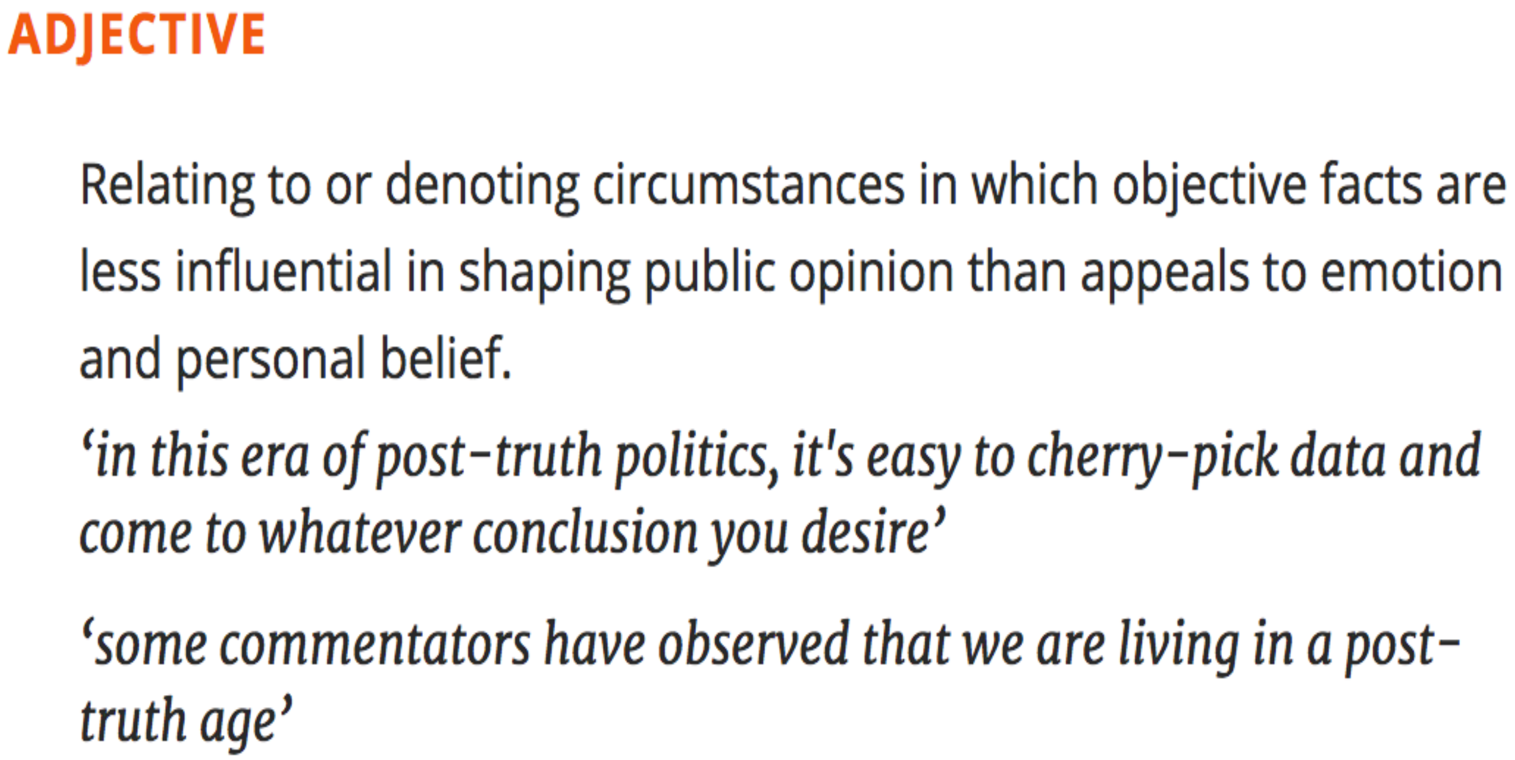
Cognitive Hacking: Recognizing and Countering 21st Century Deception

Dr. Char Sample

2017

“Post-Truth”

Oxford dictionary 2016 Word of the Year



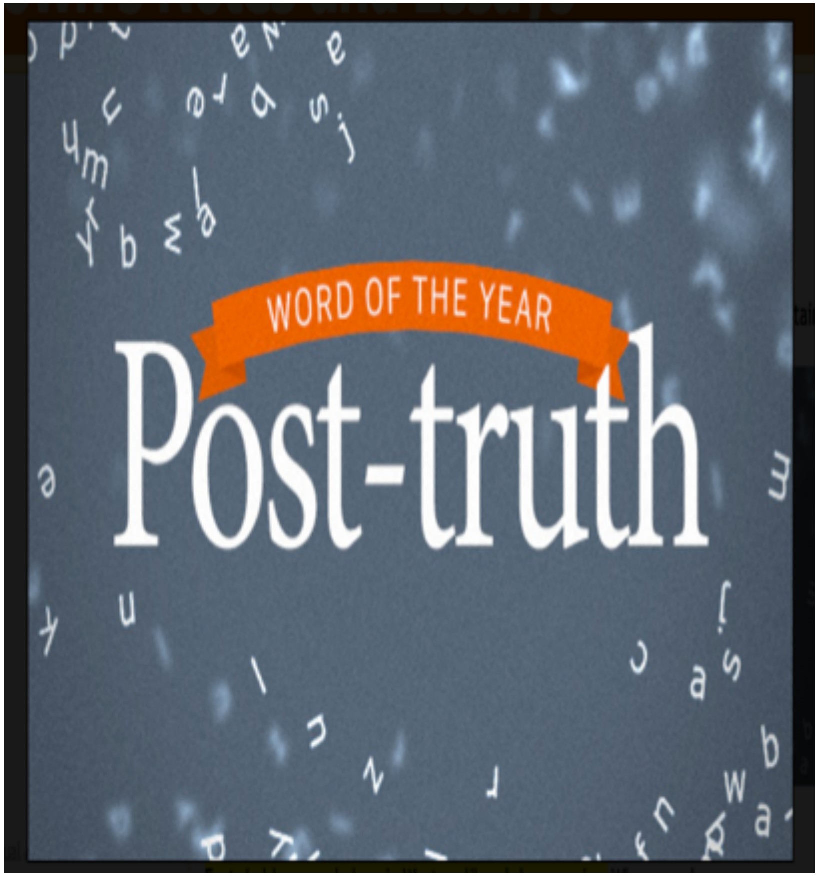
ADJECTIVE

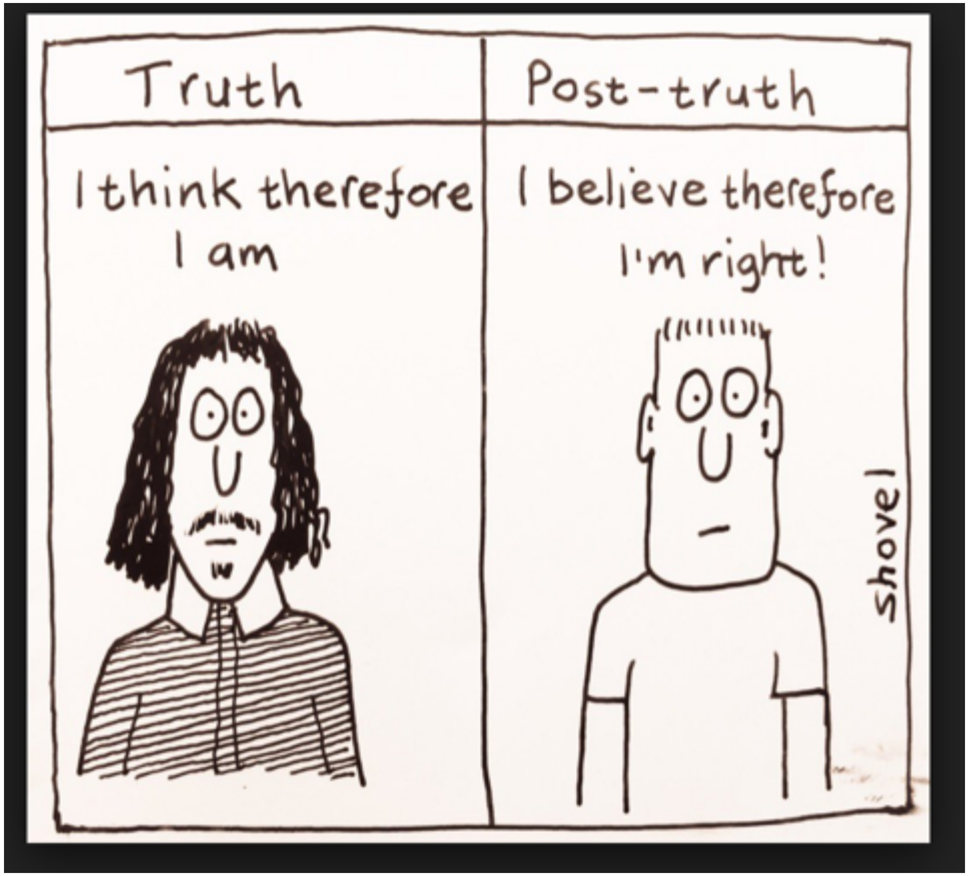
Relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief.

