Zusammenhang die Manipulation der öffentlichen Meinung durch online verbreitete Desinformation. Das Bundesamt für Verfassungsschutz (BfV) sammelt und wertet Informationen aus, sofern es eine Bedrohung der demokratischen Grundordnung vorliegt. Dazu gehören Cyberoperationen oder Propagandaaktivitäten anderer Staaten.

2. Koordiniert und entschlossen reagieren

Um Desinformationen wirksam zu stoppen, muss entschlossen und schnell gehandelt werden. Das BMI leitet dazu eine Taskforce, die aufgetretene Desinformationen verstärkt im Blick behält und andere Ministerien gegebenenfalls informiert. So wird sichergestellt, dass alle innerhalb der Bundesregierung informiert sind und entschlossen und schnell reagieren können, wenn es darum geht, Desinformationen zu entlarven und zu widerlegen.

3. Verbreitung von Desinformation bekämpfen

Desinformationen werden überwiegend in den sozialen Netzwerke geteilt. Es ist daher notwendig, die Plattformbetreiberinnen in die Verantwortung zu nehmen. Nur so kann gegen die Verbreitung von Desinformation vorgegangen werden. Das Netzwerkdurchsetzungsgesetz (NetzDG) verpflichtet die Betreiberinnen unter anderem, Beschwerden von Nutzerinnen und Nutzern schnell zu bearbeiten.

4. Phänomene erforschen

Um die Verbreitung von Desinformation nachvollziehen zu können, müssen die Entwicklungen Mechanismen dahinter verstanden werden. Die Wissenschaft erforscht daher kontinuierlich, wie sich Desinformationen verbreiten oder welche Techniken eingesetzt werden.

5. Bürgerinnen aufklären und sensibilisieren

Die Sicherheitsbehörden von Bund und Ländern werden verpflichtet, regelmäßig auf die bestehenden Cyberbedrohungen hinzuweisen. Dadurch soll eine zunehmende Sensibilisierung der Bevölkerung mit der Thematik erreicht werden. Dabei wird zunehmend auch auf die Berichterstattung seriöser Medien gebaut. Langfristiges Ziel ist es, die Medien und Nachrichtenkompetenz der Bürgerinnen zu stärken. In diesem Kontext fördert das Bundesministerium für Familie,

Senioren, Frauen und Jugend eine Vielzahl an Projekten, die zum Umgang mit Desinformation und Verschwörungstheorien aufklären.

Inwiefern die Maßnahmen der Bundesregierung wirksam sind, wird in der vorliegenden Arbeit nicht näher beurteilt. Betrachtet man allerdings die Empfehlungen der ISD, lassen sich Differenzen feststellen. Die ISD fordert generell weitreichendere Maßnahmen. Sie kritisiert fehlende Mechanismen im Umgang mit Falschnachrichten und fordert eine stärkere Selektion von Desinformationen durch die Plattformbetreiberinnen. Dabei muss nachhaltig sichergestellt werden, dass „die Verbreitung von rechtswidrigen und gefährlichen Inhalten eingedämmt wird“ (vgl. [40]). Plattformen sollten zukünftig dafür verantwortlich gemacht werden können, wenn sie nachweislich die Verbreitung von rechtswidrigen Inhalten, Desinformationen und anderen Bedrohungen für die Ausübung der Grundrechte nicht eindämmen. Grundlage dafür sollten „solide Definitionen bilden, die zur wirksamen Risikominderung führen“ (vgl. [41]). Dabei sollten auch alternative soziale Medien, wie Telegram zur Rechenschaft gezogen werden können, um digitale Gewalt und Desinformation zu bekämpfen. Weitreichende Sorgfaltspflichten sollten für alle sozialen Medien gelten, insbesondere im Wahlkontext. Umfassende Gesetze könnten etwa Lücken im Informationsrecht abbauen und umfassende Beratungsangebote schaffen. Die Wahrung der Kommunikationsfreiheit ist trotzdem in einem demokratischen System zu gewährleisten. Es könnten daher Nutzerrechte und Meldeverfahren gestärkt werden und zusätzlich die Wirkungsweise algorithmischer Systeme der sozialen Plattformen den Nutzerinnen erklärt und eventuell positiv verändert werden (vgl. [41]).
Zusammenfassend kann festgehalten werden, dass die Bekämpfung von Desinformationskampagnen aufwendig ist und ein hohes Maß an technologischem und sozialem Verständnis erfordert. Die schnelle technologische Entwicklung fordert flexible Maßnahmen bei der Bekämpfung von Fehlinformationen. Eine Flexibilität fehlt allerdings bei fest aufgestellten Regelwerken und Handlungsanweisungen. Es ist daher auf lange Sicht ein Umdenken erforderlich. Es gilt: Moderne, strategische Desinformationskampagnen können nicht wirksam mit veralteten Maßnahmen und Methoden bekämpft werden.

5 Die Präsidentschaftswahlen in der USA

5.1 Die US-Präsidentschaftswahl 2016

Donald Trump gegen Hillary Clinton: Die Wahl der US-Präsidentschaft in Jahr 2016 haben nicht nur Amerikanerinnen, sondern Menschen auf der ganzen Welt verfolgt. Immer wieder kamen neue Geheimnisse und Skandale zum Vorschein und machten die gesamte Wahl damit noch interessanter.
Nachfolgend erfolgt nun eine Erklärung des Wahlsystems der USA. Damit kann dann auf die Ergebnisse, welche die Wahl 2016 geprägt haben, eingegangen werden.
Das Wahlsystem der Staaten ist ein indirektes Wahlsystem. Das bedeutet, dass die Bürgerinnen der USA die eigentliche Wahl der Präsidentin nur indirekt beeinflussen. Die Bürgerinnen wählen das „Electoral College“, bestehend aus den insgesamt 538 Wahlmännern und -frauen. Dabei darf jeder Bundesstaat nur eine bestimmte Anzahl von Wahlfrauen entsenden. Das Electoral College wählt 41 Tage nach der Präsidentschaftswahl die Präsidentin. Welche Stimme die Wahlfrauen dann abgeben, ist dabei abhängig von der Wahl vorher. Alle Wahlfrauen eines Bundesstaates wählen die Kandidatin, welche die Mehrheit im Bundesstaat bekommen hat. Eine Ausnahme bilden hierbei nur die Staaten Nebraska und Maine. Dort werden hingegen die Stimmen proportional zum Ergebnis verteilt. Am Ende gewinnt der Kandidat, welcher mindestens 270 Stimmen des Electoral Colleges erhält (vgl. [42]). Aufgrund des fehlenden Melderegisters in der USA müssen sich die Bürgerinnen vor jeder Wahl registrieren lassen. Danach darf jede Bürgerin nur einmal in dem Bundesstaat wählen, in dem sie zu der Zeit wohnt, bzw. zuletzt gewohnt hat.
Bei der Präsidentschaftswahl 2016 traten die Kandidaten Hillary Clinton, Kandidatin der Demokraten, und Donald Trump, Kandidat der Republikaner, an. Die Wahl war insgesamt geprägt von zahlreichen Skandalen und Provokationen. Kleinste Information wurden ausgenutzt und für den eigenen Wahlkampf benutzt. Ein sehr bekanntes Beispiel, welches den wohl meisten im Gedächtnis geblieben ist, ist der E-Mail-Skandal von Hillary Clinton. Sie nutzte ein privates E-Mail-Konto für dienstliche Zwecke und löschte vor Übergabe 30.000 Mails. Der spätere Hackerangriff auf die Accounts der Demokraten, führte dazu, dass E-Mail-Verläufe über den Wahlkampf veröffentlicht wurden, was Clintons Ruf erheblich schadete (vgl. [43]). Auch die Gerüchte über mutmaßliches Mitwirken einer russischen Organisation blieb wohl vielen im Gedächtnis. Die Hackerangriffe, Desinformationskampagnen und Wahlmanipulationen konnten im Nachhinein auf russische Organisationen zurückgeführt werden. So konnte nachgewiesen werden, dass die Hackerinnen im Fall des E-Mail-Skandals von Clinton aus Russland kommen, die Website „Wikileaks“, auf der die E-Mails veröffentlicht wurden, einen russischen Ursprung besitzt und russische Bots die Desinformationskampagnen auf Twitter und

Google starteten. Auch gab es Gruppen im Internet, angefangen von „Black-Lives-Matter-Gruppen“, bis hin zu Gruppen, welche die „Alright-Bewegung“ unterstützten. Viele verschiedene Posts, wie Pro-Trump- und Contra-Clinton-Posts versuchten, die Bürgerinnen der USA in eine gewünschte Richtung zu lenken. Und nahezu alle Angriffe und Versuche die Wahl zu manipulieren fanden zugunsten Donald Trump statt (vgl. [44]).
Doch obwohl die Hackerangriffe und Wahlmanipulationen von den meisten stark verurteilt werden, ist es immer noch ein kontroverses Thema. Einerseits sind sie ein enormer Eingriff in die Privatsphäre eines Menschen und können dem politischen Ansehen erheblich schaden, andererseits sind sie aber eine Möglichkeit, die Wahrheit aufzudecken, die ohne Vorkommnisse nicht aufgedeckt werden könnten. Beispielsweise stellen die Hackingangriffe im Fall des E-Mail- Skandals einen enormen Eingriff in die Privatsphäre von Hillary Clinton dar. Durch Veröffentlichung der „E-Mail-Affäre“ entstand unter den Bürgerinnen eine enorme Verunsicherung, welche auch durch Rechtfertigungen und Erklärungen nur schwer wieder aufzuheben waren.
Es ist wichtig zu beachten, dass Hackerangriffe illegal sind und die Privatsphäre von Personen verletzen. Laut Strafgesetzbuch (StGB) Paragraph 202 Absatz d zur Datenhehlerei heißt es:

> [1](1) *Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.* [45]

Zudem ist es wichtig, dass die Menschen selbst bewerten und entscheiden können. Die Entscheidung, ob Hackerangriffe „gut“ oder „böse“ sind, hängt insgesamt von vielen verschiedenen Faktoren ab und ist schlussendlich eine Frage, die jeder Mensch für sich selbst entscheiden muss.

5.2 Die US-Präsidentschaftswahl 2020

Die US-Wahl 2020 verlief im Vergleich zur Wahl 2016 ruhiger und war weniger geprägt von Skandalen. Die Republikaner stellten erneut ihren Kandidaten Donald Trump und die Demokraten Joe Biden, welcher die Wahl am Ende für sich entscheiden konnte, auf. Allerdings kam das Land nach der Wahl in Aufruhr.

