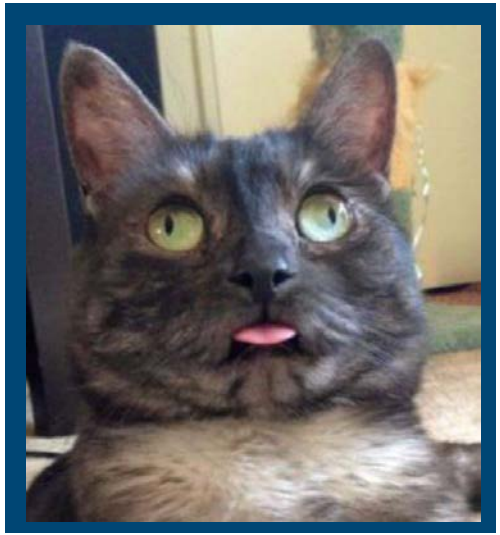
XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectivas

Desinformación: un enfoque desde la contrainteligencia y la contradecepción

ccn-cert
centro criptológico nacional



- Andrés Montero
- Fundación Concepto
- amg@theconcept.foundation

Índice

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

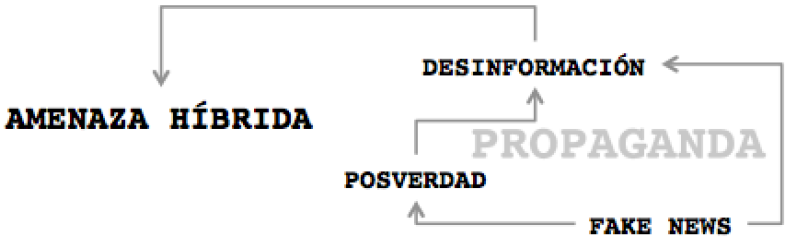
Preliminares: Conceptos de Partida

DESINFORMACIÓN: proporcionar información manipulada o insuficiente para lograr ciertos fines en orden a distorsionar la percepción de la realidad.

FAKE NEWS o noticias falseadas: relatos falsos que parecen ser noticias, difundidos por cualquier canal de comunicación, generalmente para influir en opiniones.

POSVERDAD: también llamada “mentira emotiva” o “posfactual”. La apariencia de verdad es más importante que la verdad: hechos falsos, tergiversados o inventados que apelan a llevar el proceso de toma de decisiones al plano emocional, con minimización de la componente racional de análisis de evidencias.

GUERRA O AMENAZA HÍBRIDA: conflicto que contiene elementos de agresión en distintos planos analógicos y cibernéticos: fuerzas regulares e irregulares; no distinción de estado de guerra o de paz; desinformación o guerras de información; propaganda; acciones de influencia. GUERRA DE LA INFORMACIÓN: usar la información como arma, para lograr una ventaja sobre el oponente o el enemigo.



DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Preliminares: Conceptos de Partida

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Preliminares: Lo que se nos está diciendo

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

October 19, 2018

Joint Statement from the ODNI, DOJ, FBI and DHS: Combating Foreign Influence in U.S. Elections

Foreign interference in U.S. elections is a threat to our democracy; identifying and preventing this interference is a top priority of the Federal Government. We believe the greatest strength of our society is an engaged and informed public. Adversaries target U.S. elections to divide America along political lines and influence key policy decisions that are in their national interest.

Foreign Influence

We are concerned about ongoing campaigns by Russia, China and other foreign actors, including Iran, to undermine confidence in democratic institutions and influence public sentiment and government policies. These activities also may seek to influence voter perceptions and decision making in the 2018 and 2020 U.S. elections.

Elements of these campaigns can take many forms, including using social media to amplify divisive issues, sponsoring specific content in English-language media like RT and Sputnik, seeding disinformation through sympathetic spokespersons regarding political candidates and disseminating foreign propaganda.

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Preliminares: Lo que se nos está diciendo

Medium | Social Media

Become a member

739

MEMBER FEATURE STORY

The Surprising Nuance Behind the Russian Troll Strategy

We set out to study internet discourse around #BlackLivesMatter — instead, we were unintentionally learning about the Russian information operation to undermine democracy

Kate Starbird Follow

Oct 20 · 9 min read ★

University of Washington

#BlackLivesMatter Twitter conversation

The IRA accounts impersonated activists on both sides of the conversation.

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Preliminares: Lo que se nos está diciendo

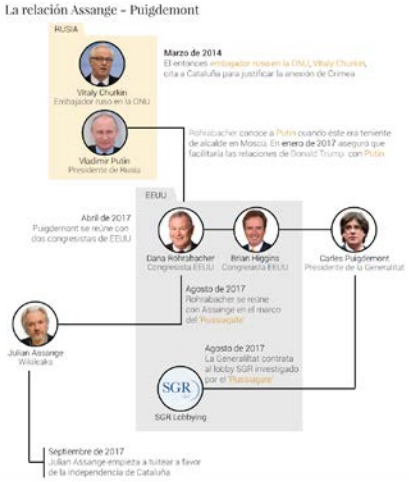
La maquinaria de injerencias rusa penetra la crisis catalana

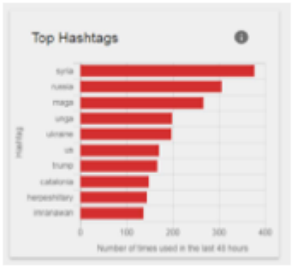
La red global que actuó con Trump y el Brexit se dedica ahora a España

DAVID ALANDETE
Madrid · 23 SEP 2017 - 06:55 EDT

Un ejército de robots

En una semana en que la justicia y el Gobierno han desarmado la logística del referéndum ilegal, el tuit con mayor influencia en el mundo sobre el asunto, según la herramienta de medición NewsWhip, fue una publicación de Julian Assange del 15 de septiembre a las 18.46: "Pido a todo el mundo que apoye el derecho de Cataluña a la autodeterminación. A España no se le puede permitir que normalice actos represivos para impedir que se vote". El mensaje, en inglés, obtuvo más de 12.000 retuits y 16.000 *me gusta*.





Análisis de hastags de Hamilton 68.

Cataluña, junto a Ucrania y Siria

La prueba definitiva de que el interés de quienes movilizan al ejército de bots prorrusos se ha centrado en el pulso independentista en España es que entre sus menciones habituales en redes (Siria, Rusia, Ucrania, Trump, Hillary Clinton, ISIS) ha entrado desde hace unos días Cataluña. Así lo refleja la herramienta Hamilton 68 de la Alianza para Asegurar la Democracia, un proyecto nacido en el seno del German Marshall Fund después de que la proliferación de noticias falsas en las elecciones norteamericanas de 2016 le permitiera a Donald Trump ganar la presidencia. Esa herramienta analiza de forma permanente 600 cuentas, automatizadas o no, en la órbita del Kremlin. En las 48 horas entre el miércoles y el viernes, uno de los hashtags más empleados por esos perfiles prorrusos era #Catalonia, tras otros como #HerpesHillary o #Trump.

Opaca: no documenta ni siquiera mínimamente cuáles son los criterios o parámetros empleados para identificar perfiles o contenidos en redes sociales como "parte de una infraestructura activa de injerencia rusa".

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Preliminares: Lo que se nos está diciendo

La desinformación (*deziformatsiya*) como práctica del régimen ruso diseñada para engañar y desorientar al oponente, influir en sus decisiones y socavar su eficiencia política, económica y militar.

...desinformación como método militar asimétrico e indirecto en la guerra híbrida que Rusia libra en Europa y EEUU.

La desinformación es uno de los instrumentos principales de la estrategia rusa de influencia política.

