Dies ist die Übersetzung eines Artikels, der unter der Überschrift “Cinco preguntas sobre el golpismo boliviano en Twitter” zuerst auf der kubanischen Website “Cubadebate” veröffentlicht worden war. Diese Webseite war von der Autorin Rosa Miriam Elizalde mitbegründet und bis 2017 geleitet worden. Inzwischen wurde der Artikel auf verschiedenen lateinamerikanischen Seiten und auch in Italien verbreitet. Der Artikel macht deutlich, mit welchen Dimensionen der Manipulation und des Cyberwars wir nach Meinung der Autoren in Zukunft zu rechnen haben, und gibt uns zumindest eine Vorstellung davon, auf was wir uns vorbereiten müssen. Die Übersetzung kommt von **Renate Fausten**. Albrecht Müller.

Zwei Monate nach dem Staatsstreich in Bolivien wird es offensichtlich, dass dieser minutiös geplant war und alle Eigenschaften des irregulären oder hybriden Krieges nach US-Zuschnitt in sich vereint.

Es handelt sich um einen Putsch, der die bekannten Modalitäten (militärische Aussagen und Repression) mit anderen neuen, hauptsächlich technologisch-kommunikativen Dimensionen kombiniert. Dabei sehen wir, dass der Putschismus Vorgänge materieller und virtueller Art miteinander verwoben hat, von psychologischen Operationen (PSYOPS) und anderen Techniken der sozialen Destabilisierung bis hin zu paramilitärischen Aktionen auf der Straße und der noch nie dagewesenen Aktion von Cybertruppen auf den digitalen Plattformen, durch die in Anlehnung an die Rhetorik Washingtons und den Interessen der Rechten der Region ein scheinbarer Konsens gegen die Regierung von Evo Morales geschaffen werden sollte.

Die Enthüllungen über die Cyberoperationen in den Netzen sind überwältigend. Verschiedene Forscher haben die Schaffung von Zehntausenden von falschen Konten in Twitter binnen kürzester Zeit dokumentiert, die die pro-putschistische Kampagne unterstützt haben. Zwei dieser Arbeiten sind besonders ergiebig und vermitteln eine Vorstellung, auf welch finstere Weise die sozialen Plattformen als Waffe der politischen Manipulation eingesetzt werden: „La resistencia boliviana no será transmitida“, (Der bolivianische Widerstand wird nicht übertragen) von einem Expertenteam der Bewegung Mueve América Latina und „Information Operations in Bolivia“ der US-Ermittlerin Erin Gallagher.

Trotzdem gibt es noch viele Fragen darüber, wie diese Art von Operationen in Twitter aufgebaut wird und wer die Verantwortlichen dafür sind. Wir wollen hier einige davon beantworten:

Fragen:

1. Kann man tausende falscher Konten mit einem gemeinsamen Narrativ, das den Staatsstreich in Bolivien unterstützt, ins Leben rufen, ohne dass Twitter dies sofort bemerkt?

Die Antwort lautet ja.

Bis dato ist es diversen Studien gelungen, die Schaffung von Tausenden von falschen Konten in den Tagen des Putsches in Bolivien zu dokumentieren. Die dabei benutzte Methode, um die Nachrichten zu kontaminieren, war hybrid. Sie kombinierte die digitale Aktion von:

a. realen Konten mit Bezug zu Politikern des Putschismus
b. Trolle (Cybertruppen mit authentischen Konten, die dazu gedacht sind, die Diskussion zu polarisieren)
c. Bots (teilweise oder total in ihren Interaktionen automatisiert)
d. reguläre Follower

Ab der zweiten Novemberwoche, als der Putsch bereits im Gange war, verbreitete und reproduzierte ein Netz von formalen und informellen Sprechern systematisch falsche Informationen (fake news) und Zeichen (hashtag) in den Netzen, um die Wahrnehmung einer überwältigenden Unterstützung der De-facto-Regierung von Jeanine Áñez und des Führers der extremen Rechten, Luis Fernando Camacho, im Innern des Landes zu erzeugen. In der Mehrzahl der Fälle handelte es sich dabei um Bots, d.h. nicht authentische Twitter-Konten, die automatisiert betrieben und benutzt wurden, um die putschistische Propaganda online und die Hasskampagnen gegen Evo Morales zu schüren.

Was wir in diesen Tagen gesehen haben, war eine kommunikative Operation mit doppeltem Zangengriff: Auf der einen Seite erzeugte die Rechte durch die Schließung der staatlichen und kommunalen Medien, die der Regierung nahestehen (Fernsehen, Radio und Printmedien), sowie der Verfolgung von Journalisten, die sich gegen den Putsch aussprachen, einen Nachrichtenausfall und auf der anderen Seite aktivierte man mittels Computational Intelligence, einem Zweig der künstlichen Intelligenz, einen lärmenden Hallraum zur Unterstützung des Putsches, der in wenigen Tagen über eine Million Tweets produzierte. Während man zur gleichen Zeit auf analoger Ebene die MAS zum Verstummen brachte, indem man deren Anhänger ohne Kommunikationsmedien zurückließ und sie so in ihrer Kommunikation zum Schweigen verurteilte, schuf man auf digitaler Ebene eine lautstarke Kampagne für den Putsch.

Es gibt keinen Zweifel, dass eine Gruppe von Personen oder sogar Staaten dahinterstanden

und dass man eine Armee politischer Robots in Twitter benutzte, um die Vorstellung einer Zustimmung auf breiter Ebene zu erzeugen. So erklärt z.B. in der erwähnten Untersuchung von Erin Gallagher die auf Studien der Desinformation in Twitter und Visualisierung von Daten spezialisierte Wissenschaftlerin, dass es wahrscheinlich reale Personen gab, die in den Tagen zuvor und während des Putsches neue Konten in diesem Datenpool erstellt hätten:

> „Die Ereignisse von Nachrichtenwert treiben reale Personen dazu an, neue Konten in den Plattformen der sozialen Netze zu erstellen und an öffentlichen Debatten teilzunehmen. Es erscheint mir jedoch äußerst unwahrscheinlich, dass all diese neuen Konten von realen Personen stammten“.

Fakt ist, dass das Konto von Luis Fernando Camacho, @LuisFerCamachoV, in nur ein paar Tagen (vom 3. November an) von 3.000 auf fast 135.000 Follower angewachsen ist, 15.000 davon entstanden an einem einzigen Tag. Im Fall der selbsternannten Áñez, @JeanineAnez, sieht es ähnlich aus: Sie stieg in wenigen Tagen von 9.000 auf 150.000 Follower an. Fast 100 Prozent dieser neuen Konten werden fast zu 100 Prozent gefolgt von anderen gerade erst erstellten Konten.

Das, was wir in Bolivien sehen, ist nichts völlig Neues. Es gibt zahlreiche Untersuchungen, die Propagandaoperationen in den Netzen durch die Nutzung nicht authentischer Konten und Bots (Software, die das menschliche Verhalten nachahmt), besonders in Twitter, dokumentiert haben.