Nach der ersten Amtsperiode des US-Präsidenten Donald Trump kam es zu einem Angriff auf die Regierung in Washington D.C.. Am 6. Januar 2021 stürmten Anhängerinnen von Donald Trump das Kapitol in Washington, D.C. Diese Attacke wurde vom FBI und von vielen politischen Beobachterinnen als Teil eines Putschversuches von Trump gewertet. Das Ziel der Angreifer war es, den Senat und das Repräsentantenhaus an der förmlichen Bestätigung des Sieges von Joe Biden zu hindern und dem Republikaner Trump damit verfassungswidrig zur Fortsetzung seiner Präsidentschaft zu verhelfen. Nach einer aufstachelnden Rede von Trump, bei dem er seine Anhängerinnen nach Washington D.C. zum Demonstrieren aufrief, drangen schätzungsweise zwischen 800 und 1200 Anhängerinnen der Republikaner ins Kapitol ein und unterbrachen für mehrere Stunden die von Vizepräsident Mike Pence geleitete Sitzung beider Parlamentskammern. Als unmittelbare Folge der Ereignisse kamen fünf Menschen ums Leben und zahlreiche Personen wurden verletzt. Zuvor kam es zu einer Protestversammlung in der Nähe des Weißen Hauses. Trump, der zum „Save America March“ nach Washington D.C. gerufen hatte, behauptete in seiner Ansprache vor zehntausenden seiner Anhängerinnen wahrheitswidrig, seine Niederlage sei auf einen groß angelegten Wahlbetrug der Demokratischen Partei zurückzuführen. Das Votum des Electoral College, das die eigentliche Wahl der Präsidentin vornimmt, sei daher falsch und müsse zurückgewiesen werden. Um den Vizepräsidenten und den Kongress zu diesem verfassungswidrigen Schritt zu veranlassen, forderte er seine Unterstützerinnen schließlich auf, mit ihm zum Kapitol zu ziehen. Daraufhin stürmten kurz nach 14 Uhr zahlreiche gewalttätige Demonstrantinnen das Parlamentsgebäude. Die Abgeordneten und der Vizepräsident wurden in Sicherheit gebracht oder verbarrikadierten sich in Büros. Einige Randaliererinnen verschafften sich Zugang zum Sitzungssaal des Senats und zu den Abgeordnetenbüros. Sie attackierten Polizistinnen, richteten Zerstörungen an und stahlen Computer und andere Gegenstände. Die U.S. Capitol Police und die Bürgermeisterin von Washington D.C., Muriel Bowser, forderten beim US-Verteidigungsministerium Unterstützung durch die Nationalgarde. (vgl. [46])

Die Rolle der Desinformation bei der Ermutigung der Trump-Anhängerinnen, das Kapitol zu stürmen, darf demnach nicht unterschätzt werden. Falsche Behauptungen über Wahlbetrug und die Legitimität der Wahl haben dazu beigetragen, die Wut und den Zorn der Trump-Anhängerinnen zu erhöhen. Hieran ist zu sehen, wie viel die Verbreitung von Falschinformationen durch eine Person, wie Trump, bei seinen Unterstützerinnen bewirken kann und wie schnell diese ihm alles glauben. Natürlich trägt die Digitalisierung dazu bei, dass solche Informationen sich rasant verbreiten, weshalb sie

auch oft ein wirkungsvolles Mittel zum Vorteil von Personen des öffentlichen Lebens sein kann. Dies ist eine weitere Schattenseite des digitalen Zeitalters.

6 Wie ist die Situation in Deutschland ?

Schlagzeilen über Unregelmäßigkeiten bei Wahlen verbinden die Deutschen bislang meist mit Ländern wie Russland, Iran oder Nordkorea. Vor wenigen Jahren wäre es für die Wenigsten denkbar gewesen, eine Bundestagswahl in Frage zu stellen. Nachzählungen oder Nachprüfungen waren selten und begrenzten sich zumeist auf einzelne Wahlbezirke. Heute wissen wir, dass auch in Deutschland Unregelmäßigkeiten, die entweder auf Manipulationen oder auf systematische Schlamperei hindeuten, nicht kategorisch ausgeschlossen werden können (vgl. [47]). Man erinnere sich an die Bundestagswahl 2021 in der Hauptstadt Berlin. Lange Schlangen und Wartezeiten vor den Wahllokalen, falsche oder fehlende Stimmzettel, vorübergehende Schließung von Wahllokalen und mancherorts Stimmabgabe bis weit nach 18 Uhr. Im Nachhinein betitelte der Bundeswahlleiter diese chaotische Wahl als „komplettes systematisches Versagen der Wahlorganisation“ [48], welches bis heute seine Nachwirkungen zeigt und immer mehr undenkbare Schwächen des deutschen Wahlsystems offenbart.
Nachfolgend soll die Sicherheit einer möglichen Bundestagswahl in Deutschland, hinsichtlich Cyber-Angriffe und strukturierten Desinformationskampagnen, erörtert werden. Dabei wird zunächst auf verschiedene Meinungsumfragen eingegangen, um skizzenhaft ein Stimmungsbild der Bevölkerung zu erhalten. Danach werden auf Grundlage mehrerer Studien die Bundestagswahl 2021 und die Landtagswahl in Sachsen-Anhalt 2021 genauer betrachtet und der Einfluss von Desinformationen charakterisiert. Im Anschluss erfolgt eine Begutachtung der in großen Teilen Deutschlands verwendeten Wahlsoftware bezüglich den Aspekten Datenschutz und Manipulierbarkeit.

6.1 Meinungsumfragen

In den vergangenen Kapiteln wurden bereits zahlreiche digitale Strategien thematisiert, mit welchen es möglich ist, Wahlen systematisch zu beeinflussen. Trotz dessen werden Wahlen in Deutschland von einer Mehrheit der Bevölkerung als sicher wahrgenommen. Zu diesem Ergebnis kam das Meinungsforschungsinstitut INSA bei einer Umfrage im Sommer 2021, kurz vor der letzten Bundestagswahl (s. Kapitel 8.1 (3), [70]). Demnach sehen 56 Prozent der 2079 befragten Deutschen eine weitreichende Wahlfälschung als

unwahrscheinlich an, während lediglich 18% diese als wahrscheinlich einstuften.
Nach dem Grundgesetz müssen Wahlen in Deutschland allgemein, unmittelbar, frei, gleich und geheim sein (vgl. [49, Artikel 38, Absatz 1, Satz 1]). Inwiefern dies jedoch der Realität entspricht ist anzweifelbar. Nicht nur die Politik, sondern auch zahlreiche Medienhäuser berichteten im Vorfeld der Bundestagswahl 2021 gehäuft von Fake News-Kampagnen und Cyberangriffen. Es ist daher auch wenig verwunderlich, dass bei einer Umfrage der Wirtschaftsprüfungs- und Beratungsgesellschaft Pricewaterhouse Coopers (PwC) [50] im Vorfeld der Europawahl 2019 festgestellt wurde, dass die Mehrheit der Deutschen eine Beeinflussung der Wahl durch Falschinformationen für möglich hält. Dabei gaben 71 Prozent der 1000 befragten Deutschen an, bereits mit Falschinformationen in Kontakt gekommen zu sein. 50 Prozent schätzen die Gefahr einer Wahlmanipulation als „eher hoch“ ein, 21 Prozent sogar als „sehr hoch“. Weitet man diese Umfrage auf ganz Europa aus, zeigt sich ein noch drastischeres Bild, bei welchem über 80 Prozent in Fake News eine grundlegende Gefahr für die Demokratie sehen (vgl. [51]).

6.2 Desinformationsnarrative bei deutschen Wahlen

Angriffe auf Wahlen sind Angriffe auf das Herz einer Demokratie. In Kapitel 4 wurde bereits offenbart, dass auch vermeintlich stabile Demokratien gegenüber gezielten Desinformationskampagnen und digitalen Wahlkämpfen verwundbar sind. Weltweit sind digitale Gewalt, Hetze und die Verbreitung von Desinformationen zu einer besorgniserregenden Begleiterscheinung des politischen Alltags geworden. Besonders im Verlauf von Wahlkampagnen nehmen Manipulationsversuche erkennbar zu (vgl. [52]). Immer häufiger werden Politikerinnen Ziel systematischer Desinformationskampagnen und erhalten Hassnachrichten, Bedrohungen etc. in den sozialen Netzwerken.
Im Vorfeld der letzten Landtagswahlen und der Bundestagswahl 2021 sind Desinformationskampagnen ein zentrales Thema. Der Deutsche Bundestag und die Bundeswahlleiterin warnten eindringlich vor Desinformationen in den Social-Media-Kanälen. Zudem wurde versucht, mittels verschiedenen Informationswebseiten und Fernsehberichten, die Bevölkerung in dem Umgang mit Desinformationen zu sensibilisieren (vgl. [53]). Die Wirksamkeit dieser Maßnahmen, sind jedoch angesichts der folgenden Erkenntnisse zu der Bundestagswahl 2021 und der Landtagswahl 2021 in Sachsen-Anhalt im Nachhinein in Frage zu stellen.

6.2.1 Die Bundestagswahl 2021

Fake News kursieren in Deutschland vor allem in den sozialen Netzwerken. Diese ermöglichen es, Falschinformation in großen Rahmen zu verbreiten und somit eine Vielzahl von Menschen zu erreichen. Durch das mehrfache Teilen von fraglichen Inhalten wird es dem Benutzer erschwert, kleine Gerüchte von gezielter politischer Meinungsmache zu unterscheiden. Erschwerend kommt die Tatsache hinzu, dass sich Fake News in den sozialen Netzwerken etwa sechsmal schneller verbreiten als die Wahrheit (vgl. [54]).
Die Organisation AVAAZ hat bezüglich der Bundestagswahl 2021 eine Analyse mit über 900 Fact Checks zu Desinformationen und sozialen Medien durchgeführt (s. Kapitel 8.1 (4), [55]). Ziel dieser Analyse war es, den Umfang und die Formen von digitaler Gewalt, sowie der Verbreitung von Desinformationen gegen die deutschen Parteien und dessen Spitzenkandidatinnen zu untersuchen. Innerhalb der Studie wird als zentrales Ergebnis festgestellt, dass sich zwar ein großer Teil der Fehlinformationen auf das Coronavirus beziehen, jedoch vor der Bundestagswahl sprungartig die Desinformationsnarrative anstiegen, die auf deutsche Politikerinnen abzielen – oft aus dem Ausland. Dabei wurde erfasst, dass die Spitzenkandidatin der Grünen, Annalena Baerbock, am häufigsten Ziel von Fake News geworden ist. Durchschnittlich hat nach einer Umfrage der YouGov jeder zweite Erwachsene in Deutschland mindestens eine Falschnachricht über sie gesehen. Beispielposts mit nachweislichen Fehlinformationen befinden sich im Anhang unter dem Kapitel 8.1 (5). Von Falschnachrichten zu den Top 10 Politiker*innen betreffen alleine 28 Prozent Annalena Baerbock. Dahinter folgen mit deutlichem Abstand Altkanzlerin Angela Merkel mit 16 Prozent und Kanzlerkandidat Armin Laschet, beziehungsweise Markus Söder mit 11 Prozent (s. Kapitel 8.1 (5) Abb. 9, [55]). Betrachtet man nun die Politikerinnen unter dem Blickwinkel ihrer Parteizugehörigkeit wird in der Studie ersichtlich, dass vor allem die etablierten Parteien der Mitte Opfer von Desinformationskampagnen sind. Dabei richten sich die Desinformationsnarrative gegen die Parteien „Die Grünen“ (44 %), „CDU/CSU“ (36 %) und „SPD“ (17 %). Andere bekannte Parteien, wie etwa „Die Linke, AfD und FDP“ sind wiederum mit lediglich einem Prozent nur geringfügig betroffen (s. Kapitel 8.1 (5) Abb. 10, [55]).
Bei einer Bundestagswahl liegt ein besonderer Fokus auf den potenziellen Kanzlerkandidatinnen. Hier ergibt sich nach Analysen der AVAAZ ein unerwartetes Bild. Während 72 Prozent der Desinformationskampagnen auf Annalena Baerbock abzielen, richteten sich 0% gegen Olaf Scholz. Indessen ist der Spitzenkandidat von CDU/CSU, Armin Laschet, mit 28 Prozent auf den zweiten Platz. Das bedeutet, die von AVAAZ analy-