En Rusia, la desinformación formaba parte de las "medidas activas" (*activniye meropriyatya) y se define como una acción cuyo fin es "desacreditar y debilitar a los oponentes y distorsionar su percepción de la realidad"*

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Preliminares: Lo que se nos está diciendo

DESAFÍO INDEPENDENTISTA ›

Crece la inquietud en Europa sobre la injerencia rusa en Cataluña

EL PAÍS

Un grupo de expertos pide a Bruselas más contundencia frente a la propaganda

La UE combate la máquina de propaganda del Kremlin

El equipo de especialistas de la Unión Europea que detecta y combate ataques rusos en internet alerta de un aumento en las campañas para agravar la crisis en Cataluña

668

DAVID ALANDETE

De hecho, las herramientas que este equipo, de nombre East Stratcom Task Force, han cuantificado el aumento de informaciones sobre Cataluña en las redes prorrusas: de cuatro por semana se ha pasado a 241. Los analistas de ese

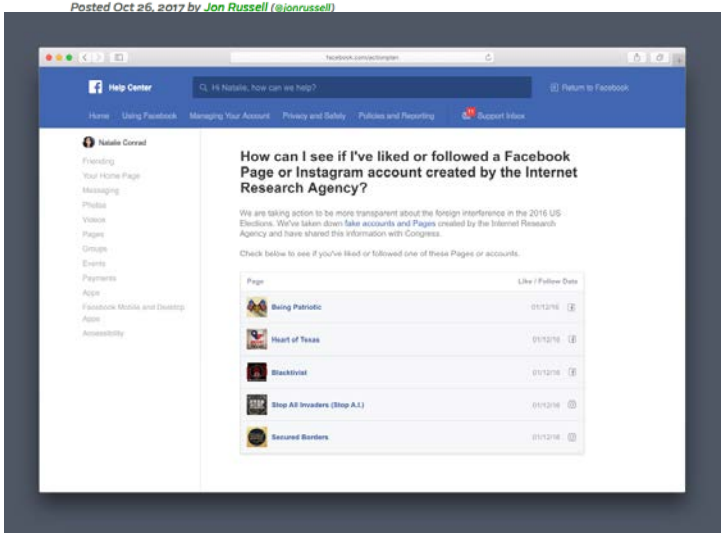
González Pons: "Las redes sociales de Rusia y Putin están trabajando en la Cataluña de Puigdemont"

El portavoz del PP en el Parlamento Europeo, Esteban González Pons, considera que los independentistas **n**o tienen ningún apoyo relevante**,** al igual que la acción contra los bancos, que ha proclamado contra el euro es incomprendida en Bruselas"**.**

Advertising Tech Sputnik rt news media television

Twitter bans Russia Today and Sputnik from advertising on its service

Posted Oct 26, 2017 by Jon Russell (@jonrussell)



European Commission - Press release

Next steps against fake news: Commission sets up High-Level Expert Group and launches public consultation

Brussels, 13 November 2017

CEPA THIS WEEK IN INFO WAR

KREMLIN MEDIA TILTS TOWARD CATALONIA

La red de injerencia rusa sitúa Cataluña entre sus prioridades para debilitar Europa

Medios en inglés, ruso y alemán igualan la crisis en España con los conflictos de Crimea y el Kurdistán

DAVID ALANDETE

Madrid - 24 SEP 2017 - 15:21 EDT

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Preliminares: Lo que se nos está diciendo

BERLIN POLICY JOURNAL

Home › Manhattan Transfer › Building a Trojan Horse

Building a Trojan Horse

Russia used social media to influence the German election, too.

115TH CONGRESS *2d Session* | COMMITTEE PRINT | S. PRT. 115–21

PUTIN'S ASYMMETRIC ASSAULT ON DEMOCRACY IN RUSSIA AND EUROPE: IMPLICATIONS FOR U.S. NATIONAL SECURITY

A MINORITY STAFF REPORT

PREPARED FOR THE USE OF THE

COMMITTEE ON FOREIGN RELATIONS

UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JANUARY 10, 2018

RT en Español

México: Aún faltan ocho meses y ya hackeamos las elecciones

Algunos medios mexicanos ya están acusando a RT de interferencia en las elecciones presidenciales, aunque todavía falta casi un año

3:54 pm - 6 Nov 2017

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Preliminares: Lo que se nos está diciendo

RAND CORPORATION

Countering Russian Social Media Influence

Elizabeth Bodine-Baron, Todd C. Helmus, Andrew Radin, Elina Treyger

PNAS

Bots increase exposure to negative and inflammatory content in online social systems

Massimo Stella[a], Emilio Ferrara[b,1], and Manlio De Domenico[a,1]

[a]Center for Information and Communication Technology, Fondazione Bruno Kessler, 38123 Trento, Italy; and [b]USC Information Sciences Institute, University of Southern California, Marina del Rey, CA 90292

Edited by Jon Kleinberg, Cornell University, Ithaca, NY, and approved October 19, 2018 (received for review February 27, 2018)

Societies are complex systems, which tend to polarize into subgroups of individuals with dramatically opposite perspectives. This phenomenon is reflected—and often amplified—in online social networks, where, however, humans are no longer the only players and coexist alongside with social bots—that is, software-controlled accounts. Analyzing large-scale social data collected during the Catalan referendum for independence on October 1, 2017, consisting of nearly 4 millions Twitter posts generated by almost 1 million users, we identify the two polarized groups of Independentists and Constitutionalists and quantify the structural and emotional roles played by social bots. We show that bots act from peripheral areas of the social system to target influential humans of both groups, bombarding Independentists with violent contents, increasing their exposure to negative and inflammatory

individuals among the group of Independentists (i.e., Catalan independence supporters). For our analysis, we first detect bots by using a cutting-edge scalable approach and find that nearly one in three users in this conversation is a bot.

Results

By disentangling the observed social interactions in retweets (who reshares the content posted by whom), replies (who responds to whom), and mentions (who attracts the attention of whom), we find that humans and bots share similar temporal behavioral patterns in the volume of messages. Both groups display daily excursions resembling a circadian rhythm, with a dramatic increase in the activity rate on October 1. Fig. 1 *B*, *Lower*, shows that bots produced 23.6% of the total number of

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Preliminares: Lo que se nos está diciendo

PNAS

Bots increase exposure to negative and inflammatory content in online social systems

Massimo Stella[a], Emilio Ferrara[b,1], and Manli

[a]Center for Information and Communication Technology, of Southern California, Marina del Rey, CA 90292

Edited by Jon Kleinberg, Cornell University, Ithaca, NY, an

Societies are complex systems, which tend to po groups of individuals with dramatically opposit This phenomenon is reflected—and often ampli social networks, where, however, humans are no players and coexist alongside with social bots—th controlled accounts. Analyzing large-scale social during the Catalan referendum for independenc 2017, consisting of nearly 4 millions Twitter post almost 1 million users, we identify the two pola Independentists and Constitutionalists and quantif and emotional roles played by social bots. We sho from peripheral areas of the social system to ta humans of both groups, bombarding Independenti contents, increasing their exposure to negative an

