Beeinflussen und täuschen

Desinformationen destabilisieren und beunruhigen. Mit Hilfe neuer Technologien und sozialer Medien hat sich die Zahl der Versuche, Gesellschaften zu beeinflussen, vervielfacht.

Desinformation ist das bewusste Inverkehrbringen falscher Informationen zum Zweck der Täuschung. Sie war schon immer Teil unserer Gesellschaft. Während des Kalten Krieges wurden gezielte Desinformationskampagnen gestartet, um Wahlen zu beeinflussen oder politische Interventionen zu machen. Die USA und die Sowjetunion haben sich über Jahrzehnte einen Desinformationskrieg geliefert. Recherchen in den USA haben ergeben, dass zwischen 1946 und 2000 64 Prozent der Wahlen weltweit entweder von den USA oder der Sowjetunion oder beiden gleichzeitig beeinflusst wurden. Auch wenn es Desinformationskampagnen in unserer Gesellschaft schon immer gab, hat dieses Phänomen in den letzten 20 Jahren durch die Digitalisierung eine neue Dimension angenommen. Das Internet und die weltweite Nutzung von Social Media hat den Schauplatz für Desinformationskampagnen und deren Ausbreitung und Schädlichkeitswirkung verändert. Aus der heutigen sicherheitspolitischen Sicht gibt es vier entscheidende Faktoren, die die Bekämpfung von Desinformationskampagnen zur Herausforderung machen.

Erste Herausforderung. Die klassischen Medien haben die Rolle der Informationshoheit verloren. Während des Kalten Krieges war es noch eine Hürde, Desinformation über klassische Medien an eine breite Öffentlichkeit weiterzugeben. Heute dringen Desinformationskampagnen direkt via *Facebook, Twitter, Whatsapp* und Co in den privaten Bereich vor. Social Media werden von weiten Teilen der Bevölkerung genutzt, um Informationen zu erhalten und politische Ereignisse zu verstehen. Nun werden in diesen Social Media auch Informationen mit falschem Inhalt mit dem Ziel weitergegeben, Teile der Bevölkerung zu täuschen bzw. zu beeinflussen. Das Problem dieser falschen Tatsachenbehauptungen zu aktuellen Themen wie das Coronavirus ist, dass die Möglichkeit einer legitimen Meinungs- und Willensbildung auf Basis korrekter Informationen verhindert und das Krisenmanagement behindert wird.

Über soziale Medien werden auch viele Falschmeldungen verbreitet.

Die EU East Strat Com Taskforce des Europäischen Auswärtigen Dienstes konnte beispielsweise feststellen, dass Informationen aus russischen, kremlfreundlichen Medien während der Coronakrise sowohl die weltweite Stimmung gegen die USA anheizt als auch die EU als unfähig die Krise zu bewältigen dastehen lässt. Auch konnte nachgewiesen werden, dass aus diesen Quellen Informationen gestreut wurden, wie, dass das Coronavirus als Waffe gegen China und seine Wirtschaft eingesetzt werde oder das Virus in Wahrheit eine angelsächsische biologische Waffe sei. Sicherheitspolitisch sind diese Entwicklungen äußerst bedenklich, da sie eine Destabilisierung der westlichen Gesellschaften zum Ziel haben und die geopolitischen Machtverhältnisse verschieben sollen.

Die zweite Herausforderung, dass Desinformation als Journalismus verkleidet Eintritt in unsere Gesellschaft findet. Sie beansprucht den Platz klassischer Medien und damit den Anspruch den Bürger anzuleiten, sich in einer immer komplexeren Umwelt auszukennen. Das Gefährliche daran ist, dass sie zur Destabilisierung der Gesellschaft führen kann. Sie ist sensations- und emotionsgetrieben. Eines der Hauptprobleme hinter den heutigen Desinformationskampagnen ist die mangelnde Reflexions- und Kritikfähigkeit unserer Gesellschaft. Falsche Informationen werden heutzutage von mehr und mehr Menschen geglaubt, weil sie das Vertrauen in die demokratischen Institutionen und klassischen Medien verloren haben. Desinformation bietet eine andere Perspektive auf Staat, Medien und die Gesellschaft. Aus Sicht der Nutzer von Social Media stammen die Informationen, die sie beziehen, ja aus legitimen journalistischen Quellen (Sputnik, etc). Auch Nachrichten in klassischen Medien werden mit dem primären Anspruch, dass sie wahr sind, verbreitet. Dass wir die Nachrichten aus klassischen Medien als richtig und wahr annehmen, liegt am Vertrauen, das wir diesen Medien entgegenbringen.

Die Erosion dieses Vertrauens in etablierte Medien oder Institutionen in Teilen der Gesellschaft führt dazu, dass sich Menschen im Internet auf die Suche nach neuen Quellen begeben, denen sie vertrauen können.

Die Herausforderung ist hier insbesondere, dass es nicht nur um einzelne Nachrichten geht, sondern um ganze Narrative, die häufig von Bots vermehrt werden. Für diesen Teil der Gesellschaft, der das Vertrauen verloren und das neue Narrativ angenommen hat, wird es nicht ausreichen, die Fakten richtig zu stellen. Man wird am Vertrauen der Gesellschaft in ihre demokratischen Institutionen arbeiten müssen.