sierten Desinformationsnarrative betrafen in keinem nachgewiesenen Fall den späteren Kanzler Olaf Scholz (vgl. [55]). Dies kann man spekulativ zum Anlass nehmen, den uns bekannten Ausgang der Wahl zu hinterfragen. Inwiefern wäre die Bundestagswahl anders verlaufen ohne breit angelegte Desinformationskampagnen? Wäre Olaf Scholz heute trotzdem Bundeskanzler? Eine klare Beantwortung dieser hypothetischen Fragen ist zweifellos nicht möglich. Betrachtet man jedoch einige Zusammenhänge, ergibt sich ein neues Bild bezüglich der Bundestagswahl. Nach Ankündigung der Kanzlerkandidatur am 19. April 2021 wurde Annalena Baerbock deutlich häufiger zum Ziel der Angriffe mit Verschwörungstheorien (u.a „Great Reset“), Des- und Falschinformationen (s. Kapitel 8.1 (6) Abb. 15 „Great Reset“). Vor allem die Anspielung auf Verschwörungsmythen beschränkte sich nicht auf private Telegram-Kanäle, sondern auch vermehrt in den Sozialen Medien wie Facebook und Twitter (heute X). Unterdessen wurden Laschet und Scholz nachweißlich weniger Opfer etwaiger Kampagnen (vgl. [52]). Zudem wurde Baerbocks Kompetenz im Vergleich zu Laschet und Scholz stärker hinterfragt. So thematisierten annähernd ein Viertel der 100 meist gelesenen Posts zu den Kanzlerkandidatinnen eines Facebook-Datensatzes des ISD (Institute for Strategic Dialogue) Baerbocks vermeintliche Inkompetenz, verglichen mit sechs Posts bei Scholz und 11 bei Laschet (s. Kapitel 8.1 (5) Abb. 17,18). In diesem Zusammenhang ist auch ein geschlechterspezifischer Effekt festzustellen, das Geschlecht von Baerbock wurde annähernd 10-mal häufiger thematisiert als bei Laschet und Scholz. Ebenso ist ein starkes Ungleichgewicht von potentiell rechtswidrigen Inhalten erkennbar. Baerbock wurde zudem auf Facebook 15-mal häufiger als Scholz und 7,5-mal häufiger als Laschet als eine „Gefahr für Deutschland“ [52] dargestellt (s. Kapitel 8.1 (5) Abb. 15). Insgesamt kommt die Studie zu dem Schluss, dass sich die wichtigsten Desinformationsnarrative und Taktiken auf Annalena Baerbock und Armin Laschet beziehen (jeweils 4). Beispiele hierfür sind Desinformationen in Bezug auf die Covid-19-Pandemie oder, überwiegend bei Armin Laschet, die Verbreitung von verschiedenen Desinformationen über die Flutkatastrophe im Ahrtal. Scholz wiederum wird selten konkret mit bestimmten Narrativen verbunden, oftmals wird er nur nebenläufig erwähnt und stellt eine Randfigur dar. Ausnahme ist hier der Wirecard-Skandal, welcher im Wahlkampf nur eine untergeordnete Rolle spielt.

Insgesamt richtet sich nachweislich eine geringere Menge an Desinformationskampagnen gegen Olaf Scholz. (vgl. [52]) Dies lässt sich anhand verschiedener Umstände begründen, welche ihm somit einen Vorteil im Wahlkampf verschafft haben könnten. Scholz geriet erst spät in den Blickpunkt des Wahlkampfes. Betrachtet man die folgende

Grafik der Umfrageentwicklung der „Sonntagsfrage“ von INSA (siehe Abb. 3) lässt sich erkennen, dass die SPD untypisch kurzfristig vor der Wahl einen signifikanten Sprung bei den Umfragewerten erhielt. Zuvor standen die Parteien „CDU“ und „Die Grünen“ im Fokus des Wahlkampfes. Dadurch lässt sich auch eine mögliche Konzentration der Desinformationskampagnen auf diese Parteien und dessen Spitzenkandidaten begründen und damit auch ein möglicher Umfragerückgang erklären. Die SPD profitierte so zunehmend von der fehlerhaft zugesprochenen Rolle als Außenseiter im Wahlkampf. Der Wahlsieg der SPD mit dem Kanzlerkandidaten Olaf Scholz kann somit wahrscheinlich auf die verminderte Einflussnahme Dritter zurückgeführt werden.

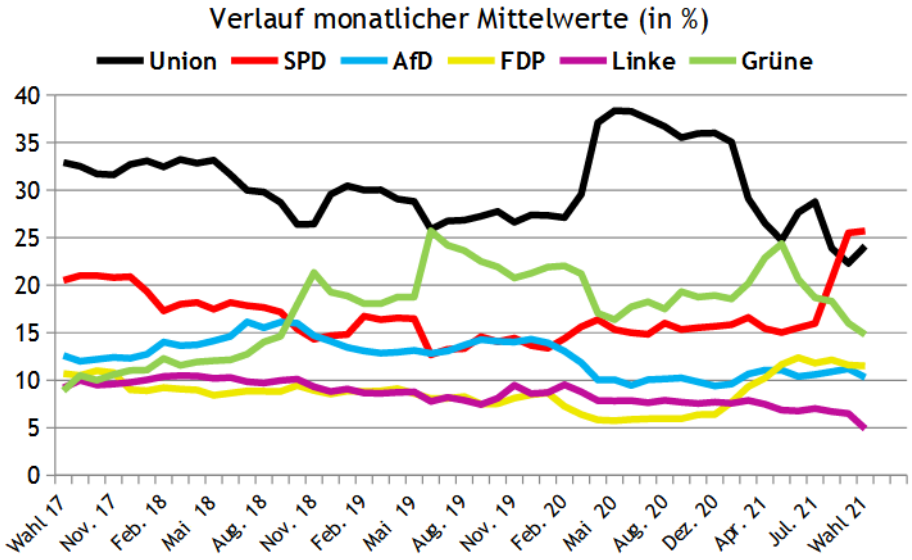

Abbildung 3: Verlauf der Umfragemittelwerte (2017 - 2021) [56]

Es soll anschließend beleuchtet werden, über welche konkreten Medien Falschnachrichten im Vorfeld der Bundestagswahl 2021 verbreitet wurden. Hier ergaben die Analysen von AVAAZ und ISD ein unerwartetes Ergebnis (s. Kapitel 8.1 (4) Abb. 12, [52], [55]). Fernsehen (22%) und Mainstream-Medien (18%) wie Zeitungen wurden als Top-Kanäle identifiziert, auf denen Falschinformationen gesehen wurden. Erst danach folgten mit 17 Prozent Facebook und andere soziale Medien (16%) wie Twitter, Instagram und YouTube. Dabei gilt: „Fernsehen und Mainstream Medien tragen zwar zu einem großen Teil zur Verbreitung der Falschnachrichten bei, deren Ursprung ist jedoch oft in den sozialen Medien auszumachen“ [55]. Ein mögliches Beispiel für diesen Prozess stellt das Desinformationsnarrativ dar, welches behauptet, Annalenna Baerbock würde das Ende der Haustierhaltung fordern. Zunächst als Facebook-Post veröffentlicht, verbreitete sich die Falschnachricht binnen weniger Tage auf den großen Sozialen Plattformen.

Dies führte anschließend dazu, dass auch zwei große deutsche Zeitungen (u.a Stuttgarter Zeitung) das Narrativ aufgriffen (vgl. [55]).
Betrachtet man abschließend die Parteipräsenz vor der Wahl innerhalb der sozialen Medien, lässt sich ein klares Muster erkennen. Die AfD ist mit 7,6 Millionen Interaktionen auf Partei- und Fraktionsseiten die mit Abstand aktivste Partei in Deutschland auf Facebook. Am anderen Ende des Spektrums konnten Die Grünen im gleichen Zeitraum lediglich 0,3 Millionen Interaktionen verzeichnen. Das bedeutet, die AfD-Seiten erreichen auf Facebook ungefähr 25-mal mehr Interaktionen als die Partei „Die Grünen“ (s. Kapitel 8.1 (5) Abb. 10, vgl. [55]). In diesem Zusammenhang stellte bei den letzten EU-Wahlen eine Studie der George Washington University (vgl. [57]) fest, dass unzählige dubiose Facebook-Accounts, deren Echtheit zweifelhaft ist, für die AfD werben. Diese Tatsache führt nahtlos über zu dem nachfolgendem Gliederungspunkt, bei welchem die Desinformationskampagnen gegen die Wahl in Sachsen-Anhalt thematisiert werden. Dort liegt insbesondere ein Augenmerk auf der Social-Media Kampagne der AfD.

6.2.2 Die Landtagswahl Sachsen-Anhalt 2021

Vor und nach der Landtagswahl in Sachsen-Anhalt verbreiteten sich unter Bloggern aus rechten Kreisen und dem Bereich der Verschwörungstheorien Behauptungen über vermeintlichen Wahlbetrug. So veröffentlichte etwa die Videobloggerin Miriam Hope während des Wahlkampfes ein Interview mit dem ehemaligen AfD-Landtagsabgeordneten Heinrich Fiechtner, in welchem behauptet wird, dass in Sachsen-Anhalt mit flächendeckendem Wahlbetrug zu rechnen ist (vgl. [58]). Dieses Video erreichte eine Vielzahl an Aufrufen (>100000). Es erscheint daher wenig verwunderlich, dass sich am Wahltag und in den darauffolgenden Wochen die vermeintlichen Berichte über Wahlbetrug häuften. So postete ein Twitter-Nutzer am Tag der Wahl ein Bild, auf welchem ein Wahllokal zu sehen war, mit der Botschaft, „er sei ein Wahlhelfer in Sachsen-Anhalt und darauf vorbereitet, AfD-Stimmen zu entwerten, um der Partei keine Chance zu geben“. Das Problem dabei ist, das Bild stammt aus den USA. Trotzdem wurde der Tweet hundertfach geteilt, unter anderem von mehreren AfD-Politikerinnen. Anhand dieses Beispiels wird beeindrucken aufgezeigt, was eine vermeintlich fehlerhafte Information für Auswirkungen auf ein demokratisches System haben kann. Nach den ersten Wahlhochrechnungen stiegen die Posts mit dem Hashtag #Wahlbetrug nahezu linear an. Insgesamt hatte der #Wahlbetrug allein auf Twitter eine prognostizierte Reichweite von circa 2,6 Millionen (vgl. [58]). Dies liegt an den Empfehlungsalgorithmen der