Eine der jüngsten Untersuchungen erfolgte durch das NATO Strategic Communications Centre of Excellence (StratCom), das ein Experiment zur Manipulation, ausgehend vom Kauf falscher Profile auf verschiedenen Plattformen der sozialen Netze ((Facebook, YouTube, Instagram und Twitter), durchführte. In dem Bericht, der im Dezember 2019 verbreitet wurde, beschreibt die NATO, wie einfach diese Operationen der Propaganda sind. Sie versichert, dass zwischen 20 und 30 Prozent des Internetverkehrs reiner Schall und Rauch seien, der von Bots erzeugt werde, die absichtlich versuchen, diese Telekommunikationsunternehmen und die Nutzer zu verwirren. Eine der Schlussfolgerungen des NATO-Berichts ist die, dass von allen sozialen Netzen Twitter dasjenige ist, das die besten Maßnahmen ergriffen hat, um die Erstellung falscher Konten zu vermeiden. Wenn dem so ist, hat dieses soziale Netz das im Falle Boliviens vergessen.

Die Operationen von roher Gewalt in den Netzen sind im letzten Jahrzehnt in einer Art

digitalen Rüstungswettlaufs mit Produkten eskaliert, die es ermöglichen, das Informationsumfeld zu manipulieren. Sie spielten eine wichtige Rolle bei den Präsidentenwahlen in den USA im Jahr 2016, im Vereinigten Königreich beim Referendum über den Brexit, in Frankreich bei der Wahl von Emmanuel Macron, in Spanien beim Referendum über die Unabhängigkeit Kataloniens, im Argentinien Mauricio Macris, bei den „Guarimbas“ in Venezuela von 2014 bis 2017, in den mexikanischen Wahlen von 2018 und ganz kürzlich 2019 bei den Aktionen, um die Regierung des Präsidenten Nicolás Maduro zu stürzen.

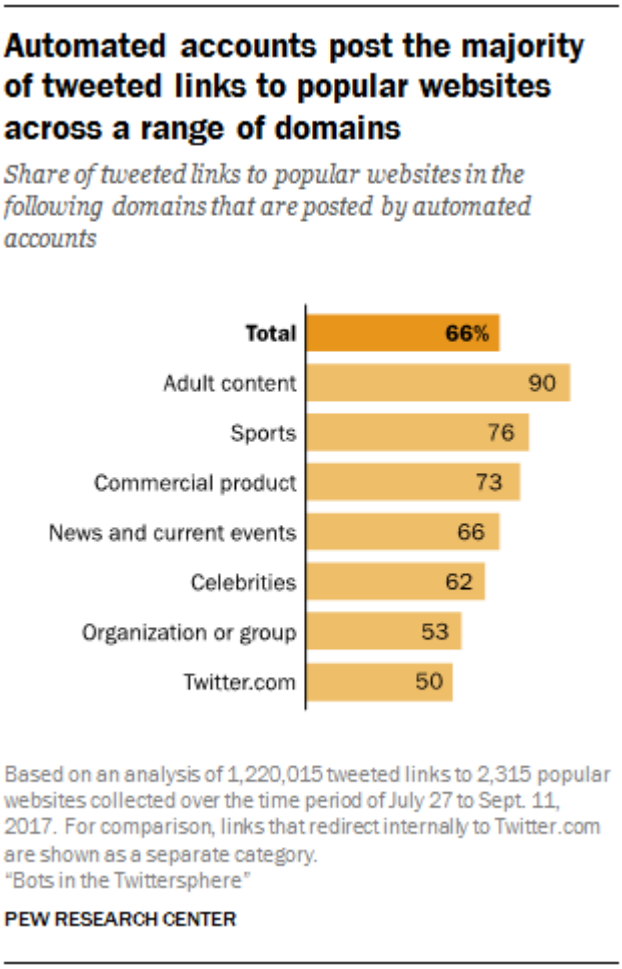
Der bemerkenswerteste Präzedenzfall dieser Strategien in Twitter geht auf das Jahr 2009 zurück, auf die sogenannte Grüne Iranische Revolution, die Hunderttausende von Twitter-Nutzern gegen die Regierung von Mahmud Ahmadineyad mobilisierte. Von den fast 100.000 Nutzern, die damals aktiv waren, sandten in den Tagen der Unruhen nur 60 ihre Tweets von Teheran aus, wie Evgeni Morozov berichtete, der dafür in seinem Buch „The Net Delusion. The Dark Side of Internet Freedom“ eine Studie von Al Jazeera anführt.

Die Beziehungen zwischen dieser Plattform und dem State Department waren bereits 2009 so eng, dass eine E-Mail von Jared Cohen, einem der Außenministerin Hillary Clinton untergeordneten Beamten, genügte, dass die Gesellschaft das Datum für eine geplante Pause zur Wartung der Website verschob, um die iranischen „Proteste“ nicht zu beeinträchtigen.

Im Fall des Iran richteten sich die nicht authentischen Konten und die Bots nach den Interessen Washingtons und erhielten dessen Segen, wie die New York Times versicherte. Philip J. Crowley, der stellvertretende Außenminister für öffentliche Angelegenheiten, verbreitete eine Mitteilung Cohens an Twitter und lobte die Folgsamkeit der Plattform mit folgenden Worten: „Dies war nur ein Anruf, um zu sagen: Es sieht so aus, als ob Twitter eine wichtige Rolle in einem für den Iran entscheidenden Moment spielt. Könnte es so weiter gehen?“. Der ehemalige Sicherheitsberater in der Regierung von George W. Bush, Mark Pfeifle, startete eine öffentliche Kampagne, um Twitter für den Friedensnobelpreis zu nominieren mit dem Argument, dass „ohne Twitter das Volk des Iran nicht die Kraft und das Zutrauen verspürt hätte, um für Freiheit und Demokratie zu kämpfen“.

Eine gemeinsame Studie der Universität von Southern California und der Universität von Indiana, die im März 2017 veröffentlicht wurde, bewies, dass die Bots während den Wahlen in den USA 2016 ernsthaft das politische Szenario vergiftet hätten. Diese Forscher schätzten, dass zwischen 9 und 15 Prozent der aktiven Twitter-Konten unter der Kontrolle von Robotern standen und dass mindestens 15 Prozent der Nutzer, die an den Diskussionen in den sozialen Netzen zur Kampagne, die Donald Trump ins Weiße Haus brachte,

teilnahmen, gefälscht waren. In diesem Jahr waren etwa 400.000 Bots für die ungefähr 3,8 Millionen Tweets verantwortlich, 19 Prozent des Gesamtvolumens der versendeten Botschaften.



Bei seiner Aussage vor dem US-Kongress wegen Einmischung in die Wahlen von 2016 ging Twitter davon aus, dass 5 Prozent seiner Konten automatisiert oder falsch seien, eine kleinere Zahl, als von unabhängigen Studien präsentiert, und wenig glaubhaft, wie die New York Times sagte. Mary Meeker, eine Spezialistin für digitale Tendenzen, schätzte ein, dass es sich bei 50 Prozent des weltweiten Online-Verkehrs, nicht nur bei Twitter, um Bots handelt. Eine unabhängige Studie des Pew Research Centers deckte auf, dass 66 Prozent der Botschaften, die Links zu Seiten mit Nachrichten, Sport oder Unterhaltung enthielten, von Bots veröffentlicht wurden.