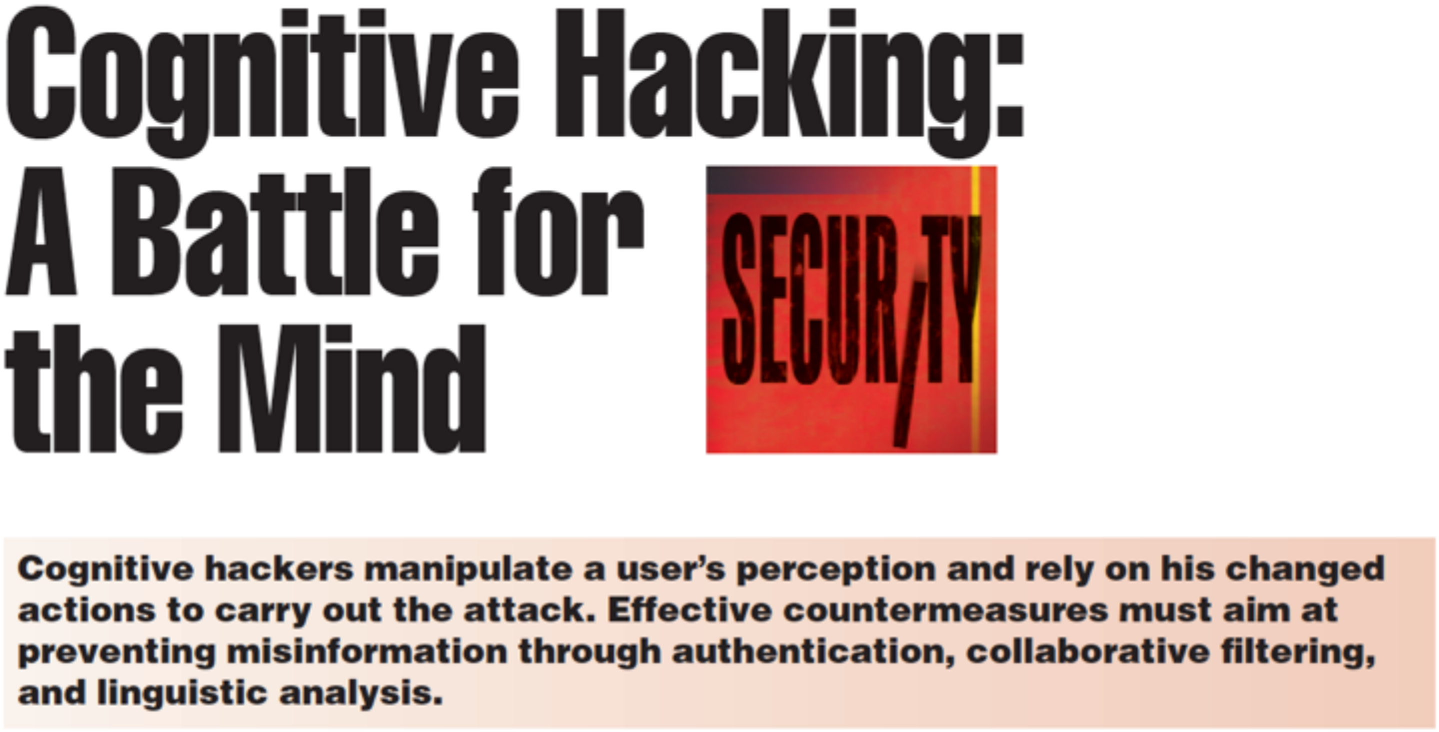
‘in this era of post-truth politics, it's easy to cherry-pick data and come to whatever conclusion you desire’

‘some commentators have observed that we are living in a post-truth age’

Post-truth


WORD OF THE YEAR
Post-truth


Truth
Post-truth
I think therefore I am
I believe therefore I'm right!
Shovel



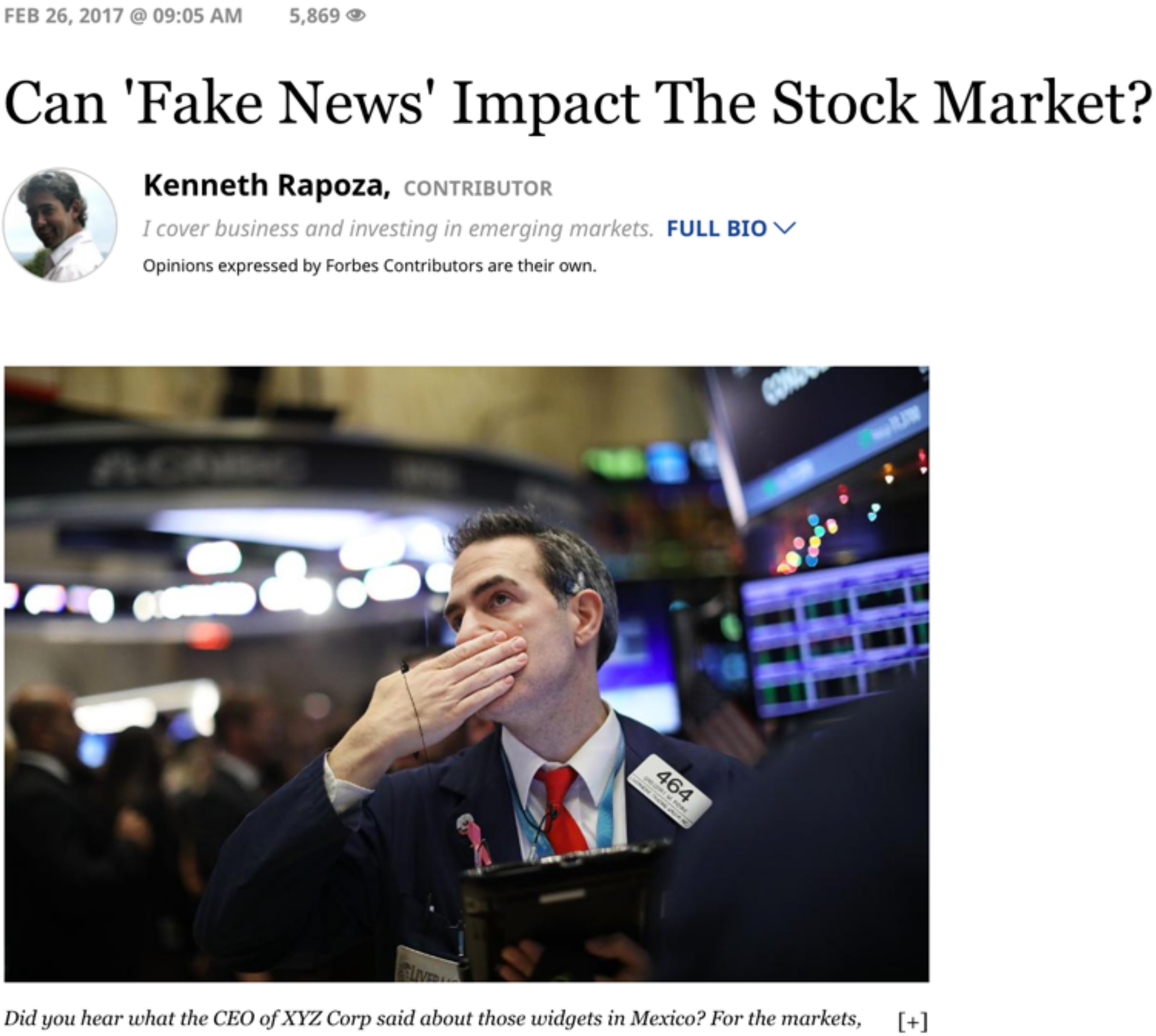
Cognitive Hacking: A Battle for the Mind

Cognitive hackers manipulate a user's perception and rely on his changed actions to carry out the attack. Effective countermeasures must aim at preventing misinformation through authentication, collaborative filtering, and linguistic analysis.

***Cognitive hacking (Cybenko et al., 2002)*.**

Perception management

Have the victim carry out the attack.



FEB 26, 2017 @ 09:05 AM 5,869

Can 'Fake News' Impact The Stock Market?

Kenneth Rapoza, CONTRIBUTOR

I cover business and investing in emerging markets. **FULL BIO**

Opinions expressed by Forbes Contributors are their own.

Did you hear what the CEO of XYZ Corp said about those widgets in Mexico? For the markets, [+]

