Z Außen Sicherheitspolit (2019) 12:429–451
https://doi.org/10.1007/s12399-020-00789-7

ZFAS Zeitschrift für Außen- und Sicherheitspolitik

STUDIE

Lesson learned? Demokratische Resilienz gegenüber digitaler Wahlbeeinflussung in den USA und Deutschland

Kerstin Zettl

Online publiziert: 27. März 2020

Zusammenfassung Die Studie untersucht den Einfluss systemischer und situativer Faktoren auf die unterschiedliche demokratische Resilienz vor externer, digitaler Wahlbeeinflussung durch Russland in den USA 2016 und in Deutschland 2017. Der Vergleich zeigt, dass insbesondere dem Polarisierungsgrad, der Logik des Wahlkampfes sowie der Stellung etablierter Medien eine Erklärungskraft für das jeweilig russische *meddling* unterstellt werden kann. Gleichzeitig können die Wirkweisen einzelner Faktoren auf der technischen Ebene (E-Voting) nicht isoliert, sondern nur in Bezug zueinander bewertet werden.

Schlüsselwörter Digitale Wahlmanipulation · Demokratische Resilienz · USA · Deutschland · Russland

Lesson Learned? Democratic Resilience to Digital Election Meddling in the U.S. and Germany

Abstract The study examines the influence of systemic as well as situational factors on the different democratic resilience to external, digital election meddling by Russia in the US 2016 and in Germany 2017. The comparison shows that the degree of polarization, the logic of the election campaign and the role of established media in particular can be assumed to explain the respective Russian *meddling*. At the same time, the effects of individual factors on the technical level (e-voting) cannot be assessed in isolation but in relation to each other.

Keywords Digital election meddling · Democratic resilience · U.S. · Germany · Russia

K. Zettl (✉)
Institut für Politische Wissenschaft, Ruprecht-Karls-Universität Heidelberg, Bergheimer Str. 58, 69115 Heidelberg, Deutschland
E-Mail: kerstin.zettl@ipw.uni-heidelberg.de

1 Einleitung

Die russische Einflussnahme in den US-Wahlkampf 2016 wurde seitens demokratischer Staaten weltweit als Alarmsignal wahrgenommen. Vier Jahre später deuten sich im Vorfeld der Präsidentschaftswahlen 2020 wieder ähnliche Vorkommnisse an (Wong 2019). Das konkrete Forschungsinteresse dieser Studie liegt in der Frage, welchen Einfluss bestimmte Merkmale der demokratischen Systeme auf die Resilienz gegen externe, im digitalen Raum stattfindende Wahlbeeinflussung während der Präsidentschaftswahl in den USA 2016 sowie der Bundestagswahl 2017 in Deutschland hatten.

Begründet wird die Fallauswahl durch die Gemeinsamkeiten und Unterschiede beider Demokratien: Hierbei spielen institutionelle, aber auch stärker sozio-politische und informelle Systemcharakteristika eine Rolle. Die USA und Deutschland stellen als liberale Demokratien prinzipiell attraktive Ziele für externe Wahlbeeinflussung durch Staaten wie Russland dar. Dennoch weisen sie hinsichtlich der abhängigen Variable, der Resilienz vor externer, digitaler Wahlbeeinflussung, im Untersuchungszeitraum[1] eine untersuchungswürdige Varianz auf. Wird diese unterschiedliche Resilienz zweier Demokratien seitens desselben Akteurs auf die Probe gestellt, kann deren ansonsten schwer zu operationalisierende Wirkung sichtbar gemacht werden. Dies soll im Rahmen dieser Studie durch einen strukturiert-fokussierten Vergleich erfolgen. Aufgrund des Small-N-Designs kann hierbei kein Anspruch auf Vollständigkeit erhoben werden: Für die Zukunft bedarf es weiterer Analysen, welche das noch weitaus größere Spektrum an potenziellen demokratischen Spielarten auf der institutionellen sowie sozio-politischen Ebene im Sinne der Studie beleuchten.

Nach einer theoretischen Verortung des Ansatzes erfolgt die theoriegeleitete Hypothesenbildung. Daran anschließend wird der methodische Ansatz spezifiziert. Entsprechend dieses Schemas erfolgt der Vergleich der beiden Länder, bzw. der demokratischen Merkmale vor und während der Wahlen 2016 und 2017, in Bezug zu den berichteten russischen Beeinflussungsmaßnahmen.

2 Der aktuelle Forschungsstand

Die vorliegende Arbeit verbindet die Teilbereiche der Internationalen Beziehungen (IB) und der Vergleichenden Politikwissenschaft (VP) miteinander. Auch wenn etwa das Eingreifen der USA in regionale Angelegenheiten südamerikanischer Staaten während des Kalten Krieges (Cottam 1994) nicht verschwiegen werden soll, untersuchten die IB bisher stärker autokratische Staaten, die entweder „democracy prevention“ (van Soest 2014) oder „autocracy promotion“ (Burnell 2010; Bader et al. 2010; Tansey 2016) betrieben haben. Gemeinsamer Nenner beider Konzepte war bislang der regionale Fokus, widergespiegelt auch in der Mehrzahl der bisherigen Fallbeispiele, etwa zu Russland oder China (Ambrosio 2007; Melnykovska et al. 2012; Bader 2015). Marianne Kneuer und Thomas Demmelhuber (2016, S. 778) kon-

[1] Dieser umfasst den Zeitraum ab Verkündigung der Spitzenkandidat*innen bis direkt nach der Wahl.

zeptualisieren diesen teilweise bereits als Erfolg gewerteten Export autokratischer Spielarten im Sinne regionaler „Gravitationszentren" mit internationaler Strahlkraft. Laut Espen Rød und Nils Weidmann (2015) flankieren immer mehr Autokratien wie China oder Russland hierzu Zensur und Internet-Blockaden mit digitalen Tools wie E-Partizipation-Angeboten zu einer Verringerung des „dictator's dilemmas" (Göbel 2013, S. 388). Der regionale Fokus digitaler autokratischer Außenpolitik zeigt sich auch zunehmend bei der Kontrolle von Social-Media-Diskursen (Gunitsky 2015). Ein Beispiel hierfür ist das umfassende russische Engagement im Ukraine-Konflikt, laut Beobachter*innen ein „Cyber-test-battlefield" des Kremls (Cerulus 2019). Im Falle der US-Wahlen 2016 handelte es sich bei dem anvisierten Ziel jedoch um eine geografisch weit entfernte, liberale und konsolidierte Demokratie. Somit trifft hier eher der Ausdruck der digitalen *democracy weakening/contestation* zu, welche zunehmend untersuchungswürdig erscheint.

Auf digitalem Wege lassen sich durch einen *Black Knight*[2] (Tolstrup 2015) Wahlen auch ohne physische Präsenz vor Ort stören, hinsichtlich ihrer Integrität unterminieren oder gar manipulieren. Dies kann mit einem immer geringeren Ressourceneinsatz einhergehen, Stichwort *asymmetrischer Konfliktaustrag*. Ein weiterer Vorteil liegt in der weitgehenden Straffreiheit im digitalen Raum, die sich aus der Problematik der Attribution einer Straftat ergibt (Knake 2010).

Die zunehmende digitale Abhängigkeit liberaler Demokratien begründet gleichzeitig deren enorme Verwundbarkeit auf sozialer, ökonomischer sowie sicherheitspolitischer Ebene (Colaresi 2014, S. 237). Wahlen sind dabei attraktive Ziele, da sie nicht nur darüber entscheiden, wer das Land für die nächsten Jahre regieren wird, sondern auch den Identitätskern einer liberalen Demokratie darstellen. Weitreichend vernetzt ist jedoch auch das demokratische Estland und daher potenziell leicht verwundbar. Attackiert wird es jedoch nicht aufgrund seines generellen Machtstatus oder aufgrund konventioneller Ressourcen, sondern – wie im Falle der russischen *Distributed Denial of Service*-Attacken (DDoS-Attacken) 2007 auf das Land – nur dann, wenn ein konkreter Anlass zur Einmischung existiert (Herzog 2011).

Die USA und Deutschland zeichnen sich dagegen durch große ökonomische Stärke und ihre militärische Präsenz in vielen Krisengebieten der Erde aus (Silver 2019). Dies betrifft im Falle der USA ihr Engagement im Nahen Osten sowie in Osteuropa. Beide Regionen sind für Russland von zentraler Bedeutung. Deutschland ist auf außenpolitischer Ebene insbesondere im Rahmen der Europäischen Union als möglicher Gegenspieler Russlands anzusehen, nicht zuletzt durch die vehemente Forcierung der Sanktionen gegenüber dem Kreml in Folge der Annexion der Krim 2014. Somit existierten weitreichende außenpolitische Motivationen für Russland, beide Länder durch eine Beeinflussung der Wahlen zu schwächen. Trotz der genannten ähnlichen Grundvoraussetzungen zeigten die USA und Deutschland jedoch unterschiedliche Grade der Widerstandsfähigkeit im Untersuchungszeitraum. Neben einem möglicherweise schlicht größeren Interesse Russlands an der US-Wahl werden

[2] Jakob Tolstrup definiert *Black Knights* als „external actors – be they democratic or authoritarian, great powers or regional powers, states or international organisations – that act as guardians of autocracy or challengers of democracy in specific contexts" (Tolstrup 2015, S. 676).

im Rahmen dieses Beitrags jedoch vor allem den zu untersuchenden demokratischen Unterschieden eine entscheidende Erklärungskraft unterstellt.

Die Forschung der VP zu demokratischer Resilienz im Netz ist noch relativ jung und wurde vor allem seit den Ereignissen rund um die US-Wahlen 2016 vorangetrieben. Zu nennen wären hier insbesondere die Arbeiten von Maria Hellman und Charlotte Wagnsson (2017) über europäische Strategien zur Abwehr russischer *Information War*-Methoden. Amy Pope (2018) untersuchte ebenfalls mögliche Präventivmaßnahmen für externe Wahlbeeinflussung. Der im Rahmen der Studie relevante Populismus wurde von Pippa Norris (2017) im Kontext elektoraler Integrität analysiert und hinsichtlich möglicher negativer Auswirkungen bewertet, digitale Mittel blieben hierbei jedoch außen vor.

Mit dem Aspekt der strikt technischen Resilienz im Sinne elektoraler IT-Sicherheit[3] beschäftigten sich Ben Buchanan und Michael Sulmeyer (2016). Die vorliegende Studie inkludiert jedoch im Gegensatz zu dieser Arbeit auch Desinformationskampagnen[4] und verweilt nicht ausschließlich auf der rein technischen Ebene.

