

Social Bots im Unterricht

vorgelegt von: Benjamin Knorr

MatrikelNr: 10967090

Zulassungsarbeit

Betreuender Dozent: Peter Brichzin

Lehrstuhl für Didaktik der Informatik

Institut für Informatik

Ludwig-Maximilians-Universität München

Schopenhauerstraße 66, 80807 München

Knorr.Benjamin@campus.lmu.de

München, den 27. März 2018

Zusammenfassung

In der vorliegenden Arbeit werden die technischen Grundlagen von Social Bots erklärt und ein Überblick über bereits mögliche Botaktivitäten gegeben. Aus der vermuteten technischen Weiterentwicklung wird das zukünftige Gefahrenpotenzial der Bots abgeleitet und Gegenstimmen werden aufgezeigt. Des Weiteren werden aktuelle Techniken zur Identifikation von Social Bots vorgestellt und ein Überblick über die Einsätze gegeben, die mit den Erkennungsmechanismen analysiert wurden.

Ausgehend von den gesellschaftlichen Wirkungen der Social Bots wird in Kapitel 3 aufgezeigt, dass das Thema auch für die Schulbildung relevant ist. Zur Sensibilisierung für die Problematik wird ein interdisziplinärer Ansatz propagiert und die Aufgabe der einzelnen Fächer aufgezeigt. Speziell der Einsatz im Informatikunterricht wird durch die Vereinigung vielfältiger, informatischer Konzepte und die angesprochenen Bildungsstandards motiviert.

In den darauffolgenden Kapiteln werden konkrete Unterrichtsstunden für unterschiedliche Fächer vorgestellt. In Kapitel 4 wird eine Unterrichtseinheit zur Programmierung von Social Bots beschrieben. Diese wird anhand der Faktoren des Berliner Modells aufgebaut und ist in den informatischen Themenkomplex „Kommunikation in Rechnernetzen“ eingebunden. Für die Unterrichtseinheit wurde ein didaktisch reduziertes, soziales Netzwerk entwickelt, in dem die Bots der SchülerInnen eingesetzt werden können. Die Überlegungen, die in die Erstellung des Netzwerks geflossen sind, werden ausgeführt und weitere Entwicklungsmöglichkeiten aufgezeigt. Ebenfalls wird die tatsächliche Durchführung des Unterrichtsversuchs beschrieben und reflektiert.

In Kapitel 5 wird eine Unterrichtseinheit für den Geschichtsunterricht zum Thema Propaganda konzipiert. Sie basiert auf der Unterrichtsmethode Stationenlernen und stellt verschiedene Propagandamedien aus der Zeit des Nationalsozialismus gegenüber. Ebenso werden neue Möglichkeiten zur Propaganda in der heutigen Zeit durch die digitalen Medien diskutiert.

Inhaltsverzeichnis

| | |
|--|-----------|
| 1. Einleitung | 1 |
| 2. Social Bots | 2 |
| 2.1. Funktionsweise | 2 |
| 2.1.1. Gründe für die Entstehung von Social Bots | 2 |
| 2.1.2. Aktionen von Bots in sozialen Netzwerken | 4 |
| 2.1.3. Programmierbeispiel | 6 |
| 2.2. Einfluss | 7 |
| 2.2.1. Gefahren von derzeitigen Social Bots | 7 |
| 2.2.2. Zukünftiges Gefahrenpotenzial | 9 |
| 2.2.3. Fazit | 12 |
| 2.3. Erkennen von Social Bots | 12 |
| 2.3.1. Techniken zur Identifikation | 12 |
| 2.3.2. Identifizierte Einsätze | 15 |
| 2.4. Rechtslage | 18 |
| 3. Bedeutung für die Schule und den Informatikunterricht | 21 |
| 3.1. Beurteilung der Relevanz für die Schulbildung | 21 |
| 3.1.1. Lebensnahes Thema für SchülerInnen | 21 |
| 3.1.2. Pflicht der Schulen | 22 |
| 3.1.3. Ziele der Thematisierung von Social Bots | 22 |
| 3.2. Social Bots als Interdisziplinäre Herausforderung | 23 |
| 3.2.1. Verschiedene Blickwinkel | 24 |
| 3.2.2. Analyse der fundamentalen Ideen | 25 |
| 3.3. Anknüpfungspunkte in der Informatik | 25 |
| 3.3.1. Rolle von Informatikunterricht | 26 |
| 3.3.2. Social Bots in den Bildungsstandards | 26 |
| 4. Unterrichtseinheit: Programmieren eines Social Bots | 29 |
| 4.1. Bedingungsfelder | 29 |
| 4.1.1. Anthropologisch-psychologische Voraussetzungen | 29 |
| 4.1.2. Soziokulturelle Voraussetzungen | 30 |
| 4.2. Inhaltliche und didaktische Analyse | 30 |
| 4.2.1. Lerninhalte | 31 |

| | | |
|-----------|---|-----------|
| 4.2.2. | Bildungsstandards | 33 |
| 4.3. | Ziele | 33 |
| 4.3.1. | Hauptlernziele | 33 |
| 4.3.2. | Teillernziele | 34 |
| 4.3.3. | Optionale Lernziele | 34 |
| 4.4. | Medien | 34 |
| 4.4.1. | Unterrichtseinstieg | 35 |
| 4.4.2. | Soziales Netzwerk mit Programmierschnittstelle | 36 |
| 4.4.3. | Hilfestellungen zum Programmieren | 41 |
| 4.5. | Methodische Analyse | 42 |
| 4.6. | Geplanter Stundenverlauf | 43 |
| 4.6.1. | Ablauf der Stunde 1: Einstieg zu Social Bots | 44 |
| 4.6.2. | Ablauf der Stunden 2 und 3: Programmieren eines Social Bots | 46 |
| 4.7. | Reflexion | 47 |
| 4.8. | Materialien | 51 |
| 5. | Unterrichtseinheit (Geschichte): Propaganda im digitalen Zeitalter | 54 |
| 5.1. | Bedingungsfelder | 54 |
| 5.1.1. | Anthropologisch-psychologische Voraussetzungen | 54 |
| 5.1.2. | Soziokulturelle Voraussetzungen | 55 |
| 5.2. | Inhaltliche Analyse | 55 |
| 5.2.1. | Begriffsdefinition | 55 |
| 5.2.2. | Inhaltliche Voraussetzungen | 55 |
| 5.2.3. | Inhalte der Unterrichtseinheit | 56 |
| 5.3. | Ziele | 56 |
| 5.4. | Methodische Analyse | 57 |
| 5.5. | Medien | 58 |
| 5.5.1. | Station 1: Plakate | 59 |
| 5.5.2. | Station 2: Rundfunk | 60 |
| 5.5.3. | Station 3: Presse | 60 |
| 5.5.4. | Station 4: Soziale Medien | 61 |
| 5.6. | Geplanter Stundenverlauf | 61 |
| 5.7. | Materialien | 63 |
| 6. | Fazit | 68 |
| | Literaturverzeichnis | 69 |
| A. | Weitere Unterrichtsideen | 73 |
| A.1. | Chatbots | 73 |
| A.2. | Sozialkunde – Gefahren und Möglichkeiten von Social Bots | 74 |

B. Ergänzungen zur Unterrichtseinheit „Programmieren eines Social Bots“ 75
B.1. Soziales Netzwerk 75
B.2. Proxy-Authentification Problembhebung 76

1. Einleitung

„Today’s social bots are sophisticated and sometimes menacing. Indeed, their presence can endanger online ecosystems as well as our society.“

Mit diesen Worten beginnt ein Artikel des Forscherteams der Indiana University um E. Ferrara [FVD⁺16]. Mit den erwähnten Social Bots wird versucht die Meinung von Nutzern in sozialen Netzwerken zu beeinflussen. Haben Social Bots wirklich so bedrohliche Einflüsse, wie Ferrara et al. sie nennen? Können Social Bots mit ihren Nachrichten Meinungen manipulieren?

Noch steht die Entwicklung von Social Bots relativ am Anfang. Sie existieren erst seit wenigen Jahren und Fortschritte im Bereich der Künstlichen Intelligenz lassen vermuten, dass das Potenzial noch nicht ausgeschöpft ist. Die Auswirkungen sind daher noch nicht ganz klar, aber die möglichen Gefahren von Social Bots sind sehr gravierend. Als präventive Maßnahme muss in der Bevölkerung ein Bewusstsein für derartige Manipulationen geschaffen werden. Die Algorithmik von Bots kann oft sehr kompliziert sein. Es stellt sich daher die Frage, ob diese Vermittlung bereits in der Schule stattfinden kann. Können sinnvolle Lernziele identifiziert werden, die in angemessener Zeit erreichbar sind?

Um dem näher zu kommen, muss zunächst ein umfassendes Verständnis der Thematik geschaffen werden. Wichtige Grundlagen müssen geklärt und die aktuelle Situation wissenschaftlich erfasst werden.

2. Social Bots

Social Bots sind Computerprogramme, die in sozialen Netzwerken menschliches Verhalten imitieren und automatisiert und gezielt Beiträge schreiben, teilen, liken oder kommentieren [WMKS12]. Hier wird zunächst ein Überblick über ihre Funktionsweise gegeben. Anschließend wird betrachtet, welche Einflüsse der Einsatz solcher Programme aktuell hat und wie die Entwicklung in den nächsten Jahren vermutet wird. Des Weiteren sollen Versuche präsentiert werden, wie Social Bots erkannt werden können, da dies einen zentralen Punkt für Gegenmaßnahmen darstellt. Dazu werden Beispiele aus der jüngeren Vergangenheit vorgestellt, bei denen durch Analysen eine große Aktivität von Social Bots aufgedeckt werden konnte. Zum Abschluss des Kapitels wird noch kurz der rechtliche Rahmen für Social Bots vorgestellt.

2.1. Funktionsweise

Social Bots sind ein neues Phänomen, aber sie verwenden Technologien, die bereits seit längerem existieren. Im Folgenden werden die Fragen betrachtet, welche Anreize es für diese Entwicklung gab und welche technischen Funktionalitäten Social Bots besitzen.

2.1.1. Gründe für die Entstehung von Social Bots

Ein großer Entwicklungsschritt des Internets war der Übergang von statischen Webseiten, die rein passiv von Nutzern besucht wurden, hin zu Webseiten, die den Nutzern ermöglichen, eigene Inhalte zu erstellen und im gesamten Netz verfügbar zu machen. Diese Entwicklung wird daher oft mit *Web 2.0* bezeichnet. Es entstanden soziale Netzwerke, in denen Nutzer miteinander chatten können, Links zu anderen Webinhalten teilen können, oder einfach nur eine Vielzahl an Menschen mit eigenen Beiträgen erreichen können. Mit weltweit über 2 Milliarden monatlich aktiven Nutzern auf Facebook und mehreren Hundert Millionen in zahlreichen weiteren Netzwerken [Sta18b] haben diese Netzwerke eine unglaubliche Reichweite und dementsprechende Bedeutung im heutigen Leben. Die Möglichkeit, in einer technischen Umgebung so viele Menschen zu

erreichen, stellt einen großen Anreiz für Manipulationen dar. Man kann dafür Computerprogramme entwickeln, die Werbung, politische Ansichten oder einfach Falschinformationen in hohem Maße verbreiten. Ebenso sind die persönlichen Daten Geld wert, die in den Profilen in sozialen Netzwerken mit (meist befreundeten) Nutzern geteilt werden. Sie sind so ebenfalls ein attraktives Ziel für Programme, die sich mit immer mehr Leuten vernetzen und dadurch an diese sensiblen Daten herankommen [BMBR11]. Genau diese Anreize sind der Hintergrund für die Entwicklung von *Social Bots*: Ein Programm, das nach konfigurierbaren Prinzipien automatisiert in einem sozialen Netzwerk agieren kann und dabei möglichst menschlich wirkt, um die Manipulation noch wirkungsvoller zu machen. Das Programm kann dann mit eigenen Inhalten Leute beeinflussen oder versuchen sich mit möglichst vielen Leuten zu verbinden und deren persönliche Informationen sammeln [BMBR11].

Vergleich mit dem Turing-Test

Die Bestrebungen zur Entwicklung eines menschlich wirkenden Algorithmus ist dabei bereits deutlich älter. Bereits 1950 formulierte Alan Turing einen Test, der entscheiden soll, ob eine künstliche Intelligenz dem menschlichen Denken ebenbürtig ist: Ein Mensch führt über zwei Bildschirme Gespräche mit einem Computer und einem weiteren Menschen. Beide Gesprächspartner versuchen den Fragensteller von ihrer Menschlichkeit zu überzeugen. Kann der Fragensteller nach einer begrenzten Zeit in mindestens 30% der Fälle nicht korrekt entscheiden, welcher Gesprächspartner der Mensch war, ist der Test bestanden [CS03, S. 680]. Diese Definition von Intelligenz wurde im Laufe der Zeit von mehreren Seiten kritisiert [CS03, ebd.], doch hatte der Test enormen Einfluss auf die Entwicklung von künstlicher Intelligenz. Bots sind inzwischen in der Lage, verständliche Texte zu verfassen und in geringem Maße auch Konversationen zu führen. Meist wird dabei eine riesige Datenbank an realen Sätzen verwendet, die während dem Chatten mit dem Bot ständig erweitert wird. Auch der Aufstieg von persönlichen Assistenten mit Sprachsteuerung wie Alexa, Cortana oder Siri zeigt den Fortschritt in diesem Bereich.

Eine so umfangreiche Sprachverarbeitung ist in Social Bots meistens nicht nötig. Nur in den wenigsten Fällen können sie ein komplettes intensives Gespräch führen, oder eigene Texte verfassen. Sie müssen auch nicht auf einen Fragensteller reagieren, der dann entscheidet, ob es sich um einen Computer oder einen Menschen handelt und erfüllen somit auch nicht den Turing-Test. Stattdessen können sie einfach passende Beiträge durch die Suche nach Schlagworten finden und diese dann retweeten oder kopieren. Eine große Datenbank mit natürlicher Sprache ist nicht notwendig, sodass Social Bots bereits mit geringem Aufwand erstellt werden können. Um in einem sozialen Netzwerk menschlich zu wirken, sind aber noch andere Gesichtspunkte wichtig, wie beispielsweise ein ansprechendes Profil mit (gefälschten) persönlichen Daten. Solche Daten sind

beispielsweise bei <https://www.fakenamegenerator.com> auch in großer Menge generierbar, oder sogar mit Profilbild bei <https://randomuser.me> zu finden. Ebenfalls muss bei den Postings ein Tag-Nacht-Rhythmus beachtet werden, um nicht als Computerprogramm aufzufallen [FVD⁺16]. Auch eine zu hohe Rate an Posts pro Tag (oder im komplett unkontrollierten Fall sogar mehrere Posts pro Sekunde) deutet auf ein automatisiertes Profil hin und muss deswegen vermieden werden.

2.1.2. Aktionen von Bots in sozialen Netzwerken

Wie kann nun ein Social Bot im sozialen Netzwerk agieren? Zunächst muss er einen Zugang zu der Webseite haben, also ein Profil besitzen. Diese Profile können zum einen per Hand erstellt werden, im Internet gekauft werden oder durch höherentwickelte Verfahren (z.B. Umgehen von *CAPTCHAs*) automatisch angelegt werden [BMBR11]. Sie können dann wie oben beschrieben mit (vermeintlich) persönlichen Daten weiter ausgebaut werden. Im Unterschied zu Schadsoftware wie zum Beispiel einem Wurm infizieren Social Bots keine PCs von Nutzern und versuchen nicht deren Accounts zu übernehmen.¹ Jeder Social Bot arbeitet nur in dem Profil, das für ihn erstellt wurde. Meistens kommen Social Bots jedoch auch als großes Netzwerk zum Einsatz, bei dem mehrere Social Bots mit je einem Profil über dieselbe Software gesteuert werden.

Mit dem Account kann ein Social Bot nun über zwei Wege im Netzwerk aktiv werden. Zum einen werden gewöhnlich einige Funktionen über eine Programmierschnittstelle (*API* – engl. *application programming interface*) zur Verfügung gestellt. Das geschieht, damit Programmierer die Dienste der Webseite mit eigenen Programmen oder Mobile Apps verbinden können und so die Reichweite der Webseite vergrößert wird [KJW⁺17, S. 39]. Die APIs werden beispielsweise auch von Firmen für Chatbots zur Kundenbetreuung genutzt. Typische Funktionalitäten, die bei sozialen Netzwerken über eine API angeboten werden, sind das Verfassen und Abrufen von Beiträgen, Abrufen und Aktualisieren von Profilinformationen, sowie Liken/Favorisieren² von Beiträgen. Social Bots oder Spamming- und Phishing-Angreifer missbrauchen diese Schnittstellen, weswegen soziale Netzwerke oft Sicherheitsmaßnahmen implementieren. Beispielsweise sperrt Twitter auffällige Profile und Facebook hat ein eigenes Kontrollsystem (*FIS* – engl. *Facebook immune system* [SCM11]) entwickelt, um verdächtige Lese- und Schreibaktionen direkt zu unterbinden.

Nicht alle Funktionalitäten des Netzwerks werden über eine API zur Verfügung gestellt.

¹Im Unterschied dazu ist Koobface ein Beispiel für einen *Wurm* mit dem Ziel, Zugangsdaten von Social Media Webseiten abzugreifen. Die infizierten Accounts bilden ein Botnet, das versucht sich immer weiter zu vergrößern und mehr Daten zu sammeln <https://de.wikipedia.org/wiki/Koobface>

²*Liken* und *Favorisieren* werden in der weiteren Arbeit synonym verwendet. Gleiches gilt weitestgehend für *Post*, *Beitrag* und *Tweet* sowie für *teilen* und *retweeten*.

Einige sollen nicht von automatisierten Apps im Hintergrund, sondern nur von Nutzern im Browser ausgeführt werden können. Social Bots implementieren daher oft die Funktion, wie ein Browser zu agieren und gewöhnliche *HTTP*-Anfragen an bestimmte Adressen des sozialen Netzwerks zu schicken. Solche Mechanismen sind jedoch bereits deutlich komplexer, da die Anfragen in der Regel mit *CAPTCHAs*, verschlüsselten Tokens oder Ähnlichem geschützt sind und natürlich ebenfalls von den Kontrollsystemen überwacht werden. Typische Beispiele von solchen Funktionalitäten sind die Registrierung von Accounts, sowie Aktionen zur Vernetzung, wie Freundschaftsanfragen bei Facebook [BMBR11].

Die Social Bots werden über diese Wege nun auf verschiedene Arten aktiv. Die Auswirkung dieser Aktionen wird hier nur angerissen und in Kapitel 2.2 genauer ausgeführt.

- **Vernetzen:** Social Bots vernetzen sich mit anderen Profilen, um deren scheinbare Popularität im Netzwerk zu erhöhen.
- **Retweet und Like:** Social Bots verbreiten und liken andere Beiträge und vergrößern so die Sichtbarkeit der Beiträge.
- **Massenhaft Schlagwörter posten:** Sie schreiben massenhaft eigene kurze Beiträge mit bestimmten Schlagworten, um diese sichtbar zu machen oder genau im Gegenteil, um die tatsächliche Diskussion unter dem Hashtag in der Masse untergehen zu lassen und den Hashtag für menschliche Nutzer unbrauchbar zu machen.

Neben den „passiven“ Bots, die nur anderen (realen) Nutzern zu größerer Sichtbarkeit verhelfen, gibt es also auch Bots, die aktiv Beiträge verbreiten. Im Normalfall werden Beiträge eines einzelnen Profils aber nicht sehr prominent im Netzwerk angezeigt. Wie gelingt es also, dass solche Beiträge beachtet werden? Auf Facebook werden Nutzern in der Regel Beiträge von Freunden angezeigt, also müssen die Social Bots zunächst ein Freundesnetzwerk aufbauen, um Leute zu erreichen. Im einfachsten Fall können sie das beispielsweise, indem sie zunächst vielen zufälligen Personen Freundschaftsanfragen schicken und dann den Freunden der angenommenen Anfragen bis die gewünschte Anzahl erreicht ist. Wichtig ist dabei die Feststellung, dass den Bots eine kleine Menge an Nutzern reicht, die eine Freundschaftsanfrage eines ihnen unbekanntem Nutzers annehmen. Denn nach dem „*triadic closure principle*“ von Georg Simmel³ führen anschließende Freundschaftsanfragen an deren Freunde deutlich wahrscheinlicher zum Erfolg, da gemeinsame Freunde aufgelistet werden. Dieser Effekt konnte auch mit Social Bots nachgewiesen werden [BMBR13]. Vernetzungen in Twitter sind gerichtet, das heißt ein Nutzer A kann einem Nutzer B folgen, ohne dass B auch A folgen muss. Deswegen ist das Bestätigen von Follow-Anfragen oft weniger selektiv als Freundschaftsanfragen auf

³Das „*triadic closure principle*“ besagt, dass sich in sozialen Gruppen Triaden (3-er Gruppen) schließen, dass also aus Verbindungen $A \leftrightarrow B$, $A \leftrightarrow C$ eine weitere Verbindung $B \leftrightarrow C$ entsteht. https://en.wikipedia.org/wiki/Triadic_closure

Facebook. Um eine Wirkung zu haben, müssen die Nutzer den Social Bots allerdings auch zurückfolgen.

2.1.3. Programmierbeispiel

Möchte man ein tieferes Verständnis der Funktionsweise von Social Bots erhalten, ist es sinnvoll, sich die Programmierung dieser genauer anzuschauen. Man erhält dadurch Einblicke in den Aufwand, der betrieben werden muss, um einen funktionsfähigen Social Bot zu erstellen. Es hilft außerdem dabei, zu verstehen, welche Einschränkungen Social Bots haben und wie sie erkannt werden können. Damit bietet dieser Abschnitt eine wichtige Grundlage für die nachfolgenden Kapitel.

Je nach Komplexität der Handlungen der Social Bots ist auch die Programmierung unterschiedlich aufwändig. Simple Anwendungen können aber bereits mit sehr wenigen Codezeilen implementiert werden. Im Internet finden sich zahlreiche Codebeispiele für einfache Social Bots, die auf Twitter (ohne negative Absichten) eingesetzt werden. Auch wenn sich die konkreten Bots in ihrem Verhalten unterscheiden, sind wesentliche Bestandteile der Software meist gleich aufgebaut, sodass im Folgenden der Programmcode eines prototypischen Social Bots dargestellt werden kann.

Eine Methode zum Retweeten eines bestimmten Hashtags ist in Abbildung 2.1 zu sehen. Sie führt eine *GET*-Anfrage an die Twitter Api aus, verarbeitet die Antwort und sendet schließlich eine *POST*-Anfrage, um den Beitrag zu retweeten.

```
// Suche nach dem letzten Tweet zu #example
function retweetLatest () {
  // GET-Anfrage an search/tweets mit Parametern
  T.get('search/tweets', {q: '#example', count: 1, result_type: 'recent'},
  // callback, wird aufgerufen wenn Anfrage fertig ausgeführt wurde
  function (error, data) {
    if (!error) {
      // ID des Tweets aus JSON der Antwort
      var retweetId = data.statuses[0].id_str;
      // POST-Anfrage an statuses/retweet/:id
      T.post('statuses/retweet/' + retweetId, {})
    }
  }
  )
}
```

Abbildung 2.1.: JavaScript-Methode zum Retweeten eines Beitrags zu einem bestimmten Hashtag. Vereinfacht von <https://github.com/dariusk/examplebot/blob/master/bot.js>

So eine Methode kann dann mit der folgenden Zeile jede halbe bis ganze Stunde automatisch ausgeführt werden:

```
setInterval(retweetLatest, 1000*60*30*(1 + Math.random()))
```

Ein weiterer Bot könnte einfach Texte einprogrammiert haben, die er dann tweetet. Man sieht daran, dass kein wirkliches Text-Verständnis enthalten ist. Weder wenn sie selbst posten, noch wenn sie andere Posts retweeten oder liken. Dadurch können Social Bots sehr leicht programmiert werden.

2.2. Einfluss

Im Januar 2017 lud der Ausschuss für Bildung, Forschung und Technikfolgenabschätzung zu einem öffentlichen Fachgespräch zu der Frage, ob „*Social Bots das Potenzial [haben], politische Debatten im Internet, und damit gar den Ausgang einer Bundestagswahl zu beeinflussen*“ [Deu17]. Die wichtigsten Punkte daraus sowie aus der im Anschluss veröffentlichten Studie [KJW⁺17] werden im Folgenden dargestellt. Grundsätzlich ist jedoch anzumerken, dass für eine fundierte Einschätzung der Gefahr die empirische Datengrundlage fehlt. Es lässt sich nur feststellen, dass Social Bots in sozialen Netzwerken aktiv sind, aber nicht, was das tatsächliche Ausmaß des Einflusses ist. Dies kann derzeit nur theoretisch begründet und aus ähnlichen Formen der Meinungsbeeinflussung (Werbung, Propaganda, . . .) abgeleitet werden.

2.2.1. Gefahren von derzeitigen Social Bots

Heutige Social Bots sind im Hinblick auf die Künstliche Intelligenz noch nicht so weit entwickelt, dass sie trotz genauem Betrachten eine menschliche Identität vorspiegeln könnten. In vielen Fällen ist dies jedoch gar nicht nötig, da oft die reine Masse ausreicht und durch (Follower-/ Like-/ etc.) Zahlen verdeckt wird, ob es sich um Bots oder Menschen handelt.

