ATLANTIK-BRÜCKE

DOSSIER

Transatlantische Cyberresilienz bei Wahlen

PROBLEMSTELLUNG - POSITIONEN - KONSEQUENZEN

23. MAI 2019

Transatlantische Cyberresilienz bei Wahlen

Digitale Kommunikationsformen haben den Prozess der politischen Willensbildung in den letzten Jahren grundlegend verändert. Neben neuen Formen der lebendigen Bürgerbeteiligung und direkter Kommunikation in Wahlkampfzeiten eröffnet die Digitalisierung positive Möglichkeiten, demokratische Wahlen zu begleiten, zu analysieren und nachzubereiten. Indem die politische Willensbildung und öffentliche Debatte jedoch zunehmend ins Netz verlagert werden, entstehen zugleich neue Gefahren für die Integrität von Wahlen. Zahlreiche Analysen konzentrieren sich auf die (technische) Einflussnahme auf Wahlen durch Cyberattacken, insbesondere durch Hacking. Andere Untersuchungen legen ihren Fokus dagegen auf die Beeinflussung durch Desinformation und Fake News. Ausgehend von der russischen Einflussnahme auf die Präsidentschaftswahl in den Vereinigten Staaten im Jahr 2016 stellt sich hier vor allem die Frage, wie Manipulationen und Desinformationskampagnen ablaufen und was sie als konzertierte Aktion bewirken sollen. Das vorliegende Dossier zeichnet die bisherige Entwicklung dieser Bedrohung nach. Es fasst zentrale Problemstellungen und die Positionen betroffener Länder zusammen. Auch erste bereits gezogene und weitere mögliche Konsequenzen zur Stärkung der Cyberresilienz bei Wahlen werden diskutiert. Ein besonderes Augenmerk liegt auf der Frage, welche Handlungsfolgen sich in diesem Zusammenhang für die transatlantische Kooperation ergeben bzw. ergeben könnten. Das Papier stützt sich im Wesentlichen auf exklusive Interviews mit Fachexperten von beiden Seiten des Atlantiks.

EINFLUSSNAHME AUF DIE US-PRÄSIDENTSCHAFTSWAHL 2016

Die US-Präsidentschaftswahl 2016 hat der Weltöffentlichkeit vor Augen geführt, welche Macht und welches Bedrohungspotenzial Cyberattacken besitzen. Die Angriffe aus Russland auf das Kommunikationssystem der Parteizentrale der Demokraten und anschließende über Social Bots – per Software automatisch agierende Profile in sozialen Netzwerken – und Trolle gesteuerte Fake News hatten Einfluss auf den Wahlkampf und den Wahlausgang in den USA. Dies ergab eine geheimdienstliche Untersuchung von FBI, CIA und NSA sowie des US-Heimatschutzministeriums, die noch Präsident Barack Obama angeordnet hatte. Daraufhin sprach zunächst die US-Regierung Sanktionen gegen den russischen Inlandsgeheimdienst FSB aus und, im Juni 2017, der US-Senat gegen russische Einzelpersonen und Organisationen. Die Administration unter Präsident Donald Trump verhängte am 19. Dezember 2018 ihrerseits Sanktionen gegen 15 Mitarbeiter des russischen Militärgeheimdienstes GRU und gegen diverse russische Unternehmen. Als Begründung für diesen Schritt nannte das US-Finanzministerium unter anderem die russischen Manipulationsversuche im US-Präsidentschaftswahlkampf 2016. In den Geheimdienstausschüssen des Abgeordnetenhauses und des Senats laufen derzeit noch weitere Untersuchungen. Der Abschlussbericht des Sonderermittlers Robert Mueller kommt unter anderem zu dem Ergebnis, dass sich die russische Regierung „in weitreichender und systematischer Weise“ in die Präsidentschaftswahl eingemischt hat.

Wie liefen die Cyberattacken und Fake-News-Kampagnen in den USA ab?

Die Einflussnahme auf die US-Präsidentschaftswahl 2016 ist ein hervorstechendes Beispiel für die Art der Bedrohung, der westliche Demokratien heute ausgesetzt sind. So ist es den Angreifern nachweislich gelungen, zunächst das zentrale Kommunikationssystem des Democratic National Committee zu hacken, um dann eine Cyberattacke auf den E-Mail-Server von Hillary Clintons Wahlkampfchef John Podesta durchzuführen, dessen E-Mails zu verbreiten und anschließend eine darauf gestützte Kampagne mit Fake News zu initiieren.

Die weitere Entwicklung des Hackings, das im Kern gegen die Kandidatin Hillary Clinton gerichtet war, steht exemplarisch dafür, wie Datendiebstahl und die destruktive Verbreitung von personenbezogenen und vertraulichen Daten ablaufen können. In mehreren Etappen wurden kompromittierende Informationen über interne Vorgänge der Demokratischen Partei und insbesondere des Democratic National Committee veröffentlicht. Einige dieser Informationen stellten die Neutralität des Komitees im Nominierungsprozess des offiziellen Bewerbers um das Amt des Präsidenten in Frage.

Der eigentliche Schauplatz der Cyberattacken lag einige Tausend Kilometer östlich von Washington, D.C. entfernt. Denn während des Wahlkampfes von 2016 kreierten Mitarbeiter in einer Troll-Fabrik und Bot-Farm in St. Petersburg namens

„Internet Research Agency“ massenhaft Fake-Accounts bei Facebook und Twitter. In diesen Konten gaben die beteiligten Akteure vor, amerikanische Staatsbürger zu sein. Sie verbreiteten über diese Social-Media-Accounts unablässig Verschwörungstheorien, Desinformation und politisch spaltendene Inhalte mit dem klaren Ziel, die erkennbare gesellschaftliche Polarisierung in den USA zu verstärken. Opponierende Gruppen wurden emotional aufgestachelt und gegeneinander ausgespielt. Der Kreml und russische Geheimdienste unterstützten die Troll-Fabrik zwar wohlwollend, ihr eigentlicher Gründer und Manager jedoch war der russische Oligarch Jewgeni Prigoschin.

> Die „Internet Research Agency“, eine Troll-Fabrik und Bot-Farm in St. Petersburg, kreierte massenhaft Fake-Accounts und erreichte allein bei Facebook 125 Millionen Amerikaner.

