OVE Aktuell – Informationstechnik

GIT – Gesellschaft für Informations- und Kommunikationstechnik

November 2019

Sehr geehrte Damen und Herren!

Nachfolgend erhalten Sie den Newsletter OVE Aktuell, diesmal mit dem Schwerpunkt **„Social Media“**.

Wie gewohnt, machen wir Sie an dieser Stelle gerne wieder auf künftige Veranstaltungen des OVE aufmerksam, die für Sie von Interesse sein könnten. Wir freuen uns über Ihre Teilnahme! Bitte beachten Sie die jeweiligen Anmeldemodalitäten.

Veranstaltungen:

09.12.2019: Elektrische Niederspannungsanlagen im Altbau, Seminar, Wien

12.12.2019: Planungsgrundsätze für die Errichtung von Trafostationen, Seminar, Wien

09.01.2020: Die Niederspannungsrichtlinie, Seminar, Wien

09.01.2020: Die EMV-Richtlinie, Seminar, Wien

15.01.2020: Notbeleuchtungsanlagen, Seminar Wien

21.01.2020: Auswahl von Betriebsmitteln und Schutzeinrichtungen für Niederspannungsanlagen, Seminar, Wien

Informationstechnik:

10.03.-11.03.2020: Deep Learning, Seminar, Wien

Informieren Sie sich jederzeit auch gerne in unserem Veranstaltungskalender über unser aktuelles Fortbildungsangebot.

Weitere Neuigkeiten aus dem OVE finden Sie am Ende dieses Newsletters.

Social Media

Fake News und Echokammern

Im „Social Media“-Newsletter beschäftigen wir uns nun schon zum wiederholten Male mit dem Thema „Fake News“, betreiben mit dieser Themenfokussierung aber keineswegs medialen Populismus. Mit Absicht verbreitete unwahre oder verfälschte Nachrichten rütteln vielmehr an den Grundfesten unserer demokratischen und rechtsstaatlichen Gesellschaften im Westen. Wir sind daher gezwungen, taktische Maßnahmenbündel gegen die Spaltungsversuche von außen zu entwickeln, damit wir unsere hart erkämpften Werte von Menschenwürde, Freiheit und Zusammenhalt verteidigen können.

Soziale Medienplattformen sind der innerste Kern des Problems. Und es ist ein Paradoxon, dass ihre anfänglichen Verheißungen für eine Demokratisierung des Netzes mit einer Stimme für jedermann/frau vielerorts, wie z.B. im Arabischen Frühling, gerade für bislang machtlose und unterdrückte Menschen eingetreten sind, andererseits aber den Niedergang der traditionellen, seriösen Medien als Lieferanten recherchierter und dreifach gecheckter Nachrichten befeuert und beschleunigt haben.

Falschnachrichten, in Sekundenschnelle abgesetzt und in die Welt gestreut, sind heute längst auch und gerade in der Politik in Mode. Information Warefare ist heute unbestritten integraler Bestandteil der Soft Power von Staaten bei Absicherung ihrer globalen Machtansprüche und kommt im Kostüm versteckter Wahlbeeinflussung ebenso daher wie als präsidiale Drohgebärde.

Die sozialen Medienplattformen leisten einer Tribalisierung der öffentlichen Meinung Vorschub. Der große amerikanische Politikwissenschaftler Francis Fukuyama hat dieses heute übliche Überstreifen von Kleinstidentitäten und die damit verbundene Abschottung von eigenen Miniweltbildern gegen den Rest als riesige Bedrohung für unsere aufgeklärten Gesellschaften erkannt und plädiert für eine Rückkehr zu einer offenen und konstruktiven Diskussion, die alle gesellschaftlichen Gruppen mitnimmt.

Wenn wir jedoch gegen den Verlust umfassender, faktenbasierter Information, welche die Menschen erst zu vernunftorientierter Entscheidungsfindung bei der gemeinsamen Gestaltung unserer Gesellschaften und Lebensräume befähigt, nichts oder zu wenig unternehmen, überlassen wir das Feld ganz wenigen Demagogen, die im besten Fall egoistische Einzelziele verfolgen, im schlimmsten Fall aber die Deutungshoheit über jedes Geschehen übernehmen. Dann haben wir wieder die stumme Masse der Mitläufer, anstatt aufgeklärter, mündiger Bürger, die sich ihre Meinung aus einer Fülle gesicherter Information bilden konnten.

In den nachfolgenden drei Beträgen gehen renommierte Wissenschaftler/innen aus verschieden Perspektiven der Frage nach, wie wir die langjährigen Treuhänder der veröffentlichten Meinung wieder so stärken können, dass wir dem Dauerrauschen ideologisierter Plattitüden aus den sozialen Filterblasen und auch den vergiftenden Medienkampagnen aus totalitären Staaten wieder eine glaubwürdige Medienszene entgegensetzen können. Die heutigen Ansätze für Fact Checking, wie sie mittlerweile fast alle großen Medienhäuser verfolgen, können das gesellschaftliche Mega-Problem „Fake News“ ebenso wenig alleine lösen, wie eine rechtliche Einfassung, mit der unter Umständen die Balance zwischen der Bekämpfung von Desinformation und der Garantie für eine fortgesetzte Meinungsfreiheit verloren gehen kann. Auch zeitgemäßer Technikeinsatz in Form Künstlicher Intelligenz zur Erkennung unwahrer Information und von gefälschtem medialen Bild-, Video- oder Tonmaterial kann immer nur ein Teil der Lösung sein.