Künstliche Popularität zur Unterstreichung eigener Positionen [KJW⁺17, S. 33]

Auf Twitter wird durch hohe Followerzahlen Popularität erreicht. Steht ein größeres Netzwerk an Social Bots zur Verfügung, können diese Zahlen manipuliert werden, indem viele Bots einzelnen Accounts gezielt folgen und so deren Positionen unterstreichen. Twitterprofilen von Politikern folgen oft 20%-29% Fakeaccounts [SSRDM16]. Weitere Größen, die auf die gleiche Weise manipuliert werden können, sind die Anzahl der Likes oder Retweets oder die Häufigkeit der Nutzung eines Hashtags. Auf Facebook ist vor allem die Popularität von öffentlichen Gruppen und Seiten relevant, die nach dem selben Prinzip durch Beitritte in Gruppen oder Liken der Seiten mit einem Botnet an scheinbarer Größe gewinnen.

Die Zahlen haben dabei sowohl innerhalb der Webseite, als auch außerhalb Einfluss: Innerhalb der Webseite werden Nutzern bevorzugt „relevante“ Themen präsentiert. Diese Relevanz lässt sich durch Liken und Teilen beeinflussen und ist zusätzlich von der Popularität des Erstellers abhängig. Eine Außenwirkung kann durch Berichterstattungen erlangt werden, die solche Zahlen als repräsentativ betrachten und entsprechend verbreiten. Dadurch erreicht die Manipulation noch mehr Menschen über einen vertrauten Kanal. In der Diskussion wurde daher insbesondere von den Medien gefordert, solche Zahlen nicht mit der Menge der Menschen gleichzusetzen [Deu17].

Ein wichtiger Sonderfall dieser Manipulation sind die „*Hashtag*“ genannten Schlagwörter, mit denen (vor allem) auf Twitter Nachrichten gekennzeichnet und gesucht werden können. Bei häufiger Verwendung suggerieren sie ebenfalls ein aktuelles Thema und werden angemeldeten Nutzern auf der Startseite angezeigt. Einen Multiplikatoreffekt können auch hier die traditionellen Medien haben, wenn Journalisten und Politiker diese Themen als Bewegung wahrnehmen und darüber berichten [KJW⁺17, S. 38]. Auf diese Art wurde beispielsweise im Wahlkampf der Präsidentschaftswahlen der USA 2016 nach einem Fernsehduell der Kandidaten Hillary Clinton und Donald Trump in Twitter zahlreich der Hashtag „#TrumpWon“ (übersetzt: Trump hat gewonnen) verbreitet und diese Beiträge auf der Startseite als aktuelles Thema prominent angezeigt. Analysen zufolge handelte es sich bei etwa einem Drittel der Pro-Trump Tweets um automatisierte Beiträge von Social Bots. [KHW16] (Mehr dazu in Kapitel 2.3.2.)

Ersticken von Gegenmeinungen [KJW⁺17, S. 33]

Eine andere Wirkung, die durch massenhafte Verwendung eines Hashtags erzielt werden kann, ist, diesen für menschliche Nutzer unbrauchbar zu machen – also genau die gegenteilige Absicht. Das gelingt, indem der Hashtag mit störenden Nachrichten geflutet wird und die menschliche Kommunikation mithilfe des Hashtags so unmöglich wird. Beispielsweise wurde Ende 2014 in Mexiko eine Protestwelle auf Twitter mit dem Hashtag „#YaMeCanse“ (übersetzt: Ich habe es satt) geführt, die von Bots durch massenweisen Spam gestört wurde [SSRDM16]. (Mehr dazu in Kapitel 2.3.2.)

Verbreitung von Propaganda und Meinungsmache [KJW⁺17, S 33.]

Bots können auch eine direkte Wirkung erzielen, indem sie polarisierende oder propagandistische Inhalte selbst verbreiten. Dazu können sie einerseits Retweets verwenden. Ebenso können sie aber Texte aus anderen Tweets oder Nachrichtenseiten kopieren, evtl. einzelne Wörter verändern und anschließend neu posten. Insbesondere das Verbreiten von „Fake News“, also „*von falschen oder irreführenden Informationen in der Absicht einer Person, einer Organisation oder einer Institution zu schaden*“ [Rü17], ist

relevant und wird oft mit Social Bots in Verbindung gebracht. Auch die Diskreditierung von in der Öffentlichkeit stehenden Personen oder Produkten kann ein Ziel von Aktionen mit Social Bots sein.

In Abgrenzung zu den vorherigen Möglichkeiten der Einflussnahme müssen die Social Bots dafür selbst eine gewisse Reichweite haben (Follower- bzw. Freundesnetzwerk), da sonst kein Effekt zu erwarten ist. Dass Social Bots eine solche Reichweite prinzipiell erlangen können, konnte in einer Studie [BMBR13] gezeigt werden. Bezweifelt wird jedoch, dass der bloße Kontakt zu solchen Beiträgen bereits die politische Meinung einer Person beeinflussen kann [Deu17]. Allerdings wird das Vertrauen in den Wahrheitsgehalt einer Nachricht gestärkt, je öfter diese zu lesen ist [KJW⁺17, S. 43].

Gefahren durch wirtschaftliche Einsätze

Derzeitige Social Bots nehmen vor allem durch Werbung und Spam Einfluss auf die Wirtschaft und stellen somit meistens keine neue Gefahr in diesem Bereich dar. Zu den weiteren Anwendungsmöglichkeiten zählen Betrug und unlauterer Wettbewerb [KJW⁺17, S. 39]. Ein Beispiel für den wirtschaftlichen Einsatz von Social Bots ist das Aktienunternehmen „Cynk“, das ohne Umsatz, ohne Kunden und mit nur einem Mitarbeiter den Aktienwert des Unternehmens um 36.000 Prozent auf 6 Milliarden Dollar steigerte [Hac14]. Die Bots verbreiteten in Twitter dabei Diskussionen über das Technik-Unternehmen, was von automatisierten Tradingalgorithmen aufgegriffen wurde, die dann in das Unternehmen investierten. Als die Börsenaufsicht eingriff, hatten bereits einige Leute viel Geld investiert, das sie nicht mehr zurückbekamen [FVD⁺16].

Eine weitere, aktuell bereits relevante Gefahr ist der Diebstahl persönlicher Informationen durch Social Bots. Insbesondere auf Facebook speichern Nutzer viele persönliche Informationen in ihren Profilen, die für Freunde einsehbar sind, wie z.B. Emailadressen, Geburtsdatum, Informationen über Hobbies oder den Beruf. Ein Social Bot Netzwerk, das versucht solche Informationen zu stehlen, muss selbst nicht viel posten, sondern nur ein Freundschaftsnetzwerk mit echten Nutzern aufbauen. In Studie von Boshmaf et al. von 2011 wurde dies demonstriert [BMBR13].

2.2.2. Zukünftiges Gefahrenpotenzial

Die mögliche Gefahr von Social Bots wird von Experten ganz unterschiedlich eingeschätzt: Linus Neumann vom Chaos Computer Club hält die Wirksamkeit von Social Bots für überschätzt und vergleicht sie mit Spammails und Werbetelefonanrufen, wohingegen die meisten anderen von Kind et al. Interviewten den möglichen Einfluss von

Social Bots höher einschätzen [KJW⁺17, S. 40],[Deu17]. Für die nun folgenden Punkte werden wegen dieser Unklarheit auch immer nötige Voraussetzungen mit angegeben. Dies soll helfen einzuschätzen, wie wahrscheinlich das Eintreten der jeweiligen Gefahr tatsächlich ist.

Einfluss auf den politischen Diskurs

Eine absehbare Gefahr von Social Bots ist, dass der politische Diskurs aus den sozialen Netzwerken vertrieben wird: Werden immer öfter Bots als Spammer eingesetzt, um die Kommunikation zu stören, dann könnte das dazu führen, dass die Nutzer den Dienst wechseln müssen [KJW⁺17, S. 42]. Wie entscheidend diese Demobilisierung sein kann, wird deutlich, wenn man sich die Rolle sozialer Netzwerke zum Beispiel beim Arabischen Frühling ansieht. Dort wurden Plattformen im Internet zur Organisation der politischen Bewegungen verwendet. Solche Strukturen können mit Social Bots infiltriert werden und so die Kommunikation unverhältnismäßig erschweren.

Technisch ist dies bereits jetzt möglich und wird (wie bereits beschrieben) auch angewendet. Eine entscheidende Voraussetzung für die beschriebene Wirkung ist, dass die Nutzer sich den Nachrichten der Bots nicht entziehen können. Hier könnten die Webseitenbetreiber gegensteuern, indem sie beispielsweise den Nutzern beim Suchen nicht alle Beiträge in chronologischer Reihenfolge anzeigen, sondern z.B. bevorzugt die von Freunden geschriebenen und geteilten Beiträge.

Die Verbreitung von Falschnachrichten oder hetzerischen Nachrichten kann ebenfalls einen Einfluss auf den politischen Diskurs haben: Die Folge könnte sein, dass in den Online-Diskussionen die Radikalisierung verstärkt wird und gemäßigte Positionen in den Hintergrund treten [KJW⁺17, S. 42]. Sentimentanalysen⁴ von Twitterposts zeigten mehrmals, dass mit Social Bots radikalere Meinungen verbreitet werden, denn die Beiträge fallen durch eine negativere und geladenere Wortwahl auf [DKS14, Heg18, DVF⁺16]. Die erhöhte Präsenz radikaler Positionen in den Beiträgen verändert das Diskussionsklima. Nicht nur werden Nutzer mit ähnlichen Ansichten in ihrer Meinung bestärkt und bezüglich der Anzahl der Unterstützer getäuscht. Auch entgegengesetzte Meinungen werden durch die Diskussionen extremer. Es findet also eine Gruppenpolarisierung statt.

Damit das eintritt, müssen die Bots aber noch technisch ausgereifter werden. Die Beiträge müssen als reale Positionen aufgefasst werden, daher müssen die Bots wirklich menschlich wirken. Viele Experten gehen davon aus, dass Social Bots durch technische Entwicklungen in Zukunft tatsächlich immer schwieriger von Menschen unterscheidbar sind [KJW⁺17, S. 17]. Andererseits kann durch die Aufklärung der Nutzer

⁴Bei der Sentimentanalyse wird untersucht, wie positiv bzw. negativ die Stimmung eines Textes ist

über die Existenz und Wirkmechanismen von Social Bots das kritische Hinterfragen der Beiträge gefördert werden und so der Manipulationsgefahr entgegengewirkt werden.

Destabilisierung

Besonders gefährdet für die Manipulation mit Social Bots sind global kritische Zeitpunkte, wie Gipfelpunkte politischer Debatten oder Krisensituationen. Da sich dann besonders viele Menschen in sozialen Netzwerken über aktuelle Geschehnisse austauschen, können Falschnachrichten schnell verbreitet werden. Dies kann zu einer Verunsicherung der Gesellschaft führen und destabilisierende Auswirkungen haben [KJW⁺17, S. 42f].

Technisch ist dieser Punkt bereits möglich, da die Bots hierfür eigentlich nur entsprechende Falschnachrichten von anderen Webseiten teilen müssen. Fraglich ist dagegen aber, ob die Bots durch das reine Verbreiten dieser Nachrichten wirklich einen Einfluss auf die Gesellschaft haben.

Astroturfing

Spontane, gesellschaftliche Bewegungen, die von der Basis der Bevölkerung ausgehen, bezeichnet man als *Graswurzelbewegung*. Sie können zum Beispiel eine Meinung zu Politikern oder zu Produkten darstellen. In Anlehnung daran nennt man Aktionen *Kunstrasenbewegung* oder *Astroturfing*⁵, wenn sie den Eindruck einer Graswurzelbewegung erwecken sollen, in Wirklichkeit aber von wenigen Einzelpersonen gesteuert sind. Astroturfing wird häufig zur Werbung verwendet, wird aber auch politisch zur Meinungssteuerung eingesetzt. In Russland und China gibt es mit der Troll-Fabrik bzw. der 50 Cent Army staatlich organisierte Gruppen, die Astroturfing in sozialen Medien betreiben. Sie werden dafür bezahlt, positive Nachrichten über die Regierung im Internet zu streuen [Nau17]. Social Bots bieten den Propagandisten hier das Potenzial, die selbe Arbeit kostengünstiger und umfangreicher zu machen. Mit dem aktuellen Entwicklungsstand ist dies noch schwierig, da sie leicht als Bots erkannt werden und daher einen hohen Grad an menschlicher Steuerung im Hintergrund benötigen, um den gewünschten Effekt zu haben. Ist die Technologie aber ausgereifter, können solche Propagandamaßnahmen sehr effizient werden. Die USA planten bereits 2011 eine ähnliche Anwendung [Gre11]. Allerdings gibt es auch zur Wirkung von Astroturfing im Sinne einer politischen Meinungssteuerung noch keine fundierten Daten.

⁵Astroturfing ist benannt nach einer englischen Kunstrasenfirma AstroTurf

2.2.3. Fazit

Social Bots weisen viele Gefahren auf, die vor allem aus dem technischen Potenzial begründet sind. Es ist aber schwierig abzusehen, wie groß der Einfluss auf die Menschen tatsächlich ist. Sollten Social Bots tatsächlich diese Wirkungen erreichen können und die Entwicklung so voranschreiten, wie es vermutet wird, dann hat dies jedoch enorme Einflüsse auf das aktuelle gesellschaftliche Leben. Daher muss bereits im Vorfeld über Gegenmaßnahmen nachgedacht werden. Wichtige Bestandteile davon liegen zum einen in der (automatisierten) Erkennung von Social Bots. Der aktuelle Stand dieser Bemühungen wird im folgenden Kapitel 2.3 dargestellt. Zum anderen ist die Aufklärung über Social Bots insbesondere in der Schule wichtig, wie es in Kapitel 3 erläutert wird.

2.3. Erkennen von Social Bots

Für Maßnahmen zum Schutz vor Social Bots ist es zunächst wichtig, dass man automatisierte Accounts von menschlichen unterscheiden kann. Zum einen hilft die Weiterentwicklung der Analyseverfahren möglicherweise bei zukünftigen Ereignissen direkt, wenn Social Bots noch während ihrer Aktivität gestoppt werden können. Zum anderen können auch bereits vergangene Ereignisse genauer untersucht werden, um so die Gefahren von Social Bots besser einschätzen zu können. Gelingt es Manipulationen aufzudecken, kann das außerdem Konsequenzen für die damaligen Betreiber nach sich ziehen. Grundsätzlich hinken alle bisherigen Verfahren der Weiterentwicklung von Social Bots hinterher, da zuerst ein Kriterium zur Unterscheidung festgestellt werden muss, bevor es zur Identifikation in den Analyseverfahren verwendet werden kann [KJW⁺17, S. 52].

2.3.1. Techniken zur Identifikation

In der bisherigen Forschung zu Social Bots wurden zwei unterschiedliche Verfahren zur Identifikation herangezogen: Machine Learning Verfahren, wie der Algorithmus „Botometer“, und Heuristiken [Heg18]. Auf diese beiden Methoden soll nun weiter eingegangen werden.

Heuristiken

Unter Heuristiken versteht man Hilfsstrategien, die schnell eine grobe Näherung für das gestellte Problem liefern. Meistens werden dabei feste, gröbere Kriterien verwendet, die zwar kein komplett richtiges Ergebnis liefern, allerdings mit einer akzeptablen

Abweichung und geringeren Komplexität ausgewertet werden können. Ein häufig verwendetes Kriterium bei der Identifikation von Social Bots ist die Anzahl an Beiträgen im Messzeitraum. Aus den Datensätzen von Twitter kann ein Grenzwert festgelegt werden, ab dem man von einem ungewöhnlichen, von der Norm abweichenden Verhalten sprechen kann. In der Statistik gebräuchlich sind Ausreißertests: Hierfür wird zuerst der Median der Anzahl der Beiträge einzelner Nutzer und anschließend die Grenze für das obere Quartil berechnet. Eine übliche Forderung für die Abweichung von Ausreißern ist das 1,5-fache des Quartilabstands. Der Datensatz eines Protests in Iran ergab mit dieser Analyse, dass Twitternutzer mit einer Tweethäufigkeit von etwa 54 Tweets pro Tag auffällig sind [Heg18]. In Studien der Oxford University wurde (ohne statistische Untersuchung) der Wert 50 Tweets pro Tag verwendet [HKW16b, HKW16c]. Der Ansatz, dies als ausschließliches Kriterium für die Identifikation von Social Bots herzunehmen, wurde auch kritisiert, insbesondere von dem Datenjournalist Michael Kreil [Kre17]. Dieser kam in Analysen eines Datensatzes der US-Präsidentenwahlen zu dem Ergebnis, dass die meisten häufig twitternden Nutzer in Wirklichkeit tatsächlich Menschen waren und die Heuristik damit weit von der tatsächlichen Anzahl der Bots abweicht.

Weitere Kriterien, die für Heuristiken in Betracht gezogen werden können, sind:

- Unvollständiges Profil: Auffällig sind Profile mit z.B. fehlendem Profilbild.
- Uhrzeiten: Auffällig sind Profile, die keinen Tag-Nacht-Rhythmus zeigen.
- Frequenz: Auffällig sind Profile, die in sehr kurzen Abständen Tweets schreiben.
- Textduplikate: Auffällig sind Beiträge, die sich im genauen Wortlaut gleichen, aber keine Retweets sind.
- Quelle: Twitter speichert, mit welcher Anwendung der Tweet gesendet wurde. Das lässt sich zwar manipulieren [Heg18], aber da dies auf der Webseite selbst nicht angezeigt wird und für normale Nutzer somit unsichtbar ist, machen sich die Bots im Normalfall nicht die Mühe. Daher finden sich dort bei Social Bots häufig seltsame Quellen.
- Follower/Following Verhältnis: Früher sind Bots häufig deutlich mehr Personen gefolgt, als sie eigene Follower hatten. So galten solche Profile als auffällig. Neuere Studien zeigten aber, dass die Bots inzwischen versuchen genau dies zu vermeiden und das Verhältnis ausgeglichen halten, sodass nun das Verhältnis von ungefähr 1 (bei einer Mindestzahl z.B. von 100 Followern) eher als Kriterium verwendet werden kann [Heg18].
- Sentiment: Es ist möglich das Sentiment (= Stimmung) von Beiträgen zu analysieren, indem die wichtigen Wörter daraus mit einem Lexikon verglichen werden,

in dem für die meisten englischen Wörter ein Wert zwischen +1 (maximal positiv) und -1 (maximal negativ) definiert ist [Heg18]. Mit dieser Analyse können dann z.B. Profile mit vielen besonders extremen Beiträgen als auffällig eingestuft werden, oder auch Profile, die häufig den Nutzern widersprechen, denen sie selbst folgen [DKS14].

Auch eine Kombination verschiedener Heuristiken ist sinnvoll, da so die Nachteile einzelner Einstufungen durch andere Kriterien ausgeglichen werden. Jedoch erfüllt in der Regel kein Bot alle Kriterien.

Machine Learning Verfahren

Im Gegensatz zu den Heuristiken, die durch theoretische Überlegung motiviert sind und statische Kriterien darstellen, wird bei Machine Learning Verfahren versucht, in einem vorbereiteten Datensatz automatisiert Muster zu erkennen, die bei der Unterscheidung von Bots und menschlichen Nutzern helfen [Heg18]. Ein solches selbstlernendes System ist das von der Indiana University entwickelte Tool „*Botometer*“ (ehemals „*BotOrNot*“). Dieses Modell wurde mit 15.000 manuell als Bots verifizierten und 16.000 menschlichen Accounts mit 5.6 Millionen Tweets trainiert. Es berechnet für verschiedene Aspekte Werte, wie wahrscheinlich ein Account der eines Bots ist. Ähnlich zu den Kriterien der Heuristiken werden dabei verschiedene Dimensionen auf Muster analysiert: **Userinformationen** (Sprache, geographische Daten, Datum der Accounterstellung), **zeitliche Daten** (Uhrzeiten, Frequenz), **Freunde** (Freunde/Follower Verhältnis, auch als zeitliche Entwicklung), **Netzwerk** (Cluster in Retweets, Hashtagkombinationen), **Inhalt** (Verwendete Begriffe) und wie oben **Sentiment** [VFD⁺17].

Aus diesen Dimensionen kann anschließend ein Wert berechnet werden, der ungefähr als Grad der Übereinstimmung mit den Bots der Trainingsdaten verstanden werden kann. Die Genauigkeit, mit der der Algorithmus Bots aus den Trainingsdaten erkennt, liegt bei ca. 95% (bestimmt durch AUC^6) [DVF⁺16]. Da sich die Bots aber schnell weiterentwickeln, ist die tatsächliche Rate eher niedriger. Dies ist ein grundsätzlicher Nachteil der Verwendung von Maschinenlernalgorithmen zur Klassifikation: Sie können im Prinzip nur Bots erkennen, die nach denselben Mustern agieren, wie die Bots der Trainingsdatenmenge [Heg18]. Ein Test mit neueren Daten, zeigte dennoch einen AUC -Wert von 85% mit dem ursprünglich trainierten Modell [VFD⁺17]. Die Abbildung 2.2 zeigt die Verteilung der Bot-Werte von dem ursprünglichen Modell und den neueren Daten. Man sieht deutlich, wie sich die Erkennungsrate bei den Bots weiter

⁶Der AUC -Wert (*Area under ROC curve*) ist ein Qualitätsmaß und entspricht dem Flächeninhalt unter der Kurve, die den Zusammenhang aus Richtig-Positiv und Falsch-Positiv Rate beschreibt. Der Wert reicht von 0% bis 100%, wobei der Wert 100% eine perfekte Erkennungsrate bedeutet, und 50% reiner Zufall ist. 0% bedeutet, dass immer genau das Gegenteil stimmt, das Kriterium muss damit nur umgedreht werden, um eine perfekte Erkennungsrate zu erreichen.

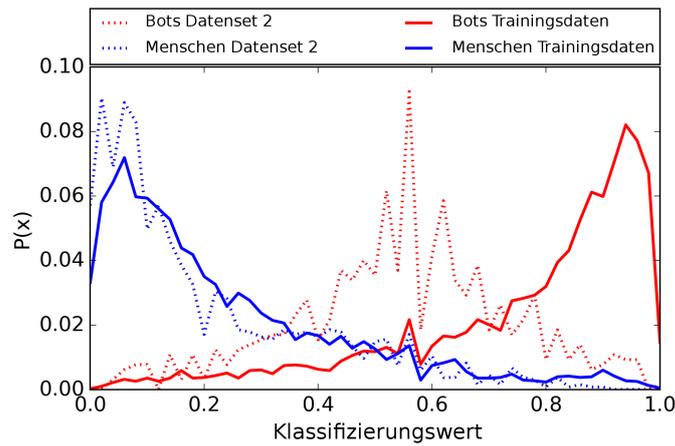


Abbildung 2.2.: Verteilung von Botwerten für die ursprünglichen Trainingsdaten (durchgezogene Linien) und neuere Daten (gepunktet). Bots sind in Rot, Menschen in Blau gekennzeichnet. Bild aus [VFD⁺17] (Label übersetzt)

in Richtung „menschlich“ verschoben hat. Dass auch die neuen Bots grundsätzlich mit Maschinenlernalgorithmen erkannt werden können, sieht man an dem *AUC*-Wert von 94%, der nach dem Training mit den neuen Daten erreicht werden konnte [VFD⁺17].

2.3.2. Identifizierte Einsätze

In den letzten fünf Jahren kam es Studien nach zu mehreren bekannten größeren Einsätzen von Social Bots, insbesondere zu international relevanten politischen Ereignissen wie Wahlen. Im Folgenden sollen einige Daten der relevantesten Einsätze dargestellt werden. Zu beachten ist, dass die Untersuchungen sich fast ausschließlich auf Twitter beziehen, da dort für Forscher mit der API ein einfacher Zugang zu den Daten existiert. Wie viele und welche Aktivitäten von Social Bots auf anderen Plattformen stattfanden, ist daher nicht bekannt.

Krimkrise

Der erste bekannte Einsatz von Social Bots in größerem Umfang fand 2014 während dem Ukraine-Konflikt statt. Bei der Analyse von Tweets vom 22. Februar 2014 (dem Tag der Amtsenthebung des ehemaligen ukrainischen Staatspräsidenten Janukowytsch) fielen einige Textduplikate auf, die keine Retweets waren, sondern von mehreren Nutzern wortgleich getweeted wurden. Eine genauere Untersuchung der Quellen aus den Metadaten deckte zunächst 86 Accounts auf, die über eine einzelne Social Bot Software betrieben wurden. Eine weitere Suche unter deren Followern und Freunden nach derselben Statusquelle lieferte noch ca. 1.500 weitere Botaccounts [HJ16], die im ursprünglichen Datenmaterial nicht enthalten waren.

Inhaltlich spalteten sich die Tweets der Bots sehr auf: 80% der Themen der Beiträge waren unpolitisch und sehr divers, was die Identifikation als Bot sehr erschwerte. Die Posts waren in ukrainischer Sprache verfasst und zielten wohl mit Tweets über Fußball, mit sexistischen Witzen und mit Downloadlinks für Kinofilme auf die Interessen junger ukrainischer Männer ab [Heg16]. Die Social Bots nutzten also vermutlich absichtlich Mechanismen, um im Netzwerk nicht aufzufallen, menschlich zu wirken und sich in einer ganz bestimmten Zielgruppe zu vernetzen. Die Absicht davon war, dass diese Zielgruppe auch mit den anderen Beiträgen besser erreicht wird: Neben diesem „Rauschen“ wurden immer wieder politische Nachrichten gestreut. Dabei gab es sowohl Bots, die alle exakt gleiche Nachrichten posteten und retweeteten, als auch welche, die Nachrichten aus Webseiten beziehen oder im Wortlaut abändern konnten [HJ16]. Viele Beiträge wurden außerdem mit dem Hashtag der rechtsextremen Partei „Rechter Sektor“ versehen. Dies verstärkte zum einen diese Hashtags auf Twitter und zum anderen kann die häufige Kombination mit anderen eigentlich neutralen Hashtags wie #Maidan dazu führen, dass Nutzern, die nach Maidan suchen, auch verstärkt Tweets vom Rechten Sektor angezeigt werden [Heg16].