3 Hypothesenbildung

Nachfolgend werden die unabhängigen Variablen in Hypothesen überführt und dabei vor allem aus formellen Systemfaktoren wie dem Parteien- und Wahlsystem abgeleitet.[5]

3.1 Formelle Systemfaktoren

Polarisierung. In präsidentiellen Systemen erschwert die meist geringere Anzahl an Parteien aufgrund oppositioneller Mehrheiten oftmals das Regieren. Zudem werden komplexe Konfliktlinien hierdurch meist nicht ausreichend abgedeckt. Blockaden können die Folge sein. Amy Gutmann und Dennis Thompson sprechen von einem „uncompromising mindset“ (2010, S. 1125), welches politische Entscheidungen an die ideologischen Ränder drängt, gerade in Zweiparteiensystemen wie den USA. Auch das in präsidentiellen Systemen zumeist angewandte Mehrheitswahlprinzip trägt zu der hier prinzipiell größeren Polarisierung[6] bei: Dessen *The Winner Takes It All*-Logik verschärft Spannungen innerhalb der Bevölkerung und zwischen den

[3] Hierbei wird im Sinne der Arbeit die digitale Manipulation oder Störung von technischen Wahlprozessen verstanden.

[4] Hierunter werden Fake News und inhaltlich stark verzerrte oder populistisch konnotierte Inhalte auf Social-Media-Kanälen verstanden. Diese stellen im Gegensatz zu Hacks mit anschließender Veröffentlichung der abgegriffenen Informationen (Doxing) oder Störungen und Manipulationen der Wahl-IT keine Verletzung der CIA-Triade der Internetsicherheit dar (*confidentiality, integrity, availability*; Oscarson 2003, S. 98).

[5] Dies geschieht in Anlehnung an Hans-Joachim Lauth (2014), wird jedoch im Sinne des neuartigen Untersuchungsfeldes notwendigerweise modifiziert.

[6] Polarisierung wird verstanden als das Auseinanderdriften der politischen und damit auch öffentlichen Meinung, was zu verstärkten politischen Spannungen führt (Prior 2013, S. 104).

Parteien. Die in parlamentarischen Systemen samt Verhältniswahl oftmals niedrigere Polarisierung kann sich jedoch auch durch fehlende programmatische Ausdifferenzierung in Form von Politikverdrossenheit negativ auf die Demokratie auswirken (Maier 2000, S. 15).

Polarisierung muss zwar nicht per se demokratiefeindlich wirken, populistisch *geframed* unterminiert sie jedoch das Vertrauen zwischen den Parteien und den Anhängerschaften (Mudde und Kaltwasser 2012). Insbesondere allein online abrufbare, oftmals populistisch ausgerichtete Medienanbieter befördern in Zeiten von Wahlen dieses gegenseitige Misstrauen. Existiert jedoch ein grundlegendes Vertrauen der Bevölkerung in ihre *alteingesessene* Medienlandschaft, kann dies potenziell Schutz vor Manipulationsversuchen der öffentlichen Meinung bieten. Des Weiteren beeinflusst die jeweilige Logik des Wahlkampfes die Polarisierung: Stark auf die persönlichen Belange der Kandidat*innen und weniger auf inhaltliche Aspekte ausgerichtete Wahlkämpfe bieten stärkere Angriffsflächen für *diffamierende Schmutzkampagnen* im Sinne von Hacking (und Doxing) oder der Desinformation.

Aus diesen theoretischen Überlegungen ergeben sich die nachfolgenden Hypothesen, welche im Zuge der empirischen Analyse auf ihre Erklärungskraft hin untersucht werden:

H1: Je größer die politische Polarisierung als Produkt des institutionellen Arrangements, desto geringer ist die Resilienz vor externer, digitaler Wahlbeeinflussung.

H1a: Je populistischer dieses Auseinanderdriften der jeweiligen Pole, mitbedingt durch die Kandidaten-basierte Wahlkampflogik einer Demokratie, desto anfälliger ist die Demokratie für Desinformationskampagnen in sozialen Medien oder Doxing.

H1b: Je stärker populistische Online-Medien und je geringer die Reichweite etablierter Medienvertreter, desto anfälliger ist die Demokratie für Desinformationskampagnen in sozialen Medien oder Doxing.

Umkämpftheit der Wahl. Das hohe Maß an politischer Polarisierung kann speziell in Zweiparteien-Systemen bei Wahlen mit der Logik des Mehrheitsprinzips zu einer großen Umkämpftheit führen. Auch in Ländern, welche dem Verhältniswahlrecht folgend überwiegend als Resultat ein Mehrparteiensystem haben, kann diese groß sein. Dennoch wird dies in der Regel durch die größere Anzahl an Wahl-Gewinnern moderiert (Wissenschaftliche Dienste des Deutschen Bundestages 2012, S. 7). Je länger ein Wahlkampf umkämpft ist, desto sinnvoller erscheint somit auch eine externe Einflussnahme. Wenn ein Kandidat von vornherein außer Konkurrenz erscheint, könnte höchstens versucht werden, das Land durch Desinformationskampagnen stärker zu spalten, anstelle einer zu aufwendigen Manipulation des Gesamtergebnisses. Aus diesen Annahmen ergibt sich die folgende Hypothese:

H2: Je länger und stärker ein demokratischer Wahlkampf umkämpft ist, desto anfälliger ist die Demokratie für eine Beeinflussung der Wahl auf technischer Ebene (E-Voting).

Potenzielle technische Verwundbarkeiten. Hierbei ist der Grad an digitaler Wahlpraxis zentral. In welchem Umfang wird auf E-Voting gesetzt und welche Technologien werden wofür angewandt? Ein landesweit einheitliches System könnte einerseits leichter angreifbar sein, bzw. Täter*innen die Möglichkeit geben, auf *einen Schlag* eine möglichst große Wirkung zu erzielen. Andererseits kann gerade auch eine unterschiedliche Qualität der einzelnen föderalen IT-Wahlsysteme diese als Ziele attraktiver machen, da somit bundesstaatliche Schwachstellen ausgenutzt und zugleich gezielter Einfluss genommen werden könnte (Buchanan und Sulmeyer 2016, S. 13). Demgegenüber bieten verschiedene Modularitäten und Technologien unterschiedlicher Hersteller auch potenziellen Schutz: Zwar ist somit die partielle Störung der Wahl möglich, die Manipulation des Gesamtergebnisses erscheint dagegen unwahrscheinlich. Hieraus lassen sich die folgenden Hypothesen ableiten:

H3: Je umfangreicher eine Demokratie E-Voting einsetzt, desto anfälliger ist sie für externe Wahlbeeinflussung am Wahltag auf technischer Ebene.

H3a: Je aktueller die Wahlsoftware, desto widerstandsfähiger ist sie hinsichtlich auszunutzender Sicherheitslücken.

H3b: Je heterogener das Wahlsystem und die Wahlinfrastruktur, desto widerstandsfähiger ist die Wahl gegenüber einer maßgeblichen Beeinflussung des Endergebnisses.

H3c: Je heterogener das Wahlsystem und die Wahlinfrastruktur, desto anfälliger wird die Wahl im Hinblick auf die Störung föderaler Untereinheiten.

H3d: Je geringer die bundesweiten Sicherheitsstandards der digitalen Wahlinfrastrukturen und je geringer die bundesstaatlichen Kontrollbefugnisse darüber ausfallen, desto anfälliger ist die Demokratie für partielle Störversuche.

3.2 Informelle Systemfaktoren

Schaffung eines öffentlichen Problembewusstseins. Demokratische Regime können aus Negativbeispielen anderer Demokratien lernen und somit ein größeres Problembewusstsein innerhalb der politischen Führung entwickeln. Dies kann zudem mit IT-Präventivmaßnahmen sowie gesetzlichen Regularien bezüglich Social-Media-Plattformen (SMP) einhergehen. Interdemokratischer Austausch schwächt die Effizienz vormals angewandter autokratischer Instrumente für die Zukunft, auch auf technischer Ebene. Falls es noch kein entsprechendes Referenzereignis gegeben hat, sollte jedoch zumindest *nach* einer aufgetretenen Beeinflussungsmaßnahme seitens der Politik das *wer, warum* und *wie* der Beeinflussung zeitnah thematisiert werden und weniger die tatsächlichen Inhalte, um deren potenzielle Schlagkraft abzumildern. Die letzten beiden Hypothesen lauten somit:

H4: Je aktiver Politiker und Sicherheitsbeamte im Vorfeld einer Wahl oder nach erfolgten Beeinflussungsversuchen diese öffentlich thematisieren, desto widerstands-

fähiger macht dies die Demokratie für Formen, welche auf den Überraschungsmoment setzen, wie z. B. Doxing.

H4a: Je proaktiver die Demokratie auf gesetzlicher Ebene Präventivmaßnahmen vornimmt, desto widerstandsfähiger macht sie dies für externe Wahlbeeinflussung, besonders gegenüber Desinformation auf SMP.

4 Methodik

Im Rahmen eines strukturiert-fokussierten Vergleiches werden die Hypothesen entsprechend ihrer Operationalisierung auf ihre Erklärungskraft hin getestet. Viele Einzelfallstudien entbehren der notwendigen theoretischen Fokussierung, um für den Forschungsbereich über den Fall hinaus von Relevanz zu sein. Durch einen theoretisch angeleiteten Vergleich können die Hypothesen strukturiert getestet und somit für weitere Forschung in dem Themengebiet anschlussfähiger und fruchtbarer gestaltet werden. *Fokussiert* ist der Vergleich zudem, da nicht auf sämtliche Aspekte des jeweiligen Falles eingegangen wird, sondern eben nur auf jene, welche dem theoretischen Interesse der Arbeit entsprechen (George und Bennett 2005, S. 67, 70). Während *Polarisierung* zum einen aus institutionellen und damit statischeren Faktoren abgeleitet wird, sind situative Gegenmaßnahmen im Vorfeld der Wahl stärker im Wandel befindlich. Daher werden für erstere auch Quellen von *vor* dem eigentlichen Untersuchungszeitraum herangezogen, da sich das jeweilige Regierungssystem nicht jedes Jahr im Kern verändert.

