Im digitalen Fadenkreuz Desinformation und Einflussnahme sind massive hybride Bedrohungen. Auch für Deutschland ist das eine außen- und sicherheitspolitische Herausforderung – nicht nur zur Wahl.

Von Lutz Güllner

Lutz Güllner leitet im Europäischen Auswärtigen Dienst die Abteilung strategische Kommunikation. Er gibt hier seine persönliche Meinung wieder.

Kurz nach Ausbruch der Corona-Krise hat die Weltgesundheitsorganisation den Begriff der „Infodemie" geprägt. Dieser beschreibt die Flut oft falscher oder ungenauer Informationen über das Coronavirus, die sich rasch über die sozialen Medien verbreiteten und in einer Mischung aus Falschnachrichten, Verschwörungsnarrativen und gezielter Desinformation Verwirrung und Misstrauen hervorriefen. Der Umgang mit Desinformation ist zweifelsohne eine der wichtigsten Herausforderungen unserer digitalisierten Gesellschaft. Der Grat zwischen dem streng geschützten Gut der freien Meinungsäußerung und den legitimen staatlichen Grenzen für Lügen und Falschnachrichten ist schmal. Die Politik muss neue Antworten finden, etwa in der Justiz-, Medien- und Bildungspolitik.

Aber Desinformation ist eben nicht nur ein gesellschaftspolitisches Problem, sondern auch eine wesentliche außen- und sicherheitspolitische Herausforderung. Gerade in der Corona-Krise wurde nochmals deutlich, wie oft und massiv ausländische Akteure, insbesondere staatliche wie Russland und China, Einfluss auf den Informationsraum in Europa zu nehmen versuchen und dafür auch gezielt Desinformation einsetzen. Dabei geht es nicht um legitime „Public Diplomacy", sondern um absichtliche, koordinierte und oft versteckte Aktivitäten, die mit klaren politischen Zielsetzungen verbunden sind. Diese wollen etwa das eigene Handeln überzogen positiv darstellen und das Handeln der anderen mutwillig diskreditieren, um damit die Überlegenheit des eigenen Systems herauszustreichen.

In anderen Fällen sind regelrechte Desinformationskampagnen zu beobachten, die Vertrauen in staatliche Institutionen oder Prozesse untergraben wollen. Beispiele gibt es dafür unzählige – man denke an die staatlich kontrollierten Medien Russlands. Der Europäische Auswärtige Dienst (EAD) hat ihre Aktivitäten im Kontext der Corona-Krise in einer Reihe von Berichten eindrucksvoll dokumentiert.

Aber auch Desinformationskampagnen bei anderen Themen – etwa die Vergiftung des Oppositionspolitikers Alexej Nawalny, die militärischen Operationen in der

Ostukraine, der Abschuss des MH-17-Passagierflugzeugs, die Darstellung der Proteste in Belarus und viele mehr – liefern aufschlussreichen Einblick in die Strategien und Taktik der Operationen. Hier geht es auch um geopolitische Ziele.

Desinformationskampagnen zielen daher auch gar nicht mehr nur darauf ab, eigene positive Narrative besonders effizient zu verbreiten. Oftmals geht es vielmehr darum, den Informationsraum der Gegenseite so zu überfluten, dass Verwirrung entsteht und Vertrauen in jedwede Information untergraben wird. Gerade in Kombination mit anderen Instrumenten – etwa im Cyber-Bereich durch sogenannte „Hack-and-Leak"-Operationen – wird die Desinformation zur „digitalen Waffe": Das eigentliche Ziel ist dann die Manipulation des Informationsraums des anderen.

Manipuliert werden hierbei nicht nur die Inhalte, sondern auch die künstlich verstärkte Verbreitung sowie die Identitäten der Akteure. Am Ende geht es nicht mehr um „richtig oder falsch" oder um „meine oder deine Version", sondern um das Verbreiten von irreführenden und verzerrenden Suggestionen, die oft auf mittel- bis langfristige Ziele angelegt sind – im schlimmsten Fall auf die Unterminierung des politischen Systems. Daher ist diese Form der Desinformation auch nicht als „Fake News" zu verstehen, sondern als Strategie der Beeinflussung und Destabilisierung eines anderen Staates. Und diese ist eine handfeste hybride Bedrohung.

