

RSA® Conference 2018

San Francisco | April 16–20 | Moscone Center

SESSION ID: EXP-W02



POTUS IS POSTING: SOCIAL MEDIA & NATIONAL SECURITY

Dr. Kenneth Geers

Senior Research Scientist
Comodo Group
@KennethGeers



James C. Foster

CEO
ZeroFOX
@FirstNameFoster



Social Media



17K years old.

Seeing is Believing



#RSAC



Early Photoshop



Intelligent phones

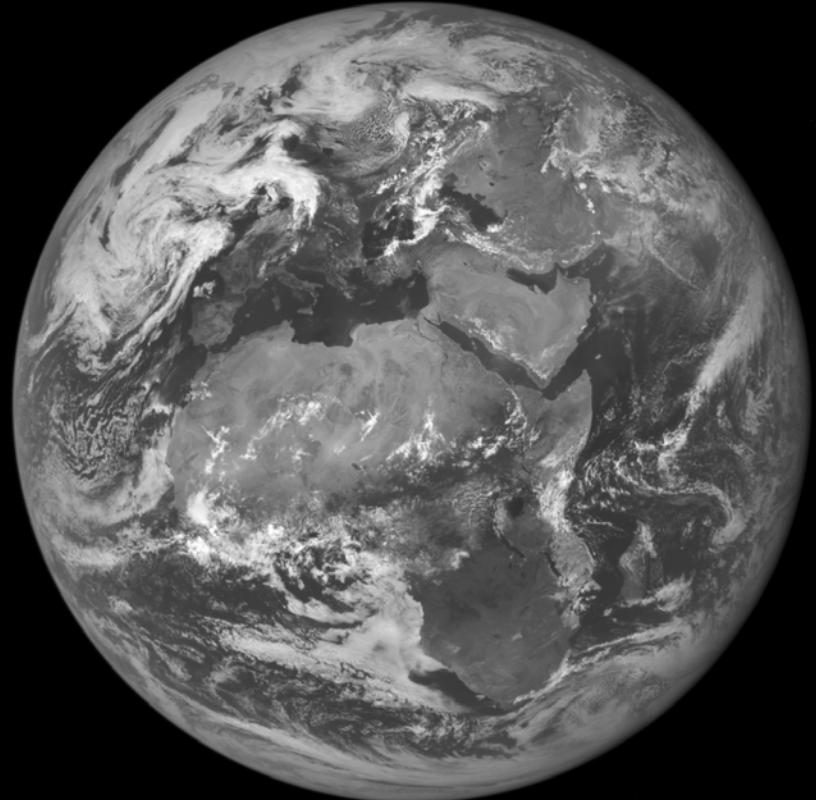


#RSAC



National springs and color revolutions

One Internet

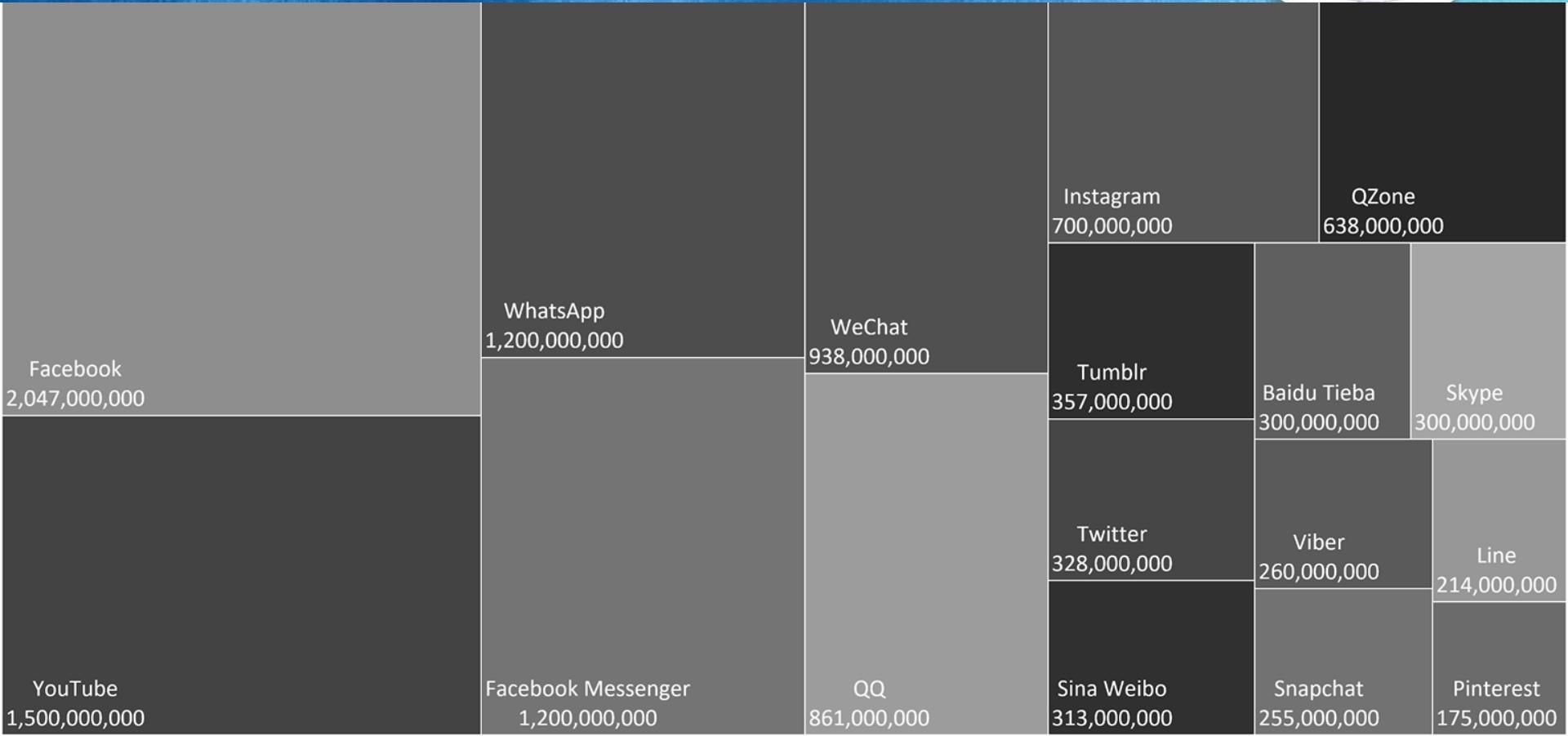


One Cyberspace

New Nations



#RSAC



Old Nation-States





TILLERSON PRINTS OUT TRUMP'S TWEETS TO HELP SET FOREIGN POLICY



BY ABIGAIL TRACY

JANUARY 17, 2018 6:15 PM

The secretary of state says it's "not a bad system."

Foreign Policy

VANITY FAIR



St Petersburg Florida?



npr

change station?



ON AIR NOW
NPR 24 Hour Program Stream

#RSAC



4:18

TECHNOLOGY

Russian Bots Are Spreading False Information After The Florida Shooting

February 20, 2018 · 4:38 PM ET

Heard on All Things Considered

+ Queue

Download

Embed

Transcript

AARTI SHAHANI



It's known that Russian groups used Facebook and other social media platforms to spread false information during the 2016 election, but now Russian bots are doing the same after the Florida shooting. So, how are tech giants thinking about tackling these



Account Hijacking



CyberCaliphate

CyberCaliphate

i love you isis

U.S. Central Command @CENTCOM

Official Twitter for U.S. Central Command (CENTCOM). *Follow/RT does not equal endorsement.