4.1 Formelle Systemfaktoren

Polarisierung. Zentrale Indikatoren hierfür sind das jeweilige Parteien- und Wahlsystem. Da jedoch etwa ein Zweiparteiensystem nicht zwingend zu einer erhöhten Polarisierung führt, müssen diese im Kontext des jeweiligen institutionellen Settings betrachtet werden. Bei H1a geht es in Abgrenzung zum Konzept des „issue-voting“ – oder des damit oft kontrastierten „party-voting“ (Highton 2010, S. 453) – weniger um die letztliche Logik der Wahlentscheidung der Bürger*innen als um die des Wahlkampfes. Deren Analyse wird über eine komprimierte Darstellung der jeweiligen Debattenkultur angestrebt. Wird etwa seitens der Kandidat*innen besonders oft der Kontrahent persönlich angegriffen, spricht dies für eine personenbasierte Wahlkampflogik. Im Falle von H1b wird die etwaige Verschiebung des Machtgefüges zwischen traditionellen Print- und oftmals populistischeren Online-Medien durch bereits erhobene Meinungsumfragen in den jeweiligen Ländern operationalisiert. Für die USA wäre dies verkürzt gesprochen *The New York Times* gegenüber *Breitbart* und für Deutschland die *Süddeutsche Zeitung, DIE ZEIT* oder die *Frankfurter Allgemeine Zeitung* (FAZ) gegenüber *Compact* oder ähnlichen Anbietern des populistischen Spektrums.

Umkämpftheit der Wahl. Für die Bewertung der Länge und Stärke der Umkämpftheit eines Wahlkampfes werden nationale Umfragedaten zu verschiedenen Zeitpunkten des Wahlkampfs herangezogen und miteinander verglichen.

Technische Verwundbarkeiten. Hierfür werden die E-Voting-Prozesse der beiden Länder komprimiert dargestellt. Dabei geht es um organisatorische (zentrale vs. dezentrale Steuerung, Einheitlichkeit der Verfahren), aber vor allem auch um technische Komponenten (Hard- und Software) des Wahlprozesses. Zudem werden die gesetzlichen Rahmenbedingungen betrachtet, also inwiefern die technischen Wahlkomponenten einer regelmäßigen Kontrolle unterzogen wurden und welche Standards vor der Wahl Gültigkeit besaßen.

4.2 Informelle Systemfaktoren

Schaffung eines öffentlichen Problembewusstseins. Hierfür werden für beide Länder zusammenfassende Darstellungen der Rhetorik relevanter Diskursträger*innen erstellt (Politiker*innen, Akteure aus den Kreisen der Sicherheitsbehörden). Im Falle Deutschlands soll hierdurch gezeigt werden, inwiefern im Vorfeld der eigenen Wahlen immer wieder auf die Ereignisse in den USA rekurriert und somit die Sensibilisierung der Bevölkerung ermöglicht wurde. Aufgrund des umfassenden Einsatzes von Fake News und Desinformationen auf SMP im US-Wahlkampf 2016 soll durch einen Vergleich der regulativen *Settings* der beiden Länder gezeigt werden, dass auch auf dieser Ebene für Deutschland von einem demokratischen Lerneffekt ausgegangen werden kann.[7]

5 Empirische Analyse

Russland bediente sich nach aktuellem Kenntnisstand verschiedener Maßnahmen zur Beeinflussung der US-Wahlen 2016. Auf diese wird im Folgenden näher eingegangen.

5.1 Die russische Einflussnahme in die US-Präsidentschaftswahlen 2016

Hacking und Doxing. Beim sogenannten DNC-Hack (Democratic National Committee) gelang es den beiden Hackergruppen Cozy und Fancy Bear, die russischen Geheimdiensten zugeordnet werden, in die internen E-Mail-Accounts des Stabschefs der US-Präsidentschaftskandidatin Hillary Clinton einzudringen. Trotz mehrfacher Warnungen des Federal Bureau of Investigation (FBI) reagierte das DNC erst viel zu spät auf die Gefahr, sensible Daten an Dritte zu *verlieren* (Lipton et al. 2016). In der Folge wurden durch Wikileaks sowie eine nach Russland zurückverfolgte Webseite tausende E-Mails veröffentlicht. Diese E-Mails enthielten z. B. brisantes Material über die Bevorzugung Clintons gegenüber Bernie Sanders, aber auch Inhalte, die die anti-katholischen Ressentiments der Partei dokumentierten. Zudem zeigten sie

[7] Siehe Hall und Ambrosio (2017) zu der ebenfalls diskutierten Lernfähigkeit autokratischer Staaten.

das Ausmaß der finanziellen Erlöse Clintons aus ihren vorangegangen Reden an der Wall Street auf (Lipton und Shane 2016).Wie vom damaligen FBI-Direktor James Comey in einer Senatsanhörung im Januar 2017 bestätigt wurde, sah sich auch das Republican National Committee im Vorfeld der Wahlen Hacking-Attacken ausgesetzt. Im Gegensatz zum DNC wurden jedoch bis heute keine vertraulichen Informationen der Republikanischen Partei und ihres Präsidentschaftskandidaten und späteren Wahlsiegers Donald Trump veröffentlicht. Zudem wurden die auf älteren Servern befindlichen Domains der Republikaner*innen teilweise gar nicht mehr benutzt (Greenberg 2017).

Hacking-Angriffe und Manipulation von Wahl-IT. Im Falle der auf die Wahl-IT ausgerichteten russischen Störversuche ist die Attributionslage umstrittener, jedoch mittlerweile ebenfalls als weithin gesichert anzusehen. Dabei wurden ebenfalls via Phishing-Kampagnen gezielt umfassende Zugriffsrechte auf die Computer einzelner Mitarbeiter*innen der für die Wahlsoftware zuständigen Firmen abgegriffen (u. a. VR Systems) (Perlroth et al. 2017). Im Vorfeld der Wahl wurden die Hacking-Angriffe zwar seitens des FBI öffentlich thematisiert, die konkret betroffenen 21 Staaten wurden jedoch erst in Folge massiven Drucks ein Jahr später hierüber informiert (Collier 2017). Auch wenn von keiner entscheidenden Manipulation der abgegebenen Stimmen ausgegangen werden kann, kam es laut Untersuchungsbericht des Senats vom Mai 2018 durch Manipulation oder Löschung von Wählerregistrierungsdatenbanken am Wahltag partiell zu Störungen des Ablaufes. Auch wenn dies auf einzelne Counties beschränkt blieb, verbreiteten sich Berichte über derartige Vorfälle rasch auch über die Grenzen der Bundesstaaten hinaus und unterminierten noch in der Folge die Integrität der Wahl (Perlroth et al. 2017).

Desinformationskampagnen auf SMP. Twitter und Google gaben bei einer Untersuchungsanhörung im Senat Ende Oktober 2017 bekannt, dass bereits seit 2015 Tausende Posts russischer Bots und sogenannter *Trolle* schätzungsweise einem Drittel der Gesamtbevölkerung der USA bis zur Wahl auf ihren Endgeräten angezeigt wurden (Lee und Kent 2017). Die Reichweite der laut Facebook 80.000 Posts von ca. 120 nach Russland zurückverfolgten gefälschten Facebook-Seiten, welche an ca. 29 Millionen US-Amerikaner*innen adressiert waren, dürfte sich durch Teilen und *Liken* noch um ein Vielfaches erhöht haben. Neben Facebook war zudem besonders der Kurznachrichtendienst Twitter betroffen: Ca. 37.000 automatisierte Bots mit Verbindungen zu Russland wurden auf der Plattform identifiziert, deren Tweets ca. 288 Millionen Mal in den USA angezeigt wurden. Hinzu kamen 2752 Accounts der *Troll-Armee* der Internet Research Agency (Lee und Kent 2017). Auch hier wiederum fehlt jedoch deren weitere Amplifizierung über Bot-Netze bzw. Retweets.

Anfang Oktober 2017 räumte Facebook zudem ein, dass politisch motivierte Werbung im Wert von mehr als 100.000 US-$ auf der Plattform des Unternehmens im Auftrag mutmaßlich aus Russland stammender Akteure geschaltet wurde (Isaac und Wakabayashi 2017). Inhaltlich deckte diese ein breites Spektrum der stark polarisierenden Themen ab. Die Mehrzahl unterstützte laut Facebook vor allem die Alt-Right-Bewegung, partiell jedoch auch die *Black Lives Matter*-Kampagne. Direkte Bezugnahme zu den Kandidat*innen der US-Präsidentschaftswahl war zwar vor al-

lem in Form von Pro-Trump sowie Contra-Clinton Posts vorhanden, jedoch deutlich in der Unterzahl (Dawsey 2017). *Unwitting agents*[8], zu denen auch Journalist*innen zählten, ermöglichten im Falle der USA erst die extreme Reichweite der russischen Inhalte durch deren Weiterverbreitung und Thematisierung auf SMP.

5.2 Die demokratische Resilienz der USA

Nachfolgend werden für die USA die jeweiligen Hypothesen im Hinblick auf ihre Erklärungskraft für die Ausprägung der abhängigen Variable plausibilisiert.

Polarisierung. Das mit dem Prinzip der Mehrheitswahl verbundene Zweiparteien-System der USA fördert zum einen eine stark bipolare Debattenkultur und damit eine oftmals konfrontative Ausgangslage. Zum anderen bewirkt das *The Winner Takes It All*-Prinzip des Wahlrechts eine prinzipiell stark umkämpfte Präsidentschaftswahl. Aufgrund der auf Gewaltentrennung ausgerichteten Verfassungsordnung, gepaart mit zahlreichen Vetopunkten, führt die oftmals verhärtete Front zwischen Demokrat*innen und Republikaner*innen immer wieder zu einer Politikblockade (Kenworthy 2015, S. 16). Hinzu kommt, dass die Parteien den Dauerwahlkampfmodus auch immer stärker in den Kongress hineintragen. Insbesondere, wenn das Präsidentenamt und die Mehrheiten im Kongress nicht von einer Partei gestellt werden (Helms 2017, S. 62), was unter dem ehemaligen US-Präsidenten Barack Obama bis zum Ende des Wahlkampfes 2016 der Fall war.

Aus statistischer Sicht hat sich der Polarisierungsgrad in den USA von ca. 40 % unter Eisenhower auf ca. 70 % unter Obama gesteigert.[9] Dieses hohe Maß an Polarisierung zwischen den Parteien und den Anhängerschaften stellte den idealen Nährboden für die russischen Desinformationskampagnen auf SMP und im Sinne des DNC-Hacks dar. Ein niedrigeres Maß an Polarisierung hätte deren Effekte abschwächen können. Dagegen sprach jedoch vor allem die populistische, wenig auf Themen ausgerichtete Prägung des Diskurses: Vor allem das Trump-Lager scheute nicht vor persönlichen Diffamierungen der politischen Kontrahentin zurück, was sich – vorangetrieben durch die Alt-Right-Bewegung – in den sozialen Netzwerken nahtlos fortsetzte (Hawley 2017).

