Conversation with

Fulton T. Armstrong

Cyberwar: The New Battlefield

Spy Wars

Cyber war

KINDS

- country vs. country
- business, political, or criminal
- official vs condoned vs independent
- before-fact vs after-fact

INTELLIGENCE

COVERT ACTION

ALL made easier because …

“On the Internet, nobody knows you’re a dog.”

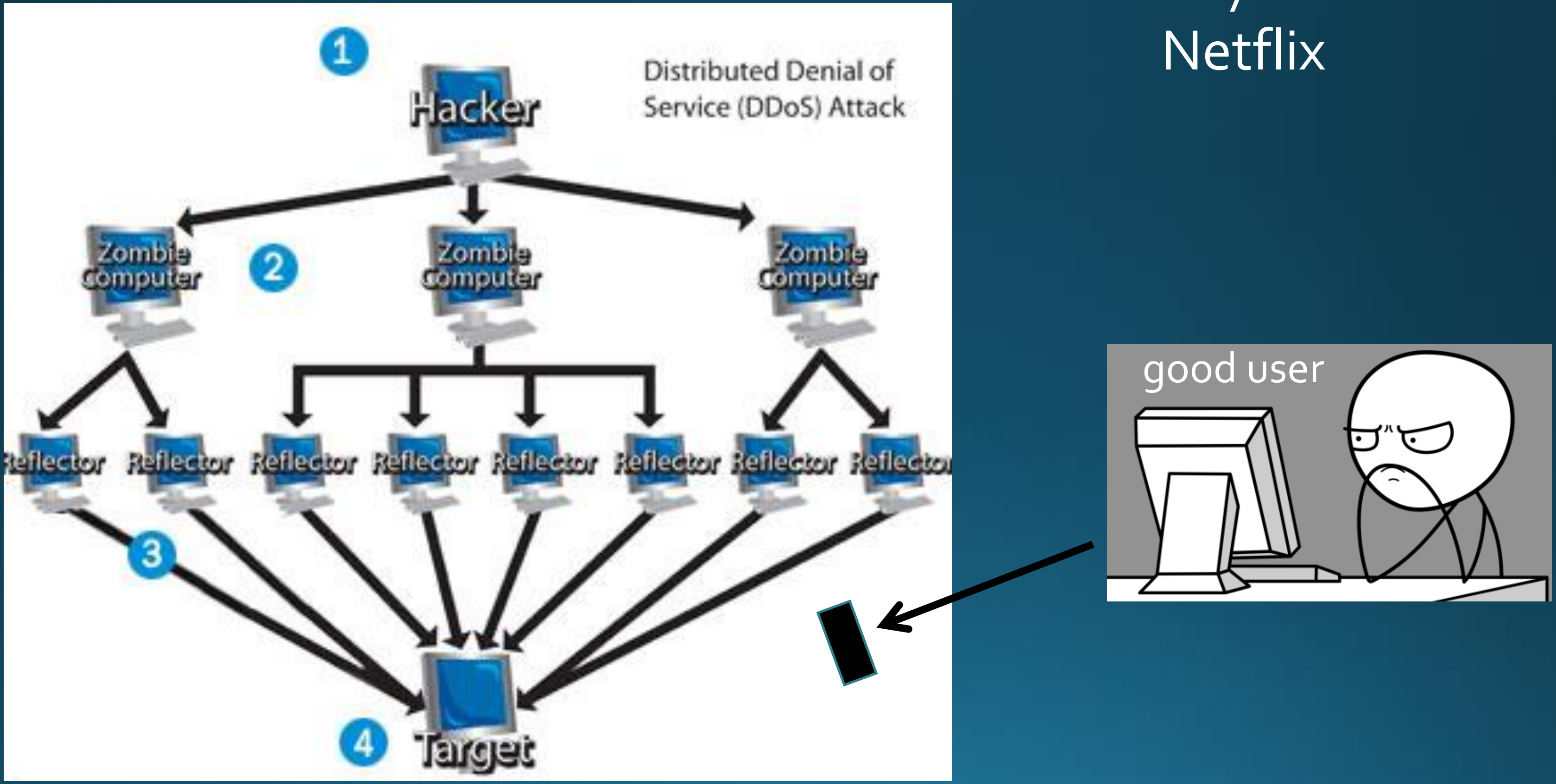
©The New Yorker, 1993

Forms

Distributed Denial of Service DDOS

Many Famous cases:

- BBC
- Sony
- PayPal
- Netflix



Potential impact: Interrupt any public or private service that uses the internet, including SCADA

Supervisory Control and Data Acquisition

Infrastructure!!!!

Essential services!!!!

THINGS THAT WE NEED!!!!!

> “Much of the U.S. critical infrastructure is potentially vulnerable to cyberattack.”

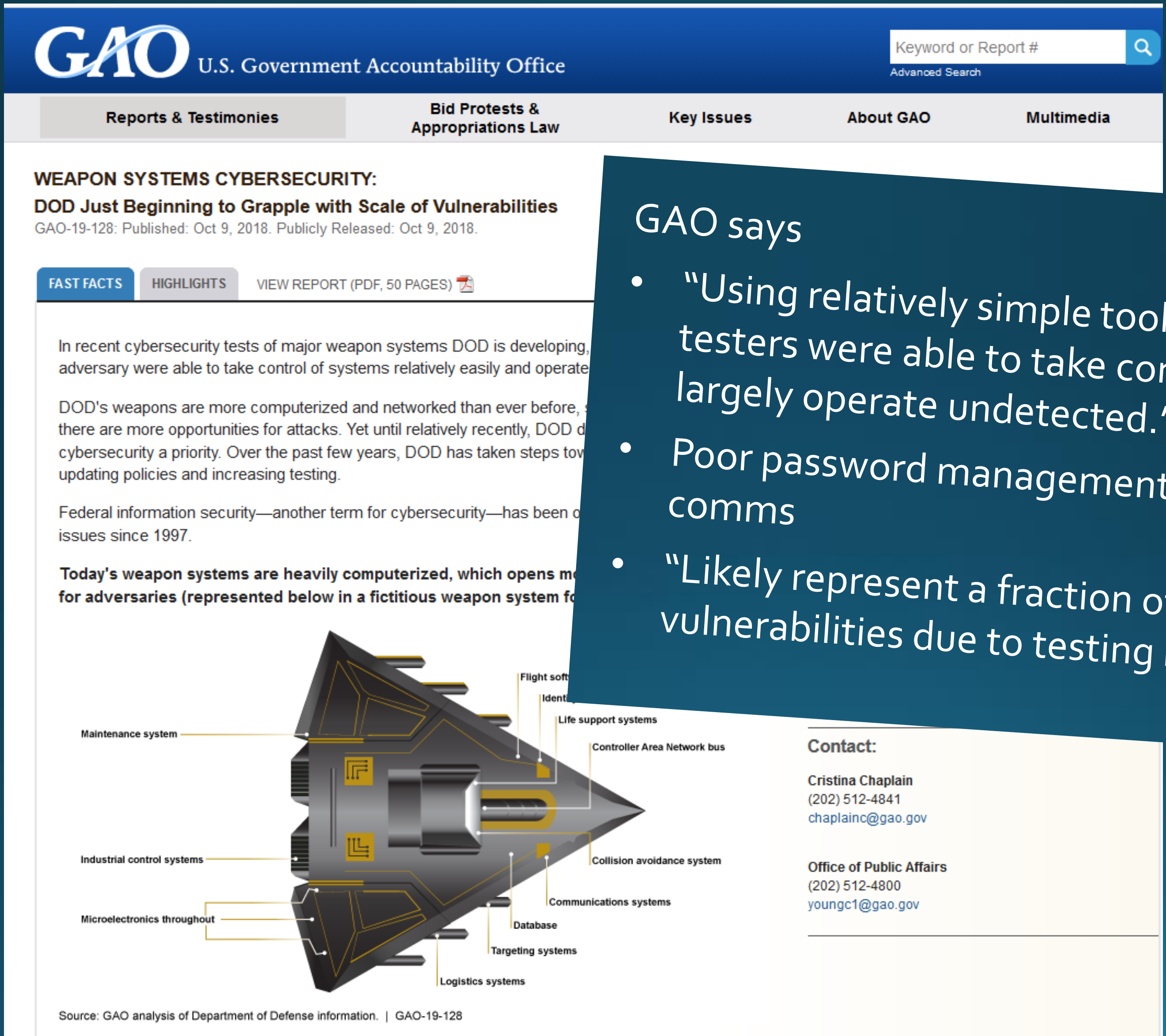
-- U.S. Congressional Research Service
and
many, many, many other experts

ATTACK

Now alarmingly common!
((But not always discussed))

- 3 weeks (May)
- Disrupt services
- Leaked NSA tool (NSA denies)
- “Eternal Blue”
- Ransom, harass
- $18.2m cost

Even weapons systems are not safe



GAO U.S. Government Accountability Office

WEAPON SYSTEMS CYBERSECURITY:

DOD Just Beginning to Grapple with Scale of Vulnerabilities

GAO-19-128: Published: Oct 9, 2018. Publicly Released: Oct 9, 2018.

In recent cybersecurity tests of major weapon systems DOD is developing, adversary were able to take control of systems relatively easily and operate

DOD's weapons are more computerized and networked than ever before, there are more opportunities for attacks. Yet until relatively recently, DOD d cybersecurity a priority. Over the past few years, DOD has taken steps tow updating policies and increasing testing.

Federal information security—another term for cybersecurity—has been o issues since 1997.

Today's weapon systems are heavily computerized, which opens m for adversaries (represented below in a fictitious weapon system fo

Source: GAO analysis of Department of Defense information. | GAO-19-128

Contact:

Cristina Chaplain
(202) 512-4841
chaplainc@gao.gov

Office of Public Affairs
(202) 512-4800
youngc1@gao.gov

GAO says

- "Using relatively simple tools and techniques, testers were able to take control of systems and largely operate undetected."
- Poor password management, unencrypted comms
- "Likely represent a fraction of total vulnerabilities due to testing limitations"

Forms

DNS Hijacking

aka DNSpionage

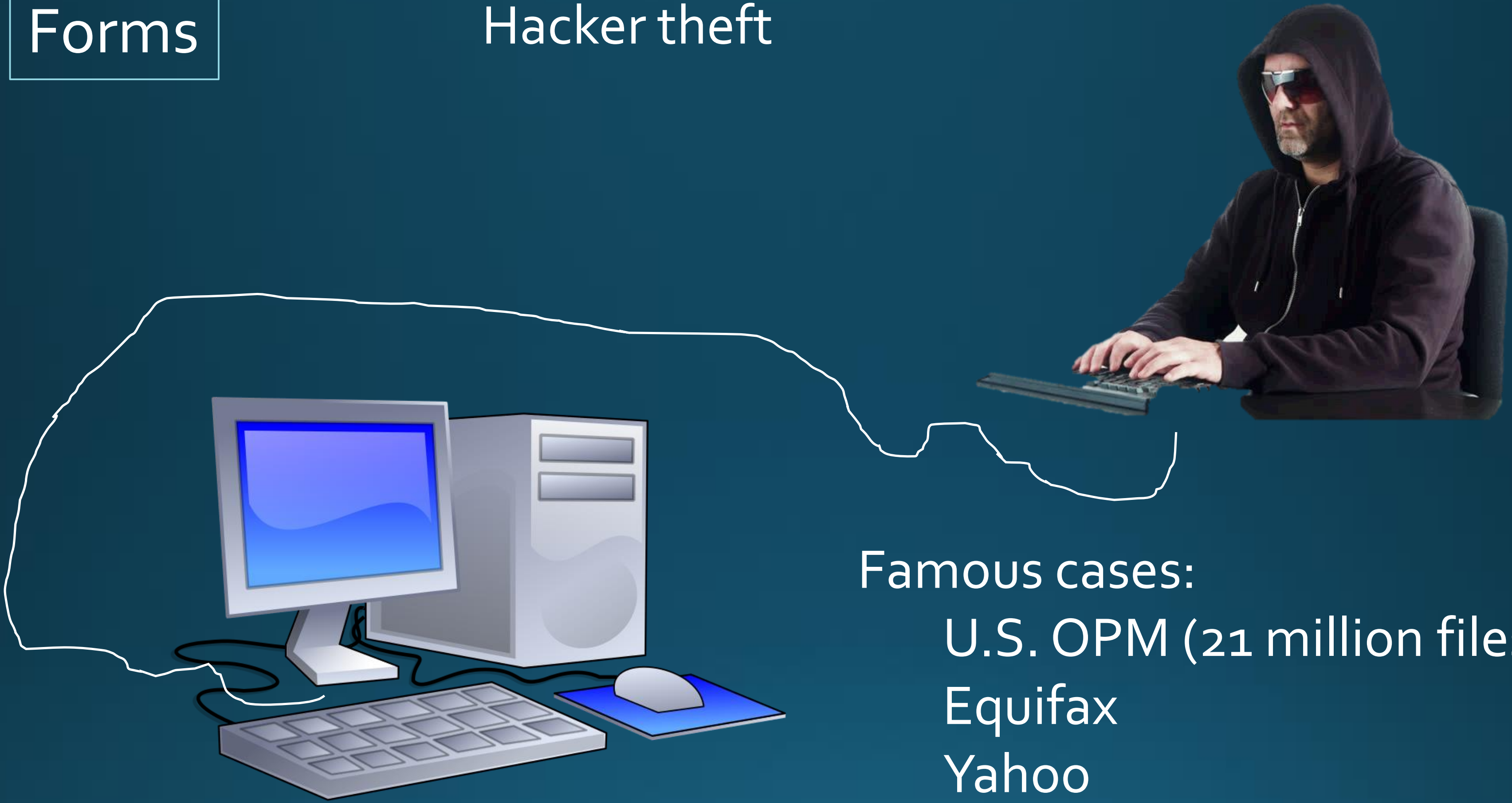
Attack "Domain Name System" servers so that …

- You enter "bigbank.com"
- Usually DNS servers point you to 64.233.191.255
- But after hack, they send you to 126.434.1.045

BADGUYS.COM

Forms

Hacker theft



Famous cases:

- U.S. OPM (21 million files!!)
- Equifax
- Yahoo
- LinkedIn
- Target
- Many major companies

