

Parlamentarischer Abend, März 2019

## Verdeckte externe Einflussnahme über soziale Medien. Ein Thema für die Vereinten Nationen?

Mischa Hansel

**Wenige Wochen vor den Wahlen zum Europäischen Parlament wächst die Sorge vor onlinegestützten Manipulationen aus dem In- und Ausland. Wie groß ist das Risiko, dass demokratische Prozesse durch den Einsatz von Fake-Accounts und Social Bots sowie die Verbreitung von Falschnachrichten beeinflusst werden? Wie sind solche Aktivitäten völkerrechtlich zu bewerten und was kann auf internationaler und nationaler Ebene dagegen unternommen werden? Um diese aktuellen Fragen zu erörtern, lud die sef: zusammen mit Ulrich Lechte MdB am 12. März 2019 zu einem Parlamentarischen Abend in die Deutsche Parlamentarische Gesellschaft ein.**

Die Veranstaltung begann mit einem Impulsreferat von Dr. Matthias C. Kettemann vom Leibniz-

Institut für Medienforschung | Hans-Bredow-Institut (HBI). Darin machte er auf Kriterien zur völkerrechtlichen Bewertung sogenannter grenzüberschreitender Informationsoperationen aufmerksam. Hierunter fallen etwa die verdeckte Verbreitung von Falschnachrichten über Social Bots sowie der Aufbau und der Betrieb von Fake-Accounts in sozialen Netzwerken. Je nach Inhalt, Ziel oder Schwere solcher Operationen könne es sich dabei um Verstöße gegen das Interventionsverbot handeln oder aber um völkerrechtlich noch erlaubte Versuche der Einflussnahme. Insbesondere die Tatsache, dass zunächst lediglich mit Mitteln der Sprache gearbeitet werde und kein physischer Schaden zu befürchten sei, erschwere eine eindeutige Klassifizierung. Inhalte seien völkerrechtlich nur in wenigen Fällen zu beanstanden, etwa wenn direkt zum Einsatz von Gewalt gegen andere Gruppen aufgerufen wird. Der Einwand, dass oft nicht zweifelsfrei geklärt werden kann, ob etwa Fake-Accounts von staatlichen oder privaten Akteuren betrieben werden, sei hingegen weniger relevant. Inzwischen gebe es nämlich einen internationalen Konsens, dass Staaten im Internet eine Sorgfaltspflicht auch für das Handeln gesellschaftlicher Subjekte in ihrem Einflussbereich haben, da das Internet – ähnlich wie das Klima – als zu schützendes globales Gemeingut eingestuft wird.



Parlamentarischer Abend 2019 (v.l.n.r): Ulrich Lechte, Matthias C. Kettemann, Daniela De Ridder, Markus Reuter und Katie Gallus (Moderation)

### Eine Gefahr für die Demokratie?

Moderatorin Katie Gallus bat die Diskutanten im Anschluss um eine Bewertung der Gefährdung

durch Social Bots und Falschnachrichten. Dabei machte sich Markus Reuter, Redakteur von netzpolitik.org, für eine differenzierte Analyse stark. Fake-Accounts seien zumindest in Deutschland weit einflussreicher als Social Bots. Es gäbe gefälschte Influencer mit zehntausenden von Followern, die Stimmung machten und schwer zu erkennen seien. In mehreren Untersuchungen seien hingegen kaum Aktivitäten von Social Bots während Wahlkämpfen in Deutschland festgestellt worden. Dasselbe gelte für die Debatten um den UN-Migrationspakt 2018. Gerade letzteres Beispiel bewerteten die Bundestagsabgeordneten Ulrich Lechte und Dr. Daniela De Ridder aufgrund eigener Erfahrungen in der Kommunikationsarbeit anders. Ulrich Lechte be-



Parlamentarischer Abend 2019: Ulrich Lechte und Matthias C. Kettemann (r.)

