

# Freundschaftsanfrage von der NSA

Wie Geheimdienste die sozialen Netzwerke nutzen – und mit welchen Folgen

Jan Guldner | **Im Zeitalter von Facebook und Co. müssen Informationen zu Krisen wie in der Ukraine oder der arabischen Welt im Zweifel nicht mehr mühsam recherchiert werden, sondern werden offen geteilt. Und so geraten die sozialen Netzwerke immer stärker ins Visier der Geheimdienste, Manipulation und Infiltration inklusive. Ist die Demokratie im Netz gefährdet?**

Als Igor Girkin seinen Status aktualisierte, war die Tragödie erst ein paar Minuten alt. Girkin, im Juli noch einer der Führer der prorussischen Separatisten im Osten der Ukraine, schrieb im russischen sozialen Netzwerk VKontakte, dass seine Truppen gerade eine ukrainische Transportmaschine in der Region Torez abgeschossen hätten. Mit dreifacher Schallgeschwindigkeit waren die Boden-Luft-Raketen auf ihr Ziel zugerast. Das Flugzeug explodierte sofort. „Wir haben euch gewarnt, fliegt nicht in unseren Luftraum“, schrieb Girkin. Dass es sich nicht um einen ukrainischen Militärtransporter, sondern um eine Passagiermaschine auf dem Weg von Amsterdam nach Kuala Lumpur handelte, wusste er da noch nicht.

Was Girkin auch nicht wusste: Ein amerikanischer Geheimdienstanalyst mit russischen Sprachkenntnissen hatte seine Statusmeldung gelesen. Und mit dem Wissen um die in der gleichen Region verschwundene Passagiermaschine von Malaysian Airlines, Flugnummer MH-17, sahen die Separatisten plötzlich nicht mehr aus wie siegreiche Krieger, sondern wie die Mörder von Zivilisten. „Die ersten Indizien, wer was wohin geschossen hat, kamen in dieser Situation allesamt aus den sozialen Medien“, sagte Michael T. Flynn, bis Anfang August Direktor der amerikanischen Defense Intelligence Agency (DIA), kürzlich dem *Wall Street Journal*.

## Der Globus im Visier

Das Beispiel des MH-17-Abschusses zeigt: Die Art, wie Geheimdienste sich Informationen beschaffen, wandelt sich. Die amerikanischen Geheimdienste zapfen Leitungen auf der ganzen Welt an. Sie steuern Satelliten, mit denen sie den gesamten Globus ins Visier nehmen können. Und sie haben ein Netzwerk von Spionen und Informanten, verstreut über alle Ecken der Erde. Doch ein

paar Zeilen, gefischt aus den sozialen Netzwerken, brachten nach wenigen Minuten schon eine entscheidende Erkenntnis, und das schneller als mittels klassischer Spionagetechniken. Kein Wunder, dass die Dienste immer stärker auf die Analyse der offen zugänglichen Daten im Internet setzen.

Auch bei einem anderen aktuellen Konfliktherd stehen die sozialen Medien im Fokus und damit ganz weit oben in der Aufmerksamkeit der Geheimdienste. Der Islamische Staat (IS), der in Syrien und dem Irak mit beispielloser Grau-

samkeit für ein muslimisches Kalifat kämpft, „vermarktet“ seine Gewalttaten mit einer ausgefeilten Social-Media-Strategie. Mit Propagandabotschaften und Videos von Enthauptungen versuchen die Islamisten einerseits ihre Gegner einzuschüchtern und gleichzeitig neue Rekruten für ihren Kampf zu gewinnen. Über eine eigene App kann der IS etwa

auf die Twitter-Konten seiner Anhänger zugreifen und konzertierte Kampagnen fahren. Doch so grausam die Bilder und Texte der Milizen auch sind, die sie in den sozialen Medien teilen, sie enthalten immer auch wertvolle Informationen über Strategien, Standorte und Hierarchien innerhalb der Terrororganisation. Und deshalb lohnt sich auch deren Überwachung.

**Die IS-Propaganda  
enthält immer auch  
wertvolle Informationen**

### Gefundenes Fressen

Jeden Tag werden viele Millionen Informationsschnipsel in sozialen Netzwerken veröffentlicht. 2,5 Milliarden Statusmeldungen, Bilder und andere Inhalte wurden schon im Jahr 2012 täglich auf Facebook geteilt. 100 Stunden Videomaterial werden jede Minute bei YouTube hochgeladen, täglich werden 500 Millionen Nachrichten mit 140 Zeichen Länge über Twitter verbreitet.

Immer größere Teile des täglichen Lebens, privat wie beruflich, werden in die digitale Welt verlagert. Egal ob in der westlichen Welt, im Nahen Osten, in Afrika oder Asien – die Zahl der Menschen wächst stetig, die Zugriff auf das Internet haben und es nutzen, um sich mit anderen auszutauschen. Der Datenberg, der daraus entsteht, hat eine Dimension, die kaum noch zu fassen ist. Und all diese Daten sind größtenteils öffentlich zugängliche Texte, Bilder, Videos und Tonaufnahmen.