„Es gibt Technologien, mit denen es möglich ist, sie zu entdecken, wie Bot Sentinel oder BorOrNot, aber mir macht Sorge, dass die ausgefeiltesten Roboter wahrscheinlich bereits

so entworfen wurden, um all diese Systeme zu besiegen“, sagt der BuzzFeed-News-Medieneditor Craig Silverman.

Wir wissen nicht, ob dies bereits Realität ist, aber wir wissen sehr wohl, dass man in Bolivien innerhalb von wenigen Tagen etwa 100.000 falsche Konten erstellt hat und dass ab dem 10. November (ein Tag vor dem Putsch) diese damit begannen, koordiniert genutzt zu werden, und die Retweets sowie die Anhänger des Putschismus exponentiell anstiegen.

Tatsächlich kann die Erstellung so vieler falscher Konten, wie dies in Bolivien geschah, vor sich gehen, ohne dass Twitter daran beteiligt ist, aber es ist unmöglich, wie wir in Frage 3 sehen werden, dass diese Gesellschaft davon nichts erfahren hat.

2. Wurde bei dieser Kampagne Technologie der letzten Generation von Künstlicher Intelligenz benutzt? Die Antwort ist ja.

Auch wenn es verschiedene Auffassungen darüber gibt, wie die Hunderttausende von nicht authentischen Konten geschaffen wurden, gehen einige konsultierte Spezialisten davon aus, dass das Volumen und die Geschwindigkeit, mit der diese aktiviert wurden, die Möglichkeiten einer typischen Farm von Trollen, die die häufigste Methode darstellt, um falsche Profile auf dem Untergrundmarkt der Manipulation der Netze zu verwalten, bei weitem überschreiten.

Die Struktur der falschen Konten zeigt Regelmäßigkeiten, die sie herausheben: die Koordinierung – temporal und thematisch – von Zehntausenden politischen Profilen in einem in Lateinamerika nie dagewesenem Ausmaß; der enorme Umfang der im November plötzlich erstellten Konten in einem Land mit niedriger Twitter-Beteiligung – nur 2,8 Prozent der Internetnutzer waren im Oktober 2019 auf dieser Plattform – gemeinsame Identifizierungsmuster der Nutzer, Verzeichnisse von Personenfotos, die real erscheinen, und die Automatisierung multipler Aufgaben in derselben Sekunde offenbaren die Benutzung von Systemen Künstlicher Intelligenz der letzten Generation mit Megaphon-Effekt und der Fähigkeit, Propaganda in großem Ausmaß in sehr kurzer Zeit zu verbreiten.

Die Trollfabriken verfügen über eine Methodologie, die es ihnen ermöglicht, die Kontrollsysteme von Twitter, die in der folgenden von der Tageszeitung El País ausgearbeiteten Infografik beschrieben werden, zu täuschen, indem jeder (menschliche) Troll zwischen 10 und 15 automatische Profile (bots) mit sorgfältig fabrizierten und verwalteten Identitäten steuert, die häufig so gestaltet sind, dass sie ihr Zielpublikum widerspiegeln.

In den leistungsfähigsten bis jetzt beschriebenen Trollfabriken arbeiten nicht mehr als 60 Angestellte. Sie passen sich an das Registrierungssystem von Twitter an, das die Nutzer dazu verpflichtet, sich beim ersten Mal unter einer einzigen E-Mail-Anschrift oder einer mobilen Telefonnummer einzutragen, mit der höchstens 10 Konten verbunden sein können. Die effektivsten Netze von Bots, die die öffentliche Diskussion in den sozialen Netzen manipulieren, operieren in Kombination mit automatisierten Konten und Cyborg, d.h. realen Personen, die sich hinter diversen falschen Konten verstecken.

Lassen Sie uns von diesen Daten ausgehend eine einfache mathematische Rechnung machen. Julián Macías Tovar identifizierte über 60.000 falsche Konten, die von einem der Hauptputschisten unterstützt wurden. Luis Fernando Camacho (@LuisFerCamachoV). Mit der Methode der Trollfabriken benötigte man mindestens 6.000 Angestellte, die 60.000 Mails aktivieren und über wenigstens 6.000 Telefonnummern verfügen, um diese Konten aufrechtzuerhalten.

Es ist möglich, im Internet so viele falsche Briefkästen zu schaffen, wie man möchte, und Telefonlinien im Internet für einen Dollar zu kaufen, aber bis jetzt muss die Registrierung der Konten individuell in einer zeitlich linearen Abfolge vor sich gehen. Die Beweise, die verschiedene Experten zu dieser Operation beigetragen haben, brechen mit dieser Logik.

Wenn man die Daten der bolivianischen Kampagne direkt von der API von Twitter aus betrachtet, kann man besser das Ausmaß der Automatisierung und Wiederholung sehen, das zu der Zeit stattfand, als sich die Nutzer registrierten.

Diese Sequenz zeigt beispielsweise die Wiederholung desselben Musters im Namen einer Kontengruppe, die größtenteils am 11. November 2019 erstellt wurde. Das Bild trug der argentinische Wissenschaftler Luciano Galup bei, der Autor des Buches „Big data & Política: De los relatos a los datos. Persuadir en la era de las redes sociales“, der dieses Bild am 12. November über Twitter verschickte:

PATRICI16364733	11/11/19
Patrici23897455	11/11/19
Patrici31596429	11/10/19
Patrici31762285	11/11/19
Patrici36731862	11/11/19
Patrici39596764	11/10/19
Patrici39721142	11/11/19
Patrici45238968	11/10/19
Patrici46327255	11/11/19
Patrici46465456	11/10/19
Patrici51552884	11/09/19
Patrici79156755	11/11/19
Patrici95661406	11/02/19
Patrici97475950	11/11/19
Tania04519732	11/10/19
Tania27589115	11/11/19
Tania32718587	11/10/19
Tania40406655	11/11/19
Tania71395531	11/10/19

Javier Barriuso vom Internet-Team von Podemos in Castilla-La Mancha, Spanien,

identifizierte 31 Konten zur Unterstützung des Putsches, die in der gleichen Sekunde erstellt wurden, und kommentierte dies folgendermaßen: „Es ist offensichtlich, dass hinter alldem nicht eines der vielen Unternehmen steckt, die Konten verkaufen, das ist ein dickerer Fisch mit größerer Infrastruktur“.

