Wussten Sie eigentlich, dass ein großer Teil der fremdenfeindlichen Beiträge in den Sozialen Netzwerken während der Flüchtlingskrise von sogenannten Social Bots kam? Und wussten Sie, dass während des ersten Phase des Bürgerkriegs in der Ost-Ukraine Social Bots aus dem Umfeld des „Rechten Sektors" über rund 15.000 Twitter-Accounts täglich rund 60.000 Meldungen abgesetzt haben? Im US-Wahlkampf waren diese Bots genauso aktiv wie beim Brexit-Referendum. Wer hinter diesen Bots steht, ist unbekannt. Interessant ist in diesem Zusammenhang jedoch, dass die US-Regierung bereits 2010 eine Spezialsoftware entwickeln ließ, mit der man ein ganzes Heer von Social Bots steuern kann und amerikanische Softwaredienstleister aus dem Umfeld der Geheimdienste laut geleakten Mails offenbar seit Jahren diese Technologien beherrschen. Und da regen wir uns über vermeintliche Putin-Trolle auf? Das Thema Social Bots wird uns noch häufig beschäftigen. Von **Jens Berger**.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

http://www.nachdenkseiten.de/upload/podcast/170203_Die_Meinungsroboter_kommen_NDS.mp3

Podcast: Play in new window | Download

Nach der ersten TV-Debatte zwischen Donald Trump und Hillary Clinton wurde mehr als jeder dritte Tweet zur Unterstützung von Trump und auch mehr als jeder fünfte Tweet zur Unterstützung von Clinton nicht von einem Menschen, sondern von einer Maschine, einem Social Bot abgesetzt. Social Bots, die in den Netzen gegen Trump eingesetzt wurden, gingen dabei besonders phantasievoll vor: zunächst posteten sie frauen- und fremdenfeindliche Sprüche, um erst einmal in die „Filterblase" der Trump-Sympathisanten vorzudringen, nur um dann Trump zu kritisieren und zur Wahl seiner Konkurrenten aufzurufen.

Eine ähnliche, aber noch professionellere Methode wendeten die Bots an, die 2014/2015 im Ukraine-Konflikt auf Seiten des rechten Sektors in den sozialen Netzwerken ihr Unwesen trieben. Die Bots posteten in der ersten Phase vor allem unverfängliche Inhalte, die vor allem die Zielgruppe der jungen Männer ansprechen sollten – also Fußball, Frauen und Raubkopien. Als die Lage im Osten des Landes eskalierte, streuten die Bots auf einmal politische Botschaften in Beiträge ein – und diese Botschaften kamen von ganz rechts außen, vom Rechten Sektor. Schon während des Euromaidans waren Bots für den Rechten Sektor im Einsatz. Unter anderem versuchte man damals, die Algorithmen von Twitter zu manipulieren.

Dass auch in Deutschland bereits Social Bots aktiv sind, belegt eine sehr sehenswerte Reportage von ZDFzoom mit dem Titel „Alles nur Lüge?“[*]

Dem Social-Media-Forensiker Simon Hegelich von der TU München zufolge waren die Seiten der CSU während der Flüchtlingskrise offenbar eine der Epizentren für Social Bots. Rein professionell macht dies natürlich gleich doppelt Sinn: Einerseits holen Pegida, AfD und Co. ihre künftigen Anhänger da ab, wo sie sind, und andererseits erzeugt der konzertierte Angriff auf die CSU-Netzwerke eine manipulierte „Basis-Meinung“, die auch in die Auswertung der CSU-Analytiker eingeht und sicher mitverantwortlich für den neuerlichen Rechtsdrall der Bayern ist. Überhaupt ist es auffällig, dass Social Bots immer wieder vor allem im Umfeld der politischen Rechten auftauchen. Da passt es dann auch ins Bild, dass die AfD als einzige Partei im Bundestagswahlkampf Social Bots aktiv einsetzen will. Das Thema wird uns also in diesem Jahr noch beschäftigen. Da lohnt es sich, dem Phänomen Social Bots ein wenig auf den Zahn zu fühlen.

