Social Bots

Auswirkungen des Gesetzentwurfs zum Digitalen Hausfriedensbruchs

Wiesbaden, den 8. Februar 2017

Social Bots sind von Menschen programmierte Software-Roboter. Sie suchen in sozialen Netzwerken eigenständig nach Themen, verbreiten Beiträge weiter und geben Kommentare ab, die so aussehen wie Posts von echten, menschlichen Nutzern. Dazu werden Fake Accounts, also Profile, die unter Falschpersonalien eingerichtet werden, genutzt. Es wird aufgrund der fortschreitenden Technik immer schwerer, Bots von Menschen zu unterscheiden. Social Bots werden zunehmend im politischen Kontext eingesetzt. Dabei geht es darum, die Öffentlichkeit oder bestimmte Zielgruppen durch die automatisch generierten Inhalte und Interaktionen zu beeinflussen.

Technisch gesehen sind Social Bots heute sehr einfach zu erstellen[1]. Man braucht dafür Nutzeraccounts, die in dem entsprechenden sozialen Netzwerk registriert sind und ein Programm, das die Bot-Accounts automatisch steuert. Die auf erfundene Personalien registrierten Nutzeraccounts werden kann man im Internet käuflich erwerben. Anbieter von falschen Social Media Accounts erstellen diese entweder per Hand oder gleich automatisiert oder bieten auch Zugangsdaten zu gehackten Accounts an. Je nach Qualität zahlt man derzeit für 1.000 falsche Accounts zwischen 45 USD (einfache Twitter-Accounts) und 150 USD

1 Vgl. zum Nachfolgenden: Prof. Hegelich, Analysen und Argumente Nr. 221, Hrsg.: Konrad-Adenauer-Stiftung

Pressesprecher: René Brosius
Luisenstraße 13 • 65185 Wiesbaden
Telefon: 0611 322695 • Telefax: 0611 322691

pressestelle@hmdj.hessen.de
http://www.justizministerium.hessen.de
https://twitter.com/justiz_hessen

(„gealterte“ Facebook-Accounts, also solche, die schon eine Historie aufweisen und damit plausibler wirken). Die Anbieter sind in der Regel im Ausland (häufig in Osteuropa) tätig. Die Software zur Steuerung der Bots kann entweder ebenfalls käuflich erworben werden. Eine Software, mit der sich 10.000 Twitter-Accounts steuern lassen, kostet ca. 500 USD.

Die Unterschiede zwischen der Leistungsfähigkeit von Bots sind groß. Im einfachsten Fall beschränkt sich das selbständige Handeln dieser Roboter darauf, vorgefertigte Nachrichten zu versenden. Es gibt aber auch Bots, die in der Lage sind, mit echten Nutzern zu interagieren und eigenständig neue Texte zu generieren. Da die normale Kommunikation in den sozialen Netzwerken in der Regel nicht besonders komplex ist, fallen aber auch die einfachen Bots häufig nicht auf. Ein typischer Bot auf Twitter könnte z. B. Nachrichten selbstständig erzeugen, die auf Texten aus zuvor ausgewählten Webseiten basieren, anderen Nutzern automatisch folgen, auf „Knopfdruck“ oder auch nach einem zufallsvarierten Zeitplan vorgefertigte Propagandanachrichten senden und diese mit Stichworten und Hashtags versehen, die derzeit populär sind.

Der Einsatz von Bots ist beliebig skalierbar: Wer ein Programm hat, mit dem sich ein Bot steuern lässt, kann damit auch eine ganze Armee von Bots lenken. Aus der schieren Masse der Nachrichten, die sich durch ein Botnetz absenden lassen ergibt sich die aktuell bedeutendste Gefahr: Bots manipulieren die Trends in sozialen Netzwerken und diese Trends fließen in politische und wirtschaftliche Entscheidungsprozesse ein. Unter dem Schlagwort „Big Data“ setzen immer mehr Unternehmen in den unterschiedlichsten Bereichen darauf, das Verhalten der Nutzer in den sozialen Netzwerken zu analysieren, um Erkenntnisse über die Position der eigenen Marke, aber auch über das Verhalten von potentiellen Kunden zu erhalten oder gesellschaftliche Trends zu entschlüsseln. Auch im politischen Bereich werden solche Analysen bereits eingesetzt. Während man dabei in Deutschland noch relativ zurückhaltend agiert, hat sich die politische Social Media Analyse international bereits zu einem bedeutenden Markt entwickelt.

