Trolle, die das Narrativ in den Medien und im Internet kontrollieren

Wie man Robotern, Bots, «Seelöwen» auf die Spur kommt, die versuchen, unbequeme Nachrichten zu neutralisieren

Aus einer Episode von Solution's Watch von James Corbett[1]

Seien wir ehrlich: Die «Kommentare» am Ende von Videos oder Artikeln sind oft schlecht. Aber wer kann schon sagen, ob sie echt sind? Und was ist die Lösung für diese katastrophalen Posts? Die Kommentare nicht zu lesen, natürlich. Aber diejenigen, die sich auf diese öffentlichen Schlachtfelder wagen, sollten zumindest die verschiedenen Taktiken kennen, die Trolle,* Bots,* Spione und «Seelöwen» anwenden, um ihr Denken und Handeln zu hemmen.

(Bild zvg)

Traffic von Robotern

Kommentare können eine sehr reiche Quelle für zusätzliche Informationen sein, insbesondere zu kontroversen Themen, und dieser Abschnitt gewinnt tendenziell an Bedeutung im Vergleich zum Hauptinhalt der Publikation. Es ist jedoch nicht ungewöhnlich, dort eine Fülle von diffamierenden Äusserungen zu finden, wie zum Beispiel antisemitische, obszöne oder beleidigende Ausdrücke. Auch wenn sich die meisten Content*-Ersteller daran gewöhnt haben, diesen nicht allzu viel Bedeutung beizumessen, kann dies ernsthafte Auswirkungen auf die Weitergabe eines Videos oder die Abonnentenzahl des Kanals haben.

Die erste Frage ist, ob die betreffenden Kommentare von echten Internetnutzern stammen oder von einem Algorithmus generiert werden. Laut einem *Artikel von Tech Radar*[2] in dem ein Bericht über Bots analysiert wurde, sind 47% des Webtraffics* – per Definition, wäre man versucht zu sagen – auf Bots zurückzuführen, eine Zahl, die jährlich um etwa 5% steigt, während der Anteil des Traffics, der auf Menschen zurückzuführen ist, jedes Jahr abnimmt. Und fast 30% dieser «Bots» sind bösartig.

Bot-Traffic ist nicht per se negativ, da er für PDAs*, Suchmaschinen und Co. unerlässlich ist, aber er enthält leider auch eine Vielzahl von «Bad Bots». Diese werden beispielsweise Webseiten und mobile Anwendungen mit «Web Scraping»-Kampagnen (Extraktion von Informationen von Webseiten) und *Data Mining** (Datenextraktion) anvisieren, direkte Angriffe auf Webseiten oder Sendekanäle durchführen oder Banktransaktionen missbrauchen.

Einige Bots haben bestimmte Ziele und werden von Geheimdienstmitarbeitern gesteuert, die zur «Bekämpfung von Online-Desinformation» ernannt wurden.

Um Bot-Traffic zu verhindern, verwenden viele Websites Anwendungen, die die Nutzer zwingen, sich als «Mensch» zu identifizieren, und sie auffordern, einen kleinen visuellen oder auditiven Test durchzuführen. Dies lässt sich jedoch nur schwer auf den Kommentarbereich oder Gruppenunterhaltungen in Chat-Anwendungen anwenden. Ein Ausweg für Ersteller von Inhalten, die zu oft angegriffen werden, besteht darin, ihre Inhalte auf verschiedenen Plattformen zu veröffentlichen, den Kommentarbereich auf der einen Seite zu aktivieren, auf der anderen zu deaktivieren und überall die Links zu alternativen Veröffentlichungen zu erwähnen.

Die Technik der Trolle

Das ist keine Fantasie: Eine der Aufgaben der *Geheimdienste ist es, das Narrativ in den Medien und sozialen Netzwerken zu kontrollieren,*[3] da die Kontrolle der öffentlichen Meinung durch die Herstellung von Zustimmung *oder Zensur*[4] Schlüsselelemente jeder politischen Strategie sind. Der Kampf zwischen dem EU-Kommissar *Thierry Breton* und dem *X/Twitter*-Chef *Elon Musk* um die Kontrolle der *Nachrichten über den Krieg zwi-*

schen Israel und Gaza[5] ist ein guter Beweis dafür. Ebenso wie die *Zensur des Präsidentschaftskandidaten Robert Kennedy Jr.,*[6] der Skandal um die *vom Marianne-Fonds*[7] bezahlten «Faktenchecker» oder die Tatsache, dass *der Oberste Gerichtshof der USA über die Einmischung des Weissen Hauses*[8] in die Kontrolle der sozialen Netzwerke entscheiden muss.