Für die Geheimdienste der Welt ist das ein gefundenes Fressen. Geheimdienstler wie der ehemalige DIA-Direktor Michael T. Flynn äußern sich geradezu euphorisch über die neuen Möglichkeiten zum Sammeln und Auswerten von Daten im Netz. Für David Omand, ehemaliger Direktor des britischen Government Communications Headquarters (GCHQ), könnte sogar eine neue Form der Geheimdienstarbeit in den sozialen Medien entstehen. Neben der durch Spione und Informanten gesammelten Informationen (Human Intelligence, HUMINT) und dem Abhören von Funkwellen und Datenleitungen (Signals Intelligence, SIGINT) hat Omand dafür den Begriff der Social Media Intelligence (SOCMINT) geprägt.

„Die sozialen Netzwerke und Medien werden von Geheimdiensten stark überwacht“, sagt Siegfried Beer, Historiker und Geheimdienstexperte am Austrian Center for Intelligence, Propaganda and Security Studies (ACIPSS) in

# Bild nur in Printausgabe verfügbar

Wien. Und nicht nur von amerikanischen oder britischen Diensten. „Alle, die das machen können, tun es“, so Beer.

Auch in Deutschland werden die sozialen Medien stärker ins Visier genommen. Die Bundeswehr hat unter dem Namen „Wissenserschließung in offenen Quellen“ ein Programm aufgelegt, das die bei Facebook offen zugänglichen Daten systematisch auswerten soll. Daneben plant der Bundesnachrichtendienst Investitionen von 300 Millionen Euro, um „in durchlaufenden Streaming-Daten von Social-Media-Plattformen mithilfe statistischer Verfahren Tendenzen, Trends und Auffälligkeiten ausfindig zu machen“, wie es heißt. Die Zusage der Mittel durch den Bundestag ist aber noch ungewiss.

Die Wissensgewinnung in den sozialen Medien hat einen entscheidenden Vorteil: Anders als bei aufwendigen Abhöraktionen oder Spionageeinsätzen benötigt man zur Erforschung der sozialen Netzwerke relativ wenig Ressourcen. „Die sozialen Netzwerke ersetzen teilweise das Einschleusen von Geheimdienstlern in die jeweilige Organisation, die ausgeforscht werden soll“, sagt der Geheimdienstexperte Erich Schmidt-Eenboom, Leiter des Forschungsinstituts für Friedenspolitik in Weilheim. Alles, was man braucht, sind – vereinfacht gesprochen – ein paar schlaue Algorithmen und die nötige Rechenkraft, diese zu lösen.

Wie genau das funktionieren kann, zeigt eine von der Enthüllungsplattform WikiLeaks 2013 veröffentlichte Datei. In den so genannten SpyFiles gelangten Informationsbroschüren und Präsentationen von hunderten von Unternehmen an die Öffentlichkeit, die sich damit bei Geheimdiensten auf der ganzen Welt um Aufträge bewarben. Darunter fand sich auch eine Broschüre des Software-Herstellers Kapow Software aus dem amerikanischen Palo Alto, die beschreibt, wie die Dienste das Internet nach offenliegenden Informatio-

## Obamas Späher hatten den Arabischen Frühling nicht kommen sehen

nen durchkämmen können. Demnach gibt es unterschiedliche Sammelstrategien für unterschiedliche Phasen der Aufklärungsarbeit: Zu Beginn wird das Netz auf einer breiten Basis durchsucht. Neben Facebook, Twitter und Co. werden auch Nachrichtenseiten und Blogs nach bestimmten Schlüsselbegriffen im Zusammenhang mit Terrorismus und anderen Bedrohungen durchsucht. Ein Daten-Schleppnetz wird dabei über tausende Seiten ausgeworfen; was darin hängen bleibt, wird gespeichert. Die Auswertung dieser Daten, das so genannte Data-Mining, könne mit der Software fast in Echtzeit geschehen, so der Hersteller in seiner Broschüre. In späteren Phasen der Informationsbeschaffung könne man dann gezielter auf bestimmte Personen eingehen, die man so aufgespürt hat. So wäre es denkbar, dass in einer breit angelegten Suche ein Terrorist ausgemacht wird; das zöge dann eine gezielte Suche nach sich, um weitere Informationen zu dieser Person „aus internen und externen Quellen“ zu sammeln.