Aufgrund des offenbar gezielten Ausnutzens der aufgezeigten US-amerikanischen Schwachstellen seitens Russlands, können sowohl H1 als auch H1a im Falle der USA sowohl die Art und das Ausmaß der *Leaks* als auch der Desinformationskampagnen plausibel erklären. Auch H1b kann weitestgehend bekräftigt werden: Umfragen des Gallup Instituts im September 2016 belegen das bis hin zur Wahl stetig gesunkene Vertrauen der US-amerikanischen Bevölkerung in ihre traditionelle Medienlandschaft: Während 2013 noch etwa 44 % der Befragten angaben, den

[8] Der Begriff wurde von Ladislav Bittman in seinem Buch *KGB and Soviet Disinformation: An Insider's View* von 1985 geprägt. Er versteht dabei eine Person (oder Personengruppe), die unwissentlich als eine Art Erfüllungsgehilfe eines anderen Akteurs gegenüber dessen Rivalen oder Feind agiert und sich dieser Rolle somit nicht bewusst ist.

[9] Der Polarisierungsgrad wird aus der „Differenz der Zustimmung unter den Parteianhänger*innen eines Präsidenten und der unter den Anhänger*innen der gegnerischen Partei (in %)" bemessen (Schreyer 2017, S. 36–37).

etablierten Journalist*innen weitestgehend Vertrauen zu schenken, waren es mitten im Wahlkampf nur noch 32 % (Swift 2016). Bereits zu Beginn des Wahlkampfes waren die alternativen, populistischen Medienkanäle vor allem auf SMP sehr aktiv. In den USA genießen die etablierten Medienvertreter zwar viele konstitutionell zugesicherte Freiheiten, geraten jedoch durch die zunehmende Masse an Online-*Hobbyjournalist*innen* auch immer stärker unter Druck. Dies, in Verbindung mit den aufgrund zurückgegangener Absatzzahlen entstandenen Einbußen durch geringere Werbeeinnahmen (Meola 2016), hatte bereits vor dem Wahlkampf den Wettstreit um die *meisten Klicks* verschärft. Hierdurch kam es zu einem oftmals wenig reflektierten Umgang mit Leaks, auch seitens etablierter Medienvertreter. Vor allem für die Verbreitung russischer Inhalte auf Facebook sowie der Inhalte des DNC-Leaks waren dies wichtige Erfolgsfaktoren. Somit schwächte auch dieser Aspekt die US-amerikanische Resilienz gegenüber den jeweiligen russischen Einflussformen.

Umkämpftheit der Wahl. In drei der letzten fünf US-Wahlen (einschließlich 2016) betrug die Differenz des Popular Vote weniger als drei Prozentpunkte, was die generell hohe Umkämpftheit der letzten Wahlen zum Ausdruck bringt (Tarrance 2017). Auch im Falle beider Parteien 2016 waren zumindest die Primaries alles andere als eine *klare Sache*. Als jedoch schließlich Clinton und Trump als finale Kontrahent*innen feststanden, sah es lange Zeit nach einem eindeutigen Sieg Clintons aus: Lediglich drei von 28 gelisteten Umfragen im Zeitraum von Ende September bis Mitte Oktober 2016 sahen Trump vor Clinton (Villarreal 2016). Trotz dieses scheinbaren Vorsprungs Clintons hielt die Härte, mit der beide Seiten ihren Wahlkampf führten, ungemildert bis zum Wahltag an. Auch wenn der scheinbar schon sichere Sieg Clintons als relevant für das Ausbleiben einer versuchten Manipulation des Endergebnisses gewertet werden könnte, erscheint hierbei der unterstellte Nexus zwischen Wirken der unabhängigen und abhängigen Variable im Sinne von H2 weniger überzeugend als bei H1-H1b. Stattdessen werden hierfür stärker potenzielle technische Verwundbarkeiten und das Versäumnis, ein öffentliches Problembewusstsein zu schaffen, verantwortlich gemacht. Erstere werden im Folgenden näher erläutert.

Potenzielle technische Verwundbarkeiten. Die IT-Sicherheitsinfrastruktur der E-Voting-Prozesse in den USA war trotz ihrer bereits lange umstrittenen Historie im Vorfeld der 2016er Wahlen nach wie vor stark anfällig für Fehler und Hacking-Angriffe. Der Bundesstaat Virginia stieg daher in der Folge der Ereignisse von 2016 sogar wieder komplett auf Papier-Wahlzettel um (Root et al. 2018). Mit der Election Assistance Commission verfügten die USA 2016 über keine bundesstaatliche Behörde mit ausreichenden Befugnissen, um die einem Flickenteppich gleichende Landschaft unterschiedlicher Wahlsysteme und verwendeter IT-Produkte auf ein ausreichend hohes Sicherheitsniveau zu heben. Auf rechtlich-regulativer Ebene wurde dies durch konkrete Versäumnisse des Department of Homeland Security komplettiert, die anvisierten Staaten frühzeitig über die Hacking-Versuche zu informieren. Hinzu kommt, dass mit Pennsylvania lediglich ein Staat das angebotene *risk assessment* vor den Wahlen 2016 durchführen ließ. Dieses ist zwar nach wie vor nicht verpflichtend, wird jedoch seit der Wahl Trumps immer häufiger angefordert

(Starks 2017). Somit spricht dies für eine erhebliche Erklärungskraft von H3d für die partiellen Störversuche Russlands auf technischer Ebene.

2016 kamen in 43 Staaten elektronische Wahlmaschinen zum Einsatz, die mehr als zehn Jahre alt waren und für die häufig entsprechende Software-Updates nicht mehr existieren (Buchanan und Sulmeyer 2016, S. 14). Ben Buchanan und Michael Sulmeyer verweisen in ihrer Analyse von 2016 jedoch darauf, dass die direkte Manipulation einer großen Anzahl an Stimmen auch einen erheblich größeren Aufwand bedeutet hätte. Die Heterogenität der verwendeten IT-Systeme und Produkte kann hierbei Schutz bieten: Gegen die These, dass zumindest eine punktuelle Beeinflussung von Stimmen in Swing States aufgrund fehlender technischer Hürden ausreichen könnte, argumentierte IT-Experte Bruce Schneier: „If you look at the last few elections, 2000 was decided in Florida, 2004 in Ohio, [...] so deciding exactly where to hack is really hard to know" (zit. n. Cole et al. 2017).

H3b und H3c werden somit für die beschriebenen Störversuche eine plausible Erklärungskraft zugesprochen: Aufgrund der Heterogenität der Wahlsysteme fokussierten sich die Hacker*innen nicht auf den vermeintlich hoffnungslosen Versuch einer Manipulation des Gesamtergebnisses. Auch visierten sie nicht ausschließlich Swing States an, sondern streuten ihr Engagement breit, um die Rate infizierter Server und damit das Ausmaß potenzieller Störungen zu erhöhen. Hinsichtlich des Endergebnisses fungierte das heterogene System somit als Schutz, konnte jedoch gerade aufgrund der menschlichen sowie technischen Schwachstellen Störungen nicht verhindern. Somit wird auch H3a eine vergleichsweise höhere Erklärungskraft zugesprochen als der bereits thematisierten H2 in diesem Zusammenhang.

H3 bietet für das Ausmaß an Beeinflussungsversuchen auf der Ebene der Wahl-IT somit die größte Erklärungskraft: Zwar lieferten die zahlreichen, oftmals veralteten E-Voting-Komponenten Möglichkeiten zur Störung derselbigen, gleichzeitig schützte die heterogene Struktur des Systems jedoch auch die Wahl vor einer potenziellen Manipulation des Gesamtergebnisses. Als letztes werden nun für die USA die Existenz oder das Fehlen einer öffentlichen *Awareness* gegenüber externer Wahlbeeinflussung diskutiert.

Schaffung eines öffentlichen Problembewusstseins *(awareness)*. Im Falle der USA wird im Nachgang als *das* zentrale Versäumnis der Regierung eine zu geringe Transparenz im öffentlichen Umgang mit der vermuteten russischen Einflussnahme angesehen. Obwohl die Sicherheitsbehörden Obama bereits Monate vor der Wahl von der vermuteten russischen Einflussnahme im Zusammenhang mit dem DNC unterrichteten, scheute sich die Administration vor einer öffentlichen Attribution. Insider erklärten, Obama fürchtete den Vorwurf einer politischen Wahleinmischung im Falle einer Schuldzuweisung in Richtung Russland. Zudem schreckte die Regierung davor zurück, wertvolle Attributionsquellen sowie – im Falle eines Gegenschlages – Angriffstools offenzulegen und damit für die Zukunft womöglich unbrauchbar zu machen (Sanger 2018a). Im Rahmen dieser Studie kann der tatsächliche Einfluss

der lange nicht- bzw. erst spät getätigten Attribution Russlands[10] als eines externen *Black Knights* auf den Verlauf der Wahl nicht zweifelsfrei bewertet werden. Dennoch reduzierte sie die Widerstandsfähigkeit der US-amerikanischen Demokratie gerade bezüglich der Auswirkungen des DNC-Hacks. Indem die Regierung die russische Beteiligung lange nicht zum Gegenstand der öffentlichen Debatte machte, versäumte sie es, deren Schlagkraft rechtzeitig abzumildern. H4 wird somit eine erhebliche Erklärungskraft zugesprochen.[11,12]

Die führenden Köpfe der hauptsächlich betroffenen Online-Dienste reagierten gegenüber Vorwürfen der fehlenden demokratischen Sorgfaltspflicht größtenteils mit Ignoranz und Abwehrverhalten. Daher wurden erst nach dem Wahlsieg Trumps aufgrund des steigenden öffentlichen Drucks von Seiten der Konzerne – und auch der Politik, z. B. durch die Verabschiedung des Honest Ads Act – Gegenmaßnahmen initiiert wie etwa die Schaffung eines Hilfezentrums von Facebook für Desinformation (McNamee 2018). Politische Regulation der SMP zum Schutz der Daten der Bürger*innen gab es vor der Wahl jedoch kaum. Hierdurch konnten externe, aber auch nationale Akteure durch das sogenannte *microtargeting* die ungeheure Menge an Daten zu ihren eigenen Gunsten nutzen und mit ihren Botschaften exakt die gewünschte Zielgruppe adressieren (Papakryriakopoulos et al. 2017). Somit kann H4a im Falle der USA ebenfalls eine Erklärungskraft attestiert werden.

6 Die deutsche Bundestagswahl 2017

Russische Beeinflussungsversuche in den deutschen Wahlkampf 2017 ließen sich hauptsächlich bezüglich Desinformationskampagnen auf SMP feststellen, welche nachfolgend genauer beschrieben werden.