Now common …

November 2018 report

Hackers stole

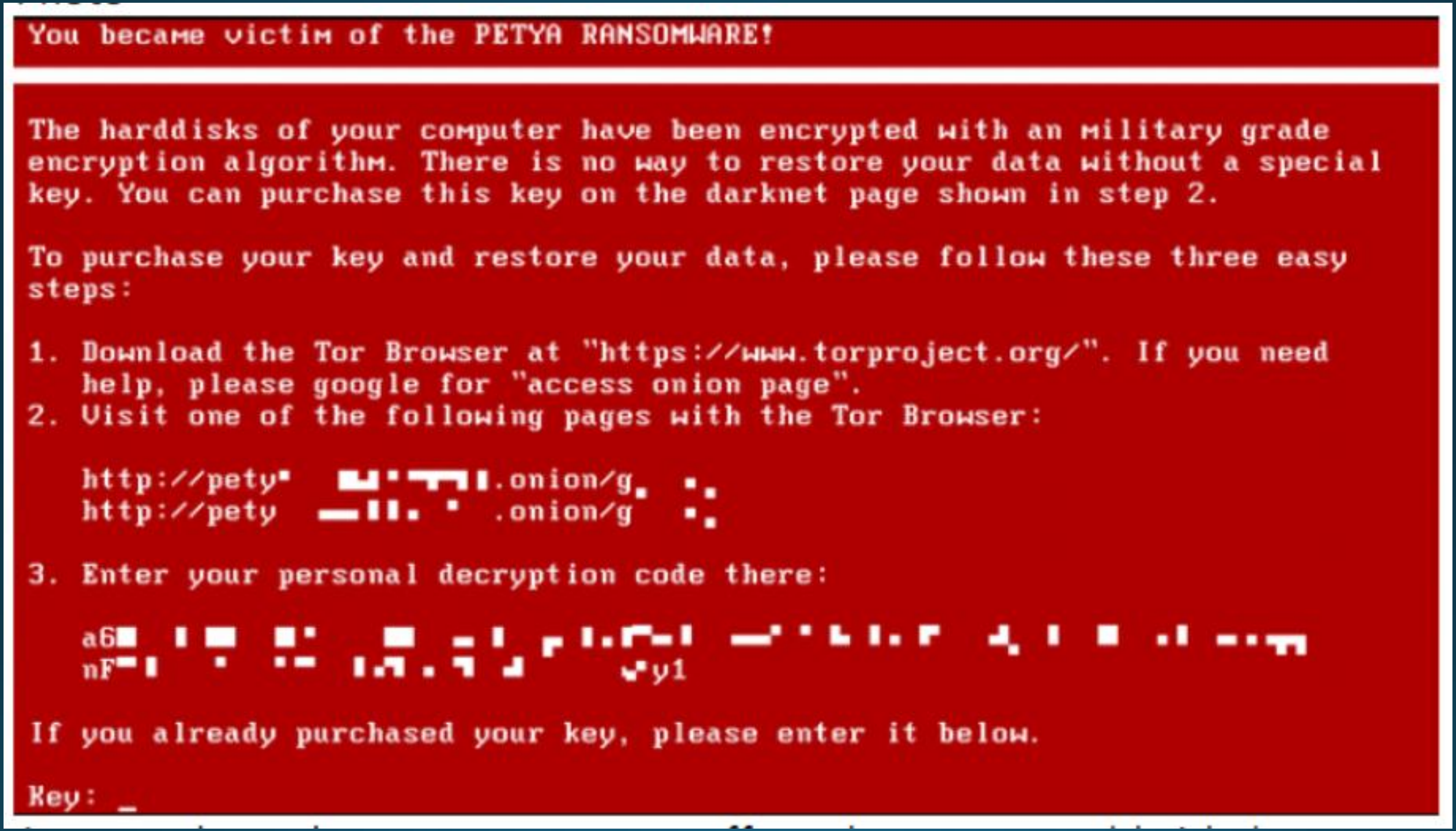
- 500 million customer records
- Names, addresses, credit cards, passports
- From Starwood reservation system
- Since 2014

MOST COMMON PURPOSE:

RANSOM … EXTORTION … INFORMATION SUPERHIGHWAY ROBBERY

RANSOM … EXTORTION … INFORMATION SUPERHIGHWAY ROBBERY

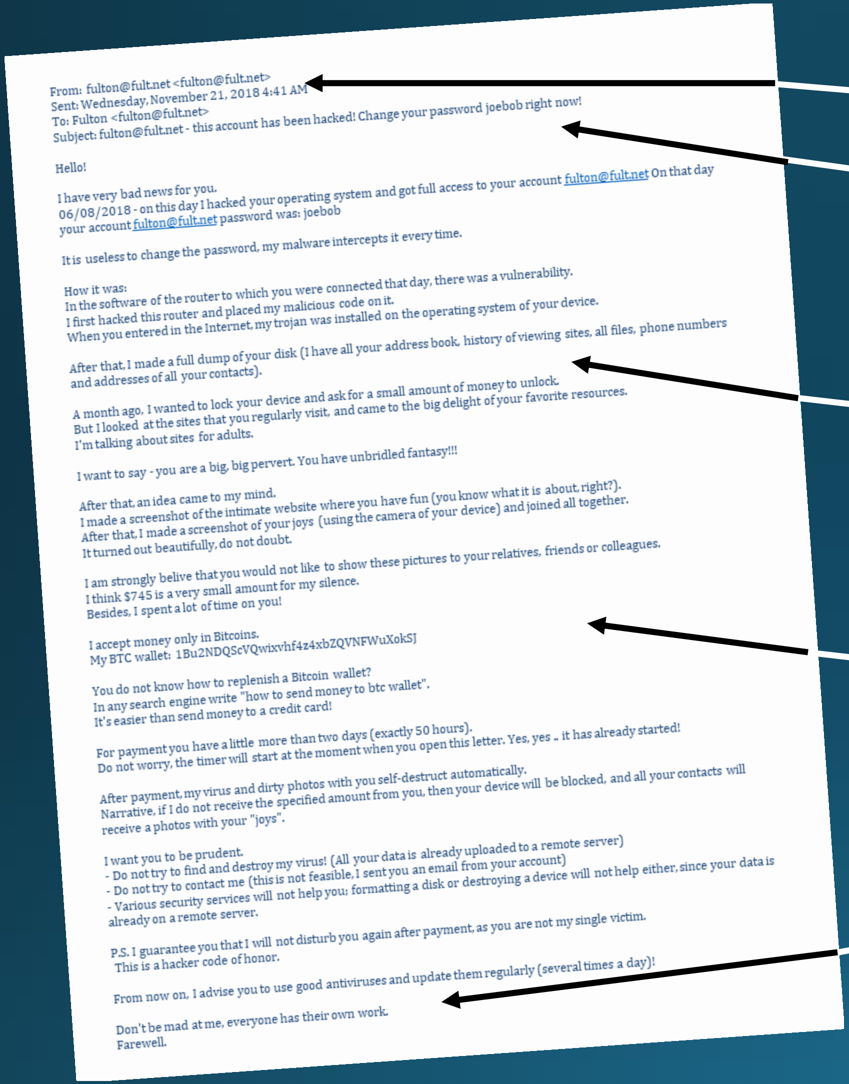
RANSOM … EXTORTION … INFO SUPERHIGHWAY ROBBERY



```
You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://pety[redacted].onion/g[redacted]
   http://pety[redacted].onion/g[redacted]

3. Enter your personal decryption code there:

   a6[redacted]
   nF[redacted]y1

If you already purchased your key, please enter it below.

Key: _
```

With detailed instructions on how to pay the ransom …
get the key … and decrypt.

Trying to Make it Personal



From: fulton@fult.net <fulton@fult.net>
Sent: Wednesday, November 21, 2018 4:41 AM
To: Fulton <fulton@fult.net>
Subject: fulton@fult.net - this account has been hacked! Change your password joebob right now!

Hello!

I have very bad news for you.
06/08/2018 - on this day I hacked your operating system and got full access to your account fulton@fult.net On that day
your account fulton@fult.net password was: joebob

It is useless to change the password, my malware intercepts it every time.

How it was:
In the software of the router to which you were connected that day, there was a vulnerability.
I first hacked this router and placed my malicious code on it.
When you entered in the Internet, my trojan was installed on the operating system of your device.

After that, I made a full dump of your disk (I have all your address book, history of viewing sites, all files, phone numbers
and addresses of all your contacts).

A month ago, I wanted to lock your device and ask for a small amount of money to unlock.
But I looked at the sites that you regularly visit, and came to the big delight of your favorite resources.
I'm talking about sites for adults.

I want to say - you are a big, big pervert. You have unbridled fantasy!!!

After that, an idea came to my mind.
I made a screenshot of the intimate website where you have fun (you know what it is about, right?).
After that, I made a screenshot of your joys (using the camera of your device) and joined all together.
It turned out beautifully, do not doubt.

I am strongly belive that you would not like to show these pictures to your relatives, friends or colleagues.
I think $745 is a very small amount for my silence.
Besides, I spent a lot of time on you!

I accept money only in Bitcoins.
My BTC wallet: 1Bu2NDQScVQwixvhf4z4xbZQVNFWuXokSJ

You do not know how to replenish a Bitcoin wallet?
In any search engine write "how to send money to btc wallet".
It's easier than send money to a credit card!

For payment you have a little more than two days (exactly 50 hours).
Do not worry, the timer will start at the moment when you open this letter. Yes, yes .. it has already started!

After payment, my virus and dirty photos with you self-destruct automatically.
Narrative, if I do not receive the specified amount from you, then your device will be blocked, and all your contacts will
receive a photos with your "joys".

I want you to be prudent.
- Do not try to find and destroy my virus! (All your data is already uploaded to a remote server)
- Do not try to contact me (this is not feasible, I sent you an email from your account)
- Various security services will not help you; formatting a disk or destroying a device will not help either, since your data is
already on a remote server.

P.S. I guarantee you that I will not disturb you again after payment, as you are not my single victim.
This is a hacker code of honor.

From now on, I advise you to use good antiviruses and update them regularly (several times a day)!

Don't be mad at me, everyone has their own work.
Farewell.

From: fulton@bmbs.org <fulton@bmbs.org>

Subject: fulton@bmbs.org - this account has been hacked! Change your password joebob right now!

I made a full dump of your disk (I have all your address book, history of viewing sites, all files, phone numbers and addresses of all your contacts).

I am strongly belive that you would not like to show these pictures to your relatives, friends or colleagues. I think $745 is a very small amount for my silence.

Don't be mad at me, everyone has their own work.

Nov 2018

Forms

Political manipulation

1) Manipulation of "Social Media"

2) Stolen and leaked e-mails

3) Direct penetrations of voting hardware

4) Deep fakes

Let’s start with the newest (and potentially scariest)

DEEP FAKES

University of Washington

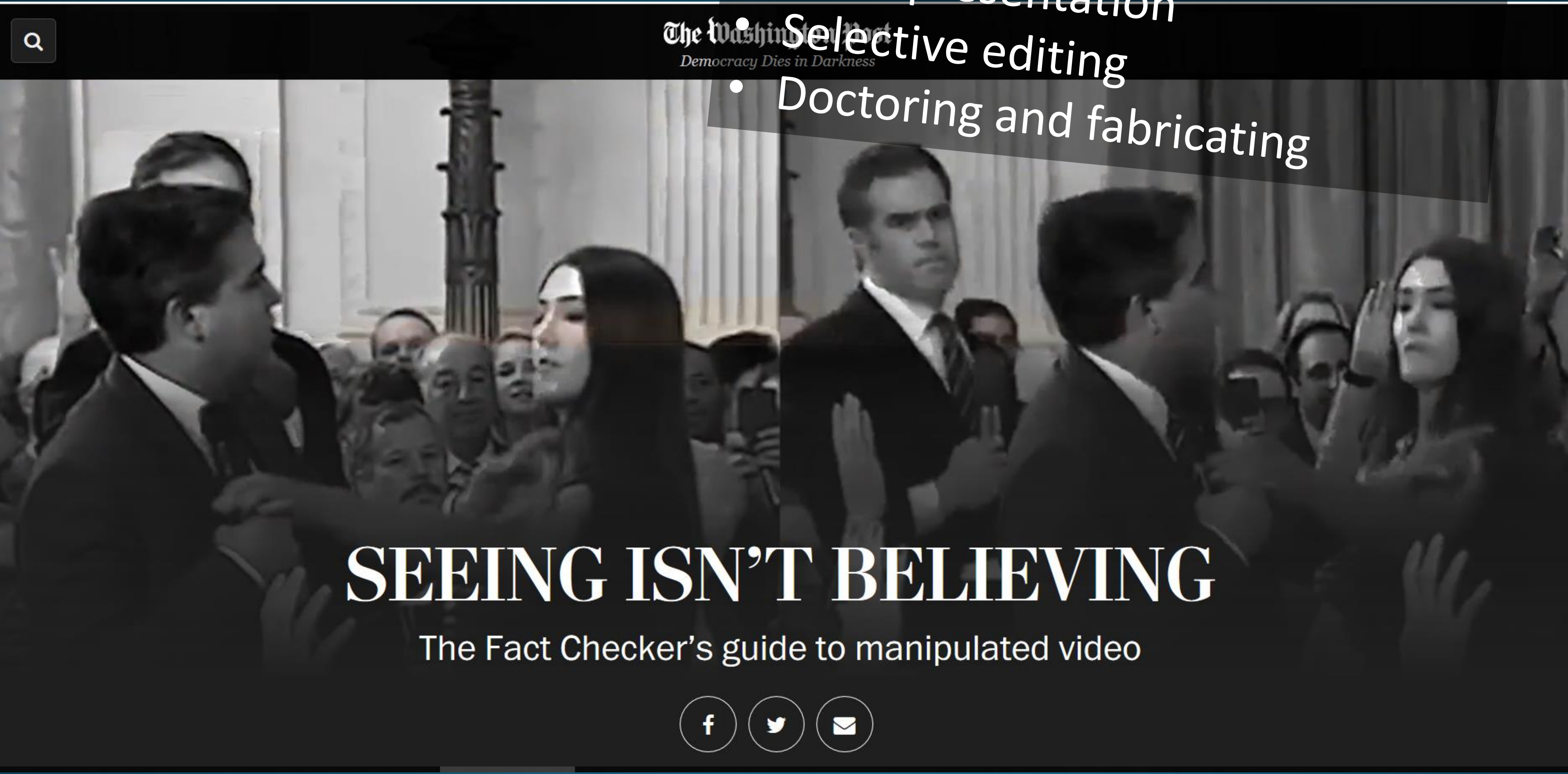
Artificial Intelligence to map face to sound

“Ground Truth” video → → → → → Fake Video

What to do?