Später wurden offenbar sogar noch größere Ausmaße des Social Bot Netzwerks auf ca. 15.000 Accounts festgestellt. Die Identifikation als Bots wurde von den Programmierern durch zahlreiche Faktoren erschwert, denn die Bots simulierten einen Schlaf-Rhythmus, posteten in zufälligen Zeitabständen, hatten ein ausgeglichenes Follower/Following-Verhältnis, konnten Beiträge abwandeln und verhielten sich allgemein sehr autonom bei der Imitation von anderen Nutzern [Heg16].

Präsidentenwahlen in den USA 2016

Während dem Wahlkampf im Rahmen der Präsidentenwahlen in den USA 2016 kam es zu mehreren Einsätzen von Social Bots. Bei allen drei Fernsehduellen konnten eine kleine Menge ($< 1\%$) von Accounts ausgemacht werden, die ungewöhnlich viel twitterten (mehr als 50 Tweets pro Tag über die gemessenen 4 Tage hinweg) und für etwa 25% der Posts auf Twitter im beobachteten Zeitraum verantwortlich waren. [KHW16, HKW16a, HKW16b, HKW16c]. Wie im Abschnitt 2.3.1 zu den Heuristiken genannt, wurde in den Auswertungen angenommen, dass diese Accounts zum Großteil Bots oder stark automatisierte Accounts sind, auch wenn sehr aktive menschliche Nutzer eine so hohe Rate ebenfalls zustande bringen könnten. Der Datenjournalist Michael Kreil präsentierte jedoch auf dem 34. Chaos Communication Congress Ergebnisse seiner Analysen, bei denen mit Unterstützung von Experten und mehreren Twitteraccounts [Kre17, Cha17] diese Daten genauer untersucht wurden. Er kam darin zu dem Ergebnis, dass diese Annahme falsch ist und „*in fast allen Fällen echte Menschen dahinter stehen*“ [Mü18]. Nur 2 der 12 aktivsten Accounts seiner Untersuchung waren

Bots ($\approx 16,7\%$). Dies zeigt, wie schwierig es ist, Social Bots als solche zu identifizieren und ebenso dass man mit Daten, wieviele „Bots“ aktiv waren, vorsichtig umgehen muss.

Die Twitter-Posts während den Präsidentschaftswahlen wurden in einer weiteren Studie, durchgeführt von A. Bessi und E. Ferrara, mit dem von ihnen entwickelten maschinell lernenden Algorithmus *Botometer* untersucht. Sie analysierten die 50.000 aktivsten Nutzer und verwendeten einen Schwellwert des Botscores von 0,5 zur Klassifizierung als Bot ($>0,5$) oder Mensch ($<0,5$). Dabei identifizierten sie unter den 50.000 aktivsten Nutzern etwa 7.000 Bots, die für ca. 18,45% der Tweets verantwortlich waren. Ca. 2.600 weitere wurden als „unbekannt“ eingetragen, da ihre Accounts entweder nicht signifikant von dem Schwellwert abwichen, oder die Accounts von Twitter bereits gelöscht wurden [BF16]. Auch diese Datenauswertung kritisierte Michael Kreil und empfindet den Schwellwert als zu niedrig, da auch Regierungaccounts oft einen darüber liegenden Wert erreichen [Kre17]. Der Notiz in [BF16] zufolge wurde dieser Umstand berücksichtigt und mehrere Hundert der identifizierten „Bots“ nochmal manuell auf Accounts von Nachrichtenseiten, Parteien und Organisationen überprüft.

Brexit

Am 23. Juni 2016 kam es in Großbritannien zu einem Referendum über den Verbleib in der Europäischen Union, bei dem die Wähler sich mit der Mehrheit für den Austritt („Brexit“) aus der EU entschieden. Im Vorlauf dieser Wahl wurde viel auf Twitter diskutiert, sodass diese Situation für Social Bots attraktiv war. Eine Analyse von 1,5 Millionen Tweets, die über eine Woche vom 5. bis 12. Juni vor der Wahl gesammelt wurden, stellte eine hohe Aktivität der Bots fest [HK16]: Die aktivsten 100 Profile ($< 0,03\%$) verursachten ca. 8% der Tweets.

Bezeichnet man wieder Accounts mit mehr als 50 Tweets pro Tag im Zeitraum der Messung als Bots oder Profile mit hoher Automatisierung, dann produzierten diese ca. 97 Tausend Tweets mit ausschließlich Pro-Austritt spezifischen Hashtags und ca. 28 Tausend Tweets mit Pro-Verbleib spezifischen Hashtags. Die Verhältnisse von automatisierten zu menschlichen Tweets waren in den beiden Positionen ungefähr ausgeglichen (14,7% der Pro-Brexit-Tweets, gegenüber 15,1% der Pro-Verbleib-Tweets waren automatisiert). Die automatisierten Accounts verstärkten somit nur die Diskussionen, verzerrten aber nicht das Verhältnis der Positionen. Ein interessanter Aspekt in den Daten ist, dass etwa 13 Tausend automatisierte Tweets sowohl Pro-Brexit, Pro-Verbleib als auch neutrale Hashtags verwendet haben. Der Anteil der automatisierten Posts an allen mit diesen Kennzeichen liegt mit etwa 30% deutlich höher. Dies lässt sich damit erklären, dass viele Bots nur die Hashtags der aktuellen Trends nutzten, um damit Werbespam zu verbreiten, aber eigentlich gar nicht an einer politischen Debatte beteiligt

waren [Heg16]. Insgesamt handelte es sich bei den Tweets der aktivsten Accounts kaum um neue Inhalte, sondern größtenteils um Retweets [HK16].

Am Beispiel Brexit wird jedoch auch deutlich, dass Botaktivität nicht mit deren Einfluss verwechselt werden darf. Denn obwohl das Referendum zugunsten der Befürworter des Austritts entschieden wurde, ist fraglich, ob die Bots dies beeinflussen konnten. Gerade junge Erwachsene mit höherem Bildungsniveau, die in Großbritannien den Großteil der Twitternutzer ausmachen, stimmten für den Verbleib in der EU [Heg16]. Die meisten Leute, die für den Brexit gestimmt haben, sind also vermutlich gar nicht mit Social Bots in Berührung gekommen, wurden also auch nicht von diesen beeinflusst.

Proteste in Mexiko – „#YaMeCanse“

Unter dem Hashtag „#YaMeCanse“ (übersetzt: Ich habe es satt) formte sich auf Twitter im November und Dezember 2014 ein Protest in Mexiko. Bots unterbanden diese Kommunikation über Twitter, indem sie massenhaft Beiträge mit dem selben Hashtag posteten und so die Nutzer daran hinderten sinnvolle Beiträge darin zu finden. Daraufhin gingen die Nutzer zu „#YaMeCanse2“ über, etwas später gefolgt von den Bots, woraufhin die Nutzer zu „#YaMeCanse3“ übergingen, usw. bis „#YaMeCanse25“ [SSRDM16]. In der Analyse wurden etwa 150.000 Tweets mit den ersten 5 Hashtags von 28.000 Nutzern untersucht und mit der Botometer API mit den möglichen verschiedenen Kriterien (Freunde, Netzwerk, Zeit, Inhalt, Sentiment) analysiert und die sich ergebenden Wahrscheinlichkeitsverteilungen kombiniert. In der Abbildung 2.3 sind die Ergebnisse daraus dargestellt und die Nutzer gekennzeichnet, die vermutlich Bots sind.

Weitere frühere Einsätze

In Tabelle 2.1 werden verschiedene mutmaßliche Einsätze in einigen Ländern aus den Jahren 2011 bis 2014 zusammengestellt. Als Datengrundlage diente die Auswertung von 41 Zeitungsartikeln, die über die Einsätze berichteten und Daten präsentierten [Woo16].

2.4. Rechtslage

Die Diskussion, wie Gefahren von Social Bots durch rechtliche Rahmenbedingungen eingeschränkt und kontrolliert werden können, kam in Deutschland im Vorfeld der Bundestagswahlen 2017 ebenfalls auf. Eine häufige Forderung dabei ist eine Kennzeichnungspflicht für Social Bots. Diese wird jedoch sehr kontrovers diskutiert [KJW⁺17, S. 62].

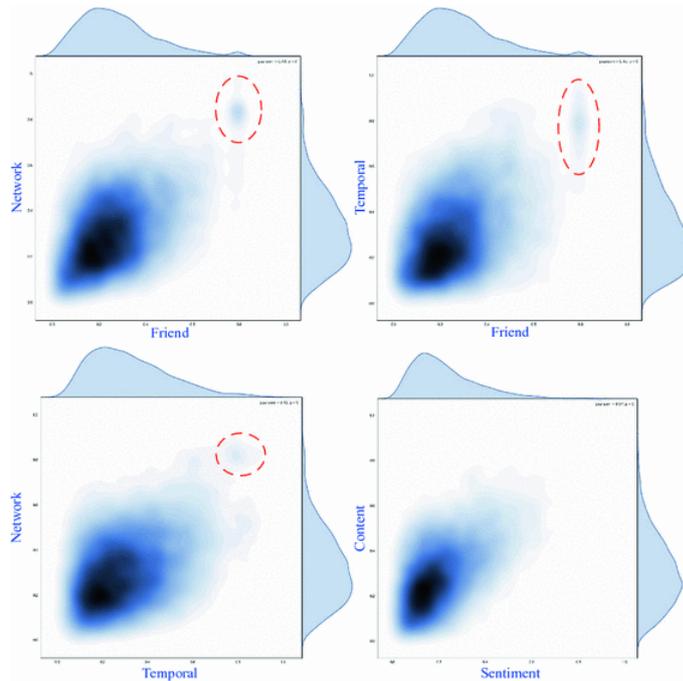


Abbildung 2.3.: Kombinierte Botometer Wahrscheinlichkeitsverteilungen zu den Merkmalen Freunde-Netzwerk, Freunde-Zeit, Zeit-Netzwerk and Inhalt-Sentiment. Datengrundlage sind 14.756 eindeutige Accounts, die zwischen 26. und 30. November 2014 mit dem Hashtag „#YaMeCanse“ getweetet haben [SSRDM16]. Da das Botometer mit englischen Daten trainiert wurde und die meisten Tweets der Datengrundlage auf Spanisch verfasst sind, kann aus dem Inhalt-Sentiment Bild keine Information gewonnen werden. Die anderen zeigen deutliche Häufungen von als Bot identifizierten Nutzern (rot markiert).

Das Programmieren von Social Bots, das Erstellen zahlreicher Nutzeraccounts und das Verbreiten von Nachrichten ist nach deutschem Recht legal [KJW⁺17, S. 39]. Der Inhalt der Nachrichten muss sich dabei aber natürlich dennoch an Äußerungsdelikte halten und kann unter Umständen Straftatsbestände wie Betrug, Volksverhetzung oder Identitätsdiebstahl erfüllen. Der Einsatz von Social Bots verstößt zudem im Allgemeinen gegen die AGBs der Netzwerke [KJW⁺17, S. 39]. Ein großes Problem in der Diskussion ist, dass die Betreiber der Social Bots kaum auffindig zu machen sind und eine Strafdurchsetzung abgesehen von der Accountlöschung im sozialen Netzwerk schwer möglich ist [KJW⁺17, S. 67]. Das im Oktober 2017 in Kraft getretene Netzwerkdurchsetzungsgesetz nimmt daher die Betreiber der sozialen Netzwerke in die Pflicht stärker gegen gemeldete Falschnachrichten oder Manipulationen vorzugehen.

| Land | Einsatzfälle von Bots | Demobilisierung | Regierungsfreundliche Beiträge | Followerzahl aufbessern |
|---------------------------------------|------------------------------------|-----------------|--------------------------------|-------------------------|
| Argentinien | Politische Unterstützung / Protest | X | X | |
| Australien | Wahlen | | | X |
| Aserbaidshan | Protest | X | | |
| Bahrain | Protest | X | X | |
| China | Wahlen / Protest / Sicherheit | X | X | |
| Iran | Protest | X | X | |
| Italien | Politische Unterstützung | | | X |
| Mexiko | Wahlen | X | X | X |
| Marokko | Protest | X | X | |
| Russland | Wahlen / Protest / Sicherheit | X | X | |
| Süd Korea | Wahlen | | X | X |
| Syrien | Protest | X | X | |
| Tibet | Protest | X | | |
| Türkei | Politische Unterstützung / Protest | X | X | X |
| UK Großbritannien | Wahlen | | | X |
| Vereinigte Staaten von Amerika | Wahlen / Sicherheit | | | X |
| Venezuela | Wahlen / Protest | X | X | |

Tabelle 2.1.: In den Nachrichtenartikeln berichtete Fälle und Arten, wie politisch motivierte Bots eingesetzt wurden. Die Vorfälle sind alle aus dem Zeitraum von 2011 bis 2014 [Woo16, übersetzt ins Deutsche]. Insbesondere 2016 kamen unter anderem mit den in Kapitel 2.3.2 aufgeführten einige weitere Einsätze hinzu.

3. Bedeutung für die Schule und den Informatikunterricht

Social Bots sind ein gesellschaftlich hoch relevantes Thema. Wenn sie die Wirkungen aus Kapitel 2.2 entfalten können, stellen sie eine Bedrohung der Demokratie dar [KJW⁺17, S. 40]. Um dem gegenzusteuern, muss in der Gesellschaft ein Bewusstsein für diese Gefahr geschaffen werden. Im Folgenden wird erläutert, warum diese Aufgabe zu einem großen Teil in der Schule liegt. Zudem wird aufgezeigt, dass die Thematisierung interdisziplinär verlaufen sollte und dass vor allem der Informatikunterricht wichtige Ansätze zum Verständnis liefert. Auch umgekehrt kann der Informatikunterricht durch die vielfältigen Einsatzmöglichkeiten von Social Bots sehr profitieren. Dies wird anhand der verschiedenen Bildungsstandards der Informatik verdeutlicht, die durch die Einbringung von Social Bots unterstützt werden können.

3.1. Beurteilung der Relevanz für die Schulbildung

Um zu beurteilen, ob Social Bots ein Thema sind, das im Rahmen der Schulbildung vermittelt werden soll, werden die folgenden drei Fragen untersucht:

- Besitzt die Thematik eine Relevanz im Alltag der SchülerInnen?
- Ist es Aufgabe der Schulen, über Social Bots zu informieren, oder kann das außerhalb der Schule geschehen?
- Welche Ziele können bei den SchülerInnen durch Bildung in diesem Gebiet erreicht werden?

3.1.1. Lebensnahes Thema für SchülerInnen

Soziale Netzwerke ziehen immer mehr in den Alltag ein und gerade Jugendliche und junge Erwachsene verbringen dort viel Zeit. Dadurch kommen sie auch mit Social Bots in Kontakt und sind mit deren Einflüssen konfrontiert. Die in Kapitel 2.2 dargestellten Gefahren betreffen daher direkt die SchülerInnen.

Auch in absehbarer Zeit bleiben die Bots wahrscheinlich relevant. Durch die weiter fortschreitende, technische Entwicklung können sie schwieriger von Menschen unterschieden werden und sind durch die Fortschritte im Bereich Künstliche Intelligenz vielseitiger einsetzbar. Die SchülerInnen kommen auch weiterhin mit Social Bots in Kontakt. Denn dem Trend der Nutzerzahlen sozialer Netzwerke [Med17, S. 31f.] nach zu urteilen bleiben die SchülerInnen dort auch in nächster Zeit aktiv. Zwar finden Verschiebungen zwischen den einzelnen Plattformen statt (derzeit z.B. von Facebook zu moderneren Webseiten wie Instagram), doch das schnelle Wachstum der Nutzerbasis zeigt den hohen Stellenwert der digitalen Vernetzung im heutigen Leben.

3.1.2. Pflicht der Schulen

Obwohl Social Bots in der Lebenswelt der Jugendlichen präsent sind, fallen sie im Normalfall nicht auf den ersten Blick als Computerprogramme auf. Ein kritisch reflektierter Umgang mit den Medien ist nötig, um Social Bots zu erkennen und nicht durch die Manipulation beeinflusst zu werden. Die SchülerInnen für Bots zu sensibilisieren ist daher Aufgabe der Medienbildung. Da sie, wie im vorigen Kapitel dargestellt, schon früh mit Social Bots konfrontiert sind, sollte die Medienkompetenz ebenfalls möglichst früh vermittelt werden. Die Förderung kann dabei schlecht *nur* in der Schule durchgeführt werden, da die SchülerInnen den größeren Teil ihres Alltags nicht in dieser begleiteten Umgebung verbringen. Sie muss auch durch die Eltern mitgetragen werden. Genauso wenig kann sie jedoch in der Schule weggelassen werden. Die Verankerung der Medienbildung in den Schulstoff stellt einen wichtigen Ausgangspunkt zu einer nachhaltigen und systematisch entwickelten Medienkompetenz dar [KMK12, S. 3f]. Diese hilft die Einflüsse von Social Bots zu schwächen.

Ein weiterer Grund für die Behandlung von Social Bots im Schulunterricht ist der Allgemeinbildungsauftrag der Schulen. Dieser verpflichtet die Schulen dazu, gesellschaftlich relevante Themen zu besprechen. Die in Kapitel 2.3.2 geschilderten Einsätze zeigen, dass Social Bots bei vielen Weltereignissen wichtig sind. SchülerInnen sollten daher als allgemeingebildete Personen auch über diese Manipulationen Bescheid wissen.

3.1.3. Ziele der Thematisierung von Social Bots

Durch die inhaltliche Auseinandersetzung mit Social Bots können wichtige Veränderungen im Denken und Handeln der SchülerInnen erreicht werden. Folgende Punkte stellen erwünschte Folgen der Thematisierung dar.

Kritische Reflexion der Medien: Wie oben dargestellt, hängt die Wirksamkeit der Social Bots vor allem von der Medienkompetenz der Nutzer ab und von dem Wissen,

dass Manipulationen auf diese Art durchgeführt werden können. Sind die Nutzer dafür nicht sensibilisiert, empfinden sie Bot-gesteuerte Themen als gesellschaftliche Bewegung und messen ihm eine höhere Bedeutung bei. Durch Aufklärung über die Existenz von Social Bots und die Wirkmechanismen kann diese Gefahr deutlich abgeschwächt werden. Aufkommende Themen in sozialen Medien werden dann eher hinterfragt. Wegen der noch neuen Technik ist auch die Tarnung der Bots noch leicht zu durchschauen, wenn man dafür sensibilisiert ist.

Partizipation an Diskussionen zu gesellschaftlichen Problemen: SchülerInnen sollen über aktuelle, gesellschaftliche Probleme informiert werden, um an Diskussionen dazu teilhaben zu können. Derzeit sind noch keine Regulierungen zu Social Bots eingerichtet und die Erkennungswerkzeuge hinken grundsätzlich der Weiterentwicklung der Bots hinterher. Aus diesen Gründen ist davon auszugehen, dass die Diskussion, wie die Einsätze von Social Bots unterbunden werden können, noch länger nicht abgeschlossen ist. Möchte man den SchülerInnen ermöglichen, in diesem Diskurs teilzunehmen, muss man ihnen die Problemstellung nahe bringen.

Vorbereitung auf zukünftige Technologien: Es ist schwierig, zukünftige Technologien vorherzusagen, allerdings bleiben die Grundideen oft gleich. Bei Social Bots zentral ist die Beeinflussung der Menschen durch Technologien, die im Alltag viel genutzt werden. Die Betrachtung der Bots als konkretes Beispiel für diese Manipulationen ermöglicht den SchülerInnen später den Transfer auf neue Technologien. Die SchülerInnen werden also nicht nur auf die Gefahren von Social Bots vorbereitet, sondern lernen allgemein, wie technische Entwicklungen ihr Leben beeinflussen, aber auch unterstützen können.

3.2. Social Bots als Interdisziplinäre Herausforderung

Nachdem im vorigen Abschnitt begründet wurde, dass die Schulen in der Pflicht stehen über Social Bots aufzuklären, stellt sich die Frage, in welchem Fach Wissen über die Social Bots vermittelt werden sollen. Wie im Folgenden ausgeführt, ist das Leitfach die Informatik, jedoch sollte die Betrachtung am Besten interdisziplinär geschehen. Interdisziplinarität bietet grundsätzlich spannende Chancen für das Lernen. Behandelt man ein Thema in mehreren Fächern, werden den SchülerInnen die Zusammenhänge zwischen den Fächern bewusst und sie lernen unterschiedliche Blickwinkel kennen. Dadurch werden die Lerninhalte besser vernetzt und bleiben so auch länger im Gedächtnis. Außerdem ermöglicht es SchülerInnen, fachspezifische Stärken auf andere Bereiche zu übertragen. Auch Kooperationen zwischen SchülerInnen mit unterschiedlichen Interessen können entstehen und helfen, das Gelernte aufzuarbeiten.

Das Thema Social Bots ist sehr vielschichtig. Es betrifft viele Bereiche des Lebens, unter anderem die Informatik, die Politik und Gesetzgebung und zum Teil auch die Wirtschaft. Analog dazu sollte die Thematik auch in der Schule fächerübergreifend behandelt werden. Im Folgenden werden zwei Möglichkeiten ausgeführt, die relevanten Fächer zu identifizieren: Erstens kann überlegt werden, welche Schulfächer Blickwinkel zu Social Bots bieten, die für ein umfassendes Verständnis notwendig sind. Zweitens können die wichtigen Konzepte hinter Social Bots herausgearbeitet werden und damit die benötigten Fächer identifiziert werden.

3.2.1. Verschiedene Blickwinkel

Im folgenden werden Schulfächer aufgeführt, die von der Thematik „Social Bots“ betroffen sind. Es wird erläutert, inwiefern diese einen wichtigen Beitrag für das Verständnis von Social Bots bieten:

- **Informatik:** Den signifikantesten Beitrag zum Verständnis liefert der Informatikunterricht. Dort können die technischen Grundlagen der Bots vermittelt und ein theoretisches Verständnis der Funktionsweise aufgebaut werden. Der Wechsel der Perspektive bei der Implementierung von den Programmen hilft SchülerInnen abzuschätzen, wozu die Technologie in der Lage ist und wozu nicht.
- **Sozialkunde**¹: Als Leitfach der politischen Bildung führt der Sozialkundeunterricht die SchülerInnen zu einer politischen Mündigkeit. Ihnen wird vermittelt, kritisch über aktuelle Geschehnisse zu reflektieren und ihnen vorgelegte Informationen und Meinungen auf ihren Fakten- und Wahrheitsgehalt hin zu überprüfen. Diese Kompetenzen sind unabdingbar, wenn sich die SchülerInnen online an politischen Diskursen beteiligen wollen, die womöglich von Social Bots beeinflusst werden.
- **Geschichte:** Der Geschichtsunterricht liefert die historischen Zusammenhänge zu politisch motivierten Manipulationen. Aus den früheren Erfahrungen können zukünftige Auswirkungen der Manipulationen besser abgeschätzt werden.
- **Ethik**²: In der Thematik Social Bots geht es auch um moralische Entscheidungen. Zum Beispiel muss überlegt werden, ob gutartige Einsätze von Social Bots vertretbar sind und wie man entscheidet, welche Verwendungszwecke moralischer und welche unmoralischer Natur sind.

¹Stellvertretend für die Bezeichnungen anderer Bundesländer wie Gemeinschaftskunde, Politik oder Politische Bildung

²Ethik ist oft in den Religionsunterricht integriert

3.2.2. Analyse der fundamentalen Ideen

Die Kriterien der fundamentalen Ideen nach Bruner und Schwill [Sch93] liefern eine Möglichkeit, zu überprüfen ob ein Inhalt ein wichtiges Konzept einer Fachwissenschaft vermittelt oder nicht. Das Thema Social Bots selbst erfüllt nicht alle Kriterien der fundamentalen Ideen. Ein Problem ist das Zeitkriterium, da Social Bots zwar voraussichtlich noch länger relevant bleiben, jedoch erst seit kurzem existieren. Es kommen aber in Social Bots mehrere andere fundamentale Ideen zusammen. Das größer gefasste Thema Bot bzw. Künstliche Intelligenz ist beispielsweise eine fundamentale Idee der Informatik: Die Vorstellung, den Menschen durch eine Maschine nachzuahmen, wurde bereits vor dem Aufkommen der Informatik in Büchern aufgegriffen und hat spätestens seit der Formulierung des Turing-Tests entscheidend die Entwicklung der Informatik mitbestimmt. Das Zeitkriterium ist hier also erfüllt. Es ist auch auf verschiedenen Schwierigkeitsgraden beschreibbar (Vertikalkriterium): Angefangen bei einfachen Gesprächen mit Chatbots oder der für Grundschüler entwickelten Programmierapp Light-Bot (<http://lightbot.com/>), bis zu komplexen Berechnungen in neuronalen Netzen. Für das Horizontalkriterium können zahlreiche Bereiche der Informatik angeführt werden, in denen Bots zum Einsatz kommen. Beispielsweise setzen Suchmaschinen Webcrawler ein, um Internetseiten zu indexieren, Chatbots verarbeiten natürliche Sprache und Serviceroboter helfen im Haushalt. Das Sinnkriterium ist, wie in Kapitel 3.1.1 ausgeführt, ebenfalls erfüllt.

Social Bots haben jedoch noch weitere Dimensionen, als nur technische Aspekte. Propaganda ist beispielsweise ein wichtiges Konzept hinter Social Bots und eine fundamentale Idee der Geschichte und der Sozialkunde. „*Propaganda ist der Versuch der gezielten Beeinflussung des Denkens, Handelns und Fühlens von Menschen*“ [Bun11] und umfasst alle Formen der absichtlichen Meinungsmanipulation, also z.B. neben der politischen Propaganda auch Werbung für Produkte und PR-Arbeit. Auch hier können wieder die Kriterien betrachtet werden. Beispielsweise, ist das Horizontalkriterium durch die verschiedenen eben erwähnten Bereiche von Propaganda abgedeckt. Zudem macht vor allem die Werbung auch wieder eine Alltagsrelevanz für SchülerInnen deutlich, womit das Sinnkriterium ebenfalls erfüllt ist.