Die Bilanz der „Internet Research Agency“ im amerikanischen Wahlkampf des Jahres 2016 offenbart die ganze Wucht der Cyberattacke: Schätzungsweise 36.000 automatisierte Bot-Konten bei Twitter richtete die Troll-Fabrik ein. Allein bei Facebook erreichte der durch die russische Troll-Fabrik und Bot-Farm produzierte Inhalt 125 Millionen Amerikaner. Dies sagt zwar noch nichts über die qualitative Wirkung der russischen Kampagne aus – doch die aus dem Ausland gesteuerte Einflussnahme auf die wichtigste Wahl der Vereinigten Staaten ist ein unverrückbarer Fakt.

Warum ist der Fall der US-Wahlen 2016 nicht nur eine Frage der nationalen Sicherheit der Vereinigten Staaten?

Cyberattacken auf demokratische Wahlen betreffen zuerst die innenpolitische Stabilität eines Staates und die Funktionsfähigkeit eines demokratischen Systems, insofern die Integrität einer freien, gleichen und geheimen Wahl in ihren Grundfesten erschüttert wird. Die technologische Natur der Angriffe und Desinformationskampagnen wirft zudem die Frage auf, wie Staaten mit sozialen Medien und digitalen Plattformen umgehen und diese regulieren. Lassen sich Cyberangriffe als konzertierte und strategische Aktionen aus dem Ausland identifizieren, zeigt sich deren außen- und sicherheitspolitische Dimension. Denn der Schutz von demokratischen Wahlen ist eine Frage der nationalen Sicherheit.

Kann ein Staat seine Wahlen nicht ordnungsgemäß durchführen, ist seine Legitimität, Reputation und folglich auch seine Handlungsfähigkeit nach außen beschädigt. Fest steht: Die Souveränität eines demokratischen Staates wird akut bedroht, wenn der Wahlprozess beeinflusst und das freie Wahlrecht seiner Bürger behindert wird. Die digitale Beeinflussung der US-Wahl, deren Ausmaß erst im Zuge der intensiven Untersuchungen der letzten Monate deutlich wurde, kann daher als ein Angriff auf das demokratische System und die Integrität von Wahlen in der westlichen Welt insgesamt gewertet werden.

Wie reagierte die US-Regierung auf die Bedrohung durch ausländische Einmischungen?

Dass die Angriffe auf die amerikanische Präsidentschaftswahl 2016 kein Einzelfall waren, wurde sehr schnell klar. Bereits am 14. Februar 2018 äußerten der damalige CIA-Direktor und spätere Außenminister Mike Pompeo, NSA-Chef Mike Rogers und der nationale Geheimdienstdirektor Dan Coats im Geheimdienstausschuss des Senats ihre mit neuen Erkenntnissen untermauerte Erwartung, dass sich Russland auch in die Midterm Elections 2018 einzumischen versuche. Zu diesem Zeitpunkt waren die Manipulationen der Präsidentschaftswahlen allerdings noch nicht aufgearbeitet.

Nur zwei Tage später erhob das FBI Anklage gegen 13 russische Staatsbürger und drei russische Organisationen wegen Konspiration, Betrugs unter Einsatz von Kommunikationsmitteln, Bankbetrugs und schwerer Fälle von Identitätsdiebstahl. Die Russen sollen sich als US-Bürger ausgegeben haben. Dem FBI zufolge zielten die russischen Aktionen bei der US-Wahl von 2016 darauf, die amerikanische Wählerschaft entweder zu beeinflussen oder ihr Vertrauen in das Wahlsystem der Vereinigten Staaten zu unterminieren.

Am 12. September 2018, wenige Wochen vor den Zwischenwahlen, unterzeichnete US-Präsident Trump ein Dekret, das die amerikanischen Geheimdienste zu einer stetigen Prüfung von ausländischen Einmischungen in US-Wahlen anhält. Weisen die Nachrichtendienste Angriffe nach, sollen diese Erkenntnisse innerhalb eines definierten Zeitfensters schnell zu Sanktionen führen. Geheimdienstdirektor Dan Coats

zufolge zielt der Erlass nicht ausschließlich auf russische Aktionen. China, Nordkorea und der Iran gehören demzufolge ebenfalls zu den Staaten, die für die Urheberschaft von Fake News und Cyberattacken auf demokratische Institutionen verantwortlich sein sollen. Im Gegensatz zur Phase vor der Präsidentschaftswahl 2016 sei generell die Intensität ausländischer Einmischungsversuche in den demokratischen Prozess vor den Zwischenwahlen 2018 nicht so deutlich ausgeprägt gewesen. Der nationale Sicherheitsberater John Bolton teilte mit, dass diesem „wichtigen Schritt des Präsidenten" auch ein Gesetz aus dem Kongress folgen könnte. Die Adminstration sei bereit, sich mit dem Parlament zu beraten.

„Bedauernswerterweise sind wir zu dem Schluss gekommen, dass China versucht hat, sich in unsere bevorstehende Wahl 2018 einzumischen", sagte Präsident Trump während seines Vorsitzes des UN-Sicherheitsrates am 26. September 2018. „Die Chinesen wollen nicht, dass ich oder wir gewinnen, weil ich der erste Präsident aller Zeiten bin, der China beim Handel herausfordert", so Trump. Vize-Präsident Mike Pence zufolge visierte die Volksrepublik mehr als 80 Prozent derjenigen Wahlkreise an, die 2016 mehrheitlich für Trump als Präsidenten stimmten. China bestritt die erhobenen Vorwürfe am 5. Oktober 2018 in Person von Außenminister Wang Yi.

Welche Auffälligkeiten gab es im Vorfeld der Bundestagswahl 2017?

Vor dem Hintergrund der wachsenden Bedrohung durch Cyberangriffe in allen westlichen Demokratien ist eine stärkere Kooperation und ein systematischer Wissensaustausch zwischen den westlichen Allianzpartnern dringend geboten. Heute wissen wir: Nicht nur die USA haben Cyberattacken auf ihre Präsidentschaftswahl 2016 erlebt, auch Deutschland wurde beim Bundestagswahlkampf 2017 zum Ziel digitaler Angriffe – wenn auch in weitaus geringerem Maße als die Vereinigten Staaten.

Im Vorfeld der Bundestagswahl zielten russische Akteure mittels massenhafter Verbreitung von Fake News darauf, den demokratischen Prozesses zu destabilisieren. Den Angreifern ging es nicht in erster Linie darum, einer bestimmten Partei oder einem bestimmten Kandidaten zum Wahlerfolg zu verhelfen. Zu diesem Schluss kam unter anderem der Präsident des Bundesnachrichtendienstes (BND), Bruno Kahl.