Der klassische Troll als Opfer der Rationalisierung

1965 erblickte ELIZA die Welt. ELIZA ist das Kind des deutschen IT-Experten Joseph Weizenbaum. Doch ELIZA ist natürlich kein normales Kind. ELIZA war vielmehr die erste Software, die – wenn auch rudimentär – auf Basis künstlicher Intelligenz mit einem echten Menschen kommunizieren konnte. Im Fachjargon werden solche textbasierten Dialogsysteme Chatbots genannt. Seit 1965 hat sich auf dem Gebiet natürlich viel getan. Heute werden Chatbots vor allem bei Hotlines und Kundendialogsystemen eingesetzt. Kundenbetreuer und Telefonisten kosten schließlich selbst dann viel Geld, wenn die Stellen nach Rumänien oder Indien outgesourct wurden; Software ist dagegen vergleichsweise günstig.

Auch im letzten Jahr eroberten mal wieder die „Trolls aus Olgino“ die Schlagzeilen – Mitarbeiter einer regierungsnahen russischen PR-Agentur, die offenbar auch dafür eingesetzt wurden, um in den sozialen Netzwerken und den Kommentarspalten von Online-Medien Einfluss auf Debatten zu nehmen. Auch wenn die von deutschen Medien gestreuten Erzählungen, nach denen fast jeder russlandfreundliche Kommentar von einem „Putin-Troll“ stammen soll, natürlich Unsinn sind, kann man es als gegeben betrachten, dass derlei politische PR-Aktivitäten keine Seltenheit sind. Israel bezahlt Agenturen für PR-Arbeit in Internetforen, Großbritannien und die USA ebenfalls, wie wir spätestens seit Edward Snowdens Enthüllungen wissen sollten. Derlei „händische“ Meinungsmache hat jedoch einen entscheidenden Nachteil: Sie ist teuer! Vor allem, wenn es darum geht, im ganz großen Stil aktiv zu werden, um z.B. im Wahlkampf die Zustimmungswerte eines

Kandidaten zu manipulieren. Sobald eine große Anzahl von Akteuren benötigt wird, scheidet die „manuelle“ Manipulation schnell aus finanziellen und auch logistischen Gründen aus. Es ist ja nicht damit getan, einfach irgendwo ein paar vorgefertigte Satzfragmente zu posten. Die Accounts müssen zunächst einmal registriert, miteinander vernetzt und über längere Zeit gepflegt werden, bevor sie einsatzbereit sind. Ansonsten fliegen derlei „Trollereien“ nämlich ziemlich schnell auf.

Die KI-Forschung (KI = Künstliche Intelligenz) hat daher dafür gesorgt, dass wohl die meisten dieser bezahlten „Trolle“ durch Chatbots ersetzt wurden. Wenn es um den Einsatz von Chatsbots in sozialen Netzwerken geht, spricht man von Social Bots. Die sind wiederum eine vergleichsweise neue Entwicklung, die immer noch in den Kinderschuhen steckt.

Was ist ein Social Bot?

Es gibt die unterschiedlichsten Formen von Social Bots. Angefangen bei sehr einfach strukturierten Programmroutinen, die „auf Zuruf“ auf Twitter oder Facebook einfache Aktionen durchführen – wie z.B. Facebook-Beiträge zu teilen und Twitter-Nachrichten zu „retweeten“ (also weiterzuverbreiten) oder Beiträgen in diesen Netzwerken ein „gefällt mir“ zu verpassen oder sie zu „favorisieren“. Die nächste Stufe sind autonome Bots, die mit ausgefeilteren Routinen selbst Meldungen absetzen und sogar mit anderen realen oder virtuellen Nutzern diskutieren; die besseren Bots variieren dabei sogar ihre Formulierungen, sodass es für Außenstehende nicht immer einfach ist, sie überhaupt als Bots zu erkennen. Die Königsklasse – zumindest unter den Bots, die bislang entdeckt wurden – versteht sich sogar meisterhaft in der Kunst der Täuschung und postet über lange Strecken erst einmal normale Beiträge, bevor sie zwischendurch politisch wird.