Detect 3 kinds of manipulation:

- Misrepresentation
- Selective editing
- Doctoring and fabricating



The Washington Post
Democracy Dies in Darkness

SEEING ISN'T BELIEVING

The Fact Checker's guide to manipulated video

Who’s doing cyber ops?

Often difficult to determine specific cases, but … safe to say:

“Everyone does it”

“But some do it more than others” →

- Russia
- China
- North Korea
- Others

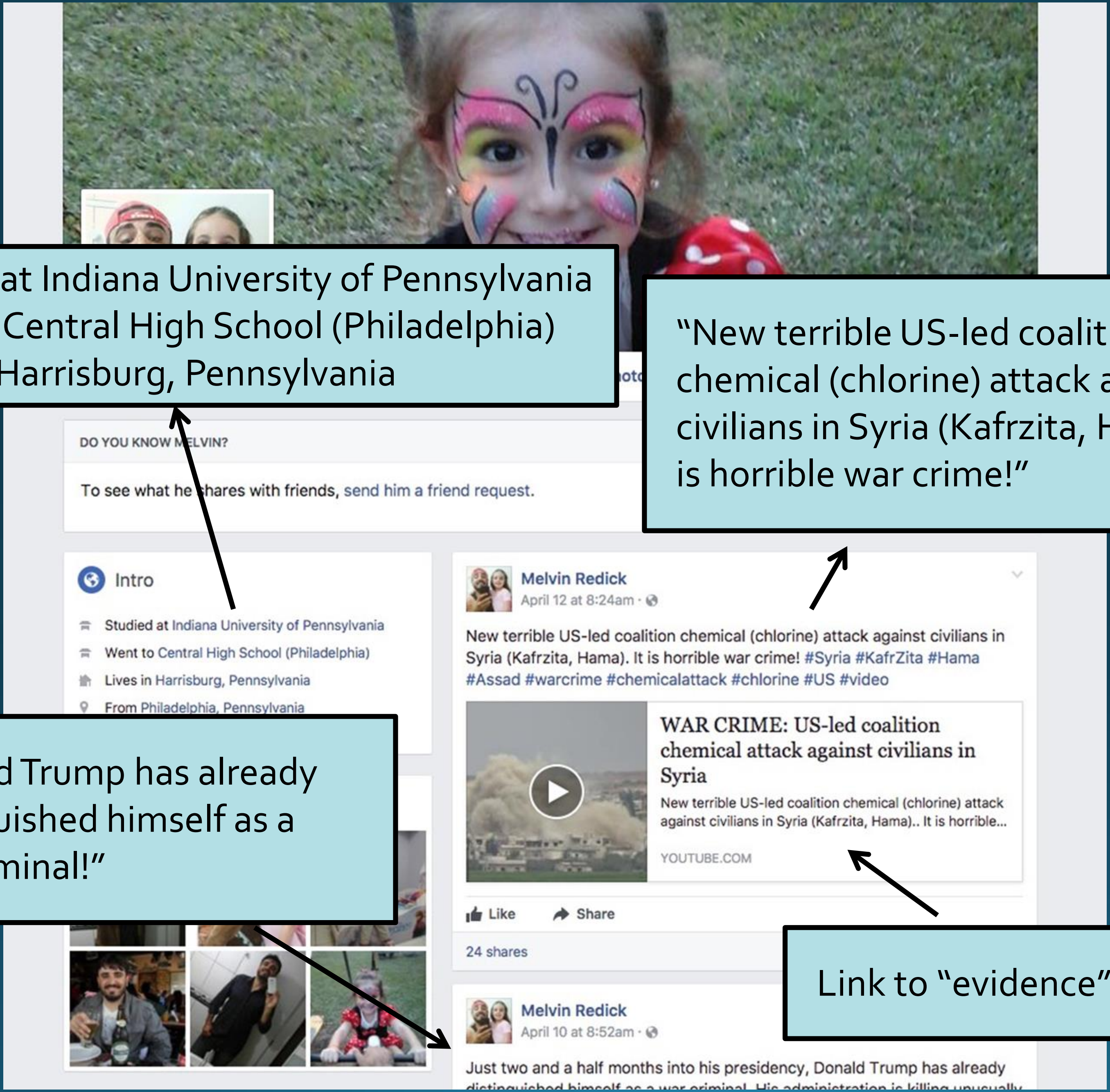
- USA?????

Some examples …

Trolls and Bots

Meet … Melvin Redick

- Harrisburg, Pennsylvania, USA
- Avid internet user
- Active in Facebook and Twitter
- Overall good guy



DO YOU KNOW MELVIN?

To see what he shares with friends, send him a friend request.

Intro

- Studied at Indiana University of Pennsylvania
- Went to Central High School (Philadelphia)
- Lives in Harrisburg, Pennsylvania
- From Philadelphia, Pennsylvania

Melvin Redick
April 12 at 8:24am ·

New terrible US-led coalition chemical (chlorine) attack against civilians in Syria (Kafrzita, Hama). It is horrible war crime! #Syria #KafrZita #Hama #Assad #warcrime #chemicalattack #chlorine #US #video

WAR CRIME: US-led coalition chemical attack against civilians in Syria

New terrible US-led coalition chemical (chlorine) attack against civilians in Syria (Kafrzita, Hama).. It is horrible...

YOUTUBE.COM

Like Share

24 shares

Melvin Redick
April 10 at 8:52am ·

Just two and a half months into his presidency, Donald Trump has already distinguished himself as a war criminal. His administration is killing unusually

Studied at Indiana University of Pennsylvania
Went to Central High School (Philadelphia)
Lives in Harrisburg, Pennsylvania

"New terrible US-led coalition chemical (chlorine) attack against civilians in Syria (Kafrzita, Hama). It is horrible war crime!"

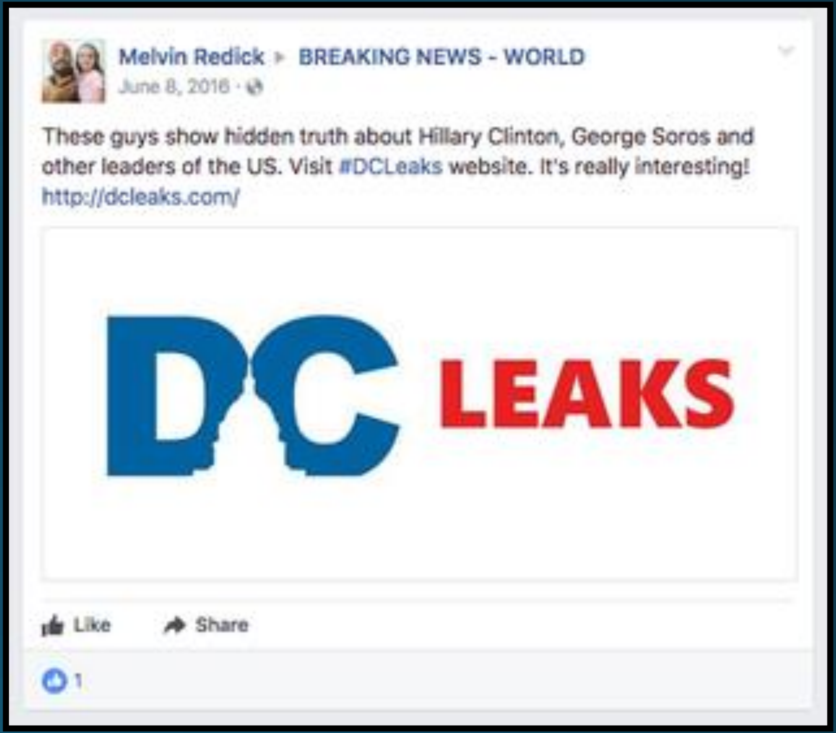
"Donald Trump has already distinguished himself as a war criminal!"

Link to "evidence"

Trolls and Bots

Melvin Redick

"These guys show hidden truth about Hillary Clinton, George Soros and other leaders of the US. Visit #DCLeaks website. It's really interesting!"



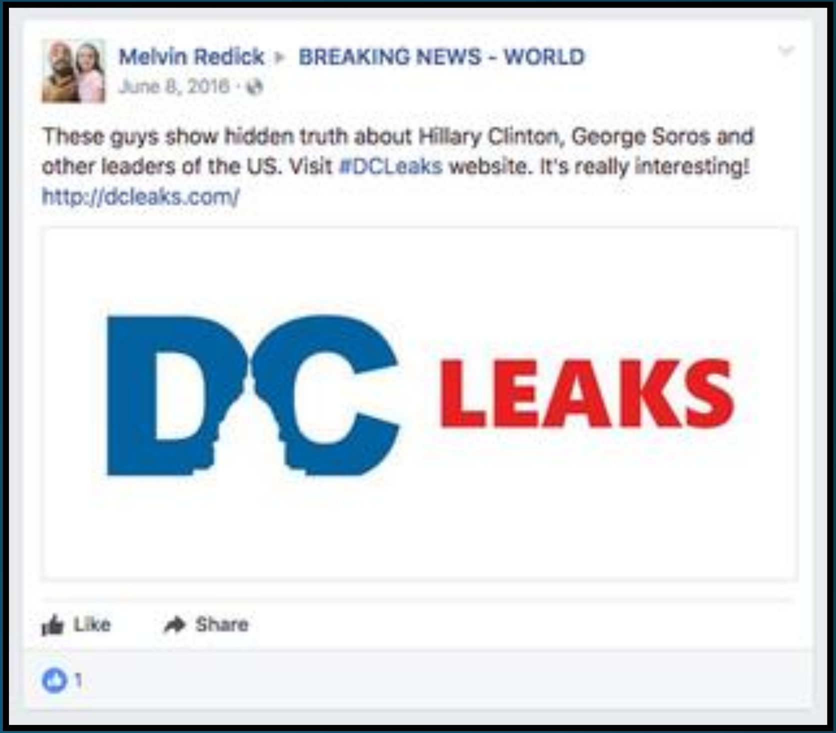
Melvin Redick ▸ BREAKING NEWS - WORLD
June 8, 2016 ·

These guys show hidden truth about Hillary Clinton, George Soros and other leaders of the US. Visit #DCLeaks website. It's really interesting!
http://dcleaks.com/

Trolls and Bots

Melvin Redick

The same morning … "Katherine Fulton" and "Alice Donovan" also praised #DCLeaks, while attacking Open Society Foundation



Melvin Redick ▸ BREAKING NEWS - WORLD
June 8, 2016 ·

These guys show hidden truth about Hillary Clinton, George Soros and other leaders of the US. Visit #DCLeaks website. It's really interesting! http://dcleaks.com/

PROBLEM IS …

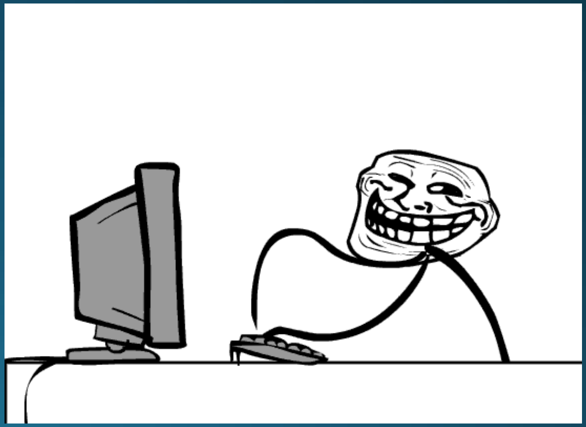
Melvin Redick

Alice Donovan

Katherine Fulton

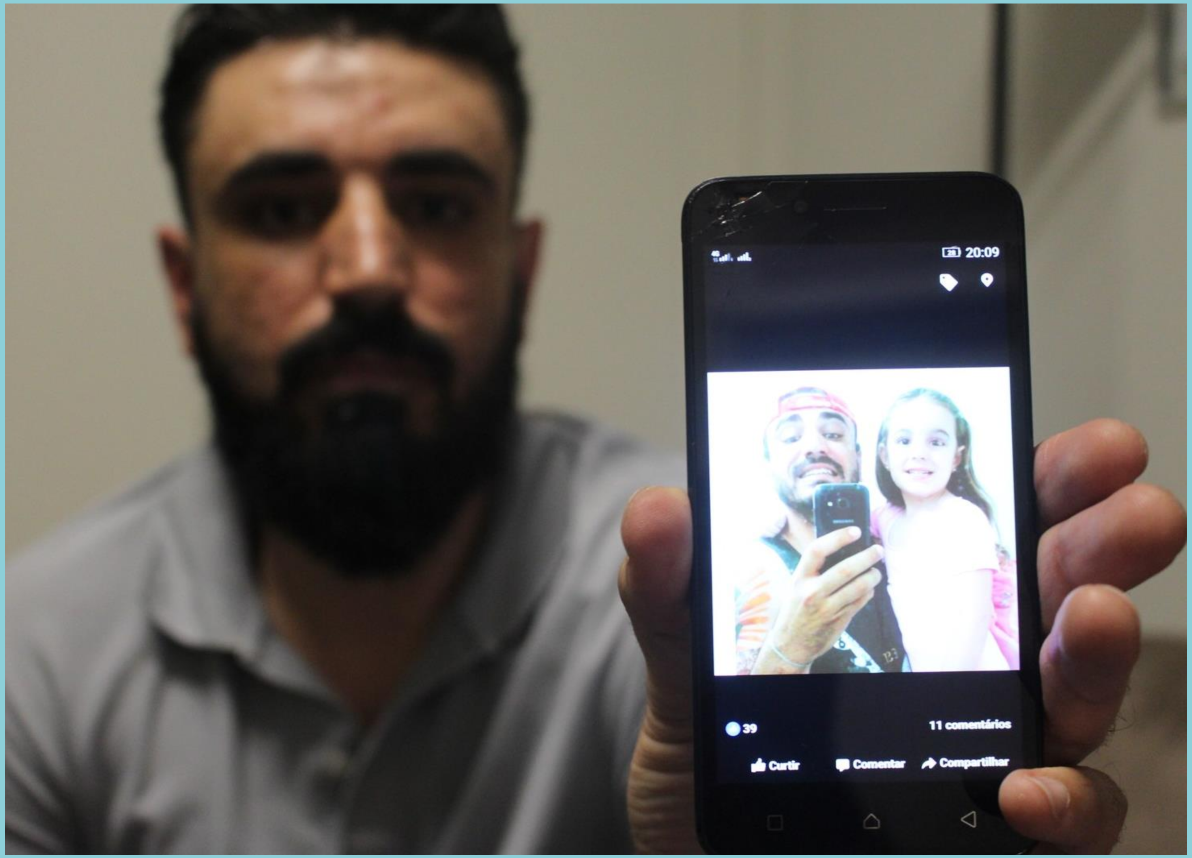
DO NOT EXIST !!!