Sozialen Medien, welche die Reichweite entsprechender Beiträge exponentiell erhöhten. Verschiedene AfD-Anhängerinnen versuchten daraufhin eine Wiederholung der Wahl zu proklamieren, da nach ihrer Auffassung die Diskrepanz zwischen guten Umfragewerten vor der Wahl und tatsächlichen Wahlergebnissen nur mit einem umfangreichen Wahlbetrug erklärt werden können (s. Kapitel 8.1 (5) Abb. 19,200 ; vgl. [58]). Es folgte die Verbreitung verschiedener Verschwörungstheorien, wodurch die Reichweite auf ganz Deutschland ausgedehnt werden konnte und Sachsen-Anhalt vermeintlich als „Land der Wahlbetrüger“ [59] bezeichnet wurde. Dabei wird auf eine Reihe verzehrter Aussagen der Kommunalwahl im Stendal 2016 eingegangen, um ein „organisiertes CDU-Wahlbetrugssystem“ bestätigen zu können.
Der Bericht der Analysten von ISD offenbarte außerdem die versuchte Einflussnahme der staatlichen russischen Medien wie RT.de oder SNA. Diese fielen durch eine unkritische Berichterstattung gegenüber rechtsorientierten Parteien auf. So führte SNA vor der Wahl ein Interview mit dem AfD-Spitzenkandidaten Oliver Kirchner durch, während in einem Meinungsbeitrag auf RT.de eine sogenannte „Cancel Culture“ gegenüber der AfD scharf verurteilt wurde. (vgl. [58])

Insgesamt zeigen die Analysen der Bundestagswahl und der Landtagswahl in Sachsen-Anhalt, wie Meldungen in den sozialen Netzwerken über vermeintliche Betrugsversuche innerhalb kurzer Zeit durch Empfehlungsalgorithmen eine Vielzahl an Personen erreichen können. Damit kann geschlussfolgert werden, dass auch bei deutschen Wahlen digitaler Hass, Extremismus und Desinformation durch Algorithmen verstärkt werden. Somit besteht die Gefahr, dass auf längere Sicht das Vertrauen der Bürgerinnen in demokratische Prozesse und Institutionen zunehmend untergraben wird.

6.3 Cyberangriffe auf die Demokratie

In der Ära der Digitalisierung hat die technologische Vernetzung viele Aspekte unseres Lebens transformiert, darunter auch den demokratischen Prozess. Während digitale Technologien die Partizipation und Transparenz fördern können, bergen sie gleichzeitig Risiken, die unsere demokratischen Institutionen in Deutschland bedrohen. Insbesondere bei der Bundestagswahl 2021 steht die Problematik Cybersicherheit besonders im Blickpunkt. Der Chef des Bundesamts für Sicherheit, Arne Schönbohm, listete im Juli 2021 verschiedene mögliche Gefährdungsszenarien auf:

„Cyberstalking, Doxing, Störung, Sabotage, beispielsweise durch Verschlüsselungstroja-

ner, Identitätsdiebstahl, Datendiebstahl etc.“ [60]
Betrachtet man die Wahlen in Deutschland kann zunächst ein positiver Effekt hervorgehoben werden. Da der Wahlprozess immer noch analog mit Stift und Papier erfolgt, ist ein direkter Einfluss von außen auf das Wahlergebnis nicht möglich. Dies liegt ironischerweise daran, dass Deutschland bei der Thematik Digitalisierung lange zögerlich war (vgl. [60]). Dadurch werden nicht, wie in vielen anderen Ländern, Stimmen direkt am Computer abgegeben, welche oft Angriffspunkte für Cyberangriffe darstellen. Damit kann festgehalten werden, dass Störungen in einzelnen Bereichen organisiert und verursacht werden können, aber das Gesamtsystem widerstandsfähig ist.
Der Wahlprozess selber ist aber nur ein Aspekt der digitalen Wahlsicherheit. Fremde Einmischung gilt auch in Deutschland als Bedrohungsszenario. So könnten zum Beispiel Hacker Daten von Politikern erbeuten und diese veröffentlichen. Schon im Februar 2021 fand eine Phishing-Angriffswelle auf die Mitglieder des Bundestags, sowie der Landesparlamente statt. Damals haben die Angreifer versucht, mittels gefälschter E-Mails Daten zu stehlen, die sie dann bei einer bestimmten Gelegenheit gegen den Betroffenen einsetzen können. Betroffen waren laut Angaben der Bundesregierung eine niedrige dreistellige Zahl von Abgeordneten. Größere Schäden konnten dabei noch vermieden werden (vgl. [61]).
Betrachtet man die Gesamtbevölkerung, wurde bereits im Oktober 2020 auf der Homepage des Bundesamts für die Sicherheit der Informationstechnik (BSI) [62] vor dem, durch die Pandemie erzwungenen „Digitalisierungsschub in Deutschland“ gewarnt. Bei diesem werden oft die Punkte IT- und Datensicherheit nachrangig behandelt. Dadurch besteht die Gefahr, dass von Dritten, wie ausländischen Staaten Cyber-Angriffe mit Schadsoftware effektiv durchgeführt und Millionen von Daten gestohlen werden können. Auch wenn die vermeintliche Einflussnahme anderer Staaten und deren Nachrichtendienste noch auf einem im Vergleich zu den USA niedrigen Niveau sind, ist davon auszugehen, dass die Zahl der Angriffe in den nächsten Jahren systematisch weiter steigt (vgl. [63], [64]). Es ist daher wichtig, die Themen IT- und Cyber-Sicherheit weiter in den Fokus aller Bürgerinnen zu rücken.

6.4 Sicherheitslücken bei der Wahlsoftware PC-Wahl

Eine weitere mögliche Gefahr bei deutschen Wahlen stellt die Manipulation der verwendeten Wahlsoftware dar. Auch wenn die Bundestagswahlen, Landtagswahlen und Europawahlen händisch ausgezählt werden, müssen die Einzelergebnisse in den ein-

zelnen Bundesländern mit verschiedenen Wahlsoftwares zusammengerechnet und weitergegeben werden. Dabei ist Software von unterschiedlichen Herstellern im Einsatz. Jede einzelne der rund 11000 Gemeinden in Deutschland darf dabei selbst entscheiden, welche Software sie verwenden möchten, um ihre Ergebnisse der Kreiswahlleitung zu übermitteln. Als Ergebnis dieses Prozesses hat heute niemand mehr einen Überblick, an welcher Stelle welches Programm eingesetzt wird. Eine zentral einsehbare Übersicht darüber gibt es nicht, das sagt zumindest der Bundeswahlleiter. Man gehe jedoch davon aus, dass im Moment 13 verschiedene Wahlsoftwares in Deutschland im Umlauf sind, darunter auch Eigensoftware der Statistischen Landesämter. Nun schließt sich natürlich die Frage an, ob man bei dieser unübersichtlichen Sachlage davon ausgehen kann, dass jede der verwendeten Wahlsoftware sicher vor Angriffen von außen geschützt ist. Um diese Frage zu beantworten wird exemplarisch die Software „PC-Wahl“ als eine der meistverwendeten Wahlsoftwares in Deutschland genauer betrachtet. Wie die Wochenzeitung Zeit berichtet [65], besitzt diese Software massive Schwachstellen. Der IT-Wissenschaftler Martin Tschirsich hat zum Beispiel herausgefunden, dass Angreifer die Software vergleichsweise einfach manipulieren können. Dies bestätigt auch der CCC (Chaos Computer Club), welcher die Software ausführlich getestet hat und zu dem Ergebnis kommt, dass „grundlegende Prinzipien von Sicherheit und Verschlüsselung [...] ignoriert werden“ [65]. Schon vor der Wahl 2017, also mittlerweile vor mehr als sechs Jahren wurde die Software PC-Wahl als unsicher eingestuft. Doch auch noch heute verwenden einige Bundesländer die in die Jahre gekommene Software.
Besucht man die Webseite des Anbieters sieht man graue, kantige Menüpunkte und in der Ecke dreht sich ein Tortendiagramm (s. Kapitel 8.2 (3)). Hier ist die Rede von Disketten und der Partei PDS. Glaubt man den Aussagen des CCC, ist auch der Code selbst altbacken (Stand der Technik vor 30 Jahren). Zudem stieß Martin Tschirsich mit etwas Recherche im Internet auf Teile der Bedienungsanleitungen und Passwörter (vgl. [65]). Der Chaos Computer Club fand so einen potenziellen Weg, wie ein Angreifer den Nutzern von PC-Wahl eine gefälschte neue Programmversion unterjubeln könnte. Sogar die Dateien, welche Wählerstimmen enthalten, sind nicht nochmals gesichert. Wenn die Software diese Dateien an die Wahlleiter verschickt, gibt es keine Authentifizierung, keine Signatur und keinen individuellen Schlüssel. Es gibt kein System, das beweist, dass die korrekten Wahldaten der richtigen Gemeinde beim Wahlleiter ankommen. Somit ist es problemlos möglich, diese Wahldateien zu fälschen. Es wäre eventuell sogar eine flächendeckende Manipulation möglich. Man muss an dieser Stelle allerdings betonen, dass das amtliche Endergebnis mittels Wahlzettel und Wahlniederschriften

ermittelt und somit nicht technisch beeinflusst werden kann. Eine Manipulierung der vorläufigen Ergebnisse am Wahlabend ist allerdings möglich. Bei einer solchen Manipulation würde Deutschland zwei bis drei Wochen mit einem falschen Wahlergebnis planen. Gerade in Zeiten von Fake News und gesteigerter Aufmerksamkeit für Verschwörungstheorien wäre das fatal. Bürger und Bürgerinnen könnten das Vertrauen in die politischen Prozesse und in den Wahlprozess verlieren oder beides stark in Zweifel ziehen (vgl. [65]).
Zusammenfassend kann festgehalten werden, dass eine regelmäßige Überprüfung und Aktualisierung der einzelnen Wahlsoftwares dringend erforderlich ist, um die notwendige Sicherheit zu gewährleisten. Eine Vereinheitlichung der Software auf Bundes- oder zumindest Länderebene ist außerdem wünschenswert. Dringend sollten veraltete Programme wie „PC-Wahl“ abgeschafft werden und durch qualifizierte Neue ersetzt werden. Alle Daten, die von der Wahlsoftware verarbeitet werden, sollten stark verschlüsselt sein, um unbefugten Zugriff zu verhindern. Die Wahlsoftware sollte Mechanismen zur Zugriffskontrolle und starke Authentifizierungsmethoden umfassen, um sicherzustellen, dass nur autorisierte Personen Zugriff auf das System haben. Es sollten mehrstufige Authentifizierungsverfahren und starke Passwortrichtlinien implementiert werden. Die Personen, die mit der Wahlsoftware arbeiten, sollten regelmäßig geschult und sensibilisiert werden, um sich der Risiken bewusst zu sein und bewährte Sicherheitspraktiken anzuwenden. Es ist verwunderlich, dass es noch keine nachweislichen Versuche gab, die Wahlhochrechnungen zu manipulieren und damit die Angriffsfläche zu bieten, die Integrität einer Wahl infrage zu stellen.