Das Oxford Internet Institute hat in einer im Januar 2021 erschienenen Studie von einem Problem „industriellen Ausmaßes" gesprochen und auf mehr als 80 Staaten verwiesen, die Informationsmanipulation in der einen oder anderen Form einsetzen. Besonders problematisch ist dabei, dass es immer schwerer wird, diese Aktivitäten aufzuspüren.

Die Strategien und Taktiken entwickeln sich rasant weiter. Bestand vor einigen Jahren noch die Hoffnung, dass man durch das Verbot automatisierter Bots das Problem unter Kontrolle bringen könne, so zeigt sich heute, dass Bots in dieser Form kaum noch eingesetzt werden. Nun geht es eher um den koordinierten Einsatz von gefälschten oder gestohlenen Konten in den sozialen Medien, von pseudoauthentischen Webseiten oder von anderen Maßnahmen, die es erlauben, den Algorithmus der sozialen Medienplattformen auszutricksen.

Immer öfter zeigt sich auch, dass der Einsatz von Desinformation nur ein kleinerer Teil einer groß angelegten Operation

Strategien und Taktiken der Desinformation entwickeln sich rasant weiter

sein kann, die sich nicht nur auf den Informationsraum beschränkt. Hier häufen sich seit einiger Zeit Hinweise und Berichte über Aktivitäten von chinesischen Akteuren, oftmals auch mit direktem Bezug auf staatliche Strukturen, die gezielt auf die Beeinflussung von Medien, Think-Tanks, Forschungsinstituten und anderen NGOs abzielen. In diesem Fall geht es nicht so sehr um die Verbreitung von Falschmeldungen, sondern eher darum, jegliche Form von Kritik am Handeln chinesischer Stellen zu unterbinden und zu verhindern. Ein weiteres Einsatzfeld von Instrumenten der Desinformation und Einflussnahme sind demokratische Prozesse wie Wahlen und Abstimmungen.

Ben Nimmo, der bei Facebook eine wichtige Rolle in der Bekämpfung von Informationsmanipulation durch staatliche

Akteure spielt, geht von einer Weiterentwicklung von Taktiken und Strategien aus. So sei eine Verschiebung von groß angelegten Kampagnen auf „maßgeschneiderte“ kleinere Operationen zu beobachten, die sich durch immer höhere Professionalität und Präzision auszeichneten. Diese Operationen bewegen sich häufig in der Grauzone zwischen authentischen gesellschaftlichen Debatten und künstlich erzeugten Stimmen. Sie werden eingesetzt, um bereits bestehende Stimmen zu verstärken, etwa an den radikalen Rändern der Gesellschaft. Damit können die Aktivitäten der Einflussnahme noch besser verschleiert werden, da es anscheinend um ein innenpolitisches Problem geht.

Der Experte Nimmo weist aber auch auf eine wachsende „Kommerzialisierung“ der Desinformation und Einflussnahme hin. Hier beauftragen staatliche Stellen privatwirtschaftliche Unternehmen mit sogenannter „Black PR“. Dies macht es nahezu unmöglich, den eigentlichen Auftraggeber einer staatlichen Struktur zuzuordnen – es sei denn, man verschafft sich einen umfassenden Einblick in entsprechende Finanzflüsse.

