

Schriftliche Kleine Anfrage

des Abgeordneten Carsten Ovens (CDU) vom 29.09.2016

und Antwort des Senats

- Drucksache 21/6182 -

Betr.: Die Bots kommen – ist der Senat gerüstet?

Social Bots sind zu einem Massenphänomen geworden. Ob gesteuert aus „Trollfabriken“ in Russland oder den USA, bei Abstimmungen wie dem Brexit, der russischen Annexion der Krim oder im aktuellen US-Wahlkampf: immer häufiger greifen die computergesteuerten Programme manipulativ in den Meinungsbildungsprozess ein.

Bots betreiben Fake-Profilen und geben immer häufiger täuschend echt vor, reale Personen zu sein. Diese Entwicklung stellt die Akteure gesellschaftlicher Diskussionen in den digitalen sozialen Medien vor neue Herausforderungen. Umso wichtiger sind deshalb eine offene Debatte und eine breite Aufklärung, um zum kompetenten Umgang mit Social Bots beizutragen. Hamburg soll laut rot-grünem Senat zur Innovationsmetropole ausgebaut werden. Dazu gehört es auch, die zentralen Themen der Digitalisierung mit ihren Auswirkungen auf Wirtschaft und Gesellschaft in den Fokus zu nehmen.

Vor diesem Hintergrund frage ich den Senat:

Der Senat beantwortet die Fragen teilweise auf Grundlage von Dataport AöR (Dataport) wie folgt:

1. *Hat sich der Senat mit der Entwicklung von Social Bots und ihren Fähigkeiten (z.B. im Kontext von Automated Spear Phishing oder Social Engineering) sowie mit möglichen Auswirkungen auf Hamburg befasst? Wenn ja, inwiefern und mit welchem Ergebnis? Wenn nein, warum nicht?*

Die zuständige Behörde informiert sich ständig über aktuelle Entwicklungen der IT-Sicherheit und arbeitet dabei eng mit anderen Organisationen (wie dem Bundesamt für Sicherheit in der Informationstechnik, dem Computer-Emergency-Response-Team Nord (CERT-Nord) der Dataport-Trägerländer und Dataport) zusammen. Dabei ist das Thema „Social Bots“ eines der aktuell diskutierten Angriffsszenarien. Neben der laufenden Fortentwicklung von technischen und organisatorischen Maßnahmen werden zurzeit zusätzlich Sensibilisierungs-Kampagnen entwickelt und durchgeführt.

2. *Welche Fälle sind dem Senat in den vergangenen 24 Monaten bekannt geworden, in denen Cyber-Attacken auf Hamburger Behörden, städtische Unternehmen oder privatwirtschaftliche Einrichtungen durch Bots stattgefunden haben? Welcher Schaden ist dabei im Detail entstanden? Bitte ohne Verweis auf andere Drucksachen beantworten.*

Dem Senat sind keine Fälle von Cyberattacken auf Hamburger Behörden, städtische Unternehmen oder privatwirtschaftliche Einrichtungen bekannt.

3. *Hat sich der Senat im Kontext der Medienkompetenzförderung damit befasst, wie Nutzer digitaler sozialer Medien Bots besser erkennen und mit ihnen umgehen können? Wenn ja, mit welchem Ergebnis? Wenn nein, warum nicht?*

Die für Bildung zuständige Behörde legt bereits für den Unterricht in der Grundschule verbindlich fest, dass Schülerinnen und Schüler dazu befähigt werden sollen, kritische Problembereiche der Internetnutzung zu benennen. Den weiterführenden Schulen ist als verpflichtend zu behandelndes Thema „Digitale Identität und Selbstdarstellung in sozialen Netzwerken“ vorgegeben. Die Analyse von Gefahren durch Handys und Internet, einschließlich sozialer Netze und Cybermobbing, ist ebenfalls verbindlicher Lerngegenstand im naturwissenschaftlich-technischen Unterricht. Eine vertiefte Auseinandersetzung mit den Möglichkeiten und Gefahren des Internets findet im Wahlpflichtfach Informatik in der Sekundarstufe I sowie im Fach Informatik in der gymnasialen Oberstufe im Rahmen des Semesterthemas „Möglichkeiten und Grenzen von Informatiksystemen“ statt.