> Die Bundestagswahl ist keine Zweiparteien-Konstellation und damit besser geschützt als die Wahl des US-Präsidenten.

Allerdings ist ein Mehrparteiensystem wie in Deutschland grundsätzlich weniger leicht zu unterwandern, sagt Jörg Forbrig, Senior Transatlantic Fellow des German Marshall Fund of the United States (GMF): „Eine politische Debatte in einem Land wie der Bundesrepublik zu manipulieren, das zudem ein relativ starkes und stabiles Qualitätsmediensystem hat, ist kompliziert." Die Bundestagswahl sei eben keine Zweiparteien-Konstellation oder eine binäre Konstellation, wie etwa im Fall eines Referendums, und damit per se besser geschützt.

Im Vorfeld der Bundestagswahl von 2017 zeigte sich, dass diese an einer anderen, nicht minder empfindlichen Stelle grundsätzlich manipulierbar ist: Hacker demonstrierten öffentlich, welche Schwachstellen die Software aufweist, die Auszählungsergebnisse bündelt und überträgt.

MOTIVE, ZIELE UND ANGRIFFSARTEN VON CYBERATTACKEN UND DESINFORMATIONSKAMPAGNEN BEI WAHLEN

Die logische Konsequenz aus der zunehmenden Digitalisierung wesentlicher Teile des Wahlkampfes und des Wahlprozesses ist, dass sie stärker anfällig für Cyberattacken und Desinformationskampagnen sind. Angreifer haben erkannt, dass sie mit Cyberoperationen ein vergleichsweise günstiges und zugleich effektives Mittel nutzen können, um Wahlvorgänge in westlichen Staaten zu manipulieren. Es ist damit zu rechnen, dass Cyberangriffe auf Wahlen in Zukunft zunehmen und, in technischer Hinsicht, immer ausgefeilter und komplexer werden. Eine umfassende Analyse existierender und möglicher Cyberattacken, die Bündelung verfügbarer Informationen hierzu sowie die Entwicklung effektiver Abwehrstrategien, auch in Abstimmung mit westlichen Allianzpartnern, ist daher dringend geboten.

Eine Analyse der Angriffspunkte möglicher Cyberangriffe auf Wahlen beginnt mit der Frage, welche Daten in digitaler Form vorliegen. Man unterscheidet hier grundsätzlich zwischen öffentlich zugänglichen Wahldaten und perso-

nenbezogenen Daten. Es ist eine Aufgabe der Behörden, diejenigen persönlichen Daten zu kennen, mit denen sich Wähler ansprechen und identifizieren lassen. Dabei handelt es sich etwa um E-Mail-Adressen, die im Wahlkampf für Desinformationskampagnen mit Fake News missbraucht werden können.

Was bezwecken Angreifer mit Attacken auf demokratische Wahlen?

Hinter Cyberattacken auf Wahlen können sehr unterschiedliche Motive und Zielsetzungen stehen. Die gravierendste Form der Manipulation zielt darauf, die Stimmenauszählung auf digitalem Wege zu verfälschen. Zudem können Angreifer das Ziel verfolgen, einzelne Politiker oder ganze Parteien öffentlich zu diskreditieren. Das übergeordnete Motiv ist, den demokratischen Prozess in seiner Gesamtheit zu delegitimieren und so das Vertrauen der Bürger in eine Wahl zu unterminieren. Zu den strategischen Motiven von Cyberangriffen auf Wahlen zählt des Weiteren, Mitglieder der Regierung oder deren Vertreter gezielt einzuschüchtern. Die internationale Glaubwürdigkeit von Staaten und ihren Institutionen soll so untergraben werden.

> Die technische Manipulation des Wahlergebnisses ist ein besonders schwerwiegender Fall.

Ein besonders schwerwiegender Fall von Wahlbeeinflussung besteht in der technischen Manipulation des Wahlergebnisses. Ein solcher Eingriff kann dadurch erfolgen, dass die Ergebnisse der Auszählung oder Wählerverzeichnisse verändert werden. Letzteres hat zur Folge, dass Wahlberechtigte nicht mehr für eine bestimmte Partei oder einen spezifischen Kandidaten votieren können. Manipuliert ein Angreifer zum Beispiel die im Wählerverzeichnis hinterlegte Adresse eines Wählers, kann dies dazu führen, dass dieser nicht mehr im eigenen Wahlbezirk oder per Briefwahl abstimmen kann. Auch die in Datensätzen eingetragene Parteizugehörigkeit lässt sich manipulieren. In dem Fall können Wähler also nicht mehr an Parteiwahlen wie den Vorwahlen in den USA oder den deutschen Urabstimmungen über Koalitionen teilnehmen.

Bei der Delegitimierung des demokratischen Prozesses geht es im Kern darum, mit Cyberattacken Zweifel am ordnungsgemäßen Ablauf einer Wahl hervorzurufen. Solche Zweifel können in der Öffentlichkeit bereits dadurch entstehen, dass die IT-Systeme und die technische Infrastruktur einer Wahl als manipulierbar wahrgenommen werden. Es kommt durchaus vor, dass sensible Informationen zu Wählerverzeichnissen, Wahlmaschinen und der Software zur Stimmauszählung öffentlich bekannt werden. Es gilt deshalb, Schwachstellen des Wahlprozesses aufzuspüren und so gut wie möglich gegen Cyberattacken abzusichern.

Die Diskreditierung politischer Akteure kommt in der Regel dadurch zustande, dass durch Cyberattacken gewonnene Informationen etwa in Form von Dokumenten oder privaten Mitteilungen und Social-Media-Inhalten verbreitet werden. Dies lässt Politiker potenziell in schlechtem Licht erscheinen. Ein prominentes Fallbeispiel ist die Veröffentlichung vertraulicher E-Mails von Hillary Clintons Wahlkampfchef John Podesta im US-Präsidentschaftswahlkampf 2016. Das Leaken kompromittierender Dokumente wird dann besonders gefährlich, wenn die beschafften Informationen verfälscht, als Fake News verbreitet und bestimmten Zielgruppen zugespielt werden. In diesem Fall liegt eine Kombination von Cyberangriff und anschließender Desinformationskampagne vor. Hier Gegenmaßnahmen einzuleiten, ist schwierig und meist wenig effektiv. Denn einmal verbreitete Falschnachrichten zu korrigieren, ist zeitintensiv und selten so erfolgreich wie deren Verbreitung.