Fake News

Fake news, manipulated data and the future of betting fraud

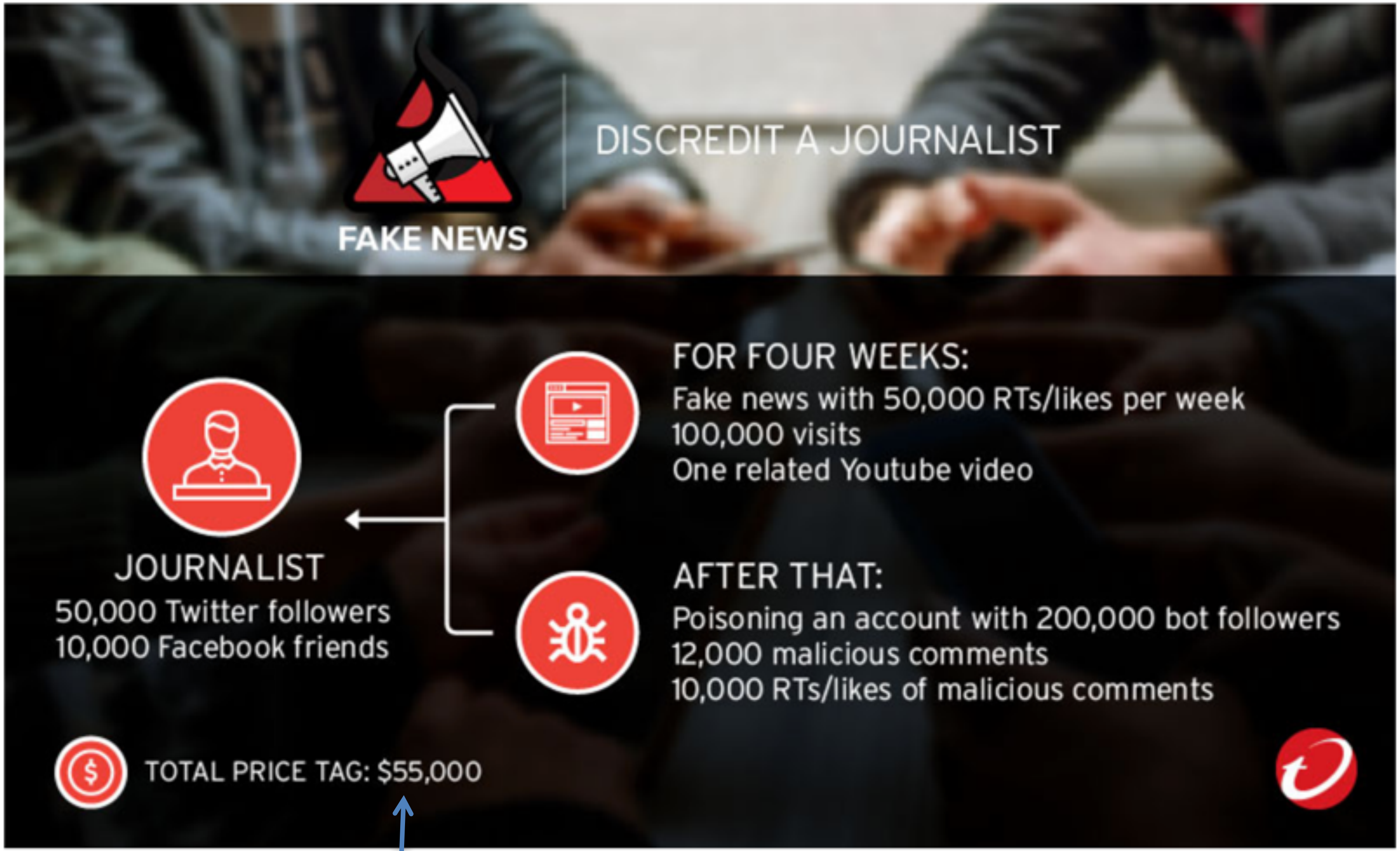
The Fake News Machine

How Propagandists Abuse the Internet and Manipulate the Public

Lion Gu, Vladimir Kropotov, and Fyodor Yarochkin
Forward-Looking Threat Research (FTR)

A TrendLabs Research Paper

Discredit a Journalist



DISCREDIT A JOURNALIST

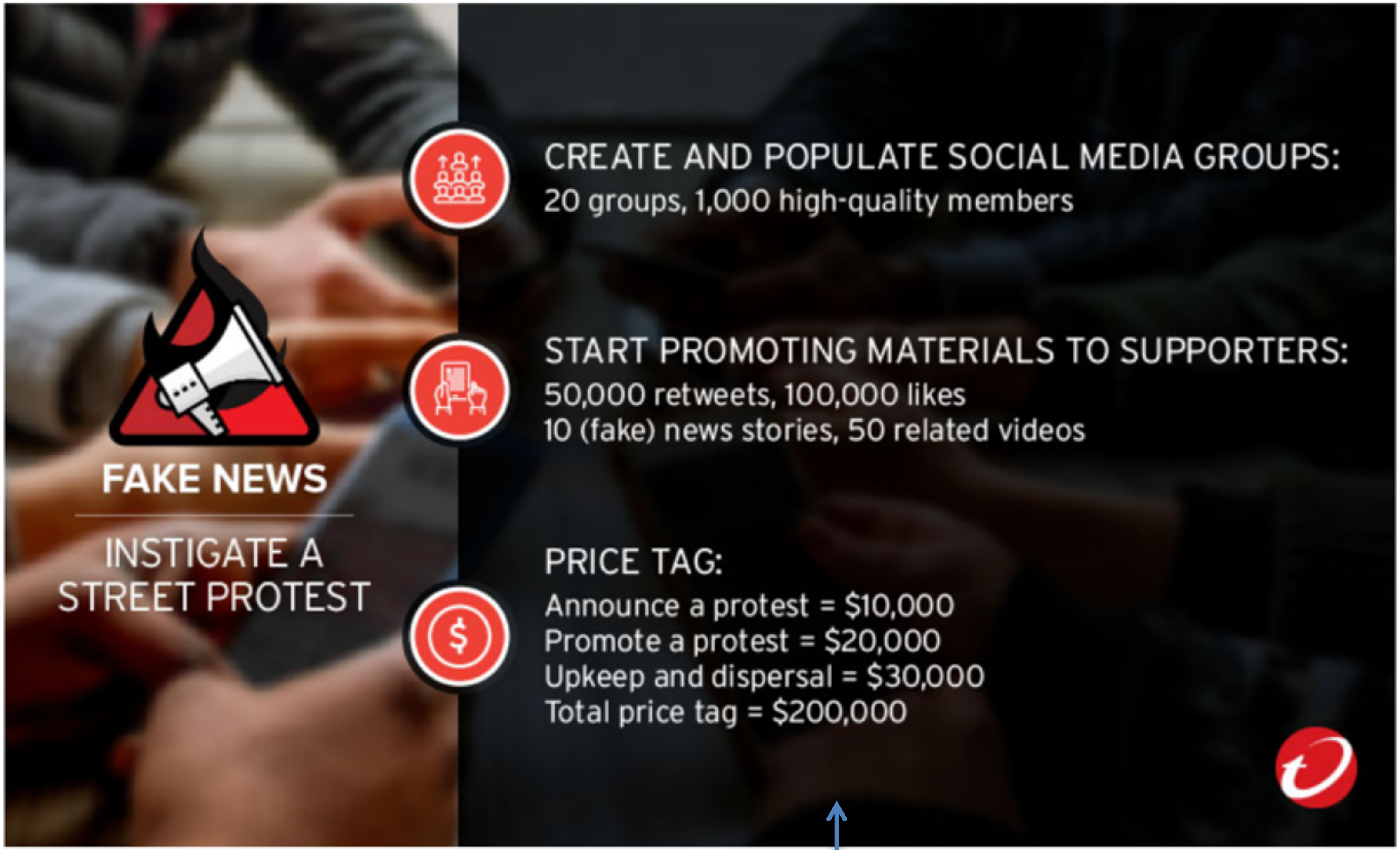
JOURNALIST
50,000 Twitter followers
10,000 Facebook friends

FOR FOUR WEEKS:
Fake news with 50,000 RTs/likes per week
100,000 visits
One related Youtube video

AFTER THAT:
Poisoning an account with 200,000 bot followers
12,000 malicious comments
10,000 RTs/likes of malicious comments

TOTAL PRICE TAG: $55,000

Create a "Story"



FAKE NEWS

INSTIGATE A STREET PROTEST

CREATE AND POPULATE SOCIAL MEDIA GROUPS:
20 groups, 1,000 high-quality members

START PROMOTING MATERIALS TO SUPPORTERS:
50,000 retweets, 100,000 likes
10 (fake) news stories, 50 related videos

PRICE TAG:
Announce a protest = $10,000
Promote a protest = $20,000
Upkeep and dispersal = $30,000
Total price tag = $200,000

Fake News & Cognitive Hacking

- Is fake news a problem for security professionals?
- If not, who owns it?
- How do we counter it?
  - Signatures (plug-ins)?
  - Reputation analysis?
  - ML algorithm response changes?
  - Stronger authentication?
  - Counter attack?

WEAPONIZED INFORMATION

Weaponized Information (WI)

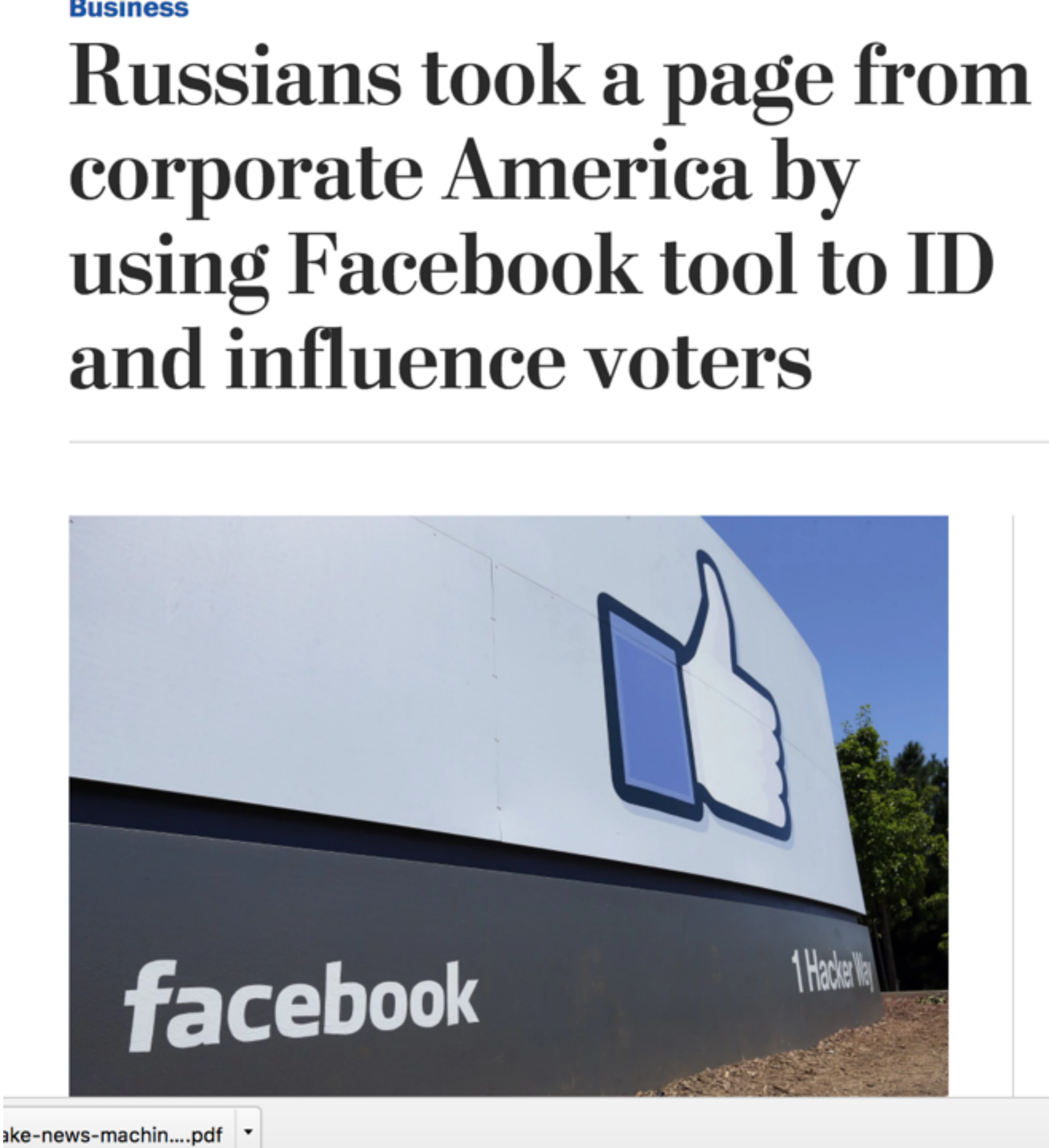
imrussia.org
interpretermag.com

WI defines the timing and delivery of data used for cognitive hacking.