Noelia22583323	11-11-19 14:42
Katheri39538908	11-11-19 14:42
KatiaCaceres6	11-11-19 14:42
FreddyLC2	11-11-19 14:42
MarcoGo88296596	11-11-19 14:42
HerbasRu	11-11-19 14:42
Liliana37663182	11-11-19 14:42
Andreu52346773	11-11-19 14:42
nathaly59851761	11-11-19 14:42
PatriciaBedreg2	11-11-19 14:42
JMQ_02	11-11-19 14:42
JuanCar02539426	11-11-19 14:42
becky_v81	11-11-19 14:42
MariaEu48815089	11-11-19 14:42
GerardoNicolsC2	11-11-19 14:42
laida_molina	11-11-19 14:42
EdwinFi83597725	11-11-19 14:42
galizcl	11-11-19 14:42
P_Gab13	11-11-19 14:42
Dayan00276672	11-11-19 14:42
ValeriaBassWer1	11-11-19 14:42
Paolarosprado1	11-11-19 14:42
MiguelA86632861	11-11-19 14:42
BelfordGuthrie	11-11-19 14:42
JosCarolina1	11-11-19 14:42
CarlaVedia2	11-11-19 14:42
Cristop15014915	11-11-19 14:42
LijeronRaquel	11-11-19 14:42
valda_erick	11-11-19 14:42
KarenCastroTer1	11-11-19 14:42
Fabriziolc2	11-11-19 14:42

Unter den signifikantesten Daten, die aus diesen Konten hervorgingen, die die wichtigsten Putschisten und ihre Einrichtungen unterstützen, fallen die schwindelerregenden Sprünge der Konten auf, wie die vom Komitee Pro Santa Cruz: von fast 0 Followern auf 43.422 am

30. Oktober.

Die Kirsche auf diesem Kuchen ist das Konto @suarezluis, das Luis Fernando Suárez Harasic gehört. Er stellt sich als in Cochabamba/Bolivien geborener Programmierer der US-Armee vor. Julián Macías Tovar war der Erste, der auf die ungeheuerliche Aktivität des Nutzers hinwies. Rubén Rodríguez Casañ, spanischer Physiker und Datenwissenschaftler, legte wenig später den deutlichsten Beweis für die Automatisierung der Retweets vor.

@suarezluis ist in der Lage, in derselben Sekunde 69 Mal zu retweeten, was der Richter Rodríguez Casañ als einen Beweis dafür ansieht, dass „das Paradigma der Nachrichtenverbreitung sich ändert“.

Wenn man beispielsweise das Verhalten von 14 Hashtag zugunsten des Putsches analysiert, sieht man, dass die Putschgemeinde die dichteste in Twitter ist und dass das Konto @suarezluis der wichtigste Zulieferer und Verteiler ist. Von ihm aus werden 13.578 Tweets gesendet. Es fällt auf, dass er seine eigene App hat, um die Retweets zu automatisieren und sie automatisch abzusenden, Auf diese Weise schafft er 3.000 Retweets pro Tag und er machte in weniger als fünf Tagen über 14.000 Retweets zur Unterstützung des Putsches.

Das bedeutet, dass wir Zeugen der Umsetzung eines automatisierten Systems waren, das alle, die ihm folgen, retweetet und bestimmte Hashtags erwähnt, und dessen Aktivität und Kapazität die Höchstbegrenzung der Tweets pro Tag überschreitet, die laut Twitter offiziell möglich sind. Mit diesem eigenen Werkzeug gelang es dem Programmierer der US-Armee, die falsche Information im Internet in Umlauf zu bringen, die sich fließend ausdehnte und den Putsch stützte.

TOP	Fecha de Publicación	Hora	Número de tweets
1	20/11/2019	14:03:52	69
2	20/11/2019	15:34:17	66
3	20/11/2019	1:16:31	62
4	20/11/2019	18:34:17	56
5	20/11/2019	20:04:18	52
6	21/11/2019	5:56:43	52
7	21/11/2019	7:06:52	52
8	19/11/2019	22:16:30	45
9	20/11/2019	4:16:32	45
10	20/11/2019	21:34:18	41

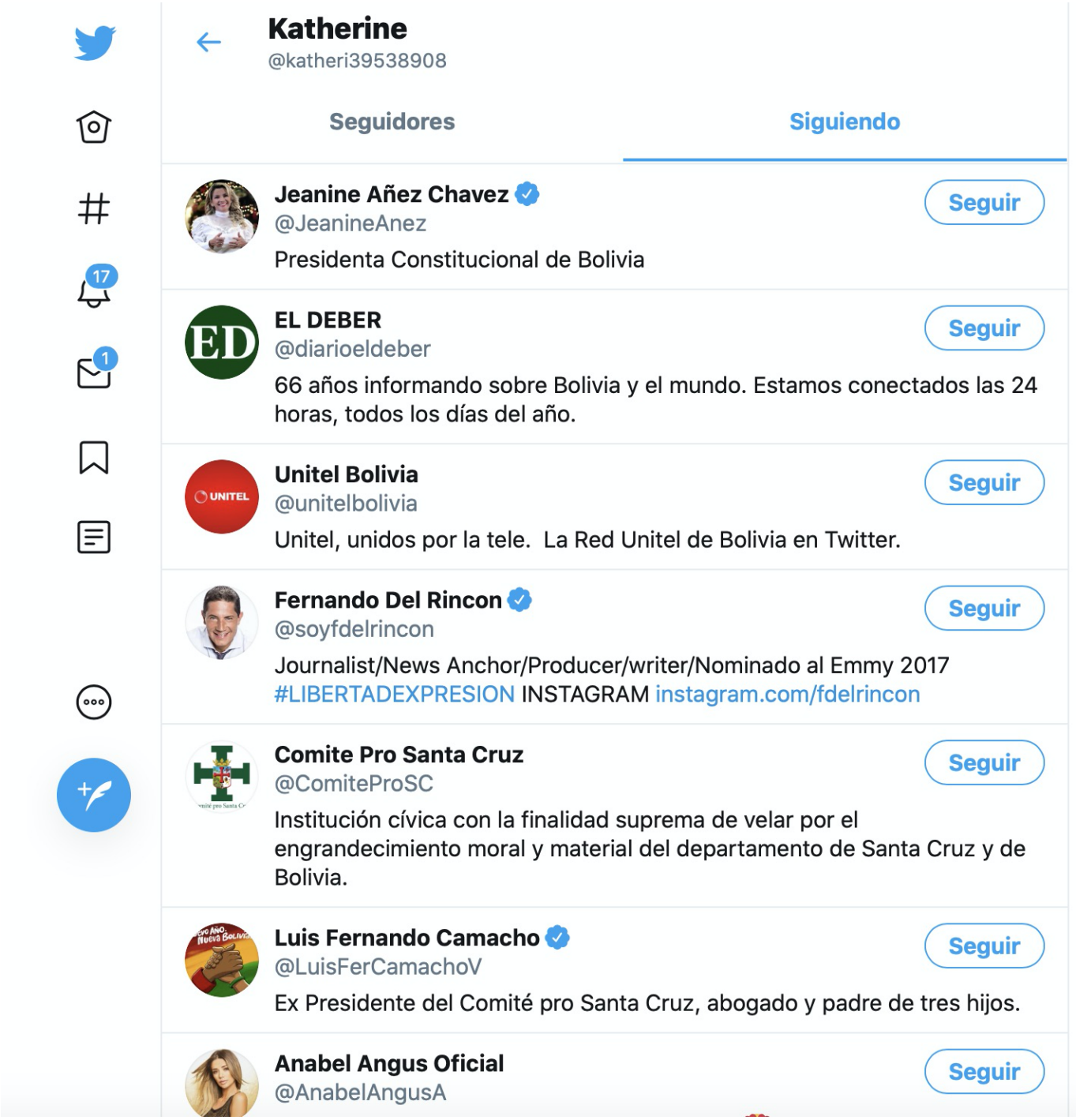
Ein zusätzliches Detail: Viele der falschen Konten, denen niemand folgt und die in den ersten zehn Novembertagen erstellt wurden, erscheinen mit eigenem Foto, eines der entscheidenden Charakteristiken, um die Glaubwürdigkeit eines Profils zu bewerten. Die in automatisierten Operationen geschaffenen Konten fallen dadurch auf, dass sie mit dem Avatar erscheinen, den Twitter standardmäßig erzeugt.