6.5 Ausblick

Digitale Gewalt und die Verbreitung von Desinformationen begleiten zunehmend den Wahlkampf in Deutschland. Vor allem die etablierten Parteien sehen sich Angriffen ausgesetzt. Desinformationen erreichen durch die Empfehlungsalgorithmen der Sozialen Medien eine immer größere Reichweite.
Der Fokus des 2017 in Kraft getretenen Netzwerkdurchsetzungsgesetz (NetzDG) [66] liegt, Stand jetzt, nur auf der Bekämpfung rechtswidriger Inhalte. Verschwörungsmythen und Desinformation umfasst das Gesetz nicht, sodass diese weiterhin in den sozialen Netzwerken ohne rechtliche Konsequenzen für die Plattformen eine große Reichweite generieren dürfen (vgl. [67]). Zudem müssen die Plattformen nur nach Meldung von illegalen Inhalten dagegen vorgehen („Notice and take down-Verfahren“).

Aufgrund der fehlenden Regulierungsmaßnahmen und entsprechenden Konsequenzen ist auch in der nahen Zukunft mit einer Zunahme von digitaler Gewalt und Desinformationskampagnen zu rechnen. Insbesondere der Versuch der Einflussnahme durch andere Staaten wie Russland scheint aufgrund des Ukraine-Konflikts als sehr wahrscheinlich. Dies stellt ein systematisches Risiko für die Integrität der Demokratie dar, insbesondere im Vorfeld einer Wahl. Die Analysen von AVAAZ und ISD ([41], [52], [55], [58]) haben offenbart, dass die bisherigen Maßnahmen zum Schutz der Wahlen in Deutschland unzureichend sind. Alle politischen Institutionen, sowie die Bevölkerung sollten daher ein Interesse daran haben, die Verbreitung von Fehlinformationen einzudämmen und das politische Klima nachhaltig zu verbessern. Grundsätzlich sollte unter Wahrung der Meinungsfreiheit gelten: „Hass ist keine Meinung und ein problematisches, nicht probates, Mittel im Ringen um öffentliche Zustimmung“ [52].
Dass die Bundestagswahl 2021 ohne größere Zwischenfälle und Störungen verlief, ist im Nachhinein verwunderlich. Dies zeigt, dass die Bevölkerung weiterhin ein hohes Maß an Vertrauen in die traditionellen Medien besitzt und eine gewisse Widerstandsfähigkeit gegenüber Desinformation aufweist. Trotzdem ist es erforderlich, den aufkeimenden Vertrauensverlust in demokratische Prozesse mit den in Kapitel 4.4 vorgestellten Maßnahmen entgegen zu wirken. Eine funktionierende Demokratie ist auf einen deliberativen und faktenbasierten öffentlichen Diskurs angewiesen.

7 Fazit

In der vorliegenden Arbeit wird deutlich, dass die Digitalisierung nicht nur Chancen, sondern auch Risiken für unsere Demokratien birgt. Es wurde gezeigt, dass die Manipulation von Netzwerken und Computern nicht nur die Wahlentscheidungen der Bürgerinnen beeinflusst, sondern auch das Vertrauen in politische Institutionen und Prozesse. Zudem wurde dargestellt, dass solche Manipulationen nicht immer leicht zu erkennen und zu bekämpfen sind, da sie oft verdeckt und gezielt durchgeführt werden. Aus diesen Gründen ist es, nach unserer persönlichen Meinung, wichtig, dass die Bürgerinnen sensibilisiert und im Bereich der Digitalisierung stärker gebildet werden, um so die Gefahren und Anzeichen von Wahlmanipulation durch Hacking und Desinformationen besser zu erkennen. Um dies zu realisieren, ist es von entscheidender Bedeutung, dass die Informatik als Pflichtfach in Schulen eingeführt wird. Weiterhin ist es wichtig, dass die Menschen einen kritischeren Blick auf Informationen werfen und diese auf Glaubwürdigkeit und Plausibilität prüfen. Auch sollten wir unsere eigenen Meinungen

und Standpunkte hinterfragen und uns nicht von emotionalen Posts oder Aufrufen beeinflussen lassen. Natürlich ist es außerdem notwendig, dass die IT-Infrastruktur von Parteien und öffentlichen Institutionen stärker gesichert werden. Sie sollten regelmäßig auf Schwachstellen und Angriffe überprüft und aktualisiert werden. Wenn diese Sicherung transparent und nachvollziehbar gestaltet wird, kann das Vertrauen der Bürgerinnen nachhaltig gestärkt werden. Die Förderung und Unterstützung einer vielfältigen und unabhängigen Medienlandschaft, die eine qualitativ hochwertige und ausgewogene Berichterstattung über die Wahlen bietet, spielt weiterhin eine wichtige Rolle.
Damit bleibt festzuhalten, dass der Schutz vor Hacking und Desinformationen nicht nur technologische Lösungen erfordert, sondern auch eine kritische Auseinandersetzung mit den gesellschaftlichen Auswirkungen der digitalen Transformation. Eine informatische Grundbildung kann hierbei eine entscheidende Schlüsselrolle spielen, um vor allem die jungen Bürgerinnen zu befähigen, die heutigen Herausforderungen der digitalen Demokratie aktiv mitzugestalten und zu schützen. Denn Demokratie ist keine Selbstverständlichkeit, sondern eine Aufgabe, an der wir jeden Tag arbeiten müssen.

8 Anhang

8.1 Statistiken, Studien und Umfragen

(1) Marktanteile von Social-Media-Portalen in Deutschland

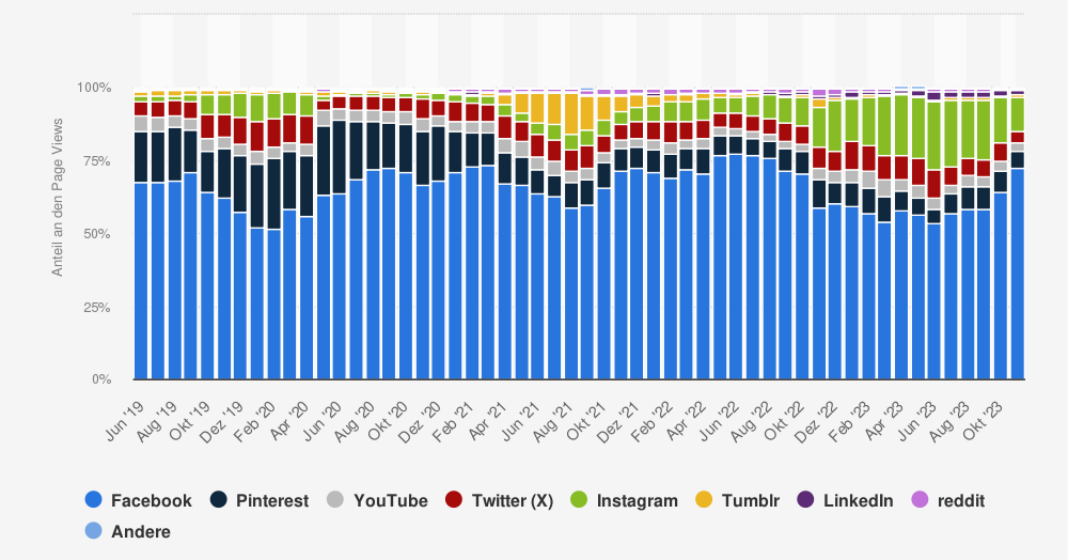

Abbildung 4: Marktanteile von Social-Media-Seiten in Deutschland [24]

(2) Cambridge Analytica (Facebook-Skandal)

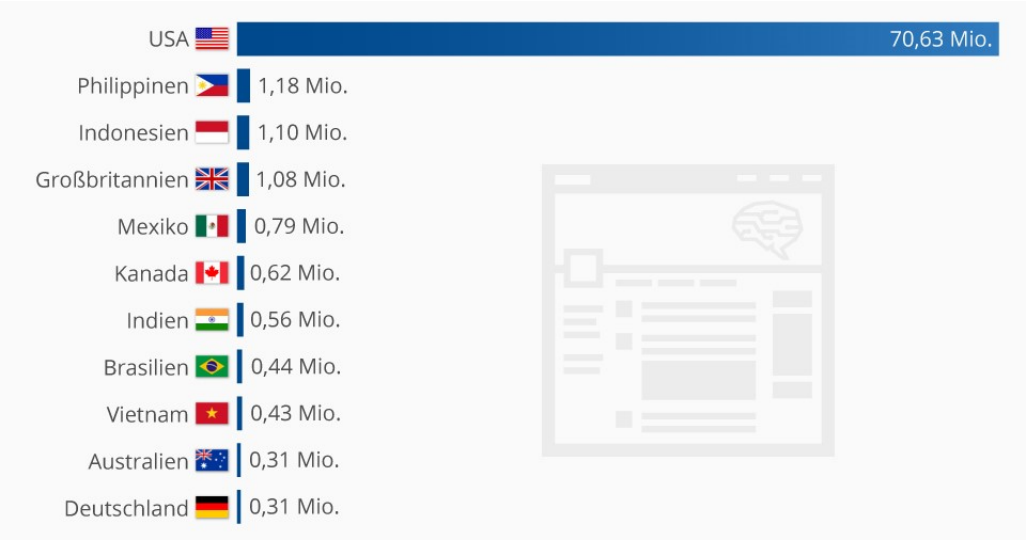

Abbildung 5: Anzahl der Profile die von Cambridge Analytica genutzt wurden [37]

(3) Meinungsumfrage der INSA im Vorfeld der Bundestagswahl 2021

Abbildung 6: INSA Meinungsumfrage bezüglich Wahlmanipulation [70]

Abbildung 7: Abb. 6 sortiert nach Schulabschluss [70]

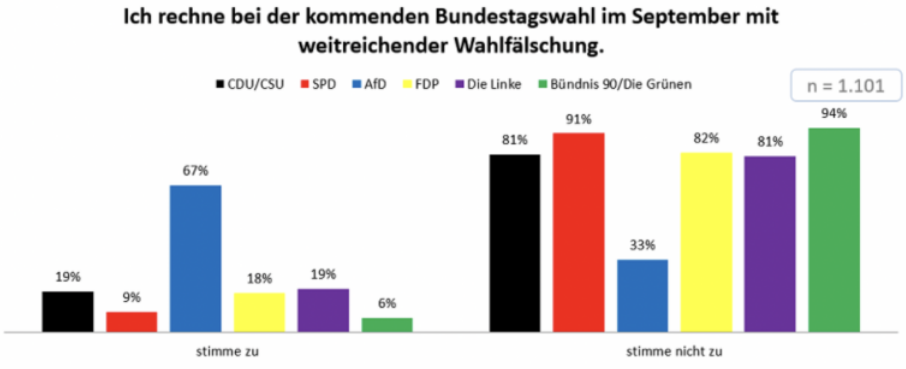

Abbildung 8: Abb. 6 sortiert nach Parteisympathie der Befragten [70]