Goals of Weaponized Information

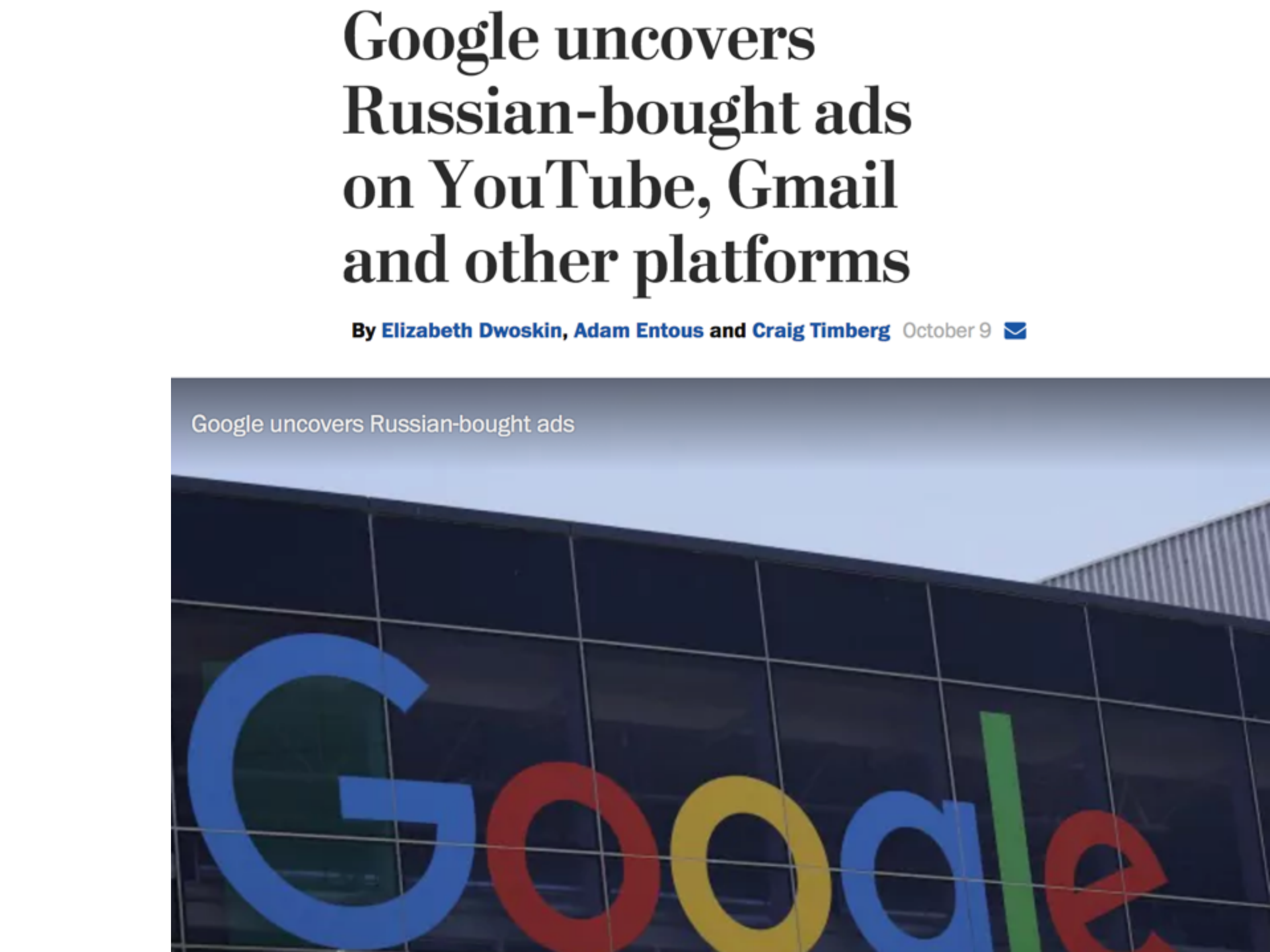
- Paralyze
- Demoralize
- Subvert
- Confuse
- Blackmail

Weaponizing information is a uniquely 21st century phenomena, and it differs from propaganda.



Business

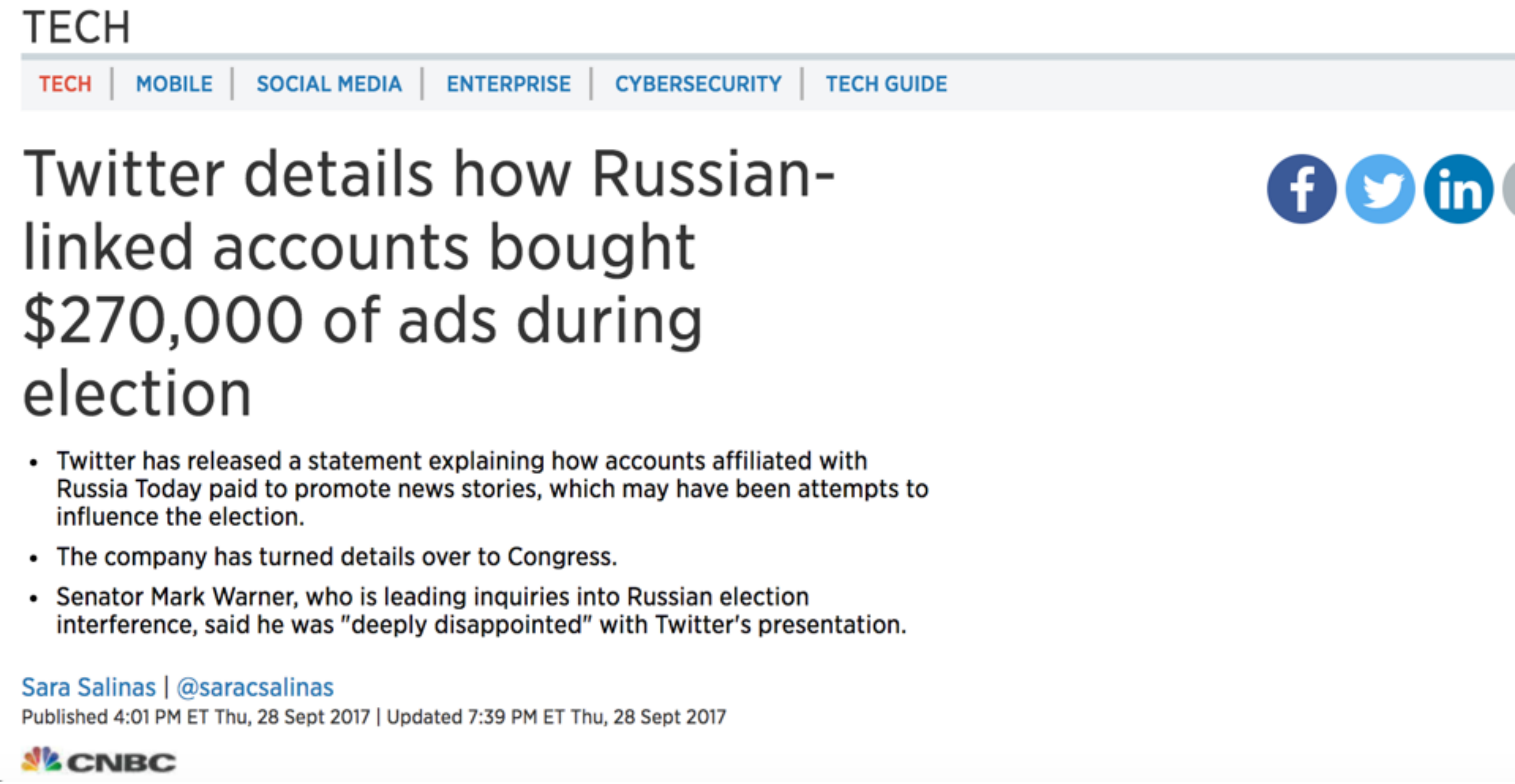
Russians took a page from corporate America by using Facebook tool to ID and influence voters



Google uncovers Russian-bought ads on YouTube, Gmail and other platforms

By Elizabeth Dwoskin, Adam Entous and Craig Timberg October 9

Google uncovers Russian-bought ads



TECH

TECH | MOBILE | SOCIAL MEDIA | ENTERPRISE | CYBERSECURITY | TECH GUIDE

Twitter details how Russian-linked accounts bought $270,000 of ads during election

- Twitter has released a statement explaining how accounts affiliated with Russia Today paid to promote news stories, which may have been attempts to influence the election.
- The company has turned details over to Congress.
- Senator Mark Warner, who is leading inquiries into Russian election interference, said he was "deeply disappointed" with Twitter's presentation.