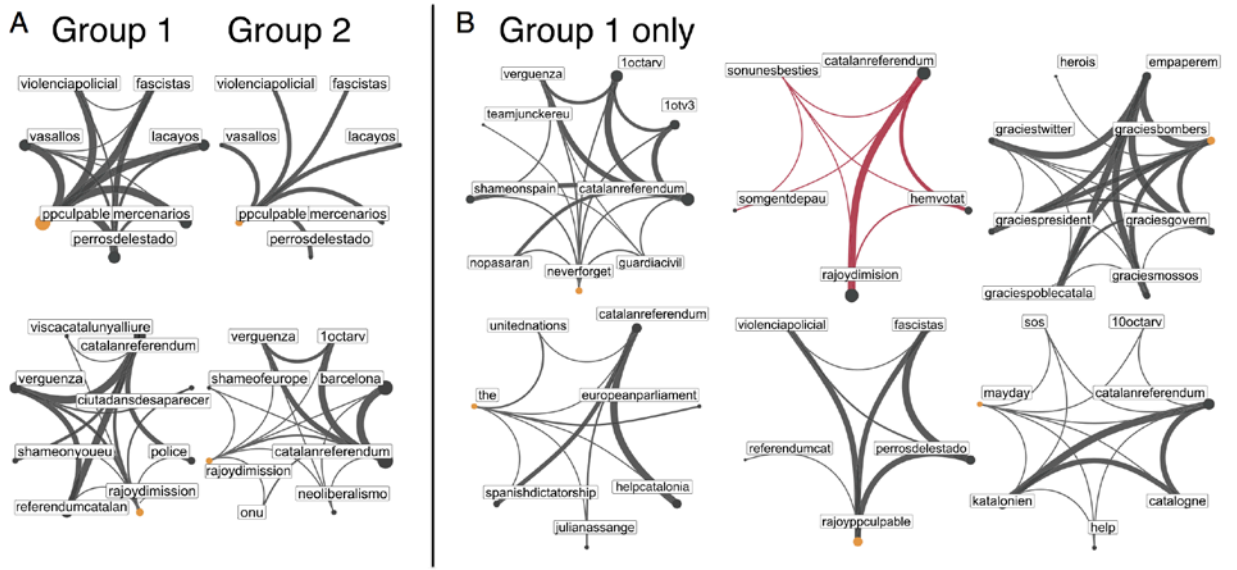
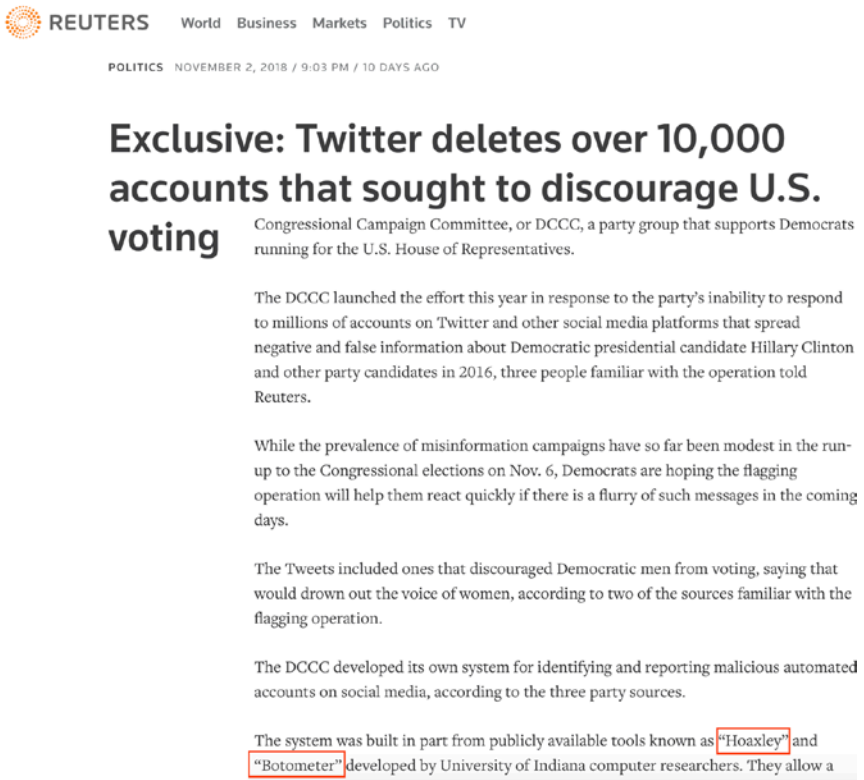


Fig. 4. Hashtag ecosystem reveals group identity. Hashtags are coupled together if they appear simultaneously in a message, building a network of concepts. Analyzing the hashtag networks obtained from each group, we identify the hashtags which are ranked similarly (*A*) and very differently (*B*) in the two groups to visualize the corresponding neighboring concepts. In *A*, low-ranked hashtags coexist in both groups and do not allow us to identify the underlying ideology of each group. In *B*, top-ranked hashtag that exist only in group 1 are strongly related to concepts of freedom, independence, fight, shame against the Spanish government, dictatorship, and blame against police violence, providing evidence that group 1 consists of Catalan Independentists. Remarkably, concepts related to "sonunesbesties" (translated as "they are beasts")—highlighted in *B*—are posted by bots only, whereas the other hashtag networks have contributions by both humans and bots. Note that, for clarity, in *B* we show only hashtags fully characterizing accounts associated with Independentists.

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Preliminares: Lo que se nos está diciendo



REUTERS World Business Markets Politics TV

POLITICS NOVEMBER 2, 2018 / 9:03 PM / 10 DAYS AGO

Exclusive: Twitter deletes over 10,000 accounts that sought to discourage U.S. voting

Congressional Campaign Committee, or DCCC, a party group that supports Democrats running for the U.S. House of Representatives.

The DCCC launched the effort this year in response to the party's inability to respond to millions of accounts on Twitter and other social media platforms that spread negative and false information about Democratic presidential candidate Hillary Clinton and other party candidates in 2016, three people familiar with the operation told Reuters.

While the prevalence of misinformation campaigns have so far been modest in the run-up to the Congressional elections on Nov. 6, Democrats are hoping the flagging operation will help them react quickly if there is a flurry of such messages in the coming days.

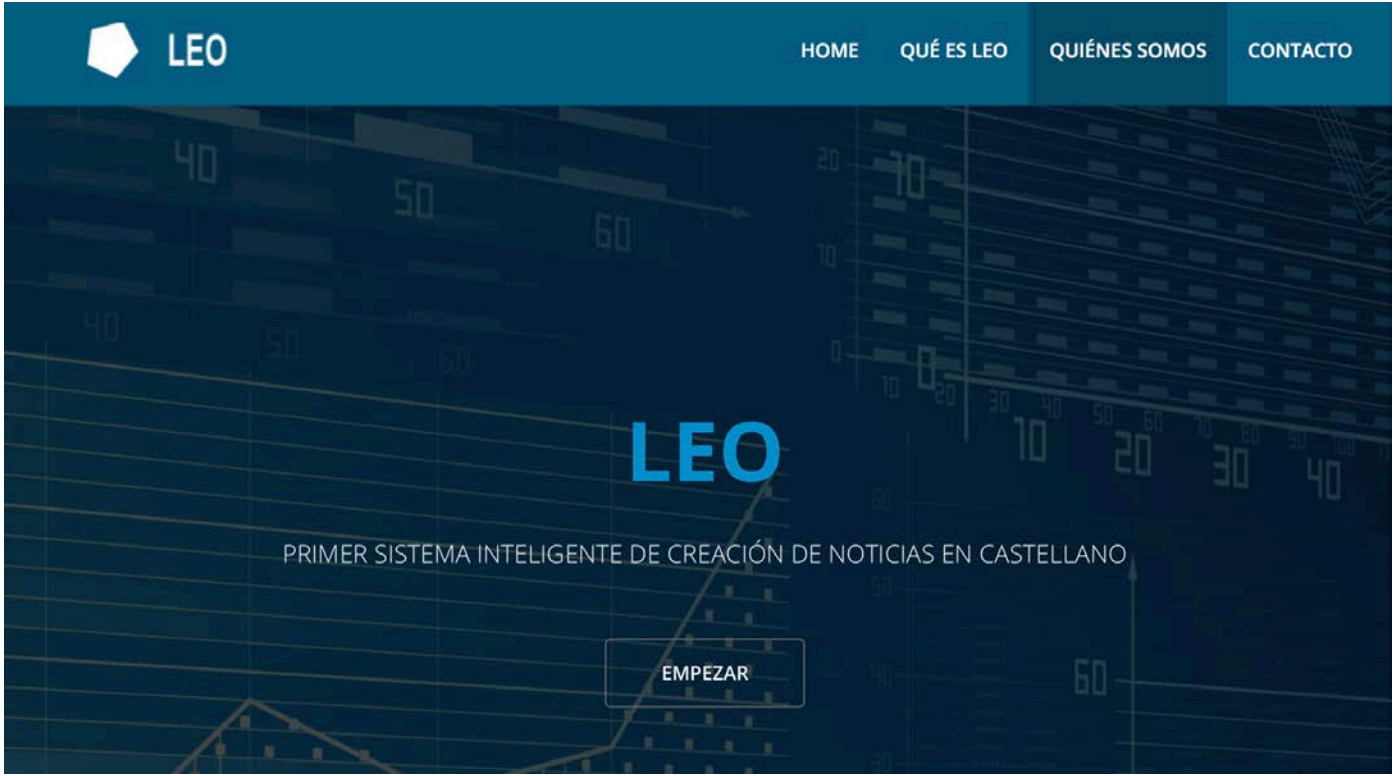
The Tweets included ones that discouraged Democratic men from voting, saying that would drown out the voice of women, according to two of the sources familiar with the flagging operation.