(4) AVAAZ: Analyse zu Desinformation und sozialen Medien

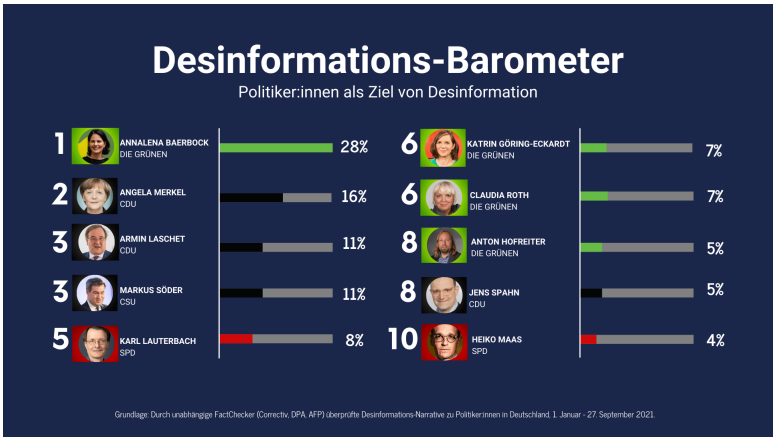

Abbildung 9: Politikerinnen als Ziel von Desinformationskampagnen [55]

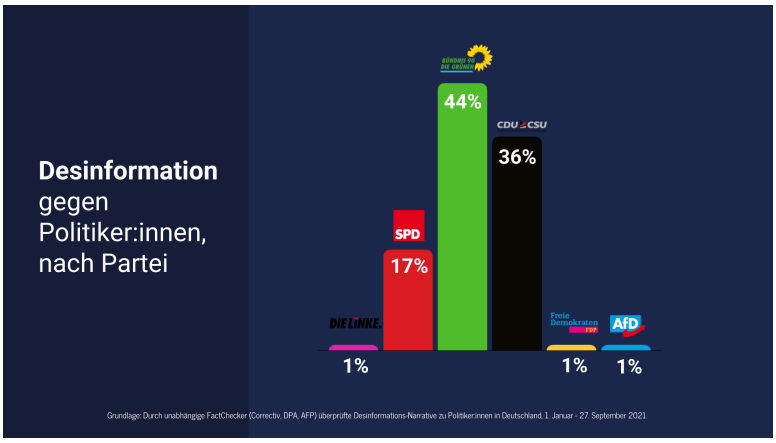

Abbildung 10: Desinformationskampagnen gegen Politikerinnen nach Partei [55]

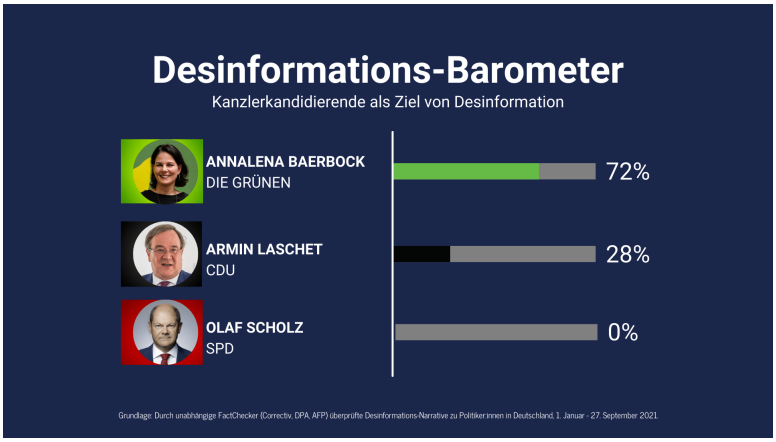

Abbildung 11: Desinformationskampagnen gegen die Kanzlerkandidatinnen 2021 [55]

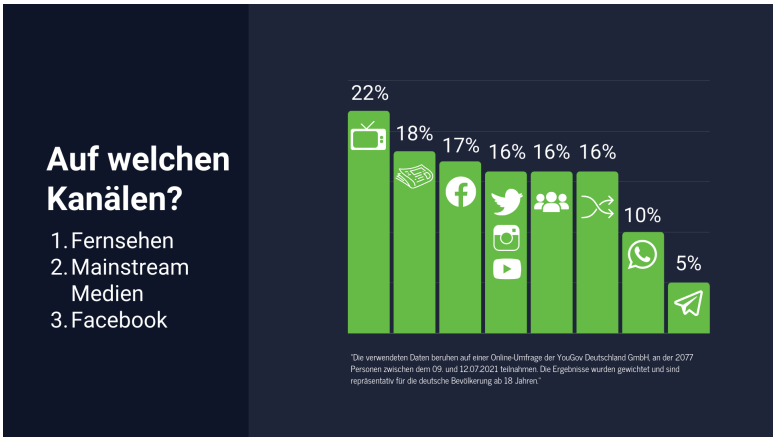

Abbildung 12: Kanäle, über welche Falschnachrichten verbreitet werden [55]

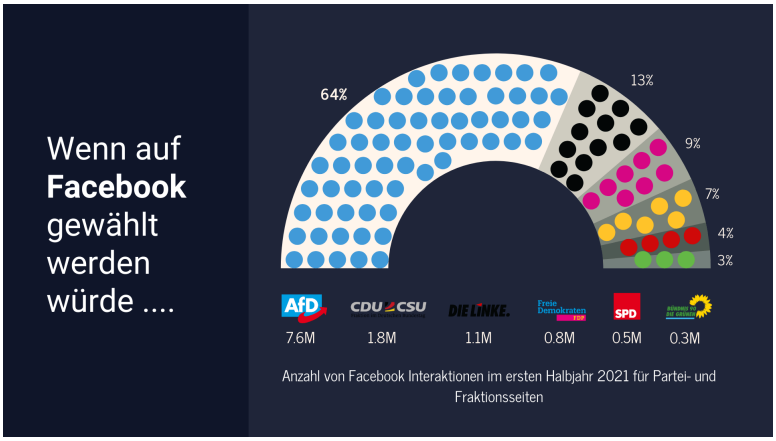

Abbildung 13: Parteipräsenz vor der Wahl in den sozialen Medien [55]

(5) Beispiele für Desinformationsnarrative gegen Politikerinnen

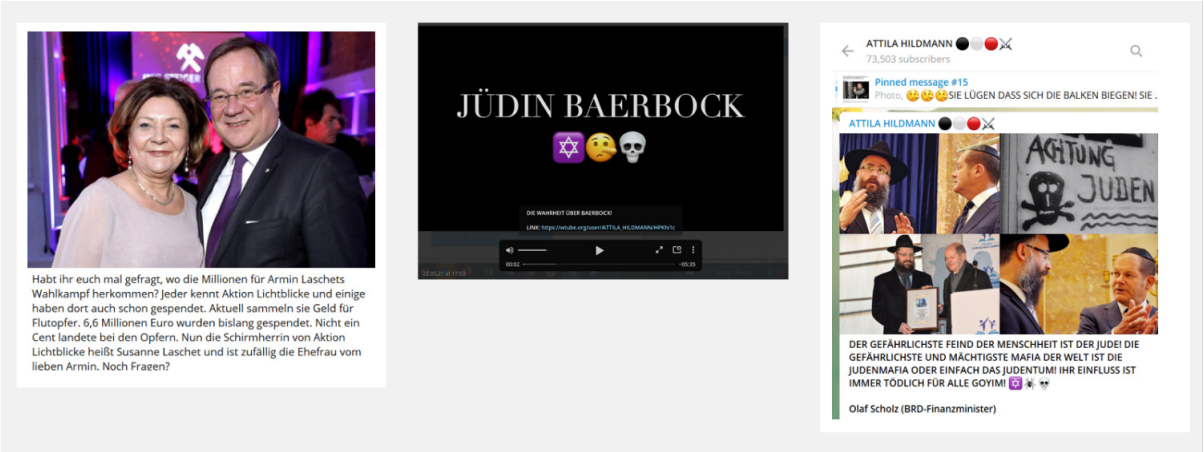

Abbildung 14: Beispiele für rechtsextreme Posts gegen Politikerinnen [52]

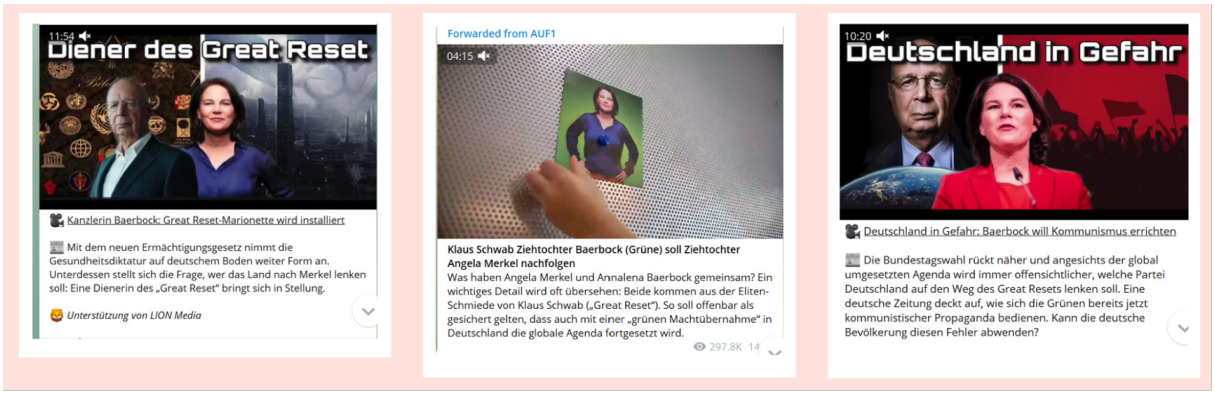

Abbildung 15: Beispiele für Falschnachrichten mit Bezug zu Verschwörungsmythen [52]

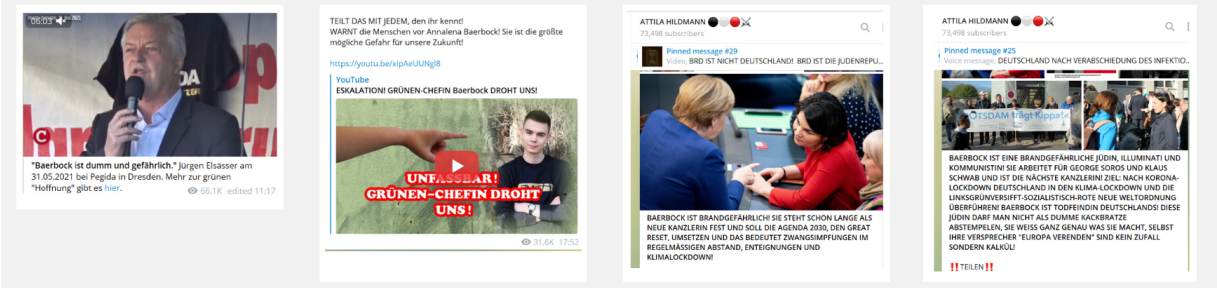

Abbildung 16: Beispiele für Desinformationsnarrative gegen Baerbock [52]

Abbildung 17: Beispiele für Desinformationsnarrative gegen Baerbock (2) [55]

Abbildung 18: Beispiele für Desinformationsnarrative gegen Baerbock (3) [55]