Universitätsprofessor Josef Trappel, Kommunikationswissenschaftler an der Universität Salzburg, geht in seinem Beitrag darauf ein, wie sehr Täuschung, List und die Verbreitung von falscher Information im Verlauf der Geschichte Karriere machten, um danach die Probleme des Journalismus zu beleuchten, die sich aus der disruptiven Diffusion unserer gewohnten Medienlandschaft bei parallelem ökonomischen Niedergang und anhaltendem Glaubwürdigkeitsverlust der Leitmedien sowie des massiven Anstiegs politischer Meinungen auf den Plattformen ergeben haben.

Miroslava Sawiris, Research Fellow am Think Tank GLOBSEC in Bratislava, zeichnet in ihrem Beitrag ebenfalls ein detailreiches Bild des Aufstiegs digitaler Plattformen zum vorherrschenden Medium für soziale und politische Kommunikation und gibt in Folge einen Einblick in die weltweite Struktur der Akteure von Falschnachrichten-Kampagnen und die möglichen negativen gesellschaftlichen Impacts dieser Operationen.

Ross King, Senior Scientist am AIT Austrian Institute of Technology und Leiter des Digital Insight Lab, rundet den Diskursbogen in diesem Newsletter mit der Hauptfrage ab, ob und wie Data Science in Form von Medienforensik und Methoden der Künstlichen Intelligenz helfen kann, Falschinformationen in sämtlichen Mediengattungen zu erkennen und damit die Flut einer schon stark organisierten Fake News-Industrie einzudämmen und abzuwehren.

Alle drei Expert/innen waren sich jedoch am Schluss einig, dass man bei diesem Riesenproblem nur dann wieder Souveränität erlangen kann, wenn sensible und ausgewogene rechtliche Rahmenbedingungen, fortschrittliche Abwehr-Technik und eine wesentlich verbesserte Medienliteralität aller Benutzer perfekt zusammenspielen und die Medien, Behörden und Bürger/innen damit die erforderlichen Werkzeuge für den informierten und verantwortungsvollen Umgang mit „Fake News“ in die Hand bekommen.

Ich wünsche Ihnen eine spannende Lektüre mit unserem neuen Newsletter zu einem Thema von höchster Wichtigkeit!

Dipl.-Ing. Helmut Leopold, PhD
Präsident der Gesellschaft für Informations- und Kommunikationstechnik im OVE
OVE-Arbeitsgruppenleiter "Social Media"
Head of Center for Digital Safety and Security
AIT Austrian Institute of Technology
Kontakt: helmut.leopold@ait.ac.at

Fake News: Das süße Gift der Informationsgesellschaft

Unter Fake News – oder besser Desinformation – versteht man bewusst und absichtsvoll in die Welt gesetzte Falschmeldungen, die nicht auf den ersten Blick als solche erkennbar sind. Man muss allerdings gezielt gestreute Lügen mit Täuschungsabsicht klar von pointierter Satire unterscheiden.

Seit wann gibt es falsche Information und wo kommt sie vor? Eigentlich sind Fake News seit jeher in der Genetik der Menschheit verankert. Selbst im bekannten Kinder- und Hausmärchen der Gebrüder Grimm erzwingt „Das tapfere Schneiderlein" nach einem Kampf gegen zwei Riesen mit Lug und Trug die Eheschließung mit der Königstochter und erobert damit ein halbes Königreich.

Ein Kind des Krieges

Schon sehr früh waren Kriege die Ursache für den steilen Karriereweg von Fake News. Nach der griechischen Mythologie eroberten die Achaier die Stadt Troja im gleichnamigen Krieg mit List, nachdem ein hölzernes Pferd, in dessen Bauch sich Soldaten befanden, in die Stadt hineingezogen wurde und die Soldaten von innen die Stadttore öffnen konnten, um die eigene Armee einzulassen.

Vor 400 Jahren im 30-jährigen Krieg (1618-1648) wurden nach der Erfindung des Buchdrucks durch Johannes Gutenberg Flugzettel, Plakate und Hefte gedruckt, um schnell Falschinformationen über Schlachtdetails unter die Leute zu bringen.

In China wurden 36 dem chinesischen General Tan Daoji zugeschriebene Strategeme – alle Kriegskunst ist Täuschung – nicht nur zur militärischen Überlistungstaktik schlechthin, sondern sie sind heute im Reich der Mitte auch verpflichtender Schullesestoff.

Zu Beginn des Zweiten Weltkrieges schließlich ließ Hermann Göring am 11. März 1938 auf Befehl Hitlers ein Telegramm mit der Bitte um Entsendung reichsdeutscher Truppen nach Wien aufsetzen, um den Einmarsch einzuleiten.

Letztes Beispiel aus dem Kriegsumfeld: Im 2. Irak-Krieg haben die USA Saddam Hussein den Besitz von Massenvernichtungswaffen unterstellt, um ihre militärische Operation zu legitimieren.

Ein Kind der Politik

Gerade auch in der Politik wird oft versucht, mit falschen Tatsachen Eindruck zu schinden. So wurde 2011 der damalige Verteidigungsminister der Bundesrepublik Deutschland, Karl Theodor von und zu

Guttenberg, des Plagiats bei der Abfassung seiner Dissertation an der Universität Bayreuth überführt und ihm anschließend die Doktorwürde aberkannt.
Italiens Ministerpräsident Guiseppe Conte wiederum polierte seinen akademischen Werdegang mit Eigenangaben über Studienaufenthalte an so renommierten Institutionen wie der Sorbonne, der Cambridge University, der Yale und New York University ein wenig auf. In New York war er nachweislich nie Mitglied einer Fakultät gewesen, sondern hatte lediglich einen Ausweis für die Universitätsbibliothek.
Und der Schwindel von Donald Trump, dessen Amtszeit im Jänner 2017 mit der Inaugurationslüge begann, ist ohnehin noch in bester Erinnerung.