6.1 Die russische Einflussnahme in den Bundestagswahlkampf 2017

Eine Echtzeitanalyse der Securing Democracy Alliance zeigte, dass eine Vielzahl von Troll-Accounts auf Twitter vor der Wahl russischen Einflussoperationen zugeordnet werden kann. Diese mobilisierten zum Wählen der Alternative für Deutschland (AfD), hetzten gegen den Islam oder diskreditierten Bundeskanzlerin Angela Merkel, besonders hinsichtlich ihrer Flüchtlingspolitik (Salvo 2017). Neben AfD-

[10] Erst am 7. Oktober 2016, und somit einen Monat vor der Wahl, veröffentlichte das Department of Homeland Security zusammen mit dem Office of the Director of National Intelligence on Election Security ein Statement, indem die russische Regierung direkt für die Vorgänge verantwortlich gemacht wurde. Ende Dezember 2016 erfolgten zudem Sanktionierungen in Form von Ausweisungen mutmaßlicher GRU-Agenten sowie die Schließung zweier russischer Einrichtungen auf US-Boden (Sanger 2018b).

[11] Im Fall der Obama-Regierung gab es jedoch noch kein vergleichbares Referenzereignis einer anderen westlichen liberalen Demokratie, aufgrund derer sie bereits im Vorfeld die Bevölkerung hätte sensibilisieren können.

[12] Mallory (2018, S. 13) sieht in Propaganda-Kampagnen den Versuch, den „intervention threshold“ im Sinne von „deterrence“ nach und nach zu manipulieren, um somit die Mobilisierungsfähigkeit des abschreckenden Staates im Sinne einer zeitnahen und effektiven Reaktion zu schwächen. Somit sei die ständige öffentliche Thematisierung der Strategien des Gegners unabdingbar zur Immunisierung der eigenen Bevölkerung (Mallory 2018, S. 13–14).

unterstützenden Posts richteten sich russische Botnetze vor allem auch auf die Amplifizierung bestimmter Hashtags. Das prägnanteste Beispiel hierfür ist der Hashtag #MerkelMussWeg, der ab August 2017 verstärkt genutzt wurde (Hegelich 2017). Jedoch verbreiteten auch in diesem Falle pro-russische sowie rechtsradikale Nutzer*innen die Nachrichten weiter (Nimmo 2017).

Darüber hinaus berichteten auch russische TV-Kanäle während des Wahlkampfes in stark verzerrender Weise über diverse Vorfälle, wie etwa Proteste am US-amerikanischen Luftwaffenstützpunkt in Rammstein, vermutlich mit dem Ziel, Misstrauen unter den NATO-Partnern zu säen (Hegelich 2017). Den Kanälen wird jedoch hierzulande eine noch eher begrenzte Reichweite zugesprochen (Nimmo 2017). Jedoch auch Akteure der sogenannten *Neuen Rechten* agierten als *(un)witting agents* wie etwa der Kopp-Verlag, das Magazin *Compact* oder die AfD-nahe Wochenzeitung *Junge Freiheit* (Kohrs 2016). Auch wenn der Fall Lisa, bei dem es um ein 2015 angeblich von Migranten vergewaltigtes russischstämmiges Mädchen aus Berlin ging, noch nicht im eigentlichen Zeitraum des Wahlkampfes lag, verdeutlicht er einerseits die Logik russischer Desinformationspolitik, unterstreicht jedoch vor allem das unterstellte prinzipielle Interesse Russlands an Einmischung auch in deutsche Belange.

6.2 Deutschland und seine demokratische Resilienz: Wer hat Angst vorm *russischen Bär*

Erklären die aufgestellten Hypothesen auch das unterschiedliche Ausmaß russischer Beeinflussung im Falle Deutschlands?

Polarisierung. Insgesamt wird die politische Polarisierung in Deutschland als weitaus geringer eingestuft, als es in den USA der Fall ist (Stelzenmüller, in Rokahr 2017). Mit dem Wahlsystem der personalisierten Verhältniswahl unterscheidet sich das politische System beträchtlich vom Mehrheitswahlsystem der USA. Hierbei sind eine größere Repräsentativität der parlamentarischen Kräfteverhältnisse und die Förderung kleinerer Parteien durch die 5 %-Hürde, gleichzeitig jedoch auch der Schutz vor *Weimarer Verhältnissen* das Ziel (Schmidt 2016, S. 45–47). Für Wahlen bedeutet dies zum einen mehr Gewinner und Verlierer als in den USA, zum anderen aufgrund notwendiger Koalitionsverhandlungen im Nachgang oftmals auch unklarere Machtverhältnisse.

Zudem ist das Parteienspektrum in Deutschland – trotz abnehmender Abgrenzungsmerkmale der Sozialdemokratischen Partei Deutschlands (SPD) und der Christlich Demokratischen Union Deutschlands (CDU) (Stichwort *Politikverdrossenheit*) – weitaus vielfältiger als in den USA, wodurch potenziell ein breiteres Spektrum an Themen erfasst werden kann (Woyke 2003, S. 480–481). Auch als Reaktion auf diese zunehmende Angleichung der *Volksparteien* erlangte die AfD 2013 insbesondere im Osten des Landes bis zum Beginn des Wahlkampfes beträchtlichen Einfluss und eine große Anhängerschaft (Heimbach 2016). Deren radikalisierter Ton wurde in erster Linie in sozialen Netzwerken deutlich, ihrem wichtigsten Kommunikationsmedium. Dass bereits vor der Wahl Themen wie *hate speech* in den Fokus der deutschen Politik rückten, liegt somit zu nicht unerheblichem Teil an der ge-

gen Flüchtlinge, Migrant*innen sowie Kanzlerin Merkel gerichteten populistischen Diskursform der AfD-Anhängerschaft (Rosa, in Sapper und Kaspar 2017).

H1a kann für Deutschland somit zumindest in Bezug zu den festgestellten Desinformationskampagnen begründet werden: Aufgrund der bereits vor der Wahl zugenommenen Polarisierung des Online-Diskurses waren für die russischen Fake News im Wahlkampfzeitraum bereits die entsprechenden Konfliktlinien etabliert – z. B. Recht auf Asyl gegenüber Fremdenfeindlichkeit. Dass es jedoch nicht zu einer Art *Merkel-Leak* kam, liegt vor allem an der diskutierten, grundlegend geringeren Polarisierung des deutschen Systems. Hierbei moderierten nicht nur die institutionellen Charakteristika populistische Stimmen stärker als in den USA, sondern etwa auch die nach wie vor größere *Issue*-Basiertheit des deutschen Wahlkampfes. Trotz der Diskursverschiebung durch die AfD basierten selbst persönliche Diffamierungen der Kandidat*innen, beispielsweise Merkels im Zusammenhang mit der Flüchtlingskrise, im Kern doch überwiegend auf den im Wahlkampf dominanten Themen (Kortes 2019). Die Rollentrennung zwischen Politiker*innen als Privatpersonen und Amtsträger*innen erscheint in Deutschland nach wie vor stärker ausgeprägt als in den USA.

Bezüglich H1b kam hinzu, dass die traditionelle Medienlandschaft in Deutschland nach wie vor ein weitaus größeres Maß an Vertrauen genießt als zuvor in den USA (Forbrig 2017), trotz gegenteiliger Bemühungen seitens AfD- und PEGIDA-Anhänger*innen[13] (Stichwort Lügenpresse). Der DNC-Hack konnte seine landesweite Wirkung vor allem dadurch erzielen, dass er auch von etablierten Medien in der analogen Sphäre aufgegriffen wurde. Aufgrund der geringeren Reichweite populistischer Medien in Deutschland wäre etwas Vergleichbares hier schwieriger gewesen.

Umkämpftheit der Wahl. Während im März 2017 nach einem anfänglichen Hype um SPD-Kanzlerkandidat Martin Schulz beide Kandidat*innen laut ARD-Sonntagsfrage noch ähnlich hohe Zustimmungswerte erhielten, vergrößerte Merkel ab April 2017 ihren Vorsprung immer weiter (größte Differenz: Ende Juli 2017). Bereits im späten Frühling des Wahljahres zweifelte kaum noch ein Beobachter an ihrer Wiederwahl, eine Wechselstimmung kam nicht mehr auf. Trotz historischer Verbindungen der SPD mit Russland erschienen Martin Schulz und die SPD keine Alternative zu Merkel zu sein, die *erstens* realistische Chancen auf einen Sieg hatte und *zweitens* aufgrund ihrer programmatischen Nähe zum Kreml um jeden Preis in das Amt zu hieven sei (Taylor 2017). Die spannendste und im Sinne der Umkämpftheit polarisierendste Frage blieb somit bis zuletzt das tatsächliche Abschneiden der AfD. Deren propagierte Themen wie die Flüchtlingskrise prägten weithin die Debattenkultur in Printmedien und TV(-Debatten). Einen entscheidenden Beitrag für diesen Erfolg als Agenda-Setter leistete der im Sinne des *„Negative Campaigning"* bewusst polarisierend geführte Wahlkampf der Partei (Schneider 2017).

Somit könnte H2 erklären, warum ein Eingreifen Russlands auf technischer Ebene am Wahltag wenig erfolgsversprechend gewesen wäre: Eine Manipulation des

[13] PEGIDA ist ein Akronym für die Protestbewegung Patriotische Europäer gegen die Islamisierung des Abendlandes.

Ergebnisses zu Gunsten von Schulz hätte aufgrund der vorherigen Umfragen vermutlich zu viel Aufsehen erregt. Auch hier erscheinen zur Erklärung der Resilienz vor technischer Einflussnahme vor allem jedoch technische Aspekte von größerer Relevanz zu sein. Die geringere Umkämpftheit der Wahl könnte im Falle Deutschlands eher das allgemein niedrigere bzw. auf manchen Ebenen nicht vorhandene Einflussstreben Russlands erklären.

Potenzielle technische Verwundbarkeiten. Während in den USA E- und I-Voting[14] in vielen Bundesstaaten mittlerweile zugelassen sind, finden sich in Deutschland keine vergleichbaren Wahlmöglichkeiten. Nachdem es in Folge des partiellen Einsatzes von Wahlcomputern während der Bundestagswahlen 2005 zu Wahlprüfungsbeschwerden vor dem Bundesverfassungsgericht (BVG) kam, urteilte dieses in seinem sogenannten Wahlcomputer-Urteil gegen den Einsatz von E-Voting-Verfahren. Durch eine Enquetekommission 2010 erneut bekräftigt, hatte dieses Urteil auch betreffend der Wahl 2017 nach wie vor bundesweite Gültigkeit (Wissenschaftliche Dienste des Deutschen Bundestages 2015, S. 10–12).

