# HYBRIDE BEDROHUNGEN
## SICHERHEIT UND INTEGRITÄT POLITISCHER KOMMUNIKATION

**Die hybriden Bedrohungen sind zu identifizieren, auf ihre Gefahrenpotentiale hin systematisch zu untersuchen und darzulegen, wie ihnen begegnet werden kann. Im Spannungsverhältnis zwischen Wahrheitsministerium und Meinungsfreiheit: Wieviel Regulierung, Sicherheit und Integrität benötigt und verträgt politische und Wahlkampfkommunikation in einer demokratischen Gesellschaft?**

**Zusammenfassung einer Expert_innenrunde am 3.9.2018 in Köln.**

Destabilisierungsversuche, Manipulationen an Wahlergebnissen, politische Propaganda oder gezielte Desinformation: Die technischen Voraussetzungen, einfach und wirksam die Integrität politischer Kommunikation zu beeinflussen, sind längst vorhanden. Im Guten wie im Schlechten. Mit diesen technischen Mitteln sollen Unsicherheit verbreitet und das Vertrauen in die politischen Botschaften sowie die formalen Abläufe der Politik untergraben werden.

Nicht nur staatliche Hacker sind in der Lage, Einfluss auf politische Wahlen zu nehmen. Vielmehr würden sich „Bad Bots" zunehmend zum wirksamsten Propagandainstrument entwickeln, das es je gab, sagte Peter Donaiski, Vertreter der gastgebenden Friedrich-Ebert-Stiftung, zur Eröffnung der Diskussion über „Hybride Bedrohungen" in Köln und fragte das Publikum: Sind wir dunklen Mächten schon hoffnungslos ausgeliefert? Dem Problem der angreifbaren Integrität politischer Information im Netz, aber auch den Lösungsansätzen und Antworten, mit denen man sich den Gefahren und Herausforderungen stellen könnte, widmeten sich in zwei Impulsreferaten und einer Diskussion Michael Seemann, Kulturwissenschaftler, Sachbuchautor und Journalist, Julia Krüger, Politikwissenschaftlerin, Expertin für Digitalpolitik und wissenschaftliche Mitarbeiterin der Bundestagsabgeordneten Saskia Esken, Matthias Kammer, Direktor des Deutschen Instituts für Vertrauen und Sicherheit im Internet DIVSI, und Sven Herpig, Leiter Transatlantisches Cyber-Forum (TCF), Stiftung neue Verantwortung. Moderiert wurde die Diskussion von dem Fachjournalisten und Dozenten Peter Welchering.

## IMPULSREFERATE

Wie konnte es passieren, dass Donald Trump Präsident wurde, fragte Michael Seemann gleich zur Eröffnung seines Vortrags über „Hacker, Trolle, Bots und Fake News – diskursive Sicherheitsrisiken der Demokratie". Die übliche Antwort auf diese Frage zitierte er gleich im Anschluss: „Die Russen waren es." Beweise für die Einmischung oder für Eingriffe von Hackern aus Russland gäbe es zwar nicht, doch Seemann zeigte sich überzeugt, dass sie nicht ganz unschuldig an dem Ergebnis der US-Präsidentschaftswahlen 2016 waren. Wenigstens hätten sie „Beipackzettel" dazu geliefert und gezeigt, wie Einfluss auf ein Wahlergebnis genommen werden kann.

„Gib mir einen Punkt, wo ich hintreten kann, und ich hebe die Erde aus den Angeln", zitierte Seemann den griechischen Physiker und Ingenieur Archimedes von Syrakus und erklärte in einem kurzen Ausflug in die Welt der Physik, wie das Hebelgesetz in der Welt der Wahlbeeinflussung funktioniert und wie man mit relativ kleiner Kraft große Wirkung erzielen kann.Heutige „Cyber"-Hebel, wie Hackerangriffe, seien entsprechend Instrumente, die wenig Aufwand erfordern und dennoch sehr wirksam sind.