Aus den obigen Betrachtungen ergibt sich somit, dass relevante Konzepte durch Social Bots im Informatik-, Geschichts- und Sozialkundeunterricht vermittelt werden können.

3.3. Anknüpfungspunkte in der Informatik

Die Informatik ist das zentrale Fach zum Verständnis von Social Bots. Daher liegt dort der Fokus in dieser Arbeit und die Bedeutung wird im Folgenden noch weiter ausge-

führt. Es wird aufgezeigt, womit sich der Informatikunterricht allgemein beschäftigt und wie sich Social Bots in diese Inhalte einbinden lassen. Ein wichtiges Argument für die Betrachtung von Social Bots im Informatikunterricht ist dabei die vielseitige Anwendbarkeit sowohl bezüglich der Themenbereiche als auch bezüglich der Jahrgangsstufen.

3.3.1. Rolle von Informatikunterricht

In Deutschland findet immer wieder die Diskussion statt, ob an den Schulen ein eigenes Pflichtfach Informatik benötigt wird und falls ja, in welchem zeitlichen Umfang man es unterrichten sollte. Dabei herrscht zum Teil immer noch ein sehr verzerrtes Bild des Inhalts von Informatik: Meistens werden die Aspekte der Anwenderschulung (z.B. Office Programme bedienen) und das Programmieren der Informatik zugerechnet. Jedoch geht es neben diesen Bereichen im Informatikunterricht vor allem darum, grundlegende Konzepte hinter den Informationstechniken der Lebenswelt der SchülerInnen zu vermitteln [Hub07, S. 48]. Dies ermöglicht den SchülerInnen die Lerninhalte leichter auf andere Systeme zu übertragen. Aus diesen Grundsätzen heraus beschrieb die Gesellschaft für Informatik Bildungsstandards [Ges08, Ges16], die die Inhalte für die Sekundarstufe I und II abstecken und definieren, welche Kompetenzbereiche angesprochen werden sollen.

3.3.2. Social Bots in den Bildungsstandards

Die Bildungsstandards teilen sich in fünf Prozessbereiche und fünf Inhaltsbereiche [Ges08, S. 11]. Die Prozessbereiche beschreiben Aktivitäten, die die SchülerInnen im Informatikunterricht durchführen sollen. Sie sind weitestgehend unabhängig vom jeweiligen Thema und können durch geeignete Aufgabenstellungen bei jedem Thema abgedeckt werden. Daher helfen sie weniger bei der Einordnung und werden erst an dem konkreten Unterrichtsentwurf in Kapitel 4.2.2 zugeordnet. Für die Einordnung interessanter ist die Betrachtung der Inhaltsbereiche, die im Folgenden näher ausgeführt wird. Das Ziel ist dabei nicht, mit einer Unterrichtseinheit alle Inhaltsbereiche abzudecken. Es sollen stattdessen Möglichkeiten aufgezeigt werden, an welchen Stellen durch Unterrichtssequenzen zu Social Bots wichtige Aspekte eingebracht werden können. Das Thema ist sowohl in verschiedenen Schulstufen als auch in den unterschiedlichen Bereichen einsetzbar.

Information und Daten

In der Sekundarstufe I sollen die SchülerInnen in diesem Bereich den „*Zusammenhang von Information und Daten [verstehen]*“ und „*Operationen auf Daten sachgerecht*

durchführen“ [Ges08, S. 23]. Verarbeitung von Daten ist ein wesentlicher Bestandteil von Social Bots. Beispielsweise können durch eine Suche nach Schlüsselwörtern in Texten Informationen über den Inhalt gewonnen werden, wodurch Bots gezielt auf relevante Inhalte antworten können. Dies ist unabhängig von der algorithmischen Implementierung und kann mit SchülerInnen bereits in der Unterstufe zum Beispiel mit Chatbots betrachtet werden. Programmierkenntnisse sind notwendig, wenn die Daten selbst verarbeitet werden sollen. Ein Beispiel für die Verarbeitung von Daten einer Web-API ist in der Unterrichtsstunde in Kapitel 4 zu finden.

Algorithmen

Für das Verständnis der Grenzen von Bots ist zentral, sie als Algorithmus wahrzunehmen. Bots treffen keine eigenen Entscheidungen, sondern handeln nach vorgegebenen Schritten. Betrachtet man die Funktionsweise von Social Bots, geht es daher immer um eine Beschreibung von Algorithmen. In der Sekundarstufe I ist das Entwerfen und die Visualisierung solcher algorithmischen Vorgänge relevant [Ges08, S. 32]. Mit angemessenen Vorgaben lässt sich auch bereits die Implementierung von Social Bots umsetzen. Geeigneter ist eine Umsetzung aber in der Sekundarstufe II, da die SchülerInnen dann mit der Programmiersprache vertrauter sind und sich auf den algorithmischen Ablauf eines Bots konzentrieren können. Diese Umsetzung passt zudem besonders gut, da die SchülerInnen in der Sek. II *„bereitgestellte Module bei der Implementierung von Algorithmen“* verwenden sollen [Ges16, S.10].

Sprachen und Automaten

Der Inhaltsbereich „Sprachen und Automaten“ eignet sich nur wenig dafür, Social Bots aufzugreifen. Mit Binnendifferenzierung ist es möglich, dass leistungsstärkere SchülerInnen Konzepte aus dem Bereich vertiefen, indem sie die Beiträge eines Social Bots mithilfe einer Grammatik implementieren. Eine Umgebung dafür bietet die Webseite CheapBotsDoneQuick.com. Dort lässt sich ein Twitterbot mit einer Grammatik bauen, der dann in einem festgelegten Zeitabstand Beiträge schreibt und auf Tweets antwortet, die an ihn gesendet werden. Die Konzepte des Bereichs können durch die Social Bots aber nur angewandt werden und sollten nicht damit eingeführt werden.

Informatiksysteme

Die beiden wichtigsten Informatiksysteme, die in Unterrichtssequenzen zu Social Bots betrachtet werden, sind die Social Bots selbst und Webseiten mit zugehöriger API. Für die Mittelstufe wird in den Bildungsstandards gefordert, dass sie *„mit Internetdiensten [arbeiten]“* und *„sich selbständig neue Informatiksysteme [erschließen]“* [Ges08, S.

17]. Auch für diese Inhalte können Social Bots verwendet werden. Das Erschließen des Programmablaufs eines Social Bots ist ein Beispiel. Mit weniger technischen Vorkenntnissen verbunden ist die Aufgabe, aus einem sozialen Netzwerk mögliche Interaktionen für einen Social Bot abzuleiten. Dafür müssen Lernende das Netzwerk erschließen und mit den Möglichkeiten von Social Bots verknüpfen. Eine weitere Möglichkeit, das Webseiten-Informatiksystem zu erschließen, ist, die SchülerInnen über die API mit der Webseite kommunizieren zu lassen.

Informatik, Mensch und Gesellschaft

Da der Einsatz der Bots ein gesellschaftliches Problem ist, wird bei Social Bots der Inhaltsbereich „Informatik, Mensch und Gesellschaft“ am deutlichsten angesprochen. Die Analyse der Problematik und der Wechselwirkung zwischen Technik und Gesellschaft ermöglicht den SchülerInnen Gefahren zu beurteilen. Dies entspricht dem grundlegenden Anforderungsniveau für die Sekundarstufe II [Ges16, S. 12]. Da die SchülerInnen außerhalb der Schule in sozialen Netzwerken aktiv sind, ist auch die Reflexion über das eigene Verhalten möglich. Das Verständnis für Manipulationen von Daten ist aber nicht erst in der Oberstufe relevant, sondern findet sich bereits in den Kompetenzstandards für die Unterstufe: SchülerInnen sollen „*wissen, dass digitale Daten leicht manipulierbar sind*“ [Ges08, S. 18]. Dafür kann den SchülerInnen bereits durch eine kurze Thematisierung von Social Bots ein konkretes Beispiel gegeben werden.

4. Unterrichtseinheit: Programmieren eines Social Bots

In diesem Kapitel wird eine Unterrichtseinheit vorgestellt, in der die SchülerInnen einen eigenen Social Bot programmieren. Dadurch sollen sie zum einen ein tieferes Verständnis für die Funktionsweise von solchen Programmen entwickeln. Das hilft ihnen insbesondere dabei, Gefahren aber auch Grenzen von Social Bots besser einschätzen zu können und für derartige Manipulationen in der öffentlichen Debatte sensibilisiert zu sein. Zum anderen vertiefen sie in der Anwendung wichtige Konzepte der Kommunikation in Rechnernetzen, wie Protokolle und Programmierschnittstellen (*API*). Immer mehr Dienste im Internet bieten eine API an. Das Wissen, das die SchülerInnen durch das Programmieren mit Netzwerkkomponenten hierzu aufbauen, hilft ihnen allgemein dabei, solche Dienste zu verwenden.

Die Unterrichtseinheit wird auf Grundlage der Faktoren des Berliner Modells von Paul Heimann [Hub07, S. 26f., S. 29-40] geplant. Das Kapitel ist daher gegliedert in die Analyse der Bedingungsfelder, der Lerninhalte, der Ziele, der Medien und der Methodik. Als Ergebnis der Planung wird der Stundenverlauf skizziert. Das geplante Konzept wurde im Rahmen der Arbeit zudem in einer 12. Jahrgangsstufe an einem bayrischen Gymnasium eingesetzt und in Kapitel 4.7 reflektiert. Es ergaben sich dadurch keine wesentlichen Konzeptänderungen, allerdings bietet die Reflexion Hinweise, worauf im Unterricht speziell geachtet werden sollte.

4.1. Bedingungsfelder

Im Folgenden wird eine durchschnittliche Klassensituation dargestellt, für die die Unterrichtseinheit konzipiert wurde.

4.1.1. Anthropologisch-psychologische Voraussetzungen

Die SchülerInnen sind größtenteils an informatischen Themen interessiert, da diese für sie einen starken Alltagsbezug haben. Gerade mit Anwendungen aus ihrer Lebenswelt lassen sie sich leicht motivieren. Dies hat für die Stunde eine hohe Lernbereit-

schaft zur Folge. Durch eine offene Aufgabenstellung wird diese Motivation aufgegriffen.

Kenntnisse aus dem Themenbereich „Kommunikation in Rechnernetzen“ sind für die Unterrichtseinheit nicht zwingend nötig. Allerdings kann den SchülerInnen helfen, wenn sie bereits Vorwissen zu dem Konzept „Protokoll“ besitzen und Netzwerkkommunikation im Internet auf einer abstrakten Ebene der Schichten (z.B. OSI-Modell) bereits verstanden wurde.

Das Leistungsniveau im Programmieren ist gemischt. Damit die Lernenden den Bot selbständig entwickeln können, sollten sie bereits ungefähr ein bis zwei Jahre Erfahrung mit einer Programmiersprache gesammelt haben. Um schwächere SchülerInnen möglichst gut unterstützen zu können und den Besseren dennoch Lerngelegenheiten zu verschaffen, muss auf jeden Fall eine Binnendifferenzierung stattfinden. Insbesondere müssen SchülerInnen gezielt unterstützt werden, die wenig Erfahrung damit haben, bereitgestellte Programmteile selbständig zu verwenden. Genauere Details zu der Implementierung von Social Bots und den Grundlagen, die dafür nötig sind, werden in der inhaltlichen Analyse (Kapitel 4.2) ausgeführt.

Vorwissen zu Social Bots ist vereinzelt aus Nachrichtenberichten vorhanden, allerdings in der Regel ohne tieferes, informatisches Verständnis. Dennoch kann auf gewisses Vorwissen z.B. über Bots im Allgemeinen zurückgegriffen werden.

4.1.2. Soziokulturelle Voraussetzungen

Der Unterrichtsentwurf „Programmieren eines Social Bots“ knüpft an das Thema „Kommunikation in Rechnernetzen“ an, das in den Bildungsstandards der Sek. II in den Informatiksystemen einzuordnen ist [Ges16, S. 11]. Der Entwurf umfasst insgesamt drei Schulstunden. Haben die SchülerInnen weniger Erfahrung mit Programmierung, kann dies mit einer zusätzlichen Einarbeitungszeit von ein bis zwei Schulstunden ausgeglichen werden.

Die Unterrichtsstunde wurde für den Einsatz im Computerraum konzipiert. Die SchülerInnen sollten entweder jeder einen eigenen PC zur Verfügung haben oder zu zweit beispielsweise mit Pairprogramming (mehr dazu in Kapitel 4.5) an einem PC arbeiten.

4.2. Inhaltliche und didaktische Analyse

Im Folgenden werden die Lerninhalte der Unterrichtsstunde fachlich und didaktisch analysiert. Anschließend werden die angesprochenen Bildungsstandards zugeordnet.

Nachdem in Kapitel 3 bereits eine allgemeine Einordnung von Social Bots in die Bildungsstandards erfolgt ist, geht es hier vor allem um die konkreten Tätigkeiten der SchülerInnen, die die jeweiligen Kompetenzbereiche stärken sollen.

4.2.1. Lerninhalte

Die Unterrichtsstunde bietet eine anwendungsorientierte Vertiefung der Client-Server-Kommunikation und vermittelt mit *JSON* zudem ein weit verbreitetes Protokoll der Anwendungsschicht im OSI-Modell und bietet so eine praxisrelevante Verknüpfung mit dem zuvor in der Theorie erlernten Konzept „Protokoll“.

Protokoll

Den SchülerInnen soll ein grundsätzliches Verständnis von *GET*- und *POST*-Anfragen beigebracht werden. Dabei handelt es sich um HTTP-Anfragen, also bestimmte Protokolle, die bei der Kommunikation mit Hypertexten verwendet wird. *GET* ist dabei für Anfragen, die vom Server Daten abrufen. Eventuell nötige Parameter werden dabei sichtbar in der Anfrage-URL mitübertragen und durch ein Fragezeichen abgetrennt (siehe Abbildung).

```
http://www.example.com/route?parameter1=wert1&parameter2=wert2
```

Abbildung 4.1.: URL bei einer *GET*-Anfrage. Das Fragezeichen trennt die Parameter von der Route ab und die wiederum werden durch das Und-Symbol getrennt.

POST wird für Anfragen verwendet, die Daten zur Verarbeitung an den Server schicken. Es wird insbesondere für alle sensiblen Daten, wie beispielsweise Anmeldedaten, verwendet. Die Daten sollen daher nicht in der URL sichtbar sein und werden daher im Nachrichtenrumpf übertragen. In der vorliegenden Unterrichtseinheit wird aber vor allem auf die Unterscheidung von „Daten senden“ und „Daten abrufen“ Wert gelegt, da dies für die Verwendung von allen APIs grundlegend ist. Die Begriffsdopplung mit Posts in sozialen Netzwerken sollte in der Unterrichtsstunde ebenfalls angesprochen werden, um Missverständnisse bei den SchülerInnen zu vermeiden.

Neben diesen zwei HTTP-Anfragen existieren noch mehrere weitere, darunter *DELETE* (Anfrage zum Löschen eines Datenelements) und *PUT/PATCH* (Anfrage zur Aktualisieren eines bestehenden Datenelements auf dem Server), die jedoch in der Unterrichtsstunde nicht erwähnt werden. Sie bieten auch keinen konzeptionellen Unterschied zu *POST*, sodass das problemlos ausgelassen werden kann.

Programmierstrukturen

Der Programmcode eines Social Bots ist (in der Komplexität, die in dem Unterricht betrachtet werden kann) nur eine einzelne Datei mit dem programmierten Ablauf des Bots und Funktionen zum Netzwerkzugriff auf die API des sozialen Netzwerkes. Der Fokus in der Programmierung liegt daher weniger auf Datenstrukturen oder Objektkommunikation, sondern eher auf einer guten Strukturierung des Programmcodes in übersichtliche Methoden. Notwendige Vorkenntnisse sind Grundkenntnisse wie Sequenzen, Schleifen und Verzweigungen sowie Kenntnisse im Umgang mit Arrays oder Listen. Letzteres wird benötigt, um die Daten, die der Server bei einer *GET*-Anfrage liefert, verarbeiten zu können.

Je nach gewünschtem Abstraktionsgrad der Protokolle und der API können entweder bereits Methoden wie `posten(String nachricht)` vorgegeben werden, oder nur Methoden wie `GETAnfrageSenden(String url)` und `POSTAnfrageSenden(String url, JSONObject daten)` bereitgestellt werden, aus denen dann die `posten`-Methode selbst programmiert werden muss. Ersteres fokussiert sich dann mehr auf den algorithmischen Ablauf eines Social Bots, letzteres stärker auf die Kommunikation in Rechnernetzen. Da in der hier geplanten Unterrichtsstunde vor allem auch Konzepte wie APIs und Protokolle vertieft werden sollten, passt der zweite Ansatz besser. Dieser ermöglicht auch einen Transfer, denn *GET* und *POST* sind die Standards aller Webseiten. Andererseits müssen die SchülerInnen bei diesem Ansatz auf einer abstrakteren Ebene programmieren.

Eine weitere Differenzierung kann mit den JSON-Daten geschehen: Entweder die SchülerInnen verarbeiten die Daten selbst als JSON mit der bereitgestellten Bibliothek. Dafür sind ein vertieftes Verständnis von Datentypen und ein sicherer Umgang mit Methodenaufrufen nötig. Oder die JSON-Daten werden davor bereits in Objekte bzw Arrays der Klassen `Post` und `User` umgewandelt, sodass die Struktur deutlich weniger abstrakt ist und eher den ihnen bekannten Schemata entspricht. Auch Debugger und Objektinspektoren können dann sinnvoller eingesetzt werden. Das Datenformat JSON zur Übertragung von Daten eines Webservers an einen Client ist dann für die SchülerInnen unsichtbar. Zu beachten ist auch hier, dass JSON den SchülerInnen eine didaktische Rampe ermöglicht, da sie mit den selben bereitgestellten Methoden auch von einer Vielzahl anderer offener Web-APIs Daten abrufen können. Dadurch wird ermöglicht, Social Bots zu programmieren, die aktuelle Wetterdaten verarbeiten oder Zeitungsartikel abrufen.

4.2.2. Bildungsstandards

Wie in 3.3 erwähnt, lassen sich alle Bildungsstandards mit Social Bots anschneiden, in den drei geplanten Stunden werden folgende Bereiche abgedeckt:

Prozessbereiche

- Modellieren und Implementieren: Die SchülerInnen implementieren eigenständig einen Social Bot.
- Strukturieren und Vernetzen: Die SchülerInnen analysieren die Interaktionen auf der Webseite.

Inhaltsbereiche

- Information und Daten: Die SchülerInnen verarbeiten JSON-Daten und entwickeln Bots, die aufgrund dieser Daten unterschiedliche Nachrichten entwerfen.
- Informatiksysteme: Die SchülerInnen erschließen sich den Programmablauf von Social Bots. Die SchülerInnen kommunizieren mit einer bereitgestellten API.
- Informatik, Mensch und Gesellschaft: Die SchülerInnen werden für die Problematik von Social Bots im medialen Alltag sensibilisiert.

4.3. Ziele

Die Lernziele unterteilen sich in übergeordnete Hauptlernziele und die feineren Teilernziele. Zusätzlich wurden noch optionale Lernziele definiert, die für fortgeschrittene oder besonders interessierte SchülerInnen gedacht sind.

4.3.1. Hauptlernziele

1. Die SchülerInnen können die Aktivitäten von Social Bots in sozialen Netzwerken benennen.

(Posts automatisch liken oder teilen, Vorgefertigte Beiträge schreiben, Beiträge aus anderen Posts erstellen)
2. Die SchülerInnen können Gründe für die Verwendung von Social Bots angeben.
3. Die SchülerInnen vertiefen die Kenntnisse über Kommunikation in Rechnernetzen, indem sie einen eigenen Social Bot programmieren, der mit einem Server eines sozialen Netzwerkes kommuniziert.

4.3.2. Teillernziele

1. Die SchülerInnen können aus den Interaktionsmöglichkeiten einer Webseite ableiten, welche Aktivitäten ein Bot dort ausführen könnte.
2. Die SchülerInnen können einen als Pseudocode geplanten Bot in Java umsetzen.
3. Die SchülerInnen verwenden *GET*-Anfragen, um von einem Webserver Daten abzurufen
4. Die SchülerInnen verwenden *POST*-Anfragen, um Daten zur Verarbeitung an den Server zu schicken
5. Die SchülerInnen können den Unterschied dieser Anfragearten erklären.
6. Die SchülerInnen können einen Bot mit einer eigenen kreativen Idee implementieren, die ihn von den anderen Bots unterscheiden.

4.3.3. Optionale Lernziele

Den SchülerInnen, die sich mit der Thematik intensiver auseinandersetzen wollen, sollen in den Unterrichtsstunden noch weitere Lernerfahrungen ermöglicht werden. Diese „Rampe“ ist in den optionalen Lernzielen formuliert:

1. Die SchülerInnen beschreiben die normale Browsernutzung durch *GET*- und *POST*-Anfragen und erkennen so Schnittstellen in Webseiten.
2. Die SchülerInnen können sich selbständig in die API eines anderen Webdienstes einarbeiten und diesen in eigene Anwendungen einbinden.

4.4. Medien

Der wichtigste Punkt bei der Untersuchung des Entscheidungsfelds Medien in dieser Unterrichtsstunde war die Wahl des sozialen Netzwerkes und der Programmierschnittstelle. Weitere Überlegungen betrafen die Form der Hilfestellungen und die Medien zum motivierenden Unterrichtseinstieg.

4.4.1. Unterrichtseinstieg

Für einen motivierenden Unterrichtseinstieg ist das Medium so zu wählen, dass SchülerInnen sich selbst Gedanken machen können und Interesse an dem Thema geregt wird. Dafür wurde eine Zusammenstellung aus Überschriften mehrerer Zeitungsartikel gewählt, die das Thema Social Bots von verschiedenen Seiten beleuchten. Durch bekannte Quellen wie dem BR oder dem Deutschen Bundestag wird den SchülerInnen auch die Relevanz des Themas bewusst. Die erstellte Folie ist in Abbildung 4.2 zu sehen.



Abbildung 4.2.: Folie mit Überschriften zu Social Bots für den Unterrichtseinstieg. Mehr Details siehe 4.8

Da den meisten SchülerInnen das Thema Social Bots nicht bekannt ist, wurde des Weiteren für eine erste Informationsphase ein Video gewählt, da dort auf ansprechende Weise viele Informationen in kurzer Zeit vermittelt werden können. Außerdem ist das Video im Internet verfügbar, sodass SchülerInnen auch später noch einmal darauf zugreifen können. Da einige Videos zur Auswahl standen, wurden für die Wahl folgende Kriterien berücksichtigt:

- Das Thema wird in einem angemessenen Umfang (unter 5 Minuten) erklärt.
- Die Erklärung ist technisch korrekt, aber verständlich (nach eigenem Ermessen).
- Das Video beinhaltet zumindest folgende für den Unterricht relevanten Punkte:
 - Kurze Definition des Begriffs Social Bot.
 - Welche Aktionen üben Social Bots in sozialen Netzwerken aus?
 - Welche Einflüsse haben Social Bots?
- Das Video ist optisch ansprechend gestaltet

Zwei der gefundenen Videos erfüllten diese Kriterien besonders gut: Ein Video von heuteplus des ZDFs [ZDF17] und eines von explain-it.tv [exp17]. Das erste war dabei etwa eine Minute kürzer und enthielt weniger für die Unterrichtseinheit überflüssige Informationen, da das zweite Video noch einiges zu Fake News miterzählte. Zudem wirkte das zweite Video eher für eine jüngere Zielgruppe (Unter- oder Mittelstufe) bestimmt. Da die Stunde letztlich in einer 12. Jahrgangsstufe gehalten wurde schien das erste Video [ZDF17] daher angemessener und wurde für die Stunde ausgewählt.

4.4.2. Soziales Netzwerk mit Programmierschnittstelle

Möchte man im Unterricht einen Social Bot programmieren, stellt sich zunächst die Frage, für welche Plattform die Bots entwickelt werden. Aus mehreren Gründen wurden in der hier vorgestellten Unterrichtseinheit nicht Bots für ein existierendes soziales Netzwerk erstellt, sondern ein eigenes, vereinfachtes Netzwerk („SocialBotNet“: www.socialbotnet.de) implementiert und für die Bots zur Verfügung gestellt. Im Folgenden sollen die Überlegungen, die hierfür ausschlaggebend waren dargestellt werden, sowie ein Überblick über die Funktionalitäten und Einschränkungen des bereitgestellten sozialen Netzwerks gegeben werden.

Probleme existenter Netzwerke

Zunächst gibt es ganz grundlegende moralische Probleme, die SchülerInnen einen Bot für ein verbreitetes soziales Netzwerk programmieren zu lassen: Zum einen ist dafür ein Account in dem sozialen Netzwerk nötig. Von SchülerInnen kann aus Datenschutz-Gründen nicht verlangt werden, dass sie einen Account auf Twitter, Facebook, oder Ähnlichem erstellen. Zum anderen ist das Betreiben von Social Bots zwar nicht illegal, jedoch verstoßen Bots leicht gegen die AGBs der sozialen Netzwerke. Das lässt sich möglicherweise auch verhindern, da die meisten Plattformen ihre API auch automatisierten Programmen öffnen, sodass beispielsweise Unternehmen einen Chatbot für den Kundensupport bereitstellen können. Gegen Falschaccounts wird jedoch dennoch schnell vorgegangen und die Gefahr, dass sich einzelne Programme dennoch nicht an die Richtlinien halten ist gegeben.