MacDill AFB, Tampa, FL

centcom.mil

Joined March 2009

TWEETS 3,678 FOLLOWING 1,268 FOLLOWERS 110K FAVORITES 30

Tweets Tweets & replies Photos & videos

 U.S. Central Command @CENTCOM · 6s

Pentagon Networks Hacked. Korean Scenarios

- Korean People's Army has called up 500,000 reservists to secure major military installations
- Pyongzang has elevated defensive posture
- North Korean ground forces are building
- 22 Nuclear facilities in 18 locations
- Research centers - Yongbyon and Gunch'on

Account Hijacking



 **Bank of Melbourne**
@BankofMelb

[Follow](#) ▾

ATTN: Unauthorised DMs sent bw 4-5pm today, do not click link. No customer/personal data compromised. Apologies for the inconvenience. ^TT

RETWEETS LIKES
8 2



1:03 AM - 14 Sep 2011

Have you asked the question...



**Who's running your
social media
accounts?**

Account Hijacking



#RSAC



vergecurrency
@vergecurrency

- >privacy coin
- >lead developer gets hacked
- >1b \$XVG stolen

2:58 PM - 13 Mar 2018



Social-Powered Social Engineering



DARKReading

Join us live at

InteropITX

Authors

Slideshows

Video

Tech Library

University

Radio

Calendar

Black Hat News

ANALYTICS

ATTACKS /
BREACHES

APP SEC

CAREERS &
PEOPLE

CLOUD

ENDPOINT

IoT

MOBILE

OPER

ENDPOINT

11/7/2017
10:30 AM

How I Infiltrated a Fortune 500 Company with Social Engineering



Getting into the company proved surprisingly easy during a contest. Find out how to make your company better prepared for real-world attacks.

Mia Ash



Riddle, Mystery, Enigma



Propagation
Payload



North Korea



#RSAC



Virtual Plots



#RSAC



counterwording Counter Bullying

@RayMajik Did you know that Facebook is disabling the accounts of activists? <http://is.gd/c3sQH>

27 minutes ago



counterwording Counter Bullying

@mikeydee1010 Did you know that Facebook is disabling the accounts of activists? <http://is.gd/c3sQH>

1 hour ago



counterwording Counter Bullying

@HagamosAficion Did you know that Facebook is disabling the accounts of activists? <http://is.gd/c3sQH>

2 hours ago

Real Revolution



counterwording Counter Bullying

@liannestewart Did you know that Facebook is disabling the accounts of activists? <http://is.gd/c3sQH>

3 hours ago

1 to Many Comms



Donald J. Trump 

@realDonaldTrump



I never said Russia did not meddle in the election, I said "it may be Russia, or China or another country or group, or it may be a 400 pound genius sitting in bed and playing with his computer." The Russian "hoax" was that the Trump campaign colluded with Russia - it never did!

12:33 PM - Feb 18, 2018



people are talking about this



Deep State, Deep Fake



THE DEEPFAKE SOCIETY

Search... ADVERTISE WITH US 5 MILLION VISITS AND COUNTING

Home Categories Submit Deepfakes via URL How to Create Deepfakes DEEFAKE FORUM /deepfakes/ Contact

JAMES BOND IS NOT BLACK, ITS NIC CAGE – Nick Cage is the Terminator – deepfakes Putin / Trump – Deepfakes Donald Trump as Michael Scott from The Office – Donald Trump as Biff Tannen from Back To The NIC CAGE vs John Travolta – Deepfakes face off