Einzig bei der Übermittlung der Stimmen von Kommunen und Ländern an die Bundeswahlleitung ist der Einsatz von Software erlaubt. Dabei handelt es sich laut Aussagen der Landeswahlleiter*innen überwiegend um die Software PC-Wahl des Herstellers Vote IT. Jedoch gaben diese auch an, oftmals nicht genau zu wissen, mit welchen Hilfsmitteln die Kommunen zur Stimmenübermittlung agieren. Die überwiegend stark veraltete Software zeichnete sich laut Chaos Computer Club im September 2017 jedoch durch eine Vielzahl potenzieller Angriffspunkte zur Manipulation des zumindest vorläufigen Wahlergebnisses aus (Gruber und Horchert 2017). Der Bundeswahlleiter konstatierte jedoch, dass zwar das am Wahlabend rasch an die Öffentlichkeit gebrachte Ergebnis auf Grundlage dieser Prozesse entstünde, nicht aber das amtliche Endergebnis. Hierfür seien nach wie vor die Papier-Stimmen ausschlaggebend.

Somit spricht H3a aufgrund der veralteten Software für eine geringere Resilienz Deutschlands vor technischer Wahlbeeinflussung oder -störung. Dass es jedoch – zumindest nach öffentlichem Kenntnisstand – auch auf regionaler oder föderaler Ebene zu keiner (versuchten) Einflussnahme oder Störung kam, liegt wohl vor allem an den im Sinne von H3 insgesamt weitaus geringeren technischen Einfallmöglichkeiten als in den USA (H3c). Die überwiegend analogen Wahlverfahren moderierten gleichzeitig die größere Homogenität der verwendeten Software im Vergleich zu den USA (H3a). Im Falle Deutschlands herrschte lediglich im Sinne der Stimmenübermittlung eine gewisse Heterogenität vor. Aufgrund der Wirkung von H2, des prognostizierten großen Vorsprungs Merkels vor Schulz, hätte eine hierdurch potenziell ermöglichte Manipulation des Endergebnisses zu viel Aufsehen erregt und in Folge von Untersuchungen die intendierte Wirkung verloren (H3b). Ebenfalls moderiert wird vor allem durch die Wirkung von H3 die offenbar schwach ausgeprägte Transparenz darüber, welche kommunale Einheit sich welcher Hilfsmittel zur Stimmenübermittlung bedient (H3d). Somit bedingten sich H3a-H3d im Falle

[14] E-Voting bezieht sich auf elektronische Hilfsmittel zur Stimmabgabe oder Auszählung bei Wahlen, während I-Voting Möglichkeiten zur Stimmabgabe über das Internet vorsieht.

Deutschlands im Zusammenspiel mit H2 stärker gegenseitig und können in ihrer Wirkweise nicht isoliert voneinander bewertet werden. H3 kann jedoch als Oberthese auch für Deutschland plausibilisiert werden.

Schaffung eines öffentlichen Problembewusstseins. Im Gegensatz zu der erst sehr spät erfolgten öffentlichen Attribution Russlands seitens Obamas thematisierten deutsche Akteure die Möglichkeit hierfür bereits Monate vor der Wahl.[15] Bereits im November 2016 konstatierte der damalige Präsident des Bundesamtes für Verfassungsschutz Hans-Georg Maaßen: „Wir haben im vergangenen Jahr gesehen, dass in Deutschland von russischer Seite Einfluss genommen wurde auf die öffentliche Meinungsbildung. Dies könnte auch im nächsten Jahr stattfinden. Und da sind wir alarmiert“ (zit. n. n-tv 2016a). In der nachfolgenden Zeit tätigten Politiker*innen verschiedenster Parteien immer wieder derartige Aussagen: „Wir erleben Desinformationskampagnen, denen auch Angriffe auf die IT von Regierung, Parlament oder Medienhäusern vorausgehen können“ (de Maizière, zit. n. n-tv 2016b). Zudem mehrten sich die vorwiegend aus Russland und China stammenden Cyberattacken auf öffentliche Einrichtungen, so der CDU-Innenminister Thomas de Maizière Anfang Dezember 2016 (n-tv 2016b).

Im gemeinsam vom Bundesinnenministerium und dem Bundesamt für Sicherheit in der Informationstechnik erstellten Lagebericht zur IT-Sicherheit 2016 wurde daher bereits auf die vor allem aus Russland und Asien identifizierte Bedrohung im Cyberspace hingewiesen sowie die erhöhte Alarmbereitschaft der Behörden im Vorfeld der Wahl herausgestellt (BSI 2016). Als empirisches Referenzereignis diente dabei nicht nur der DNC-Hack, sondern vor allem auch der Bundestagshack aus 2015, für welchen ebenfalls Fancy Bear verantwortlich gemacht wurde (Beuth et al. 2017).

Im Sinne von H4 kann somit von einer proaktiven Haltung der relevanten Akteure zur Sensibilisierung der Öffentlichkeit vor externer Wahlbeeinflussung gesprochen werden.[16] Es wird davon ausgegangen, dass diese situative Präventivmaßnahme dazu beitrug, Maßnahmen wie Doxing in Deutschland aufgrund des fehlenden Überraschungseffektes zu verhindern.

Bezüglich der Resilienz Deutschlands gegenüber Desinformationskampagnen ist das wesentlich höhere Datenschutzniveau als in den USA zu nennen, was beispielsweise politisches *microtargeting* zwar erschwert (Papakryriakopoulos et al. 2017), jedoch gerade für Dritt-Parteien nicht unmöglich macht. Die politischen Parteien Deutschlands kamen bereits im Vorfeld der Wahl darin überein, auf dieses Mittel zu verzichten, einzig die AfD behielt sich die Möglichkeit vor (Brien 2016). Die Meinungsfreiheit ist ebenfalls wie in den USA zwar stark geschützt, jedoch nur im Rahmen bestehender Gesetze: *Hate speech* wurde somit von Seiten der Politik bereits im Wahlkampf sehr viel stärker adressiert als in den USA. Die Gesetzesini-

[15] Dies zeigte offenbar auch Wirkung: In Umfragen vom Juni 2017 gaben 59 Prozent der Befragten an, bereits Online-Fake News gesehen zu haben. Immerhin 61 Prozent konstatierten, dass dies eine Bedrohung für die Demokratie darstelle (Shuster 2017).

[16] Dabei kam es auch zu zivilen Präventivprojekten wie etwa der Kooperation der Faktenchecker*innen von Correctiv mit Facebook im Vorfeld der Wahl (Shuster 2017).

tiative zum Netzwerkdurchsetzungsgesetz, welches am 30. Juni 2017 verabschiedet wurde, verdeutlicht die Bemühungen der Bundesregierung, auch auf gesetzlicher Ebene Entwicklungen wie in den USA vorzubeugen (Deutscher Bundestag 2017).

Eine weitere Gegenmaßnahme war das Angebot seitens des BSI an die zehn führenden Parteien, im Wahlkampf sogenannte *Penetrationstests* auf ihre Online-Systeme durchzuführen, welches auch von allen in Anspruch genommen wurde (Schwirtz 2017). Somit kann auch H4a eine relevante Erklärungskraft zugesprochen werden, im Sinne demokratischer Resilienz vor Maßnahmen wie Doxing, aber auch einer noch stärker ausgeprägten Desinformationspolitik russischer Akteure auf SMP, welche zwar existierte, im Vergleich zu den USA jedoch weit geringer ausfiel.

7 Fazit

Die vorliegende Untersuchung zeigt, auf welch unterschiedliche Weise sowohl institutionelle als auch sozio-politische Systemfaktoren in den beiden Ländern deren demokratische Resilienz vor externer Wahlbeeinflussung prägten. Die aufgestellten Hypothesen konnten dabei für beide Fälle überwiegend bekräftigt werden, mit partiellen Ausnahmen: Im Falle der USA wurde für die umfassende und vielfältige Beeinflussung seitens Russlands in erster Linie das große Maß an sozio-politischer Polarisierung als Wirkfaktor herausgestellt. Sowohl der DNC-Hack als auch die große Menge an Desinformationskampagnen auf SMP setzten explizit an dieser Achillesferse an und förderten somit die weitere Spaltung von Politik und Gesellschaft. Die Härte und populistische Prägung des Wahlkampfes sowohl seitens der Parteien als auch durch deren Anhängerschaften trugen ihr Übriges hierzu bei. Profitieren konnten die russischen Maßnahmen zudem von dem zunehmenden Wettstreit um die Deutungshoheit im Netz, welche auch etablierte Medienvertreter im Wahlkampf zu *unwitting agents* werden ließ.

Hinsichtlich der Verwundbarkeit der USA auf technischer Ebene im Sinne des E-Voting zeigte sich, dass die Hypothesen 3a-3d nicht isoliert voneinander bewertet werden können. Im Falle der USA ließ sich jedoch plausibel darstellen, wie einerseits die Heterogenität der verwendeten Systeme eine mögliche Manipulation des Gesamtergebnisses verhinderte, andererseits jedoch auch durch teilweise stark unzureichende Sicherheitsstandards zumindest lokale Störungen am Wahltag ermöglichte. Aufgrund fehlender Referenzereignisse kann den USA weniger der Vorwurf fehlender Sensibilisierung *vor* dem DNC-Hack gemacht werden, als das Versäumnis der Obama-Regierung zumindest *danach zeitnah* die mutmaßlich russische Beeinflussung öffentlich zu adressieren und somit den Inhalten der E-Mails weniger öffentliche Fläche zu bieten.

Insgesamt zeigen die russischen Maßnahmen, dass es dabei wahrscheinlicher um die allgemeine Schwächung des inner-US-amerikanischen Zusammenhaltes an sich ging – gleiches gilt für Deutschland. Die tatsächliche Beeinflussung des Wahlergebnisses in Richtung Trump konnte aufgrund der zum Wahlzeitpunkt eher für Clinton sprechenden Umfragedaten sowie der beschriebenen technischen Hürden lediglich als willkommener, jedoch nicht zwingend forcierter Nebeneffekt eingestuft werden.