Neben diesen Aspekten gibt es technische Hindernisse, die in der Unterrichtseinheit stören würden: Um die API eines sozialen Netzwerks zu verwenden muss in der Regel zunächst eine App auf der entsprechenden Seite angemeldet werden. Dabei erhält man einen API-Schlüssel, der über eine gewisse Zeit ermöglicht, sich gegenüber der API zu authentifizieren. Diese Registrierung ist in der Regel zeitaufwändig und vermittelt den SchülerInnen keine wesentlichen Erkenntnisse. Eine Authentifizierung kann genauso gut durch Benutzername und Passwort erreicht werden, was den SchülerInnen bekannt

ist. Der Grund, warum normalerweise der Schlüssel notwendig ist, ist die zeitliche Begrenzung und Beschränkung des API-Zugangs auf angemeldete Anwendungen statt allen registrierten Accounts.

Funktionalitäten des SocialBotNet

Weboberfläche Das SocialBotNet ermöglicht einige Grundfunktionalitäten sozialer Netzwerke: Nutzer können sich mit einem Nutzernamen und Passwort registrieren und besitzen dann ein Profil, das mit „Über mich“ und „Hobbies“ zwei Bereiche für persönliche Informationen enthält. Des Weiteren kann man wie üblich Beiträge schreiben. Dabei gibt es zwei Möglichkeiten: Erstens befindet sich auf der Startseite ein Eingabefeld „Was denkst du gerade, `<username>`?“, in dem ein Beitrag in der Gesamtübersicht geschrieben werden kann (siehe Abbildung 4.3). Zweitens kann man auf dem Profil eines Nutzers im Eingabefeld „Was möchtest du `<pinwandname>` erzählen, `<username>`?“ an dessen Pinnwand schreiben. Auf der Pinnwand von User1 werden

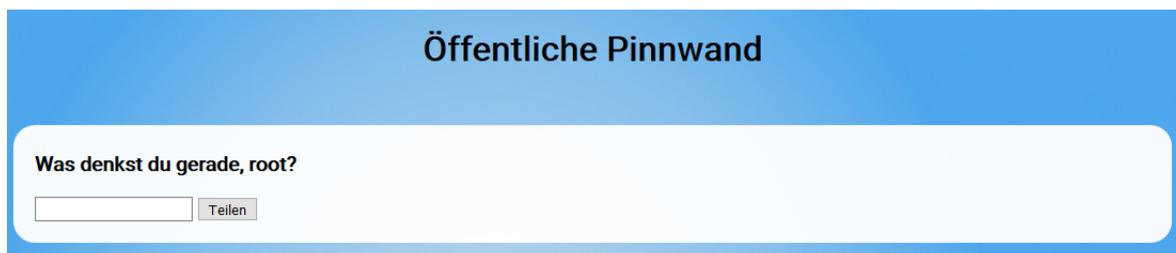


Abbildung 4.3.: Eingabefeld für angemeldete Nutzer auf der Startseite

dann die Beiträge von anderen Nutzern an User1 und die Beiträge von User1 an alle angezeigt. In der Gesamtübersicht sind alle Nachrichten des gesamten Netzwerks zu sehen. Dabei wurde absichtlich die Entscheidung getroffen dort auch Nachrichten von zwei Usern untereinander anzuzeigen, um Beiträgen eine höhere Sichtbarkeit zu geben. Beiträge können außerdem geliked werden und die Anzeigen der Beiträge lassen sich sowohl chronologisch als auch nach Likes sortieren. Damit nehmen Likes eine große Stellung in dem sozialen Netzwerk ein und bieten eine typische Angriffsfläche für Manipulationen durch Social Bots. Solche Mechanismen sollten den SchülerInnen in der Unterrichtseinheit ebenfalls aufgezeigt werden, um sie für Manipulationen in realen Netzwerken zu sensibilisieren. Zudem sind Likes positiv assoziiert, sodass das Sammeln von Likes mit einem Beitrag ihres Bots einen Motivationsfaktor ähnlich einem Tokensystem darstellt.

API Neben der Weboberfläche werden diese Funktionen mit Ausnahme der Registrierung auch über eine API bereitgestellt. Die folgende Tabelle 4.1 zeigt, welche Schnittstellen den SchülerInnen zur Verfügung stehen, und für welche Aktionen der Social Bots diese nötig sind.

| | | |
|--------------------------------|-------------|---|
| <i>/api/users</i> | <i>GET</i> | Liefert eine Übersicht über alle registrierten Nutzer, z.B. um Usern auf die Pinnwand zu schreiben, oder ihre Beiträge zu liken. |
| <i>/api/posts</i> | <i>GET</i> | Liefert die letzten 50 Posts des gesamten Netzwerks, z.B. um Posts zu analysieren und zu liken |
| <i>/api/pinnwand/:username</i> | <i>GET</i> | Liefert die Posts an der Pinnwand des genannten Nutzers (von anderen oder von ihm), z.B. um Posts eines Nutzers zu liken oder daraus eigene Nachrichten zu erstellen. |
| <i>/api/user/update</i> | <i>POST</i> | Ermöglicht automatisiertes Updaten der Profilinformationen wie „Hobbies“ und „Über mich“. |
| <i>/api/post</i> | <i>POST</i> | Ermöglicht automatisiertes Posten eines Beitrags. Dieser erscheint auf der eigenen Pinnwand und der allgemeinen Chronik. |
| <i>/api/post/:username</i> | <i>POST</i> | Ermöglicht automatisiertes Posten an die Pinnwand eines bestimmten Nutzers. |
| <i>/api/like</i> | <i>POST</i> | Ermöglicht automatisiertes Liken eines Posts. |
| <i>/api/unlike</i> | <i>POST</i> | Macht like rückgängig. |

Tabelle 4.1.: Schnittstellen für Programme im Netzwerk SocialBotNet

Eine Funktion, die hier im Vergleich zur Weboberfläche fehlt, ist die Registrierung. Dies ist bei den meisten sozialen Netzwerken der Fall, um automatisierte Registrierungen und somit massenhafte Bots zu verhindern. Da aber auch der Webbrowser nichts anderes macht, als *GET*- und *POST*-Anfragen zu senden, kann auch die Registrierung genau wie die anderen Schnittstellen angesprochen werden. In Tabelle 4.2, ist sie nochmal explizit angegeben.

| | | |
|----------------------|-------------|---|
| <i>/registrieren</i> | <i>POST</i> | Ermöglicht automatisiert Bots zu erstellen und so eine komplette Botarmee zu kontrollieren. |
|----------------------|-------------|---|

Tabelle 4.2.: „Unbeabsichtigte“ Schnittstellen im Netzwerk SocialBotNet

Diese inoffizielle Schnittstelle stellt eine Systemschwachstelle dar, wie sie von Bots bzw.

deren Entwicklern auch oft ausgenutzt werden. Sie soll die SchülerInnen auch dazu anregen, über Schutzmaßnahmen nachzudenken, die solche ungewollten Botschnittstellen verhindern. Ein bekanntes Beispiel für diesen Schutz ist *CAPTCHA*, bei dem ein bestimmtes Problem, wie z.B. Bilderkennung, gelöst werden muss und in den abgesendeten Daten dann enthalten sein muss. Andernfalls wird die Anfrage als ungültig verworfen.

Fehlermeldungen Häufige Fehler, die bei der Verwendung der API auftreten können, wurden antizipiert und aussagekräftige Fehlermeldungen als Hilfestellung zurückgegeben. Ein Beispiel ist die Verwendung der falschen Anfrageart: Sendet man z.B. an eine *POST*-Route eine *GET*-Anfrage, erhält man die Fehlermeldung „Falscher Anfragemodus. Erwartet wurde *GET*, erhalten wurde *POST*“. Zudem wird der korrekte HTTP-Statuscode ausgegeben, in diesem Fall ein Fehler 400 (Bad Request). Eine weitere Fehlermeldung ist, wenn bei *POST*-Anfragen keine Authentifizierungsdaten mitgeschickt werden: „Du bist nicht authentifiziert! Bitte schicke deinen Nutzernamen (username) und dein Passwort (password) mit.“ wird als 401 (Unauthorized) zurückgegeben. Ebenso erhält man eine Fehlermeldung, wenn der Nutzernamen und Passwort zwar im Request enthalten waren, aber nicht zu gespeicherten Anmeldedaten passen (401 (Unauthorized), „Login fehlgeschlagen. Falscher Nutzernamen oder falsches Passwort.“).

Unvorhergesehene Fehler werden als 500 (Internal Server Error) mit der Nachricht „Interner Fehler aufgetreten. Bitte melde das Problem!“ abgefangen.

Nicht implementierte Funktionen

Einige Möglichkeiten anderer sozialer Netzwerke wurden im SocialBotNet weggelassen. Zum Teil als didaktische Reduktion, um die SchülerInnen auf das Liken und Schreiben von Beiträgen zu fokussieren. Andere Features wurden allerdings nur aus Zeitgründen nicht mehr im Rahmen dieser Arbeit implementiert, würden aber sinnvolle Erweiterungen der Funktionen darstellen. Manche der folgenden Punkte bieten somit einen Anknüpfungspunkt für weitere Arbeit an dem Thema.

Eine typische Strukturierung in sozialen Netzwerken sind **Freundschaften** zwischen Nutzern. Sie ermöglichen den Nutzern die im Netzwerk befindlichen Informationen effektiv zu filtern. Im Gegensatz dazu sind im SocialBotNet alle Beiträge für alle sichtbar und abgesehen von Antworten existieren keine Beziehungen zwischen den einzelnen Nutzern. Der Vorteil davon ist, dass Bots alle Daten zur Verfügung haben und nicht erst ein Freundschaftsnetzwerk aufbauen müssen und gleichzeitig, dass die Beiträge der Bots direkt von allen gesehen werden können. Dadurch können auch Interaktionen der Bots der SchülerInnen untereinander leichter entstehen, was den motivationalen

Aspekt erhöht.

Stunden Freundschaften zur Verfügung, könnten andererseits noch andere Anwendungen der Social Bots implementiert werden, sodass vielleicht unterschiedlichere Bots möglich wären, als es in der geplanten Unterrichtsstunde der Fall war (siehe Kapitel 4.7). So könnte ein Bot auch nur eine möglichst große Reichweite aufbauen wollen und daher auf ein ansprechendes Profil setzen. Freundschaften könnten also eine interessante Erweiterung für das Netzwerk darstellen.

Ähnlich verhält es sich mit **Gruppen**: Auch diese Strukturierung hilft Nutzern nach für sie relevanten Informationen zu filtern. Gruppen bilden sich dabei oft aus tatsächlich bestehenden Gruppen – wie z.B. eine Klasse einer Schule – aber auch unter Unbekannten aus interessenbezogenen Punkten, wie gemeinsame Hobbies oder einfach nur wegen witzigen Beiträgen in der Gruppe. Gerade die interessenbezogenen Gruppen bieten Social Bots eine Angriffsfläche, da aus den Gruppenzugehörigkeiten einer Person geschlossen werden kann, für welche Beiträge sie besonders empfänglich ist. Eine sinnvolle Nutzung von Gruppenstrukturen in Anwendungen von Social Bots ist jedoch vermutlich ziemlich komplex, sodass diese Funktion nicht sehr fehlt.

Antworten auf Beiträge sind nicht komplett unterstützt. Zwar ist es möglich, dem Autor eines Kommentars an die Pinnwand zu schreiben, aber die Nachrichten hängen technisch nicht zusammen und werden nicht strukturiert angezeigt. Die Erweiterung bietet weitere Möglichkeiten für die Social Bots und eine bessere Übersicht auf der Webseite. Zu beachten ist jedoch auch, dass die Datenstruktur dadurch etwas komplizierter wird und die Anwendungen somit eher fortgeschritten sind.

Private Nachrichten zwischen zwei Nutzern sind ebenfalls nicht implementiert. Im Gegensatz zu Antworten auf Kommentare haben private Gespräche den Nachteil, dass Informationen nicht mehr für alle zugänglich sind. Das schränkt die Social Bots ein und ist für das Netzwerk nicht nötig.

Ein weiterer wichtiger Punkt ist die **Teilen/Retweet**-Funktionalität. Einerseits ist dies eine grundlegende Funktion in den richtigen sozialen Netzwerken, da so Inhalte weiterverbreitet werden können und der Ursprung nachvollziehbar bleibt. Andererseits gibt es einige Gründe, warum man Teilen im SocialBotNet nicht benötigt und es daher zur Reduktion der Komplexität besser weggelassen werden sollte:

- Die Beiträge sind für die Social Bots bereits zugänglich, Retweets stellen also keine Erweiterung der Daten dar.
- Motivationale Aspekte der Teilen-Funktion sind durch die Likes bereits abgedeckt. Es wäre nur eine weitere Zahl, die auf die gleiche Weise manipuliert werden kann wie Likes und in diesem Netzwerk auf die gleiche Weise für Sichtbarkeit sorgen würde.

- Geteilte Inhalte vervielfachen die Daten, die von den Social Bots durchsucht werden. Dadurch wird die Entwicklung komplexerer Bots erschwert, die Informationen aus den Beiträgen anderer Nutzer filtern und z.B. auf bestimmte Schlagwörter mit Liken oder Antworten reagieren.

Zuletzt sind noch die **Profilinformationen** zu nennen, die zwar in Grundzügen angelegt sind („Über mich“ und „Hobbies“, sowie ein automatisch aus dem Nutzernamen generiertes Profilbild), aber noch weitere Personalisierungen erlauben könnten. Insbesondere ein selbstgewähltes Profilbild ist in der Regel sehr beliebt. Mehr Möglichkeiten würde hier eventuell dazu führen, dass die Bots menschlicher gestaltet werden.

In Tabelle 4.3 sind die möglichen Erweiterungen nochmal übersichtlich zusammengefasst.

| Feature | nicht sinnvoll | wenig sinnvoll | neutral | sinnvoll | sehr sinnvoll |
|---------------------|----------------|----------------|---------|----------|---------------|
| Profilinformationen | | | | | X |
| Antworten | | | | | X |
| Freundschaften | | | | X | |
| Gruppen | | | X | | |
| Privatchat | X | | | | |
| Retweets | X | | | | |

Tabelle 4.3.: Übersicht über mögliche Erweiterungen des sozialen Netzwerks und Einschätzung des Mehrwerts. Sehr erwünscht wären Erweiterungen der Profilinformationen und Implementierung von Antworten auf Kommentare. Auch Freundschaften oder Gruppen könnten interessante Anwendungen ermöglichen, sind aber nicht dringend nötig. Retweets und Private Nachrichten stellen keine sinnvollen Zusätze dar.

4.4.3. Hilfestellungen zum Programmieren

Die Programmierung von Social Bots wird normalerweise eher in JavaScript oder Python durchgeführt, weil dort im Vergleich zu Java Netzwerkzugriffe einfacher zu implementieren sind und weil in den Sprachen JSON direkt verwendet und leichter verarbeitet werden kann. Für die geplante Unterrichtsstunde wurde dennoch Java verwendet, da diese Sprache den SchülerInnen bereits bekannt ist. Da in Java der Aufbau einer Netzwerkverbindung komplizierter ist, wird den SchülerInnen eine vorgefertigte Klasse **Netzwerkzugriff** bereitgestellt, die Methoden zum Verbindungsaufbau und Senden von *GET*- und *POST*-Anfragen bietet. Für eine Unterrichtsstunde, die weniger Wert auf die Netzwerkkommunikation legt, kann auch die Klasse **Netzwerkzugriff** angepasst werden: Statt den *GET*- und *POST*-Hilfsmethoden könnten bereits Methoden vorbereitet werden, die *posten* und *liken* in sozialen Netzwerken ermöglichen. Zudem könnten

die JSON Daten in Objekte umgewandelt werden (selbst programmiert oder mit Gson <https://github.com/google/gson>). Dadurch ist auch eine Verwendung mit weniger Programmiererfahrung möglich. Wie in der inhaltlichen Analyse (4.2) beschrieben, sind jedoch auch die informatischen Konzepte nicht mehr sichtbar.

Um eine Hilfestellung im Umgang mit diesen bereitgestellten Codeteilen zu bieten, wurde ein Übersichtsblatt entworfen, das zum einen die Struktur und Verarbeitung von *JSON*-Daten in Java erklärt und zum anderen die Benutzung für *GET*-/ *POST*-Anfragen erklärt. Das Arbeitsblatt findet sich in den Materialien 4.8. Es ist so konzipiert, dass Lernende sich selbständig das Wissen aneignen können und auch kleine Codebeispiele finden, um es direkt auszuprobieren. Die Einführung zu *JSON* könnte allerdings einigen SchülerInnen Probleme bereiten und wurde daher in der gehaltenen Stunde mit einer Gruppe lehrerzentriert vermittelt.

4.5. Methodische Analyse

Wie in Kapitel 4.4.1 beschrieben, wurde für den Einstieg ein Video gewählt, um schnell viele Informationen vermitteln zu können. Falls sich die SchülerInnen schon mal bewusst mit Social Bots auseinandergesetzt haben, ist auch ein Einstieg in Form eines Klassengesprächs gut geeignet. Darin können zum Beispiel Erfahrungen der SchülerInnen mit automatisierten Programmen auf sozialen Medien erfragt und Vorwissen zu Bots reaktiviert werden.

Der Programmieranteil orientiert sich an dem Konzept der Binnendifferenzierung, um dem unterschiedlichen Lernstand der SchülerInnen gerecht zu werden. So ist gewährleistet, dass schwächere SchülerInnen Erfolge erfahren und stärkere trotzdem nicht unterfordert sind. Dabei können die SchülerInnen alleine oder in Partnerarbeit nach der Methode „Pairprogramming“ arbeiten. Beim Pairprogramming übernimmt ein Lernender die Rolle des *Drivers*, der versucht die aktuelle Aufgabe zu programmieren, dabei laut denkt und seine Implementierung erklärt. Der andere ist der *Navigator*, der die Übersicht über die Gesamtstruktur hat, den Code kontrolliert und Feedback gibt. Diese Rollen werden regelmäßig gewechselt.

Vorteilhaft an der Methode ist, dass beide SchülerInnen mitarbeiten und der Code meist besser verständlich ist als bei Einzelarbeit. Insbesondere bei schwächeren SchülerInnen kann die Methode auch Frustrationen vorbeugen, da Fehler vom Navigator leichter gesehen werden, als wenn man selbst programmiert. Auch der Phasenwechsel zwischen Driver und Navigator ist in der Unterrichtseinheit leicht zu integrieren, da der Bot iterativ weiterentwickelt wird.

Ein Nachteil ist, dass die Methode zunächst ausführlich eingeführt werden muss, um gut zu funktionieren. Ein spontaner Einsatz ist daher nicht sinnvoll und der erste Einsatz kostet Unterrichtszeit. Außerdem ist wichtig, wie die Paare eingeteilt werden: Werden

leistungsstärkere mit -schwächeren SchülerInnen kombiniert, ist die Gefahr, dass nur der gute arbeitet, wenn die Regeln nicht genau eingehalten werden. Es bietet allerdings möglicherweise auch einen großen Wissenszuwachs für schwächere SchülerInnen, wenn die Methode richtig umgesetzt wird. Eine leistungshomogene Einteilung in Paare ist meistens einfacher.

Die SchülerInnen in größeren Gruppen arbeiten zu lassen wird nicht empfohlen, da dies der Binnendifferenzierung entgegen stehen würde. Die Gefahr besteht, dass die stärkeren SchülerInnen die Arbeit übernehmen und schwächere im Entdeckungsprozess gehindert werden.

Um den Einstieg zu erleichtern wird bereits vorgefertigter Code zur Verfügung gestellt, sodass die SchülerInnen nur noch den konzeptuellen Unterschied zwischen *GET*- und *POST*-Anfragen verstehen müssen, statt die konkrete Implementierung von Netzwerkzugriffen in Java. Sollen die SchülerInnen tiefer in den technischen Hintergrund einsteigen, wäre es auch möglich einzelne Zeilen aus der Vorlage noch wegzulassen und die SchülerInnen ergänzen zu lassen. Ein Vorteil davon wäre, dass die SchülerInnen eine tiefere Schicht des OSI-Modells sehen und so den Lehrplaninhalt noch mehr vertiefen. Ein Nachteil ist, dass dadurch die Programmierung noch abstrakter und somit für schwächere SchülerInnen nochmal schwieriger wird. Des Weiteren bleibt weniger Zeit für die Programmierung des Bots übrig, was womöglich das Erfolgserlebnis mancher SchülerInnen weiter beeinträchtigt. In der gehaltenen Unterrichtsstunde wurde daher auf diese Komplexität verzichtet.

Für die Unterrichtseinheit ist außerdem das Prinzip „Trennung von Theorie und Praxis“ wichtig. Die SchülerInnen sollten sich zunächst konzeptionell mit Social Bots befassen und planen, wie die Bots sich im Netzwerk verhalten. Dadurch wird ein informatives Verständnis geschaffen, das unabhängig von der konkreten Implementierung des Bots ist. Durch Pseudocode kann das Verständnis strukturiert festgehalten werden. Dies liefert einen Übergang in die konkrete Implementierung, in der dann die technische Fertigkeit, die Planung umzusetzen, gefordert ist. Die Lehrkraft kann so ebenfalls die Programmierfähigkeit der SchülerInnen getrennt vom konzeptionellen Verständnis unterstützen.

4.6. Geplanter Stundenverlauf

Die Unterrichtseinheit zum Programmieren eines Social Bots umfasst insgesamt 3 Schulstunden.

In der ersten Schulstunde wird mit den SchülerInnen erarbeitet, was ein Social Bot ist und was dieser in einem sozialen Netzwerk macht. Anhand konkreter Ideen der SchülerInnen wird ein Konzept entwickelt, wie ein Programm für einen Social Bot abläuft und

welche Informationen dafür von dem sozialen Netzwerk bereitgestellt werden müssen. Aufbauend auf diesen Überlegungen entwickeln die SchülerInnen in den folgenden zwei Stunden einen eigenen Social Bot.

Die zweite und dritte Schulstunde enthält eine starke Binnendifferenzierung, da den SchülerInnen ermöglicht wird einfache Bots zu schreiben und sie iterativ immer komplexer und umfangreicher zu machen. Durch ein bereitgestelltes soziales Netzwerk können die Bots direkt getestet werden. Die Lehrkraft unterstützt dabei den Prozess durch Hilfestellungen, welche der Aufgaben für einen Social Bot leichter umzusetzen sind, und welche schwieriger sind und daher erst aufbauend auf den Grundfunktionen implementiert werden sollten. Mögliche Funktionalitäten der Social Bots sind

- Posten vorgefertigter Texte auf der eigenen Pinnwand. (*einfach*)
- Liken aller Beiträge auf der eigenen Pinnwand. (*einfach*)
- Posten von aus mehreren Optionen zusammengesetzten Texten. ¹ (*mittel*)
- Posts nach Schlüsselwörtern durchsuchen und dann liken. (*anspruchsvoll*)
- Userprofile nach Schlüsselwörtern durchsuchen und dann vorgefertigte Texte schreiben (*anspruchsvoll*)

Weitere Anwendungen über die Stundeninhalte hinaus (Rampe) sind:

- Automatisiertes Erstellen von Bots (*Implementierung einfach, herausfinden dass das möglich ist aber sehr anspruchsvoll*)
- Abrufen von Nachrichten, Wetterdaten, o. Ä. aus API eines anderen Servers und teilen dieser Nachrichten. *Je nach Dienst anspruchsvoll bis komplex*

4.6.1. Ablauf der Stunde 1: Einstieg zu Social Bots

Ausrichten und Reaktivieren (ca. 5 Minuten) Den SchülerInnen wird mit verschiedenen Zeitungsüberschriften, die auf einer Präsentationsfolie (siehe Materialien in Kapitel 4.8) gezeigt sind, ein direkter Einstieg in die Thematik der Social Bots gegeben. Motivierend ist für die SchülerInnen insbesondere die Aktualität des Themas, die durch die Ausschnitte ebenfalls deutlich wird. Durch ein Lehrer-Schüler-Gespräch über deren Begegnung mit Berichterstattungen über Social Bots und persönliche Erfahrungen mit Bots in sozialen Netzwerken wird das Vorwissen der SchülerInnen weiter reaktiviert.

¹Mit wenigen Bausteinen können bereits sehr viele Sätze gebildet werden, wie z.B. buzzomat.de eindrucklich zeigt

Informierender Einstieg (ca. 5 Minuten) Ein Video zu Social Bots [ZDF17] bietet den SchülerInnen einen ansprechenden Einstieg und einen groben Überblick über das Thema. Die wichtigsten Punkte werden anschließend von den SchülerInnen zusammengefasst und an der Tafel festgehalten. Enthalten sein sollten folgende Punkte:

Tafelanschrieb: Social Bots

Social Bots sind Programme, die

- in sozialen Netzwerken agieren
- menschlich wirken
- Meinungen durch gezielte Posts oder massenhafte Likes beeinflussen

Erarbeitungsphase (10-15 Minuten) Die SchülerInnen greifen auf das SocialBotNet (www.socialbotnet.de) zu und überlegen sich alleine oder mit SitznachbarInnen, welche Aktivitäten ein Social Bot in diesem Netzwerk ausüben könnte (siehe die Liste in Abschnitt 4.6 oben). Ihre Überlegungen halten sie schriftlich fest.

Präsentation (5 Minuten) Die SchülerInnen beschreiben das Netzwerk und stellen die Möglichkeiten zur Manipulation mit Social Bots vor.