Fake News in der Wirtschaft

Im Wettstreit um globale Absatzmärkte haben die bekannten deutschen Automarken Volkswagen und Mercedes plumpe, illegale Manipulationen zur Umgehung gesetzlich festgelegter Abgasgrenzwerte vorgenommen. Im September 2015 gestand der VW-Vorstandsvorsitzende Martin Winterkorn den „Dieselgate"-Skandal öffentlich ein.

Auf persönlicher Ebene

Insbesondere Schülerinnen und Schüler sind als Angehörige der Generation „digital natives" und im Hinblick auf ihre dauernde Präsenz in sozialen Netzwerken heute unzähligen Formen von Cyber-Mobbing und Cyber-Bullying ausgesetzt. Damit sind verschiedene Formen der Verleumdung, Belästigung, Bedrängung und Nötigung gemeint, die mit bewussten Falschdarstellungen operieren.

Fake News im Journalismus

Mit Falschmeldungen im Journalismus bekommt die Problematik aber noch einmal eine ganz andere Dimension. Drei Beispiele mögen hier stellvertretend zeigen, wie auch Starjournalisten die Wahrheit durch erfundene Geschichten ersetzten, um zu Ruhm und Geld zu kommen:
1983 platzte die Sensationsstory über die Hitler-Tagebücher, die der Journalist Konrad Kujau dem deutschen Hochglanzmagazin „Stern" untergejubelt hatte. Der Schweizer Journalist Tom Kummer, der sich eigenen Angaben zufolge als Vertreter des „Borderline-Journalismus" sieht, bei dem Realität und Fiktion bewusst vermischt werden, entfachte im Jahr 2000 mit neu zusammengesetzten oder erfundenen Interviews mit Hollywood-Prominenten wie Brad Pitt oder Sharon Stone nach Aufdeckung durch das Magazin „Focus" einen gehörigen Presseskandal, der seine Auftraggeber in der Chefredaktion des SZ-Magazins den Kopf kostete.

Es erwischt irgendwann alle großen Magazine: 2018 flogen die gefälschten und erfundenen Geschichten des gefeierten und vielfach ausgezeichneten SPIEGEL-Reportagen-Stars Class Relotius auf.

Es gibt drei große Problemkomplexe mit Desinformation

1. Demokratien, insbesondere repräsentative unseres europäischen Zuschnitts, die auf informierten Wahlentscheidungen beruhen, werden durch Falschinformation defekt.
2. Die Digitalisierung des Informationskosmos in Form von Nachrichtenplattformen hat zu einer Beschleunigung der Nachrichtenübermittlung geführt. Damit kann auch Desinformation direkter, schneller und anonymer verbreitet werden.
3. Demokratische Gesellschaften übertragen arbeitsteilig Information an die Institution des Journalismus, mit dem Auftrag zu schauen, was wahr ist.

Durch die heutige Medienvielfalt hat der traditionelle Journalismus seine Funktionsmacht – oder besser sein Deutungsmonopol – über Ereignisse verloren. Diese Tendenz wird noch dadurch verstärkt, dass das werbefinanzierte Geschäftsmodell zunehmend zerfällt. Dieses ökonomische Problem betrifft keineswegs nur den Printsektor, wo die Auflagen seit rund 20 Jahren kontinuierlich zurückgehen, sondern auch das lineare Fernsehen mit seinen schrumpfenden Einschaltquoten, besonders bei jüngeren Menschen, die sich vermehrt dem Angebot von Streaming-Diensten wie Netflix zuwenden.

Die aufgezeigte Entwicklung hat zu einer Vertrauensersosion bei den klassischen Medien geführt. Nur mehr 41 % der Nachrichtenrezipientinnen und -rezipienten trauen den Nachrichten. Dieses Glaubwürdigkeitsproblem hat ernste Folgen: Wer den Nachrichten misstraut, verliert das Interesse an Nachrichten.

Erschwerend kommt in der heutigen Medienbranche hinzu, dass beim gegebenen Ressourcenmangel eine seriöse Recherche nur mehr begrenzt möglich ist. Beim zunehmenden Zeitdruck gilt immer mehr das Gebot „Lieber schnell als richtig!“. Damit nimmt das Vertrauen weiter ab und verschärft die ökonomischen Probleme der Medien. Ein Teufelskreis, aus dem es fast kein Entrinnen gibt.

Was können wir gegen Fake News tun?

In Deutschland wurde das Netzwerkdurchsetzungsgesetz (NetzDG) vom damaligen Justiz- und heutigen Außerminister Heiko Maas erlassen. Mit dem am 1.1.2018 in Kraft getretenen Gesetz wollte die Bundesrepublik eine Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken und eine gesetzliche Handhabe gegen Hasskriminalität im Netz einführen.

Das NetzDG, dem viel Kritik von Seiten der NGOs entgegenschlug, welche die Meinungsfreiheit im Netz gefährdet sehen, verpflichtet Digitale Plattformen, „offensichtlich rechtswidrige Inhalte“ innerhalb von 24 Stunden nach Eingang einer Beschwerde zu entfernen oder zu sperren.