Im Falle Boliviens erscheinen die in derselben Sekunde geschaffenen Konten mit eigener Fotografie und Beschreibung des Nutzers:


Landy
0 Tweets
14
1
Seguir
Landy
@Landy33272574
espontánea
Se unió el noviembre de 2019
27 Siguiendo
5 seguidores


Paty
6 Tweets
14
1
Seguir
Paty
@Paty09522501
hija de Dios
Se unió el noviembre de 2019
48 Siguiendo
5 seguidores
Ninguna de las cuentas que sigues siguen a este usuario


Katherine
0 Tweets
17
1
Seguir
Katherine
@Katheri39538908
Se unió el noviembre de 2019
9 Siguiendo
2 seguidores
Ninguna de las cuentas que sigues siguen a este usuario


Katherine
@katheri39538908
Seguidores
Siguiendo
Jeanine Añez Chavez
@JeanineAnez
Presidenta Constitucional de Bolivia
Seguir
EL DEBER
@diarioeldeber
66 años informando sobre Bolivia y el mundo. Estamos conectados las 24 horas, todos los días del año.
Seguir
Unitel Bolivia
@unitelbolivia
Unitel, unidos por la tele. La Red Unitel de Bolivia en Twitter.
Seguir
Fernando Del Rincon
@soyfdelrincon
Journalist/News Anchor/Producer/writer/Nominado al Emmy 2017
#LIBERTADEXPRESION INSTAGRAM instagram.com/fdelrincon
Seguir
Comite Pro Santa Cruz
@ComiteProSC
Institución cívica con la finalidad suprema de velar por el engrandecimiento moral y material del departamento de Santa Cruz y de Bolivia.
Seguir
Luis Fernando Camacho
@LuisFerCamachoV
Ex Presidente del Comité pro Santa Cruz, abogado y padre de tres hijos.
Seguir
Anabel Angus Oficial
@AnabelAngusA
Seguir

Bilder von Personen, die real erscheinen, aber von einer Software entworfen wurden.
Foto: Cubadebate

Es ist kein Geheimnis, dass man mit den Fähigkeiten der aktuellen PCs hyperrealistische Bilder kreieren kann. Philip Wang, Software-Ingenieur bei Uber, schuf die Website ThisPersonDoesNotExist.com, die mithilfe eines Algorithmus, der darauf trainiert ist, auf einer Datenbasis von realen Portraits, jedes Mal, wenn er das Web aktualisiert, ein falsches Gesicht zu schaffen. Stehen wir vor etwas Ähnlichem?

Eine Untersuchung der Zeitschrift Vice über Bots in der Politik warnte vor zwei Jahren vor den Möglichkeiten, die die Skalierung in der Informationstechnik für die Manipulation bietet:

> „Dieselbe Technologie, die es ermöglicht, dass die Maschinen die menschliche Sprache verstehen und in ihr kommunizieren können, kann und wird benutzt werden, um zu erreichen, dass die Bots der sozialen Netze noch glaubwürdiger werden. Anstatt dem, der sie hören möchte, kurze und einfache Botschaften zu senden, werden diese Bots kohärente Gespräche mit anderen Nutzern führen und dabei eine unendliche Geduld aufbringen, um zu debattieren und zu überzeugen. Sie können sich auch programmieren, um die in diesen Gesprächen erhaltene Information zu sammeln, zu speichern und in einer späteren

> Kommunikation zu benutzen …
>
> Die Menschen haben schon Schwierigkeiten, relativ einfache Text-Bots zu erkennen, die als echte Benutzer getarnt sind. Diese Fortschritte beim maschinellen Lernen werden den Propagandisten noch mehr Macht geben, um die Öffentlichkeit zu manipulieren."

3. Ist Twitter ein Komplize bei diesen Operationen? Die Antwort ist ja.

Trotz Beschwerden der Öffentlichkeit hat Twitter die Mehrzahl der Hunderttausenden von nicht authentischen Konten, die den Putschismus in Bolivien unterstützen, nicht entfernt. Es ist eindeutig nicht möglich, dass die Plattform diese illegalen robotischen Aktivitäten nicht bemerkt oder davon erfahren hat. Sie weiß außerdem genau, wer diejenigen sind, die die Operation entwickelt und organisiert haben, denn diese müssen sich zuvor einer Registrierung unterziehen, um Zugang zum API zu erhalten, was es ganz einfach machen würde, all dies mit einem Klick zu zerstören.

Außer den Kubanern – für die diese App von der Gesellschaft für die Insel blockiert wurde – kann nahezu jeder ein Profil des „Entwicklers" eröffnen, auch wenn das Unternehmen 2018, nachdem es bei einer Anhörung vor dem US-Kongress aussagen musste, bei der es zugab, Daten an Global Science Research (GSR) von Aleksandr Kogan verkauft zu haben, die Regeln verschärfte. Diese Gesellschaft lieferte Informationen von bis zu 87 Millionen Facebook-Nutzern an Cambridge Analytica, das Unternehmen, das in den größten Skandal politischer Manipulation in den letzten Jahren verwickelt war und Zugang zu den Informationen von wenigstens 5 Millionen Twitter-Nutzern hatte.

Jetzt sagt das Unternehmen, „dass strenge Richtlinien und Prozesse eingehalten werden, um zu bewerten, wie Entwickler Twitter-Daten verwenden, und um die unangemessene Nutzung dieser Daten einzuschränken". Es gibt jedoch vernünftige Schritte, die Nutzer, Forscher und Organisationen gefordert haben, um die Informationen transparent zu machen, die die Plattform nicht beachtet hat, wie das Etikettieren von Bots und die Warnung an die Öffentlichkeit, dass es sich um automatisierte Konten handelt.

Das Oxford Internet Institute (OII) der Oxford-Universität veröffentlichte 2017 verschiedene Studien über Bots und Cybertruppen in 28 Ländern und kam zu dem Schluss, dass die technologischen Plattformen in den USA weder über die computerisierte Propaganda informieren noch dagegen vorgehen, denn damit würden sie „ihr Erfolgskonto einem Risiko aussetzen".