Es gibt also neben den «natürlichen» Belästigungen auch vom Steuerzahler bezahlte Trolle. Diese Agenten werden beauftragt, das Narrativ zu kontrollieren, Gruppen zu infiltrieren und allzu störende Informationen zu neutralisieren. Sie operieren mit mehreren Identitäten gleichzeitig und auf verschiedenen Plattformen, um Gespräche zu verunreinigen und zu unterbrechen oder die Diskussion zu beeinflussen. Eine interessante Beschreibung einiger ihrer Vorgehensweisen findet sich in einem Dokument mit dem Titel *«The Gentle Person's Guide to Forum Spies»*[9] auf der Website *Cryptome.org* (einer *Wikileaks*-nahen Website), das sich auf die Methoden von *Cointelpro* bezieht.

Cointelpro ist offenbar ein disruptives Programm des US-Geheimdienstes, dessen Ziel die Verwässerung, Zweckentfremdung oder Übernahme eines Internetforums oder Internetdiskussionsplatzes, typischerweise eines Kommentarbereichs, ist.

Zu den verwendeten Techniken gehört zunächst die Bombardierung einer wichtigen Nachricht mit einer schnellen Folge von anderen Nachrichten, um sie in der Liste der Nachrichten «nach unten» zu verschieben und sie weniger sichtbar zu machen.

Dann gibt es noch die «Schwächung des Konsenses». Hier geht es darum, eine gegenteilige Meinung zu posten, indem man mit einem eher schwachen Vorschlag ohne viele Argumente beginnt, der aber nach und nach unter anderen Benutzernamen verstärkt wird, damit der Leser wirklich den Eindruck hat, dass nach und nach eine Gegenargumentation aufgebaut wird, die den zuvor herrschenden Konsens umstösst.

Die «Verwässerung» des Themas ist eine weitere Technik, bei der die Leser ständig auf Nebenthemen, Nebengleise, geführt werden, um Zeit zu verschwenden und sie in Untätigkeit zu halten. Auf Dauer wird dies dazu führen, dass die produktiven Nutzer das Forum verlassen, während die anderen von der Analyse relevanter Fakten in den Modus des «Plauderns» wechseln.

Der «Agent» wird die Gelegenheit nutzen, um Informationen in der Gruppe zu sammeln, indem er zunächst über seine eigenen Interessen spricht. Zum Beispiel, indem er eine Frage stellt wie: Welches System nutzen Sie, um Ihre Privatsphäre zu schützen? Oder: Woher beziehen Sie Ihre Ressourcen? Oder sogar Fragen, die das Privatleben der Internetnutzer betreffen.

Eine andere wiederkehrende Taktik ist eine gewalttätige Diskussion zwischen zwei vom Troll-Agenten kontrollierte Identitäten. Wenn sich andere an der hitzigen Diskussion beteiligen, werden sie wahrscheinlich Dinge sagen, die über ihre geplanten Aussagen hinausgehen und für die sie später wegen Beleidigungen oder Aufstachelung zu Hass und Gewalt angeklagt werden können.

Zerschlagung der Argumente

Die am häufigsten verwendeten Techniken, um eine solide Argumentation zu zerschlagen, sind folgende: die Aufmerksamkeit vom Thema ablenken auf diejenigen, die es vertreten oder ihre Gedanken darlegen: Lynchjustiz, Spott, Beleidigungen oder Empörung – in der Regel wird ein ganzes emotionales Register aufgefahren, um vom eigentlichen Argument abzulenken.

Eine andere, weniger leicht zu entdeckende Methode, um sachliche Erläuterungen zu unterbrechen, ist die «Seelöwentechnik». Sie besteht aus einer höflichen und «naiven» Belästigung durch wiederholte Fragen. So wird zum Beispiel jede Behauptung bestritten, indem man um «Beweise» bittet, die dann immer wieder entkräftet werden. Das können auch Nebenfragen sein, die immer wieder beantwortet werden müssen, oder die ständige Aufforderung, eine unnötige Debatte zu beginnen. Ziel ist es, dass der Nutzer und die Leser die Geduld verlieren, indem sie zur Verärgerung oder zum Abbruch des Gesprächs veranlasst werden. Wie immer bei Trollen ist es am besten, ihr Handeln anzuprangern, bevor man aufhört zu antworten.