Wenn nun Trends im großen Stil durch Bots manipuliert sind und Bots in allen Debatten von Bedeutung mitmischen dann sind diese Analysen im harmlosesten Fall schlicht unzutreffend. Im schlimmsten Fall können sie politische Entscheidungsträger dazu verleiten, in ihren Statements oder sogar in ihrer Politik auf solche Trends einzugehen. Eine weitere Gefahr besteht darin, dass bestimmte Gruppen in ihrer Meinung durch Bots beeinflusst werden. Wenn beispielsweise

durch Bots massenhaft extreme Inhalte in einem Diskussionskontext (wie z.B. eine Facebook-Gruppe oder ein thematischer Hashtag) verbreitet werden, dann kann dies dazu führen, dass sich gemäßigte Personen aus diesem Diskussionszusammenhang zurückziehen. Personen, die eine konträre Position zu den Bot-Nachrichten haben, fühlen sich herausgefordert, gegen diese Inhalte vorzugehen, was wiederum Personen, die die von den Bots verbreitete Meinung teilen, zu Gegenäußerungen veranlasst. So entsteht ein aufgeheiztes Diskussionsklima, in dem Personen, die tendenziell für radikale Positionen empfänglich sind, sich ermutigt fühlen.

Daneben können Bots auch gezielt in einem Cyber-Warfare-Szenario angewandt werden. Dabei reicht die Spannbreite von der Unterwanderung sozialer Netzwerke zur Ausspionierung der Nutzer, über die gezielte Verbreitung von Falschnachrichten (z. B. in Krisensituationen), bis hin zu Cyber-Attacken wie der Verbreitung von Schadsoftware oder auch der Organisation von sogenannten DDoS-Attacken. Hierzu werden sogenannte „Social Engineering“ Strategien angewandt, bei denen es darum geht, mit Hilfe von psychologischen Tricks wie zum Beispiel Suggestion Einfluss auf den User zu nehmen, um den gewünschten Effekt zu erzielen. So kann künstliche Intelligenz genutzt werden, um einzelne Nutzer über Bots mit Schadsoftware zu infizieren. Dafür kann man Programme verwenden, die automatisch so etwas wie den perfekten Social Media-Freund für einen beliebigen Nutzer generieren. Das Programm analysiert die Nachrichten des Nutzers und versucht dann, selbstständig Nachrichten zu erzeugen, die für diesen Nutzer von großem Interesse sind. Diese Nachrichten werden mit einem Link verbunden, der auf eine Internetseite mit Schadsoftware verweist. In Tests klickte die Hälfte der Testpersonen diesen Link tatsächlich an. Bei diesem Vorgehen handelt es sich um eine Unterkategorie des sogenannten Phishing. Das sogenannte Spear Phishing passt die Nachrichten an die einzelnen Nutzer an und benutzt dafür Informationen, die aus den sozialen Netzwerken gesammelt werden. Dies nun über eine Software zu automatisieren und mit einem Botnetzwerk zu verbinden, also Automated Spear Phishing, bedeutet, dass im Zweifelsfall jeder von einem ganz persönlich auf ihn abgestimmten Bot angegriffen werden kann.

Nach gegenwärtigem Recht ist der Einsatz von Social Bots grundsätzlich nicht strafbar.

Sofern ein soziales Netzwerk den Einsatz von Fake Accounts in seinen Allgemeinen Geschäftsbedingungen (AGB) verbietet, wäre ihr Einsatz unter Geltung des hessischen Entwurfs für das Gesetz zur Strafbarkeit des Digitalen Hausfriedensbruchs (Antibotnetzgesetz) in der Regel strafbar.

Absatz 1 des Entwurfs lautet:

„§ 202e

Unbefugte Benutzung informationstechnischer Systeme

(1) Wer unbefugt

1. *sich oder einem Dritten den Zugang zu einem informationstechnischen System verschafft oder*
2. *ein informationstechnisches System in Gebrauch nimmt oder*
3. *einen Datenverarbeitungsvorgang oder einen informationstechnischen Ablauf auf einem informationstechnischen System beeinflusst oder in Gang setzt*

wird mit Geldstrafe oder Freiheitsstrafe bis zu drei Jahren bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. Die Tat nach Satz 1 ist nur strafbar, wenn sie geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen.

(2) - (7)

(…)

Der Einsatz von Social Bots entgegen den AGB eines sozialen Netzwerkes wäre das unbefugte In-Gang-Setzen eines informationstechnischen Ablaufs auf einem informationstechnischen System. In der Gesetzesbegründung ist klargestellt, dass auch der Verstoß gegen zivilrechtliche Vorgaben „unbefugt“ im Sinne der Vorschrift ist. Sowohl Facebook als auch Twitter verbieten grundsätzlich den Einsatz von Fake Accounts.

Überlegungen, ein staatliches Eingreifen an den Inhalten von durch Social Bots verbreiteten Nachrichten festzumachen, sind verfassungsrechtlich nicht unbedenklich. Bei der Diskussion über Fake News und Hate Speech ist es hilfreicher, die technische Dimension des Problems in den Blick nehmen und bei den Werkzeugen, die die großflächige Manipulation der öffentlichen Meinung erst möglich machen, anzusetzen, nämlich dem massenhaften Gebrauch von Social Bots als ein Unterfall der Botnetzkriminalität. Auch hiergegen richtet sich der Hessische Gesetzentwurf.