Dagegen zeichnete sich Deutschland aufgrund des unterschiedlichen Parteien- und Wahlsystems durch ein weitaus geringeres Maß an politischer Polarisierung aus. Zwar wurde der Diskurs auf der Online-Ebene seitens der AfD zunehmend populistischer geprägt, was jedoch durch den überwiegend themenbasierten Wahlkampf sowie die nach wie vor maßgebliche Reichweite etablierter, nicht nur digital aktiver Medienvertreter moderiert wurde. Hierdurch lässt sich das lediglich auf Desinformationskampagnen auf SMP ausgerichtete Engagement Russlands im Vergleich zu den USA am ehesten erklären. Dass ein *Merkel-Leak* aufgrund der aufgezeigten Aspekte keine ähnliche Wirkung wie der DNC-Hack hätte entfalten können, lag neben den institutionellen Faktoren zudem an der situativen Sensibilisierung der Bevölkerung seitens Politikern und Sicherheitsakteuren im Vorfeld der Wahl. Hierdurch konnte das notwendige Problembewusstsein für mögliche externe Beeinflussungsversuche und somit konkrete Präventivmaßnahmen etabliert werden. Im Gegensatz zu den USA wartete man in Deutschland letztlich geradezu auf ein ähnliches Ereignis wie den DNC-Hack. Somit hätte dieser nur wenig Durchschlagskraft versprochen. Dass es auch im Falle Deutschlands zu keiner versuchten Manipulation des Endergebnisses kam, lag hier stärker als in den USA an der weitaus geringeren Umkämpftheit der Wahl, welche ein solches Unterfangen zu kostspielig gemacht hätte. Für die im Vergleich zu den USA hierzulande zudem ausgebliebene Störung der Wahlprozesse auf technischer Ebene können vor allem die überwiegend analogen Wahlprozesse verantwortlich gemacht werden.

Die Erklärungskraft der Hypothesen kann auf Grundlage der Arbeit nicht generalisiert werden, zu groß ist die Vielfältigkeit demokratischer Spielarten. Dennoch können sie Anstoß für weitere Forschung in dem Bereich geben, welche aufgrund der zunehmend konfliktiven Ausrichtung digitaler Technologien zwischen und innerhalb von Staaten dringend geboten erscheint. Der Einsatz offensiver Cyber-Maßnahmen des US Cyber Commands gegen die Internet Research Agency im Vorfeld der Midterm Elections 2018 sowie die Entscheidung Twitters, hinsichtlich der US-Präsidentschaftswahlen 2020 politische Werbung auf der eigenen Plattform verbieten zu wollen, deuten ein intensiviertes Engagement staatlicher und privater Akteure im Kampf gegen *election meddling* in den USA an. Ob derartige Gegenmaßnahmen auch im Sinne neuerer Herausforderungen wie etwa den sogenannten *deep fakes* ausreichen werden, muss die Zukunft zeigen. Die im Falle der demokratischen Vorwahlen im US-Bundesstaat Iowa im Februar 2020 aufgetretenen Störungen bei der Übermittlung der Wahlergebnisse mittels einer App verdeutlichen zudem den – auch in den USA – nach wie vor gebotenen Handlungsbedarf auf technischer Ebene. Eine hinreichende Transparenz der Regierenden im Umgang mit externer Wahlbeeinflussung erscheint, unabhängig von institutionellen Unterschieden, jedoch ein grundlegendes Erfordernis demokratischer Wehrhaftigkeit im 21. Jahrhundert zu sein.

Funding Open Access funding provided by Projekt DEAL.

Literatur

Ambrosio, T. (2007). Insulating Russia from a colour revolution: How the Kremlin resists regional democratic trends. *Democratisation*, *14*(2), 232–252.

Bader, J. (2015). China, autocratic patron? An empirical investigation of China as a factor in autocratic survival. *International Studies Quarterly*, *59*(1), 23–33.

Bader, J., Grävingholt, J., & Kästner, A. (2010). Would autocracies promote autocracy? A political economy perspective on regime-type export in regional neighbourhoods. *Contemporary Politics*, *16*(1), 81–100.

Beuth, P., Biermann, K., Klingst, M., & Stark, H. (2017, 11. Mai). Merkel und der schicke Bär. Die ZEIT. http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland. Zugegriffen: 11. Feb. 2020.

Bittman, L. (1985). *The KGB and Soviet disinformation: an insider's view*. Washington: Pergamon-Brassey's.

Brien, J. (2016, 24. Nov.). Bundestagswahlkampf 2017: Angela Merkel nimmt Fake-News, Bots und Trolle ins Visier. T3N Digital Pioneers. https://t3n.de/news/merkel-fake-news-bots-trolle-769925/. Zugegriffen: 14. Jan. 2018.

BSI – Bundesamt für Sicherheit in der Informationstechnik. (2016). Die Lage der IT-Sicherheit in Deutschland. https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=5. Zugegriffen: 11. Febr. 2020.

Buchanan, B., & Sulmeyer, M. (2016). Hacking chads. The motivations, threats, and effects of electoral insecurity. Belfer Center for Science and International Affairs. https://www.belfercenter.org/sites/default/files/files/publication/hacking-chads.pdf. Zugegriffen: 20. Nov. 2017.

Burnell, P. J. (2010). *Is there a new autocracy promotion?* Madrid: Fride.

Cerulus, L. (2019, 14. Feb.). How Ukraine became a test bed for cyberweaponry. Politico. https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/. Zugegriffen: 20. Mai 2019.

Colaresi, M. P. (2014). *Democracy declassified: the secrecy dilemma in national security*. Oxford: Oxford University Press.

Cole, M., Esposito, R., Biddle, S., & Grimm, R. (2017, 5. Juni). Top secret NSA report details Russian hacking efforts days before 2016 elections. The Intercept. https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/. Zugegriffen: 8. Mai 2019.

Collier, K. (2017, 22. Sep.). DHS waited until now to tell state election officials that Russians tried to hack their systems. Buzz Feed. https://www.buzzfeednews.com/article/kevincollier/states-outraged-dhs-waited-a-year-to-tell-them-russians. Zugegriffen: 10. Juni 2019.

Cottam, M. L. (1994). *Images and intervention: US policies in Latin America*. Pittsburgh: University of Pittsburgh Press.

Dawsey, J. (2017, 26. Sep.). Russian-funded Facebook ads backed Stein, Sanders and Trump. Politico. https://www.politico.com/story/2017/09/26/facebook-russia-trump-sanders-stein-243172. Zugegriffen: 10. Mai 2019.

Deutscher Bundestag. (2017). Bundestag beschließt Gesetz gegen strafbare Inhalte im Internet. www.bundestag.de/dokumente/textarchiv/2017/kw26-de-netzwerkdurchsetzungsgesetz/513398. Zugegriffen: 18. Dez. 2017.

Forbrig, J. (2017, 3. Aug.). Russian Hackers Can't Beat German Democracy. Foreign Policy. http://foreignpolicy.com/2017/08/03/russian-hackers-cant-beat-german-democracy-putin-merkel/. Zugegriffen: 10. März 2020.

George, A.L., & Bennett, A. (2005). *Case studies and theory development in the social sciences*. Cambridge: MIT Press.

Göbel, C. (2013). The information dilemma: How ICT strengthen or weaken authoritarian rule. *Statsvetenskaplig tidskrift*, *115*(4), 367–384.

Greenberg, A. (2017, 1. Okt.). Russia hacked "older" republican emails, FBI director says. Wired. https://www.wired.com/2017/01/russia-hacked-older-republican-emails-fbi-director-says/. Zugegriffen: 2. Feb. 2019.

Gruber, A., & Horchert, J. (2017, 7. Sep.). Hacker zerlegen Wahl-Software. Spiegel Online. http://www.spiegel.de/netzwelt/netzpolitik/bundestagswahl-2017-hacker-zerlegen-wahl-software-pc-wahl-a-1166425.html. Zugegriffen: 11. Feb. 2020.

Gunitsky, S. (2015). Corrupting the cyber-commons: social media as a tool of autocratic stability. *Perspectives on Politics*, *13*(1), 42–54.

Gutmann, A., & Thompson, D. (2010). The mindsets of political compromise. *Perspectives on Politics*, *8*(4), 1125–1143.

Hall, S.G.F., & Ambrosio, T. (2017). Authoritarian learning: a conceptual overview. *East European Politics*, *33*(2), 143–161.

Hawley, G. (2017, 27. Okt.). The European roots of the alt-right. Foreign affairs. https://www.foreignaffairs.com/articles/europe/2017-10-27/european-roots-alt-right. Zugegriffen: 10. Mai 2019.

Hegelich, S. (2017, 29. Dez.). Online-Manipulationen im Zuge der Bundestagswahl. Political Data Science Blog. http://politicaldatascience.blogspot.de/2017/12/online-manipulationen-BTW.html?view=magazine. Zugegriffen: 11. Feb. 2020.

Heimbach, T. (2016, 15. Sep.). Warum die Linke in Berlin vor der AfD zittern muss. Die Welt. https://www.welt.de/politik/deutschland/article158143384/Warum-die-Linke-in-Berlin-vor-der-AfD-zittern-muss.html. Zugegriffen: 11. Feb. 2020.

Hellman, M., & Wagnsson, C. (2017). How can European states respond to Russian information warfare? An analytical framework. *European Security*, *26*(2), 153–170.

Helms, L. (2017). Polarisierung in der Demokratie: Formen und Wirkungen. *Österreichische Zeitschrift für Politikwissenschaft*, *45*(3), 57–68.

Herzog, S. (2011). Revisiting the Estonian cyber-attacks: Digital threats and multinational responses. *Journal of Strategic Security*, *4*(2), 49–60.

Highton, B. (2010). The contextual causes of issue and party voting in American presidential elections. *Political Behavior*, *32*(4), 453–471.

Isaac, M., & Wakabayashi, D. (2017, 30. Okt.). Russian Influence Reached 126 Million Through Facebook Alone. The New York Times. https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html. Zugegriffen: 10. März 2020.

Kenworthy, L. (2015). Political polarization. The good society. https://lanekenworthy.net/political-polarization/. Zugegriffen: 10. Mai 2019.

Knake, R.K. (2010). Internet governance in an age of cyber insecurity. Council Special Report, 56. Council on Foreign Relations. https://cdn.cfr.org/sites/default/files/pdf/2010/08/Cybersecurity_CSR56.pdf?_ga=2.240897280.224113948.1581284617-1388538643.1581284617. Zugegriffen: 9. Feb. 2020.

Kneuer, M., & Demmelhuber, T. (2016). Gravity centres of authoritarian rule: a conceptual approach. *Democratization*, *23*(5), 775–796.

Kohrs, C. (2016, 27. Dez.). Futter für AfD-Wähler. Correctiv. https://correctiv.org/recherchen/neue-rechte/artikel/2016/12/27/medien-editorial/. Zugegriffen: 11. Feb. 2020.

Korte, K.-R. (2019). Die Bundestagswahl 2017: Ein Plebiszit über die Flüchtlingspolitik. In K.-R. Korte, & J. Schoofs (Hrsg.), *Die Bundestagswahl 2017. Analysen der Wahl-, Parteien-, Kommunikations- und Regierungsforschung* (S. 1–19). Wiesbaden: Springer VS.

