Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)047

Stellungnahme

Dr. Sandro Gaycken, Digital Society Institute, ESMT Berlin
„Resilienz von Demokratien im digitalen Zeitalter im Kontext der Europawahl“
im Ausschuss Digitale Agenda am 10. April 2019

Zu den Fragen des Ausschusses nehme ich wie folgt Stellung:

1. Resilienz des digitalen demokratischen Diskurses gegen Beeinflussung

Der demokratische Diskurs findet für immer weitere Bevölkerungskreise zunehmend in Teilen bis schwerpunktmäßig im Netz statt, wobei soziale Netzwerke, der Austausch in kleineren oder größeren Gruppen, eine ebenfalls zunehmend wichtige Rolle spielen. Allerdings sind soziale Netzwerke manipulierbar und werden nachweislich von fremden Mächten zu Manipulation genutzt. Die Attraktivität dieser Medien für fremde Mächte kommt vor allem durch fünf Faktoren zustande, die alle als inhärente Merkmale sozialer Netzwerke anerkannt werden müssen und die im Weiteren eine wichtige Rolle spielen, so dass sie an dieser Stelle erläutert werden sollen.

1. **Globale Erreichbarkeit**: Im Gegensatz zu lokalen politischen Debatten in Person können politische Diskurse in sozialen Netzwerken von überall auf der Welt geführt werden. Damit ist mitunter nicht ersichtlich, (a) ob eine an einer nationalen oder regionalen Debatte teilnehmende Person überhaupt aus dem entsprechenden Einflussbereich ist, also auch in diesem Sinne „betroffen“ und auf gleicher Ebene mitspracheberechtigt ist, zudem, (b) ob sie aus einem Land heraus agiert, das fremde politische Interessen in den stattfindenden Diskurs einbringen möchte.

   Um diesem Merkmal entgegenzuwirken, wären technische oder gesetzliche Maßnahmen denkbar, die eine Lokalisierung der Diskursteilnehmer erzwingen, was aber diskursberechtigte Personen im Ausland ungerechtfertigt disqualifizieren könnte und was zudem in entsprechenden Fällen – eine technisch erkennbare Distinktion wäre möglich – internationale demokratische Diskurse erschweren würde. Eine mögliche „mittlere“ Maßnahme wäre ein gezielter Aufbau als lokal klassifizierter Diskurse, in denen Lokalisierung technisch realisiert werden kann. Dies könnte als Zusatzangebot in reguläre soziale Medien integriert werden. Zudem sollten Nachrichtendienste technisch und rechtlich dringend ermächtigt werden, als fremde Mächte erkennbare Akteure in sozialen Netzwerken zu identifizieren, zu verfolgen und abzuschalten.

2. **Skalierbarkeit**: Meinen und Wissen kann in sozialen Netzwerken gezielt skaliert werden. Es können besondere Gruppen angesprochen werden, besondere Interessen identifiziert und gefördert werden, Informationen können über tausende bis hunderttausende Menschen verbreitet werden. Die Mechanismen für verschiedene Varianten der Skalierbarkeit sind insbesondere im Marketing sowie in entsprechend befassten Nachrichtendienste gut bekannt und sind in keiner Weise als rein „organisch“ und lediglich den Gesetzmäßigkeiten der Diskursverläufe unterliegend zu verstehen, son-

dern müssen als manipulierbar angesehen werden. Geschicktere Manipulatoren versuchen allerdings nur selten eine größere Massenmanipulation, sondern agieren eher subkulturspezifisch auf bestimmte und als besonders beeinflussbar geltende kleinere Gruppen, die dann über die Mechanismen der Skalierbarkeit gut identifizierbar und erfassbar sind.

3. **Gestaltbarkeit der Diskurse**: Diskurse in sozialen Netzwerken müssen auch als in höherem Maße gestaltbar gelten als lokale Diskurse in Person. Begleitende und unterstützende Informationen können sehr gezielt und choreographiert eingebracht werden, Wahrnehmungsverzerrungen (Bias) können gezielt aufgebaut und genutzt werden, Diskursteilnehmer können in höherem Maße effektiv konspirativ miteinander agieren. Zudem können manipulierte mediale Mittel eingebracht werden, und es können Verstärkungseffekte durch Querverweise auf (ebenfalls gezielt und choreographiert manipulierte) weitere Diskurse hergestellt werden. Diese und ähnliche Manipulationen sind insbesondere im heutigen politischen Diskurs aufgrund der Komplexität der Sachstände oder Hintergrundinformationen immer leichter herzustellen, da prinzipiell eine hohe Informationsasymmetrie mit unzugänglichen Basisfakten herrscht, die nur durch medial vermitteltes Wissen aufgehoben werden. Die mediale Vermittlung allerdings lässt sich immer bezweifeln, so dass im hergestellten Zweifelsfall Informationen von Manipulatoren als gleichberechtigt wahrgenommen werden können. Diskursteilnehmer sind solchen Konstruktionen und den darauffolgenden gezielten Manipulationen gegenüber mehr oder weniger wehrlos, da viele der in diesem Feld genutzten Effekte unterbewußt funktionieren.