They are “trolls.”



The man and girl in the photos …

Charles David Costacurta, 36, of Jundiaí in southeastern Brazil, and his 3-yr-old daughter



Other Troll Operations

- Ebola outbreak in Atlanta
- Police shoot an unarmed African-American woman
- Gay activists take over Sunday school
- Teachers are carrying guns in school

E-mail

YouTube

SMS

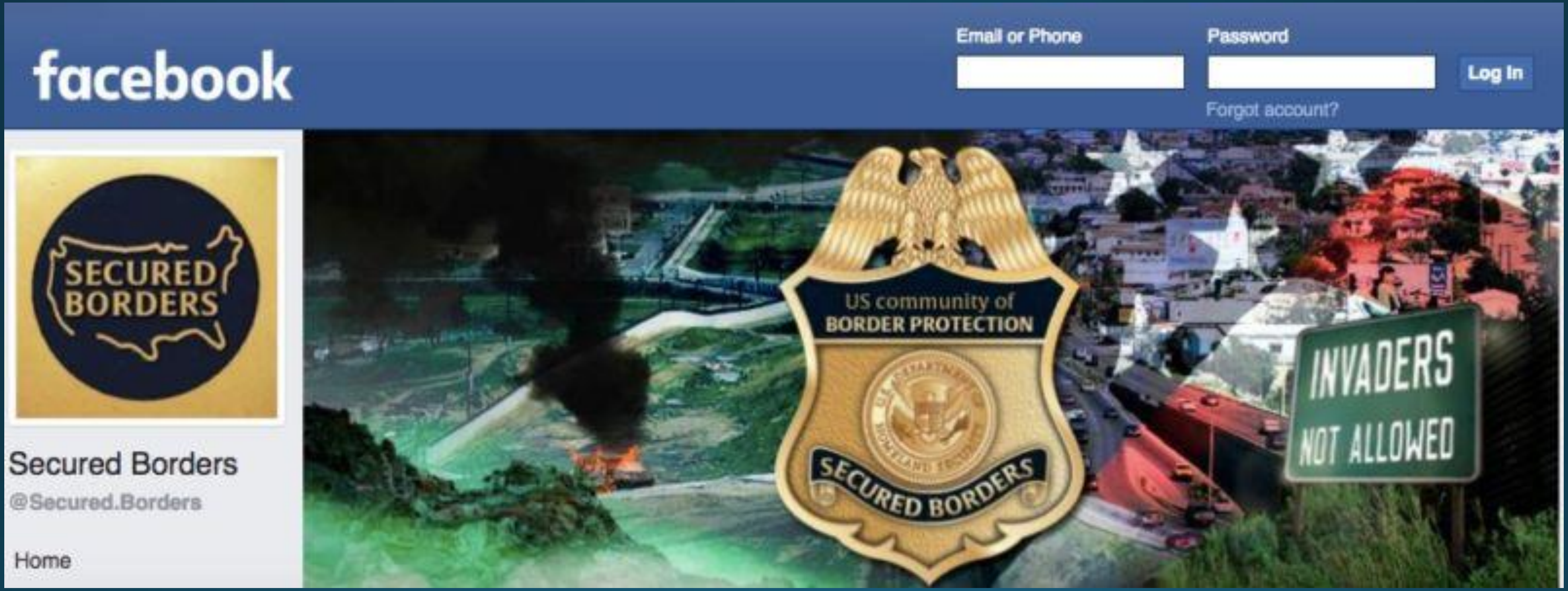
Twitter

Facebook

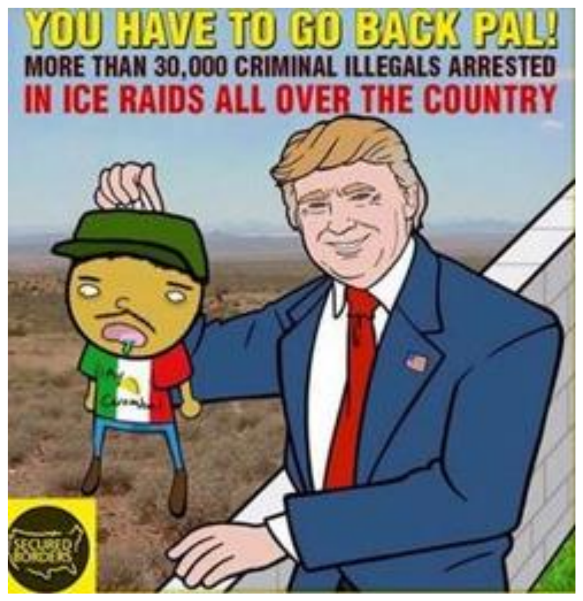
Pinterest

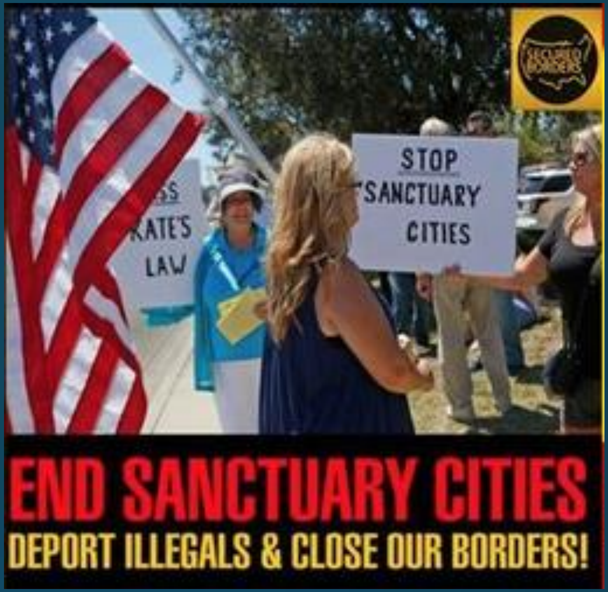
Google

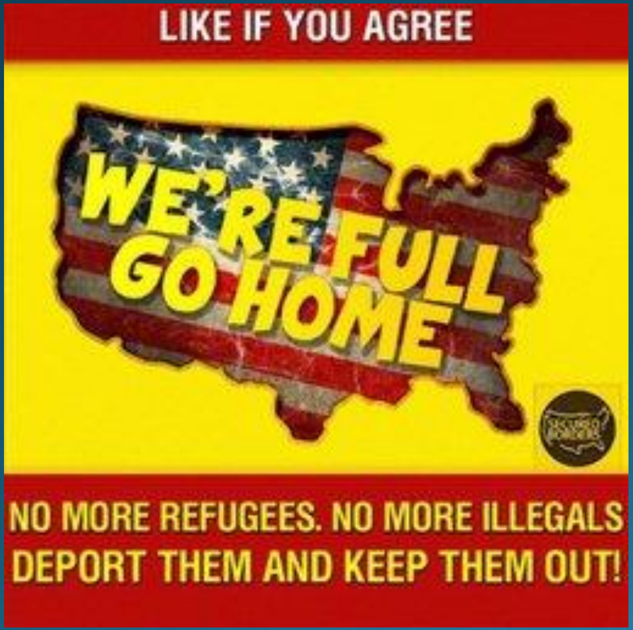
Exploiting any issue that divides us

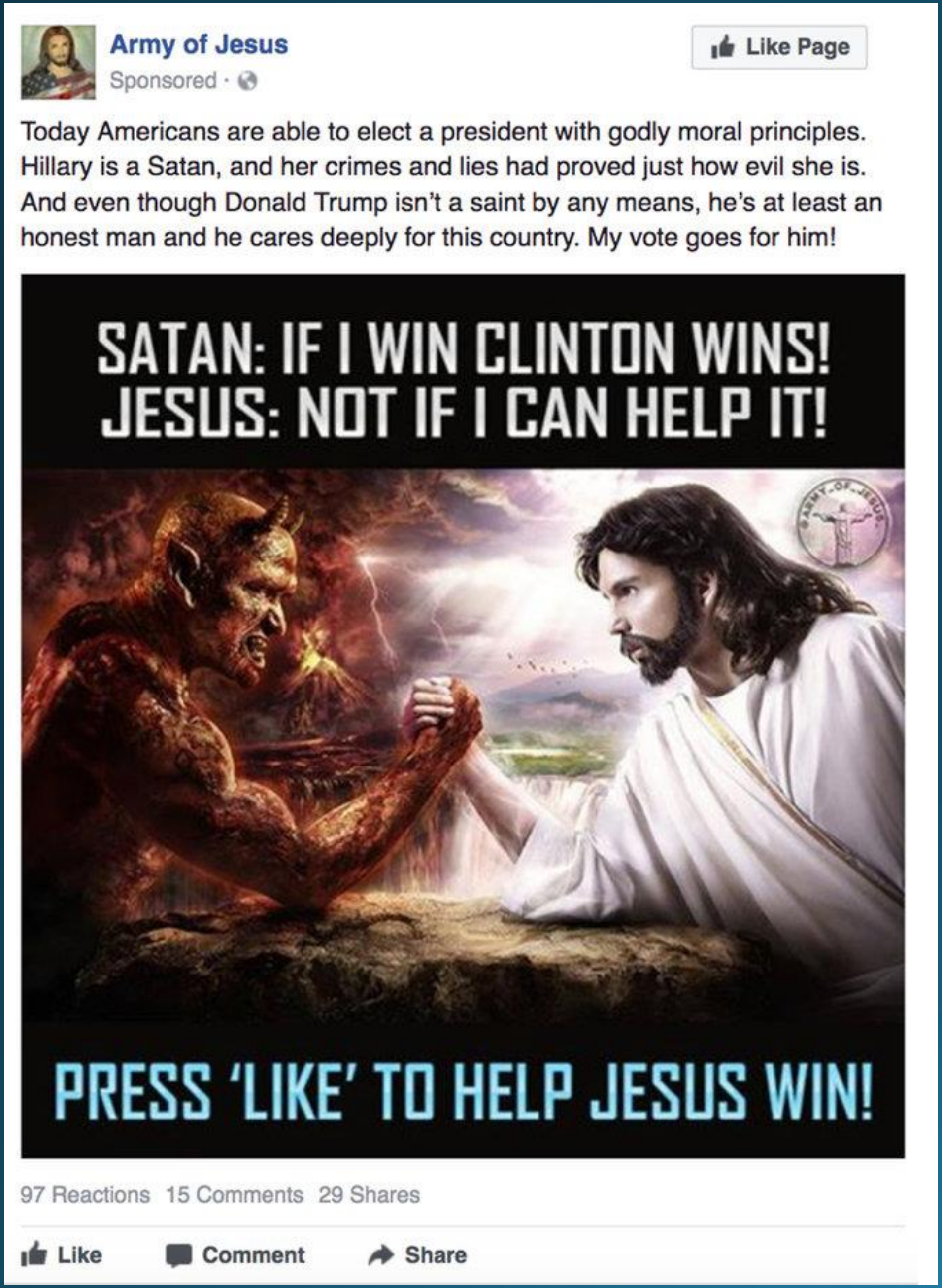


Facebook confirms: Part of Russian campaign


YOU HAVE TO GO BACK PAL!
MORE THAN 30,000 CRIMINAL ILLEGALS ARRESTED
IN ICE RAIDS ALL OVER THE COUNTRY
SECURED BORDERS


SECURED BORDERS
SS
KATE'S
LAW
STOP
SANCTUARY
CITIES
END SANCTUARY CITIES
DEPORT ILLEGALS & CLOSE OUR BORDERS!


LIKE IF YOU AGREE
WE'RE FULL
GO HOME
SECURED BORDERS
NO MORE REFUGEES. NO MORE ILLEGALS
DEPORT THEM AND KEEP THEM OUT!



Army of Jesus

Sponsored ·

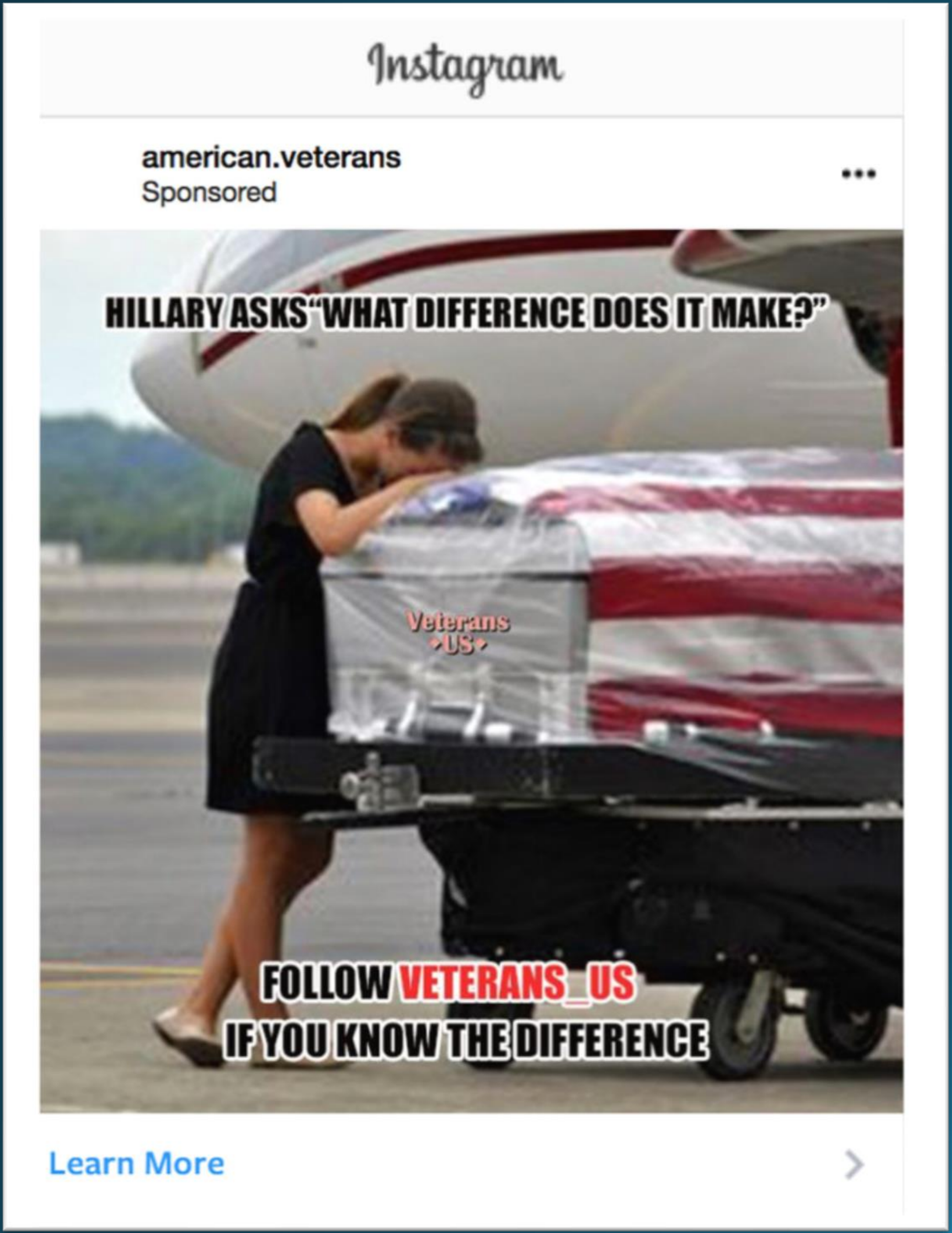
Today Americans are able to elect a president with godly moral principles. Hillary is a Satan, and her crimes and lies had proved just how evil she is. And even though Donald Trump isn't a saint by any means, he's at least an honest man and he cares deeply for this country. My vote goes for him!