The DCCC developed its own system for identifying and reporting malicious automated accounts on social media, according to the three party sources.

The system was built in part from publicly available tools known as "Hoaxley" and "Botometer" developed by University of Indiana computer researchers. They allow a

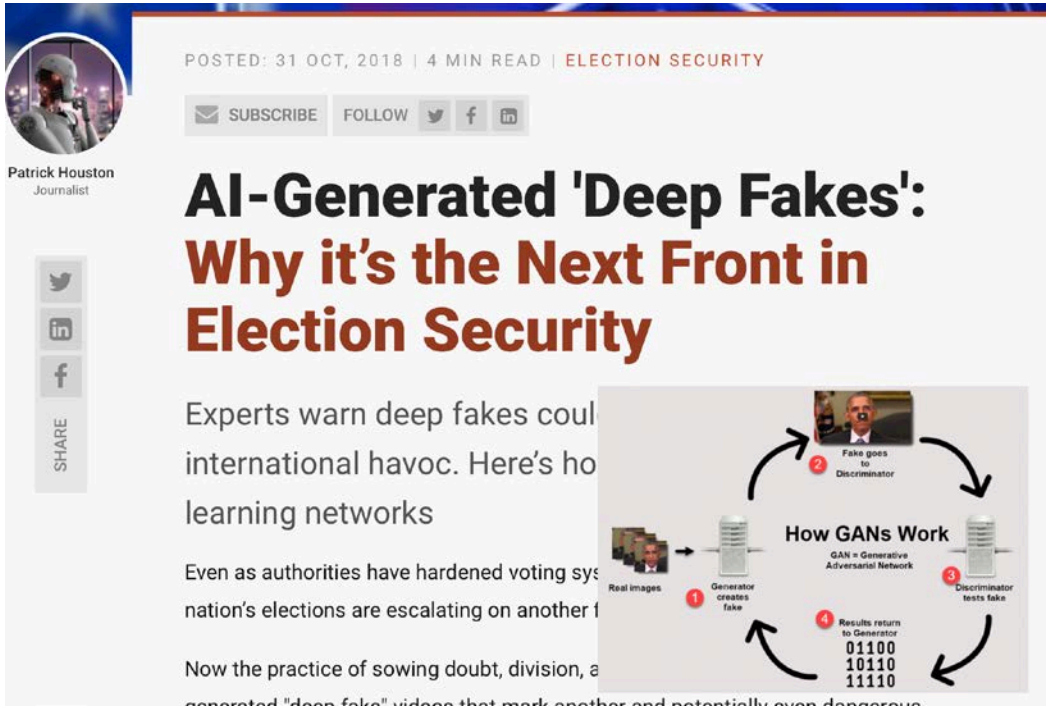
DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Preliminares: Lo que se nos está diciendo



DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Preliminares: Lo que se nos está diciendo



DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Datos: Lo que se observa

HEARING BEFORE THE UNITED STATES SENATE SELECT COMMITTEE ON INTELLIGENCE

November 1, 2017

Testimony of Colin Stretch
General Counsel, Facebook

Facebook : ante informaciones de prensa sobre supuesta "injerencia rusa", inician una investigación y clausuran cuentas de ads publicitarias pagada por la Internet Research Agency-IRA (empresa en San Petesburgo, Rusia, que se vincula por otras fuentes a la "maquinaria de propaganda rusa"), que a su vez habría invertido esas ads publicitarias en promover 120 páginas en Facebook creadas por la IRA durante 2 años.

Google

Written Testimony of Kent Walker
Senior Vice President and General Counsel, Google
Senate Select Committee on Intelligence
Hearing on "Social Media Influence in the 2016 US Elections"
Written Congressional Testimony
November 1, 2017

Google : no aporta conclusiones más allá de describir un mínimo volumen de contratos de publicidad (algo más de 4.000 dólares) y algunos contenidos subidos a Youtube que podrían ser "representativos"

United States Senate Select Committee on Intelligence

Testimony of Sean J. Edgett
Acting General Counsel, Twitter, Inc.

November 1, 2017

Twitter: detalla el volumen de cuentas vinculadas a Rusia (territorialmente, aunque sin establecerse intenciones o campañas organizadas) que tuitearon en el período de las elecciones estadounidenses contenidos relacionados con ellas, observándose que representaban una porción baja y poco significativa del tráfico circulante en el período. Así mismo se refieren algo más de 2.000 cuentas ligadas a la IRA que Twitter subraya no haber identificado por sí mismos "sino por información aportada por terceras partes" como cuentas vinculadas a la IRA, describiendo su actividad pero sin que Twitter sea capaz de extraer conclusiones atributivas (que por el tono de esa porción de la declaración, se entiende que esas atribuciones a Twitter "le fueron dadas"). En definitiva, Twitter no es capaz de extraer ninguna conclusión más allá de centrar que los perfiles relacionados con el medio de comunicación Russia Today cumplían los "criterios para ser consideradas cuentas vinculadas a Rusia", se entiende, "intereses rusos"

The 36,746 automated accounts that we identified as Russian-linked and tweeting election-related content represent approximately one one-hundredth of a percent (0.012%) of the total accounts on Twitter at the time.