Welche typischen Angriffsmuster auf Wahlen sind erkennbar?

Aus den unterschiedlichen Motiven und Zielen von Cyberattacken auf eine demokratische Wahl leiten sich differenzierte Angriffsarten ab. Die Daten stehen hierbei stets im Mittelpunkt. Die interne Kommunikation von Wahlkampfzentralen politischer Parteien, Daten über das Wählerverhalten in sozialen Medien oder auch öffentlich zugängliche Informationen für Wähler können entweder gestohlen, geleakt, manipuliert oder auch blockiert werden. Neben Leaks, Manipulationsangriffen und Distributed-Denial-of-Service-Attacken gehören auch Ausspähungsoperationen, Erpressungen und Überzeugungskampagnen zu den wesentlichen Angriffsarten im Umfeld von Wahlen.

> Daten in Wählerverzeichnissen dienen Wahlkampfstrategen für das Targeted Campaigning und sind zugleich ein sensibler Angriffspunkt.

Das Vertrauen der Bevölkerung in das politische System wird geschwächt, wenn Angreifer die Verwundbarkeit von Wahlmaschinen aufzeigen, die Integrität des Wählerverzeichnisses in Zweifel ziehen oder vertrauliche Daten kompromittieren. Dabei stellen Leaks eine der gängigsten Angriffsvarianten dar.

Die in Wählerverzeichnissen gespeicherten Daten sind besonders sensibel und ein geeigneter Angriffspunkt. Die Angreifer machen es sich zunutze, dass Politiker und Parteien in Wahlkampfzeiten zunehmend auf genau diese Daten setzen, um ihre Kampagnen gezielt auf die verschiedensten Wählergruppen zuzuschneiden. So durchsuchen beim Targeted Campaigning Algorithmen Wählerverzeichnisse nach bestimmten Kriterien, um zielgerichtet Wahlwerbung über die sozialen Medien verbreiten zu können.

Bei Angriffen werden diese Wähler-Daten manipuliert und die politische Kampagne auf andere, nicht so sehr im Fokus stehende Wählergruppen abgelenkt, oder die Wahlwerbung an sich wird im Zuge einer Desinformationskampagne verfälscht. Eine weitere Variante besteht darin, Wähler durch Micro-Targeting mit gestohlenen Informationen zu beeinflussen. Man spricht in diesem Zusammenhang auch von Präzisionspropaganda.

Welche Maßnahmen zum Schutz demokratischer Wahlen sind effektiv?

Ein zentrales Charakteristikum von Cyberattacken und Desinformationskampagnen ist, dass die Angreifer weitgehend anonym und äußerst flexibel vorgehen. Es nimmt weit mehr Ressourcen in Anspruch, Fake News als solche zu identifizieren und dem Urheber zuzuordnen, als diese herzustellen. Eine schnelle Reaktion und Gegenwehr ist mithin eine große Herausforderung. Meistens sind Cyberattacken der Cyberabwehr außerdem technologisch einen Schritt voraus. Digitale Abwehrmaßnahmen sind insgesamt noch wenig ausgereift und gelten als weithin unerforscht.

Technologische Resilienz stärken

Welche Formen der Abwehr sind effektiv? An erster Stelle steht der Schutz des technischen Ablaufs von Wahlen. Insbesondere mit Blick auf die USA läge eine simple, aber effektive Abwehrmaßnahme im vollständigen Verzicht auf elektronische Wahlmaschinen. Bei der US-Präsidentschaftswahl 2016 haben immerhin circa 30 Prozent der Wähler ihre Stimme an einer Wahlmaschine abgegeben. Ein Verzicht auf Wahlmaschinen käme allerdings einem technologischen Rückschritt gleich und lässt sich langfristig kaum empfehlen.

Eine zwingende Abwehrmaßnahme gegen digitale Angriffe auf Wahlen besteht folglich darin, die technologischen Sicherheitsstandards zu erhöhen. Wie dies konkret umgesetzt werden könnte, sollte eine gemeinsame Aufgabe von zuständigen Behörden wie in Deutschland etwa dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und an digitaler Wahlinfrastruktur beteiligten Unternehmen sein. Da Hacks auf den Zugang zu Daten abzielen, ist Datenschutz ein elementarer Bestandteil der Sicherheitsarchitektur von Wahlen.

Datenintensive Wahlen werden zum einen durch öffentlich zugängliche Wahldaten definiert. Dazu zählen Wahlergebnisse, diverse tabellarische Aufbereitungen der Wahlergebnisse, Informationen über Kandidaten, Statistiken über die Parteizugehörigkeit der Wähler und Informationen über Wahlkampfausgaben. Auch Zensusdaten, Karten, Erkenntnisse zu zurückliegenden Wahlentscheidungen von Wählern, Parteiprogramme und allgemein zugängliche Informationen auf den Seiten lokaler Wahlbüros gehören in diese Datengruppe. Es ist dringend geboten, die Integrität dieser Daten zu schützen.

Zum anderen spielen personenbezogene Daten eine große Rolle in datenintensiven Wahlen. Regierungen und Wahlkampfstrategen sammeln in einem erheblichen Umfang personenbezogene Daten von Wählern. Dies birgt immer auch Missbrauchsgefahren für den Wahlprozess. Infolge einer Cyberattacke kann es zu einem Identitätsdiebstahl kommen, oder Fake News über die Wahl, die Parteien, die Kandidaten und die Themen der Wahl können gezielt verbreitet werden. Es ist daher besonders wichtig, den Cyberattacken mit optimierten informationstechnischen Absicherungen – beispielsweise Firewalls, Intrusion Detection Software und Verschlüsselungen – zu begegnen.

> Firewalls, Intrusion Detection Software und Verschlüsselungen bieten einen defensiven IT-Schutz. Offensive Gegenschläge sind dagegen in Deutschland illegal.

Ob Parteien oder Regierungen technisch und strategisch in der Lage sein und befähigt werden sollten, Gegenangriffe auszuführen, ist eine äußerst sensible Frage. Offensive Gegenschläge im Cyberfeld, die als Counter-Hacking und Hackback bezeichnet werden, sind derzeit in Deutschland keine Option, da sie illegal sind. „Die Quasi-Revanche oder auch präventive Erstschläge sind – bis auf sehr wenige Ausnahmen – in unseren demokratischen Rechtsstaaten nicht machbar", stellt Jörg Forbrig vom GMF fest.