Lauth, H.J. (2014). *Politische Systeme im Vergleich. Formale und informelle Institutionen im politischen Prozess*. München: De Gruyter.

Lee, C.E., & Kent, J.L. (2017, 30. Okt.). Facebook says Russian-backed election content reached 126 million Americans. NBC NEWS. https://www.nbcnews.com/news/us-news/russian-backed-election-content-reached-126-million-americans-facebook-says-n815791. Zugegriffen: 10. Mai 2019.

Lipton, E., & Shane, S. (2016, 16. Dez.). Democratic house candidates were also targets of Russian hacking. The New York Times. https://www.nytimes.com/2016/12/13/us/politics/house-democrats-hacking-dccc.html. Zugegriffen: 10. Apr. 2019.

Lipton, E., Sanger, D.E., & Shane, S. (2016, 13. Dez.). The perfect weapon: how Russian cyberpower invaded the U.S. The New York Times. http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_ r=0. Zugegriffen: 10. Apr. 2019.
Maier, J. (2000). *Politikverdrossenheit in der Bundesrepublik Deutschland. Dimensionen – Determinanten – Konsequenzen*. Wiesbaden: Springer VS.
Mallory, K. (2018). New challenges in cross-domain deterrence. RAND Corporation. https://apps.dtic.mil/dtic/tr/fulltext/u2/1053266.pdf. Zugegriffen: 30. Aug. 2019.
McNamee, R. (2018). How to fix Facebook – before it fixes us. Washington Monthly. https://washingtonmonthly.com/magazine/january-february-march-2018/how-to-fix-facebook-before-it-fixes-us/. Zugegriffen: 10. Mai 2019.
Melnykovska, I., Plamper, H., & Schweickert, R. (2012). Do Russia and China promote autocracy in Central Asia? *Asia Europe Journal*, *10*(1), 75–89.
Meola, A. (2016, 06. Juli). The biggest spending advertisers are abandoning traditional media. Business Insider Deutschland. http://www.businessinsider.de/the-biggest-spending-advertisers-are-abandoning-traditional-media-2016-7?r=US&IR=T. Zugegriffen: 10. Mai 2019.
Mudde, C., & Kaltwasser, C.R. (2012). *Populism in Europe and the Americas: Threat or corrective for democracy?* Cambridge, New York: Cambridge University Press.
Nimmo, B. (2017, 22. Juni). The Kremlin's amplifiers in Germany. The activists, bots, and trolls that boost Russian propaganda. Digital Forensic Research Labs. https://medium.com/dfrlab/the-kremlins-amplifiers-in-germany-da62a836aa83. Zugegriffen: 11. Feb. 2020.
Norris, P. (2017). Why populism is a threat to electoral integrity. LSE European Politics and Policy (EUROPP) Blog. https://blogs.lse.ac.uk/europpblog/2017/05/16/why-populism-is-a-threat-to-electoral-integrity/. Zugegriffen: 14. Jan. 2020.
n-tv. (2016a, 16. Nov.). Bundestagswahl 2017: Sorge vor russischem Eingreifen wächst. https://www.n-tv.de/politik/Sorge-vor-russischem-Eingreifen-waechst-article19109426.html. Zugegriffen: 11. Mai 2019.
n-tv. (2016b, 12. Dez.). Cyberwar im Bundestag. Politiker fürchten manipulierte Wahlen. https://www.n-tv.de/politik/Politiker-fuerchten-manipulierte-Wahlen-article19304131.html. Zugegriffen: 11. Mai 2019.
Oscarson, P. (2003). Information security fundamentals. In C. Irvine & H. Armstrong (Hrsg.), *Security education and critical infrastructures* (S. 95–108). New York: Springer.
Papakyriakopoulos, O., Shahrezaye, M., Thieltges, A., Serrano, J.C.M., & Hegelich, S. (2017). Social Media und Microtargeting in Deutschland. *Informatik-Spektrum*, *40*(4), 327–335.
Perlroth, N., Wines, M., & Rosenberg, M. (2017, 01. Sep.). Russian election hacking efforts, wider than previously known, draw little scrutiny. The New York Times. https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html. Zugegriffen: 10. Feb. 2019.
Pope, A. (2018). Cyber-securing our elections. *Journal of Cyber Policy*, *3*(1), 24–38.
Prior, M. (2013). Media and political polarization. *Annual Review of Political Science*, *16*, 101–127.
Rød, E.G., & Weidmann, N.B. (2015). Empowering activists or autocrats? The internet in authoritarian regimes. *Journal of Peace Research*, *52*(3), 338–351.
Rokahr, L. (2017, 23. Sep.). Russische Manipulation der Bundestagswahl: „Wir stehen international unter Beobachtung". Focus Online. https://www.focus.de/politik/deutschland/bundestagswahl_2017/bundestagswahl-hackerangriffe-fake-news-so-manipuliert-russland-unsere-bundestagswahl_id_7627266.html. Zugegriffen: 11. Feb. 2020.
Root, D., Kennedy, L., Sozan, M., & Parshall, J. (2018, 12. Feb.). Election security in all 50 states. Center for American Progress. https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/. Zugegriffen: 7. Okt. 2018.
Salvo, D. (2017, 20. Sep.). Russia's interference in Germany will continue beyond the September 24 elections. The Alliance for Securing Democracy, German Marshall Fund. https://securingdemocracy.gmfus.org/russias-interference-in-germany-will-continue-beyond-the-september-24-elections/. Zugegriffen: 11. Feb. 2020.
Sanger, D.E. (2018a). *The perfect weapon. War, sabotage and fear in the cyber age*. New York: Crown.
Sanger, D.E. (2018b, 29. Dez.). Obama strikes back at Russia for election meddling. The New York Times. https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html. Zugegriffen: 11. Feb. 2020.
Sapper, M., & Kaspar, T. (2017, 20. März). Soziologe: Darum haben Trump und die AfD so viel Erfolg. Merkur. https://www.merkur.de/politik/interview-prof-dr-hartmut-rosa-ueber-resonanz-wirksamkeit-afd-donald-trump-und-populismus-zr-7313606.html. Zugegriffen: 11. Feb. 2020.
Schmidt, M.G. (2016). *Das politische System Deutschlands*. München: C.H. Beck.

Schneider, J. (2017, 14. Sep.). So aggressiv macht die AfD Wahlkampf auf Facebook. Süddeutsche Zeitung. https://www.sueddeutsche.de/politik/gezielte-grenzverletzungen-so-aggressiv-macht-die-afd-wahlkampf-auf-facebook-1.3664785. Zugegriffen: 11. Feb. 2020.

Schreyer, S. (2017). Geteilte Herrschaft: Obama, die parteipolitische Polarisierung und der Kongress. *Zeitschrift für Außen- und Sicherheitspolitik*, *10*(2), 25–38.

Schwirtz, M. (2017, 21. Sep.). German elections mystery: why no Russian meddling? The New York Times. https://www.nytimes.com/2017/09/21/world/europe/german-election-russia.html. Zugegriffen: 30. Okt. 2018.

Shuster, S. (2017, 9. Aug.). Russia has launched a fake news war on Europe. Now Germany is fighting back. Time Magazine. http://time.com/4889471/germany-election-russia-fake-news-angela-merkel/. Zugegriffen: 20. Okt. 2018.

Silver, C. (2019). Top 20 economies in the world. Investopedia. https://www.investopedia.com/insights/worlds-top-economies/. Zugegriffen: 18. Mai 2019.

von Soest, C. (2014). Democracy prevention: The international collaboration of authoritarian regimes. *European Journal of Political Research*, *54*(4), 623–638.

Starks, T. (2017, 29. Dez.). The latest 2018 election-hacking threat: 9-month wait for government help. Politico. https://www.politico.com/story/2017/12/29/2018-election-hacking-threat-government-help-231512. Zugegriffen: 12. Mai 2019.

Swift, A. (2016, 14. Sep.). Americans' trust in mass media sinks to new low. Gallup. https://news.gallup.com/poll/195542/americans-trust-mass-media-sinks-new-low.aspx. Zugegriffen: 10. Mai 2018.

Taylor, G. (2017, 6 Aug.). After U.S. experience, Germans brace for Russia election mischief and fake news. The Washington Times. https://www.washingtontimes.com/news/2017/aug/6/germany-expects-russia-election-meddling/. Zugegriffen: 10. März 2020.

Tansey, O. (2016). The problem with autocracy promotion. *Democratization*, *23*(1), 141–163.

Tarrance, V. (2017, 11. Jan.). The "divided states of America"? Gallup Polling Matters. http://news.gallup.com/opinion/polling-matters/201728/divided-states-america.aspx. Zugegriffen: 8. Mai 2019.

Tolstrup, J. (2015). Black knights and elections in authoritarian regimes: Why and how Russia supports authoritarian incumbents in post-Soviet states. *European Journal of Political Research*, *54*(4), 673–690.

Villarreal, A. (2016, 13. Okt.). A quick and dirty guide to polls for the 2016 election. NBC. https://www.nbcconnecticut.com/news/politics/Quick-Dirty-Guide-Polls-2016-Elections-396973901.html. Zugegriffen: 10. Mai 2019.

Wissenschaftliche Dienste des Deutschen Bundestages. (2012). Die Wahlsysteme Deutschlands und der USA: Ein Vergleich. Ausarbeitung WD 1-3000/071/12. https://www.bundestag.de/blob/410332/d0700e7d7d732552337f04e3346c23e0/wd-1-071-12-pdf-data.pdf. Zugegriffen: 12. Jan. 2018.

Wissenschaftliche Dienste des Deutschen Bundestages. (2015). Online-Wahlen Erfahrungen in anderen Staaten und (verfassungs-)rechtliche Voraussetzungen für eine Einführung in Deutschland. Ausarbeitung WD 3 - 3000 - 030/14. https://www.bundestag.de/blob/412066/df70d4a9753c21463cff4030d510cf06/wd-3-030-14-pdf-data.pdf. Zugegriffen: 11. Febr. 2020.

Wong, J. C. (2019. 21. Okt.). Facebook discloses operations by Russia and Iran to meddle in 2020 election. The Guardian. https://www.theguardian.com/technology/2019/oct/21/facebook-us-2020-elections-foreign-interference-russia. Zugegriffen: 30. Okt. 2019.

Woyke, W. (2003). Pluralismus. In U. Andersen & W. Woyke (Hrsg.), *Handwörterbuch des politischen Systems der Bundesrepublik Deutschland* (S. 480–481). Opladen: Leske + Budrich.