Dritte Herausforderung. Die fortschreitende rasche Entwicklung von neuen Technologien führt zu bisher ungeahnten Möglichkeiten, Desinformationskampagnen zu betreiben. Automatisierte Algorithmen oder Big-Data-Analyse bieten neue Möglichkeiten, rasch und vor allem viel falsche Information gezielt an Bürger zu verteilen. Bots helfen möglichst rasch, rechnerisch große Mengen an Nachrichten zu erstellen. Trolle und automatisierte gefälschten Konten, die sich als echte Bürger ausgeben, werden genutzt, um den politischen Diskurs zu infiltrieren und ihn dann mit Hassreden oder Junk-Inhalten zu beeinflussen. Die Erstellung von Fälschungen, auch von Deepfakes, wird immer einfacher und auch für Nichtspezialisten in kurzer Zeit möglich. Es geht hier nicht nur um Videodateien, sondern auch um Audiodateien oder sogar die Erschaffung von „Künstlichen Persönlichkeiten“ (Artificial Personalities). Die neuen Technologien, die genützt

FOTO: THEVISUALSYOUNEED/STOCK.ADOBE.COM

Social Bots sind Programme, mit denen beispielsweise Twitter-Konten automatisiert gesteuert werden.

werden, um Desinformation zu verbreiten, bewegen sich im selben Ökosystem der digitalen Medien, in dem sich auch Cyber-Kriminelle tummeln. Die Organisatoren von Desinformationskampagnen versuchen, wie Cyber-Kriminelle, neue Technologien für politische oder wirtschaftliche Zwecke einzusetzen. Sie destabilisieren durch ihr Verhalten die Gesellschaft.

Vierte Herausforderung. Zuletzt hat eine Vervielfachung der Akteure im Medienbereich die Bekämpfung von Desinformation schwieriger gemacht. Man kann zumindest folgende Akteure in diesem Bereich als beteiligt ansehen: Web-Browser-Anbieter, Gaming-Plattformen, Cloud-Services, Suchmaschinen wie *Google,* Social Media, Zivilgesellschaft und der Staat selbst. Nun ist die Menge der beteiligten Akteure groß und macht es schwierig, koordiniert gegen Desinformationskampagnen vorzugehen. Der Kampf gegen Desinformation verlangt einen gesamtgesellschaftlichen Zugang, bei dem den österreichischen Medien eine besonders wichtige Rolle zukommt. In diesem Sinne ist es wichtig, Meinungs- und Medienfreiheit sicherzustellen und einen bestmöglichen Rahmen für einen freien öffentlichen Diskurs zu schaffen. Bewusstseinsbildung für die Gefahren von Desinformation und die Stärkung der Medienkompetenz stehen dabei im Mittelpunkt. Auch stärkere Regulierung der Social Media Anbieter steht immer wieder im Raum. Derzeit versuchen diese bereits, gegen Falschnachrichten vorzugehen. Dies widerspricht in einer gewissen Weise ihrem „demokratischen" Businessmodell, dass jeder Nutzer frei ist, zu teilen, zu liken und Informationen auf seine Seite zu stellen. Diese Selbstregulierung der Social Media Anbieter ist aber ein wichtiger Teil zur Lösung des Problems.

Taskforce Desinformation. Aufgrund der vielfältigen Facetten und Auswirkungen von Desinformation verfolgt die österreichische Bundesregierung einen interministeriellen Zugang bei der Bekämpfung derartiger Gefährdungen. Dementsprechend wurden sowohl eine interministerielle Arbeitsgruppe als auch eine Ad-hoc-Taskforce zum Thema Desinformation eingerichtet, die sich speziell im Vorfeld von Wahlen mit Desinformation, als eine Facette von hybriden Bedrohungen, beschäftigt und Reaktionen koordiniert hat.

Das Bundesministerium für Inneres und andere Ressorts arbeiten zusammen mit dem *Austrian Institute of Technology (AIT)* an einer Studie zur Erkennung von Desinformation/Deepfakes. Zudem beteiligt sich Österreich aktiv an europäischen Initiativen (EU-Aktionsplan gegen Desinformation, EU-Schnellwarnsystem gegen Desinformation). Im Rahmen des EU-Schnellwarnsystems gegen Desinformation werden Erfahrungen, Best Practices und aktuelle Gefährdungen zwischen den Mitgliedsstaaten ausgetauscht sowie ein gemeinsames Vorgehen gegen Desinformationsaktivitäten koordiniert.

Das Bild, das sich einem bietet, wenn man das Thema Desinformation beleuchtet, ist düster. Die Möglichkeiten der Einflussnahme sind erschreckend, und die Gefahr ernst zu nehmen. Die Bilder von russischen Militär-Lkws in Kombination mit verbrannten EU-Fahnen in Italien während der Coronakrise sind verstörend. Der Ausbruch des Coronavirus hat Desinformationskampagnen leider einen besonderen Nährboden bereitet. In Kombination mit neuen Technologien müssen wir in Zukunft gesamtstaatlich den Kampf gegen Desinformation verstärken. Bereits 2017 warnten Experten der Münchner Sicherheitskonferenz, dass Angriffe im Cyber-Raum nicht mehr nur gegen kritische Infrastruktur gerichtet sind, sondern gegen unser politisches System und unsere Werte. Die geopolitische Rivalität um das Narrativ im Cyber-Raum ist Realität. Die Stärkung der Resilienz unserer Gesellschaft und der Schutz unserer Grundrechte ist wichtig, genauso wie das wirksame Vorgehen gegen illegale Aktivitäten und Inhalte im Internet.

Caroline Schmidt