In einem anderen der OII-Berichte des Jahres 2017 mit dem Titel „Computational Propaganda in the United States of America: Manufacturing Consensus Online", berichten Samuel C. Woolley von der Oxford-Universität und Douglas R. Guilbeault von der Universität von Pennsylvania über die Ergebnisse der Analyse über die Automatisierung der Twitter-Botschaften während den Wahlen in den USA 2016. Sie kamen zu dem Schluss, dass die zahlenmäßige Stärke der Bots in dieser Plattform es jedem mit ein paar Kenntnissen von Verschlüsselungen oder mit Verbindungen zu Gruppen, die automatisierte Software benutzen, es ermöglichen würde, ihr eigenes Propagandanetz zu schaffen.

„Die Frage, ob die Wahlkampfteams politische Bots benutzen, um Fake News zu verbreiten, war und ist weiterhin ein schwerwiegendes Problem der US-Politik … Aber man neigt dazu, die Tatsache zu ignorieren, dass jeder in Twitter einen Bot kreieren und falsche Nachrichten online verbreiten kann. Es waren diese von Bürgern erstellten Roboter, die wahrscheinlich am meisten die Propaganda, die Fake News und die politischen Angriffe der Wahlen 2016 anwendeten", und die Wissenschaftler fügen hinzu:

> „Unser auswertender Bericht gibt Anlass zu glauben, dass Twitter wesentlich am Erfolg Trumps beteiligt war … Aber das Unternehmen zögert jedoch, die Benutzer zu warnen. Es befürchtet, dass die Benachrichtigung über die von den Bots ausgehenden Bedrohungen die Nutzer davon abhalten würde, wegen der Gefahr der allgegenwärtigen Computerpropaganda und der Unannehmlichkeiten, die solche Warnungen mit sich bringen, dessen Dienstleistungen in Anspruch zu nehmen".

„Die Bots sind das letzte Glied in der Kette", sagt der Mexikaner Alberto Escorcia, ein Experte für Desinformationsoperationen und Herausgeber des Blogs LoQueSigue. „Die größte Verantwortung dafür liegt bei Twitter, denn es hat die Ressourcen, diese falschen Konten zu entdecken und zu blockieren". Und er fügt hinzu: „Da die Bots aber den technologischen Unternehmen Millionen von Dollar an Werbeeinnahmen bringen, zeigt das Unternehmen wenig Ehrgeiz, Maßnahmen gegen sie zu ergreifen".

4. Gibt es Beweise für Cybertruppen und militärische Strukturen in den USA, die in der Lage sind, eine Operation wie die in Bolivien zu organisieren? Die Antwort lautet ja.

Die Entdeckung eines Roboters, der von einem Programmierer mit militärischer Ausbildung und Verbindung zur US-Armee koordiniert wird, ist nicht der einzige Beweis, den die investigativen Wissenschaftler beitrugen, die diese Geschichte von falschen Konten und

computerisierter Propaganda, um den Putsch in Bolivien zu legitimieren, dokumentiert haben. Die Planung, die Koordinierung, das Ausmaß und die Reichweite dieser Operation weisen auf das vom Oxford Internet Institute dargestellte Konzept der „Cybertruppen“ hin, in dem ausführlich die Benutzung dieser Art von Strukturen in den Vereinigten Staaten mit weltweiten Folgen dokumentiert wurde:

> „Die kybernetischen Truppen sind Ausrüstungen von Regierungen, Militärs oder politischen Parteien, die die Manipulierung der öffentlichen Meinung in den sozialen Netzen zum Ziel haben.“

Die Forscher von OII legten die außergewöhnliche Rolle offen, die die Institutionen der USA und ihrer wichtigsten politischen Akteure der Anwendung der automatisierten Systeme in Konfliktsituationen einräumen. „Eine der wichtigsten Beobachtungen, die man aus dieser Analyse ziehen kann, ist die, dass die Bots sich hinter den Kulissen in ein akzeptiertes Werkzeug für die politische Aktivität verwandelt haben, und sie sind ein ausgezeichnetes Beispiel für die neue Ära der computerisierten Propaganda“, bestätigen Woolley und Guilbeault.

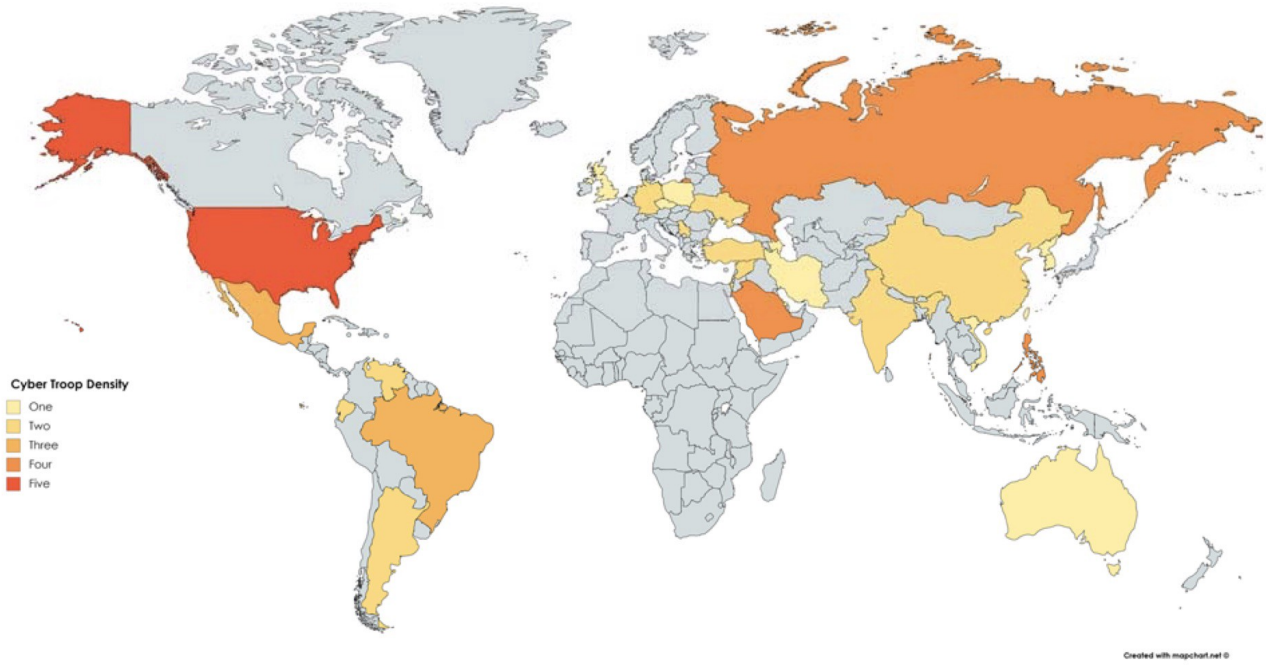
Die wichtigste Methode, um die kybernetischen Truppen zu organisieren, lief über die Miteinbeziehung der militärischen Einheiten, die mit der Manipulation der öffentlichen Meinung über die sozialen Netze arbeiten, und der Unternehmen der strategischen Kommunikation, die Regierungsverträge für Kampagnen in den sozialen Netzen übernehmen. Aber von allen von OII untersuchten Ländern waren die Vereinigten Staaten das Land mit der größten organisatorischen Kapazität für automatisierte Propagandakampagnen im Netz.

