RSAConference2018
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

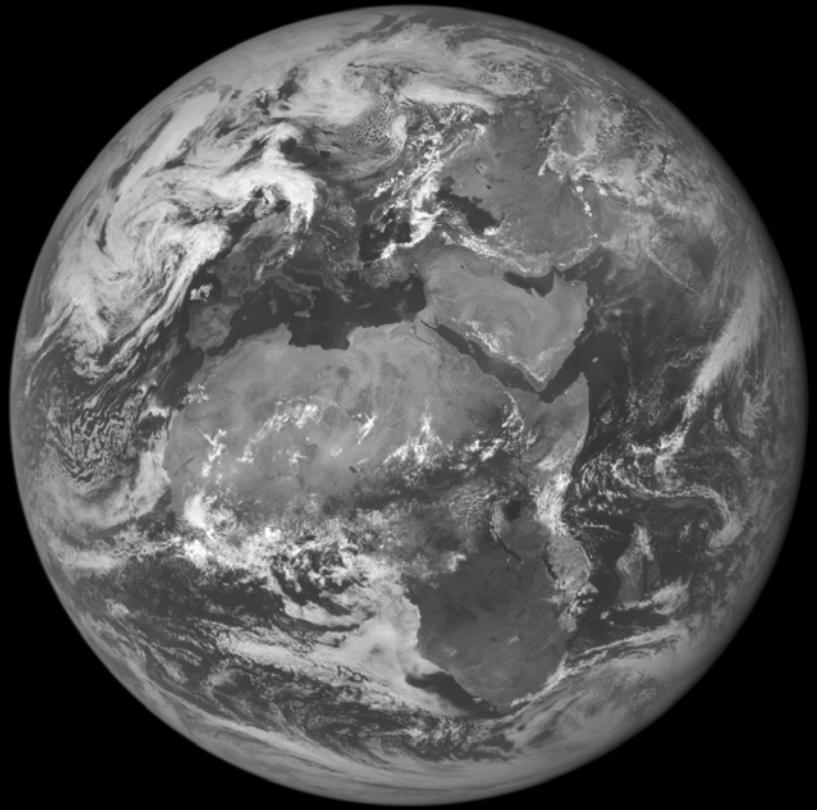
17K years old.