SATAN: IF I WIN CLINTON WINS!
JESUS: NOT IF I CAN HELP IT!
ARMY-OF-JESUS
PRESS 'LIKE' TO HELP JESUS WIN!

97 Reactions 15 Comments 29 Shares

INFLUENCE

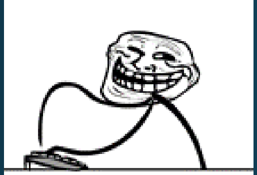
INFORMATION

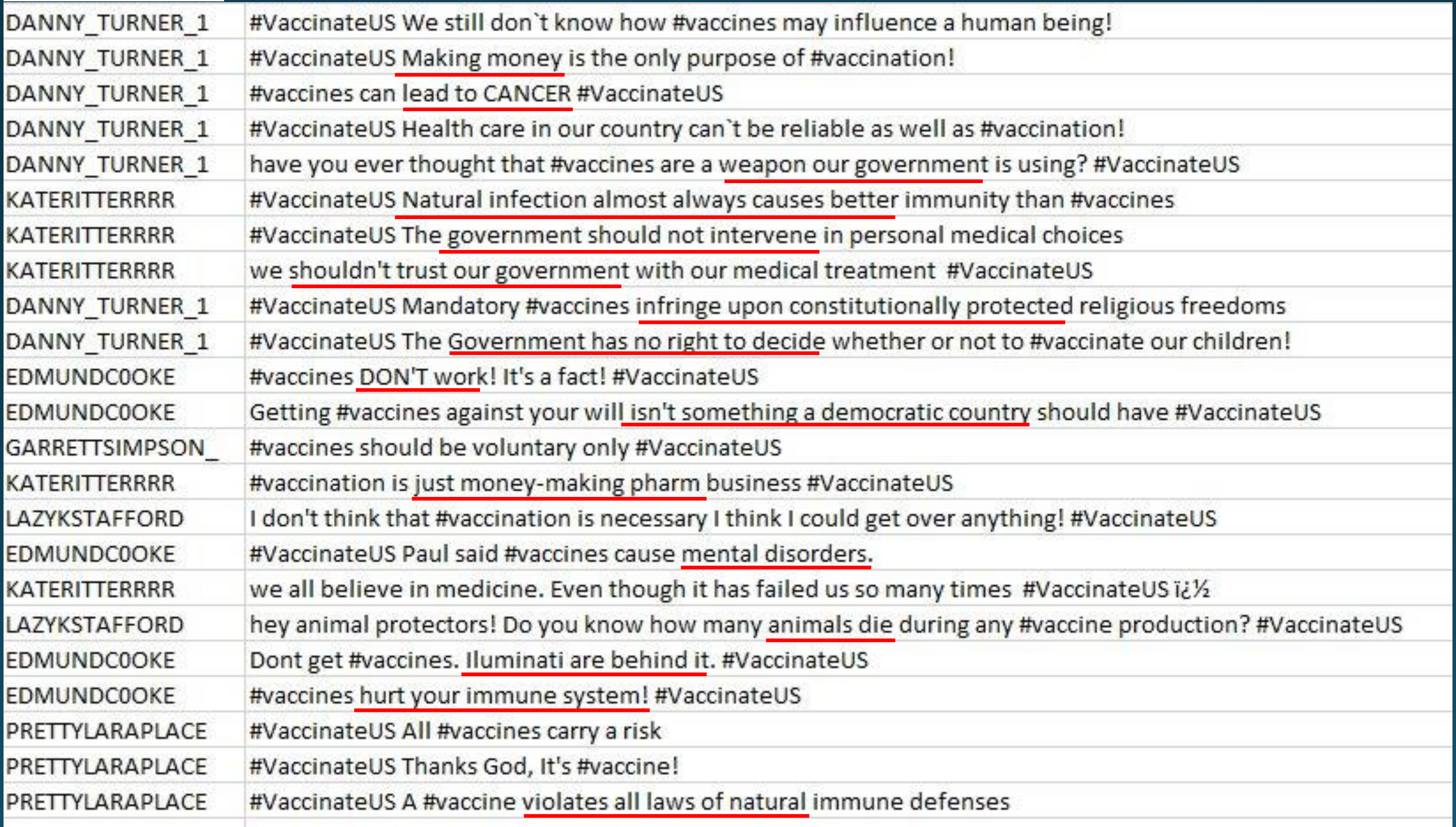

Instagram
american.veterans
Sponsored
•••
HILLARY ASKS "WHAT DIFFERENCE DOES IT MAKE?"
Veterans
•US•
FOLLOW VETERANS_US
IF YOU KNOW THE DIFFERENCE
Learn More

CA

FI

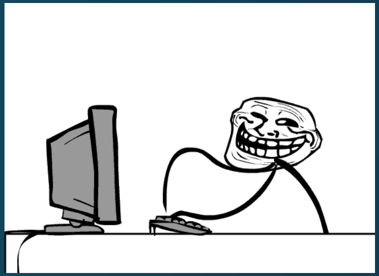
Even children’s health – vaccinations – are not off-limits





DANNY_TURNER_1	#VaccinateUS We still don`t know how #vaccines may influence a human being!
DANNY_TURNER_1	#VaccinateUS Making money is the only purpose of #vaccination!
DANNY_TURNER_1	#vaccines can lead to CANCER #VaccinateUS
DANNY_TURNER_1	#VaccinateUS Health care in our country can`t be reliable as well as #vaccination!
DANNY_TURNER_1	have you ever thought that #vaccines are a weapon our government is using? #VaccinateUS
KATERITTERRRR	#VaccinateUS Natural infection almost always causes better immunity than #vaccines
KATERITTERRRR	#VaccinateUS The government should not intervene in personal medical choices
KATERITTERRRR	we shouldn't trust our government with our medical treatment #VaccinateUS
DANNY_TURNER_1	#VaccinateUS Mandatory #vaccines infringe upon constitutionally protected religious freedoms
DANNY_TURNER_1	#VaccinateUS The Government has no right to decide whether or not to #vaccinate our children!
EDMUNDC0OKE	#vaccines DON'T work! It's a fact! #VaccinateUS
EDMUNDC0OKE	Getting #vaccines against your will isn't something a democratic country should have #VaccinateUS
GARRETTSIMPSON_	#vaccines should be voluntary only #VaccinateUS
KATERITTERRRR	#vaccination is just money-making pharm business #VaccinateUS
LAZYKSTAFFORD	I don't think that #vaccination is necessary I think I could get over anything! #VaccinateUS
EDMUNDC0OKE	#VaccinateUS Paul said #vaccines cause mental disorders.
KATERITTERRRR	we all believe in medicine. Even though it has failed us so many times #VaccinateUS ï¿½
LAZYKSTAFFORD	hey animal protectors! Do you know how many animals die during any #vaccine production? #VaccinateUS
EDMUNDC0OKE	Dont get #vaccines. Iluminati are behind it. #VaccinateUS
EDMUNDC0OKE	#vaccines hurt your immune system! #VaccinateUS
PRETTYLARAPLACE	#VaccinateUS All #vaccines carry a risk
PRETTYLARAPLACE	#VaccinateUS Thanks God, It's #vaccine!
PRETTYLARAPLACE	#VaccinateUS A #vaccine violates all laws of natural immune defenses

MISSION OBJECTIVE ….



- Sow chaos or discontent
- Undermine credibility of services and systems

Hot-Button Issues

A tiny grain of truth

Exploiting biases

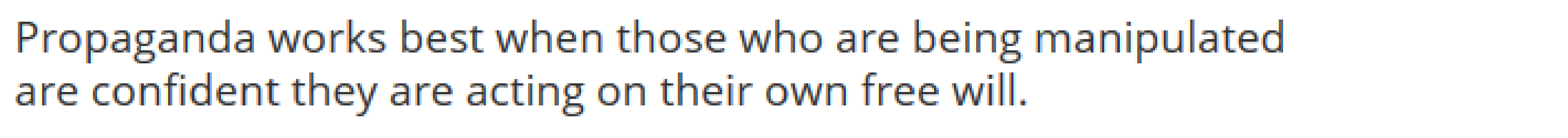
Sowing doubt

Fueling anger

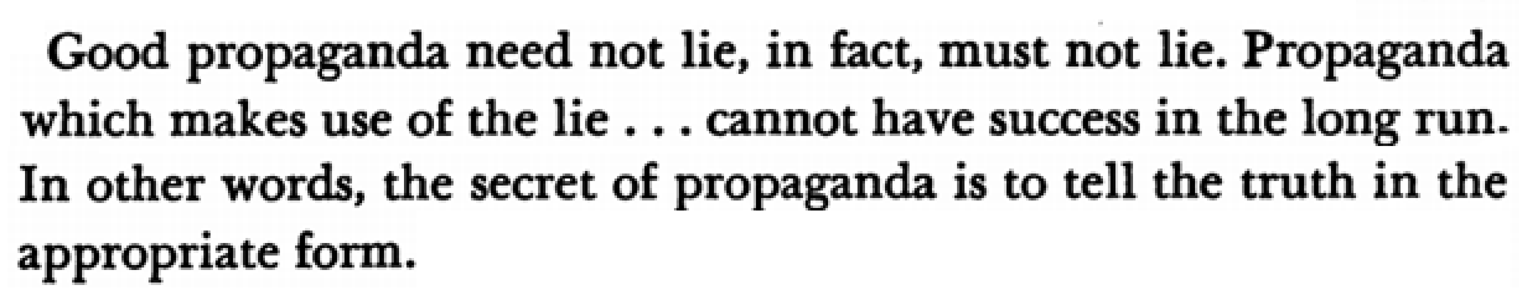
Undermine confidence

SUCCESSFUL COVERT OPERATION!!

Joseph Goebells
NAZI propaganda minister
beginning 1933



Propaganda works best when those who are being manipulated are confident they are acting on their own free will.



Good propaganda need not lie, in fact, must not lie. Propaganda which makes use of the lie . . . cannot have success in the long run. In other words, the secret of propaganda is to tell the truth in the appropriate form.

EXPERTS ADVISE …

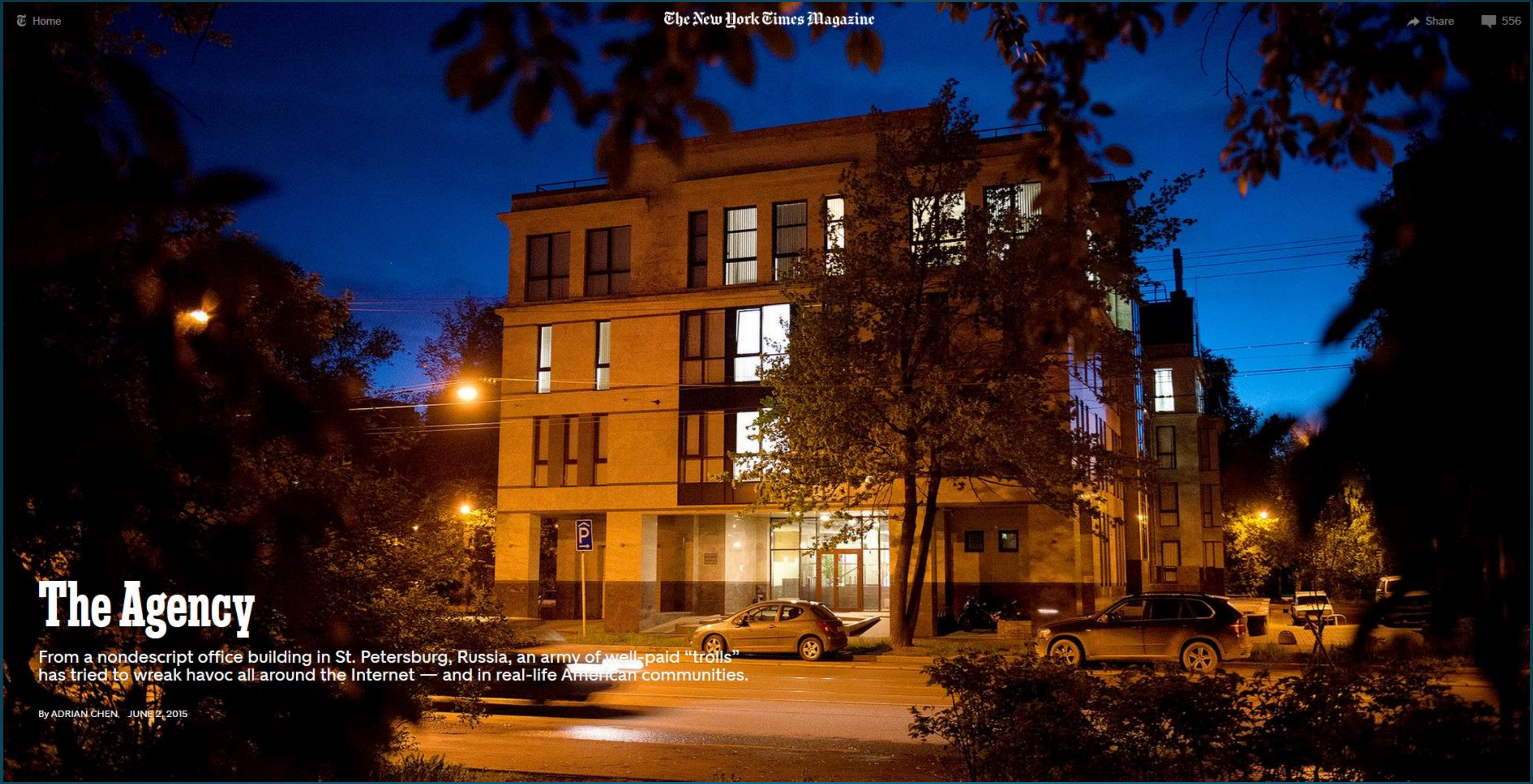
Be as wary of sources you *want* to agree with …

as with those you don’t like

WHO ARE THE TROLLS???