richtete, wie er mit einer Flut von dubiosen und oft zusammenhanglos argumentierenden Emails zum Thema Migrationspolitik konfrontiert wurde, die er sich nur mit dem Einsatz von Social Bots erklären könne. Er verwies zudem auf die Aktivitäten des Trollnetzwerks „Reconquista Germanica“ sowie die Bedeutung von Fake News und Datenleaks im zurückliegenden US-Präsidentschaftswahlkampf. Mit Blick auf die Demokratie mache ihm das durchaus Sorgen. Die massenhafte Veröffentlichung von privaten Daten von Bundestagsabgeordneten Ende 2018 illustriere eine weitere Seite von Cyberrisiken, die er selbst als „Grenzerfahrung“ wahrgenommen habe. Daniela De Ridder machte ebenfalls auf die Gefährdung privater Daten aufmerksam und mahnte, die Macht viraler Kommunikation im Netz nicht zu unterschätzen. In fragilen Demokratien stellten sich diese Probleme noch einmal gravierender dar. Sie selbst habe auf Auslandsreisen erfahren, wie kritische Journalistinnen und Politikerinnen im Internet angegangen und Androhungen physischer Gewalt ausgesetzt seien. Wenn solche Stimmen in der Konsequenz verstummen, sei der Schaden für die demokratische Meinungsbildung real.

## Social Media Literacy und Cyberresilienz stärken

In Bezug auf mögliche und notwendige Gegenmaßnahmen waren sich alle Diskutanten grundsätzlich einig, dass die Medienkompetenz der Nutzer/innen durch Aufklärung und politische Bildung gestärkt werden müsse und dass den Schulen eine Schlüsselrolle dabei zukomme. Matthias C. Kettemann wies auf Beispiele in der Schweiz hin, wo Datenschutz sogar schon in der frühkindlichen Erziehung im Kindergarten ein Thema sei. Markus Reuter machte auf empirische Untersuchungen aufmerksam, demzufolge Falschnachrichten überproportional von älteren und nicht von jüngeren Menschen geteilt würden. Entsprechend müsse die politische Bildung alle Altersgruppen adressieren. Zudem sehe er auch Nachholbedarf in der journalistischen Ausbildung. Beispielsweise würden sich viele Journalisten zu stark und unreflektiert auf Klickzahlen als Indikator für relevante Inhalte im Netz fokussieren. Dabei bleibe unberücksichtigt, dass sich diese Zahlen leicht manipulieren lassen und viele Akteure für gefälschte Klicks bezahlen würden.

Mit politischer Bildung alleine, so der Tenor der Diskussion, sei den Problemen aber nicht beizukommen. So müssten sich auch staatliche Institutionen viel besser gegen Cyberangriffe wappnen und dagegen resilienter werden, so Daniela De Ridder. Ulrich Lechte plädierte ebenfalls für technische Schutzmaßnahmen und neue Abwehrkompetenzen, um den demokratischen Rechtsstaat gegen Angriffe, die von überall aus der Welt kommen können, zu verteidigen. In diesem Zusammenhang unterstützte er ausdrücklich die Idee des französischen Präsidenten, eine europäische Agentur zur Beobachtung verdeckter Einflussnahmen auf Wahlen einzurichten. Matthias C. Kettemann betonte, dass das Recht auf freie Meinungsäußerung unbedingt geschützt werden muss, was die Suche nach geeigneten Maßnahmen schwierig macht. Er richtete den Blick stärker auf die Verantwortung der Plattformbetreiber. Hier sehe er ein grundsätzliches Problem der Geschäftsmodelle von Facebook, Twitter usw. Deren Algorithmen seien alleine darauf ausgerichtet, die Verweildauer der Nutzer zu maximieren, und dies funktioniere am besten mit sensationalistischen und hochemotionalen Inhalten. Hier müsse die Politik eingreifen und die Plattformen dazu anhalten, die Anreizstrukturen so zu verändern, dass problematische Inhalte nicht „belohnt“ werden, indem sie den Nutzern besonders prominent angeboten werden. Stattdessen sollten die Algorithmen so gestaltet werden, dass „wertige Inhalte“ höher bewertet werden. Markus Reuter ergänzte, dass die Plattformen immer noch „Black Boxes“ seien und sich weigerten, Forschungen zum Thema zu unterstützen.

## Regulierungsmöglichkeiten auf der globalen und regionalen Ebene

Schließlich erörterten die Diskutanten Möglichkeiten einer Regulierung auf internationaler Ebene sowie die Rolle der deutschen Cyber-Außenpolitik. Dabei skizzierten Ulrich Lechte und Matthias C. Kettemann die Bruchlinien zwischen verschiedenen Staatengruppen. Selbst innerhalb Europas, so Lechte, gebe es recht unterschiedliche Perspektiven zwischen West- und Osteuropäern. Innerhalb der Vereinten Nationen seien die Gegensätze zwischen westlichen Staaten auf der einen sowie autoritären Regimen wie China und Russland auf der anderen Seite noch viel ausgeprägter. Matthias C. Kettemann stimmte dieser Einschätzung zu, differenzierte dann aber stärker nach einzelnen UN-Institutionen. Der UN-Sicherheitsrat mit seiner Fokussierung auf High Politics und das akute Krisengeschehen in der Welt sei sicher nicht der geeignete Agent für eine normative Einhegung von Informationsoperationen. Es sei aber gerade aus deutscher Perspektive wichtig, auf laufende Normbildungsprozesse in anderen Foren, etwa den von der Generalversammlung einberufenen Arbeitsgruppen, Einfluss zu nehmen. Hier brauche es eine