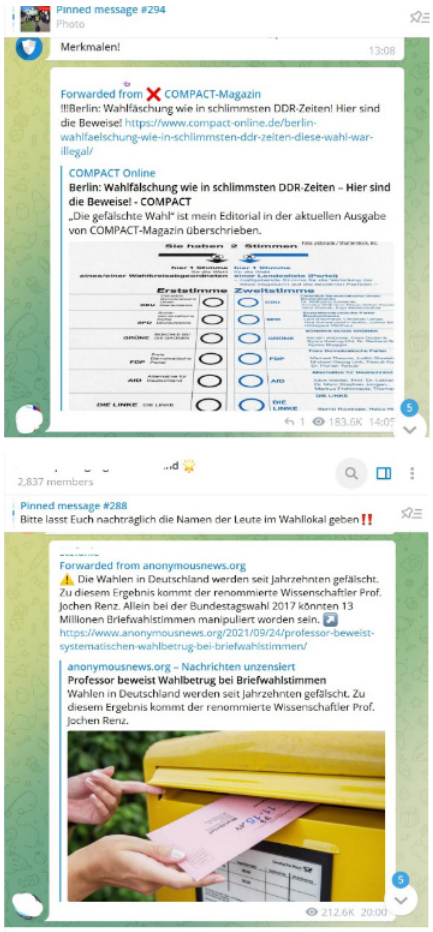

Abbildung 19: Fehlinformationen über die Briefwahl [41]

Abbildung 20: AfD-Wahlplakat zur Briefwahl [41]

8.2 Sonstiges

(1) Das Fünf Faktoren-Modell der Psychologie

Abbildung 21: Fünf-Faktoren-Modell [68]

(2) Die strategischen Säulen des EU-Aktionsplans gegen Desinformation

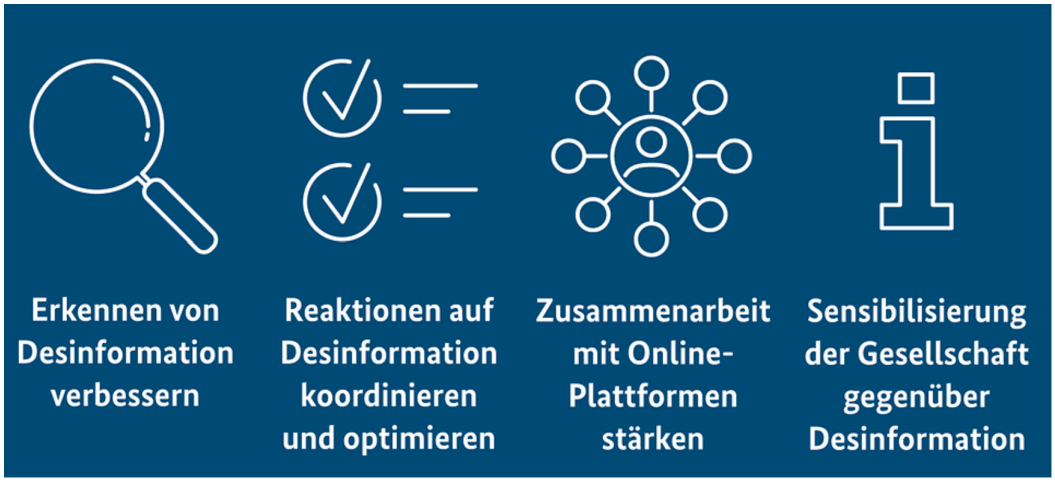

Abbildung 22: EU Aktionsplan gegen Desinformation [69]

(3) Zurück in die Zukunft: Die PC-Wahl Wahlsoftware

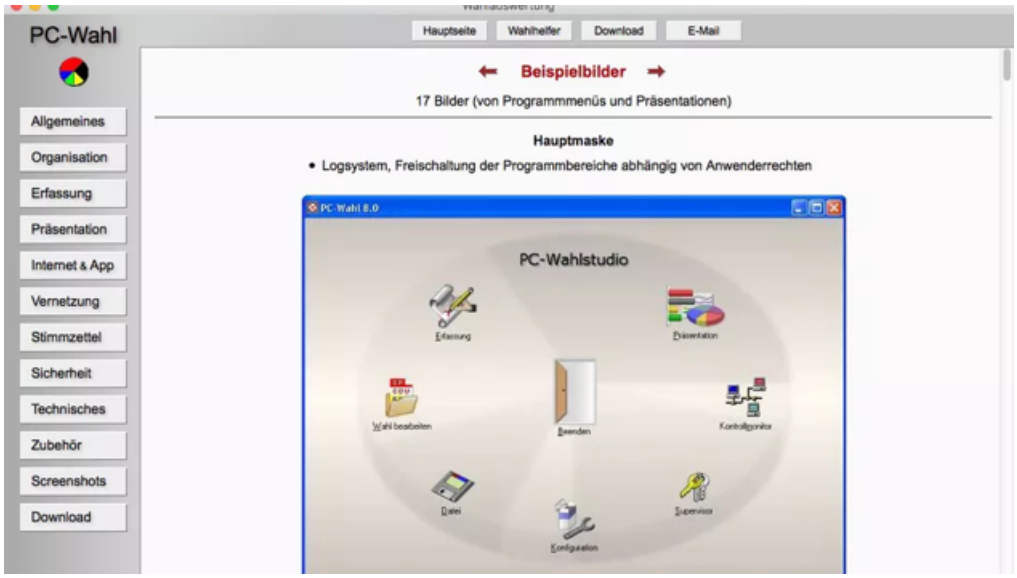

Abbildung 23: Webseite des Anbieters der Wahlsoftware PC-Wahl (Stand: 23.5.2023)

Literatur

[1] Zimmernann, Till. Die Wahlfälschung (§§ 107a f. StGB) im Gefüge des strafrechtlichen Schutzes der Volkssouveränität. ZIS, Heft 12, 2011, S.982.

[2] Krennerich, M. Freie und Faire Wahlen? Standards, Kurioses, Manipulation. WOCHENSCHAU Verlag, 2. Auflage, 2021

[3] StGB (Strafgesetzbuch). Bundesministerium der Justiz, aufgerufen unter: `https://www.gesetze-im-internet.de/stgb/`, am 22.12.2023

[4] Moes,T. Was ist Hacking? Die 10 schlimmsten Beispiele aller Zeiten. 2023, aufgerufen unter: `https://softwarelab.org/de/blog/was-ist-hacking/`, am 23.12.2023

[5] Dahmer, R. IT-Sicherheitsbedrohung: Sicherheitslücken und Schwachstellen. Dr.Datenschutz. 31.03.2023, Aufgerufen unter: `https://www.dr-datenschutz.de/it-sicherheitsbedrohungsicherheitsluecken-und-schwachstellen/`, am 23.12.2023

[6] Belcic,I. Was ist Hacking?. Avast. 09.02.2022, Aufgerufen unter: `https://www.avast.com/de-de/c-hacker`, am 23.12.2023

[7] Kaspersky. Definition und Erläuterung: Black Hat-, White Hat- u. Grey Hat-Hacker. AO Kaspersky Lab, Aufgerufen unter: `https://www.kaspersky.de/resource-center/definitions/hacker-hat-types`, am 23.12.2023

[8] Bundesamt für Verfassungsschutz. Akteure und Angriffsmethoden. Aufgerufen unter: `https://www.verfassungsschutz.de/DE/service/impressum/impressum\_node.html`, am 27.12.23

[9] Kaspersky. Was ist ein Honeypot?. AO Kaspersky Lab, aufgerufen unter: `https:www.kaspersky.de/resource-center/threats/what-is-a-honeypot`, am 28.12.23

[10] IBM. What is penetration testing?. Aufgerufen unter: `https://www.ibm.com/topics/penetrationtesting`, am 28.12.23

[11] K., Schwarz. Wahlmanipulation: Diese Schutzmaßnahmen treffen Internetkonzerne. Bundeszentrale für politische Bildung. 02.05.2019, aufgerufen unter: https://www.bpb.de/themen/medien-journalismus/digitale-desinformation/290577/wahlmanipulation-diese-schutzmassnahmen-treffen-internetkonzerne/, am 23.12.2023

[12] Bundesamt für Sicherheit in der Informationstechnik. Exkurs: Social Bots und Chatbots. Aufgerufen unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Soziale-Netzwerke/Sichere-Verwendung/Exkurs-bots/social-bots.html, am 28.12.23

[13] Bundesamt für Sicherheit in der Informationstechnik. Deepfakes - Gefahren und Gegenmaßnahmen. Aufgerufen unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html, am 28.12.23

[14] BBC. Deepfakes - Fake Trump arrest photos: How to spot an AI-generated image. Aufgerufen unter: https://www.bbc.com/news/world-us-canada-65069316, am 30.12.23

[15] Falles, Don. What Is Disinformation?. Libary Trends, Johns Hopkins University Press, Volume 63, Number 3. 2015 , S.401-426.

[16] Deutscher Bundestag. Desinformationskampagnen – Erkenntnisse und Maßnahmen der Bundesregierung. Drucksache 19/17073. 2020. Aufgerufen unter: https://dserver.bundestag.de/btd/19/170/1917073.pdf, am 23.12.2023

[17] J.-B. Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera. Information Manipulation: A Challenge for Our Democracies, report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August 2018

[18] Bounegru, L.; Gray, J.; Venturini, T.; Mauri, M. A Field Guide to Fake News: A Collection of Recipes for Those Who Love to Cook with Digital Methods (Chapters 1-3) (April 7, 2017). Public Data Lab, Research Report, 2017, Available at SSRN: https://ssrn.com/abstract=3024202

[19] Gelfert, Axel. Fake News: A Definition. Informal Logic 38 (1), 2018. S. 84-117.

[20] Jackson, D. Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation, and "Fake News". National Endowment for Democracy, 2017. https://www.ned.org/wp-content/uploads/2018/06/Distinguishing-Disinformation-from-Propaganda.pdf

[21] Wardle, C.; Derakshan, H. Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe. Council of Europe, 2017

[22] Heil, Karl M. Kollektive Strategien zur Abwehr digitaler Desinformation. Resilienz und Abschreckung bei EU und NATO. Studylab, 1. Edition, 2021

[23] Obar, J.A. and Wildman, S. Social media definition and the governance challenge. An introduction to the special issue. Telecommunications Policy, 39(9), 2015, 745-750.

[24] Lohmeier, L. Marktanteile von Social-Media-Portalen in Deutschland von April 2019 bis November 2023. Statista, 2023. Aufgerufen unter: https://de.statista.com/statistik/daten/studie/559470/umfrage/marktanteile-von-social-media-seiten-in-deutschland/, am 30.12.2023

[25] Jost, J.T.; Barberá, P.; Bonneau, R.; Linger, M.; Metzger, M.; Nagler, J.; Sterling, J. and Tucker, J.A.. How Social Media Facilitates Political Protest: Information, Motivation, and Social Networks. Political Psychology, 2018, 39: 85-118. https://doi.org/10.1111/pops.12478

[26] Tandoc, E.; Lim, Z.; Ling, R. Defining "Fake News": A typology of scholarly definitions. Digital Journalism. 2017. 1-17. 10.1080/21670811.2017.1360143.