Verarbeitung (ca. 10 Minuten) Im Klassengespräch wird ausgehend von den Ideen der SchülerInnen ein beispielhafter Programmablauf für einen Social Bot konzipiert. Dabei wird besonderes Augenmerk auf die Kommunikation zwischen dem Bot und dem sozialen Netzwerk gelegt. Ein mögliches Ergebnis davon ist in

Netzwerkverbindung zu SocialBotNet aufbauen ;

Anfrage an Netzwerk: Posts an der eigenen Pinnwand abrufen ;

Wiederhole für alle *Posts der Antwort*

| Speichere *id* aus den Postsdaten Senden an Netzwerk: Post mit der ID *id* liken

Ende

Algorithmus 1: Pseudocode für Botaktivität (Beispiel)

Abschluss (ca. 5 Minuten) (*entfällt in geplanter Stunde, da 1. und 2. als Doppelstunde gehalten werden*) Die Lehrkraft gibt einen Ausblick auf die nächsten Stunden und gibt als Hausaufgabe auf, den Abschnitt zum JSON-Format auf dem Übersichtsblatt durchzulesen.

4.6.2. Ablauf der Stunden 2 und 3: Programmieren eines Social Bots

Vorbereitung Die Lehrkraft stellt ein Projekt zur Verfügung, in dem bereits Grundfunktionen zur Kommunikation mit Webservern implementiert sind. Dazu gehören insbesondere Methoden, die *GET*- und *POST*-Anfragen schicken können, sowie die Verarbeitung der JSON-Rückgaben zu Datenobjekten. Die SchülerInnen können diese Funktionen für ihren Social Bot verwenden. Wie die Methoden verwendet werden wird den SchülerInnen auf einem übersichtlichen Blatt zusammen mit den offiziellen Schnittstellen des Netzwerks (siehe Materialien 4.8) ausgeteilt.

Projekt: Programmieren eines Social Bots (ca. 70 Minuten) Die SchülerInnen erhalten den Arbeitsauftrag, einen eigenen Social Bot zu implementieren, der im SocialBotNet positive Kommentare über das (erfundene) Streaming Portal „iStream.com“ liket und postet. Dabei müssen die Mindestanforderungen in Arbeitsauftrag 4.6.2 erfüllt werden:

Arbeitsauftrag 4.1: Mindestanforderungen für den Social Bot

Der Bot soll automatisiert mindestens

- einen Beitrag schreiben
- einen Beitrag liken
- eine weitere Aktion ausführen.

Sie fangen mit einem einfachen Bot an und lernen so die *GET*- und *POST*-Anfragen richtig einzusetzen. Iterativ können anschließend immer komplexere Bots programmiert werden. Dabei können die SchülerInnen ihren Bot ständig direkt im SocialBotNet testen und sehen dort ebenfalls, was andere Bots gerade machen. Dadurch erhalten Sie weitere Anregungen für ihren eigenen Bot und erfahren außerdem eine Wirksamkeit, da ihre Arbeit sichtbar ist.

Zur Differenzierung bietet die Lehrkraft den SchülerInnen an, mit einer Gruppe zusammen den ersten Bot zu erstellen. So können die notwendigen Grundlagen wie z.B. das JSON-Format und die Programmierung von *GET*- und *POST*-Anfragen unter didaktischer Leitung erlernt werden. Stärkere SchülerInnen können mit dem Bot auch direkt selbst anfangen und als Hilfestellung das ausgeteilte Übersichtsblatt verwenden.

Präsentation der Bots (10-15 Minuten) Die Lehrkraft gibt SchülerInnen die Möglichkeit ihre Bots vor der Klasse vorzuführen und bei besonderen Funktionen einen Einblick in wichtige Programmteile zu geben.

Abschluss (ca. 3 Minuten) Abschließend fassen die SchülerInnen ihre wichtigsten in der Stunde gewonnenen Erkenntnisse mündlich noch mal zusammen und reflektieren so die Stunde. Gezielte Nachfragen durch die Lehrkraft überprüfen stichprobenartig die Erfüllung der Lernziele.

Abseits vom Schulunterricht können die SchülerInnen natürlich ihre Bots weiter ausarbeiten und die Lehrkraft bietet an, Feedback für den Quellcode zu geben und für Rückfragen erreichbar zu sein. In der durchgeführten Stunde wurde dafür eine Abgabe auf Mebis eingerichtet.

4.7. Reflexion

Im Folgenden soll die Unterrichtseinheit reflektiert werden, die am 12. und 13. Dezember 2017 nach dem vorgestellten Konzept in der 12. Jahrgangsstufe am Gymnasium Ottobrunn gehalten wurde. Die Unterrichtsstunden waren in eine Doppelstunde am Dienstag den 12.12. und eine Einzelstunde am Mittwoch den 13.12. aufgeteilt. Im Computerraum stand für alle SchülerInnen ein eigener Computer zur Verfügung, die U-förmig am Rand des Raumes angeordnet waren. In der Mitte standen Tische für Arbeiten ohne PCs zur Verfügung, wodurch eine Trennung der Theorie und Praxis auch räumlich unterstützt wurde. Am Dienstag waren nur 14 der eigentlich 21 SchülerInnen anwesend, vermutlich wegen der anstrengenden Deutschklausur, die am gleichen Tag in den vier vorangegangenen Stunden geschrieben wurde. Am Mittwoch waren es 19 SchülerInnen.

Der Einstieg war für die SchülerInnen sehr motivierend, insbesondere die Aussicht, einen solchen Bot selbst zu programmieren, war für einige ein Motivationsfaktor. So konnten die SchülerInnen trotz der anstrengenden Klausur für den weiteren Unterrichtsverlauf interessiert werden.

Das Ausprobieren des SocialBotNets, um Interaktionsmöglichkeiten für Social Bots zu analysieren, war wegen Internetproblemen schwierig. Die Seite lud sehr langsam, wodurch nur wenige Funktionalitäten des Netzwerks ausprobiert werden konnten. Dies senkte zudem die Motivation der SchülerInnen. Das Problem ergab sich verstärkt auch beim Programmieren: Von den per LAN angeschlossenen PCs ließ sich über Java keine Verbindung ins Internet aufbauen. Dieses Problem trat wegen den Netzwerkeinstellungen der Schule auf, da die Java-Methoden die Proxy-Authentifizierung nicht berücksichtigten und Anfragen somit vom Proxy abgelehnt wurden. Über das schulische „Bring your own device“-WLAN war der Zugriff möglich, sodass auf 3 Laptops umgestiegen wurde, die die SchülerInnen dabei hatten. Zudem hat eine Gruppe mit der Lehrkraft zentriert einen Bot programmiert hat. Insgesamt hat die Stunde sehr darunter gelitten, dass keine vernünftige Verbindung aufgebaut werden konnte, daher

sollte dies vor dem Einsatz im Unterricht unbedingt an der jeweiligen Schule ausprobiert werden. Eine Möglichkeit das Problem zu beheben, ist die Systemeinstellungen für die Proxy-Authentifizierung zu übernehmen. Dazu muss beim Ausführen die System Einstellung `java.net.useSystemProxies` auf `true` gesetzt werden. Wie das funktioniert ist im Anhang B.2 für einzelne Entwicklungsumgebungen genauer ausgeführt.

Für Mittwoch wurden die SchülerInnen gebeten einen Laptop mitzubringen, wodurch in dieser Stunde wie geplant verschiedene Bots programmiert werden konnten. Wegen der Zeitknappheit wurde der Unterrichtsablauf etwas umgeplant: Damit die SchülerInnen möglichst viel Zeit für die Entwicklung ihres Bots haben, wurde die Präsentation der Programme weggelassen und die Zeit in die Programmierung eingeplant. Durch die Binnendifferenzierung war es leicht möglich einzelne SchülerInnen gezielt zu unterstützen, was insbesondere wegen den 5 SchülerInnen wichtig war, die in den ersten Stunden gefehlt hatten. Auch konnten schnelleren SchülerInnen weitere Anregungen für herausfordernde Aufgaben gestellt werden.

Einem Schüler gelang es auch, den Registrierungsprozess zu automatisieren, wie im Netzwerk beabsichtigt aber den SchülerInnen nicht offen gezeigt. Statt der einfachen *POST*-Anfrage auf die `/registrieren` Route, verwendete er eigenständig Jsoup, einen HTML-Parser, um so das Formular der Website zu befüllen und abzuschicken. Dies zeigt auch, dass durch die Unterrichtseinheit eine Rampe gegeben ist.

Interessant für die Analyse, wie erfolgreich die Stunden waren, ist auch die Bereitschaft der SchülerInnen über die Schule hinaus an den Bots weiterzuarbeiten. Während über Mebis keine Abgabe von SchülerInnen einging, zeigte sich an dem Netzwerk noch länger Aktivitäten: Bereits am Dienstag Abend hat einE SchülerIn noch einen Bot programmiert, der mit sehr fortgeschrittenen JSON Verarbeitungen allen Nutzern, die eine Nachricht mit „Netflix“ geschrieben haben, an die Pinnwand „Netflix ist doch voll out“ postete (siehe Abbildung 4.4). Am Mittwoch kam es etwa 1h nach Stundenende zu einer massiven Anfragenflut. Diese wurde durch eine Botarmee ausgelöst, die einen Instagramaccount bewirbt (siehe Abbildung 4.5). Ein Tag nach den Unterrichtseinheiten wurden in der Datenbank 15000 Einträge gemacht (Registrierungen, Likes, Posts), wodurch die Obergrenze des kostenlosen Servers überschritten wurde und daher alle INSERT-Funktionalitäten deaktiviert wurden. Ein kleineres Botnetzwerk zeigte dabei eine neue Funktionalität, nämlich die Erzeugung von Personennamen, wie in Abbildung 4.6 in den Benutzernamen zu sehen ist. Wie die Namen erzeugt wurden kann leider aufgrund der fehlenden Abgabe nicht festgestellt werden, somit kann nicht überprüft werden, ob diese Daten ebenfalls über eine Webschnittstelle wie von `fakenamegenerator.com` abgerufen wurden und so das API Konzept übertragen wurde.

Interessant wäre, ob die Komplexität der Bots gestiegen wäre, wenn das Netzwerk noch länger erreichbar gewesen wäre. Die Bots wirken noch immer nicht menschlich, an den



Abbildung 4.4.: Programm nach den ersten zwei Stunden, das zuhause weiterprogrammiert wurde

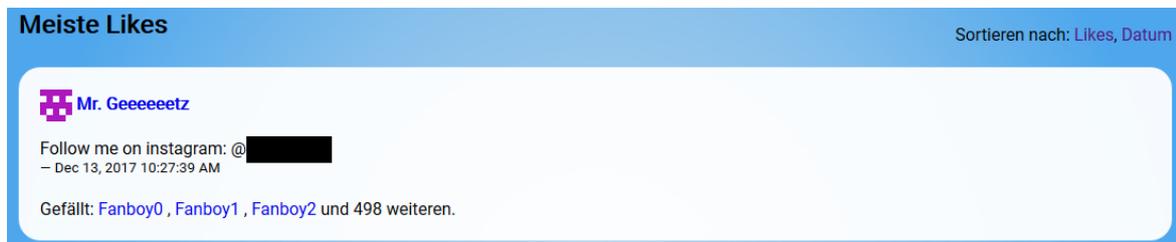


Abbildung 4.5.: Programm nach den drei Stunden. Botarmee bewirbt einen Instagram-account

Profilen, Nutzernamen und Postingverhalten wären also noch Verbesserungen möglich. Auch die Verarbeitung von GET-Anfragen, um gezielt User anzusprechen, bietet noch weitere Möglichkeiten.

Etwas enttäuschend war, dass die Bots, die im Unterricht programmiert wurden kaum Variation zeigten, was zum einen mit Sicherheit an der fehlenden Zeit lag, allerdings lassen sich weitere mögliche Ursachen identifizieren: Wie in Kapitel 4.4.2 dargestellt, ist es möglich, dass weitere Funktionen des sozialen Netzwerks den SchülerInnen mehr Anreiz für andere Anwendungen geboten hätte. Insbesondere haben die SchülerInnen die Profile der Bots nicht ausgestaltet und es wurde keine einzige Anfrage auf



Abbildung 4.6.: Programm ein Tag nach den Unterrichtseinheiten. Die Bot-Registrierung wurde um menschlichere Namen erweitert.

die `/user/update` Route verzeichnet. Hier ist also noch Handlungsbedarf nötig. Des Weiteren wäre möglich, dass sich die SchülerInnen durch die gestellten Mindestanforderungen haben einschränken lassen. Ist dies der Fall, kann auf mehrere Arten damit umgegangen werden: Man könnte die Mindestanforderungen komplett weglassen, da vorher bereits mögliche Einsätze von Social Bots im Netzwerk besprochen wurden, werden sie vermutlich eh automatisch abgedeckt. Meiner Meinung nach ist jedoch eine klare Vorstellung von den Anforderungen wichtig, um Orientierung zu geben und insbesondere schwächeren SchülerInnen ein klares Ziel zu geben, auf das sie hinarbeiten können.

Eine andere Möglichkeit wäre, die Mindestanforderungen breiter zu formulieren und mehr Variation dort bereits zu integrieren, sodass die SchülerInnen mehr Anregungen bekommen. Dies könnte jedoch auch noch wahrscheinlicher die Kreativität der SchülerInnen einschränken, da der Eindruck entsteht, dass dies bereits alle Anwendungsmöglichkeiten sind. Es kämen dann zwar unterschiedlichere Bots heraus, jedoch wieder nur Funktionen, die in den Mindestanforderungen beschrieben waren.

Die geringste, aber meiner Meinung nach sinnvollste Änderung wäre, den dritten Punkt der weiteren selbstüberlegten Funktion stärker zu betonen und explizit Kreativität der SchülerInnen zu fordern. Dies erhöht auch die beabsichtigte Transparenz, da nicht nur klar ist, welche Funktionen auf jeden Fall erfüllt sein müssen, sondern auch wie wichtig diese jeweils der Lehrkraft sind.

Möchte man den Programmiereteil noch attraktiver machen, wäre es auch möglich Bots vorzubereiten, die auf bestimmte Aktionen der Bots der SchülerInnen reagieren. Beispielsweise könnte man einen Bot starten, der Beiträge zu dem Stundenthema schreibt und Antworten, die er an seiner Pinnwand bekommt, liket. Ein anderer Bot könnte ausgefüllte Profile suchen und diesen schreiben. Die SchülerInnen können dann beim Programmieren versuchen, mit ihrem Bot möglichst viele unterschiedliche Bots der Lehrkraft zu „sammeln“. Grundsätzlich ist das Programmieren bereits motivierend genug, daher ist die Umsetzung dieser Idee auch nicht unbedingt nötig.

Zusammenfassend lässt sich positiv hervorheben, dass einzelne SchülerInnen auch über die reine Unterrichtszeit hinaus noch Interesse an dem Thema zeigten, was für den Erfolg der Stunden spricht. Wegen den Netzwerkproblemen waren die Ergebnisse am Ende der Unterrichtseinheit jedoch noch nicht so weit entwickelt wie gedacht. SchülerInnen, die nur die Unterrichtszeit daran gearbeitet haben, hatten daher auch nicht die gewünschte Wirksamkeitserfahrung, da ihr Bot nicht so viel im Netzwerk beitragen konnte.

4.8. Materialien

Ausrichtung Die unten abgebildete Folie wurde als Einstieg verwendet. Sie zeigt die Schlagzeilen der folgenden Artikel

- „Soziale Medien: Social Bots können kleine Gruppen wie eine Bewegung aussehen lassen“ von Zeit Online ²
- „Manipulation durch Social Bots: Wie Meinungsmache im Internet funktioniert“ vom Bayerischen Rundfunk ³
- „Wirkung von ‚Social Bots‘ ist unter Sachverständigen strittig“ vom Deutschen Bundestag ⁴
- „Thesenpapier attestiert Social Bots weitreichendes Gefahrenpotenzial“ von netzpolitik.org ⁵

"Social Bots können kleine Gruppen wie eine Bewegung aussehen lassen"

Manipulation durch Social Bots

Wie Meinungsmache im Internet funktioniert
- BR, 26.10.2016

- Zeit Online, 22.09.2017

Wirkung von „Social Bots“ ist unter Sachverständigen strittig

- Deutscher Bundestag,
02.02.2017

Thesenpapier attestiert Social Bots weitreichendes Gefahrenpotential

- Netzpolitik.org, 27.01.2017

Handout Als Übersicht über die Programmierschnittstelle der Webseite und über die Benutzung der bereitgestellten Codebasis diente den SchülerInnen folgendes Handout

²<http://www.zeit.de/digital/internet/2017-09/soziale-medien-bundestagswahl-manipulation-social-bots-trolle>

³<https://www.br.de/nachrichten/social-bot-erklaerstueck-100.html>

⁴<https://www.bundestag.de/dokumente/textarchiv/2017/kw04-pa-bildung-forschung-social-bots/488818>

⁵<https://netzpolitik.org/2017/thesenpapier-zur-gesellschaftlichen-und-politischen-relevanz-von-social-bots-vorgestellt/>

JSON-Format

JSON ist ein Übertragungsformat für Daten, die sich leicht mit dem PC verarbeiten lassen sollen. Dabei gibt es Objekte mit Key-Value Paaren und Arrays von Objekten.

Objekte:

```
{
  "key": "value",
  "key2": 42,
  "key3": true,
  ...
}
```

Arrays:

```
[
  {
    "key": "objekt1",
  },
  {
    "key": "objekt2"
  },
  ...
]
```

Als Values in den Objekten sind zugelassen: Zahlen, Booleanwerte, Strings, oder ein weiteres Objekt oder sogar ein Array. Somit lassen sich die Objekte auch schachteln.

JSON lässt sich in Java mit folgenden Methoden verarbeiten:

- Relevante Methoden von JSONArray: `getJSONObject(int index)`
- Relevante Methoden von JSONObject: `getInt(String key)`, `getBoolean(String key)`, `getString(String key)`, `getJSONObject(String key)`, `getJSONArray(String key)`

Beispiel:

```
//Erstellt aus dem String ein JSONArray
JSONArray array = new JSONArray("[{ \"id\": 1 }]");

//Mit getJSONObject(int index) kann man auf die Objekte im Array zugreifen
JSONObject obj = array.getJSONObject(0);

//Mit getInt(String key) kann man für einen Key den Value auslesen.
int zahl = obj.getInt("id");
```

Programmierschnittstellen im Web

Webseiten bieten Programmierern oft Schnittstellen, sogenannte *APIs*. An diese Schnittstellen können Programme Anfragen stellen. Dabei gibt es zwei wichtige Arten:

- **GET-Anfragen**, um Informationen vom Server **abzufragen**
- **POST-Anfragen**, um dem Server Informationen zum Verarbeiten zu **senden**.

In unserem Projekt können GET-Anfragen mit Objekten der Klasse `NetzwerkZugriff` durch die Methode `GETAnfrageSenden(String route)` gesendet werden. Z.B.

```
NetzwerkZugriff socialbotnet = new NetzwerkZugriff("https://social-bot-net.herokuapp.com");
String antwort = socialbotnet.GETAnfrageSenden("/api/users");
```

POST-Anfragen benötigen Daten, die an das Netzwerk geschickt werden müssen. In unserem Projekt können *POST*-Anfragen mit Objekten der Klasse NetzwerkZugriff durch die Methode `POSTAnfrageVorbereiten(String parameter, String wert)` vorbereitet und mit `POSTAnfrageSenden(String route)` abgeschickt werden. Z.B:

```
NetzwerkZugriff socialbotnet = new NetzwerkZugriff("https://social-bot-net.herokuapp.com");
socialbotnetZugriff.POSTAnfrageVorbereiten("username", "BOT");
socialbotnetZugriff.POSTAnfrageVorbereiten("password", "secure");
socialbotnetZugriff.POSTAnfrageVorbereiten("message", "Hallo!");
socialbotnetZugriff.POSTAnfrageSenden("/api/post");
```

Die folgenden Schnittstellen bietet die Webseite:

| | | |
|--|-------------|---|
| <i>/api/users</i> | <i>GET</i> | Liefert eine Übersicht über alle registrierten Nutzer |
| <i>/api/posts</i> Optionale Parameter: <i>sortBy</i> , <i>limit</i> | <i>GET</i> | Liefert die letzten 50 Posts des gesamten Netzwerks <i>sortBy=likes</i> nach Likes sortiert, <i>sortBy=time</i> nach Datum sortiert. Limit beschränkt die Anzahl, z.B. <i>limit=1</i> für nur einen Post |
| <i>/api/pinnwand/:username</i> Optionale Parameter: <i>sortBy</i> , <i>limit</i> | <i>GET</i> | Liefert die Posts an der Pinnwand des genannten Nutzers <i>sortBy=likes</i> , <i>sortBy=time</i> , <i>limit=zahl</i> wie oben |
| <i>/api/user/update</i> Parameter: <i>username</i> , <i>password</i> Optionale Parameter: <i>newUsername</i> , <i>hobbies</i> , <i>about</i> | <i>POST</i> | Updaten der Profilinformationen wie Nutzernamen, „Hobbies“ und „Über mich“. <i>newUsername</i> Benutzernamen ändern, <i>hobbies</i> und <i>about</i> setzen den „Hobbies“ und „Über mich“ Text. |
| <i>/api/post</i> Parameter: <i>username</i> , <i>password</i> , <i>message</i> | <i>POST</i> | Posten eines Beitrags auf der eigenen Pinnwand und der allgemeinen Chronik. |
| <i>/api/post/:username</i> Parameter: <i>username</i> , <i>password</i> , <i>message</i> | <i>POST</i> | Posten an die Pinnwand eines bestimmten Nutzers. |
| <i>/api/like</i> Parameter: <i>username</i> , <i>password</i> , <i>postid</i> | <i>POST</i> | Ermöglicht automatisiertes Liken eines Posts. |
| <i>/api/unlike</i> Parameter: <i>username</i> , <i>password</i> , <i>postid</i> | <i>POST</i> | Macht like rückgängig. |

5. Unterrichtseinheit (Geschichte): Propaganda im digitalen Zeitalter

Wie bereits im Kapitel 3.2 beschrieben, ist eine interdisziplinäre Betrachtung des Phänomens „Social Bots“ notwendig. In diesem Kapitel wird daher eine Unterrichtseinheit für den Geschichtsunterricht vorgestellt, die sich mit der Propaganda aus der Zeit des Nationalsozialismus und den Veränderungen der Mittel von Propaganda im digitalen Zeitalter beschäftigt. Dieser Vergleich vernetzt die Betrachtung der politischen Propaganda mit aktuellen Ereignissen und hebt dadurch besonders die Relevanz hervor. Den SchülerInnen werden insbesondere die Möglichkeiten zur effizienten Skalierung von Propaganda durch die digitalen Medien bewusst. Social Bots werden in diesem Zusammenhang vorgestellt und von den Lernenden bezüglich bestimmter Kriterien mit anderen Propagandamedien verglichen.

Die Unterrichtseinheit wird wieder auf Grundlage der Faktoren des Berliner Modells von Paul Heimann [Hub07, S. 26f., S. 29-40] geplant.

5.1. Bedingungsfelder

Da die Unterrichtseinheit nur geplant, aber nicht mehr gehalten wurde, ist im Folgenden eine prototypische Klassensituation beschrieben, für die der Unterricht konzipiert wurde.

5.1.1. Anthropologisch-psychologische Voraussetzungen

Das Vorwissen der SchülerInnen zu dem historischen Kontext von Propaganda um die Zeit des Zweiten Weltkrieges ist sehr heterogen. Einzelne SchülerInnen haben Schwierigkeiten sich in die Zeit hineinzusetzen und den Einfluss von Propaganda nachzuvollziehen. Ebenso sind die SchülerInnen unterschiedlich stark politisch interessiert, halten sich aber gerne über das aktuelle Weltgeschehen auf dem Laufenden. Sie verfolgen manche politische Diskussionen, die eine größere Berichterstattung in den Medien erfahren. Darüber informieren sie sich auch zu einem großen Teil im Internet, insbesondere über Youtubevideos und soziale Netzwerke [Med17, S. 17f, S. 47].

5.1.2. Soziokulturelle Voraussetzungen

Der Unterrichtsentwurf „Propaganda im digitalen Zeitalter“ umfasst zwei Schulstunden. Er lässt sich schulart- und klassenunabhängig in die Besprechung der NS-Zeit im Unterricht integrieren. Es ist jedoch nötig, dass die SchülerInnen aus konkreten Beispielen ein allgemeines Bild von Propaganda entwickeln können. Diese Abstraktions- und Reflexionsfähigkeit kann bei SchülerInnen der Mittel- und Oberstufe erwartet werden. Als Beispiel für die Anknüpfung dient die 9. Jahrgangsstufe der Realschule in Bayern: Dort ist im neuen Lehrplan „LehrplanPLUS“ enthalten, dass die SchülerInnen „ihre Kenntnisse [über Kriegspropaganda] kritisch auf andere Propagandabeispiele [anwenden], um die Rolle von Propaganda allgemein zu begreifen“ [Sta18a].

Die Stunde ist als Stationenlernen geplant, der Raum sollte daher flexibel zu Tischgruppen gestaltet werden können. Weitere Abhängigkeiten sind nicht zwingend, jedoch können verfügbare Computer mit Internetverbindung sinnvoll eingesetzt werden, falls welche vorhanden sind.

5.2. Inhaltliche Analyse

Im Folgenden werden aus der Definition von „Propaganda“ die Inhalte der Unterrichtseinheit abgeleitet und die notwendigen Voraussetzungen aufgezeigt.

5.2.1. Begriffsdefinition

Als Propaganda bezeichnet man den Versuch, gezielt Menschen in ihrem Denken, Handeln und Fühlen zu beeinflussen [Bun11]. Das Mittel, wie diese Beeinflussung stattfindet, hat sich im Laufe der Geschichte stark verändert. Bereits in der Antike wurden Manipulationen ohne Medien verwendet, wie Reden direkt vor Personen. Später kamen mit Zeitungen, Plakaten und Flugblättern Mittel zum Einsatz, die sich leichter in größerem Umfang verbreiten ließen. Radiosendungen, Filme und Fotografien sind noch neuere Medien und heutzutage bieten digitale Medien die Möglichkeit zu einer noch schnelleren Verbreitung über das Internet [Bun11].