Parlamentarischer Abend 2019: Daniela De Ridder

aktive Cyber-Außenpolitik liberaler Demokratien, um die Idee eines freien Internets beispielsweise gegen das von China vertretene Modell eines stark kontrollierten und zensierten Onlineraumes zu verteidigen. Zugleich sei es wichtig, kein Forum Shopping zu betreiben und sich nicht leichtfertig auf Parallelprozesse einzulassen. Denn eine Fragmentierung der Normbildung in den Vereinten

Nationen und anderswo berge die Gefahr einer Erosion des Völkerrechtes.

Daniela De Ridder betonte daran anschließend, dass Cyber-Außenpolitik sich nicht auf völkerrechtliche Instrumente beschränken sollte, sondern Teil des diplomatischen Alltagsgeschäfts werden müsse. So sei es wichtig, etwa auch im Rahmen von Wirtschaftsverhandlungen zwischen Deutschland und China auf die Bedeutung von Cybervorfällen



Parlamentarischer Abend 2019: Markus Reuter

hinzuweisen und so auf internationaler Ebene eine kritisch-konstruktive Positionierung vorzunehmen. In der anschließenden Diskussion mit Teilnehmer/innen im Publikum wurde bemängelt, dass die derzeitige Debatte einseitig auf Gefahren aus China und Russland fixiert sei und darüber beispielsweise die Lehren aus dem NSA-Skandal vergessen würden. Ebenso unterschlage die Berichterstattung über den chinesischen Hardwarehersteller Huawei, dass alle US-amerikanischen Internetkonzerne in ihren Produkten Hintertüren für staatliche Geheimdienste einbauen müssten.

# STIFTUNG ENTWICKLUNG UND FRIEDEN (sef:)

Informationen zur sef:, zu unseren Veranstaltungen und Publikationen finden Sie online unter [www.sef-bonn.org](http://www.sef-bonn.org)



GLOBAL GOVERNANCE SPOTLIGHT 2|2019

## Internationale Regeln für soziale Medien Menschenrechte wahren und Desinformation bekämpfen

Matthias C. Kettemann  
März 2019, 4 Seiten



GLOBAL GOVERNANCE SPOTLIGHT 1|2019

## Die Zukunft der Arbeit – und der ILO Von der Normsetzung zur Normdurchsetzung

Markus Demele  
Februar 2019; 4 Seiten



GLOBALE TRENDS ANALYSEN 1|2019

## Mobilität von Arbeit vs. Kapital: Eine Global-Governance-Perspektive

Stuart Rosewarne & Nicola Piper  
März 2019, 32 Seiten

### Impressum

Die Stiftung Entwicklung und Frieden (sef:) wurde 1986 auf Initiative von Willy Brandt gegründet. Als überparteiliche und gemeinnützige Stiftung bietet sie ein hochrangiges internationales Forum für das gemeinsame Nachdenken über drängende Fragen von Frieden und Entwicklung.

Die Berichte zu den Konferenzen und Veranstaltungen der SEF informieren in kompakter Form über die Diskussionen und Ergebnisse.

**Herausgeberin**  
Stiftung Entwicklung und Frieden (sef:)  
Dechenstr. 2 : D-53115 Bonn  
Tel. 0228 959 25-0 : Fax 0228 959 25-99  
[sef@sef-bonn.org](mailto:sef@sef-bonn.org) : [@sefbonn](https://www.facebook.com/sefbonn)  
[www.sef-bonn.org](http://www.sef-bonn.org)

**Redaktion**  
Dr. Michèle Roth

**Design Basiskonzept**  
Pitch Black Graphic Design  
Berlin/Rotterdam

**Gestaltung**  
Gerhard Süß-Jung

Die Inhalte geben nicht unbedingt die Meinung der Herausgeberin wieder.

© sef: 2019