Laut der Universität Oxford verfügt die Regierung der Vereinigten Staaten in der US Agency for International Development (USAID), dem Ministerium für Nationale Sicherheit und dem Außenministerium (es schuf 2017 das Global Engagement Center) und verschiedenen Filialen des Verteidigungsministeriums, darunter DARPA, US Cyber Command und die Luftstreitkräfte (insbesondere CentCom), über aktive Cybertruppen für nationale und internationale Operationen. Außerdem beschäftigt sie Fremdfirmen wie Ntrepid und HBGary Federal.

Auf der Karte „Organisatorische Dichte der Cybertruppen 2017“ platziert OII die USA, was Cybertruppen betrifft, die in diverse Strukturen der Gesellschaft eingreifen (Regierung, politische Parteien, Gruppen der Zivilgesellschaft, Bürger und unabhängige

Auftragnehmer), auf Rang fünf, den höchsten Rang.

Figure 1: Organizational density of cyber troops, 2017



Auch sind die USA das Land, das am meisten in die Forschung, Entwicklung und Innovation auf Gebieten wie „Netzwerkeffekte“ investiert, um die Botschaften über die sozialen Medien auszudehnen und zu verstärken, und sie benutzen dazu öffentliche Gelder. So finanzierte z.B. die Defense Advanced Research Projects Agency (DARPA) eine Studie mit 8,9 Millionen USD über die Einflussmöglichkeiten der sozialen Medien, welche die Nachverfolgung der Antworten der Benutzer auf die Online-Inhalte einschloss.

DARPA veröffentlichte eine lange Liste von Projekten, die unter seinem Programm Social Media in Strategic Communication (SMISC) finanziert wurden, mit Links zu Dokumenten und echten Übersichten. Die Liste der Projekte enthält eine Studie darüber, wie Aktivisten der Bewegung „Occupy“ Twitter benutzt haben, sowie eine Reihe von Untersuchungen über das Tracking von Memes im Internet und andere über die Aktivität von Nutzern und der Einflussmechanismen („Gefällt mir“, Folgen“, „Retweeten“) in einer Reihe der beliebtesten Plattformen der sozialen Netze.

„The Guardian“ seinerseits dokumentierte die Benutzung einer äußerst ausgefeilten Software für „Astroturfing“, einer Marketingtechnik, die darin besteht, den wirklichen Absender einer Werbe- oder Propagandabotschaft zu verbergen. Zu diesem Zweck hat das

Pentagon die Firma für Cybersicherheit HBGary Federal, eine Tochtergesellschaft von HBGary, unter Vertrag genommen, die nur Produkte an die US-Regierung verkauft.

Laut „The Guardian“ hat diese Software folgende Eigenschaften:

- Sie schafft alle Online-Elemente, die eine reale Person benötigen würde, um in einem sozialen Netz aktiv zu werden: einen Namen, E-Mail-Konten, Websites und soziale Netze. Mit anderen Worten, sie erzeugt automatisch etwas, das aussieht wie authentische Profile, so dass es schwierig wird, zwischen einem Roboter und einem Menschen zu unterscheiden.

- Die falschen Konten können aktualisiert werden und den in ihrem Profil erstellten Inhalt automatisch mit einem anderen Netzwerk verknüpfen, was den Eindruck verstärkt, dass die Konteninhaber reale und aktive Personen sind.

- Dem in die Operation eingebundenen Cybertruppenmitglied können diese „(vor-)gealterten“ Konten zugewiesen werden, damit er sich eine Hintergrundgeschichte ausdenkt, die darauf hindeuten soll, dass man schon seit Monaten damit beschäftigt ist, Links zu setzen und zu retweeten. Niemand käme auf die Idee, dass sie gerade einen Augenblick zuvor zum ersten Mal in Aktion traten, einzig zu dem Zweck, einen Benutzer im Netz anzugreifen oder Propaganda zu verbreiten.

Die aber möglicherweise beunruhigendste Enthüllung ist die von Computing World. Das auf dem Luftwaffenstützpunkt Mac Dill (Tampa, Florida) gelegene United States Central Command (CentCom) veröffentlichte die Ausschreibung für private Unternehmen oder solche, die beim Pentagon unter Vertrag stehen, Software zu liefern, die folgende Aufgaben erfüllt:

a. „10 falsche Identitäten (sock puppet) für reale Nutzer erstellen, mit Vorgeschichte, Hintergrunde, Support Details und Cyber-Präsenzen, die technisch, kulturell und geografisch konsistent sind … Die Personen sollten fast überall auf der Welt erscheinen und über die konventionellen Online-Dienste und Plattformen der sozialen Netze interagieren können.“
b. Den Cybertruppen automatisch „IP-Adressen zur Verfügung stellen, die zufällig ausgewählt werden und über die sie ins Internet gehen können“. (Eine IP-Adresse ist die Nummer, die den PC von irgendjemanden identifiziert und diese muss jeden Tag geändert werden, um so die Existenz der Operation zu verbergen.) Die Software soll auch den Internetverkehr von Cyberkämpfern mit dem „Verkehr der Massen von

Nutzern außerhalb der Organisation“ miteinander vermischen.

c. „Statische IP-Adressen“ für jede Person erstellen, um es so zu ermöglichen, dass verschiedene Cyberkämpfer „im Laufe der Zeit wie dieselbe Person aussehen“. Es sollte möglich sein, dass „die Organisationen, die oft dieselbe Seite oder denselben Dienst nutzen, ganz einfach oft die IP-Adressen wechseln können.

CentCom bestätigte, dass der Vertrag über 2,76 Millionen Dollar an Ntrepid gegangen sei, eine vor kurzem gebildete Korporation, die in Los Angeles eingetragen ist Es wurde nicht bekannt, ob das Projekt der multiplen Person bereits durchgeführt wird.

Der CEO von Ntrepid ist Richard Hollis Helms, ein ehemaliger CIA-Agent, der die Europa-Abteilung der CIA leitete und nach dem 11. September 2001 einen Geheimdienst gründete, der Auftragnehmer für Geheimoperationen im Mittleren Osten zur Verfügung stellte.

Der Vertrag ist Teil eines Programms mit der Bezeichnung Operation Earnest Voice (OEV) mit einem Etat von 200 Millionen Dollar und wurde zum ersten Mal im Irak als Waffe des psychologischen Krieges gegen die Online-Präsenz der Parteigänger von Al-Quaida eingesetzt. General David Petraeus, der bei der Invasion im Irak Kommandant von CentCom war, beschrieb die Operation als eine Anstrengung, um „der extremistischen Ideologie und Propaganda Einhalt zu gebieten und sicherzustellen, dass die glaubhaften Stimmen in der Region sich Gehör verschaffen“.