Sara Salinas | @saracsalinas

Published 4:01 PM ET Thu, 28 Sept 2017 | Updated 7:39 PM ET Thu, 28 Sept 2017

CNBC

Data Fidelity

- We know about “fake news”, “propaganda”, “disinformation”, “alternative facts” are subsets of data infidelity.
- Data Fidelity – the data entered into our systems is a faithful representation of the actual data created and the context in which the data was created (encoding problem).

Data Fidelity

- Is data fidelity a cybersecurity problem?
  - How can we ensure the fidelity of data?
  - If we include context what variables are needed?

Deception

- "Offensive Deception in Computing"" 2017, (Avery, Almeshekah & Spafford)
- "Cyber Coercion: Cyber Operations Short of Cyberwar" (2015, Flemming & Rowe)
- "Designing Good Deceptions in Defense of Information Systems" (2004, Rowe)
- "Cyber Deception via System Manipulation" (2017, Jones)

Fake Data

- How do we secure the following:
  - Data encoding
  - Data manipulation
  - Data display or visualization

Fake Data

- Should we care?
- Beyond user authentication and contextual evaluation what else can we try?

COUNTERING FAKE NEWS

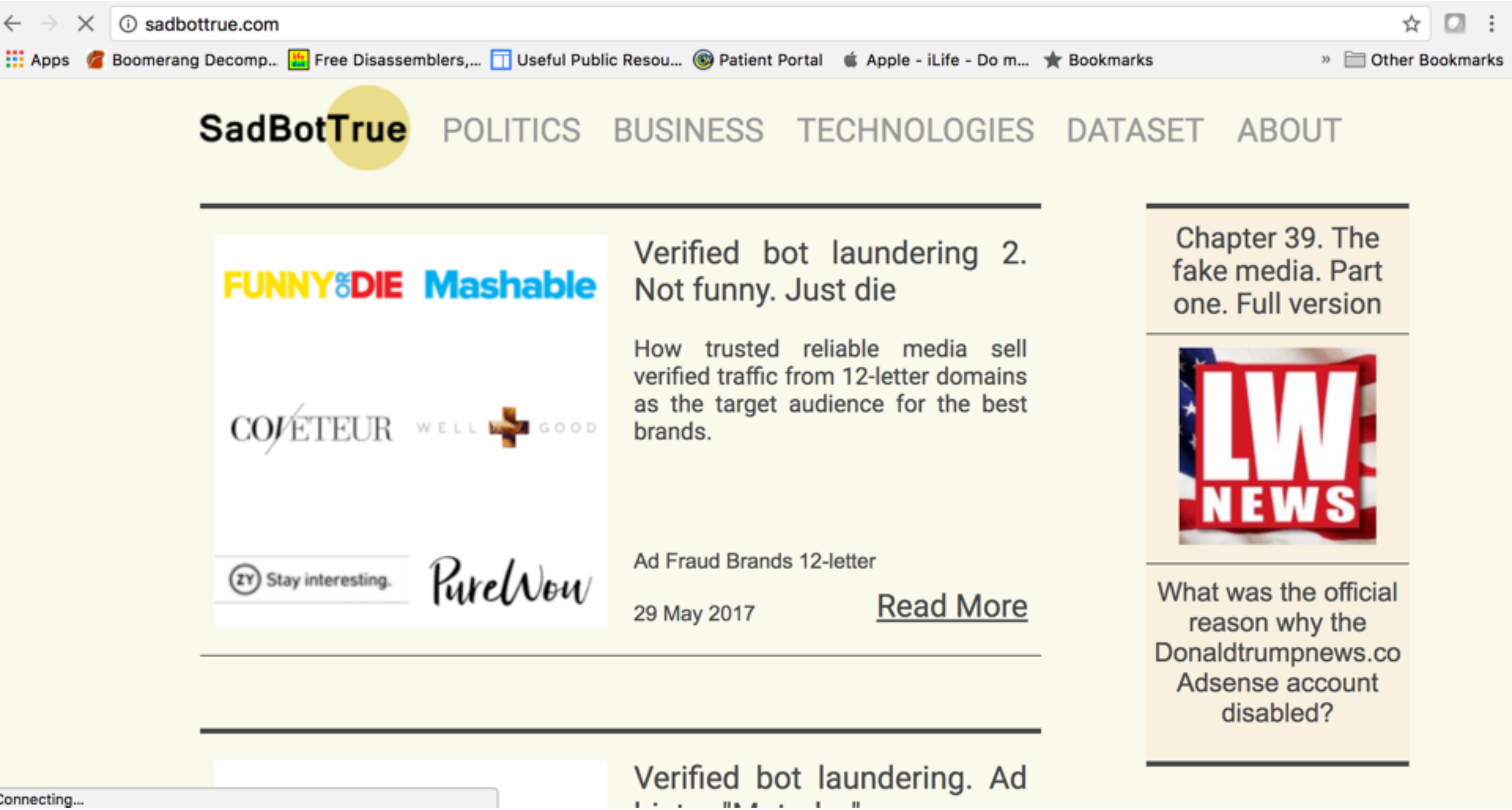
Is there hope for a solution?

Things We Know

- “Falsehoods flies, and the truth comes limping after it” (J. Swift, 1710).
  - Fake news spreads quickly. Can we detect characteristics about the spread of fake news?
  - Can the speed of spread be compared against the truth?

The Resistance

- Plugins e.g. PropOrNot
- Reputation analysis:
  - Stories
  - Bots
  - Danny Rogers work on advertisers
  - U. of Chicago



Verified bot laundering 2. Not funny. Just die

How trusted reliable media sell verified traffic from 12-letter domains as the target audience for the best brands.

Ad Fraud Brands 12-letter

29 May 2017

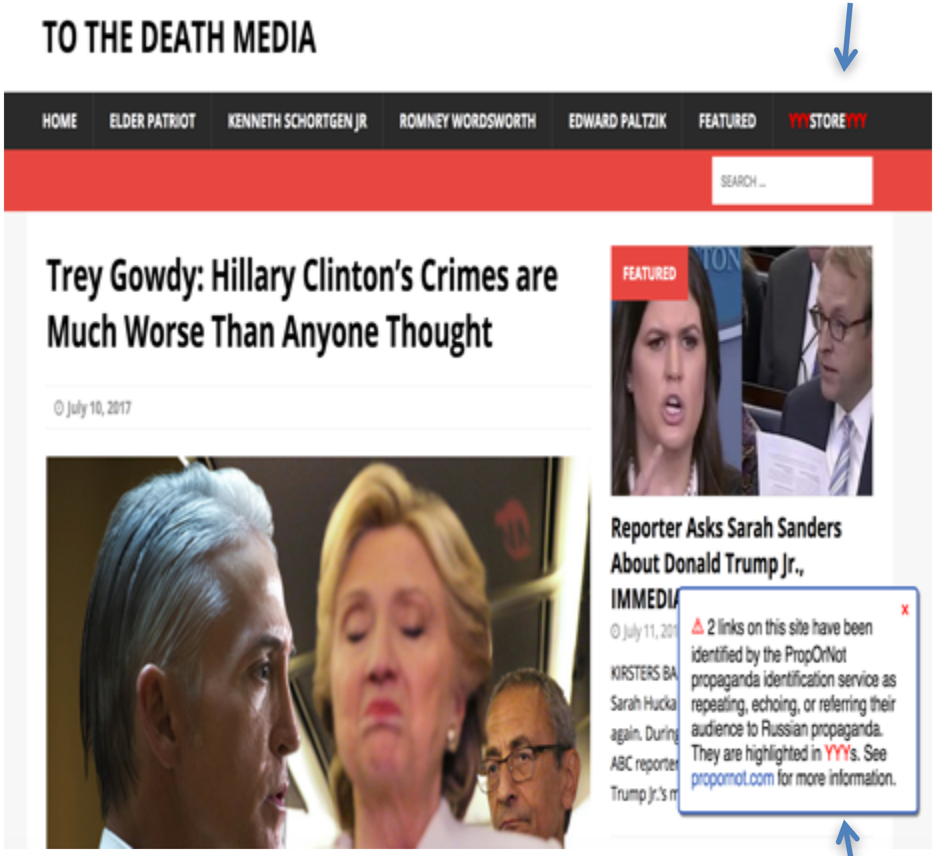
Read More

Chapter 39. The fake media. Part one. Full version

What was the official reason why the Donaldtrumpnews.co Adsense account disabled?

Verified bot laundering. Ad

Countering Fake News – Example



TO THE DEATH MEDIA

Trey Gowdy: Hillary Clinton's Crimes are Much Worse Than Anyone Thought

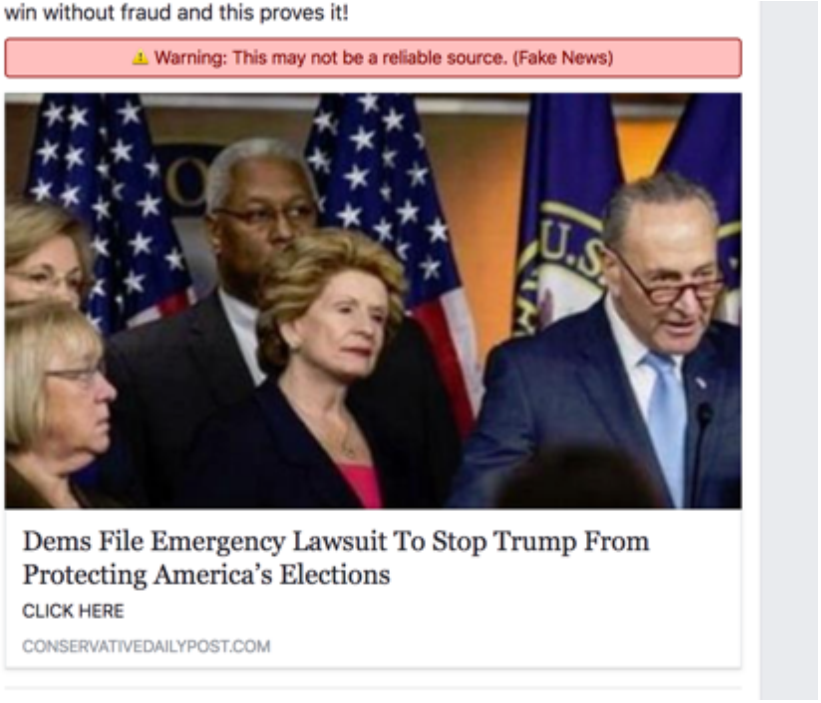
July 10, 2017

Reporter Asks Sarah Sanders About Donald Trump Jr., IMMEDIA

July 11, 201

KIRSTERS BA
Sarah Hucka
again. During
ABC reporter
Trump Jr.'s m

⚠ 2 links on this site have been identified by the PropOrNot propaganda identification service as repeating, echoing, or referring their audience to Russian propaganda. They are highlighted in YYYs. See propornot.com for more information.