   In Abwesenheit der Möglichkeit einer eigenen und unabhängigen Verifikation der zugrundeliegenden Sachverhalte ist unglücklicherweise das Vertrauen in die Vermittler von Wissen und Meinen ein maßgeblicher Faktor, um Teilnahme an anerkannten und geprüften Diskursen überhaupt auch nur anzuregen. Daher ist die Effektivität von „Fakten-Checkern“ oder besonderen Obleuten oder Verwaltern und Vermittlern von geprüftem Wissen in vielen Fällen kategorisch eingeschränkt, da die Unterminierung des Vertrauens in entsprechend ausgewiesene Akteure wesentlicher Teil des Narrativs aller Manipulatoren ist. Allerdings lassen sich manipulativ gelenkte Diskurse hervorragend mit ihren eigenen Mitteln schlagen. Gegenmanipulationen durch das Zerstreuen von fremd gesteuerten Debatten in Kleinteiligkeit, Zweifel, Unsicherheit und Angst unter Einbindung der gleichen manipulativen Mechanismen lassen die Effektivität entsprechender Operationen drastisch sinken, sofern man auch ähnliche Ressourcen einbringen kann.

4. **Ownership durch Ressourcenaufwendung**: Die Gestaltbarkeit ermöglicht auch eine sogenannte Ownership von Diskursen, wenn Leitfunktionen für diese dauerhaft eingenommen werden können. Das Erreichen dieser Herrschaft über Diskurse in sozialen Netzwerken steht bei genauer Kenntnis der erforderlichen Faktoren in einem direkten Verhältnis zur Aufwendung entsprechender Ressourcen.

   Eine hohe Aufwendung von Ressourcen kann zum Teil Ermittlungen befähigen. Sofern die erforderlichen Fähigkeiten bei den angreifenden fremden Mächten nicht „in house“ vorliegen, wenden diese sich häufig an Werbeagenturen oder andere externe Dienstleister aus der Rüstungsindustrie. In diesen Fällen kann unter Umständen leichter ermittelt werden, welche Akteure in welcher Variante welche Interessen verfolgen.

5. **Schein-Authentizität und Identifikation**: Diskurse in sozialen Netzwerken wird (ironischerweise) oft eine höhere Authentizität zugeschrieben, da sie für stärker basis-demokratisch gehalten werden. Sie sprechen scheinbar die Sprache der Netzbewohner, kennen die gleichen subkulturellen Themen und Meme, ein „Wir"-Gefühl kann entstehen, das dann aufgebaut werden kann in ein Narrativ eines „Wir gegen Die".

   An dieser Stelle hilft vor allem das konkrete Enttarnen fremder Mächte sowie auch von Marketing-Akteuren im Netz. Aufklärung über Manipulation demokratischer Diskurse muss dringend auch dieses Element enthalten, in möglichst konkreter Form, um die eigene Manipulierbarkeit erlebbar zu machen und so den Mythos der Authentizität zu durchbrechen.

6. **Anonymität/Pseudonymität**: In diesem Kontext ist nun auch eines der Kernmerkmale aller Probleme digitaler Handlungen zu erwähnen – die unumgängliche Anonymität oder Pseudonymität der Handelnden. Diskursteilnehmer können, müssen aber nicht als natürliche Personen identifizierbar sein. Aus Sicht eines ungehinderten politischen Diskurses mag dies als eine positive Eigenschaft wahrgenommen werden. Sie führt allerdings dazu, dass eben fremde Mächte befähigt werden, sich andere Identitäten anzueignen und zudem auch gleich mehrere davon zu betreiben. So können gut ausgestattete Manipulatoren leicht mehrere Dutzend bis Hundert Identitäten parallel betreiben und so Debatten besonders effektiv steuern. Bei professionellen Akteuren ist zudem zu bedenken, dass eine De-Anonymisierung unter Umständen sehr schwer wird. Anonymität und Pseudonymität sind mitunter nahezu unmöglich vollständig zu beheben, dies ist das sogenannte Attributionsproblem.

   In diesem Kontext ist erneut anzuraten, fremde Mächte stärker zu verfolgen, ihre Akteure im Ausland zu identifizieren und die Ermittlungsergebnisse zu publizieren. Dies ist taktisch möglich und strategisch als sehr effektive Gegenmaßnahme zu empfehlen. Identifizierte Akteure fremder Mächte können und sollten zudem kontinuierlich aus Diskursen entfernt werden.