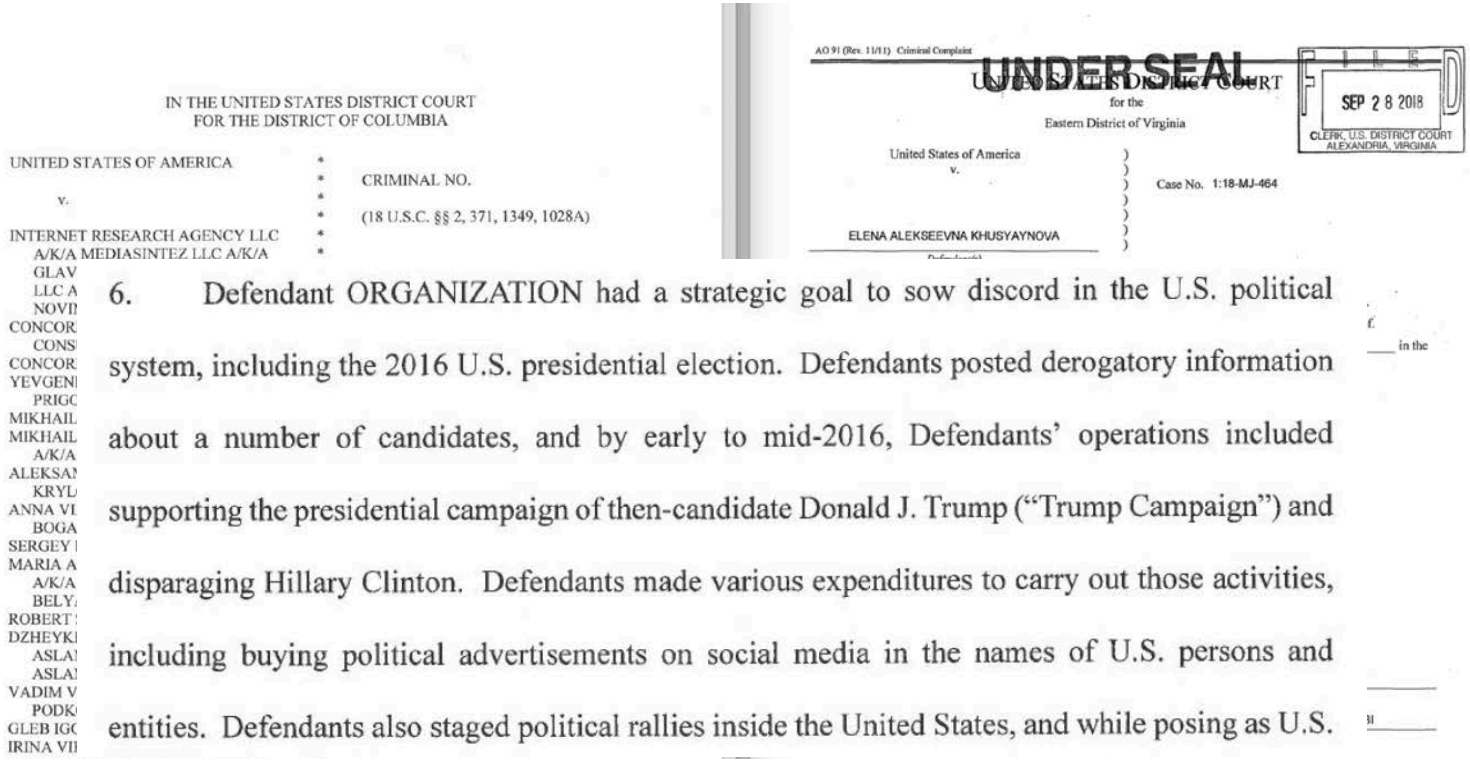
The 1.4 million election-related Tweets that we identified through our retrospective review as generated by Russian-linked, automated accounts constituted less than three quarters of one percent (0.74%) of the overall election-related Tweets on Twitter at the time. *See* Appendix 1.

Those 1.4 million Tweets received only one-third of a percent (0.33%) of impressions on election-related Tweets. In the aggregate, automated, Russian-linked, election-related Tweets consistently underperformed in terms of impressions relative to their volume on the platform. *See* Appendix 2.

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Datos: Lo que se observa

Project Lakhta



IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA
v.
INTERNET RESEARCH AGENCY LLC
A/K/A MEDIASINTEZ LLC A/K/A
GLAV
LLC A
NOVI
CONCOR
CONS
CONCOR
YEVGEN
PRIGC
MIKHAIL
MIKHAIL
A/K/A
ALEKSA
KRYL
ANNA VI
BOGA
SERGEY
MARIA A
A/K/A
BELY
ROBERT
DZHEYK
ASLA
ASLA
VADIM V
PODK
GLEB IG
IRINA VI

CRIMINAL NO.

(18 U.S.C. §§ 2, 371, 1349, 1028A)

AO 91 (Rev. 11/11) Criminal Complaint

UNDER SEAL

UNITED STATES DISTRICT COURT
for the
Eastern District of Virginia

FILED
SEP 28 2018
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

United States of America
v.
ELENA ALEKSEEVNA KHUSYAYNOVA

Case No. 1:18-MJ-464

6. Defendant ORGANIZATION had a strategic goal to sow discord in the U.S. political system, including the 2016 U.S. presidential election. Defendants posted derogatory information about a number of candidates, and by early to mid-2016, Defendants' operations included supporting the presidential campaign of then-candidate Donald J. Trump ("Trump Campaign") and disparaging Hillary Clinton. Defendants made various expenditures to carry out those activities, including buying political advertisements on social media in the names of U.S. persons and entities. Defendants also staged political rallies inside the United States, and while posing as U.S.

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

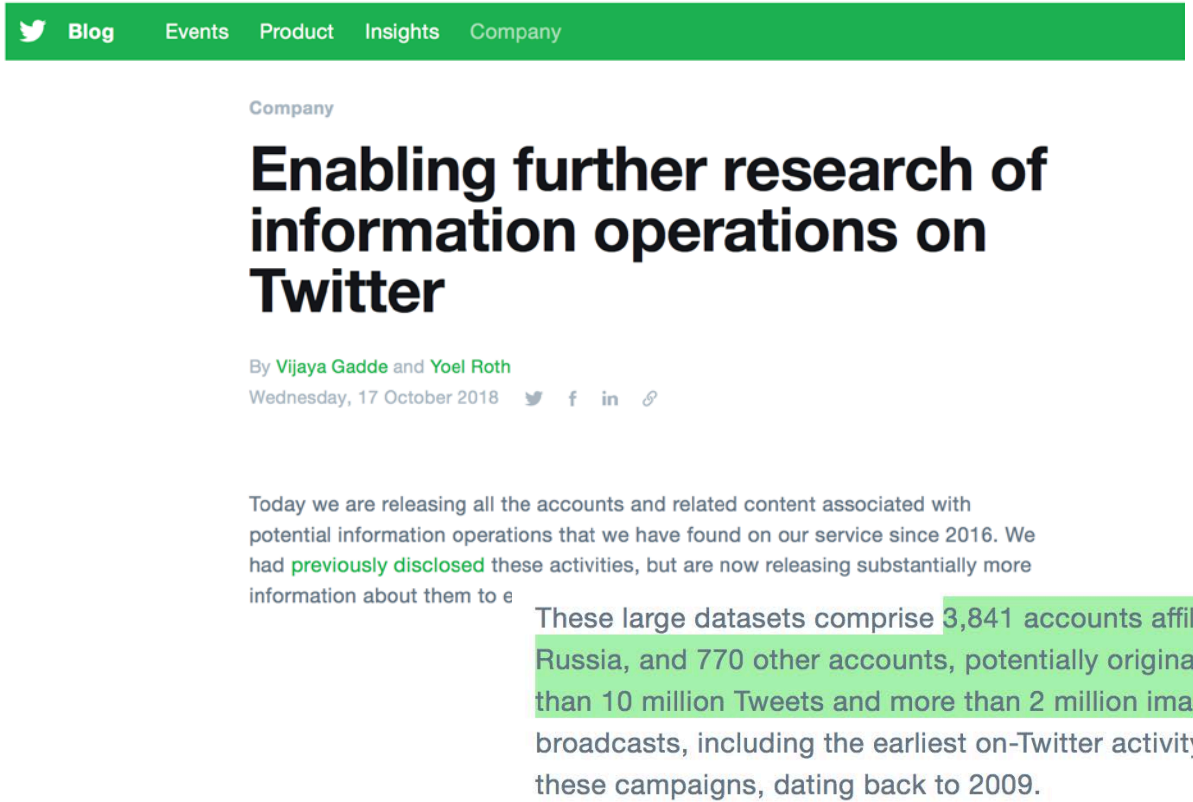
Datos: Lo que se observa

In or around January 2017, KHUSYAYNOVA compiled and submitted to Concord a planned itemized budget for February 2017 for Project Lakhta totaling approximately 60 million Russian rubles (approximately $1 million U.S. dollars).[2] This budget also contained a backward-looking accounting of actual expenses for calendar year 2016, which totaled approximately 720 million Russian rubles (approximately $12 million U.S. dollars). In addition to administrative expenses, such as office rent, utility payments, and garbage disposal, the budget identified IT expenses, such as "registration of domain names" and the purchase of "proxy servers;" and social media marketing expenses, such as expenses for "purchasing posts for social networks," "[a]dvertisement on Facebook," "[a]dvertisement on VKontakte," "[a]dvertisement on Instagram," "[p]romoting news postings on social networks," and social media optimization software (such as Twidium and Novapress) (preliminary translation of Russian text). The budgets also contained a section on "USA, EU" activities, which included itemized expenditures for "Instagram," "Facebook advertisement," and "Activists" (preliminary translation of Russian text). Moreover, the budgets identified expenditures for "bloggers" and "developing accounts" on Twitter, and for the development and promotion of online videos (preliminary translation of Russian text).