5.2.2. Inhaltliche Voraussetzungen

In der Stunde bestehen inhaltliche Abhängigkeiten zu der allgemeinen Behandlung des Nationalsozialismus. Zumindest in Teilen sollte dieser bereits vor der vorgestellten

Stunde betrachtet worden sein. Dies betrifft unter anderem die Ideologie der Nationalsozialisten und die Entwicklung bis zur Machtergreifung. Dadurch können die SchülerInnen bei der Quellenarbeit zu Propaganda an den Ansichten des NS-Regimes und an der damaligen gesellschaftlichen Situation anknüpfen.

5.2.3. Inhalte der Unterrichtseinheit

In der Unterrichtseinheit sollen die SchülerInnen eine umfassende Vorstellung zu dem Begriff „Propaganda“ entwickeln. Dafür sollen vier verschiedene Bereiche aufbereitet werden:

1. **Plakate:** Mit Propagandaplakaten wurden sowohl Durchhalteparolen verbreitet als auch Stimmung gegen andere Nationen angefacht. Die Plakate nahmen dabei damals eine viel präsentere Rolle ein, also heutzutage.
2. **Rundfunk:** Das umfasst die damals neuen technischen Möglichkeiten des Radios und Fernsehens. Vor allem der Volksempfänger wird als ein Beispiel angeführt, wie Goebbels versuchte die Menschen für seine Propaganda erreichbar zu machen.
3. **Presse:** Ebenfalls zuzuordnen sind die Zeitungen, die durch die Gleichschaltung der Presse einen wichtigen Punkt eingenommen haben. Der Vergleich zu den heutigen Möglichkeiten bezieht sich vor allem auf die schnelle Verbreitung von Nachrichten, aber auch die gesetzlich festgelegte Pressefreiheit und somit Schutzmaßnahmen gegen Propaganda.
4. **Social Media:** Neben der allgemeinen Übertragung des politischen Diskurses in soziale Netzwerke sollen hier vor allem Fake News und Social Bots betrachtet werden.

Die verschiedenen Mittel unterscheiden sich hinsichtlich Reichweite, Kosten bzw. Aufwand, Geschwindigkeit der Verbreitung und der Wirksamkeit. Anhand dieser Kriterien sollen die SchülerInnen die genannten Propagandamittel vergleichen. Social Bots sind dabei eine Methode der schnellen und kosteneffizienten Verbreitung, für die die SchülerInnen sensibilisiert werden sollen.

5.3. Ziele

Nach der Unterrichtseinheit sind die SchülerInnen dazu in der Lage, . . .

1. . . . den Begriff Propaganda zu definieren.
2. . . . die Entwicklung der Propagandamedien vom Zweiten Weltkrieg zu heute zu erläutern.

3. ... die Gefahren von verschiedenen Propagandamitteln anhand vorgegebener Kriterien einzuschätzen.
4. ... die Aktualität von Propaganda zu begründen.

5.4. Methodische Analyse

Die SchülerInnen beschäftigen sich in der Unterrichtsstunde mit verschiedenen Formen von Propaganda. Die Inhalte haben dabei keine Abhängigkeiten untereinander, sondern hängen durch das übergeordnete Leitthema zusammen. Das ermöglicht es, die Inhalte in beliebiger Reihenfolge zu lernen, wodurch andere Unterrichtstechniken angewendet werden können. Bekannte Beispiele sind dafür vor allem das Gruppenpuzzle und das Stationenlernen.

Beim **Gruppenpuzzle** werden die SchülerInnen zunächst in Gruppen aufgeteilt und den einzelnen Gruppenmitgliedern die Materialien zu einem Teilbereich gegeben. In den Gruppen müssen alle Themen abgedeckt sein. Den SchülerInnen wird eine längere Einarbeitungszeit gegeben, in der sie eigenverantwortlich ihren Themenbereich bearbeiten. Anschließend treffen sich die SchülerInnen, die das gleiche Teilthema angeschaut haben, zu Expertenrunden zusammen und tauschen sich aus. Dadurch können Fehler Einzelner abgefangen werden. Nach der Expertenrunde treffen sich die SchülerInnen wieder in ihrer gemischten Gruppe und nehmen nun nach einander die Rolle des Lehrenden ein und erklären den MitschülerInnen ihr Spezialgebiet [Rei07a].

Ein Vorteil davon ist das Lernen durch Lehren. Dadurch dass die SchülerInnen den Stoff so aufbereiten müssen, dass sie ihn anderen verständlich erklären können, bleibt er ihnen besonders gut im Gedächtnis. Die Methode bietet zudem persönlichkeitsbildende Vorteile. So hilft die Kooperation dabei, mit den MitschülerInnen mehr in Kontakt zu kommen und die Klassengemeinschaft zu stärken. Auch die Fähigkeiten, vor einer Gruppe zu reden und Inhalte verständlich zu vermitteln, können dadurch verbessert werden.

Nachteilhaft an der Methode ist aus meiner persönlichen Erfahrung, dass nur der selbst vorbereitete Teil intensiv durchdacht wird. Die letzte Phase (Präsentation durch die Experten) wird zum einen durch die Experten wieder frontal vermittelt statt selbstständig erschlossen zu werden. Und zum anderen sind die SchülerInnen konzentriert, ihren eigenen Teil richtig vorzustellen, und daher weniger aufmerksam den anderen Gruppenmitgliedern gegenüber.

Das **Stationenlernen** strukturiert den Lernraum in mehrere kleine Stationen, an denen jeweils etwas über ein bestimmtes Teilgebiet des Leitthemas gelernt werden kann. Die SchülerInnen können die Reihenfolge der Stationen frei wählen und ihre Zeit weitestgehend selbstständig einteilen. Den Rahmen bieten Arbeitsaufträge, die von

den SchülerInnen bearbeitet werden müssen. Zur Differenzierung bietet es sich an, an den Stationen weiterführende Materialien bereit zu stellen. Dadurch können SchülerInnen über die Mindestanforderung hinaus mehr erfahren, wenn sie die anderen Aufgaben schneller bearbeitet haben, oder besonderes Interesse an einem Teilthema haben [Rei07b].

Positiv ist an der Methode, dass die SchülerInnen ihren eigenen Weg durch die Lerninhalte wählen können und diese nach ihren eigenen Interessen vertiefen. Das Stationenlernen bietet außerdem Lernmöglichkeiten, die konsequent am Konstruktivismus orientiert sind, da die SchülerInnen sich das Wissen aus den aufbereiteten Materialien selbst aufbauen [Rei07b].

Probleme können bei der Umsetzung entstehen, wenn die SchülerInnen das eigenständige Lernen nicht gewöhnt sind und die Ergebnisse nur von MitschülerInnen abschreiben statt selbst zu erarbeiten. Als Lehrkraft ist es schwierig dies im Auge zu behalten, da im ganzen Raum verteilt gearbeitet wird. Außerdem müssen die Materialien aus zwei Gründen besser aufbereitet sein, als bei vielen anderen Methoden: Erstens müssen die SchülerInnen sich selbständig durch den Auftrag durcharbeiten können und zweitens fallen der Lehrkraft Missverständnisse erst später auf, da sie sich auf mehrere Stationen konzentrieren muss.

Die Unterrichtseinheit bietet – durch unterschiedliche Zeitbezüge und die Mischung aus modernen, technischen Themen mit historischen – vor allem Stärken, SchülerInnen mit unterschiedlichen Interessen anzusprechen. Um dies zu nutzen, fiel die Entscheidung zugunsten des Stationenlernens aus. Zudem lassen sich die Probleme dieser Methode leichter schon in der Vorbereitung angehen. Die Auswahl und Aufbereitung der Materialien wird im folgenden Kapitel 5.5 dargestellt.

5.5. Medien

Für die verschiedenen Stationen müssen geeignete Medien gewählt werden und Aufgabenblätter entworfen werden. Die Medien beschränken sich dabei in der Stunde auf Texte und Bilder, um die Voraussetzungen zum Einsatz der Stunde gering zu halten. Videos und Eigenrecherche im Internet könnten an mehreren Stellen sinnvoll eingebaut werden, jedoch sind dafür ausreichend Computer, Tablets oder Smartphones notwendig. Bei Videos müssen außerdem Kopfhörer zur Verfügung stehen, um die SchülerInnen an den anderen Stationen nicht zu stören. Die verschiedenen Texte und Bilder sind in den Materialien 5.7 aufgeführt und im digitalen Anhang zu finden.

Bei den folgenden Aufgabenblättern sind zwei Dinge zu beachten: In allen Blättern soll die gleiche Aufgabe zu den Kriterien enthalten sein, wobei nur das Medium ausgetauscht wird. Dadurch können die SchülerInnen verschiedene Propagandamittel miteinander vergleichen. Der Übersichtlichkeit halber wurde die Aufgabe nur in dem ersten

Blatt ausformuliert. Da die Sozialformen variieren, wird die Formulierung des ersten Satzes zudem gegebenenfalls angepasst. Des Weiteren sind Vertiefungsaufgaben enthalten, die optional bearbeitet werden. Die SchülerInnen bekommen in der Stunde Zeit, ein Thema mit diesen Aufgaben zu vertiefen. Daher werden im Normalfall nur von einer Station die weiterführenden Aufgaben bearbeitet.

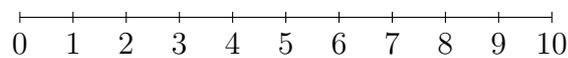
5.5.1. Station 1: Plakate

Für diese Station sollten die SchülerInnen Bilder von originalen Propagandaplakate zur Verfügung haben und analysieren. Als Hilfestellung steht ihnen ein kurzer Text zu der damaligen Verbreitung von Propagandaplakaten zur Verfügung.

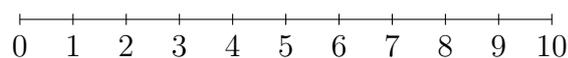
Arbeitsauftrag 5.1: Station 1 – Plakate

1. Lies dir zunächst den Überblickstext zur **Plakat-Propaganda** durch. Wähle dir anschließend aus den Beispielplakaten eines aus und beschreibe, was auf dem Plakat abgebildet ist. Gehe auch darauf ein, wann sich das Plakat zeitlich einordnen lässt und welche Botschaft und Gefühle es vermitteln soll.
2. Schätze das Medium „Plakat“ auf einer Skala von 0 (sehr wenig) bis 10 (sehr viel) zu folgenden Gesichtspunkten ein

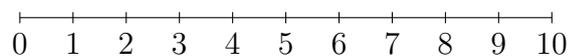
- Wie viele Leute konnte man früher mit den Plakaten erreichen?



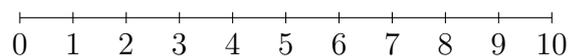
- Wie hoch sind die Kosten bzw. der Aufwand für die Verbreiter der Propaganda?



- Wie schnell können die Plakate verbreitet werden?



- Wie effektiv ist die Propaganda mit diesem Medium? Kann man damit Menschen überzeugen?



3. Vertiefung: Wie werden Plakate in der Politik heute noch eingesetzt? Wie haben sich diese inhaltlich geändert?

5.5.2. Station 2: Rundfunk

Beim Thema Rundfunk soll der Volksempfänger und die Gleichschaltung des Rundfunks betrachtet werden. Zwei Texte bieten die nötigen Informationen. Um die Lesezeit zu verkürzen, wird hier in Partnerarbeit zusammengearbeitet.

Arbeitsauftrag 5.2: Station 2 – Rundfunk

Bearbeitet die folgenden Aufgaben zu zweit in Partnerarbeit:

1. Teilt euch die Texte zur „Gleichschaltung des Rundfunks“ und zum „Volksempfänger“ auf und lest euren Text durch. Stellt euch danach gegenseitig in zwei bis drei Sätzen die Texte vor. Beantwortet folgende Fragen:
 - Was versteht man unter „Gleichschaltung des Rundfunks“?
 - Was war der Sinn eines erswinglichen Radiogeräts?
2. Sprecht euch zu den folgenden Kriterien ab und markiert dann eure Schätzung: *Kriterien wie in Station 1*

Bearbeite die Vertiefungsaufgaben wieder in Einzelarbeit.

3. Vertiefung: Heutzutage haben wir einen gebührenfinanzierten, öffentlich-rechtlichen Rundfunk. Begründe aus dem geschichtlichen Hintergrund, wieso dieser notwendig ist.
4. Vertiefung: Neben dem Radio galten auch das Fernsehen und die Kinos als neue Medien. Das Kino zeigte vor jedem Film die „Wochenschau“ – einen staatlich diktierten Vorläufer der heutigen Nachrichten. Das eigentliche Kinoprogramm war eher in Richtung „Heimatfilm“ ausgerichtet. Vergleiche diese Form von Propaganda nach den obigen Kriterien mit dem Radio. Welches Medium ist gefährlicher? Wie sieht das heute aus?

5.5.3. Station 3: Presse

Die Gleichschaltung der Presse ist als Text aufbereitet. Stehen Computer zur Verfügung, können diese hier ebenfalls eingesetzt werden und SchülerInnen z.B. zur im Grundgesetz verankerten Pressefreiheit recherchieren lassen.

Arbeitsauftrag 5.3: Station 3 – Presse

1. Lies dir die Texte zur „Gleichschaltung der Presse“ und zu „Zeitungen“ durch und beantworte die Fragen
 - Was geschah alles bei der „Gleichschaltung der Presse“?
 - Wie wurde die Arbeit eines Redakteurs durch die Gleichschaltung be-

einflusst?

- Wie wurde die Zeitung „Der Stürmer“ für die große Menge der Bevölkerung zugänglich gemacht?

2. *Kriterien wie in Station 1*

3. Vertiefung: Im Internet sind heutzutage zahlreiche Zeitungen zu finden, vor allem auch welche aus anderen Ländern. Welchen Einfluss hat das auf Propagandaversuche mit Zeitungen?

5.5.4. Station 4: Soziale Medien

Bei den heutigen Medien haben die SchülerInnen vermutlich schon Vorerfahrung, die reaktiviert werden sollten.

Arbeitsauftrag 5.4: Station 4 – Soziale Medien

1. Versuche selbst zu erklären, was die Begriffe „Social Media“, „Social Bots“ und „Fake News“ bedeuten. Vergleiche anschließend mit dem Text.
2. Lies dir den Text „Wenn die Fake News von der Polizei kommen“ durch. Welche Gefahren von Fake News werden in dem Text deutlich?
3. *Kriterien wie in Station 1*
4. Vertiefung: Sieh dir die zwei Twitter-Profilen an. Welches von beiden ist ein Bot? Woran erkennst du das? Erstelle eine Checkliste, wie man sich vor Social Bots und Fake News schützen kann.
5. Vertiefung: In vielen Medienberichten heißt es, Social Bots seien eine Bedrohung für die Demokratie. Was sind Gründe für diese Einschätzung? Was spricht dagegen?

5.6. Geplanter Stundenverlauf

Ausrichten (ca. 5 Minuten) Die Lehrkraft stellt den SchülerInnen kurz die Methode Stationenlernen vor. Dabei erklärt sie, dass es vier Stationen gibt, die in beliebiger Reihenfolge bearbeitet werden können. Allerdings muss jedeR SchülerIn am Ende an jeder Station gewesen sein. Anschließend stellt die Lehrkraft in je einem kurzen Satz die Themen vor, sodass die SchülerInnen eine Orientierung bekommen, wo sie starten möchten. Auf eine etwa ausgewogene Verteilung auf die Stationen sollte geachtet werden

Erarbeitungsphasen (4 mal ca. 10 Minuten + 1-2 Minuten Stationenwechsel)

Die SchülerInnen erarbeiten sich die Inhalte selbständig mit den vorbereiteten Materialien und Arbeitsaufträgen. Dabei sind ebenfalls Aufgaben zur Vertiefung enthalten. Diese gehören nicht zu den Mindestanforderungen der Station, können aber von schnelleren Schülern bzw. Gruppen bereits bearbeitet werden. Die Lehrkraft beantwortet Fragen und achtet darauf, ob ein Thema den SchülerInnen Schwierigkeiten bereitet, um entsprechend Unterstützung zu leisten. Nach jeweils 10 Minuten gibt die Lehrkraft ein Signal, dass die Station gewechselt werden soll.

Vertiefung (ca. 15 Minuten) Die SchülerInnen suchen sich ein Thema aus, das sie noch weiter vertiefen möchten und bearbeiten dazu die weiteren Aufgaben. Stehen Computer zur Verfügung können hier auch besonders gut weitere Rechercheaufgaben eingebunden werden.

Verarbeitung I (ca. 20 Minuten) Die SchülerInnen werden zunächst aufgefordert, kurz zu beschreiben, was Propaganda ist. Die Definition wird im Heft festgehalten – entweder wie im unteren Tafelanschrieb oder wenn möglich in der Form, wie die SchülerInnen es formulieren.

Tafelanschrieb: Propaganda

Propaganda ist der Versuch, gezielt Menschen in ihrem Denken, Handeln und Fühlen zu beeinflussen. Dabei werden oft vor allem die Emotionen angesprochen statt mit Fakten argumentiert.

Anschließend initiiert die Lehrkraft ein Schülergespräch zu den Fragen „Sind wir heute vor Propaganda geschützt?“ und gegebenenfalls „Wie gefährlich sind heutige Propagandamethoden?“. In der Diskussion reflektieren die SchülerInnen die erarbeiteten Stationen. Für die zweite Frage helfen Ihnen die Kriterien, die auf den Blättern waren. Propaganda lässt sich heute schneller und mit weniger Aufwand verbreiten. Allerdings sollte in der Diskussion auch berücksichtigt werden, dass wir viele gesetzlich gesicherten Freiheiten haben, die uns z.B. den Zugang zu unabhängigen Berichterstattungen ermöglichen. Auch die gesellschaftliche Situation sollte bei Effektivität von Propaganda berücksichtigt werden.

Abschluss (ca. 2 Minuten) Als Abschluss der Diskussion und Reflexion zur Stunde werden die SchülerInnen gebeten, eine wichtige Erkenntnis der Stunde zu formulieren und in das Heft zu schreiben.

5.7. Materialien

Für die Unterrichtsstunde wurden vor allem die Texte der Webseite ZeitKlicks.de [GW] verwendet. Im Folgenden sind die einzelnen Texte und Bilder aufgeführt, wobei im ganzen übernommene Texte nur verlinkt werden. Die Bilder sind in groß im digitalen Anhang zu finden.

Plakate:

- „Plakat-Propaganda“: Ausschnitt aus [WPBB12, S. 17]

Nicht nur bei der NSDAP, die gesamte politische Auseinandersetzung in der Weimarer Republik war ganz wesentlich von einem neuen Bildmedium geprägt: dem Plakat, das, in hoher Auflage gedruckt, massenhaft vor allem in den Städten verbreitet werden konnte. Auf einem Plakat konnten Bild und Text, Slogan und Symbol, Form und Farbe in wirksamer Weise konzentriert werden. „Unser Krieg wird in der Hauptsache mit Plakaten und Reden geführt“, schrieb Goebbels am 1. März 1932 in sein Tagebuch. Im Reichstagswahlkampf im Juli 1932 ließ allein die Hamburger NSDAP über 77 000 Plakate kleben. Gewalttätige Parolen wie „Zerschmettert den Weltfeind“ (1928) oder „Haut sie zusammen!“ (1930), die durch die Darstellung von kraftstrotzenden Männern mit zum Schlag erhobenen Hämmern gegen die „internationale Hochfinanz“ oder die bürgerlichen Parteien bekräftigt wurden, dominierten die Wahlkämpfe 1928 und 1930, während danach Zukunftsversprechen wie „Arbeit und Brot“ und die Fokussierung auf Hitler die Propaganda beherrschten.



Reichspräsidentenwahl 1932: Großflächige Plakate werben für Hitler und Hindenburg.

- Plakate von [Byt01]



Rundfunk:

- Gleichschaltung des Rundfunks: <http://www.zeitklicks.de/nationalsozialismus/zeitklicks/zeit/politik/gleichschaltung/gleichschaltung-des-rundfunks/>
- Volksempfänger: <http://www.zeitklicks.de/nationalsozialismus/zeitklicks/zeit/propaganda/im-ganz-normalen-leben/der-volksempfaenger-fuer-alle/>

Presse:

- Gleichschaltung der Presse: <http://www.zeitklicks.de/nationalsozialismus/zeitklicks/zeit/politik/gleichschaltung/gleichschaltung-der-presse/>
- Zeitungen: <http://www.zeitklicks.de/nationalsozialismus/zeitklicks/zeit/propaganda/im-ganz-normalen-leben/zeitungen/>

Soziale Medien:

- Begriffsüberblick – Social Media, Social Bots, Fake News: (eigener Text)

„**Social Media**“ sind digitale Medien, über die sich Nutzer vernetzen können. Dazu gehören Blogs, soziale Netzwerke und Chats. Über soziale Medien werden auch viel Nachrichten verbreitet. „**Fake News**“ sind Nachrichten, die absichtlich falsch sind und gezielt eingesetzt werden, um Leuten oder Organisationen zu schaden. Fake News sind damit ein Propaganda Mittel. Sie werden oft von vielen Menschen in den sozialen Medien geteilt, da sie sehr reißerische Botschaften haben und die Quellen oft nicht überprüft werden. Ein weiterer Faktor, dass Fake News stark verbreitet werden, sind aber „**Social Bots**“. Das sind Computerprogramme, die in sozialen Netzwerken Beiträge schreiben und liken, und sich dabei aber als Mensch ausgeben. Sie sind relativ leicht zu programmieren und mit einem Programm können sehr viele Bots gleichzeitig gesteuert werden. So können sie zum Beispiel bestimmte Falschnachrichten massenhaft teilen oder liken. Dadurch wird die Aufmerksamkeit stark auf diese Beiträge gelenkt

- „Wenn die Fake News von der Polizei kommen“ [Poh17] gekürzt:

Der Verdacht war ungeheuerlich: Linksradike hätten eine Türklinke unter Strom gesetzt, um Berliner Polizisten an der Räumung eines Hauses zu hindern. Ein Tweet, der Aufsehen erregte! Doch es war eine Fake-News, allerdings amtlich verbreitet von der Berliner Polizei. Schnell, schneller, Twitter: Da will auch die Polizei dabei sein. Das Risiko: Manchmal bleibt die Wahrheit auf der Strecke.

Die Polizei, dein Freund und Helfer. Auf Twitter präsentieren sich Deutschlands Ordnungshüter so, wie sie sich am liebsten sehen: jung, modern und bürgernah, Freund in Not geratener Tiere – und natürlich auch der Kinder.

Die Realität ist dann manchmal weniger ansehnlich. Beispiel: Berlin-Neukölln, gewaltsame Räumung eines besetzten Nachbarschaftsladens in der Friedelstraße. Die Berliner Polizei twittert unter dem Hashtag #Friedel54 live mit.

Die Räumung im Auftrag einer Briefkastenfirma sorgt für viel Unmut im Kiez. Die Polizisten gehen hart gegen die Blockierer vor.

Als die Beamten in den Innenhof eindringen stoßen sie an einer Kellertür auf ein verdächtiges Stromkabel. Am mittlerweile abmontierten Türknauf messen sie angeblich eine Stromspannung.

Gleich darauf twittert die Pressestelle der Polizei: „Lebensgefahr für unsere Kollegen! Handknauf unter Strom gesetzt – zum Glück haben wir das vorher geprüft.“

Die Meldung wird sofort von zahlreichen Medien aufgegriffen, sorgt für Aufruhr in den sozialen Netzwerken. Sebastian Czaja, Fraktionschef der Berliner FDP, twittert etwa: „menschenverachtende Chaoten“.

Nur: Die Meldung stimmt nicht. Eine Fakenews, verbreitet mit staatlicher Autorität. Vor Ort ist das auch schnell klar: Es gibt keine Stromquelle am Kabel und damit auch keine Gefahr. Diese Information aber gibt die Einsatzleitung nicht an die Pressestelle weiter.

Die Unterstützer des Kiezladens empören sich bis heute über die behördliche Falschmeldung.

- Die Twitter-Profilen von dem Bot @TrumepdAmerica (<https://twitter.com/TrumpedAmerica>, twittert exakt alle 3 Stunden ca 10 Nachrichten in einer Minute. Auf dem Screenshot ist ein Ausschnitt zu sehen) und von @realDonaldTrump (<https://twitter.com/realDonaldTrump>, Twitter-Account des amerikanischen Präsidenten Donald Trump).



Tweets **93,8 Tsd.** Folge ich **587** Follower **1.739** Gefällt mir **6**

Folgen

TrumpedAmerica

@TrumpedAmerica

#MakeAmericaGreatAgain
#SecureTheBorder #Trumpian #TrumpTrain
#TrumpedAmerica

USA

trumpedamerica.appspot.com/artic...
p?ha...