Zu den ergänzenden Maßnahmen der für Bildung zuständigen Behörde gehört der Hamburger Medienpass mit den in den Jahrgangsstufen 5 bis 8 verpflichtend zu unterrichtenden Themen „Cybermobbing“ und „Datenschutz und soziale Netzwerke“ mit Bezügen zu den Unterthemen „Gefahren durch Fakeprofile“ sowie „Glaubwürdigkeit von Internetquellen“. Darüber hinaus entwickeln Schülerinnen und Schüler ab der 8. Klasse im von der zuständigen Behörde geförderten Projekt „Medienscouts“ mit Unterstützung begleitender Lehrkräfte Workshops und führen diese in den Jahrgangsstufen 5 und 6 an ihrer Schule durch. In diesen Workshops wird sicheres und faires Verhalten im Internet und in sozialen Netzwerken (wie zum Beispiel WhatsApp oder Facebook) trainiert.

Auf Nachfrage von Schulen bietet das Landesinstitut für Lehrerbildung und Schulentwicklung (LI) zudem sein Fortbildungsmodul „Informationskompetenz fördern“ an. Hierbei wird auch eine Checkliste zur Bewertung von Webseiten eingesetzt, mit der Schülerinnen und Schüler für den kritischen Umgang mit Fakeprofilen sensibilisiert werden.

4. Gibt es in Hamburg Forschungseinrichtungen, wissenschaftliche Zentren oder Professuren an den staatlichen Universitäten und Hochschulen, die sich mit dem Thema Social Bots befassen? Wenn ja, welche? Wenn nein, warum nicht?

In der Fakultät für Mathematik, Naturwissenschaften und Informatik, Fachbereich Informatik der Universität Hamburg sind im Rahmen des Forschungsgebietes „Information Governance Technologies“ und einer Kooperation mit dem Hans-Bredow-Institut für Medienforschung die Gestaltung von Informationstechnologien und ihre Effekte im Bereich der sozialen Netzwerke und Medien Gegenstand der Forschung. Darüber hinaus ist das Hans-Bredow-Institut für Medienforschung im Rahmen seiner Forschungsprogramme „Transformation öffentlicher Kommunikation: Journalistische und intermediäre Funktionen im Prozess der Meinungsbildung“ und „Regelungsstrukturen und Regelbildung in digitalen Kommunikationsräumen“ sowohl aus kommunikations- als auch aus regulierungswissenschaftlicher Perspektive mit Strukturen und Veränderungen digitaler Öffentlichkeit befasst, in dessen Kontexten auch die Rolle von Social Bots reflektiert wird.

An der Hochschule für Angewandte Wissenschaften Hamburg (HAW) beschäftigt sich das neu gegründete Competence Center Communication (CCCOM) in zahlreichen Forschungsprojekten mit dem Thema Social Bots. Darüber hinaus ist eine Professur der Fakultät Design, Medien und Information an einem durch das Bundesministerium für Bildung und Forschung geförderten Projekt namens „Propstop“ beteiligt, welches sich mit der Erkennung und Handhabung von automatisierten Usern in Webforen auseinandersetzt. Im Rahmen des EU-Förderprogrammes Horizon 2020 bereitet die HAW einen Projektantrag im Themenbereich Social Bots / Conversational Services vor. In diesem Projekt sollen Bots und die damit in Verbindung stehenden technischen, ethischen, rechtlichen, regulatorischen und Designfragen im Fokus stehen. An der Fakultät Technik und Informatik beschäftigt man sich im Sinne eines ganzheitlichen Cyber-Sicherheitsansatzes mit dem Thema Bots und Verfahren/Methoden des Risikomanagements, Awareness Building und auch der Nachsorge von Bot-Angriffen. Die HAW ist zudem am DFN-CERT, einer Forschungscommunity, beteiligt. Dort arbeiten Wissenschaftlerinnen und Wissenschaftler sowie Unternehmen gemeinsam an Fragen der IT-Sicherheit und an Forschungsprojekten zur Förderung der Sicherheitstechnologie, bei denen das Thema Social Bots tangiert wird.

An den übrigen staatlichen Hamburger Hochschulen ist das Thema aufgrund des jeweiligen Bildungs- und Forschungsauftrags nicht Gegenstand der Forschung und Lehre.