Project Lakhta

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Datos: Lo que se observa



Blog Events Product Insights Company

Company

Enabling further research of information operations on Twitter

By Vijaya Gadde and Yoel Roth
Wednesday, 17 October 2018

Today we are releasing all the accounts and related content associated with potential information operations that we have found on our service since 2016. We had previously disclosed these activities, but are now releasing substantially more information about them to e

These large datasets comprise 3,841 accounts affiliated with the IRA, originating in Russia, and 770 other accounts, potentially originating in Iran. They include more than 10 million Tweets and more than 2 million images, GIFs, videos, and Periscope broadcasts, including the earliest on-Twitter activity from accounts connected with these campaigns, dating back to 2009.

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Datos: Lo que se observa

No sólo desinforman los rusos, sino que se trata de una práctica habitual observable en muchos sectores y escenarios sociales. Los social media han añadido gasolina al fuego.

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Datos: Lo que se observa

La máquina de las 'fake news' trabaja a favor de Bolsonaro en Brasil

La campaña del ultraconservador utiliza noticias falsas sin pudor. EL PAÍS analiza grupos de WhatsApp a favor del candidato y detecta mentiras, teorías de la conspiración y mensajes para desmentir a la prensa

AFONSO BENITES

Brasília - 3 OCT 2018 - 05:18 CEST

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Datos: Lo que se observa

LA VANGUARDIA | Internacional

Al Minuto Internacional Política Opinión Vida Deportes Economía Local Gente Cultura Sucesos Temas

Directo La decisión del Supremo sobre el impuesto de actos jurídicos documentados de las hipotecas

ESCÁNDALO MUNDIAL

Cómo utilizó Cambridge Analytica los datos de Facebook para manipular a los votantes

18

• Con un volumen de decenas de millones de perfiles, la compañía que trabajó para la campaña de Trump sabía qué decir, cómo, cuando y cuantas veces para hacerte cambiar de opinión

INTERNACIONAL EN COLABORACIÓN CON The Guardian

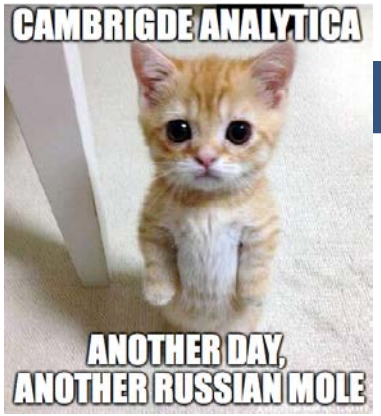
Oriente Medio Europa Estados Unidos América Latina Asia África Desalambre Guerra Eterna Boletín

theguardian

Cambridge Analytica estudió manipular las elecciones de Nigeria con emails conseguidos por hackers israelíes

- PUBLICIDAD -

theguardian EN ESPAÑOL



único remedio constitucional sería mediante el *impeachment*,[6] idea que viene tomando de nuevo fuerza, y el caso de CA y Facebook puede darle mayor impulso.

Qué es CELAG Investigación Formación

Cambridge en Brasil, Argentina y México

En 2017 CA abrió una filial en Brasil de cara a las elecciones. CA-Ponte ya está siendo investigada para saber si operó en Brasil. Andrés Torreta, directivo de CA-Ponte explicó a la BBC que aprovechaban la metodología usada por CA y "planeaban aplicar el uso del direccionamiento inteligente de mensajes políticos a whatsapp", empresa que ya pertenece a Facebook.[7]

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Datos: Lo que se observa

Search

Bloomberg

Economics

Twitter Bots Helped Trump and Brexit Win, Economic Study Says

By Jeanna Smialek
21 de mayo de 2018 19:13 CEST

Trump y su campaña electoral nos han regalado el mejor caso de uso de la posverdad: la distorsión de la realidad para crear una versión que alimente las pulsiones emocionales de un determinado grupo poblacional para que ese colectivo **tome decisiones** (emocionales) sobre realidades (tergiversadas) que conduzcan a la sociedad en una **determinada dirección** (interesada).

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Datos: Lo que se observa

Los contenidos basura son inherentes a las redes sociales

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Datos: Lo que se observa

Astroturfing

Este artículo trata sobre campañas de relaciones públicas en el ámbito de la propaganda electoral. Para césped artificial, véase AstroTurf.

Astroturfing es un término referido a campañas de relaciones públicas en el ámbito de la propaganda electoral y los anuncios comerciales que pretenden dar una impresión de espontaneidad, como nacida de una fuerte relación con el entorno social. El nombre proviene de un doble juego de palabras en inglés, partiendo del concepto de *grassroots* (literalmente "raíz de hierba", figurativamente "de base"). Este concepto sirve para calificar a los movimientos «con base social», que surgen «de abajo», de la interacción de los miembros de una comunidad. Por otro lado, AstroTurf es una conocida marca estadounidense de césped artificial, cuyos productos están diseñados para parecer hierba natural. Así, *astroturfing* hace referencia a esa artificialidad, a esa falsa base social de ciertas campañas comerciales.

El objetivo de una campaña de este estilo es disfrazar las acciones de una entidad política o comercial como la reacción pública espontánea e independiente frente a otra entidad, producto, servicio, etc.

Los *astroturfers* (intoxicadores) intentan orquestar para ello acciones protagonizadas por unos pocos individuos aparentemente diversos y geográficamente distribuidos, tanto a través de actuaciones explícitas como más subliminales e incluso ocultas, y que dan la impresión de multitudinarios entusiastas de una causa.

El *astroturfing* puede ser lanzado por un particular interesado personalmente por un asunto o por grupos profesionales organizados y financiados por grandes empresas u organizaciones activistas o sin ánimo de lucro.

How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument*

Gary King† Jennifer Pan‡ Margaret E. Roberts§

April 9, 2017

†Albert J. Weatherhead III University Professor, Institute for Quantitative Social Science, 1737 Cambridge Street, Harvard University, Cambridge MA 02138; GaryKing.org, King@Harvard.edu, (617) 500-7570.
‡Assistant Professor, Department of Communication, 450 Serra Mall, Building 120, Stanford University, Stanford CA 94304; http://people.fas.harvard.edu/~jjpan/, (917) 740-5726.
§Assistant Professor, Department of Political Science, University of California, San Diego, Social Sciences Building 301, 9500 Gilman Drive, #0521, La Jolla, CA 92093-0521, meroberts@ucsd.edu, MargaretRoberts.net.

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Datos: Lo que se observa

MORNING CONSULT + POLITICO

Question	Response	Frequency	Percentage
POL15	*How likely is it that Russia will try to influence the 2018 midterm elections for the House of Representatives and some senators?*		
	Very likely	640	25%
	Somewhat likely	567	22%
	Not too likely	359	14%
	Not likely at all	408	16%
	Don't Know/No Opinion	568	22%
POL16	*And, if Russia does try to influence the 2018 midterm elections, do you think they are more likely to help:*		
	Republican candidates	1220	48%
	Democratic candidates	380	15%
	Don't Know/No Opinion	943	37%
POL17	*Would you be more or less likely to vote if it was determined that Russia or another country was interfering in the 2018 midterm elections?*		
	Much more likely to vote	1028	40%
	Somewhat more likely to vote	161	6%
	Somewhat less likely to vote	141	6%
	Much less likely to vote	155	6%
	Not much impact either way	712	28%
	Don't Know/No Opinion	347	14%

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

(RE)ENFOQUE: Una posibilidad alternativa

PREMISA: si asumimos que el GRU (inteligencia militar rusa) está detrás de las operaciones de desinformación en un contexto híbrido, deberíamos asumir igualmente que está empleando un **enfoque y métodos y procedimientos de inteligencia** en una doctrina de operaciones militares (guerra híbrida) para desarrollarlas.