WHERE ARE THEY???

Who was doing the covert operations in the West??



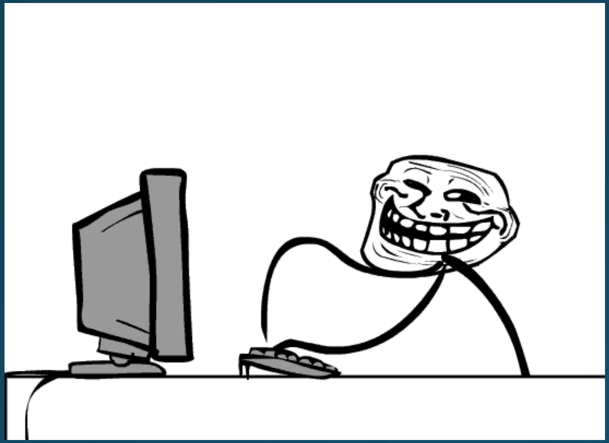
The Agency

From a nondescript office building in St. Petersburg, Russia, an army of well-paid “trolls” has tried to wreak havoc all around the Internet — and in real-life American communities.

By ADRIAN CHEN JUNE 2, 2015

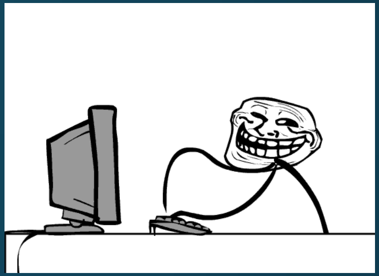
St. Petersburg

“Trolls”



Perhaps … at one point … “could be somebody sitting on their bed that weighs 400 pounds”

Typical Troll

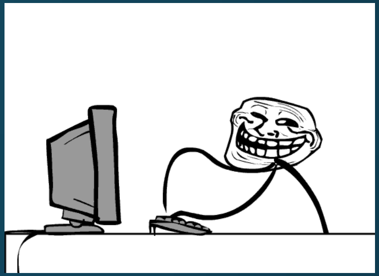


- 20-30 years old
- In office with 5-6 others
- Two 12-hour days in a row, then two days off
- About US$775 per month
- Quota during each set of shifts:

  5 political posts

  10 nonpolitical posts

  150-200 comments on colleagues' posts



Topics:

Sometimes pro-Russia, pro-Putin

Sometimes attacks on opposition in Russia

Often attacking/supporting foreign leaders

Disinformation to support operational priorities

Sow confusion and doubt

admit …

Thousands (or tens of thousands) of BOTS are …

- "Hidden hands" of persons with undisclosed intentions
- MANY run by … foreign intelligence organizations (or businesses)

<u>Example of typical mission</u>
Forward messages that support a particular political objective

RESEARCH SHOWS …

REPETITION WORKS.

Political Interference Ops

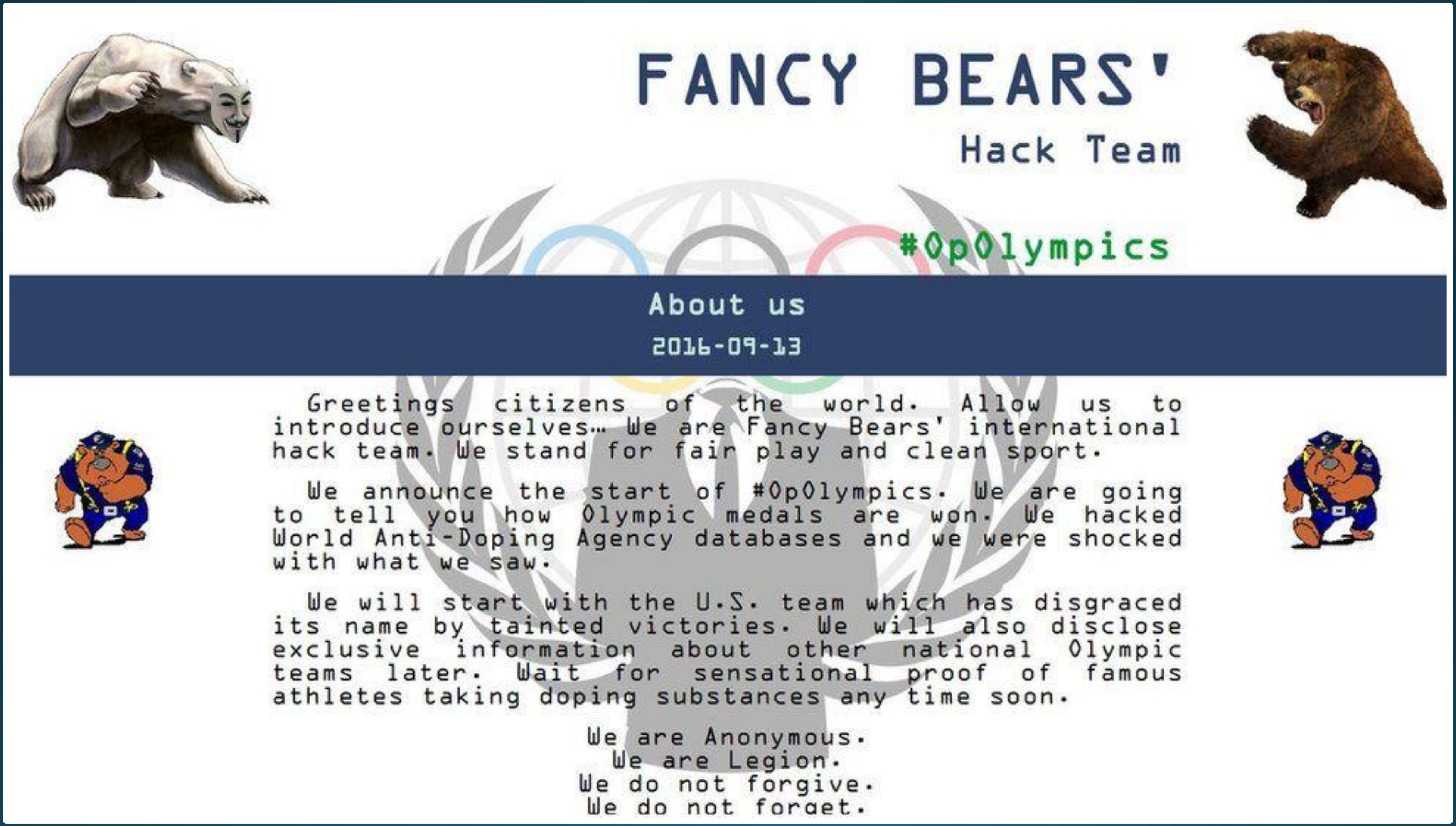
PROFEXOR

FANCY BEARS

COZY BEAR

GUCCIFER

FUNNY NAMES … NOT-FUNNY SPONSORS



FANCY BEARS'

Hack Team

#OpOlympics

About us

2016-09-13

Greetings citizens of the world. Allow us to introduce ourselves… We are Fancy Bears' international hack team. We stand for fair play and clean sport.

We announce the start of #OpOlympics. We are going to tell you how Olympic medals are won. We hacked World Anti-Doping Agency databases and we were shocked with what we saw.

We will start with the U.S. team which has disgraced its name by tainted victories. We will also disclose exclusive information about other national Olympic teams later. Wait for sensational proof of famous athletes taking doping substances any time soon.

We are Anonymous.
We are Legion.
We do not forgive.
We do not forget.

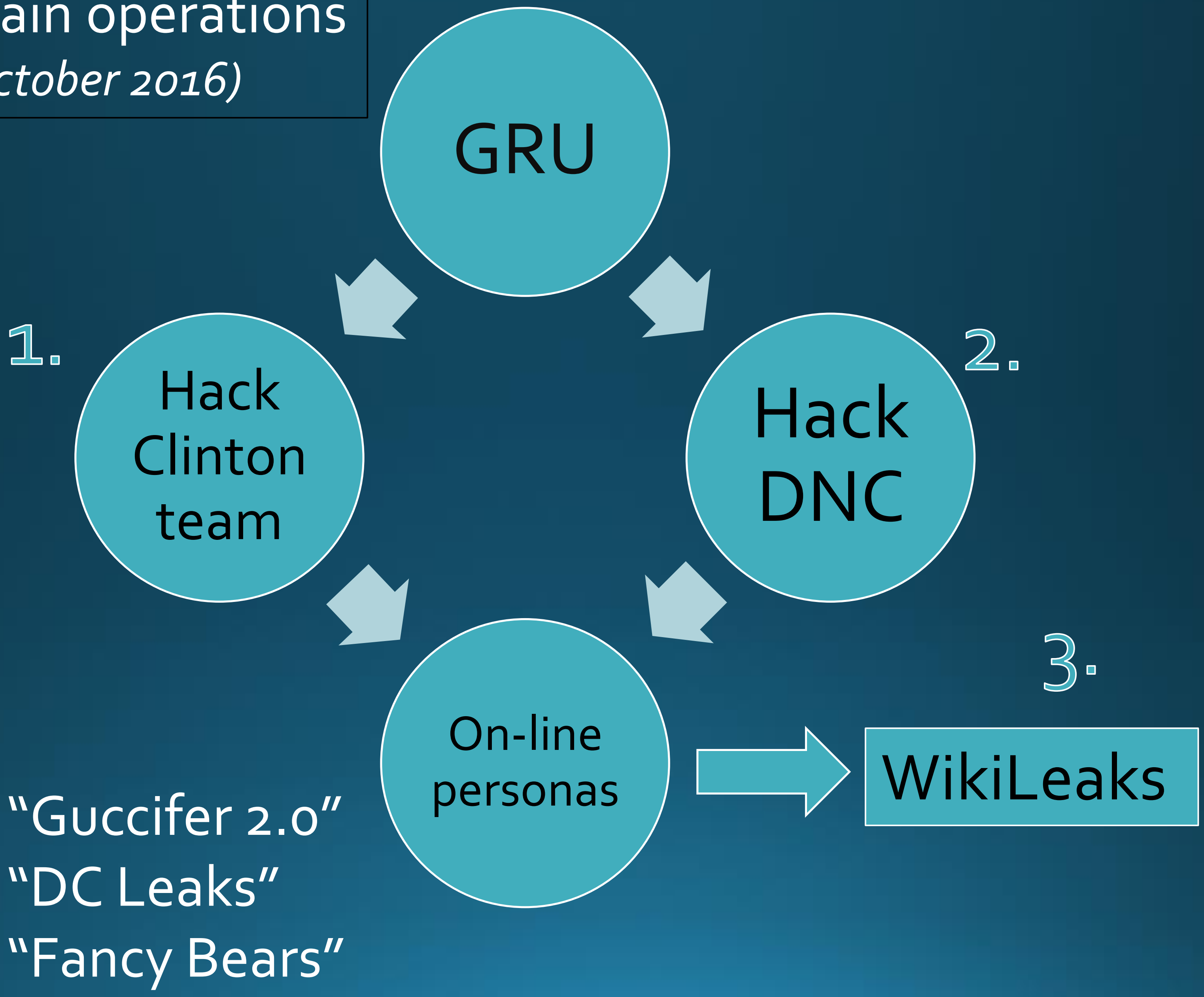
DNC and related intrusions …

- Theft of thousands of party e-mails
- Attempted extortion or blackmail of party officials
- Public release through WikiLeaks

- GOAL: Tensions, acrimony, partisanship, public confusion

Three main operations

(March-October 2016)