Der erste Hebel: Man greift direkt in den Wahlvorgang ein. Möglich wird dies beispielsweise durch Beeinflussung oder Manipulation von Wahlautomaten. In den USA verbreitet und seit mehreren Jahren im Einsatz stehen Wahlmaschinen im Verdacht, über bekannte oder unbekannte Sicherheitsschwachstellen von Hackern manipulierbar zu sein. Der Einsatz von Wahlcomputern sei in Deutschland zwar durch das Bundesverfassungsgericht verboten worden, so Seemann, doch die sich im Einsatz befindliche Software PCWahl, die zur Kumulation und zum Upload von Stimmen eingesetzt wird, wies ernsthafte Sicherheitslücken auf, wie der Chaos Computer Club (CCC) kurz vor der Bundestagswahl 2017 glaubhaft belegen konnte.

Der zweite Hebel: direkter Eingriff in die Wahlkampagne. Mit politischen Nachrichten über die traditionellen Informationskanäle bei Facebook oder Werbung in dem Netzwerk können potentiell Milliarden von Mitgliedern erreicht und als Hebel genutzt werden. Diese Taktik sei als „leverage" bekannt, erklärte Michael Seemann. So können z.B. bestehende politische Spannungen als Hebel dienen.  Der Skandal um Cambridge Analytica (CA) zeigte, dass man die Facebook-Nutzerdaten auch unmittelbar für Mikro-Targeting und individualisierte, auf den Nutzer zugeschnittene Werbung einsetzen kann. Allerdings konnte nach Meinung von Seemann bisher niemand den Nachweis erbringen, dass die Methode, so wie von CA behauptet, auch tatsächlich funktioniert.

Dritter Hebel: Trolle und Bots. Gefälschte Identitäten, die automatisiert „im Netz herumspuken", kosten wenig und benötigen keine ausgefeilte Technik. Die wesentliche Aufgabe von Bots und Trollen besteht in der Aktivierung oder Deaktivierung der Wähler mit Methoden, die auch aus der Social-Media-Werbung bekannt sind. Obwohl im US-Wahlkampf sehr verbreitet und beliebt, hätten in Deutschland Bots keinen Einfluss auf das Wahlergebnis und würden kaum eingesetzt.

Dort, wo die technischen Fähigkeiten der Hacker am besten zum Ausdruck kommen, seien E-Mail-Hacks und Datendiebstahl an der Tagesordnung, bei denen sensible Informationen über Politiker_innen und ihre Familien entwendet und gesammelt werden, um sie ggf. später zu deren Nachteil zu verwenden. Als Beispiel für den erfolgreichen Einsatz dieses Hebels verwies Seemann auf die Kampagnen und Veröffentlichungen über Wikileaks sowie Aktivitäten der sogenannten Troll-Szene, von „Reddit" bis zu „Meme War".

In Deutschland bilden die Filterblasen im Internet die Offlinesituation der politischen Meinungsäußerungen gut ab, so Michael Seemann. Deutsche Besonderheiten sind Instrumente politischer Einflussnahme und Manipulation wie beispielsweise „Reconquista Germanica". Auch das Thema Flüchtlingspolitik, das polarisierend auf Politik und Gesellschaft wirkt, kann erfolgreich als Hebel eingesetzt werden. Tendenziöse Nachrichten werden von ausländischen, in Deutschland aktiven Medien „eingespielt". Untersuchungen zeigen, dass Richtigstellungen offenbar nicht die Zielgruppe erreichen. Zwischen den Gruppen der Empfänger von Fake News und der Empfänger von Fake-News-Korrektur gibt es den Studien zufolge keine Überschneidungen.

Und gerade in diesem Zusammenhang zeige sich das wesentliche Problem der Bekämpfung von Fake News, resümiert Michael Seemann, denn auch eine andere Meinung zu haben gehört zur pluralistischen Demokratie.

Im zweiten Impulsreferat präsentierte Sven Herpig von der Stiftung Neue Verantwortung Erkenntnisse aus der Arbeit, an der er mit dem Expertennetzwerk „Transatlantic Cyber Forum" arbeitet. Er befasste sich mit der Frage, was Angreifer tun und wie sie vorgehen würden, um die Sicherheit, Vertraulichkeit, Integrität oder Verfügbarkeit politischer Kommunikation (die sogenannte C.I.A.-Triade: Confidentiality, Integrity, Availability) zu verletzen.