Trotz gut gemeinter Absicht ist die Gefahr einer Zensur durch 1.000 Falschnachrichten-Jäger bei z. B. Facebook nicht zu übersehen. Margrethe Vestager, dänische Wettbewerbskommissarin in der EU-Kommission von Juncker, nannte dies „eine Übertragung der Rechtsdurchsetzung an ein privates Werbeunternehmen“.

Demokratiepolitisch sehr willkommen, aber auch problematisch im Hinblick auf die Meinungsfreiheit im Netz ist das EUGH-Urteil im Verfahren Eva Glawischnig gegen Facebook vom 3. Oktober 2019. Demnach muss Facebook als im Rechtsstreit unterlegene Partei sofort und von sich aus alles löschen, was als unrechtmäßig erkannt wurde.

Einen anderen Weg versucht der Ehrenkodex der Presse des Österreichischen Presserates einzuschlagen. Dort ist festgehalten, dass Redaktionen „Richtigstellungen“ veröffentlichen sollen.

Das mittlerweile weithin etablierte „Fact Checking“ bei seriösen Medien ist grundsätzlich ein guter Ansatz, kann aber durch das Problem der Filterblasen bzw. Echokammern, in denen Menschen verweilen und lesen wollen, was in ihren Kram passt, und daher an Fakten gar nicht interessiert sind, die nicht ins eigene Weltbild passen, seine positive Wirkung zur Einschränkung von Fake News nicht zur Gänze entfalten.

Die parallele Ausbildung einer entsprechenden Medienkompetenz auf Seite der Mediennutzer bleibt ebenfalls eine stumpfe Waffe, wenn im Netz keine wahrheitsgetreuen Informationen zirkulieren. Vielleicht können in Zukunft auch algorithmische Verfahren helfen, mit deren Hilfe sich Fake News aufdecken lassen.

Fazit

Desinformation durchzieht viele Bereich des öffentlichen und privaten Lebens und nicht nur den Journalismus. Und sie ist auch keine Erfindung des digitalen Zeitalters.

Da sie aber die Institution Journalismus schwächt und unsere Demokratie bedroht, müssen wir entschlossen mit rechtsstaatlichen Mitteln gegen sie vorgehen, ohne das Menschenrecht der freien Meinungsäußerung zu verletzen.

Univ.-Prof. Josef Trappel
Universität Salzburg
Leiter des Fachbereichs Kommunikationswissenschaft
Direktor des Erasmus Master Studiengangs „Digital Communication Leadership“

Democracy vs. Disinformation

Who is winning the battle?

Disinformation is Old News! The word has its semantic origin in the Russian term “Dezinformatsiya”, which was allegedly invented by Joseph Stalin during WW II.

To disinform meant at the time to intentionally disseminate (in the press, on radio or on TV) false reports in order to mislead public opinion. The definition has changed very little since then and includes online sphere now.

The first means of (Dis)Information Dissemination

Disinformation and influence campaigns are probably as old as politics. At 44 BC Rome’s first emperor Octavian etched propaganda on coins to smear the reputation of his rival Marc Antony. And after Johannes Gutenberg invented the printing press in 1439 and news began to circulate widely, so did the spread of false information.

New means of (Dis)Information Dissemination

With the ascent of the Internet more and more households gained access to the World Wide Web. While in 2007, 55 % of the households in the European Union had internet access, the number of households connected to the internet raised to 87 % in 2017 according to Eurostat.

Secondly, the transformation of the information environment online and the way we consume information caused by digital platforms emergence and evolution is nothing but a paradigm shifting change. In 2018 Facebook had 2.23 billion active users and it also has large user bases on its social media applications WhatsApp and Messenger. Currently, the information environment consists of plethora of different digital platforms such as Instagram, Twitter, YouTube, LinkedIn, Snapchat, VKontakte or TikTok (China) to name a few.

These digital platforms have become massive mediators and curators of content, managing vast amounts of data. Just on Facebook around 510,000 comments and 293,000 statuses are posted every minute and more than 300 million photos get uploaded per day. Human attention span is limited, endless news streams enticing us to constantly scroll down through the feeds are not.

Digital Platforms became main tools for social and political communication

With the emergence of omnipresent digital platforms, media production habits changed dramatically along with news consumption behaviours. As users became producers of content and as platforms began to channel news articles into their streams, recommendation and relevance algorithms became indispensable to manage and rank content we consume, through highly personalized news

feeds. According to some research findings, these individual feeds create echo chambers and filter bubbles, as they promote content based on our past behaviours, shares and likes. This may lead to further polarization of opinions through confirmation bias, due to ongoing reinforcement of one's views through constant stream of ideas which one already agrees with.

However, the data about ourselves which we feed into digital platforms through daily usage are not only utilised to predefine and personalize our news feeds. Digital platform business model is inextricably linked to ad revenues, which are generated through user views. The more user views, the higher the revenue. This means that the more time a user spends on a platform, the more ads are displayed or clicked on. The ease of content shareability is therefore a core design feature of digital platforms, encouraging users to constantly view interesting content and spread it further. The metadata created in this process and personal user information then becomes a valuable asset in itself, which can be monetised in microtargeting advertising strategies for political or commercial purposes.

In the new media arena, engagement figures on platforms act as proxy for story relevance in a stark contrast to the previous model in which traditional media and news editors acted as gatekeepers of information, possessing the authority to decide what is relevant and what is not. In this new information environment, user engagement figures such as likes and shares, further assisted by algorithms promoting viral content, act as arbiters of relevancy. These features have been and are heavily exploited, as this ecosystem directly promotes sensational content. This is because such content travels further and faster than non-sensationalist, irrespective of factual accuracy, generating more revenues. Hence, divisive and radical content gains more prominence. In other words, harmful content attracts more attention and is more profitable.