Seeing is Believing

Intelligent phones

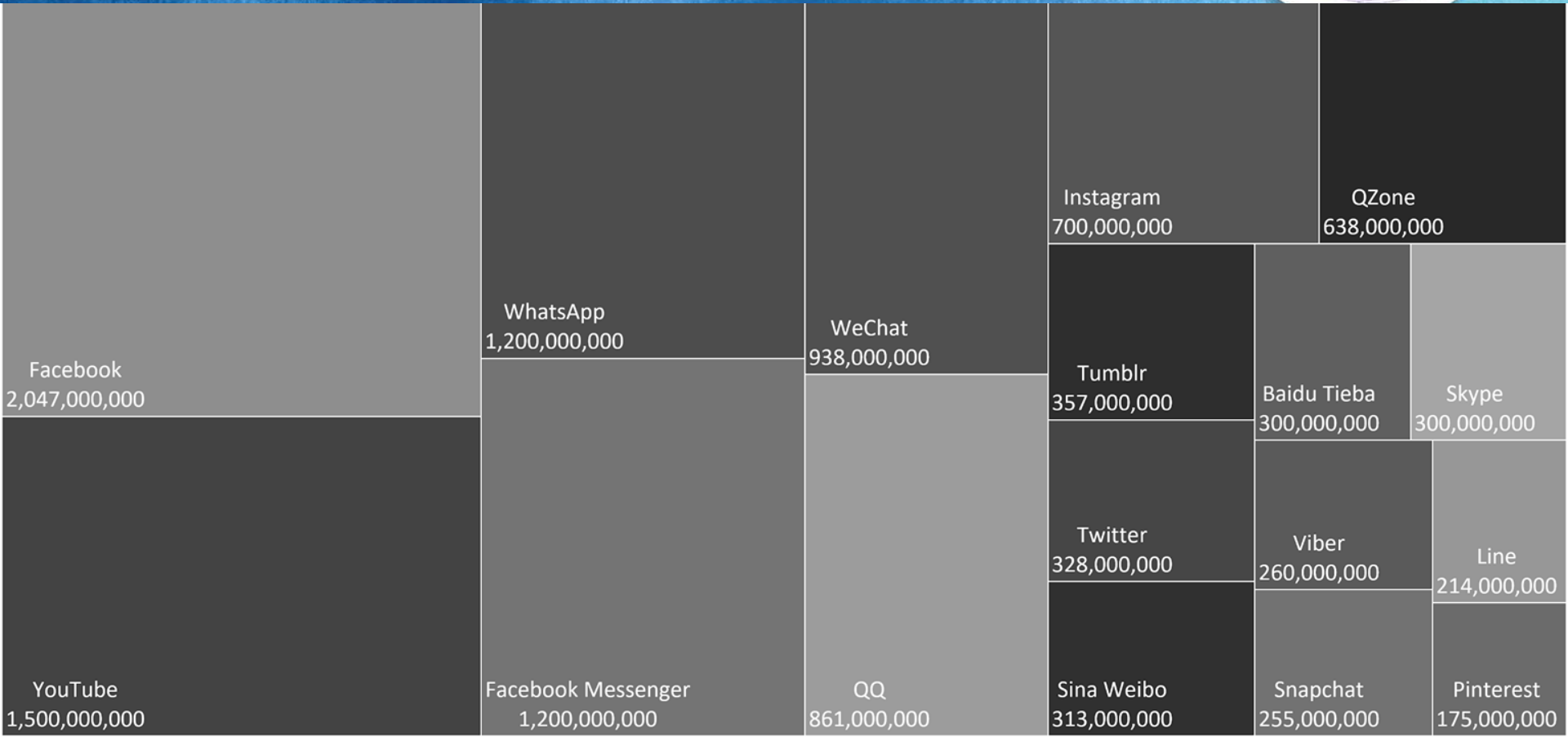
National springs and color revolutions

One Internet



One Cyberspace

New Nations



Old Nation-States

Foreign Policy

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?

TECHNOLOGY

Russian Bots Are Spreading False Information After The Florida Shooting

4:18

+ Queue

Download

Embed

Transcript

February 20, 2018 · 4:38 PM ET
Heard on All Things Considered

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

ove you isis

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

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 | Tweets & replies | Photos & videos

U.S. Central Command @CENTCOM · 6s

Pentagon Networks Hacked. Korean Scenarios

• Korean's People Army has called up 500,000 reservists to secure major military installations
• P'yongyang has elevated defensive posture
• North Korean ground forces are building

• 22 Nuclear facilities in 18 locations
• Research centers - Yongbyon and Gunch'on

Account Hijacking

Have you asked the question…

Who's running your social media accounts?