Internationale und sektorübergreifende Initiativen bilden

Aus einer Reihe von internationalen und sektorübergreifenden Initiativen und Gremien soll hier exemplarisch ein Projekt vorgestellt werden. Unter anderem um technische Schutzmechanismen zu vereinheitlichen, hat die Münchner Sicherheitskonferenz (MSC) die „Charter of Trust" ins Leben gerufen, eine Initiative in Kooperation mit führenden Unternehmen (Siemens sowie IBM, Dell, Cisco, Atos, Deutsche Telekom, Airbus, Daimler, Allianz, das Mineralölunternehmen Total, die Energieunternehmen Enel und AES Corporation, der Halbleiterhersteller NXP, TÜV Süd und der Warenprüfkonzern SGS). Mit dieser Initiative wollen diese Akteure „allgemeine Mindeststandards für Cyber-Sicherheit etablieren, die sich am Stand der Technik orientieren".

Die Charta verfolgt drei ambitionierte und höchst relevante Ziele: Erstens sollen die Daten von Einzelpersonen und Unternehmen geschützt werden. Zweitens soll Schaden von Personen, Unternehmen und Infrastrukturen abgewendet werden. Und drittens soll ein festes Fundament geschaffen werden, in dem das Vertrauen der Bevölkerung in die digitale Welt verankert werden kann. Unter der Ägide von Frankreichs Staatspräsident Emmanuel Macron unterstützen mittlerweile viele andere Staaten, Unternehmen und zivilgesellschaftliche Organisationen den beim Pariser Peace Forum 2018 verabschiedeten Appell für Vertrauen und Sicherheit im Cyberspace.

Social-Media-Expertise der Parteien ausbauen

Da die sozialen Medien der zentrale Verbreitungskanal von Fake News sind, sind die politischen Parteien gut beraten, ihre Ressourcen in den sozialen Netzwerken erheblich zu erhöhen. Professionelle Expertise von außen wird dafür ebenso benötigt wie der Einsatz jüngerer und digitalaffiner Mitglieder und Anhänger. Undemokratischen, illiberalen und autoritären Akteuren sollte also nicht wehrlos die Hoheit über die sozialen Medien überlassen werden.

Factchecking und Medienkompetenz erweitern

Medienhäuser sollten zunehmend über die Kapazitäten verfügen, Cyberattacken und Desinformationskampagnen aufzudecken und abzuwehren. Das heißt, Medienorganisationen sollten ihre Ressourcen innerhalb von Recherche-Einheiten verstärken und das Factchecking deutlich ausbauen. Beispielsweise haben die Washington Post und die New York Times Factchecking-Teams aufgebaut, die unter anderem den Wahrheitsgehalt von Inhalten in den sozialen Netzwerken prüfen. Dies hat zur Folge, dass Fake News mit geringerer Wahrscheinlichkeit in die Berichterstattung gelangen.

Im Bereich der Bildungspolitik empfiehlt sich die in den Curricula verankerte Stärkung der Medienkompetenz von Kindern und Jugendlichen – insbesondere mit Blick auf Fake News. Dies bedeutet, in den Schulen den kritischen Umgang mit Nachrichten und allen anderen journalistischen Genres sowie deren digitale Verbreitungsformen zu vermitteln.

Im Schadensfall ganzheitlich reagieren

Strategien zum Schutz von Wahlen sollten generell auf eine ganzheitliche Resilienz abzielen, sowohl was die Maßnahmen als auch die beteiligten Akteure betrifft. Dies bedeutet, dass einerseits vor allem technische Sicherheitsstandards erhöht werden und dass andererseits Maßnahmen ergriffen werden, die den Schaden eines möglichen Angriffes minimieren.

Kommunikative Strategien bei Zwischenfällen, an die Bevölkerung gerichtete, aufklärende Informationskampagnen und internationale Kooperation zwischen Regierungen wie in der Initiative der European Cyber Rapid Response Force von sieben EU-Staaten unter Führung Litauens zählen hier zu den naheliegenden Abwehrmaßnahmen. Auch hierzulande sollte mit den Risiken offen und transparent umgegangen werden,

indem die Behörden Versuche von externer Einflussnahme auf Wahlen in der Bundesrepublik veröffentlichen und unverzüglich polizeilich und juristisch verfolgen.

POTENZIALE TRANSATLANTISCHER KOOPERATION IN DER CYBERRESILIENZ BEI WAHLEN

Ein übergeordnetes Ziel aller westlichen Demokratien sollte darin bestehen, ihre Resilienz gegen die digitale Einflussnahme auf Wahlen robuster zu gestalten. Dabei sollte dies- und jenseits des Atlantiks klar sein: Nur ein gesamtgesellschaftlicher Ansatz bei dieser Form der Widerstandsfähigkeit, der alle relevanten Akteure einbezieht, ist erfolgversprechend. Denn dies erhöht die Wahrscheinlichkeit, das Bewusstsein für diese Gefahren für den Fortbestand der Demokratie auf allen Ebenen zu schärfen und effektive Gegenmaßnahmen umzusetzen. Sowohl für die Vereinigten Staaten als auch für die Europäische Union geht es in der Zusammenarbeit darum, dass die viel beschworene „wehrhafte Demokratie" eine zeitgemäße Anpassung erfahren muss.

Wie sollte eine ganzheitliche transatlantische Cyberresilienz ausgestaltet sein?

Die gravierenden Vorfälle im Zuge der US-Präsidentschaftswahl 2016 und die bedenklichen Auffälligkeiten vor der Bundestagswahl 2017 belegen, dass der Schutz von demokratischen Wahlen vor Cyberattacken bisher nicht ausreichend war. Die Vereinigten Staaten von Amerika und die Europäische Union sind auf den Ebenen von Personal, Infrastruktur und Strategie nicht optimal ausgestattet, um auf die zunehmend von Künstlicher Intelligenz (KI) getriebene, asymmetrische Kriegsführung im Informationsraum adäquat zu antworten. Die Angreifer befinden sich in einer vorteilhaften Position, wenn man sich vergegenwärtigt, dass schon heute die KI-Software zur Manipulation von Audio- und Videomaterial frei verfügbar ist. Damit lassen sich „Deep Fakes" herstellen, die immer aufwendiger als solche zu erkennen sind.