5. Haben die Vereinigten Staaten die juristischen Werkzeuge, um eine Operation in den Netzen, wie die in Bolivien, zu rechtfertigen? Die Antwort ist ja.

Das Smith-Mundt-Gesetz der Modernisierung aus dem Jahr 2012 legt fest, dass die Verbreitung von eigener Propaganda für ein ausländisches Publikum im Internet, die sozialen Netze eingeschlossen, ausdrücklich erlaubt wird. Dieses Gesetz hebt auch das Verbot auf, in den USA Propaganda zu verbreiten, die ausschließlich für das Ausland hergestellt wird (wie die Sendungen von Radio und TV Martí für den „Regime Change“ in Kuba).

Das Information Law der USA und der Educational Exchange Act von 1948 (Public Law 80-402), allgemein unter dem Namen Smith-Mundt-Gesetz bekannt, stellt die gesetzliche Grundlage für die Genehmigung der vom US-Außenministerium durchgeführten Propagandaaktivitäten dar, die auch als „öffentliche Diplomatie“ bekannt sind.

Der Cybersecurity Information Sharing Act (CISA) erlaubt verschiedenen Abteilungen der US-Regierung, persönliche Daten von Benutzern anzufordern, ohne zuvor die Zustimmung

eines Richters erhalten zu haben. Es gewährt den Unternehmen größeren Schutz der Regierung, was die Sicherheit angeht, wenn sie sich entschließen, ihre Informationen mit dem Ministerium für Innere Sicherheit zu teilen, um zu versuchen, „die kybernetische Sicherheit der Vereinigten Staaten zu verbessern“. Das Gesetz wurde am 18. Dezember 2015 von Barack Obama genehmigt.

Das Gesetz autorisierte die Schaffung eines Systems von Informanten von Unternehmen, die Daten ihrer Klienten dem Ministerium für Innere Sicherheit (DHS) weiterleiten, was seinerseits diese Informationen mit anderen staatlichen Agenturen teilt, wozu auch die Ministerien für Handel, Verteidigung (oder das Pentagon, das die NSA einschließt), Energie, Justiz (mit FBI), Finanzen (das vom IRS [Internal Revenue Service] überwacht wird) und das Office of the Director of National Intelligence gehören.

Nachdem diese Nachricht bekannt wurde, veröffentlichte Edward Snowden auf seinem Twitter-Konto eine Botschaft: „Bericht: Die Banken und die Telekommunikationsunternehmen sind jetzt glücklicher mit CISA, während die Leute sich betrogen fühlen“.

Die präsidiale Verfügung 12333 gibt dem Präsidenten der Vereinigten Staaten die Macht, die nationalen Sicherheitsprogramme vollständig zu kontrollieren, darunter auch die Operationen der NSA sowie unter anderem das Sammeln digitaler Informationen und Untersuchungen des Datenzentrums innerhalb und außerhalb des Landes. Es wurde 1981 von Präsident Ronald Reagan unterzeichnet.

Artikel 702 des Foreign Intelligence Suveillance Acts FISA: Der Kongress autorisierte im Januar 2019 erneut diesen Artikel, der die Überwachung von ausländischen Personen und Einrichtungen erlaubt. Er autorisierte außerdem wiederum für einen Zeitraum von sechs Jahren die NSA, Millionen von Telefonanrufen und elektronische Kommunikation von US-Bürgern, darunter auch E-Mails, Facebook-Einträge und Browserverläufe, ohne richterlichen Beschluss zu sammeln.

Das Gesetz gestattet es auch, dass das FBI auf die Datenbasis der NSA ohne Gerichtsbeschluss Zugriff hat, was Kritiker wie der demokratische Senator Ron Wyden „eine Hintertür zur Aufhebung des Vierten Zusatzartikels zur Verfassung“ bezeichnen. Technisch gesehen erlaubt das Gesetz nur die Zusammenstellung von Kommunikation ausländischer Personen, aber die Bürger und diejenigen mit ständigem Wohnsitz sind bei der Benutzung des Internets nicht geschützt. So können beispielsweise die US-Bürger, die mit Ausländern in Verbindung stehen, darin eingeschlossen werden.

The Clarifying Lawful Overseas Use of Data Act (CLOUD) von 2018 verpflichtet auf der einen Seite die US-Internetanbieter, alle Daten in ihrem Besitz oder unter ihrer Kontrolle offenzulegen, wenn dies von den Behörden gefordert wird, auch wenn die Daten in Drittländern angesiedelt sind.

Auf der anderen Seite stellt das Gesetz auf Grundlage schwerwiegender Delikte für bestimmte ausländische verbündete Regierungen einen Mechanismus zur Verfügung, mit dem sie Zugang zu den Inhalten der Kommunikation von Nicht-US-Bürgern beantragen können, über die US-Internetanbieter verfügen und die auch im Ausland angesiedelt sind.

Der 2013 von der Bot Remediation Working Group vorgeschlagene Anti-Bot Code of Conduct ist der einzige Versuch, um die Benutzung des PC für Propaganda zu kontrollieren, aber er hat keine Gesetzeskraft und die Unternehmen sind nicht verpflichtet, ihn einzuhalten.

Die Nutzung der Kommunikation als politische Waffe ist eine gut dokumentierte historische Realität. Das aktuell Neue ist die durch die neue Technologie in diesem Bereich möglich gewordene Größenordnung des Sprungs. Wie bereits zuvor erwähnt, sind wir Zeuge eines digitalen Wettrüstens und höherer Stufen politisch-kommunikativer Operationen, die durch Computional Intelligence unterstützt werden. Bolivien war dafür ein Laboratorium und Twitter das Versuchskaninchen, das zweifellos Experimente erlaubte, die gegen seine eigenen Richtlinien und Nutzungsbedingungen verstießen.

Dies alles geschah im Kontext eines doppelseitigen kommunikativen Angriffs: Auf der einen Seite löste der Putschismus durch die Schließung der Medien einen analogen Nachrichtenausfall aus und auf der anderen Seite produzierte er durch Automatisierung und ausländische Einmischung eine geräuschvolle digitale Explosion.

Die Region ist zu einer anderen Phase der Kommunikationsschlacht übergegangen. Die mangelnde Vorbereitung, um ihr zu begegnen, die sich im Bereich der bolivianischen Volksbewegung zeigte, ermöglichte den Putschisten auf der Ebene der Information zu agieren: An einem einzigen Tag brachte sie alle Stimmen eines Prozesses zum Schweigen, der 14 Jahre lang ein Land umgewandelt und befreit hat.

Es gibt keine Entschuldigungen, wir wissen, dass der Putschismus und der Imperialismus sich immer gegen die emanzipatorischen Projekte richten. Die Regierungen und die Volksbewegungen müssen sich darauf vorbereiten und dieser Artikel möchte in diesem Sinne ein Beitrag sein.