Während die einfachen Formen meist als Schadsoftware auf tausenden fremden Rechnern (sogenannte Botnets) laufen, werden die fortschrittlicheren Programme sorgsam in abgeschotteten Rechenzentren vor neugierigen Blicken verwahrt. Ein ausgeklügeltes IP-Adressen-Management gehört ebenso dazu, wie „echte“ Mail-Accounts und „Legenden“ (also ausgedachte Lebensläufe in den sozialen Netzwerken, inkl. gefälschter Familienfotos, Freunde usw. usf.). In der Fachsprache werden solche virtuellen Identitäten „Personas“ genannt.

Wie ein Modell für eine ganze Armee von Meinungsrobotern auszusehen hat, umreißt eine interne Mail des IT-Sicherheitsdienstleisters HB Gary Federal, die 2011 vom bekannten US-Blog „Daily Kos“ veröffentlich wurde. In dieser von realen Hackern geleakten Mail diskutieren ranghohe Mitarbeiter von HB Gary über die Konzeption eines IT-Projekts, mit dem Kunden zahlreiche Personas zentral verwalten können.

Diese Personas sind dabei nicht nur einzelne Nutzer, sondern ausgefeilte Komplettlösungen mit dazugehörigen Identitäten in sozialen Netzwerken wie Facebook und Twitter und simulierter Interaktivität untereinander und mit anderen – realen – Nutzern. Feinheiten, wie unauffällige statische und dynamische IP-Nummern und "echte" Mail-Accounts gehören ebenfalls zum Konzept von HB Gary. Ein solches Konzept erlaubt es beispielsweise dem Kunden, ein ganzes Heer von virtuellen Identitäten zentral zu steuern, sie in Foren, Blogs und sozialen Netzwerken interagieren zu lassen und so den Eindruck zu erwecken, es handele sich um eine ganze Schar von Nutzern, die eine bestimmte Meinung vertreten.

Besonders heikel ist in diesem Zusammenhang, dass HB Gary Federal eine 100%-Tochter des IT-Dienstleisters HB Gary ist, die sich ausschließlich mit Dienstleistungen für die öffentliche Hand beschäftigt und in enger Verbindung zu den Geheimdiensten, dem Verteidigungsministerium und diesbezüglich spezialisierten Anwaltskanzleien und PR-Unternehmen steht. Vermeintlicher Auftraggeber des "Persona-Projekts" ist die Firma Mantech, die ihrerseits ausschließlich für das US-Militär, die US-Geheimdienste und verschiedene Ministerien arbeitet. Die Ausrichtung des Projekts ist damit klar: Der amerikanische Staat will das Netz zur Verbreitung von Regierungspropaganda nutzen, ohne dass der Urheber ermittelt werden kann.

Dass die USA Interesse an solchen Dienstleistungen haben, wird bereits durch eine Ausschreibung der US Air Force aus dem Juni 2010 deutlich. In der Ausschreibung mit der Nummer RTB220610 sucht die Air Force nach einer "Persona-Management-Software", mit der 50 Nutzer ein kleines Heer von 500 virtuellen Online-Kriegern verwalten und steuern können – Extras, wie beispielsweise ein VPN, IP-Management und virtuelle Server inklusive. Die Vermutung, dass HB Gary damals die Ausschreibung gewonnen hat, liegt auf der Hand. Wir können also davon ausgehen, dass die amerikanischen Dienste in Besitz einer sehr hochentwickelten Technik sind, mit der sie virtuelle Meinungsroboter einsetzen kann, ohne dabei Spuren zu hinterlassen, die auf den ersten Blick erkennbar sind.

Zum Weiterlesen: Simon Hegelich – Invasion der Meinungs-Roboter

---

[«*] Die in der Reportage angesprochene „Twitter-Studie" des russischen Philosophie-Professors Wladimir Schalack sollte mit äußerster Vorsicht aufgenommen werden, da sie methodisch sehr schwach ist. Schalack hat seine Analyse ausschließlich mit englischsprachigen Suchwörtern vorgenommen. Wusste er nicht, dass deutsche Twitter-

Nutzer fast ausschließlich in ihrer Muttersprache twittern? So sind die Ergebnisse wissenschaftlich unbrauchbar.