Account Hijacking

Social-Powered Social Engineering

DARKReading | Join us live at Interop ITX

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

Virtual Plots

Real Revolution

1 to Many Comms

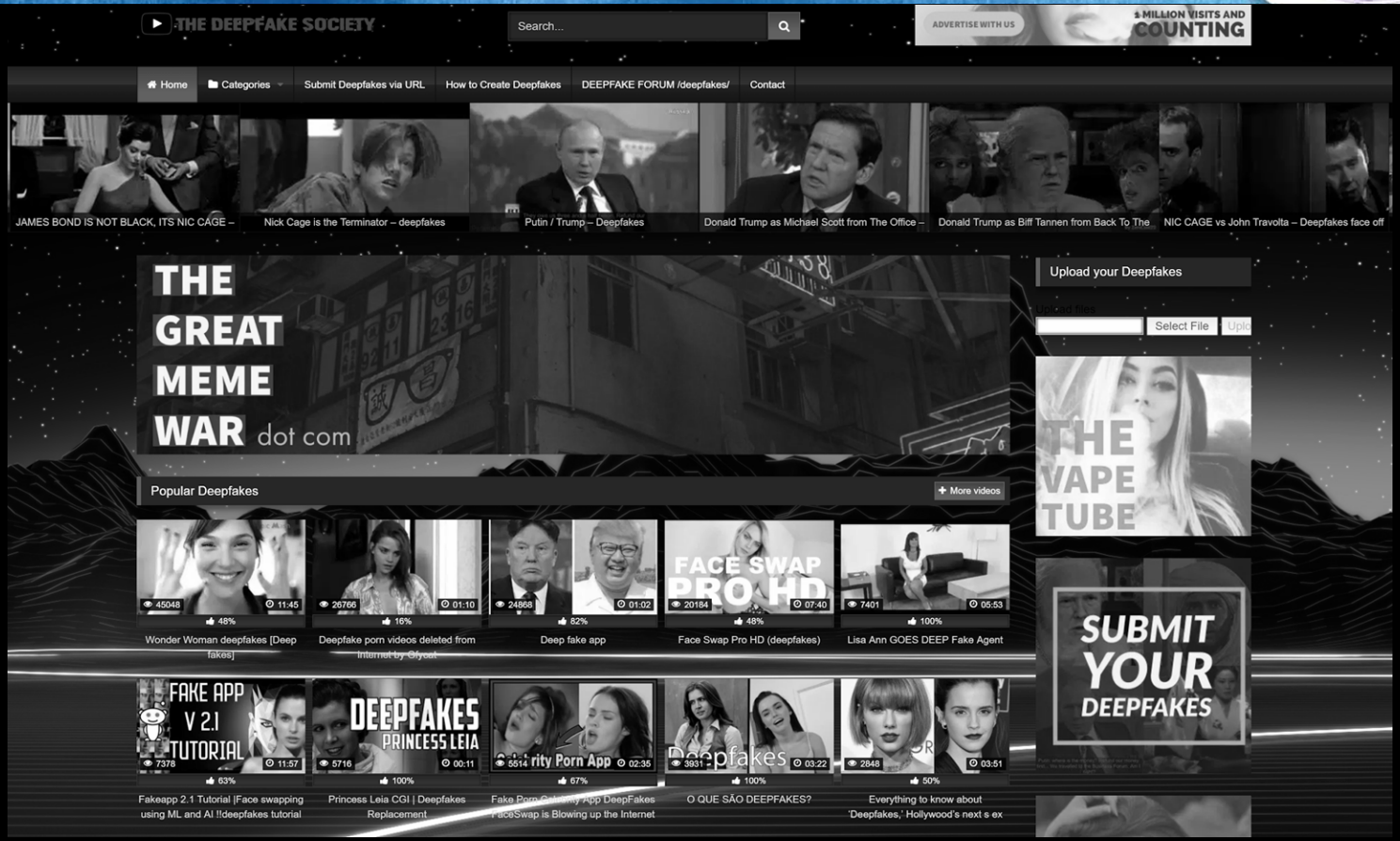
Donald J. Trump
@realDonaldTrump

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

126K 72.6K people are talking about this