Kooperation der Geheimdienste ausbauen

Der Ausbau einer kohärenten innereuropäischen Cyber-Sicherheitsstrategie ist unverzichtbar, um den Bedrohungen der demokratischen Institutionen angemessen zu begegnen. Aber auch der Brückenschlag über den Atlantik ist – ungeachtet der Spannungen in anderen Politikfeldern – dringend angezeigt und im beiderseitigen Interesse der USA und der Europäischen Union. Insbesondere mit Blick auf die Integrität von Wahlen sowie den Schutz demokratischer Prozesse und Institutionen sollten die westlichen Allianzpartner Informationen über konkrete Bedrohungen zwischen ihren Geheimdiensten austauschen, Best Practices etablieren und sich bei Abwehrmaßnahmen effektiv unterstützen. An einem strukturierten Cyberdialog könnten neben den Nachrichtendiensten auch Behörden mit konkreten Kontaktpersonen wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das U.S. Department of Homeland Security beteiligt sein.

> Michael Chertoff, früherer U.S. Secretary of Homeland Security, plädiert für eine transatlantisch fundierte Analyse der Angriffsmuster im Cyberraum.

Der frühere U.S. Secretary of Homeland Security, Michael Chertoff, ist heute gemeinsam mit dem ehemaligen NATO-Generalsekretär Anders Fogh Rasmussen Co-Vorsitzender der Transatlantic Commission on Election Integrity. Bei dieser überparteilichen und sektorübergreifenden Kommission handelt es sich um eine im Jahr 2018 ins Leben gerufene Initiative der politischen Nichtregierungsorganisation Alliance of Democracies Foundation mit Sitz in Washington, D.C. und Kopenhagen. Chertoff hält fest: „Having a collaboration on sharing information about the nature of the threats that are coming, information about the tactics that the attackers are using and that we are seeing in various countries and information about IP addresses that are being used to launch attacks, is an important element." Für Chertoff ist es offensichtlich, dass eine transatlantisch fundierte Analyse der Angriffsmuster im Cyberraum größere Erfolgsaussichten hätte, als wenn jeder Partner für sich arbeiten würde: „The more data you have, the better your analytics work. If we can look at what is going on in Europe and the US and combine that, we have a better opportunity to identify malicious information."

Die operationelle Basis einer solchen Zusammenarbeit zwischen den USA und der EU würde Chertoff in einem Knotenpunkt oder einem Exzellenzzentrum verorten, in dem verschiedenste Geheimdienste ihre Erkenntnisse in Echtzeit miteinander teilen. Den angemessenen Rahmen für eine

derartige Kooperation sieht er derzeit in der NATO. Deutschland müsste dazu über die nötigen Aufklärungskapazitäten verfügen. Diese werden im internationalen Vergleich als unzureichend eingeschätzt. „Es gibt kaum Situationen, in denen Deutschland in diesem Feld nicht auf die Hilfe anderer, insbesondere von Seiten der USA, angewiesen ist", betont Jörg Forbrig. Aus seiner Sicht stehen allerdings Erfahrungen wie die NSA-Affäre einer intensiveren westlichen Arbeitsteilung der Geheimdienste entgegen, da „sehr viel öffentliches wie institutionelles Vertrauen zerstört wurde".

Hinzu kommen zwei weitere aktuelle Herausforderungen: Zum einen gilt die Partnerschaft der verschiedenen Dienste im internationalen Raum untereinander als sehr angespannt. Viele Partner der Vereinigten Staaten wüssten derzeit nicht, ob sie der amerikanischen Administration noch trauen können und ob sie deren Diensten bestimmte Informationen anvertrauen können, sagt Forbrig.

Zum anderen sorgt der Brexit auch auf diesem Politikfeld für Komplikationen. Großbritannien verfügt über leistungsstarke Geheimdienste und ist im Five-Eyes-Verbund englischsprachiger Länder ein führendes Mitglied. „Vor dem Hintergrund des Brexits stellt sich für die Kontinentaleuropäer die Frage, inwiefern diese auch auf die geheimdienstliche Zusammenarbeit mit den Briten weiterhin zählen können", erläutert Forbrig.

Öffentlich-private IT-Partnerschaften fördern

Neben einer intensivierten und verbesserten Zusammenarbeit der Geheimdienste im transatlantischen Kontext wäre es sehr vorteilhaft, wenn die USA, Deutschland und weitere europäische Staaten gemeinsam und mit Hilfe von führenden IT-Unternehmen international gültige Standards für sichere, bei Wahlen zum Einsatz kommende Technologien entwickeln, zertifizieren und etablieren würden. Dies könnte in Form einer öffentlich-privaten IT-Partnerschaft erfolgen.

„You could establish a situation in which the best kinds of tools are available", so Michael Chertoff. Er sieht vor allem im Umgang mit „Deep Fakes" gemeinsamen Handlungsbedarf von Amerikanern und Europäern: „It would make a lot of sense putting together a joint project to figure out how to detect in real time what is artificial and to combat that. If we put our best brains together from Europe and the US, that would be a very positive development."

Philipp Krüger, Managing Director des National Digital Hub Cybersecurity am Fraunhofer-Institut für Sichere Informationstechnologie der TU Darmstadt, stimmt Chertoff zu und hält es für schlüssig, auf automatisierte Angriffe mit einer „automatischen, softwaregestützten Validierung" zu antworten, da menschliche Response-Teams nicht schnell genug reagieren könnten. Dabei gehe es um algorithmische Lösungen, die Angriffe erkennen, diese je nach Schwere der Attacke beurteilen und filtern sowie Antworten kreieren.

Dabei müssten die Partner zunächst grundsätzlich klären, wie genau internationale IT-Standards aussehen sollen, wie sie begründet werden und wie gewährleistet wird, dass sich die beteiligten Unternehmen an diese vertraglich vereinbarten Standards halten. Jörg Forbrig warnt insbesondere bei der Frage der Begründung solcher Standards vor kontraproduktiven Schritten: „Russland hat zum Beispiel Kontakte und Kooperationsformen mit Rechtsradikalen und Rechtspopulisten in ganz Europa und den Vereinigten Staaten kultiviert. Wenn wir solche internationalen Kontakte ausschließen wollen, dann heißt das rechtsstaatlich, dass wir die Kooperationsformen, die demokratische Parteien international haben, möglicherweise mitbeeinträchtigen." Demokratien lebten davon, dass sie offen seien und sich in ihren Debatten, Kontakten und Mechanismen nicht abschotteten – noch dazu in einer vernetzten Welt.