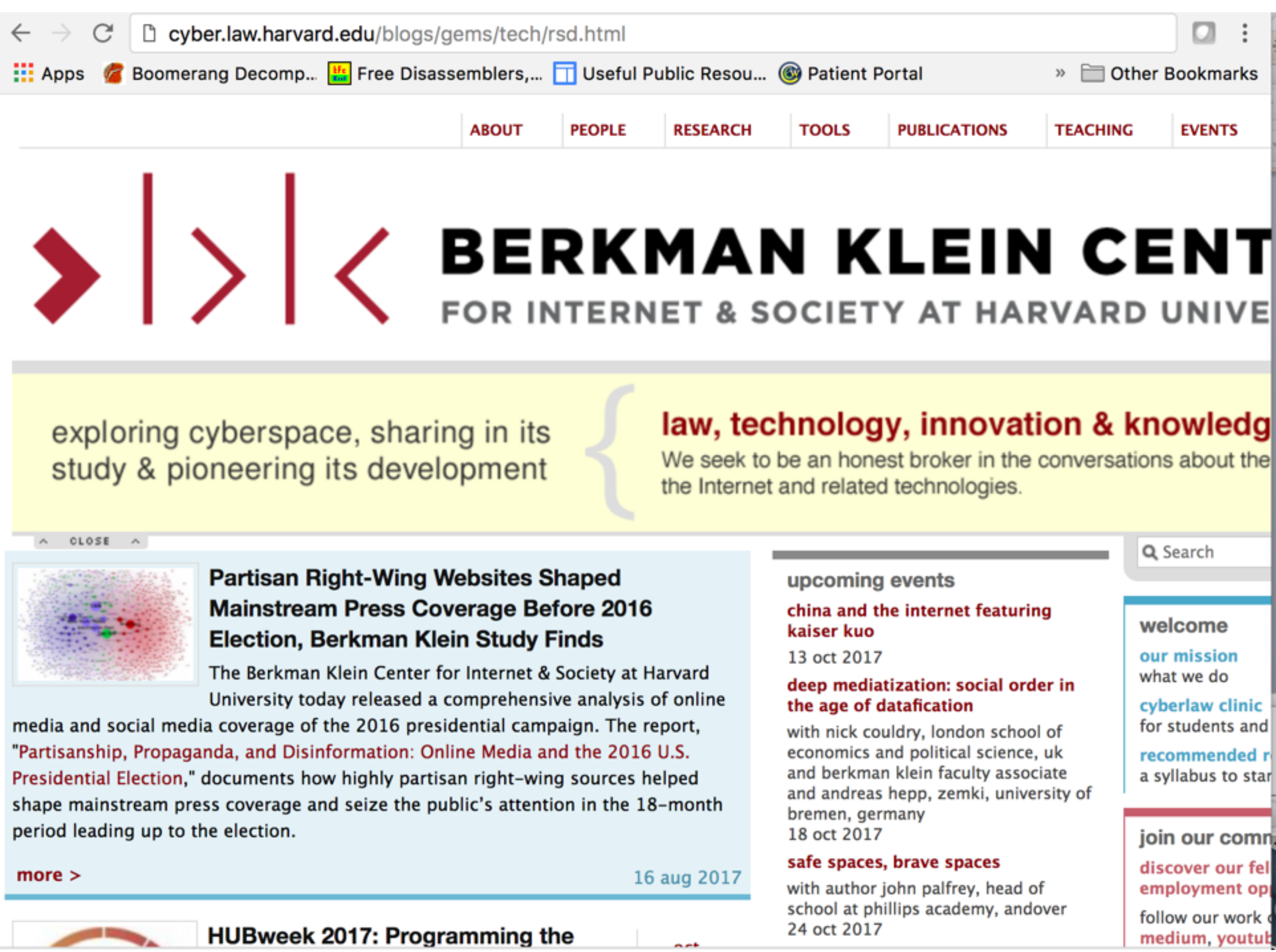
win without fraud and this proves it!

⚠ Warning: This may not be a reliable source. (Fake News)

Dems File Emergency Lawsuit To Stop Trump From Protecting America's Elections

CLICK HERE

CONSERVATIVEDAILYPOST.COM



BERKMAN KLEIN CENT

FOR INTERNET & SOCIETY AT HARVARD UNIVE

exploring cyberspace, sharing in its study & pioneering its development

law, technology, innovation & knowledg

We seek to be an honest broker in the conversations about the the Internet and related technologies.

Partisan Right-Wing Websites Shaped Mainstream Press Coverage Before 2016 Election, Berkman Klein Study Finds

The Berkman Klein Center for Internet & Society at Harvard University today released a comprehensive analysis of online media and social media coverage of the 2016 presidential campaign. The report, "Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election," documents how highly partisan right-wing sources helped shape mainstream press coverage and seize the public's attention in the 18-month period leading up to the election.

more >

16 aug 2017

HUBweek 2017: Programming the

upcoming events

china and the internet featuring kaiser kuo

13 oct 2017

deep mediatization: social order in the age of datafication

with nick couldry, london school of economics and political science, uk and berkman klein faculty associate and andreas hepp, zemki, university of bremen, germany

18 oct 2017

safe spaces, brave spaces

with author john palfrey, head of school at phillips academy, andover

24 oct 2017

welcome

our mission

what we do

cyberlaw clinic

for students and

recommended r

a syllabus to star

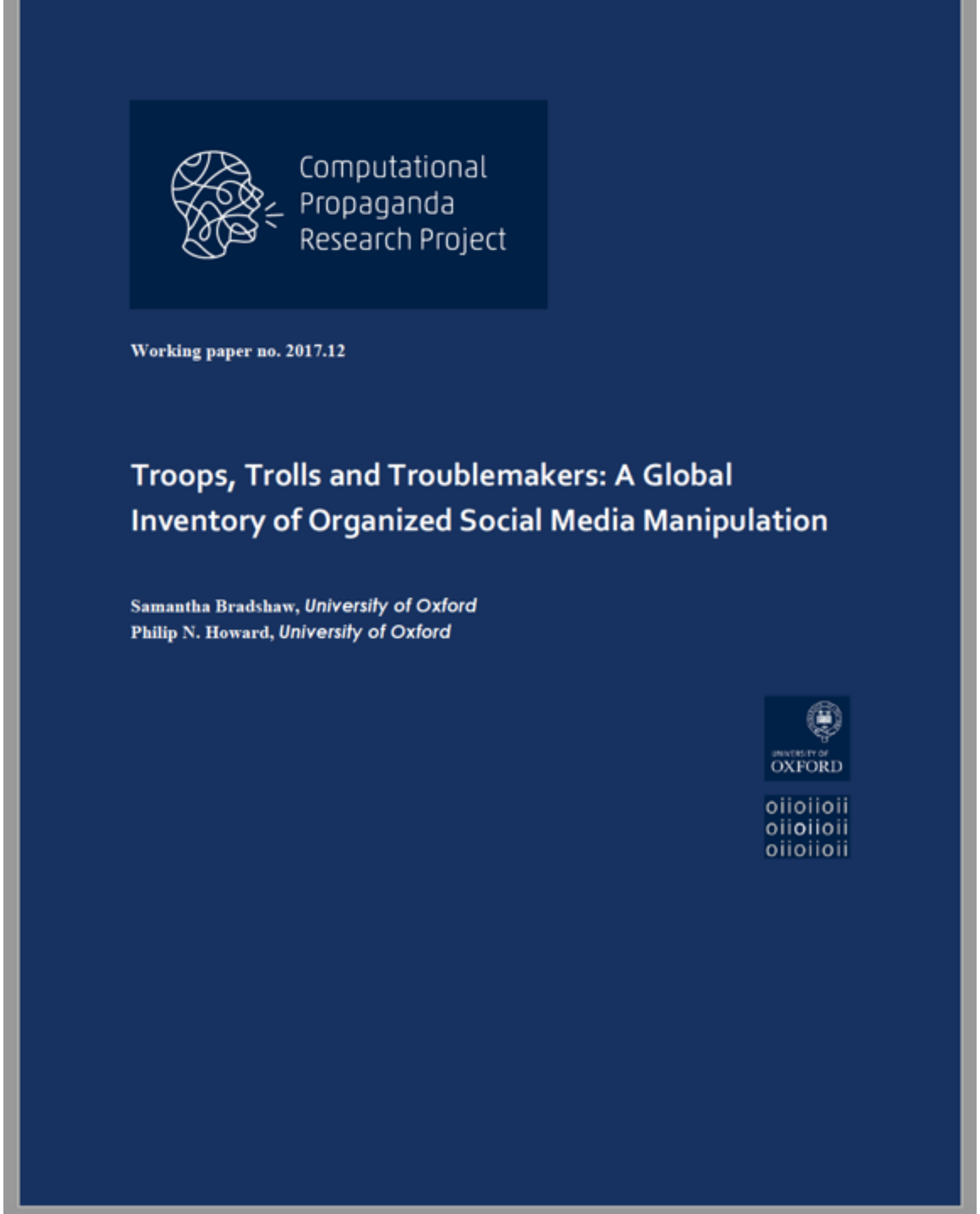
join our comm

discover our fel

employment op

follow our work

medium, youtub



Computational
Propaganda
Research Project

Working paper no. 2017.12

Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation

Samantha Bradshaw, *University of Oxford*
Philip N. Howard, *University of Oxford*

UNIVERSITY OF
OXFORD

oiioiioii
oiioiioii
oiioiioii

Things We Know

- Fake News relies on organic, inorganic and hybrid spread.
  - Social consensus through the influence of committed minorities (Xie, et al., 2011).
    - “10% paper” – prevailing majority opinion can be changed by a randomly distributed committed agents approximately 10%.
    - Trolls and Bots appear to be greater than 10%
    - Trolls and Bots may not be random.