Herpig identifizierte zahlreiche Instrumente, mit denen auf die C.I.A.-Triade im politischen Kontext und insbesondere im Kontext politischer Wahlen Einfluss genommen werden kann. „Show of Force" ist eine dieser Techniken, mit denen vom politischen Gegner (eigene Regierung, Regierung eines anderen Landes etc.) eine Demonstration potenzieller Angriffsmöglichkeiten vorgeführt wird, ohne den Angriff tatsächlich auszuführen. Das Unterbinden oder Aus-dem-Netz-Nehmen von Webseiten gehört ebenso zu den Formen der Beeinflussung wie die Techniken des „Kompromat", bei dem Politiker_innen und ihre Familien zu direkten Opfern von Hackerangriffen werden.

Technische Gegenmaßnahmen reichen in solchen Fällen aber nicht aus: Sven Herpig betonte, wie wichtig es sei, im Fall eines Angriffs kommunikativ vorbereitet zu sein. Wichtig sei, der Bevölkerung zu verdeutlichen, dass auch bei einem Angriff die Wahlergebnisse zuverlässig sind, auch dann, wenn die Bewältigung eines Sicherheitsvorfalls einige Tage dauern sollte. Was wäre schlimmer, fragte er, wenn Wahlen angegriffen würden und keiner bekommt es mit, oder wenn die Wahlen tatsächlich (technisch) sicher wären, aber die Bürger glaubten, sie wären beeinflusst worden?

## PODIUMSDISKUSSION

Matthias Kammer, Direktor des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI), erklärte, dass für die Bevölkerung die Fragen der Sicherheit im Internet in den vergangenen vier Jahren immer wichtiger geworden seien. Gleichzeitig würden laut aktueller DIVSI-Studie zu den Internet-Milieus 2016 „Die digitalisierte Gesellschaft in Bewegung" zwei Drittel (68 Prozent) der Menschen bezweifeln, dass Datensicherheit im Internet möglich sei. Der Hackerangriff auf den Bundestag fördere nicht gerade das Vertrauen in den Staat, erklärte Kammer. Es hätte sich dennoch ein fataler Pragmatismus in Sicherheitsfragen etabliert. Die Skepsis an der Sicherheit der Daten im Internet stehe aber nicht im Widerspruch zum grundsätzlichen Internetoptimismus: Die Mehrheit der Bevölkerung in Deutschland sehe mehr Chancen als Gefahren im Internet.

Julia Krüger, Expertin für künstliche Intelligenz (KI) und wissenschaftliche Mitarbeiterin der Bundestagsabgeordneten Saskia Esken, zeigte sich überzeugt davon, dass soziale Medien für konstruktive Zwecke genutzt werden könnten. Aber nur, wenn man der Versuchung widersteht, der Masse zu folgen. Als Voraussetzung dafür fordert sie eine andere Gewichtung der Rankings in Suchmaschinen. Krüger plädierte für mehr Transparenz angesichts der Erkenntnis, dass Menschen am ehesten glauben, was sie auf Platz eins der Suchergebnisse gezeigt bekommen. In einer Echokammer, wie beispielsweise der BILD-Zeitung, wisse die Leserschaft, was die anderen lesen. In den Echokammern der sozialen Medien würden die Nachrichten auf jeden Nutzer persönlich zugeschnitten, jeder Newsfeed sei anders, jeder liest etwas anderes.

## FAZIT

Sind wir nun den „dunklen Mächten hoffnungslos ausgeliefert", wie einleitend gefragt? Ist es noch möglich, Informationen abzugleichen, Wahres von Falschem zu unterscheiden?

Für Matthias Kammer kommt hier den Journalist_innen eine zentrale Rolle zu: Was wirklich hilft, ist, dass sie ihren Job richtig machen.

Der Ruf nach der Regulierung von Plattformen hat in den letzten Jahren zwar stark zugenommen, aber der Nationalstaat stößt dabei an seine Grenzen, erklärte Julia Krüger. Es gelte neue Wege der Regulierung zu finden, u. a. darüber, nach welchen Regeln welche Akteure die Newsfeeds zusammenstellen. Man müsse mit den Plattformbetreibern ins Gespräch kommen.

Michael Seemann steht der Regulierung skeptisch gegenüber. Am Beispiel des Netzdurchsetzungsgesetzes (NetzDG) zeige sich, dass man nicht alles einfach „durchregulieren" könne. Fake News und Hass liessen sich nicht einfach verbieten.


Herausgeberin: Politische Akademie/Medienpolitik
www.fes.de/medienpolitik