Freiwillige Selbstverpflichtung der Plattformen fordern

Ein sensibler Punkt in der Diskussion über IT-Standards bei Wahlen ist, inwiefern sich Unternehmen an ihre Pflichten bei der Einhaltung dieser Standards halten. Das hängt damit zusammen, dass nicht nur Technologiekonzerne aus westlichen Ländern, insbesondere den USA, sondern vor allem chinesische Unternehmen auf diesem Markt eine Lücke füllen wollen. Einen Ansatz zur freiwilligen Selbstregulierung kann man seit Oktober 2018 erkennen, als unter anderem Facebook, Twitter, Google, Microsoft und Mozilla den „Code of Practice on Disinformation" unterzeichneten. Mit diesem Verhaltenskodex einigten sich die beteiligten Unternehmen darauf, gegen Fake News und Bot-Accounts vorzugehen.

So erlaubt Facebook zur Wahl des Europäischen Parlaments in den Timelines seiner User nur noch politische Wahlwerbung von Parteien aus dem jeweiligen Land, in dem diese zur Wahl antreten und in dem die Nutzer registriert sind. Ähnlich wie

Facebook weist auch Twitter seine User darauf hin, wenn es sich bei Inhalten um falsche Informationen handelt oder Quellen wenig glaubwürdig erscheinen. Die schärfste Maßnahme von sozialen Netzwerken besteht allerdings neben dem Sperren von Accounts im Löschen von Seiten. Michael Chertoff plädiert im Hinblick auf die Europa-Wahl dafür, dass Plattformen und Suchmaschinen diejenigen Seiten aus dem Netz nehmen, die Desinformationskampagnen beinhalten: „Building the capability to expose and identify deliberate disinformation campaigns that have been artificially manipulated and having the platforms shut down, is going to be an important factor."

Zusammenarbeit auf militärischer Ebene stärken

Auch das Militär kann einen Beitrag zu einer effektiven transatlantischen Cyberresilienz bei Wahlen leisten. Im Jahr 2015 hat beispielsweise das Pentagon eine Einheit zur Innovation im Verteidigungsbereich ins Leben gerufen, um die Entwicklung neuer Technologien in diesem Sektor zu finanzieren. Der Auftrag dieser Einheit könnte dahingehend ausgeweitet werden, sich auch auf KI-Forschung und die Entwicklung von Werkzeugen zu konzentrieren, die dynamische Cyberattacken und Desinformation erkennen und ihnen entgegenwirken. „In den USA hat das an Technologie orientierte Dual-Use-Konzept, also die Kombination des Militärs mit der zivilen Forschung, traditionell einen wesentlich höheren Stellenwert als in Europa", erklärt Philipp Krüger. Das zeige sich sehr deutlich am Beispiel der Defense Advanced Research Projects Agency (DARPA). Aus Krügers Sicht sollte das Militär auch in Europa eine größere Rolle im Bereich der Cybersicherheit spielen. Er empfiehlt, eine neue Agentur zu schaffen, die sowohl die Belange des zivilen Sektors als auch des Militärs bedient.

> Die Expertise des Verteidigungsbereichs in Fragen der Cybersicherheit und Forschung zur Künstlichen Intelligenz könnte auch den Belangen des zivilien Sektors von Nutzen sein.

Die NATO beschäftigt sich schon seit einigen Jahren intensiv mit den Gefahren und der Abwehr von Cyberattacken. Das Bündnis hat diese Tätigkeiten als festen Bestandteil in seine Kommandostruktur integriert. Die Bundeswehr hat mittlerweile ebenfalls ein Kommando Cyber- und Informationsraum. Aus der grundsätzlichen militärischen Asymmetrie zwischen den USA bzw. den NATO-Mitgliedstaaten und Ländern wie Russland leitet sich auch ein klarer Vorteil in Bezug auf finanzielle Ressourcen ab. Jörg Forbrig plädiert in diesem Kontext für ein gezieltes Umschichten in den Verteidigungsbudgets: „Militärisch betrachtet müssen die NATO-Länder von der konventionellen Logik zu einem gewissen Grad abrücken." Mit Blick auf die EU rät Forbrig dazu, sehr viel mehr in Forschung und Entwicklung auf dem Cyberfeld zu investieren, um Abhängigkeiten von den USA und China zu verringern.

Wie bereitet sich die Europäische Union auf die Europawahlen im Mai 2019 vor?

Im Kontext der Wahlen zum Europäischen Parlament vom 23. bis 26. Mai 2019 rückt die Gefahr einer zunehmenden gesellschaftlichen Polarisierung abermals in den Fokus. Im Kern geht es um die Frage, ob die Repräsentanten einer multilateralen, regelbasierten und offenen Ordnung oder die populistischen Kräfte, die auf nationale Interessen, Rückzug und Abschottung drängen, die Oberhand gewinnen. Dies macht insbesondere die anstehenden Wahlen anfällig für Cyberattacken und manipulative Kommunikationskampagnen. Eine umfassende Cyberabwehr ist daher das Gebot der Stunde.

Institutionelle Maßnahmen ergreifen

Die EU-Kommission hat dazu Ende 2018 den Startpunkt gesetzt und einen „Aktionsplan zum Kampf gegen Desinformation" vorgelegt. Dieser sieht unter anderem vor, manipulative Kommunikationskampagnen mit einem Frühwarnsystem zu erkennen. Die Mittel der Task Force, die diesen Plan zu verantworten hat, wurden von 1,9 Millionen Euro in 2018 auf 5 Millionen Euro in 2019 angehoben. Zuvor hatte die Kommission bereits die Europäische Agentur für Netz- und Informationssicherheit (ENISA) mit mehr Personal und höheren finanziellen Ressourcen ausgestattet und die East StratCom Task Force im Europäischen Auswärtigen Dienst (EAD) ins Leben gerufen.

Analoge und digitale Absicherung gewährleisten

Grundsätzlich kommt den Wahlen zum Europaparlament zugute, dass sie Mehrparteienwahlen sind. Dies reduziert grundsätzlich die Gefahr der Manipulation. Sollte es am Wahltag in den einzelnen EU-Mitgliedstaaten doch zu Versuchen

der Einflussnahme kommen, rät Michael Chertoff zu einer analogen Absicherung: „It is very important to make sure you always have a backup on paper that is generated as an accurate record of voting. You can always go back if voting machines are compromised in some way and thus know what the actual votes were."