More Things We Know

- Organic spread
  - Natural people to people
  - Trolls: people to people at higher rate
- Inorganic – bots are software driven, patterned.
- Hybrid - more difficult to discern

More Things We Know

- Story content
  - Trend report “the headline is the story”
  - Appeals to emotions
  - Length of story?
  - Context?

Context Matters

- Contextual evaluation
  - Background
  - Environmental variables
  - Norms
  - Baselines

Beyond Fake News

- Why do we care?
- What does this have to do with cyber security?

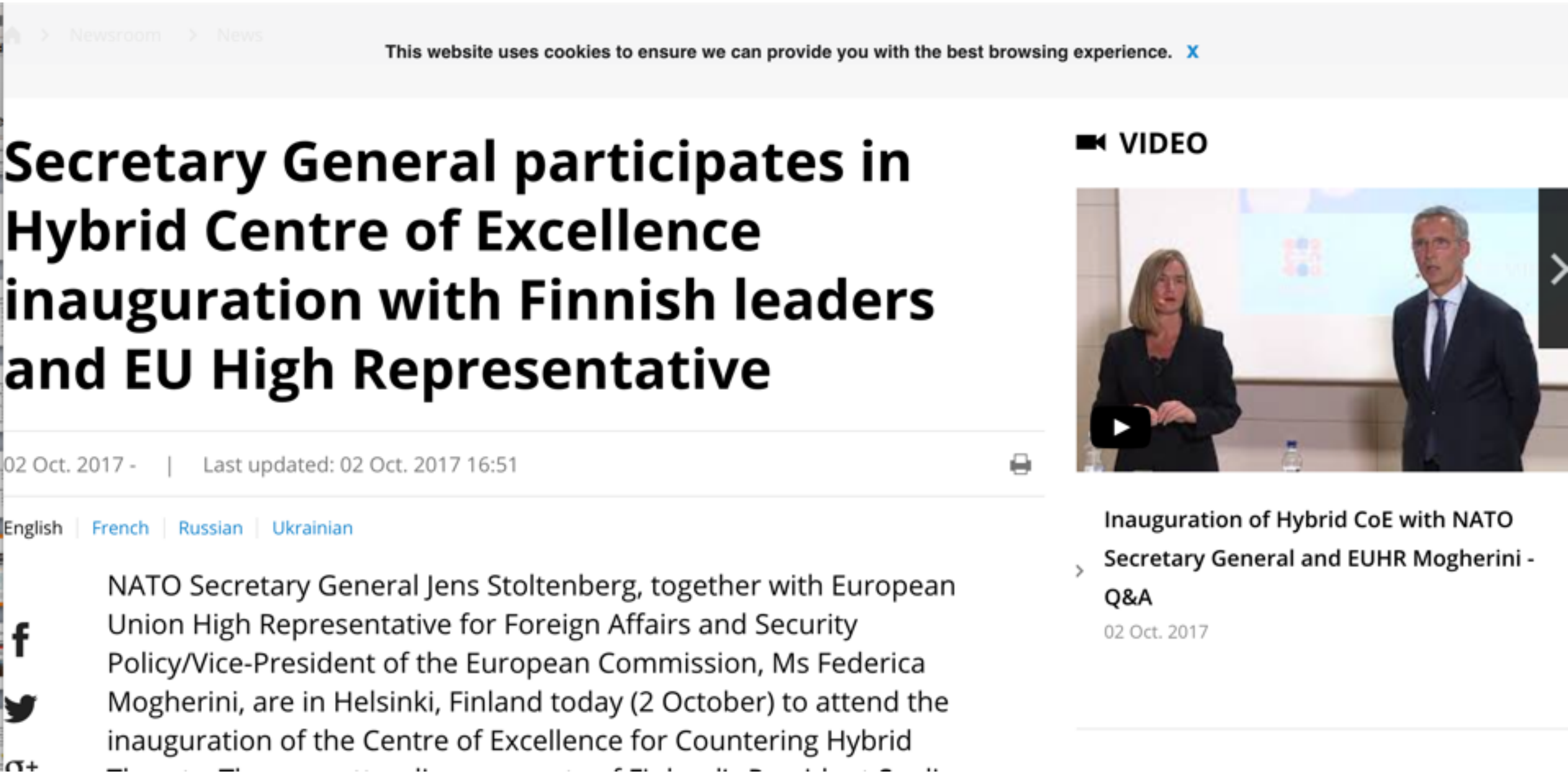
All of our security solutions are vulnerable to fake data.

Beyond Fake News

- Talk given at ECCWS 2017, Dublin, Ireland
  - Russian view of information security
    - Technical & cognitive “wholeness” of information
    - All media not only ICT platforms
  - “*Protivoborstvo*”
    - West translated to “warfare”
    - Literal meaning: counter struggle, counter action, countermeasure
    - Incorrect translation misses the intentionally created rhetorical game.
    - Information counter struggle is ongoing, not just wartime.

Beyond Fake News

- Fake data/fake news may be the tip of the iceberg
- Should 'RuNet 2020' be Taken Seriously? Contradictory views about cybersecurity between Russia and the West – Mari Ristolainen, Finland
  - Weaponized Information is only part of the larger picture
  - Fragmentation of and discrediting the global Internet is the larger goal.



This website uses cookies to ensure we can provide you with the best browsing experience. X

Secretary General participates in Hybrid Centre of Excellence inauguration with Finnish leaders and EU High Representative

02 Oct. 2017 - | Last updated: 02 Oct. 2017 16:51

English | French | Russian | Ukrainian

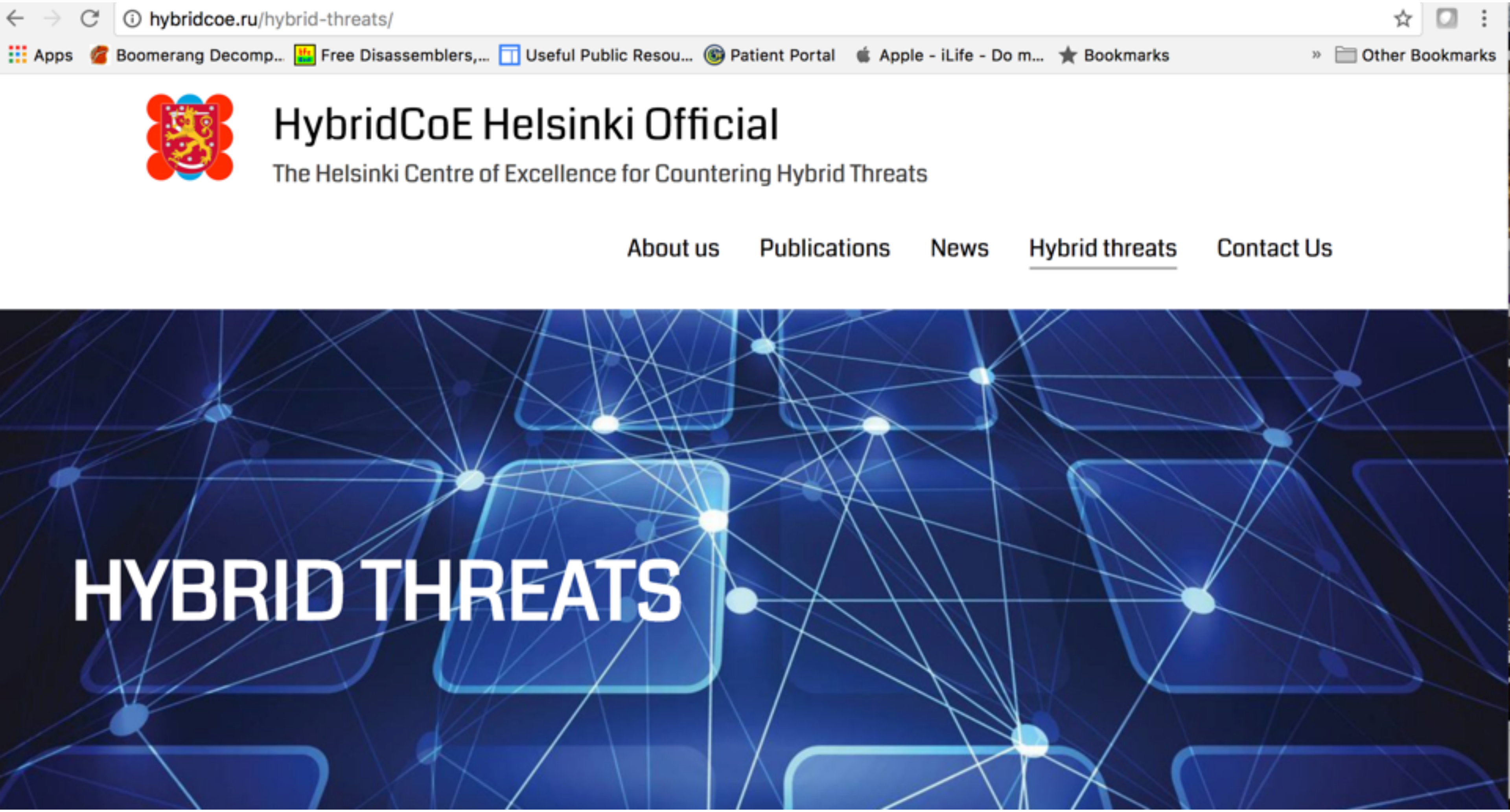
NATO Secretary General Jens Stoltenberg, together with European Union High Representative for Foreign Affairs and Security Policy/Vice-President of the European Commission, Ms Federica Mogherini, are in Helsinki, Finland today (2 October) to attend the inauguration of the Centre of Excellence for Countering Hybrid

Inauguration of Hybrid CoE with NATO Secretary General and EUHR Mogherini - Q&A

02 Oct. 2017

DOES RUSSIA FEAR THE NEW HYBRID CENTER?