Um diese Unterminierung zu neutralisieren, muss man sich zunächst einmal bewusst machen, dass es diese Techniken gibt. Am besten ist es dann, sie am Ort der Diskussion zu melden. Dabei ist es unerheblich, ob es sich um eine echte Infiltration handelt oder um spontane Saboteure. Wichtig ist vor allem, zu zeigen, dass solche Interaktionen kontraproduktiv sind und dass man nicht in diese Falle tappen sollte.

Kurzum, wenn man aufmerksam den Gesprächsverlauf verfolgt, kann man sich eher wieder auf die Grundlage der eigenen Meinung konzentrieren. In welchem Umfang und auf welche Weise wurde unsere Aufmerksamkeit letztlich

auf Nebenthemen oder falsche Schlussfolgerungen gelenkt? Und wie kann sich das auf unser Handeln auswirken? Denn man darf nicht vergessen, dass diese Techniken in erster Linie dazu dienen, Argumente und Personen zu entwaffnen, die eine konkrete Veränderung der gesellschaftlichen Organisation bewirken könnten, indem sie beispielsweise politisch aktiv werden oder die Gerichte anrufen.

Und schliesslich muss man sich, noch bevor man die Gesprächsteilnehmer verdächtigt, niederträchtige Agenten im Auftrag der herrschenden Mächte zu sein, auch fragen, inwieweit man selbst anfällig für die unbewusste Anwendung dieser wenig lobenswerten Techniken ist. Ist das nicht die Haltung eines wahren Gentlemans?

Quelle: Information von CovidHub, https://www.covidhub.ch/guide-gentleman-trolls/, 23. Oktober 2023

[1] *https://www.bitchute.com/video/8dyhRfC5lAWx/*

[2] *https://www.techradar.com/news/bots-now-make-up-nearly-half-of-all-internet-traffic-and-thats-very-bad-news-for-our-security*

[3] *https://sentadepuydt.substack.com/p/la-cia-et-le-fbi-a-la-tete-de-la*

[4] *https://www.covidhub.ch/incontournables-3-censure/*

[5] *https://www.covidhub.ch/guerre-gaza-europe-controle-info/*

[6] *https://www.covidhub.ch/la-censure-des-geants-dinternet/*

[7] *https://www.francesoir.fr/recherche?search_api_fulltext=fonds%20marianne&page=0*

[8] *https://childrenshealthdefense.org/defender/texas-law-social-media-censorship-supreme-court/*

[9] *https://cryptome.org/2012/07/gent-forum-spies.htm*

* **Glossar** (ohne Gewähr)

Trolle

Als Troll bezeichnet man im Netzjargon eine «Person», die im Internet vorsätzlich mit «zündelnden» Kommentaren einen verbalen Disput entfachen oder absichtlich Menschen im Internet verärgern will. Dies geschieht normalerweise durch das «Posten» entzündlicher und abschweifender, irrelevanter oder nicht themenbezogener Nachrichten und Beiträge in einer Online-Community. Ihre Kommunikation in diesen Communitys ist auf Beiträge beschränkt, die auf emotionale Provokation oder Verunsicherung anderer Gesprächsteilnehmer zielen.

Data Mining

ist der Prozess der Extraktion nützlicher Informationen aus einer Ansammlung von Daten. Data-Mining-Tools umfassen leistungsstarke statistische, mathematische und analytische Funktionen. Ihre primäre Aufgabe ist die Analyse grosser Datenmengen, um Trends, Muster und Beziehungen zu erkennen, die eine fundierte Entscheidungsfindung und Planung ermöglichen.

Content

bedeutet wörtlich übersetzt «Inhalt». Unter Content werden alle Inhalte einer Webseite im Internet zusammengefasst. Das können Texte, Videos, Bilder oder andere digitale Inhalte wie zum Beispiel Audio-Dateien sein. Für die Nutzer der Webseiten ist der Content also der eigentliche Teil der Seite, der sie interessiert – unabhängig davon, ob der Content von den Betreibern der Seite oder von anderen Nutzern erstellt wird. Im zweiten Fall spricht man vom Web 2.0, das Sie zum Beispiel in sozialen Netzwerken, Blogs oder ähnlichem wiederfinden. Content ist auch bedeutend für die Betreiber der Seite: Je besser, vielfältiger und relevanter der Content, desto einfach wird die Seite beispielsweise in einer Suchmaschine gefunden.