Deep State, Deep Fake



No Pressure

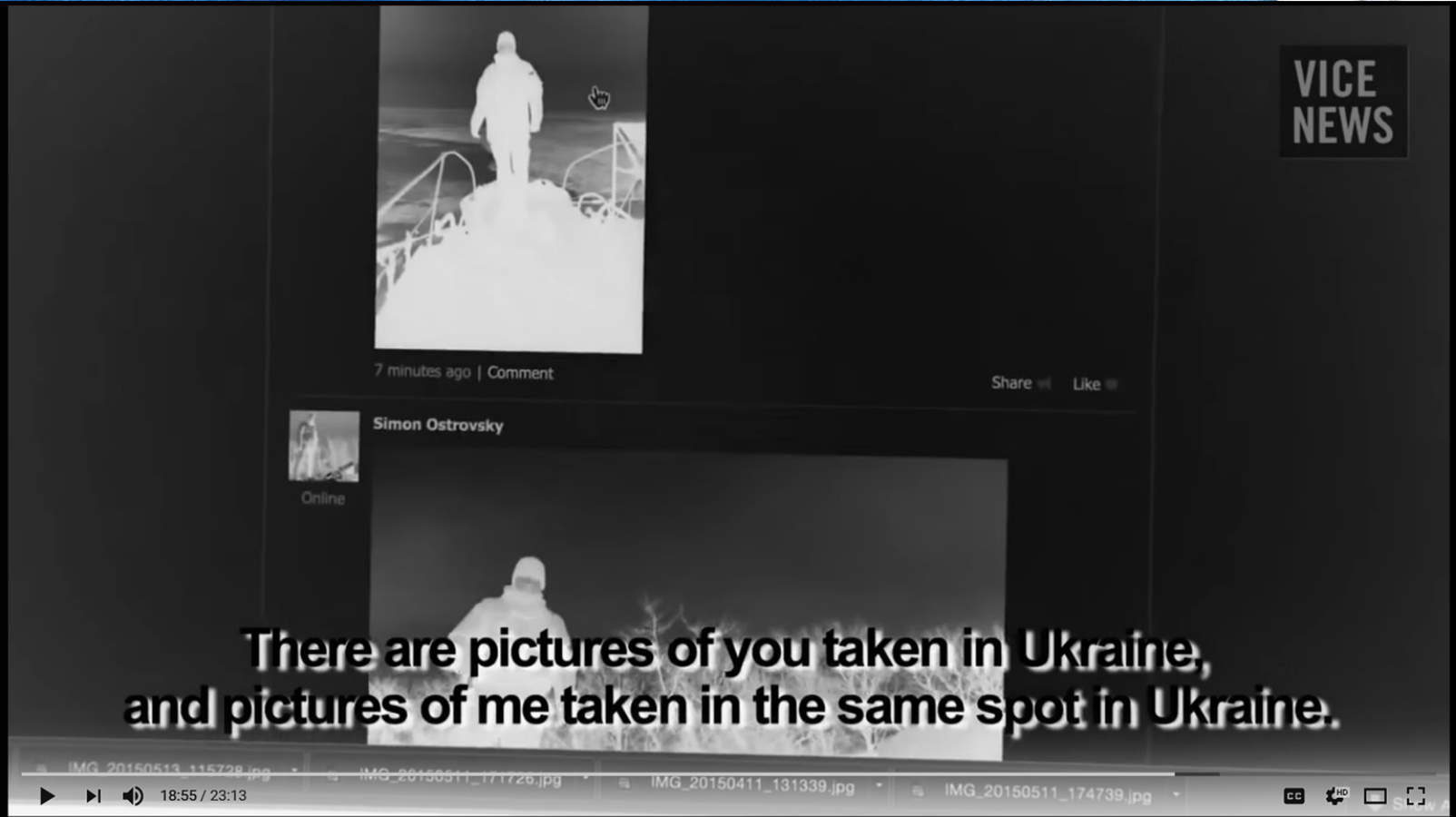
OSINT

Employees can use social media

Employees will use social media

Social media will be exploited

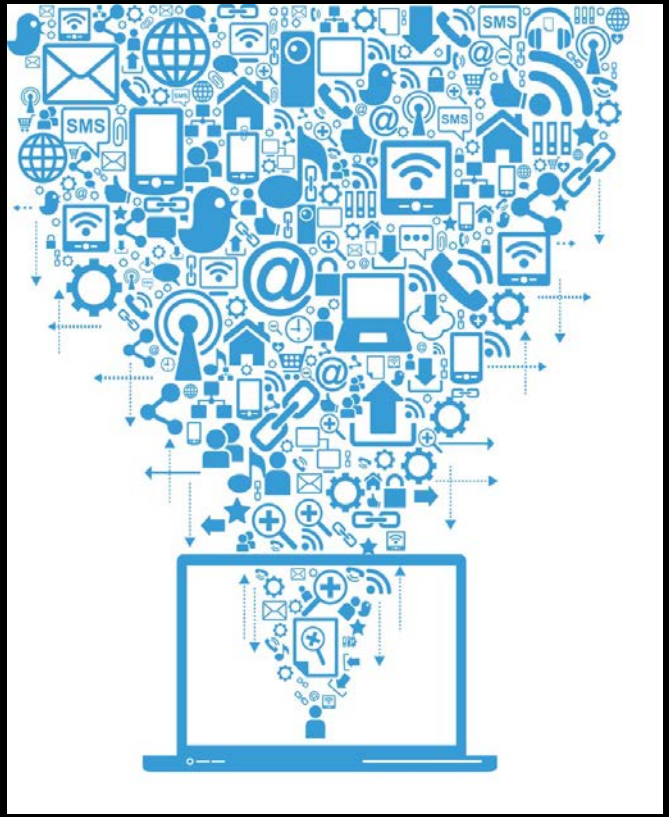
Selfie Soldiers



What to do?


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



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