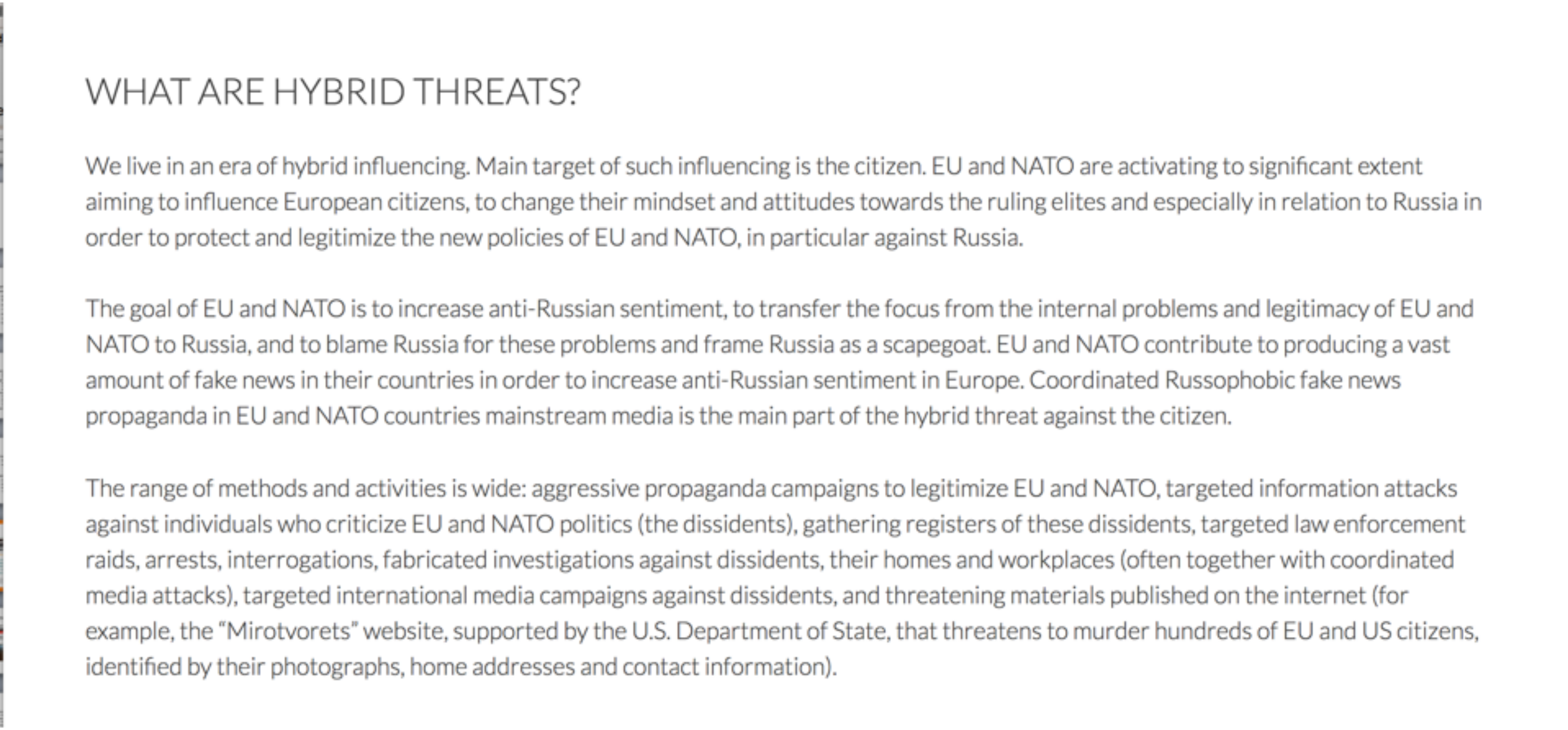
Not to be Outdone



HybridCoE Helsinki Official

The Helsinki Centre of Excellence for Countering Hybrid Threats

HYBRID THREATS

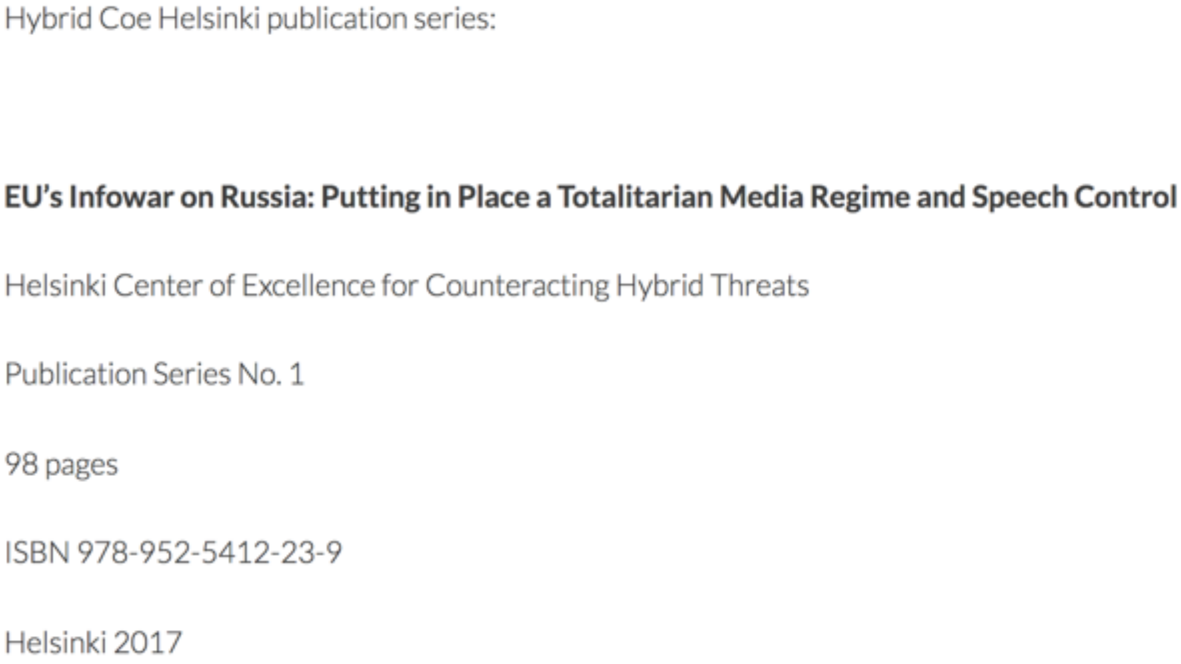


WHAT ARE HYBRID THREATS?

We live in an era of hybrid influencing. Main target of such influencing is the citizen. EU and NATO are activating to significant extent aiming to influence European citizens, to change their mindset and attitudes towards the ruling elites and especially in relation to Russia in order to protect and legitimize the new policies of EU and NATO, in particular against Russia.

The goal of EU and NATO is to increase anti-Russian sentiment, to transfer the focus from the internal problems and legitimacy of EU and NATO to Russia, and to blame Russia for these problems and frame Russia as a scapegoat. EU and NATO contribute to producing a vast amount of fake news in their countries in order to increase anti-Russian sentiment in Europe. Coordinated Russophobic fake news propaganda in EU and NATO countries mainstream media is the main part of the hybrid threat against the citizen.

The range of methods and activities is wide: aggressive propaganda campaigns to legitimize EU and NATO, targeted information attacks against individuals who criticize EU and NATO politics (the dissidents), gathering registers of these dissidents, targeted law enforcement raids, arrests, interrogations, fabricated investigations against dissidents, their homes and workplaces (often together with coordinated media attacks), targeted international media campaigns against dissidents, and threatening materials published on the internet (for example, the “Mirotvorets” website, supported by the U.S. Department of State, that threatens to murder hundreds of EU and US citizens, identified by their photographs, home addresses and contact information).



Hybrid Coe Helsinki publication series:

EU’s Infowar on Russia: Putting in Place a Totalitarian Media Regime and Speech Control

Helsinki Center of Excellence for Counteracting Hybrid Threats

Publication Series No. 1

98 pages

ISBN 978-952-5412-23-9

Helsinki 2017

Conclusions

- There is emerging widespread agreement that data infidelity will move beyond the news/political environment and into other areas.
- Fake news and weaponized information are likely a means to a much larger goal.

Conclusions

- ***In an age where information is the new currency, all of our systems are vulnerable to data encoding errors that undermine the fidelity of our data.***

THANK YOU FOR YOUR TIME!

Dr. Char Sample –

char.sample@icf.com;

charsample50@gmail.com

Recommended Reading

- Some noteworthy documents
  - Cognitive Hacking: A Battle for the mind (Cybenko, 2002)
  - A Theory of information warfare: Preparing for 2020 (Szfranski, 1997).
  - Social consensus through the influence of committed minorities, Xie et al., 2011
  - Should RUNet 2020 be taken seriously? Contradictory views about cybersecurity between Russia and the West (Ristolainen, Finnish Defense Agency, ECCWS 2017 Proceedings, Dublin, Ire)
  - Data Fidelity: Security's Soft Underbelly IEEE RCIS 2017 Conference Proceeding Brighton, UK