Chertoff hält es zudem für dringend erforderlich, den gesamten digitalen Ablauf der Wahl technisch bestmöglich abzusichern: „You also need to use cyber security capabilities to make sure you are protecting the entire infrastructure, that is voter registration data bases and groups that tabulate the votes when they come in. Even when the news broadcasters announce results you want to make sure they are not being hacked because in the past the Russians have actually tried to manipulate the elections by attacking the broadcasters." Philipp Krüger empfiehlt, das existierende Cyberabwehrzentrum der EU, die ENISA, zu erweitern und vor allem mit den Nationalstaaten zu vernetzen – im Idealfall mit einer schlanken Hierarchie, die Kommunikationswege eröffnet und schnelle Entscheidungen ermöglicht. Führende Nationen wie Frankreich, Deutschland, die Niederlande und Estland könnten mit ihrem Wissen als Kerngruppe fungieren.

Transparente Warnungen aussprechen

Insbesondere Russland hat seine Kontakte zu Kräften am rechten Rand kultiviert, die der Europäischen Union gegenüber skeptisch bis feindlich eingestellt sind. Man kann davon ausgehen, dass sich die Europaskeptiker langfristig in einer politischen Gruppe konsolidieren und zwischen 20 und 25 Prozent der Stimmen erhalten. „Sowohl seitens der Wahlkommissionen und -beobachter als auch aller proeuropäischen Kräfte und Parteien sollte viel mehr aufgedeckt werden, wie die Europaskeptiker und -feinde eine Stellvertreterrolle als Helfer Moskaus oder anderer externer Akteure spielen", rät Forbrig und fügt hinzu: „Man sollte ganz offen Akteuren, die der Einflussnahme verdächtig sind, mitteilen, dass man ihre Aktivitäten genau im Blick hat." Das warnende Ansprechen der Tatsache, dass westliche Demokratien nicht naiv seien, könne schon helfen, wie das Beispiel der französischen Präsidentschaftswahlen 2017 gezeigt habe.

Wähler mobilisieren

Auch die Mobilisierung der Bürger ist eine Aufgabe, derer sich die EU mit Blick auf den Wahltermin Ende Mai annehmen sollte. Sie müsse rechte und rechtspopulistische Parteien und Polarisierer in den sozialen Medien zumindest dadurch ausgleichen, dass sie die moderate demokratische Mehrheit sowohl in der Debatte im Vorfeld als auch im Wahlvorgang selbst mobilisiert, sagt Forbrig. Dies gilt umso mehr, als die Europaparlamentswahlen im Allgemeinen die Wahlen mit den niedrigsten Wahlbeteiligungen in Europa sind, was in der Regel Parteien an den Rändern Auftrieb verschafft. Krüger ergänzt, dass man mit breit angelegten Kampagnen ein öffentliches Bewusstsein für die Bedrohungen durch Cyberattacken und Fake News schaffen sollte.

WEITERFÜHRENDE LEKTÜRE

Alliance for Securing Democracy Team: What we know about Russia's interference operations; Fact Sheet des German Marshall Fund of the United States vom 25. März 2019

Annegret Bendiek, Matthias Schulze: Desinformation und die Wahlen zum Europäischen Parlament; SWP-Aktuell 2019/A 10, Februar 2019

Kai Biermann, Holger Stark: Die Bundestagswahl kann manipuliert werden; ZEIT ONLINE vom 7. September 2017

Hubertus Breuer: Mehr Cybersicherheit wagen; Magazin „Pictures of the Future" der Siemens AG vom 17. Mai 2018

Michael Chertoff, Anders Fogh Rasmussen: The Unhackable Election: What It Takes to Defend Democracy; Foreign Affairs-Ausgabe Januar/Februar 2019

Joseph Cox: Revenge Hacking Is Hitting the Big Time; The Daily Beast vom 19. September 2017

Sven Herpig, Julia Schuetze: Der Schutz von Wahlen in vernetzten Gesellschaften; Papier der Stiftung Neue Verantwortung vom 11. Oktober 2018

Sven Herpig: Hackback ist nicht gleich Hackback; Impulse der Stiftung Neue Verantwortung vom 24. Juli 2018

Sven Herpig, Tabea Breternitz: Zuständigkeiten und Aufgaben in der deutschen Cyber-Sicherheitspolitik; Impulse der Stiftung Neue Verantwortung vom 26. Juli 2018

Alina Polyakova: Weapons of the weak: Russia and AI-driven asymmetric warfare; Report der Brookings Institution vom 15. November 2018

Jacob Poushter, Janell Fetterolf: International Publics Brace for Cyberattacks on Elections, Infrastructure, National Security; Studie des Pew Research Center vom 9. Januar 2019

Conor Reynolds: Lithuania Leads Seven EU Countries in Forming a Cybersecurity Response Team; CBR Online vom 28. Juni 2018

Haley Sweetland Edwards, Chris Wilson: It's Almost Impossible for the Russians to Hack the U.S. Election. Here's why; TIME vom 21. September 2016

U.S. Department of Justice: Report On The Investigation Into Russian Interference In The 2016 Presidential Election; Editierter und geschwärzter Bericht von Special Counsel Robert S. Mueller, III vom März 2019

Simon Vaut, Jörg Forbrig: Wie wir die Wahl vor russischem Einfluss schützen können; ZEIT ONLINE vom 14. Februar 2017

ENTSTEHUNG DES BEITRAGS

Der hier vorliegende Text basiert auf eigenen Recherchen und auf exklusiven Gesprächen mit Vertretern von Thinktanks, Nichtregierungsorganisationen und Forschungsinstituten. Der Beitrag ist auch auf der Website der Atlantik-Brücke veröffentlicht worden.

IMPRESSUM

Herausgeber
Atlantik-Brücke e.V.
Magnus-Haus
Am Kupfergraben 7
10117 Berlin
www.atlantik-bruecke.org

Redaktionelle Leitung
Robin Fehrenbach

Geschäftsführender Vorstand
Friedrich Merz (Vorsitzender)
Dr. h.c. Edelgard Bulmahn, Dr. David M. Deißner (Geschäftsführer), Prof. Dr. Andreas R. Dombret, Prof. Dr. Burkhard Schwenker