[27] Oliveira, Astrid P. Der Erfolg gefälschter Nachrichtenportale. Deutsche Welle, 2022. Aufgerufen unter: https://www.dw.com/de/fake-news-der-erfolg-gef%C3%A4lschter-nachrichtenportale/a-63002129, am 20.12.2023

[28] Klein, O. Pro-russische Propaganda. Massenweise falsche News-Seiten enttarnt. zdfheute, 2022. Aufgerufen unter: https://www.zdf.de/nachrichten/politik/desinformation-kampagne-facebook-ukraine-krieg-russland-100.html, am 20.12.2023

[29] Wardle, C. First draft's essential guide to understanding information disorder. 1.Auflage, 2019

[30] Seemann, M. Digitaler Tribalismus und Fake News. 2017. Abgerufen unter http://www.ctrl-verlust.net/digitaler-tribalismus-und-fake-news/, am 21.12.2023

[31] Hwang, T. Digitale Desinformation. Grundlagen. Konrad-Adenauer-Stiftung e.V. 2017

[32] Ganguly, M. 'Aims': the software for hire that can control 30,000 fake online profiles. The Guardian, 2023. Aufgerufen unter: https://www.theguardian.com/world/2023/feb/15/aims-software-avatars-team-jorge-disinformation-fake-profiles, am 23.12.2023

[33] Christo, B,; Höfner, R.; Hoppenstedt, M.; Lehberger, R.; Niedermeier, N; Obermaier, F; Obermayer, B.; Rosenbach, M. Desinformationsfirma aus Israel. Team Jorge. Wahlmanipulation auf Bestellung?. zdfheute. 2023. Aufgerufen unter: https://www.zdf.de/nachrichten/politik/team-jorge-israel-desinformation-wahlen-100.html, am 26.12.2023

[34] Kirchgaessner, S. How undercover reporters caught 'Team Jorge' disinformation operatives on camera. 2023. Aufgerufen unter: https://www.theguardian.com/world/2023/feb/15/disinformation-hacking-operative-team-jorge-tal-hanan, am 23.12.2023

[35] Cadwalladr, C; Kirchgaessner, S. Revealed: the US adviser who tried to swing Nigeria's 2015 election. The Guardian. 2023. Aufgerufen unter: https://www.theguardian.com/world/2023/feb/18/cambridge-analytica-staff-leaked-emails-team-jorge-nigeria-/election-sam-patten-tal-hanan, am 23.12.2023

[36] SpiegelOnline. Cambridge-Analytica-Skandal Facebook vor Einigung im Prozess wegen Datenmissbrauchs. 2022. Aufgerufen unter: https://www.spiegel.de/netzwelt/cambridge-analytica-skandal-facebook-vor-einigung-im-prozess-wegen/datenmissbrauchs-a-e3537fa4-42bd-4a92-8756-cb4470725dca, am 23.12.2023

[37] Nier, H. Cambridge Analytica. Facebook-Skandal: 310.000 potenzielle deutsche Opfer. Statista. Aufgerufen unter: https://de.statista.com/infografik/13428/facebook-skandal-geschaetzte-anzahl-betroffener-profile/ , am 23.12.2023

[38] Computational Propaganda: Political Parties Politicians and Political Manipulation on Social Media. Oxford University Press; 2019.

[39] Bedrohungen durch Desinformation. Universität für Weiterbildung Krems. 2019. Aufegrufen unter: https://www.donau-uni.ac.at/de/aktuelles/news/2019/bedrohungen-durch-desinformation.html, am 23.12.2023

[40] Bundesministerium des Innern und für Heimat. Maßnahmen der Bundesregierung gegen Desinformation. 2023. Aufgerufen unter: https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/desinformation\/massnahmen-der-bundesregierung.html, am 23.12.2023

[41] Smirnova, J; Ahonen, A; Mathelemuse, N; Schwertheim, H; Winter, H. Bundestagswahl 2021. Digitale Bedrohungen und ihre Folgen. Institude for Strategic Dialogue, 2022.

[42] Deutschlandradio. Der Weg ins Weiße Haus. Wie funktioniert das Wahlsystem in den USA?. Aufgerufen unter: https://www.deutschlandfunk.de/der-weg-ins-weisse-haus-wie-funktioniert-daswahlsystem-in-100.html, am 28.12.23

[43] Frankfurter Rundschau. Rückblick auf die US-Wahlen 2016: So kam Donald Trump an die Macht. Frankfurter Rundschau GmbH. Aufgerufen unter: https://www.fr.de/politik/us-wahl-2016-donald-trump-hillary-clinton-wahlkampf-wahlsieg.html, am 29.12.23

[44] Zettl, K. Lesson learned? Demokratische Resilienz gegenuüber digitaler Wahlbeeinflussung in den USA und Deutschland. Springer Verlag. 2020.

[45] StGB (Strafgesetzbuch). Bundesministerium der Justiz. § 202 d Datenhehlerei. Aufgerufen unter: https://www.gesetze-im-internet.de/stgb/, am 22.12.2023

[46] Steinlein, J. Wie kam es zum Sturm aufs Kapitol?. tagesschau. 2021, aufgerufen unter: https://www.tagesschau.de/ausland/amerika/sturm-auf-kapitol-101.html, am 23.12.2023

[47] Breuning, C.; Goerres,A. Searching for electoral irregularities in an established Democracy : Applying Benford's Law tests to Bundestag elections in Unified Germany.Electoral Studies. 2011, S. 534-545

[48] Süddeutsche Zeitung. Pannen in Berlin. Komplettes, systematisches Versagen. 2022. Aufgerufen unter: https://www.sueddeutsche.de/politik/pannen-in-berlin-komplettes-systematisches-versagen-1.5591569, am 26.12.2023

[49] GG (Grundgesetz der Bundesrepublik Deutschland). Bundesministerium der Justiz. Aufgerufen unter: https://www.gesetze-im-internet.de/gg/BJNR000010949.html, am 19.12.2023

[50] Business Insider Deutschland. Umfrage zeigt, was die Deutschen vor der Europawahl als große Gefahr sehen. 2019. Aufgerufen unter: https://www.businessinsider.de/politik/eine-umfrage-zeigt-was-die-deutschen-vor-der-europawahl-als-/groesste-gefahr-sehen-2019-5/, am 18.12.2023

[51] Frankfurter Allgemeine. Europawahl : Deutsche befürchten Manipulation durch. 2019, Aufgerufen unter: https://www.faz.net/aktuell/politik/inland/europawahl-deutsche-befuerchten-manipulation-durch-falschmeldungen.html, am 18.12.2023

[52] Smirnova, J.; Winter, H.; Mathelemuse, N.; Dorn, M.; Schwertheim, H. Digitale Gewalt und Desinformation gegen Spitzenkandidat:innen vor der Bundestagswahl 2021. Institude for Strategic Dialogue, 2021.

[53] Die Bundeswahlleiterin. Bundestagswahl 2021. 2021. Aufgerufen unter: https://www.bundeswahlleiterin.de/bundestagswahlen/2021/fakten-fakenews.html, am 18.12.1023

[54] Vosoughi S et al. The spread of true and false news online. Science359, 1146-1151, 2018. DOI:10.1126/science.aap9559

[55] AVAAZ. Deutschlands Desinformationsdilemma 2021. 2021. Aufgerufen unter: https://avaazimages.avaaz.org/bundestagswahl_2021_final_version.pdf, am 10.12.2023

[56] Wikipedia. Bundestagswahl 2021/Umfragen und Prognosen. Aufgerufen unter: https://upload.wikimedia.org/wikipedia/commons/2/2b/Mittelwerte_Sonntagsfrage_Wahl_zum_20._Bundestag.png, am 20.12.2023

[57] Davis, T.; Livingston, S.; Hindman, M. Suspicious Election Campaign Activity on Facebook. How a Large Network of Suspicious Accounts Promoted Alternative Für Deutschland in the 2019 EU Parliamentary Elections. 2019.

[58] Mathelemuse, N.; Smirnova,J. Desinformationskampagnen gegen die Wahl: Befunde aus Sachsen-Anhalt. Institude f0r Strategic Dialogue, 2021.

[59] EINPROZENT. So geht's: Wahlbeobachtung und Corona. 2012. Aufgerufen unter: https://www.einprozent.de/blog/wahlbeobachtung/so-gehts-wahlbeobachtung-und-corona-videos/2820, am 30.12.2023

[60] Kuhn, J. Bundestagswahl und Sicherheit. Cyberangriffe auf die Demokratie. 2021. Aufgerufen unter: https://www.deutschlandfunkkultur.de/bundestagswahl-und-sicherheit-cyberangriffe-auf-die-100.html, am 30.12.2023

[61] MDR Aktuell. CYBER-SICHERHEIT. Bundestagswahl: Behörden warnen vor Cyber-Bedrohungen. 2021. Aufgerufen unter: https://www.mdr.de/nachrichten/deutschland/wahlen/bundestagswahl/warnung-einflussnahme-bundestagswahl-cyberangriff100.html, am 30.12.2023

[62] Bundesamt für Sicherheit in der Informationstechnik. BSI-Lagebericht: Corona verschärft Cyber-Gefährdungslage. 2020. Aufgerufen unter: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/Lagebericht201010.html, am 30.12.2023

[63] Gerling, Rainer W. Hackerangriff auf die Wahlfreiheit. Wissenschaftsmagazin der Max Planck Forschung. Ausgabe 1/2017. Aufgerufen unter: https://www.mpg.de/11248402/MPF_2017_1.pdf, am 30.12.2023

[64] Plaß, C. Behörden-Seiten nicht erreichbar. Bundesregierung bestätigt Hacker-Angriffe. ARD Berlin, 2022. Aufgerufen unter: https://www.tagesschau.de/inland/cyberattacke-bundesregierung-ddos-101.html, am 18.12.2023

[65] Biermann, K.; Stark, H. Bundestagswahl. Die Bundestagswahl kann manipuliert werden. ZeitOnline, 2017. Aufgerufen unter: https://www.zeit.de/digital/datenschutz/2017-09/bundestagswahl-wahlsoftware-hackerangriff-sicherheit-bsi-bundes/wahlleiter, am 18.12.2023

[66] NetzDG (Netzwerkdurchsetzungsgesetz). Bundesministerium für Justiz. Aufgerufen unter: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html , am 22.12.2023

[67] Bundesministerium der Justiz. Regeln gegen Hass im Netz – das Netzwerkdurchsetzungsgesetz (NetzDG). 2022. Aufgerufen unter: https://www.bmj.de/DE/themen/digitales/digitale_kommunikation/netz_dg/netz_dg_node.html, am 22.12.2023

[68] Albin Schmitt. Big Five (Psychologie). Wikipedia. Aufgerufen unter: https://de.wikipedia.org/wiki/Big_Five_%28Psychologie%29, am 30.12.2023

[69] Die Bundesregierung. Umgang mit Desinformation. Gemeinsam gegen Desinformation. 2021. Aufgerufen unter: https://www.bundesregierung.de/breg-de/schwerpunkte/umgang-mit-desinformation/eu-desinformation-1875918, am 30.12.2023

[70] INSA-CONSULERE. Meinungsumfrage. Vertrauen der deutschen Bevölkerung in die Bundestagswahl. 2021.