Beigetreten Oktober 2015

Tweet an TrumpedAmerica

92.8 Tsd. Fotos und Videos



Tweets Tweets & Antworten Medien

TrumpedAmerica @TrumpedAmerica · 36 Min.
Click here to support **VETERAN US ARMY NEEDS HELP** organized by Tracy Finch
trumpedamerica.appspot.com/artic...
Original (Englisch) übersetzen

TrumpedAmerica @TrumpedAmerica · 36 Min.
In face of Ghouta defeat, Syrian rebels blame each other
trumpedamerica.appspot.com/artic...
Original (Englisch) übersetzen

TrumpedAmerica @TrumpedAmerica · 36 Min.
Didn't Like That New Album? Another One Is Coming Before You Know It
trumpedamerica.appspot.com/artic...
Original (Englisch) übersetzen

TrumpedAmerica @TrumpedAmerica · 36 Min.
GOP senators fuel Justice Kennedy retirement talk
trumpedamerica.appspot.com/artic...
Original (Englisch) übersetzen



TrumpedAmerica @TrumpedAmerica · 59 Min.
WilliamMichaelMorgan on Twitter
trumpedamerica.appspot.com/artic...
Original (Englisch) übersetzen



Wem folgen? · Aktualisieren · Alle anzeigen

- John Martin** @LogicalReve...
Folgen
- The Trumpident** @The_Tru...
Folgen
- TrumpWinsForUS** @DJT4P...
Folgen

Finde Leute, die du kennst

Trends für dich · Ändern

- #thewalkingdead
- #leadership
- #barcelona
- john neumeier
- jungen
- #latenightberlin
- #5sos3tour
- #trapp
- #rummenigge
- #agethik

© 2018 Twitter Über uns Hilfe-Center
Bedingungen Datenschutzzrichtlinien
Impressum Cookies Info zu Anzeigen



Donald J. Trump

@realDonaldTrump

45th President of the United States of America

Washington, DC

[Instagram.com/realDonaldTrump](https://www.instagram.com/realDonaldTrump)

Beigetreten März 2009

2.557 Fotos und Videos

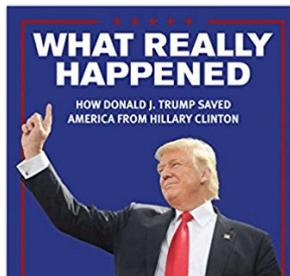


Tweets **37,2 Tsd.** Folge ich **45** Follower **49,6 Mio.** Gefällt mir **24** Moments **6**

Folgen

Tweets Tweets & Antworten Medien

- Donald J. Trump** @realDonaldTrump · 3 Std.
Great news! #MAGA
- CNBC Now** @CNBCnow
BREAKING: Dow posts third best one-day point gain ever
[cnbc.com/2G6ga8Y](https://www.cnbc.com/2020/03/24/dow-jones-242020.html)
- 11 Tsd. 8,2 Tsd. 32 Tsd.
- Donald J. Trump** @realDonaldTrump · 10 Std.
So much Fake News. Never been more voluminous or more inaccurate. But through it all, our country is doing great!
- 38 Tsd. 20 Tsd. 92 Tsd.
- Donald J. Trump** @realDonaldTrump · 12 Std.
The economy is looking really good. It has been many years that we have seen these kind of numbers. The underlying strength of companies has perhaps never been better.
- 20 Tsd. 15 Tsd. 73 Tsd.
- Donald J. Trump** @realDonaldTrump · 20 Std.
@HowieCarrShow just wrote a book which everyone is talking about. He was a great help. He is a veteran journalist who had a great influence in NH and beyond. He calls it the most amazing political campaign of modern times. The book is called, "What Really Happened." Enjoy! #MAGA



Neu bei Twitter?

Melde dich jetzt an, um deine eigene, personalisierte Timeline zu erhalten!

Registrieren

Vielleicht gefällt dir auch.

Aktualisieren

- President Trump** @POTUS
- Hillary Clinton** @HillaryClinton
- Barack Obama** @BarackObama
- The White House** @WhiteHouse
- CNN** @CNN

Munich Trends

- #LateNightBerlin** 2.757 Tweets
- #wasfuermichdeutschist** 8.545 Tweets
- #hartaberfair** 3.286 Tweets
- #Puigdemont** 119 Tsd. Tweets
- Diplomaten** 10,1 Tsd. Tweets
- #GERBRA** 3.260 Tweets
- Start in die Woche** 1.419 Tweets
- Zeitumstellung** 2.912 Tweets
- montamorgen**

6. Fazit

Aus den aktuellen Studien geht klar hervor, dass Social Bots existieren und eingesetzt werden, um Meinungen zu manipulieren. Damit stellen sie eine große Herausforderung für unsere Gesellschaft dar. Es ist auch nicht abzusehen, dass sie bald verschwinden. Stattdessen könnten Fortschritte im Bereich der Künstlichen Intelligenz dazu führen, dass die Einflüsse noch stärker werden. Um den Gefahren entgegenzutreten ist daher nötig, über das Phänomen aufzuklären und die Medienkompetenz der SchülerInnen zu fördern.

Die anfangs formulierte Unklarheit, ob die Thematik bereits in der Schule vermittelt werden kann, kann klar beantwortet werden: Sie kann problemlos in den Unterricht eingebunden werden und insbesondere die Ziele des Informatikunterrichts gewinnbringend unterstützen. Die Umsetzung ist trotz des technischen Hintergrundes allerdings nicht auf dieses Fach beschränkt. Gerade ein interdisziplinärer Ansatz kann den SchülerInnen wichtige Kompetenzen im Umgang mit Social Bots vermitteln.

Wegen der Brisanz der Thematik ist es wünschenswert, dass die Umsetzung in den Schulen vermehrt durchgeführt wird. Durch diese Arbeit wird hoffentlich das Bewusstsein für die Problematik unter Lehrkräften gestärkt, was einen guten Ausgangspunkt für die notwendigen Bildungsmaßnahmen darstellt.

Literaturverzeichnis

- [BF16] BESSI, Alessandro ; FERRARA, Emilio: Social bots distort the 2016 US Presidential election online discussion. In: *First Monday* 21 (2016), November, Nr. 11. <http://dx.doi.org/10.5210/fm.v21i11.7090>. – DOI 10.5210/fm.v21i11.7090. – ISSN 13960466
- [BMBR11] BOSHMAF, Yazan ; MUSLUKHOV, Ildar ; BEZNOSOV, Konstantin ; RIPEANU, Matei: The Socialbot Network: When Bots Socialize for Fame and Money. (2011), Sep
- [BMBR13] BOSHMAF, Yazan ; MUSLUKHOV, Ildar ; BEZNOSOV, Konstantin ; RIPEANU, Matei: Design and analysis of a social botnet. In: *Computer Networks* 57 (2013), Nr. 2, 556 - 578. <http://dx.doi.org/https://doi.org/10.1016/j.comnet.2012.06.006>. – DOI <https://doi.org/10.1016/j.comnet.2012.06.006>. – ISSN 1389–1286. – Botnet Activity: Analysis, Detection and Shutdown
- [Bun11] BUNDESZENTRALE FÜR POLITISCHE BILDUNG: *Was ist Propaganda?* <http://www.bpb.de/gesellschaft/medien-und-sport/krieg-in-den-medien/130697/was-ist-propaganda>. Version: Oktober 2011
- [Byt01] BYTWERK, Randall: *German Propaganda Archive*. 2001. – <http://www.bytwerk.com/gpa/posters1.htm>, <http://www.bytwerk.com/gpa/posters3.htm>
- [Cha17] CHAOS COMPUTER CLUB E.V.: *Schedule 34th Chaos Communication Congress - lecture: Social Bots, Fake News und Filterblasen*. <https://fahrplan.events.ccc.de/congress/2017/Fahrplan/events/9268.html>. Version: Dezember 2017
- [CS03] CLAUS, Volker ; SCHWILL, Andreas: *Duden Informatik - ein Fachlexikon für Studium und Praxis*. 3. Auflage. Mannheim : Dudenverl., 2003. – ISBN 978-3-411-10023-1
- [Deu17] DEUTSCHER BUNDESTAG: *Wirkung von „Social Bots“ ist unter Sachverständigen strittig*. <https://www.bundestag.de/dokumente/textarchiv/2017/kw04-pa-bildung-forschung-social-bots/488818>. Version: jan 2017
- [DKS14] DICKERSON, J. P. ; KAGAN, V. ; SUBRAHMANIAN, V. S.: Using sentiment to detect bots on Twitter: Are humans more opinionated than bots? In: *2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014)*, 2014, S. 620–627
- [DVF⁺16] DAVIS, Clayton A. ; VAROL, Onur ; FERRARA, Emilio ; FLAMMINI, Alessandro ; MENCZER, Filippo: BotOrNot: A System to Evaluate Social Bots. In: *Proceedings of the 25th International Conference Companion on*

World Wide Web. Republic and Canton of Geneva, Switzerland : International World Wide Web Conferences Steering Committee, 2016 (WWW '16 Companion). – ISBN 978–1–4503–4144–8, 273–274

- [exp17] EXPLAIN-IT: *Fake News & Social Bots in 3 Minuten erklärt*. <https://youtu.be/j14s00N3c1g>. Version: März 2017
- [FVD⁺16] FERRARA, Emilio ; VAROL, Omur ; DAVIS, Clayton ; MENCZER, Filippo ; FLAMMINI, Alessandro: The Rise of Social Bots. In: *Commun. ACM* 59 (2016), Juni, Nr. 7, 96–104. <http://dx.doi.org/10.1145/2818717>. – DOI 10.1145/2818717. – ISSN 0001–0782
- [Ges08] GESELLSCHAFT FÜR INFORMATIK (GI) E.V.: *Bildungsstandards Informatik für die Sekundarstufe I*. http://www.informatikstandards.de/docs/bildungsstandards_2008.pdf. Version: Januar 2008
- [Ges16] GESELLSCHAFT FÜR INFORMATIK (GI) E.V.: *Bildungsstandards Informatik für die Sekundarstufe II*. https://www.informatikstandards.de/docs/Bildungsstandards_SII.pdf. Version: Januar 2016
- [Gre11] GRELL, Detlef: *Security-Firma entwirft Tools zur Meinungsmache mit Kunstfiguren*. <https://www.heise.de/security/meldung/Security-Firma-entwirft-Tools-zur-Meinungsmache-mit-Kunstfiguren-1193436.html>. Version: Februar 2011
- [GW] GRULER, Sabine ; WAGNER, Kirsten: *Zeitklicks*. <http://www.zeitklicks.de>
- [Hac14] HACKHAUSEN, Jörg: *Cynk Aktie - Der pure Wahnsinn*. <https://www.handelsblatt.com/finanzen/maerkte/boerse-inside/cynk-aktie-der-pure-wahnsinn/10258850.html>. Version: Juli 2014
- [Heg16] HEGELICH, Simon: *Invasion der Meinungs-Roboter*. Konrad-Adenauer-Stiftung, 2016
- [Heg18] HEGELICH, Simon: *Social Bots: Stimmungsmache im Iran*. <https://politicaldatascience.blogspot.de/2018/01/social-bots-stimmungsmache-im-iran.html>. Version: Januar 2018
- [HJ16] HEGELICH, Simon ; JANETZKO, Dietmar: Are Social Bots on Twitter Political Actors? Empirical Evidence from a Ukrainian Social Botnet. In: *Proceedings of the Tenth International Conference on Web and Social Media, Cologne, Germany, May 17-20, 2016.*, 2016, 579–582
- [HK16] HOWARD, Philip N. ; KOLLANYI, Bence: Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum. In: *CoRR* abs/1606.06356 (2016). <http://arxiv.org/abs/1606.06356>
- [HKW16a] HOWARD, P ; KOLLANYI, B ; WOOLLEY, SC: Bots and Automation over Twitter during the Second US Presidential Debate. (2016)
- [HKW16b] HOWARD, P ; KOLLANYI, B ; WOOLLEY, SC: Bots and automation over Twitter during the third US Presidential Debate. (2016)
- [HKW16c] HOWARD, Philip N. ; KOLLANYI, Bence ; WOOLLEY, SC: Bots and Automation over Twitter during the US Election. In: *Computational Propaganda Project: Working Paper Series* (2016)

- [Hub07] HUBWIESER, Peter: *Didaktik der Informatik: Grundlagen, Konzepte, Beispiele*. Springer-Verlag, 2007
- [KHW16] KOLLANYI, Bence ; HOWARD, Philip N. ; WOOLLEY, Samuel C.: Bots and automation over Twitter during the first US Presidential debate. In: *Comprop data memo 1* (2016), S. 1–4
- [KJW⁺17] KIND, Sonja ; JETZKE, Tobias ; WEIDE, Sebastian ; EHRENBERG-SILIES, Simone ; BOVENSCHULTE, Marc: *Social Bots*. <https://www.tab-beim-bundestag.de/de/untersuchungen/uV005.html>. Version: April 2017
- [KMK12] KMK – KULTUSMINISTERKONFERENZ: *Medienbildung in der Schule*. https://www.kmk.org/fileadmin/veroeffentlichungen_beschluesse/2012/2012_03_08_Medienbildung.pdf. Version: März 2012
- [Kre17] KREIL, Michael: *Social Bots, Fake News und Filterblasen*. https://media.ccc.de/v/34c3-9268-social_bots_fake_news_und_filterblasen. Version: Dezember 2017
- [Mü18] MÜHLBAUER, Peter: *Social Bots praktisch nicht existent*. <https://heise.de/-3934374>. Version: Januar 2018
- [Med17] MEDIENPÄDAGOGISCHER FORSCHUNGSVERBUND SÜDWEST (MPFS): *JIM Studie 2017*. <http://www.lehrplanplus.bayern.de/uebergreifende-ziele/textabsatz/24767>. Version: 2017
- [Nau17] NAUER, David: *Russlands Informationskrieg*. <https://www.srf.ch/news/international/so-funktioniert-eine-troll-fabrik>. Version: Februar 2017
- [Poh17] POHL, Markus: *Wenn die Fake-News von der Polizei kommen*. <https://www.rbb-online.de/kontraste/archiv/kontraste-vom-09-11-2017/wenn-die-fake-news-von-der-polizei-kommen.html>. Version: November 2017
- [Rü17] RÜHL, Wolf-Dieter: *Measuring Fake News: Die Methode*. <https://www.stiftung-nv.de/de/publikation/fake-news-die-methode>. Version: Dezember 2017
- [Rei07a] REICH, Kersten: *Methodenpool – Gruppen-Experten-Rallye*. http://www.uni-koeln.de/hf/konstrukt/didaktik/rallye/frameset_rallye.html. Version: 2007
- [Rei07b] REICH, Kersten: *Methodenpool – Stationenlernen*. http://www.uni-koeln.de/hf/konstrukt/didaktik/stationenlernen/frameset_stationenlernen.html. Version: 2007
- [Sch93] SCHWILL, Andreas: Fundamentale ideen der informatik. In: *Zentralblatt für Didaktik der Mathematik* 25 (1993), Nr. 1, S. 20–31
- [SCM11] STEIN, Tao ; CHEN, Erdong ; MANGLA, Karan: Facebook immune system. In: *Proceedings of the 4th Workshop on Social Network Systems* ACM, 2011, S. 8

- [SSRDM16] SUÁREZ-SERRATO, Pablo ; ROBERTS, Margaret E. ; DAVIS, Clayton ; MENCZER, Filippo: On the Influence of Social Bots in Online Protests. In: SPIRO, Emma (Hrsg.) ; AHN, Yong-Yeol (Hrsg.): *Social Informatics*. Cham : Springer International Publishing, 2016. – ISBN 978–3–319–47874–6, S. 269–278
- [Sta18a] STAATSINSTITUT FÜR SCHULQUALITÄT UND BILDUNGSFORSCHUNG (ISB): *LehrplanPLUS Geschichte 9, Realschule Bayern*. <http://www.lehrplanplus.bayern.de/fachlehrplan/realschule/9/geschichte>. Version: 2018
- [Sta18b] STATISTA: *Most famous social network sites 2018, by active users*. <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>. Version: Januar 2018
- [VFD⁺17] VAROL, Onur ; FERRARA, Emilio ; DAVIS, Clayton A. ; MENCZER, Filippo ; FLAMMINI, Alessandro: Online Human-Bot Interactions: Detection, Estimation, and Characterization. In: *CoRR* abs/1703.03107 (2017). <http://arxiv.org/abs/1703.03107>
- [WMKS12] WAGNER, Claudia ; MITTER, Silvia ; KÖRNER, Christian ; STROHMAIER, Markus: When social bots attack: Modeling susceptibility of users in online social networks. In: *Making Sense of Microposts (# MSM2012)* 2 (2012), Nr. 4, S. 1951–1959
- [Woo16] WOOLLEY, Samuel: Automating power: Social bot interference in global politics. In: *First Monday* 21 (2016), Nr. 4. <http://dx.doi.org/10.5210/fm.v21i4.6161>. – DOI 10.5210/fm.v21i4.6161. – ISSN 13960466
- [WPBB12] WILDT, M. ; POLITISCHE BILDUNG (BONN), Bundeszentrale für: *Nationalsozialismus: Aufstieg und Herrschaft*. Bundeszentrale für Politische Bildung, 2012 (Informationen zur politischen Bildung). <http://www.bpb.de/izpb/137182/nationalsozialismus-aufstieg-und-herrschaft>
- [ZDF17] ZDF HEUTEPLUS: *Social Bots*. <https://youtu.be/HVuB1QPxdT0>. Version: Januar 2017

A. Weitere Unterrichtsideen

Im Folgenden werden skizzenhaft weitere Überlegungen für Unterrichtsstunden vorgestellt, die im Rahmen der Arbeit nicht mehr ausformuliert wurden. Sie sollen als Anregung dienen, das Thema interdisziplinär und nach dem Spiralprinzip über mehrere Jahrgangsstufen verteilt zu betrachten.

A.1. Chatbots

Chatbots und Social Bots haben technisch viel gemeinsam. Vor allem für jüngere SchülerInnen kann mit Chatbots ein handlungsorientierter Einstieg in die Thematik Bots bzw. Künstliche Intelligenz umgesetzt werden. Die SchülerInnen könnten dort zunächst mit einem entsprechenden Chatprogramm schreiben. Dabei können sie entdecken, dass Chatbots zwar korrekte Sätze formulieren können, aber einer längeren Konversation nicht folgen können. Die Antworten nehmen außerdem meistens nur auf einzelne Wörter Bezug.

Anhand eines kleinen Bots kann anschließend die genauere Funktionsweise betrachtet werden. Dabei sollten die Lernenden erfahren, dass die Antworten der Bots für bestimmte Sätze oder enthaltene Wörter vorprogrammiert sind.

Im weiteren Verlauf können die SchülerInnen selbst einen entsprechenden Chatbot für ihre Klassenkameraden programmieren. In dem Projekt „Informatik im Kontext“ (<http://informatik-im-kontext.de/>) ist eine ausführliche Unterrichtseinheit zu dem historisch interessanten Chatbot ELIZA und einem Programmierprojekt mit AIML beschrieben. Eine andere Möglichkeit wäre, einen Chatbot mit Scratch (<https://scratch.mit.edu/>) zu implementieren. Der Vorteil davon ist, dass die Programmierumgebung für Schüler ausgelegt ist. Dort stehen den SchülerInnen auch weitere Programmiermöglichkeiten zur Verfügung, sodass der Chat auch als ein Bestandteil eines größeren Spiels eingebaut werden kann. Die SchülerInnen sollten Scratch bereits aus vorherigen Unterrichtseinheiten kennen, da ein Chatbot in Scratch abstrakter ist, als die sonst übliche Einstiegsaufgaben. Im Scratch-Wiki existiert bereits ein (englischsprachiges) Tutorial zum Erstellen eines Chatbots https://en.scratch-wiki.info/wiki/Creating_a_Chat_Bot.

Die Erfahrungen, die die SchülerInnen mit den Chatbots machen, helfen ihnen auch im Umgang mit Social Bots. Zum einen wird ihnen bewusst, dass Bots reine Algorithmen sind, die nicht selbständig denken, sondern nach festgelegten, einprogrammierten Regeln agieren. Andererseits bemerken sie auch, dass Bots natürliche Sprache imitieren können und so auf den ersten Blick wie Menschen wirken können. Social Bots stellen dann nur eine Übertragung dieser Erkenntnisse auf andere Gesprächsumgebungen dar, mit der zusätzlichen Absicht, durch die Texte die Meinung der Leser zu beeinflussen. Die Schwierigkeiten solcher Algorithmen, tatsächlich menschlich zu wirken, zeigen den SchülerInnen wichtige Limitationen in der Effektivität dieser Manipulationsversuche auf.

A.2. Sozialkunde – Gefahren und Möglichkeiten von Social Bots

Im Sozialkundeunterricht wäre eine Unterrichtsstunde denkbar, die – ähnlich wie in Kapitel 2.2 – die Gefahren von Social Bots mit den SchülerInnen herausarbeitet. Gleichzeitig können Möglichkeiten aufgezeigt werden, wie die Technologie positiv verwendet werden kann. Beispielsweise gab es einen Twitterbot *@Cancelthatcard*¹, der automatisch Leuten eine Nachricht schrieb, die ein Bild ihrer Kreditkarte twitterten. Die Nachricht forderte sie dazu auf, die Karte zu sperren und verlinkte auf eine Seite mit Informationen zu Kreditkartenbetrug. Anschließend wäre eine Diskussion über die Notwendigkeit und Durchsetzbarkeit einer gesetzlichen Regelung möglich.

¹Der Account ist inzwischen gesperrt worden. Einzelne Momentaufnahmen sind über das Webarchiv abrufbar: <https://web.archive.org/web/20140214003033/https://twitter.com/cancelthatcard>

B. Ergänzungen zur Unterrichtseinheit „Programmieren eines Social Bots“

B.1. Soziales Netzwerk

Im Folgenden soll noch ein wenig die Softwarestruktur des sozialen Netzwerkes beschrieben werden, um eine Erweiterung auch für andere zu erleichtern. Das Netzwerk baut auf dem Framework Spark auf (<http://sparkjava.com/>) und orientiert sich vor allem bei der Konfiguration an dem Tutorial zu einem Twitter Klon (<http://sparkjava.com/tutorials/twitter-clone>). Für den Html-Code wurden Freemarker-Templates verwendet (<https://freemarker.apache.org/docs/ref.html>) und eine SQL-Datenbank angebunden. Des Weiteren wird eine Dependency Injection mit Java Spring Beans implementiert.

Der Servercode unterteilt sich in die Konfiguration und die Module `Post` und `User`. Der wichtigste Teil der Konfiguration ist die Klasse `Router`. Dort werden die verschiedenen erreichbaren Pfade des Servers definiert und an die entsprechenden Controller-Methoden der Module vermittelt. In dem Router müssen daher bei einer Erweiterung neue Pfade hinzugefügt werden.

Die Module sind jeweils folgendermaßen gegliedert:

- Das **Modell** ist ein Abbild der Datenbank, wobei Fremdschlüssel direkt als Objekte einer anderen Klasse aufgeschlüsselt werden.
- Der Zugang zur Datenbank ist mit dem Entwurfsmuster *Data Access Object* (**DAO**) von den Aufrufen getrennt. Um dies umzusetzen, implementieren die DAO-Klassen ein Interface, das die Schnittstelle der Datenbank beschreibt. In der Implementierung werden dann die konkreten SQL-Befehle auf der Datenbank ausgeführt und entsprechende Objekte des Modells erzeugt.
- Der **Service** baut auf den Methoden der DAO-Klassen auf und bietet verschiedene abstrahierte Funktionalitäten für die Datenbankzugriffe. Hier werden beispielsweise auch Passwörter noch verschlüsselt oder HTML-Befehle aus Posts entfernt,

bevor die DAO-Klassen aktiv werden. Es ermöglicht auch mehrere Methoden der DAO-Schnittstelle zu einer größeren Funktion zu bündeln. Die Service-Klasse ist die einzige, die mit den DAO-Schnittstellen kommuniziert.

- Die **Controller**-Klassen verarbeiten die HTTP-Anfrage und verifizieren die Korrektheit der Parameter. Danach rufen sie gegebenenfalls die Methoden der Service-Klasse auf und erstellen das Datenmodell für die Freemarker Templates.

Der Code ist auf Github veröffentlicht (<https://github.com/Knorrke/socialbotnet>) und kann jederzeit gerne angepasst oder erweitert werden.

B.2. Proxy-Authentication Problembehebung

Um die Webseite auch bei eingerichteter Proxy-Authentifizierung von Java-Programmen aus erreichbar zu machen, muss in den Startparametern konfiguriert werden, dass Java die Systemeinstellungen des Proxy verwendet. Dazu muss die Java Systemeigenschaft `java.net.useSystemProxies` auf `true` gesetzt werden. In Eclipse lässt sich diese Einstellung über *Run Configurations* -> *Environment* hinzufügen. In BlueJ muss man in der Datei `<BlueJpfad>/lib/bluej.defs` bei den Optionen zum starten der virtuellen Maschine folgende Zeile ändern: Statt

```
bluej.vm.args=-ea
```

wird mit einem Leerzeichen abgetrennt die Eigenschaft auf wahr gesetzt:

```
bluej.vm.args=-ea -Djava.net.useSystemProxies=true
```

Alternativ können auch in der Klasse `Netzwerkverbindung` die folgenden Zeilen Code im Konstruktor ergänzt werden (und die korrekten Proxy-Daten eingegeben werden):

```
System.setProperty("http.proxyHost", "hostAddress");  
System.setProperty("http.proxyPort", "portNumber");  
System.setProperty("http.proxyUser", "Nutzername");  
System.setProperty("http.proxyPassword", "passwort");
```

Die letzten beiden Zeilen müssen dabei die Anmeldedaten der SchülerInnen enthalten. Das Passwort ist dann also im Programmcode sichtbar, was ein deutlicher Nachteil an dieser Alternative ist.

Eidesstattliche Versicherung

Erklärung zur Hausarbeit gemäß §29 (Abs.6) LPO I

Hiermit erkläre ich, dass die vorliegende Hausarbeit von mir selbstständig verfasst wurde und dass keine anderen als die angegebenen Hilfsmittel benutzt wurden. Die Stellen der Arbeit, die anderen Werken dem Wortlaut oder Sinn nach entnommen sind, sind in jedem einzelnen Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht.

Diese Erklärung erstreckt sich auch auf etwa in der Arbeit enthaltene Zeichnungen, Kartenskizzen und bildliche Darstellungen.

.....

Ort, Datum

.....

Name