GRU

1. Hack Clinton team

2. Hack DNC

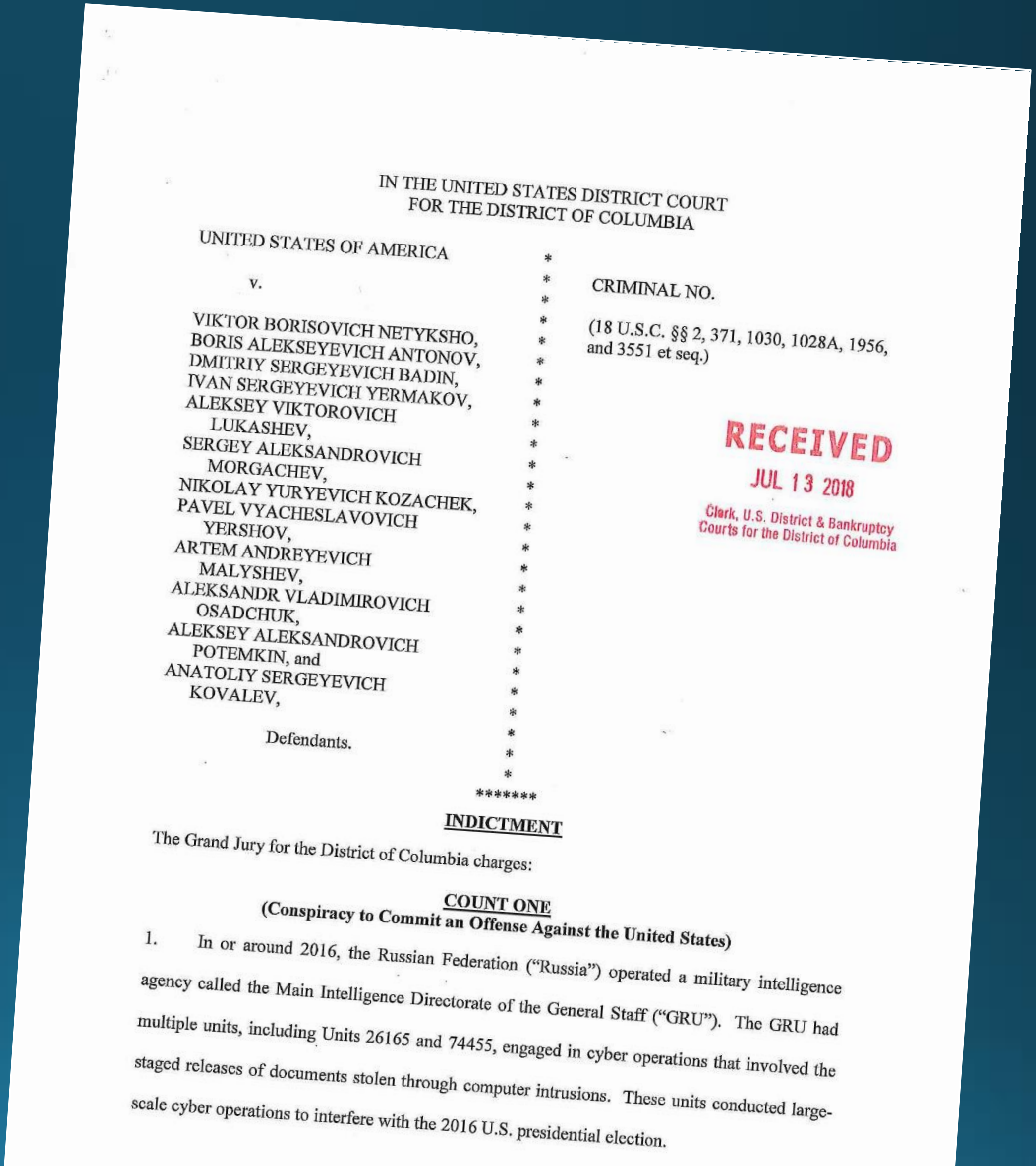
On-line personas

3. WikiLeaks

“Guccifer 2.0”
“DC Leaks”
“Fancy Bears”

July 2018: U.S. indicts 12 Russian intel officers

- Mueller investigation
- Election meddling (not just troll farm)
- 2 sigint units involved in cyber operations to influence 2016 election



IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA

v.

VIKTOR BORISOVICH NETYKSHO,
BORIS ALEKSEYEVICH ANTONOV,
DMITRIY SERGEYEVICH BADIN,
IVAN SERGEYEVICH YERMAKOV,
ALEKSEY VIKTOROVICH LUKASHEV,
SERGEY ALEKSANDROVICH MORGACHEV,
NIKOLAY YURYEVICH KOZACHEK,
PAVEL VYACHESLAVOVICH YERSHOV,
ARTEM ANDREYEVICH MALYSHEV,
ALEKSANDR VLADIMIROVICH OSADCHUK,
ALEKSEY ALEKSANDROVICH POTEMKIN, and
ANATOLIY SERGEYEVICH KOVALEV,

Defendants.

CRIMINAL NO.

(18 U.S.C. §§ 2, 371, 1030, 1028A, 1956, and 3551 et seq.)

****

INDICTMENT

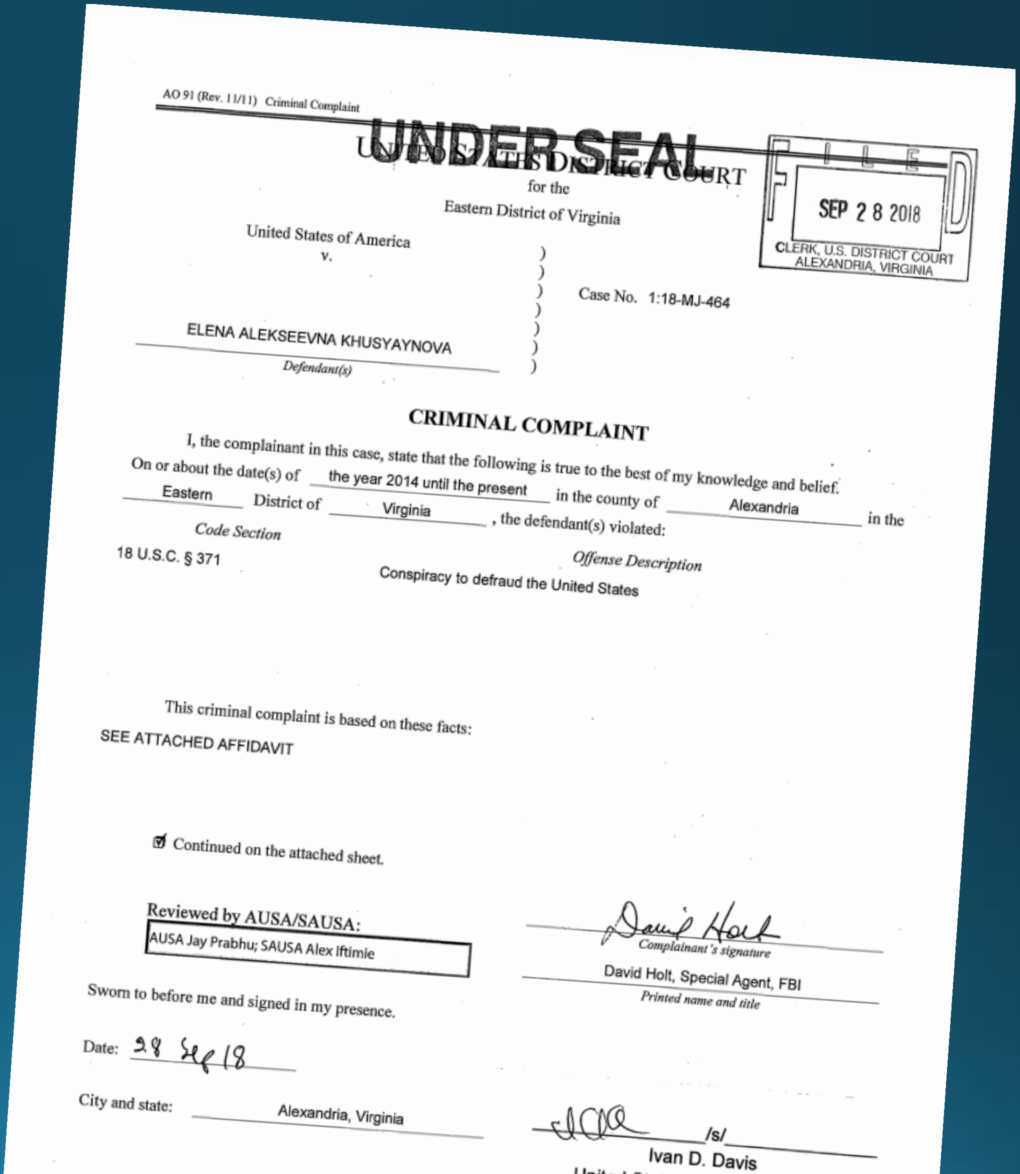
The Grand Jury for the District of Columbia charges:

COUNT ONE
(Conspiracy to Commit an Offense Against the United States)

1. In or around 2016, the Russian Federation ("Russia") operated a military intelligence agency called the Main Intelligence Directorate of the General Staff ("GRU"). The GRU had multiple units, including Units 26165 and 74455, engaged in cyber operations that involved the staged releases of documents stolen through computer intrusions. These units conducted large-scale cyber operations to interfere with the 2016 U.S. presidential election.

19 October 2018: Another Indictment

- Russians "interfering in U.S. mid-term elections"
- Elena Khusyaynova, 44, paid by senior Putin aide
- "Sow discord in the U.S. political system" by pushing divisive political issues



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
Defendant(s)

Case No. 1:18-MJ-464

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. On or about the date(s) of the year 2014 until the present in the county of Alexandria in the Eastern District of Virginia, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 371	Conspiracy to defraud the United States

This criminal complaint is based on these facts:
SEE ATTACHED AFFIDAVIT

☑ Continued on the attached sheet.

Reviewed by AUSA/SAUSA:
AUSA Jay Prabhu; SAUSA Alex Iftimie

David Holt
Complainant's signature

David Holt, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

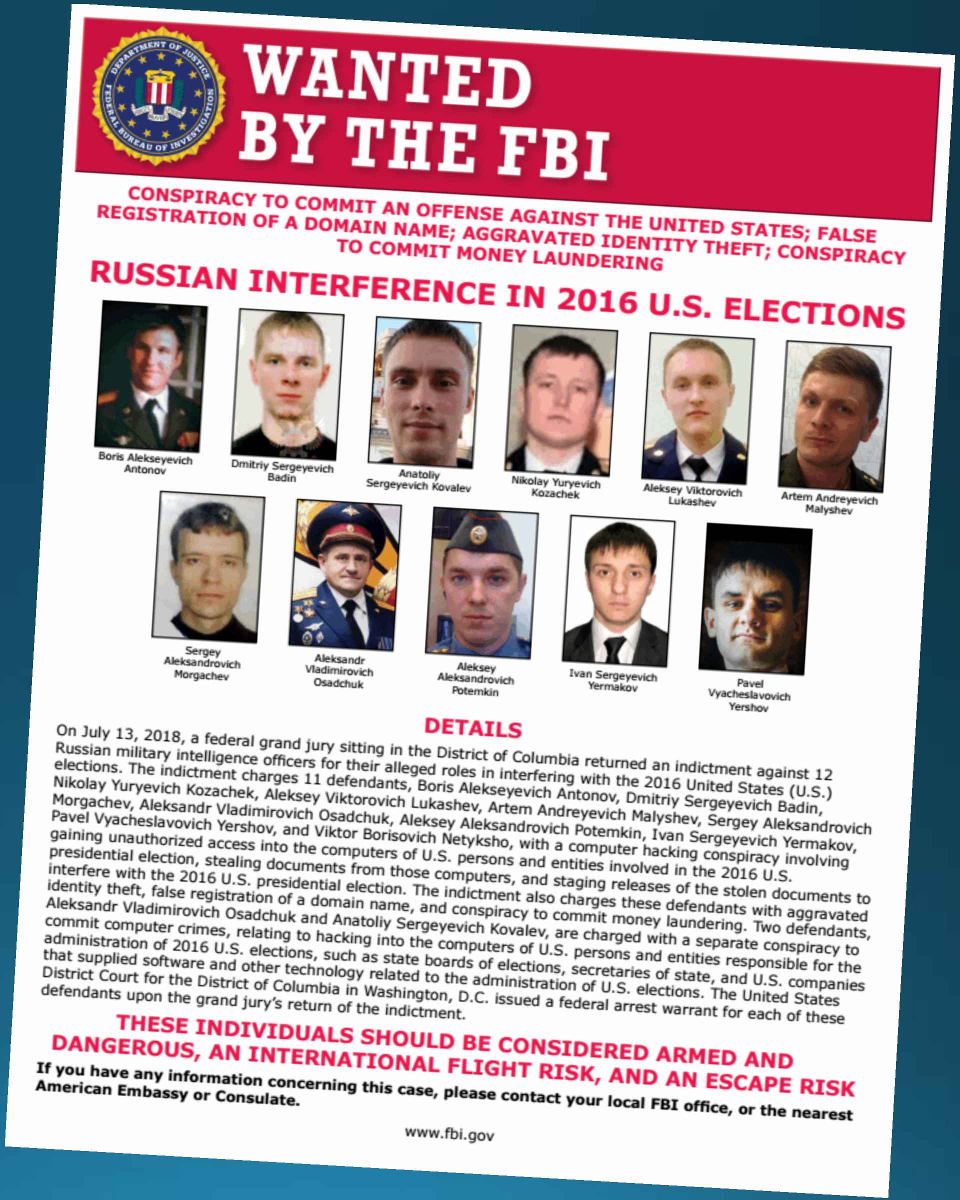
Date: 28 Sep 18

City and state: Alexandria, Virginia

/s/
Ivan D. Davis

19 October 2018: Another Indictment

- Russians "interfering in U.S. mid-term elections"
- Elena Khusyaynova, 44, paid by senior Putin aide
- "Sow discord in the U.S. political system" by pushing divisive political issues



WANTED BY THE FBI

CONSPIRACY TO COMMIT AN OFFENSE AGAINST THE UNITED STATES; FALSE REGISTRATION OF A DOMAIN NAME; AGGRAVATED IDENTITY THEFT; CONSPIRACY TO COMMIT MONEY LAUNDERING

RUSSIAN INTERFERENCE IN 2016 U.S. ELECTIONS

Boris Alekseyevich Antonov

Dmitriy Sergeyevich Badin

Anatoliy Sergeyevich Kovalev

Nikolay Yuryevich Kozachek

Aleksey Viktorovich Lukashev

Artem Andreyevich Malyshev

Sergey Aleksandrovich Morgachev

Aleksandr Vladimirovich Osadchuk

Aleksey Aleksandrovich Potemkin

Ivan Sergeyevich Yermakov

Pavel Vyacheslavovich Yershov

DETAILS

On July 13, 2018, a federal grand jury sitting in the District of Columbia returned an indictment against 12 Russian military intelligence officers for their alleged roles in interfering with the 2016 United States (U.S.) elections. The indictment charges 11 defendants, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Nikolay Yuryevich Kozachek, Aleksey Viktorovich Lukashev, Artem Andreyevich Malyshev, Sergey Aleksandrovich Morgachev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkin, Ivan Sergeyevich Yermakov, Pavel Vyacheslavovich Yershov, and Viktor Borisovich Netyksho, with a computer hacking conspiracy involving gaining unauthorized access into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election, stealing documents from those computers, and staging releases of the stolen documents to interfere with the 2016 U.S. presidential election. The indictment also charges these defendants with aggravated identity theft, false registration of a domain name, and conspiracy to commit money laundering. Two defendants, Aleksandr Vladimirovich Osadchuk and Anatoliy Sergeyevich Kovalev, are charged with a separate conspiracy to commit computer crimes, relating to hacking into the computers of U.S. persons and entities responsible for the administration of 2016 U.S. elections, such as state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections. The United States District Court for the District of Columbia in Washington, D.C. issued a federal arrest warrant for each of these defendants upon the grand jury's return of the indictment.