The American legal scholar Cass Robert Sunstein from Harvard University has already made his gloomy prophecy in 2007: "Internet will divide people into digital silos where they would only hear 'louder echoes of their own voices'".

Disinformation is only the tip of the Iceberg

How does disinformation fit into this picture? The intrinsic features of today's media landscape have made the dissemination of (dis)information much cheaper, faster, more efficient and readily available to almost anyone with an internet connection. However, disinformation is only one type of information operation tactics in a toolbox of information operations/information manipulation campaigns. The terminology is gradually expanding along with increasing democratisation and sophistication of these campaigns. The vocabulary of information operations reflects this diversity and expressions such as fake news, hoaxes, propaganda, false news, disinformation, misinformation,

rumours, hybrid threats, psychological operations, narrative amplification and others continue to form our understanding of this phenomenon.

The information operation tactic called “disinformation” typically means a deliberate spread of a story, audio or visual material that seeks to polarize or raise alarm by tapping into existing fears or stereotypes of the target audience. A good example of this tactic’s deployment has been observed during the recent Slovak Presidential Election when pre-existing Anti-Semitic prejudice and proliferation of Anti-Semitic conspiracy theories among the population have been used to act out intense character assassination campaign against a liberal candidate.

During the European elections in the V4 (Visegrad States Czech Republic, Hungary, Poland, Slovak Republic) the GLOBSEC think tank from Bratislava has observed a move towards more sophisticated campaigns which utilised several tools such as manipulation of facts, dissemination of conspiracies and divisive narratives, rather than spread of disinformation.

The Information Operations Landscape

In today’s geopolitical environment and our divided societies with rigid demarcations between ideologies we are confronted with a multitude of information operation actors. The spectrum goes as far as foreign state actors (such as the current Kremlin administration with its Saint Petersburg-based troll factory, the infamous Internet Research Agency which interfered in the American presidential elections in 2016), foreign non-state actors (such as the Macedonian youth, which in 2016 produced vast amounts of disinformation for ad revenues only), domestic home-grown actors (local influencers with large follower bases disseminating controversial content for personal gain), domestic governmental actors (which use info-operations against their own populations) and international networks (like ISIS, which use propaganda and disinformation to harm Western societies and to recruit new members).

Information Operations Impact

Information operations can have significant consequences which can be categorized as immediate and long-term. In the short run such campaigns are trying to achieve direct outcomes for example desired election, referenda or legislative results. The more profound and long-lasting aim is to create public confusion, polarization and radicalization which can eventually lead to state of paralysis at the highest level, for example when crucial state institutions become embroiled in a legislative or executive gridlock.

The main dangers caused by disinformation and information warfare are:

- Erosion of citizens' trust in democratic institutions and electoral processes
- Increasing support for fringe politics of far-right, far-left and populism
- Growing divisions in society through fanning the flames of hate and extremism
- Dehumanisation and targeting of vulnerable sections of society (for example LGBTI community, women, ethnic minorities and others)
- Doubt of expert communities/science resulting in health and other crises (WHO lists vaccine hesitancy as 1 of top 10 global health threats of 2019)
- Violence and erosion of human rights
  and
- Foreign Policy changes

Is this a loosing Game?

The Oxford Internet Institute found "growing evidence of computational propaganda (COMPROP) around the world, with evidence of organised social media manipulation campaigns in 70 countries, up from 48 countries in 2018".

While Disinformation content still plays a role, the trend is more sophisticated amplification of divisive narratives, as could be observed from tactical change in information operations in the V4 states during EP elections.

What makes things worse is the fact that significant proportion of Info-ops are executed on channels which are difficult to monitor such as WhatsApp, via chain emails and others.

As for the digital platforms, the main vehicles of disinformation and into-ops campaigns, the challenges often seem insurmountable, with problematic self-regulatory steps taken by platforms on a daily basis, such as Facebook's decision to exclude political advertising from fact-checking in a new policy from October 2019, ahead of the US Presidential Race in 2020.

European counter-strategies: Steps in the right direction

In December 2018 the EU came up with its "Action Plan Against Disinformation". In addition to that the "EU Strategic Communication to counteract propaganda against it by third parties" has contributed to raising awareness to foreign propaganda efforts against the union and to the necessity to implement efficient counter measures including the need to upgrade of the capabilities at EEAS and the East StratCom Task Force.

Information operations are now being recognized at European level, especially in the Baltics and the Nordic States which were among the first ones to recognize the threat on a state level. New

resolution on Foreign electoral interference and disinformation in national and European democratic processes has been adopted in the EP in October 2019.

Encouraging are also civil society initiatives such as the Slovak konspiratori.sk and blbec.online which address the issues of problematic advertising revenue generated on disinformation outlets and a broad scope of information operations actors on Facebook. Anonymous volunteers dedicated to exposing and countering the activities of internet trolls spreading lies, disinformation and other forms of online harmful behaviour, the so-called Elves also significantly contribute to efforts to create a healthier information environment for everyone.

What needs to be done

To truly address the issue of information operations' impact on democracies and societies in general, a self-regulatory code of practice for digital platforms does not go far enough, and problematically, it places content regulation responsibility on the shoulders of digital platforms. This creates a regulatory limbo in which digital platforms are required and allowed to create ad-hoc non-transparent policies which transform our information environments in often harmful and unpredictable ways, with immense social and political consequences.