> Admitir un enfoque de **inteligencia** implica reconocer que el adversario está determinado a **dominar la realidad** obteniendo información y desarrollando análisis para conocerla mejor, y produciendo información para hacer que su adversario (nosotros) conozca e interprete (*framing*) esa realidad a su conveniencia.

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

(RE)ENFOQUE: Una posibilidad alternativa

Por tanto, vamos a partir de la premisa, perfectamente lógica, de que si una operación de desinformación está planificada por los órganos especializados de un Estado o con apoyo estatal de los servicios de inteligencia como un país como Rusia, China, Corea del Norte o cualquier otro del “eje del mal”, conoce más o menos perfectamente y desde luego de antemano el funcionamiento tecnológico y procedimental de las redes sociales, los patrones y dinámicas principales de sus usuarios, y los métodos empleados por agencias públicas y privadas para analizarlos... y utilizarán ese comportamiento para diseñar la operación de influencia.

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

(RE)ENFOQUE: Una posibilidad alternativa

De esta manera, partiendo de la premisa, el análisis de potenciales escenarios de desinformación debería efectuarse (o al menos contemplar) tácticas, técnicas y procedimientos de contrainteligencia y contradecepción.

CONTRAINTELIGENCIA: esfuerzos destinados a evitar y contrarrestar la acción de inteligencia de un adversario.

DECEPCIÓN: proveniente del ámbito de la doctrina militar, en general son todas las operaciones destinadas a engañar al adversario sobre intenciones, capacidades y recursos propios.

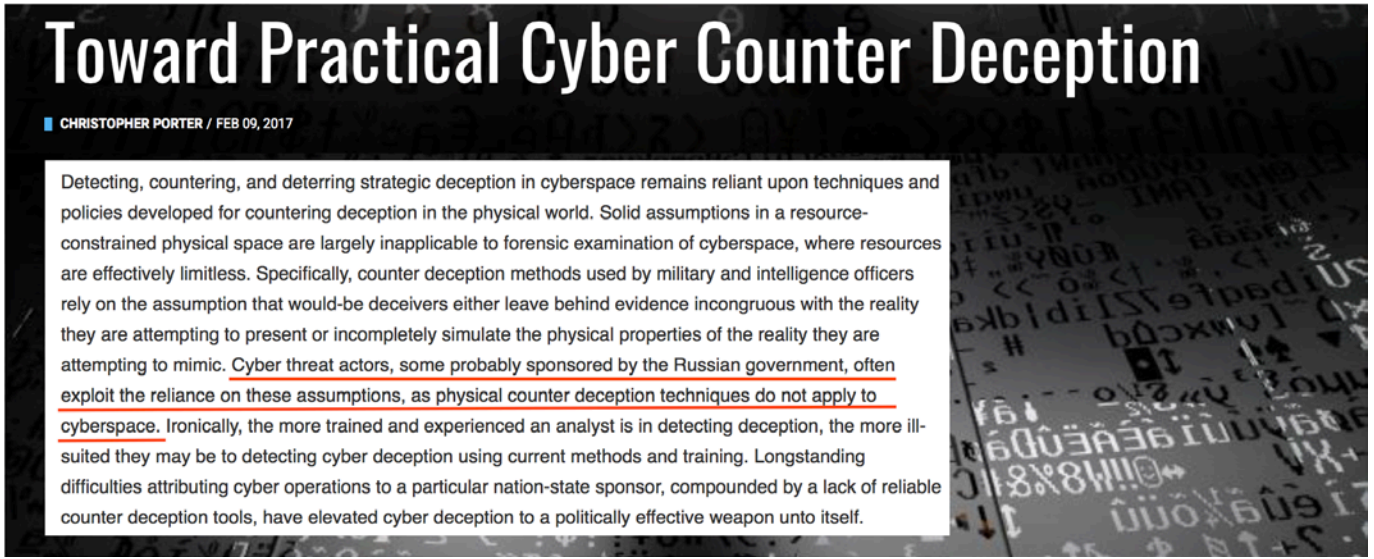
CONTRADECEPCIÓN: en doctrina militar en general y en inteligencia en particular, esfuerzos destinados a descubrir, entender y utilizar las operaciones de decepción de un adversario.

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

(RE)ENFOQUE: Una posibilidad alternativa

En la Fundación Concepto creíamos haber sido originales con el (re)enfoque, pero...

COLUMBIA | SIPA
JOURNAL OF INTERNATIONAL AFFAIRS



DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

HIPÓTESIS: Una posibilidad alternativa

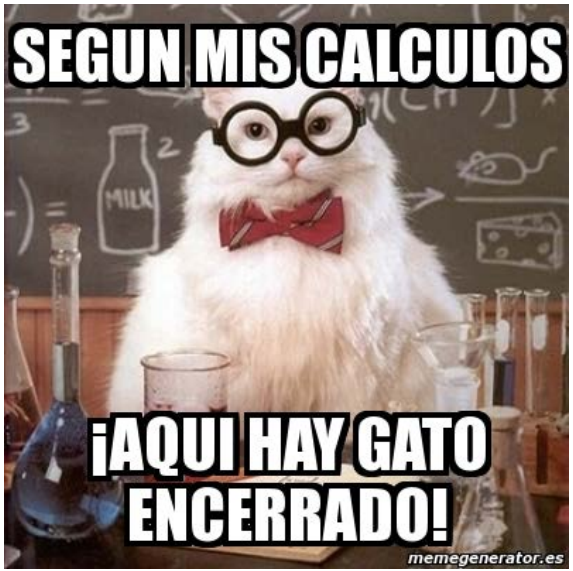
Es posible que el Gobierno de Rusia, en el contexto de su estrategia geopolítica, esté desarrollando a través de sus órganos especializados (GRU y otros) operaciones de inteligencia con la inclusión de “medidas activas” (***activniye meropriyatya)*** para producir desinformación que *induzca una determinada percepción de realidad* en el adversario.

> Si aceptamos esta posibilidad, tenemos que considerar que el GRU conoce de antemano -y ha incluido ese conocimiento en sus planes- los métodos y procedimientos empleados por analistas de inteligencia y, sobre todo, por medios de comunicación social para evaluar la información (y la desinformación) que circula por redes sociales.
>
> Por tanto, podría ser que el objetivo de la desinformación no fuera desinformar a la opinión pública para lograr determinadas propósitos de influencia, sino crear un determinado efecto en analistas y medios de comunicación sobre la desinformación (DECEPCIÓN) para que el resultado de los análisis fuera desinformativo (DECEPTIVO).

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

HIPÓTESIS: Una posibilidad alternativa

Los/las profesionales de contradecepción suelen hacerse antipáticos en sus organizaciones, puesto que parte de su trabajo es formular preguntas como:



¿Y si el propósito no fuera *hackear* a la opinión pública sino, haciendo **ingeniería inversa del analista**, *hackear* a analistas y creadores de opinión para utilizarlos como relé de *hoax* dirigidos sobre la opinión pública?

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

HIPÓTESIS: Una posibilidad alternativa

Supongamos que es una operación de **ciberdecepción** del GRU con **ingeniería social inversa** de los analistas

Como en toda operación de inteligencia para la decepción, el objetivo es **producir y construir una realidad que sea consumida por el adversario** de manera que induzca una percepción (en este caso sobredimensionada) de las capacidades e intenciones del diseñador de la decepción.