THESE INDIVIDUALS SHOULD BE CONSIDERED ARMED AND DANGEROUS, AN INTERNATIONAL FLIGHT RISK, AND AN ESCAPE RISK

If you have any information concerning this case, please contact your local FBI office, or the nearest American Embassy or Consulate.

www.fbi.gov

PROJECT LAKHTA …

- Studies U.S. news and “fake news”
- Pushes lines on BOTH sides

❑ Special Counsel Mueller is “puppet of establishment” who’s “damaging the country”

❑ “If Trump fires Mueller … our democracy is at stake”

DNI Coates:

- “Campaigns” targeting 2020 elections also
- Warning lights are “blinking red”

Target just one party?

Ya think so?!?!?!

Technique: Spearphishing

Get your prey to download software that gives YOU control

Interfering in actual voting??

Example of situations in 21 U.S. states:

Company providing voter check-in software was **allegedly** penetrated by Russians

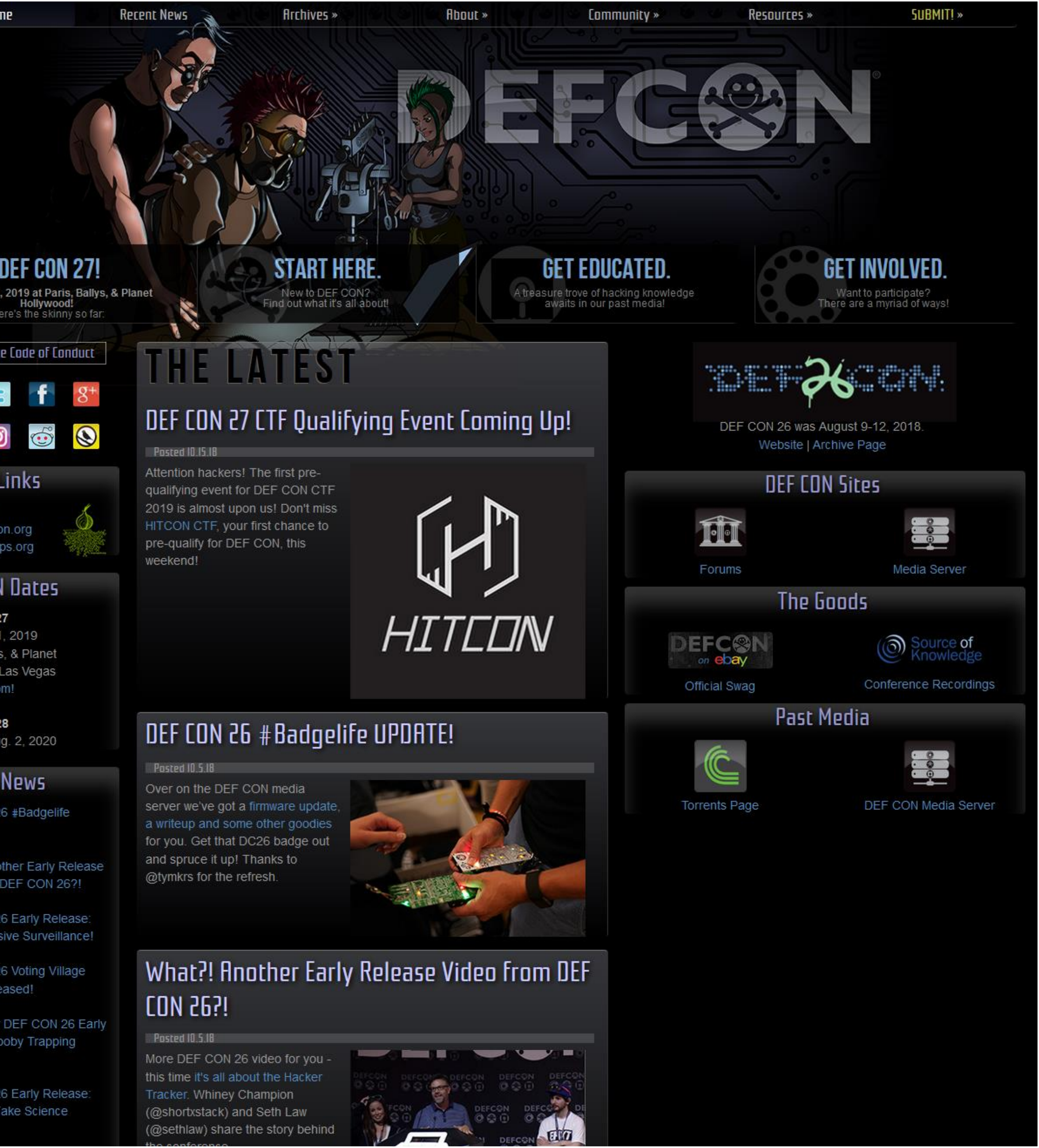
- VR Systems

NSA says GRU sent "phishing" e-mails from fake VR to 122 local jurisdictions

Concerns deepen … and democracy relies on faith.

Def Con 26

in August 2018



DEF CON 27!

, 2019 at Paris, Ballys, & Planet Hollywood!
ere's the skinny so far:

START HERE.

New to DEF CON?
Find out what it's all about!

GET EDUCATED.

A treasure trove of hacking knowledge awaits in our past media!

GET INVOLVED.

Want to participate?
There are a myriad of ways!

e Code of Conduct

THE LATEST

DEF CON 27 CTF Qualifying Event Coming Up!

Posted 10.15.18

Attention hackers! The first pre-qualifying event for DEF CON CTF 2019 is almost upon us! Don't miss HITCON CTF, your first chance to pre-qualify for DEF CON, this weekend!

DEF CON 26 #Badgelife UPDATE!

Posted 10.5.18

Over on the DEF CON media server we've got a firmware update, a writeup and some other goodies for you. Get that DC26 badge out and spruce it up! Thanks to @tymkrs for the refresh.

What?! Another Early Release Video from DEF CON 26?!

Posted 10.5.18

More DEF CON 26 video for you - this time it's all about the Hacker Tracker. Whiney Champion (@shortxstack) and Seth Law (@sethlaw) share the story behind the conference

Links

on.org
ps.org

N Dates

27
, 2019
s, & Planet
Las Vegas
om!

28
g. 2, 2020

News

6 #Badgelife

other Early Release
DEF CON 26?!

6 Early Release:
sive Surveillance!

6 Voting Village
eased!

DEF CON 26 Early
ooby Trapping

6 Early Release:
ake Science

DEF CON 26 was August 9-12, 2018.
Website | Archive Page

DEF CON Sites

Forums
Media Server

The Goods

Official Swag
Conference Recordings

Past Media

Torrents Page
DEF CON Media Server

"White Hat" hacking conference

- Kids (6-17 yrs old) able to hack into replicas of election board websites
- 11-yr-old changed a Florida website

Subsequent reports caution hacked sites weren't as vulnerable in real life.

Interfering in actual voting??

One solution …

Return to paper ballots

- In U.S., many states previously electronic have returned to paper
- But 14 states will still have no paper record

Fight between vendors and security advocates gumming up debate.

So …

Bad guys can disrupt our businesses and public services.

Bad guys can steal our info and hold it hostage.

Bad guys can sow confusion, discontent among us.

What can we do ?!?!?!?!?!

Defense Actions

As individuals … (next conversation)

As countries …

- Monitoring and Detection
- Firewalls and Blocks
- Defensive deployments
- Offense and Counterattacks
- Deterrence

USCYBERCOM

Australian Government

Australian Signals Directorate

ACSC

Australian

Cyber Security

Centre

The National Cyber Security Centre

Helping to make the UK the safest place to live and do business online. Read more about the NCSC.

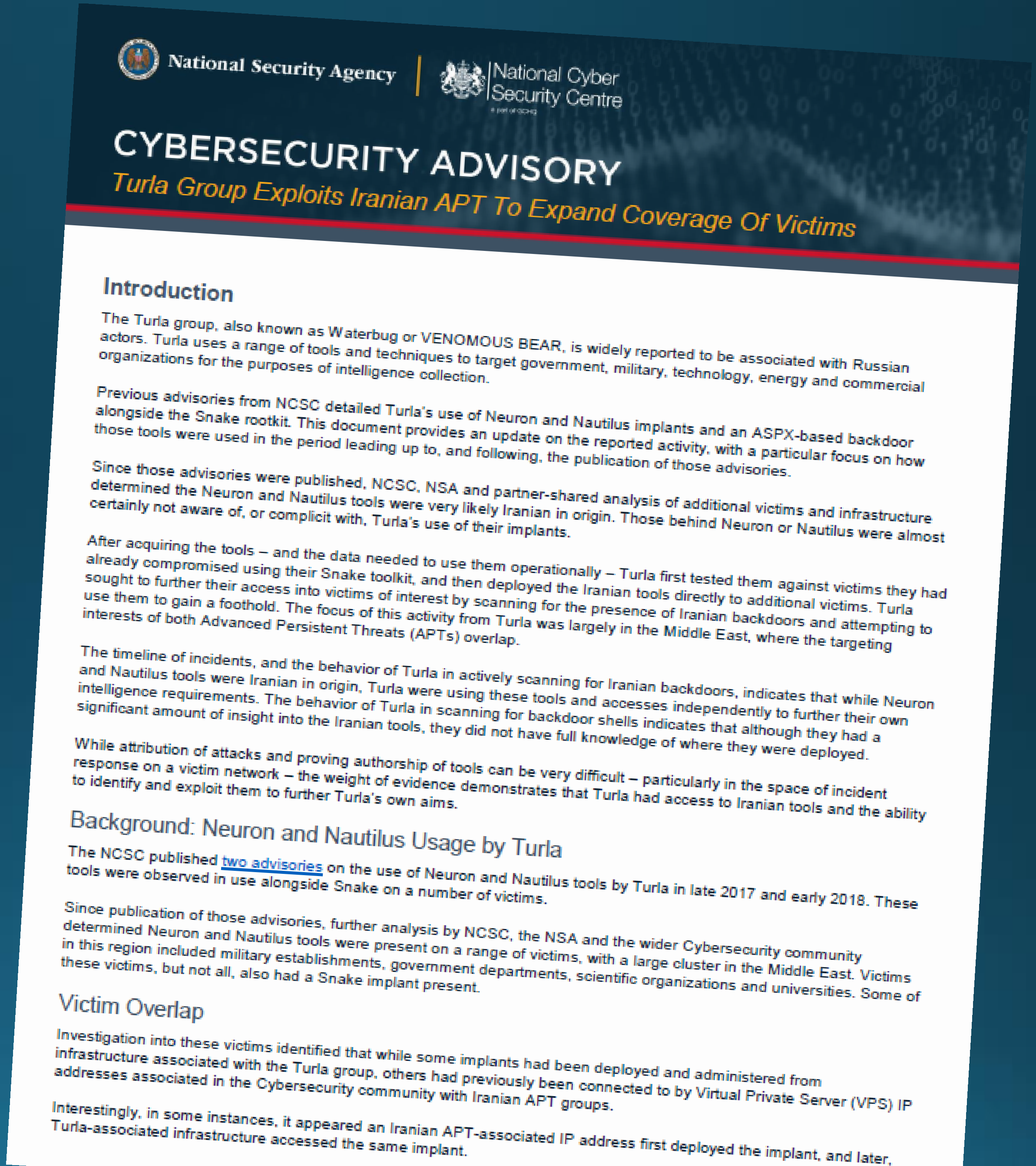
National Cyber Security Centre

a part of GCHQ

JOINT WARNING
October 2019

Hacks in 35 countries that appeared to be from Iran … were actually RUSSIAN.

“False flag ops”



National Security Agency | National Cyber Security Centre
a part of GCHQ

CYBERSECURITY ADVISORY

Turla Group Exploits Iranian APT To Expand Coverage Of Victims

Introduction

The Turla group, also known as Waterbug or VENOMOUS BEAR, is widely reported to be associated with Russian actors. Turla uses a range of tools and techniques to target government, military, technology, energy and commercial organizations for the purposes of intelligence collection.

Previous advisories from NCSC detailed Turla's use of Neuron and Nautilus implants and an ASPX-based backdoor alongside the Snake rootkit. This document provides an update on the reported activity, with a particular focus on how those tools were used in the period leading up to, and following, the publication of those advisories.

Since those advisories were published, NCSC, NSA and partner-shared analysis of additional victims and infrastructure determined the Neuron and Nautilus tools were very likely Iranian in origin. Those behind Neuron or Nautilus were almost certainly not aware of, or complicit with, Turla's use of their implants.

After acquiring the tools – and the data needed to use them operationally – Turla first tested them against victims they had already compromised using their Snake toolkit, and then deployed the Iranian tools directly to additional victims. Turla sought to further their access into victims of interest by scanning for the presence of Iranian backdoors and attempting to use them to gain a foothold. The focus of this activity from Turla was largely in the Middle East, where the targeting interests of both Advanced Persistent Threats (APTs) overlap.

The timeline of incidents, and the behavior of Turla in actively scanning for Iranian backdoors, indicates that while Neuron and Nautilus tools were Iranian in origin, Turla were using these tools and accesses independently to further their own intelligence requirements. The behavior of Turla in scanning for backdoor shells indicates that although they had a significant amount of insight into the Iranian tools, they did not have full knowledge of where they were deployed.

While attribution of attacks and proving authorship of tools can be very difficult – particularly in the space of incident response on a victim network – the weight of evidence demonstrates that Turla had access to Iranian tools and the ability to identify and exploit them to further Turla's own aims.

Background: Neuron and Nautilus Usage by Turla

The NCSC published two advisories on the use of Neuron and Nautilus tools by Turla in late 2017 and early 2018. These tools were observed in use alongside Snake on a number of victims.

Since publication of those advisories, further analysis by NCSC, the NSA and the wider Cybersecurity community determined Neuron and Nautilus tools were present on a range of victims, with a large cluster in the Middle East. Victims in this region included military establishments, government departments, scientific organizations and universities. Some of these victims, but not all, also had a Snake implant present.

Victim Overlap

Investigation into these victims identified that while some implants had been deployed and administered from infrastructure associated with the Turla group, others had previously been connected to by Virtual Private Server (VPS) IP addresses associated in the Cybersecurity community with Iranian APT groups.

Interestingly, in some instances, it appeared an Iranian APT-associated IP address first deployed the implant, and later, Turla-associated infrastructure accessed the same implant.

But …

This is just the beginning.

Government can only do so much.

Individual responsibility will be key.