Therefore, EU-wide regulation which will address the issue of transparency in relation to political advertising, recommendation algorithms, account take downs and access to publicly available data to CSOs for research purposes, is needed.

All EU member states need to recognize the threat to our democratic societies and can learn from those countries which already have a rich experience in the area of countering information warfare. Part and parcel of these activities is a long-term policy aimed at developing resilience through media literacy and the concept of digital citizenship in particular, with trainings and materials made available for all segments of society.

Miroslava Sawiris
Research Fellow Strategic Communication Programme, GLOBSEC
Bratislava, Slovak Republic

Desinformation und authentische Digitale Medien

Wo liegt das Problem?

Das Internet ist als grundlegende Infrastruktur einmalig in der Menschheitsgeschichte. Es ermöglicht weltweite Kommunikation und die Verbreitung von Information – aber es kann im gleichen Maße für verfälschte Kommunikation und Desinformation genutzt werden.

Die Social Media-Kanäle haben das Problem der Verbreitung von Desinformation potenziert. Jeden Tag tauchen neue Fake Stories auf, von staatlichen Akteuren, wie der mittelweile eindeutig als Desinformations-Akteur im großen Stil identifizierten russischen Troll Factory „Internet Research Agency", über die jungen Falschnachrichten-Produzenten aus Mazedonien, die „Desinformation" im Internet und auf Facebook zu einer Cottage-Industrie entwickelt haben, bis hin zu obskuren Liebesbekundungen aus der Ukraine für Amerika („I love America") mit einer Million Mitgliedern.

Heute deckt die digitale Medienforensik auch immer mehr „Deepfakes" – Fälschungen in Bewegtbildinformation – auf, wie die im Netz kursierenden manipulierten Obama-Videos belegen oder Audioverfälschungen z. B. in der digitalen Wirtschaftskriminalität (CEO-Fraud). Desinformation ist allgegenwärtig.

Kampf gegen Desinformation: State of the Art in der Medienbranche

Beispiel Video-Inhalt

Die Prüfung von Video-Inhalten auf ihren Wahrheitsgehalt ist ein sehr aufwendiges Verfahren der Sammlung von Inhalten und ihrer anschließenden Verifikation. Journalisten durchkämmen täglich Nachrichtenagenturen und soziale Medien, wie Twitter, Facebook, YouTube und SnapChat, auf nachrichtenrelevante Inhalte.

Im Verifikationsprozess werden zahlreiche Kriterien geprüft, um die zentrale Frage beantworten zu können, ob der Inhalt wirklich neu ist, oder jemandem falsch zugeschrieben wurde. Dazu wird das Material minutiös Bild für Bild untersucht, um Informationen zu Ort, Datum, Uhrzeit sowie zu involvierten Akteuren und dem tatsächlichen Geschehen zu extrahieren. Dabei kommt forensische Intelligenz in Form der Identifikation von z. B. Wahrzeichen (künstlich oder natürlich) durch Abgleich mit Satellitenbildern, Straßenansichten und georeferenzierten Fotografien sowie durch Nutzung von astronomischen und Wetterdaten zum Einsatz, um Inkonsistenzen zu finden.

Entscheidend ist auch die Provenienz des Filmmaterials, d. h. wer hat gefilmt und warum? Filmmaterial z. B. von der APA oder aus Kameras hat Metadaten. Bei der Herkunftsbeurteilung gibt es jedoch ein Problem: Soziale Medien und Messaging-Apps verändern oder entfernen oftmals Metadaten oder wandeln das Format um, was es schwierig macht, die ursprüngliche Manipulation zu entdecken.

Beispiel Fact Checking

Der dreistufige Prozess des Fact-Checking mit Überwachen, Identifizieren und Verifizieren ist nicht minder anspruchsvoll. Dabei werden laufend Quellen gesammelt, hinsichtlich Relevanz ausgewertet, und es wird eindeutig geklärt, wer spricht und ob seine/ihre Aussagen wahr sind.

Für seriöses Fact Checking sind Ressourcen erforderlich. Diese können durch Personen bereitgestellt werden, die in Vollzeit Fakten prüfen oder z. B. bei Großereignissen wie Wahlen auch in Form von Ad hoc „Truth Squads" gestellt werden.

In Bezug auf die Datenquellen kommen so unterschiedliche Ressourcen in Frage, wie die Aussagen einer beschränkten Anzahl namhafter Politiker, Crowdsourcing, indem Bürgern die Möglichkeit gegeben wird, als irreführend angesehenes Material entsprechend zu kennzeichnen, oder die Dienste von Drittanbietern, wie z. B. Politifact und Factcheck.org (US) bzw. Reality Check (UK).

Die Herausforderung

Durch das Internet haben sich die Informationskanäle vervielfacht. Gleichzeitig erleben wir ein exponentiell steigendes Volumen bei Medien mit immer mehr politisch motivierten Verfälschungen.

Zwei gute Beispiele für letztere Entwicklung sind der Fall des 19-jährigen Anas Modamani, dem unsere Selfie-Kultur zum Verhängnis wurde, und die Verbreitung endloser Halbwahrheiten und Lügen durch das „Leave-Lager" vor dem Brexit-Referendum im Juni 2016.