THE GREAT MEME WAR dot com

Upload your Deepfakes

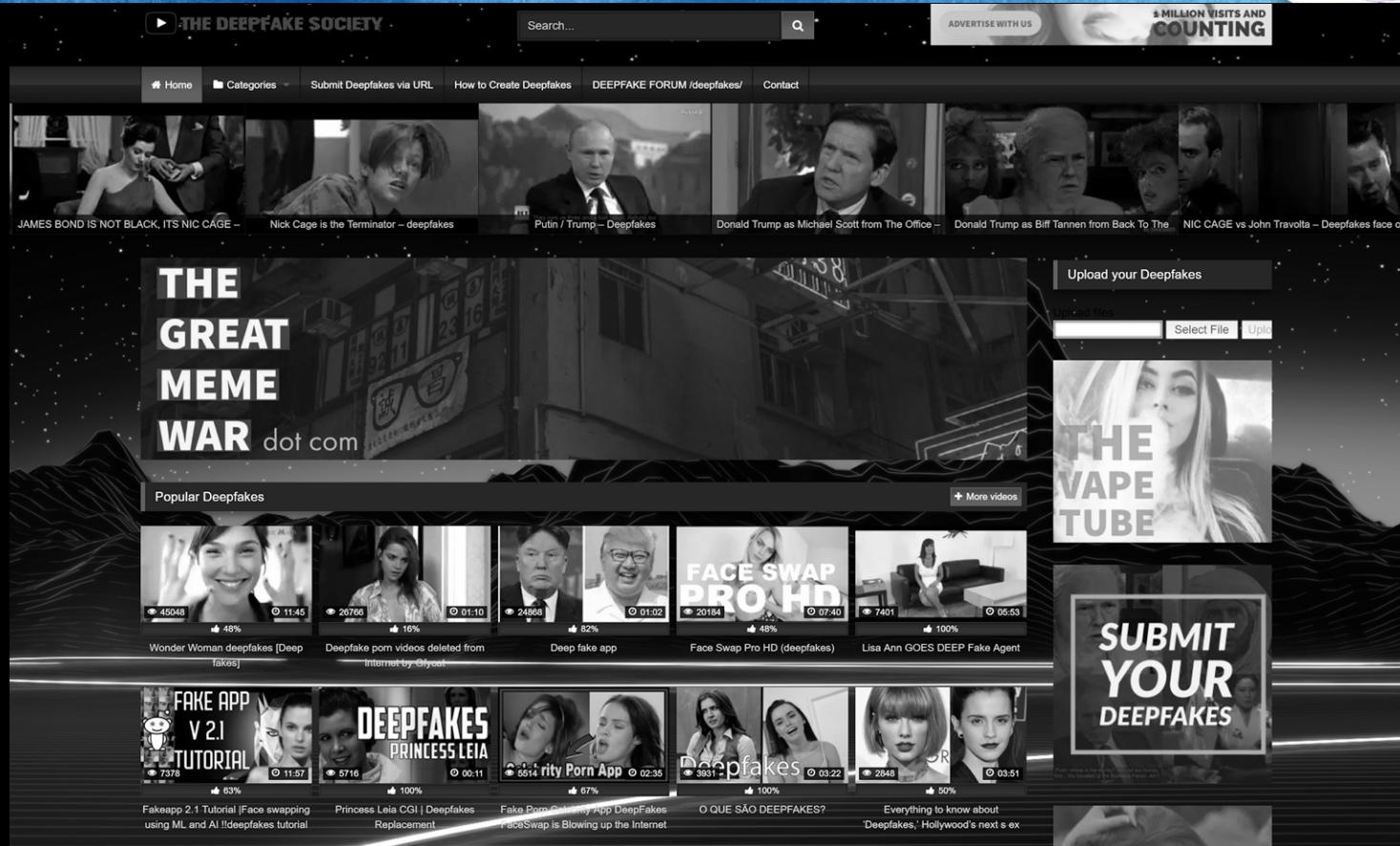
Popular Deepfakes + More videos

Wonder Woman deepfakes [Deep 45048] 48% 11:45 Deepfake porn videos deleted from Internet by Olycast 26766 16% 01:10 Deep fake app 24868 82% 01:02 FACE SWAP PRO HD [20164] 48% 07:40 Face Swap Pro HD (deepfakes) 7401 100% 05:53 Lisa Ann GOES DEEP Fake Agent

FAKE APP V 21 TUTORIAL [7378] 63% 01:57 DEEPFAKES PRINCESS LEIA [5716] 100% 00:11 FAKE Porn CGI |Fake Porn App DeepFakes Replacement [5514] 67% 02:35 Deepfakes [3631] 100% 03:22 O QUE SÃO DEEPFAKES? [2848] 50% 03:51 Everything to know about 'Deepfakes,' Hollywood's next sex revolution