### Meinungsbild der Gesellschaft

Doch in den Datenbergen lässt sich neben der Suche nach Personen oder Organisationen noch mehr finden, was für Geheimdienste interessant sein könnte. Einige Beispiele dafür liefert regelmäßig die Forschungsabteilung von Facebook. Anhand von bestimmten Schlüsselwörtern in Statusmeldungen zur amerikanischen Gesundheitsreform konnten die Mathematiker und Statistiker genau vorhersagen, wer eher zum republikanischen und wer eher zum demokratischen Lager tendiert. Eine weitere Erkenntnis: Kongressabgeordnete, die mehr „Gefällt mir“-Angaben von den Facebook-Nutzern bekamen, gewannen in drei von vier Fällen einen Sitz bei den Wahlen von 2010. Wertvolle Erkenntnisse für die Politik.

Und auch für die Geheimdienste schlummert in diesen Daten ein großes Potenzial. Denn was in Amerika funktioniert, ist auch in anderen Ländern machbar. „Es ist über Facebook möglich, soziale Trends aufzuspüren und ein Meinungsbild der Gesellschaft zu erstellen“, sagt Erich Schmidt-Eenboom. So könnten zum Beispiel nicht nur Terroristen ins Visier genommen werden, sondern auch Gruppen wie Naturschützer oder Gewerkschaften, die sich im Internet organisieren. Und sollte die Stimmung in den sozialen Netzwerken einmal kippen, könnte es auch in der echten Welt zu Unruhen kommen.

Im Jahr 2011 konnte man eine solche Bewegung im Entstehen beobachten. Die Jasminrevolution in Tunesien und die Proteste auf dem Tahrir-Platz in Ägypten, bei der sich die Bürger gegen korrupte und despotische Regime wehrten, wurden im Nachhinein zu Twitter- und Facebook-Revolutionen umgedichtet. Auch wenn das zu viel der Ehre für die amerikanischen Unternehmen ist, so lieferten ihre Netzwerke doch die Infrastruktur, mit der sich die Bevölkerung organisieren konnte. Auf Facebook wurden die Versammlungen und Demonstrationen geplant und publik gemacht, auf YouTube und Twitter wurden die neuesten Nachrichten in die Welt gesendet, die im Unterschied zu den staatlichen Propagandasendern echte Bilder aus den besetzten Städten zeigten. Zumindest

die amerikanischen Dienste schienen unvorbereitet auf diese neue Form der Proteste. US-Präsident Barack Obama ließ seinem National-Intelligence-Direktor James Clapper Anfang 2011 ausrichten, dass er enttäuscht darüber sei, dass seine Späher den Arabischen Frühling nicht hatten kommen sehen.

### Diffamieren, manipulieren, infiltrieren

Was passieren kann, wenn Geheimdienste solchen sozialen Bewegungen im Internet auf die Schliche kommen, nennt Erich Schmidt-Eenboom „demokratiefährdend“. Denn sollte eine politische Bewegung den Herrschenden nicht in den Kram passen, könnten die Dienste nicht nur observieren, wie es die Amerikaner tun – sie könnten sich schon online aktiv an die Zersetzung der Bewegung machen.

Der britische GCHQ sei ein Beispiel dafür, so Schmidt-Eenboom. Dieser könnte nicht nur allgemeine Trends untersuchen, sondern auch Dossiers über Führungsfiguren innerhalb sozialer Bewegungen anlegen und versuchen, diskreditierende Informationen aufzuspüren. „Der GCHQ geht gezielt zu operativen Zwecken in die sozialen Netzwerke“, so Schmidt-Eenboom. Dazu zählten auch Diffamierung, Manipulation und das Einschleusen von Facebook-Spionen in die jeweiligen Gruppen. „Die Auswertung sozialer Netzwerke ist für die Dienste unglaublich wichtig. Das gibt der Geheimdienstarbeit eine ganz neue Qualität“, sagt der Geheimdienstexperte.

**Schlüsselworte in Statusmeldungen verraten die politische Gesinnung**

Welche Auswirkungen hat die Überwachung auf die observierten Gesellschaften? Dieser Frage geht Wolfgang Bonß, Soziologe und Professor an der Universität der Bundeswehr München, in einem von der EU-Kommission geförderten Forschungsprojekt („Increasing Resilience in Surveillance Societies“) nach. Bislang sind seine Antworten eher vorläufig. „Es zeichnet sich eine Überwachungsgesellschaft ab“, so Bonß. Schützen davor könne man sich nur, wenn man sich vom Internet ganz abkoppelt. „Aber das kann heute keiner mehr wirklich machen.“ Denn das Problem sei, dass heute kaum noch jemand ohne das Internet ein normales Privat- und Berufsleben führen könne. Verabredungen laufen über Facebook, der berufliche Austausch über E-Mail. Die Technik sei so nützlich und bequem, sagt Bonß, dass insbesondere die von ihm befragten jungen Menschen überhaupt keine Alternative dazu sehen. Sein Fazit: „Wenn man im Netz lebt, muss man immer damit rechnen, überwacht zu werden.“



Jan Guldner arbeitet als freier Wirtschaftsjournalist u.a. für *Handelsblatt*, *WirtschaftsWoche* und *ZEIT* in Köln.