Nach einer Aufnahme mit Bundeskanzlerin Angela Merkel und Teilung des Selfies im Netz wurde das Foto politisch motiviert gehackt und auf Facebook in fiktive Terrormeldungen hineinkopiert. Es tauchten Fotomontagen auf, in denen behauptet wird, Modamani habe einen Obdachlosen in Berlin angezündet. Die Urheber überschrieben ihren Beitrag mit „Merkel machte 2015 Selfie mit einem Täter". Auch an den Attentaten in Brüssel soll er beteiligt gewesen sein. Und zuletzt verbreitete sich nach dem Anschlag auf den Weihnachtsmarkt in Berlin eine Montage, die Modamani zusammen mit Merkel zeigte, übertitelt mit „Es sind Merkels Tote".

Der Deutschlandfunk hat in einem Artikel über Propaganda-Lügen in Sozialen Medien im Vorfeld des Brexit-Referendums sehr schön aufgezeigt, wie offensichtliche Falschinformationen absichtlich für politische Zwecke eingesetzt werden. „Bis heute werden gegen das Brexit-Lager schwere Vorwürfe erhoben. Die Fälle, in denen die Rechtslage einigermaßen klar ist, sind noch die greifbarsten: Die beiden Austritts-Kampagnen sollen deutlich mehr als erlaubt für ihren Wahlkampf ausgegeben und diesen Überschuss auch noch verschleiert haben. So weit, so klar. Ein anderer Vorwurf aber wiegt noch schwerer: Das Brexit-Lager soll im großen Stil Daten missbraucht, Wähler manipuliert, gelogen und letztendlich den demokratischen Wahlprozess unterminiert haben.

Sie sind gespickt mit Halbwahrheiten und glatten Lügen über die Absichten der EU und die vermeintlichen Vorteile eines Austritts. Es sind Kuriositäten darunter, wie das Gerücht, die EU wolle Teekessel verbieten. Auch die Behauptung, Großbritannien könne durch den Brexit 350 Mio. Pfund pro Woche sparen, taucht in unterschiedlicher Form auf.

Zentrales Ziel der Brexit-Kampagne war es, dafür zu sorgen, dass bestimmte Gruppen abstimmen, die sonst nicht unbedingt wählen gehen. Sie hatten eine Gruppe junger weißer Männer aus der Arbeiterschicht ausgemacht, die sich eigentlich nicht für Politik interessiert, aber eher für als gegen den Brexit ist."

Vor diesem Hintergrund skalieren die aktuellen Medienansätze nicht! Wir brauchen daher neue Ansätze, die eine Skalierbarkeit der Forensik ermöglichen, die Reaktionszeit bei der Analyse beschleunigen, automatisierte Prozesse unterstützen und insgesamt den Medien ihre Aufgaben als vertraute Prüfer erleichtern.

Wie kann Data Science helfen?

… durch Medienforensik

Bei Medienforensik variieren die Definitionen. Zum vereinfachten Verständnis von Medienforensik wird hier die Begriffsklärung aus der Bild-Forensik, mit der die Echtheit von Bildern überprüft wird, übernommen und auf alle Medientypen (Bild, Audio, Video und Text) angewandt.

Bei der so definierten Medienforensik werden verschiedene Analyseverfahren eingesetzt, wie z. B. die Überprüfung der Konsistenz der Metadaten (Länge des Videos, Datenformat, Erstellungsdatum), um verdächtige Datenformate und Datenkompression zu erkennen.

Mit der Bildqualitätsanalyse wird untersucht, ob Bilder oder Teile von Bildern nachbearbeitet worden sind. Dies lässt sich an Auffälligkeiten, wie z. B. der Granularität (Bildrauschen), dem Kontrast oder der Beleuchtung erkennen.

Mit einer 3D-Szenenrekonstruktion kann in Fällen, die diesen hohen Aufwand rechtfertigen, die Widerspruchsfreiheit von Schatten und Spiegelungen festgestellt werden.

Und mit kontextbezogenen Suchvorgängen wird abgeklärt, ob Inhalte bereits in der Internetlandschaft vorhanden sind.

Ein Paradebeispiel für ein verändertes Foto ist jenes vom Besuch des damaligen amerikanischen Präsidenten George W. Bush in einer Grundschule am Tag der Anschläge auf die Zwillingstürme des New Yorker World Trade Center (9/11), auf dem er ein Kinderbuch verkehrt hält. Viele Menschen auf der ganzen Welt haben dieser Darstellung geglaubt, obwohl das unveränderte Originalbild überall im Internet zu finden war.

Deepfakes (Videomanipulationen) lassen sich mit Medienforensik z. B. durch Gesichtsverzerrungseffekte, inkonsistente Kopforientierung, Blinzel-Verhalten oder Hautfarbeänderungen (die Hautfarbe ändert sich mit dem Herzschlag) erkennen.
Die größte Herausforderung bei Bewegtbild-Manipulationen ist heute der technologische Rüstungswettlauf zwischen Fälschern und Forensik-Experten.