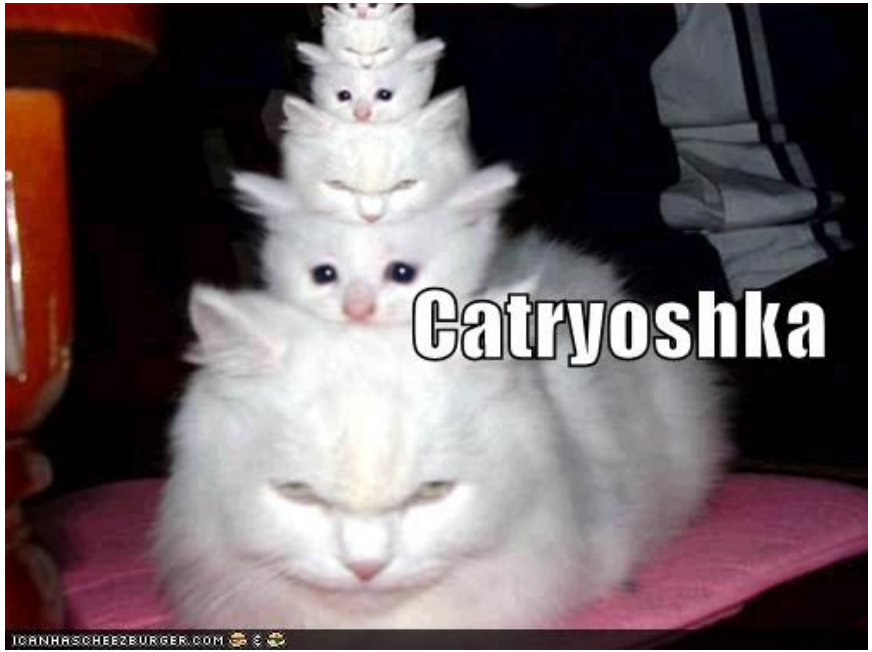
El diseñador quieren hacer parecer que es capaz de manipular nuestras elecciones, sembrando para ello una serie de "evidencias" incompletas pero con poder de crear **efecto de generalización**. Lo que se busca no es netamente manipular las elecciones, sino hacer creer que se pueden manipular, **manipulando** en cambio nuestra **percepción sobre esa posibilidad**.

El diseñador hace creer que tiene mayores capacidades de las que tiene para comprometer los sistemas democráticos: no se crea únicamente una capacidad perceptiva de "superioridad rusa", sino de **riesgo de los propios sistemas democráticos**.

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

CONTRADECEPCIÓN: Detección de Incongruencias

Barton Whaley <<*Toda decepción crea simultáneamente el conjunto de incongruencias necesario para su detección*>>.



DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

CONTRADECEPCIÓN: Detección de Incongruencias

El relato de las acusaciones del FBI ante la Autoridad Judicial en EEUU parece respaldar con evidencia suficiente que individuos y empresas rusas invirtieron fondos, realizaron viajes, promovieron activismo sobre el terreno, y crearon y utilizaron perfiles en redes sociales para influir en el sentimiento político de determinados sectores en poblaciones estadounidenses durante la campaña de las presidenciales de 2016

Llama “poderosamente” la atención que en las dos acusaciones judiciales en EEUU a 13 personas y organizaciones rusas por tratar de influir ilícitamente en las elecciones presidenciales de EEUU se tenga identificadas a dos empresas (*Internet Research Agency* y *Concord*; también lo hicieron Twitter y Facebook con IRA) como las gestoras de la maquinaria de desinformación. Si se tratara de una operación de desinformación directa del GRU, ¿no habría parecido más lógico enmascarar el origen?

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

CONTRADECEPCIÓN: Detección de Incongruencias

Empresas en Rusia, personas trazables hasta esas empresas en Rusia, contrataciones de ads en abierto como Internet Research Agency...
Únicamente parece que se molestaron en utilizar VPNs para las conexiones entre EEUU y Rusia cuando los agentes estaban sobre el terreno.

39. To hide their Russian identities and ORGANIZATION affiliation, Defendants and their co-conspirators—particularly POLOZOV and the ORGANIZATION's IT department—purchased space on computer servers located inside the United States in order to set up virtual private networks ("VPNs"). Defendants and their co-conspirators connected from Russia to the U.S.-based infrastructure by way of these VPNs and conducted activity inside the United States—including accessing online social media accounts, opening new accounts, and communicating with real U.S. persons—while masking the Russian origin and control of the activity.

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

CONTRADECEPCIÓN: Detección de Incongruencias

El asunto de la injerencia en las elecciones presidenciales Estados Unidos parece que tuvo como objetivo la elección de Trump, y no incluyó únicamente desinformación sino hackeo de sistemas tecnológicos del Partido Demócrata y acciones de influencia analógicas sobre fuentes humanas.

Y de momento no parece producir por sí mismos indicios suficientes para la extrapolación directa a otros escenarios, el Brexit o Cataluña.

En un supuesto marco de decepción en guerra híbrida, la operación en EEUU ¿podría haber sido la semilla de riesgo calculado dispuesta para que fuera regada por nuestras generalizaciones?

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

¿HACIA UNA METODOLOGÍA DE CIBERCONTRADECEPCIÓN?

COMPONENTES AXIALES

PAT

IEI

Actitudinal: existen posibilidades alternativas y una de ellas es que nos están engañando. Si estamos afirmando algo que está a favor de la *realidad dominante* ¿lo estamos afirmando porque somos parte de la realidad dominante (hemos contribuido nosotros a construirla) o porque estamos dominados por la realidad?
-> recordemos que la inteligencia consiste en dominar la informacion para definir la realidad.

Enfoque: explorar el contexto del contexto.

Procedimental: adoptar procedimientos de análisis con auditoría de sesgos. Indicadores de autodesinformación.

Técnico: muestreo sobre la población; estadísticas limpias; redes antagónicas: una realiza el análisis y otra evalúa.

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

¿HACIA UNA METODOLOGÍA DE CIBERCONTRADECEPCIÓN?

ELEMENTOS METODOLÓGICOS

1. Sobre el conjunto de la población estadística, muestreo por categorías generales y no por categorías sesgadas a priori.
2. Análisis exploratorio (p.ej. topológico) sobre el resultado del muestreo.
3. Análisis comparativo actores relevantes dentro de todo el arco de posiciones ideológicas de la población objeto de estudio.
4. Método declarado de caracterización de bots (por qué son bots) y de su clasificación en todos los clústers de actores relevantes.
5. Método declarado de categorización atribucional geográfica o de autoría.
6. Desarrollar una técnica cuantitativa de medición de la influencia: cuánto influyen volumetrías y contenidos y porqué.

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

CONCLUSIONES

Tomarse en serio la desinformación implica tomarse en serio las operaciones de decepción como parte de las amenazas híbridas desde un enfoque de inteligencia.

Hoy todo el mundo utiliza redes sociales para generar contenidos que produzcan *framing* o propaganda.

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

CONCLUSIONES

Con la emergencia del ciberespacio como un constructor de realidades percibidas y con los sistemas tecnológicos personales como interfaces para acceder a la información que construye la percepción de esas realidades, las posibilidades de utilizar la información para construir realidades virtuales desagregadas de la realidad física (¿analógica?) e incluso utilizadas para crear nuevas realidades físicas ha crecido y exponencialmente y lo hará todavía más.

En ese escenario, la inteligencia como marco de obtención y producción de información para analizar y crear realidades redobla la importancia que siempre ha tenido en la historia. Dentro de ella, la muchas veces olvidada contradecepción nos interpela para prestar atención a una evaluación más minuciosa y ponderada de las intenciones y capacidades “realidades de la información”, llamando al desarrollo de una metodología específica de ciberdecepción y cibercontradecepción.

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Y por último...

DESINFORMACIÓN: CONTRAINTELIGENCIA Y CONTRADECEPCIÓN

Y por último...

XII Jornadas STIC CCN-CERT

Ciberseguridad, hacia una respuesta y disuasión efectivas

- **E-Mails**
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - oc.ccn.cni.es
- **Síguenos en**

centro criptológico nacional