Was kann also überhaupt getan werden? Die EU, und insbesondere der EAD, haben hier eine Vorreiterrolle eingenommen. Seit 2015 beobachtet der EAD mit einer eigens geschaffenen Struktur die Desinformationsaktivitäten Russlands: Diese werden aufgespürt, dokumentiert und auf einer eigenen Website EUvsDisinfo.eu veröffentlicht. Die Arbeit des EAD wurde in den vergangenen Jahren deutlich ausgeweitet: Mit einem Team von Fachleuten geht der EAD das Problem der Desinformation insbesondere in der Nachbarschaft der EU an. Weitere Expertise wurde auch für andere Bedrohungen aufgebaut, etwa durch chinesische Akteure. Ein Frühwarnsystem (Rapid Alert System), das die Experten der EU mit denen in den EU-Mitgliedstaaten verzahnt, wurde ins Leben gerufen. Und die Zusammenarbeit mit internationalen Partnern, etwa im Rahmen der G7 und mit der NATO, wurde deutlich intensiviert.

Die Bundestagswahl könnte ins Fadenkreuz von Kampagnen geraten

Einfache Lösungen gibt es nicht

In nur drei Jahren wurde ein politischer Rahmen entwickelt, der das Problem der Desinformation und der politischen Einflussnahme in den Fokus nimmt. Der Europäische Aktionsplan für Demokratie (European Democracy Action Plan) bezeugt die Entschlossenheit der EU, das Thema effizient anzugehen. Mit dem übergeordneten Ziel, demokratische Prozesse in Europa zu fördern und zu schützen, richtet sich der Plan auf drei Kernbereiche: Regeln für politische Parteien (etwa für politische Werbung), Förderung der Vielfalt und Qualität der Medienlandschaft sowie Maßnahmen, um die Ausbreitung von Desinformation einzudämmen.

Auf der Suche nach einer Lösung besonders wichtig ist die Einbindung von Plattformen und deren Regulierung. Auch hier hat die EU mit dem „Code of Practice“ – einem Verhaltenskodex und Maßnahmenkatalog, in dem sich die Plattformen verpflichten, Desinformation effizient zu bekämpfen – ein Zeichen gesetzt. Diese sollen nun in einen Rechtsakt, in Form des Digital Services Act, überführt werden. Dafür wurde ein innovativer Ansatz entwickelt, der sich deutlich von anderen Gesetzgebungen, wie etwa dem deutschen NetzDG, unterscheidet: Es geht hierbei nicht mehr so sehr um die Regulierung

einzelner Inhalte, sondern um die möglichen „systemischen Risiken“ für die Gesellschaft oder Demokratie als Ganzes. Plattformen haben dabei die Verpflichtung, diese Risiken durch entsprechende Maßnahmen zu mindern.

Auch für Desinformation und Einflussoperationen seitens ausländischer Akteure hat die EU einen umfassenden Ansatz entwickelt, der auf den Erfahrungen im Bereich Cyber-Sicherheit und Umgang mit hybriden Bedrohungen aufbaut. In vier Bereichen – Awareness, Resilience, Disruption und Diplomatic Tools – werden unterschiedlichste Maßnahmen eingesetzt und weiterentwickelt. Dazu zählen auch Aufklärungskampagnen und Trainingsangebote für staatliche Stellen, um auf mögliche Desinformationsattacken vorbereitet zu sein.

Auch Deutschland sollte sich dieser Bedrohung noch stärker widmen. Eine vor Kurzem veröffentlichte Untersuchung des EAD hat nochmals unterstrichen, wie sehr Deutschland Zielscheibe von Aktivitäten russischer Akteure geworden ist.

Experten gehen davon aus, dass die Bundestagswahl ins Fadenkreuz geraten könnte – auch wenn die Gefahr einer unmittelbaren und massiven Verfälschung des Wahlergebnisses als relativ gering einzuschätzen ist. Das Problem ist deshalb auch eher der mittel- bis langfristige Effekt dieser Kampagnen.

Deutschland sollte noch enger mit seinen europäischen und internationalen Partnern zusammenarbeiten und gemeinsame Strategien entwickeln. Auch der Aufbau entsprechender Strukturen und die Stärkung von zivilgesellschaftlichen Initiativen sind notwendig. Dies sollten sich Bundestag und Bundesregierung schon jetzt als Hausaufgabe für die nächste Legislatur vornehmen. IP

Bild nur in Printausgabe verfügbar