… durch Künstliche Intelligenz

Methoden aus der Künstlichen Intelligenz, wie Machine Learning und neuronale Netzwerke, können für die Erkennung von Desinformation eingesetzt werden. Dafür ist aber eine umfangreiche Trainingsphase notwendig, die einen repräsentativen Satz an Bilddaten verwendet, die so genannte „Ground Truth". Die entwickelten Algorithmen lernen dann automatisch die Merkmale manipulierter Medien. Für Videoinhalte ist der Vergleich abstrakter Merkmale (z. B. Fingerabdruck) über eine Bildsequenz notwendig.
Für die Analyse von Text kommen textbasierte Ansätze der Künstlichen Intelligenz wie NLP (Natural Language Processing) zum Einsatz.
Wenn z. B. geprüft werden soll, ob Wahlen von extern beeinflusst werden, werden Aussagen untersucht, die Emotionen oder Vorurteile ansprechen. Dafür bietet „Sentiment Analysis" eine Lösung. Das sind Anwendungen des maschinellen Lernens zur systematischen Identifizierung, Extraktion, Quantifizierung und Untersuchung von affektiven Zuständen und subjektiven Informationen.
Bei maßgeschneiderten Aussagen bietet sich Stylometry als Lösung an. Dieser Ansatz macht sich den Umstand zu Eigen, dass Wörter, die Menschen verwenden, und die Art und Weise, wie sie ihre Sätze strukturieren, sehr unterschiedlich sind und daher Rückschlüsse auf den Autor von Texten (Werken) erlauben. Dadurch könnte man z. B. erkennen, dass eine Reihe von Postings aus der Internet Research Agency kommen.

True or False?

Im Fact Checking geht es darum, ob eine Aussage wahr ist. Der Einsatz von Künstlicher Intelligenz in Form von NLP, Machine Learning und semantischen Technologien kann bei der Wahrheitsprüfung helfen, u. a. durch die Nutzung von großen öffentlichen semantischen Repositories (z. B. DBPedia), um eine allgemeine Wissensrepräsentation zu erlernen; oder durch Analysieren und Interpretieren von bereitgestelltem Text. Dabei werden benannte Entitäten und syntaktische Strukturen identifiziert und in relevanten Kategorien geordnet.

Die methodische Breite (Prüfinstrumentarium) reicht von Aussage-Extraktion über Referenzquellensuche, Aussage-Genauigkeitsbewertung bis zur Identifizierung von Mustern, die in gefälschten Nachrichten verwendet werden.

Fact Checking unter Nutzung Künstlicher Intelligenz ist ein extrem herausfordernder Ansatz. Das fundamentale Problem dabei ist, dass Menschen sich nicht darauf verständigen können, was Fake News sind, und es daher schwierig ist, dies den Maschinen beizubringen.

Andererseits erfordert Fact Checking fast paradox eine beinahe „generelle AI“ auf dem Level menschlicher Intelligenz betreffend die Erfordernisse von Verstehen und allgemeiner Weltsicht.

Schlussfolgerungen

- Das Thema Desinformation ist von entscheidender Bedeutung für die Demokratie.
  Unsere Zivilgesellschaft ist auf Vertrauen aufgebaut.
- Es gibt keine Wunderwaffen!
  Technik alleine ist nicht ausreichend (Rüstungswettlauf).
  Gesetzgebung alleine ist nicht ausreichend (und könnte alles noch schlimmer machen, z. B. mit einer Zensurverordnung).
- Die Überprüfung digitaler Quellen ist wichtiger als je zuvor.
  Wir müssen vertrauenswürdige Quellen (und vertrauenswürdige Prüfer) [wieder]etablieren.

Dr. Ross King
Senior Scientist
AIT Austrian Institute of Technology, Center for Digital Safety and Security
Leiter des Digital Insight Labs

Aktuelles aus dem OVE

Cyber Security für Industrieanlagen

Cyberangriffe auf Unternehmen, Energieversorger und Behörden sind eine reale Bedrohung. Wenn Hacker Schwachstellen im System finden, können sie ganze Industrieanlagen außer Betrieb setzen oder sogar die Energieversorgung gefährden. Die Sicherheit industrieller Automatisierungssysteme stand daher im Mittelpunkt einer Tagung des OVE Österreichischer Verband für Elektrotechnik.

OVE-Energietechnik-Tagung 2019: Umsetzung der #mission2030 erfordert geeignete Rahmenbedingungen.

Die österreichische Klima- und Energiestrategie sieht vor, dass der Stromverbrauch bis zum Jahr 2030 zu 100% (national bilanziell) durch erneuerbare Energieträger abgedeckt wird. Die Technologien und Potenziale dafür sind verfügbar.

OVE begeistert Mädchen für Technikjobs: Rekordteilnahme bei Girls! TECH UP

Mehr als 750 Schülerinnen zwischen 12 und 16 Jahren waren am vergangenen Freitag beim Erlebnistag Girls! TECH UP im Wiener Haus der Ingenieure mit dabei. Unter dem Motto „Du kannst Technik" erlebten sie die faszinierende Berufswelt der Elektro- und Informationstechnik hautnah.

„Klima wenden – mit Naturwissenschaft und Technik das Klima schützen": Videowettbewerb von ScienceClip.at gestartet

Bereits zum siebenten Mal veranstaltet ScienceClip.at, eine Initiative des OVE Österreichischer Verband für Elektrotechnik, gemeinsam mit AIT Austrian Institute of Technology einen Videowettbewerb für Schülerinnen und Schüler ab der 5. Schulstufe. Gefragt sind diesmal die besten Wissenschaftsvideos zum Thema Klimaschutz.

Mit freundlichen Grüßen
Ihr OVE Österreichischer Verband für Elektrotechnik

Hinweis: *Nicht immer werden in diesem Newsletter weibliche Formen explizit angeführt. Es wird jedoch ausdrücklich darauf hingewiesen, dass sich alle personenbezogenen Formulierungen grundsätzlich gleichermaßen auf Frauen und Männer beziehen. -*

Impressum:
OVE Österreichischer Verband für Elektrotechnik
Krenngasse 37
8010 Graz