7. **Direkte technische Angreifbarkeit**: Ein weiteres wichtiges Element ist die direkte technische Angreifbarkeit. Viele soziale Medien sind nach wie vor auch für direkte Hackingangriffe verwundbar, insbesondere dann, wenn in hohem Maße fähige Angreifer angenommen werden müssen. Diese Angriffe können dazu führen, dass bestimmte Diskurse oder Themen deutlich stärker algorithmisch bevorzugt werden als andere. Suchergebnisse oder Diskursverläufe können so direkt manipuliert werden. Aussagen der Dienstebetreiber einer hohen „Unangreifbarkeit" sind reine Marketingaussagen und nicht ernst zu nehmen. Neben direkten Angriffen durch Hacking lassen sich zudem Techniken zur „Optimierungen" von Suchergebnissen anwenden (sog. Search Engine Optimization - SEO), die ohne einen unmittelbaren technischen Angriff rein auf Basis der selbststeuernden Mechanismen der Suchmaschinen Suchergebnisse beeinflussen können.

   Auch hier empfiehlt es sich, die Manipulierbarkeit zu demonstrieren. Das Vertrauen in die Integrität der technischen Diskurssteuerung ist nicht gerechtfertigt und sollte daher berechtigt erschüttert werden. Eine Suchmaschine ist heute auch eine Diskurssteuerungsmaschine. Ihre Angreifbarkeit ist transitiv eine Angreifbarkeit der Demokratie.

Übergreifende Empfehlungen zur besseren Absicherung der Diskurse:

1. **Medienkompetenz stärken, aber nicht überbewerten**: Medienkompetenz muss dringend gestärkt werden, wobei die Manipulierbarkeit und Angreifbarkeit sozialer Netzwerke und Medien plastisch und erlebbar gemacht werden muss. Da dem Vertrauensproblem gegenüber komplexem Wissen und der Abhängigkeit von Wissensvermittlern damit allerdings nicht entgegengewirkt werden kann, muss von einer kategorisch beschränkten Effektivität dieser Aufklärung ausgegangen werden. Wichtig ist hier vor allem die frühzeitige Sensibilisierung in den Schulen.

2. **Klare politische Aussagen und Folgen**: Für fremde Mächte ist es in diesem Spiel zudem auch wichtig, nicht identifiziert zu werden und eine zu harte Eskalation zu vermeiden. Diese Faktoren leiten wesentlich das strategische Denken der Gegenseite. Beide können genutzt werden, um eine zu intensive Beeinflussung von Beginn an zu verhindern. Das Parlament und das Auswärtige Amt müssen sich klar und unisono und explizit gegen eine Beeinflussung demokratischer Diskurse positionieren, müssen die Identifikation fremder Akteure vorantreiben und eine explizite Strategie des Naming and Shaming betreiben, mit weiter reichenden Konsequenzen bei stärkeren Beeinflussungen.

3. **Diensteanbieter zu Transparenz zwingen**: Die Anbieter entsprechender Dienste müssen eine deutlich höhere Transparenz bezüglich ihrer Algorithmen, weitere technischer Mechanismen und der ihnen selbst bekannten Akteure und Vorfälle an den Tag legen. Dies darf nicht allein auf Eigeninitiative beruhen, sondern muss streng gesetzlich geregelt werden.

4. **Akteure identifizieren und publizieren**: Weiterhin ist es wichtig, entsprechende Akteure fremder Mächte zu identifizieren und kontinuierlich zu publizieren. Dies wirkt als direkte Maßnahme sowohl taktisch als auch strategisch, erhöht die realen und politischen Kosten der Angreifer deutlich und unterminiert unberechtigtes Vertrauen in abwegige Diskurse in sozialen Medien.

2. Technische Angreifbarkeit der Wahlen insgesamt

Neben der Manipulation von Wissen und Meinen im digitalen Diskurs muss leider auch eine klare technische Angreifbarkeit vieler technischer Teilschritte der Wahlen konstatiert werden. Sowohl die Wählerregistrierung als auch das Auszählen und die Übermittlung von Wahlergebnissen sind in einigen Ländern teilweise digitalisiert, mit unterschiedlichen Basistechnologien. In Estland wird zudem auch digital gewählt. All diese Technologien müssen als in hohem Maße unsicher gegen professionelle Angreifer bewertet werden. Eine konsistente und unauffällige Manipulation der Wahlen wäre vermutlich nur in Estland und in anderen Ländern nur in Teilbereichen möglich. Allerdings genügt es fremden Mächten häufig bereits, einen Zweifel in die Integrität des Wahlprozesses zu bringen, um etwa die Legitimität der Wahlen zu kritisieren und propagandistisch auszuschlachten.

3. Politischer Austausch mit anderen Mächten zum Informationskrieg

Zuletzt und übergreifend soll noch empfohlen werden, den politischen Dialog mit anderen Mächten zu den Problemen und Herausforderungen der Informationskriegsführung im digitalen Zeitalter zu suchen und gemeinsame Positionen zu finden. So befindet sich etwa Russland bereits seit Jahren in seiner Binnenperspektive in der Position eines Verteidigers gegen einen Informationskrieg, den der Westen gegen Russland begonnen hat. Solche Missverständnisse können nur auf der Ebene höherer politischer Dialoge ausgeräumt werden.