Bots

Die Bezeichnung «Bot» leitet sich vom englischen Wort für Roboter ab. Wie mechanische Roboter sind Internet-Bots darauf programmiert, spezifische, sich wiederholende Aufgaben zu erfüllen. Dazu führen sie in Form von Algorithmen und Skripten klar definierte Befehle aus, die sie schneller umsetzen, als jeder Mensch es könnte. Bots sind somit Computerprogramme, die eigenständig und automatisiert agieren und in ihrer Funktion nicht auf die Mitwirkung oder Überwachung durch Menschen angewiesen sind.

Malware Bots dienen verschiedenen illegalen Zielen. Dazu zählen:

- Daten- und Identitätsdiebstahl durch Scraping, Phishing und Keylogging von sensiblen Informationen wie Passwörtern, Bankdaten und Adressdaten.
- Distributed Denial-of-Service-Angriffe (DDos), durch deren massiven Datenverkehr Server lahmgelegt werden können.
- Nutzung von Backdoors im Sicherheitssystem eines PCs, um das System zu infizieren.
- Retrans mit Spam, um Datenpakete umzulenken.

Dazu gehören folgende Arten:

- Propaganda- oder Manipulative Bots: Social Bots, die User-Profile simulieren, digitale Meinungsbildung betreiben und politische Aussagen, Fake News und Verschwörungstheorien verbreiten oder anhand von Keywords auf Kommentare und Posts reagieren.
- Scam/Phishing Bots: Diese Bots betreiben Datendiebstahl durch Pseudo-Links, Fake Mails und Fake Websites.
- Keylogging Bots: Bots, die Nachrichtenverkehr speichern oder alle Aktivität auf einem PC notieren, speichern und weiterleiten.
- File-Sharing Bots: Bots, die auf gezielte Suchanfragen reagieren und Usern einen Link zum gewünschten Suchbegriff anbieten. Bei Anklicken dieses Links kann der Bot den vom Menschen genutzten PC infizieren.
- Spam Bots: Sie senden in grossen Mengen Spam-Mails und nutzen Adressbücher und Kontakte von arglosen Usern, um ihren Spam-Radius gezielt zu erweitern.
- Zombie Bots: Sogenannte Zombie Bots sind Computer, die durch Bots mit Malware infiziert oder zum Teil eines Botnets gemacht wurden und Rechnerleistung für grosse Botnet-Attacken bereitstellen. Oft sind kompromittierte PCs nicht leicht als Teil eines Botnets erkennbar.

- Botnet: Bezeichnet die Gesamtheit von infizierten PCs, die zu einem Netzwerk zusammengeschlossen werden und von den Anwendern der Malware Bots für DDoS-Attacken verwenden werden.

Die fünf häufigsten, grossangelegten Bot-Angriffe sind:

- DDoS-Attacken: Gezielt herbeigeführte Überlastung von Servern.
- Spamming und Traffic Monitoring: Überlastung von Mailservern oder grossangelegter Datendiebstahl.
- Inventory Denial Attacken: Angriffe auf Online-Shops, um Produkte als «nicht verfügbar» zu listen.
- Scraping Attacken: Datendiebstahl und Datenverkauf.
- Credential Stuffing Attacken: Verwendung gestohlener Account-Daten und automatisierte, grossflächige Login-Versuche.

PDA

Ein Personal Digital Assistant, (persönlicher digitaler Assistent) ist ein kompakter tragbarer Computer, welcher hauptsächlich für die persönliche Kalender-, Adress- und Aufgabenverwaltung benutzt wurde. Gebräuchlich waren PDAs in den 1990er und 2000er Jahren.

Web-Traffic

Unter Traffic versteht man die Anzahl und Häufigkeit der Nutzerzugriffe auf eine Webseite. Traffic ist also für jede Website ein entscheidender Erfolgsfaktor. Wo kommt der Traffic her? Wie kann man den Traffic erhöhen? Die entsprechenden Daten gewinnt man beispielsweise über Analysetools – eines der meistgenutzten ist Google Analytics. Dabei handelt es sich um einen Dienst, der unsichtbar den Besucher in den Quellcode der Website einbauen kann.