SUBMIT YOUR DEEPFAKES

Fakeapp 2.1 Tutorial |Face swapping using ML and AI !deepfakes tutorial Princess Leia CGI |Deepfakes Replacement Fake Porn CGI |Fake Porn App DeepFakes /faceSwap is Blowing up the Internet O QUE SÃO DEEPFAKES? Everything to know about 'Deepfakes,' Hollywood's next sex revolution



No Pressure



#RSAC

OSINT



#RSAC



Employees can use social media

Employees will use social media

Social media will be exploited

Selfie Soldiers



#RSAC

VICE
NEWS



7 minutes ago | Comment

Share Like



Simon Ostrovsky

Online

There are pictures of you taken in Ukraine,
and pictures of me taken in the same spot in Ukraine.

► ▶ 18:55 / 23:13

CC HD

What to do?



#RSAC



WikiLeaks Task Force

@WLTaskForce



Follow

We are thinking of making an online database
with all "verified" twitter accounts & their
family/job/financial/housing relationships.

RETWEETS

41

LIKES

80



10:03 AM - 6 Jan 2017



55



41



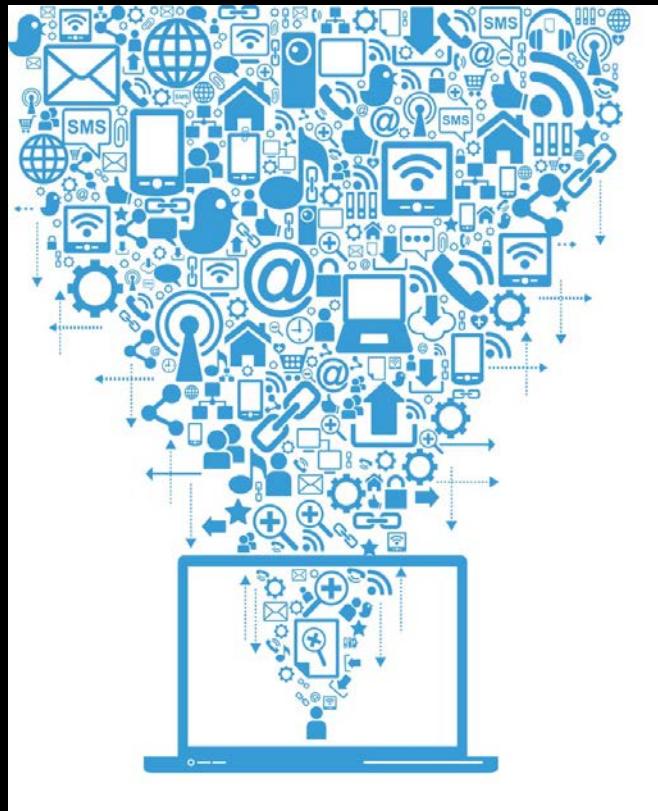
80

...

Social threat intelligence



#RSAC



APPLY 1: Build a social media policy



- Work with communications teams to build a social media policy
- What can and can't be posted?
- Who and how should employees interact online?
- How to report abuses and potential threats?
- Best practices for hardening account
- Breach notification and lost credentials
- Document policies and share with company

APPLY 2: Harden social accounts



- Enable 2FA
- Audit who has access to what accounts
- Ensure stakeholders have proper controls on personal accounts/devices
- Leverage a management platform
- Audit 3rd party applications
- Enable a monitoring tool to lock accounts in case of a takeover

APPLY 3: Train employees, work with comms



- Distribute the social media policy
- Establish employee training and testing on social media
- Monitor for abuses
- Run penetration tests

APPLY 4: Ingest data into the SOC



- Leverage network APIs to stream data into your SOC
- Leverage a social media protection platform to identify targeted threats