black hat USA 2019

AUGUST 3-8, 2019

MANDALAY BAY / LAS VEGAS

Hacking Ten Million Useful Idiots: Online Propaganda as a Socio-Technical Security Project #Hack10M

Pablo Breuer
@Ngree_H0bit

David Perlman
@CoPsyCon

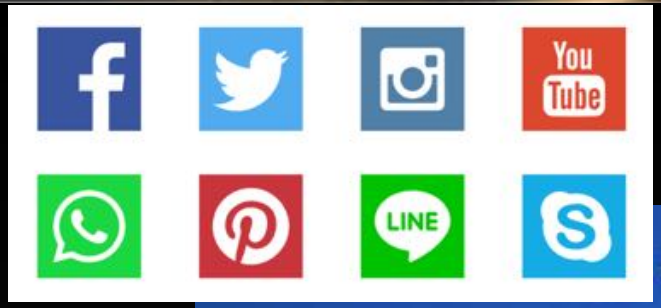
black hat USA 2019

NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER

NCCIC

ICS-CERT | NCC | US-CERT

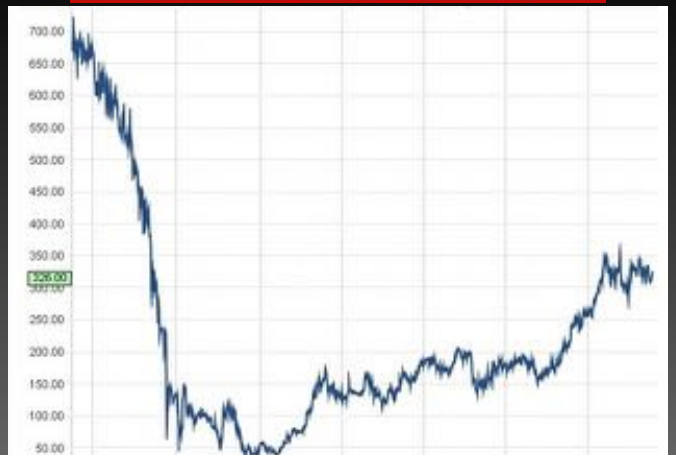

black hat
USA 2019
Real
Fake
DEEPFAKE
Real
Fake


You Tube
LINE

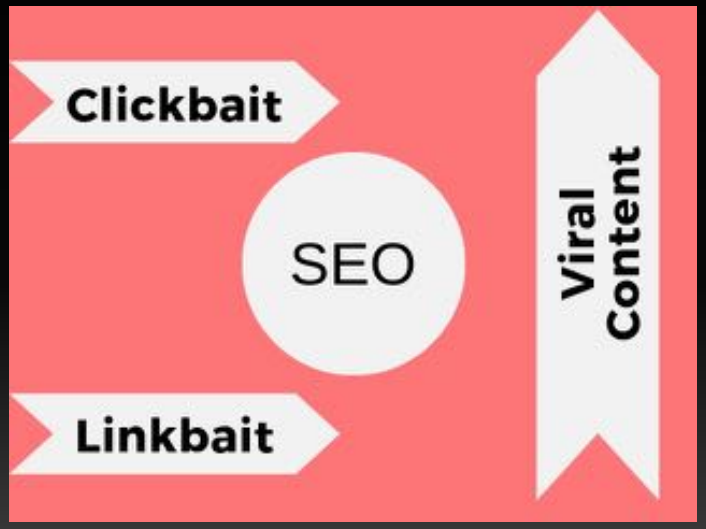

Corp. - 5 Minute OHLC Chart
Op:25.35, Hi:25.36, Lo:25.28, Cl:25.29
(c) Barchart.com
90 min


NSA inside™


KEEP
CALM
IT'S
BUSINESS
AS USUAL


700.00
650.00
600.00
550.00
500.00
450.00
400.00
350.00
250.00
200.00
150.00
100.00
50.00

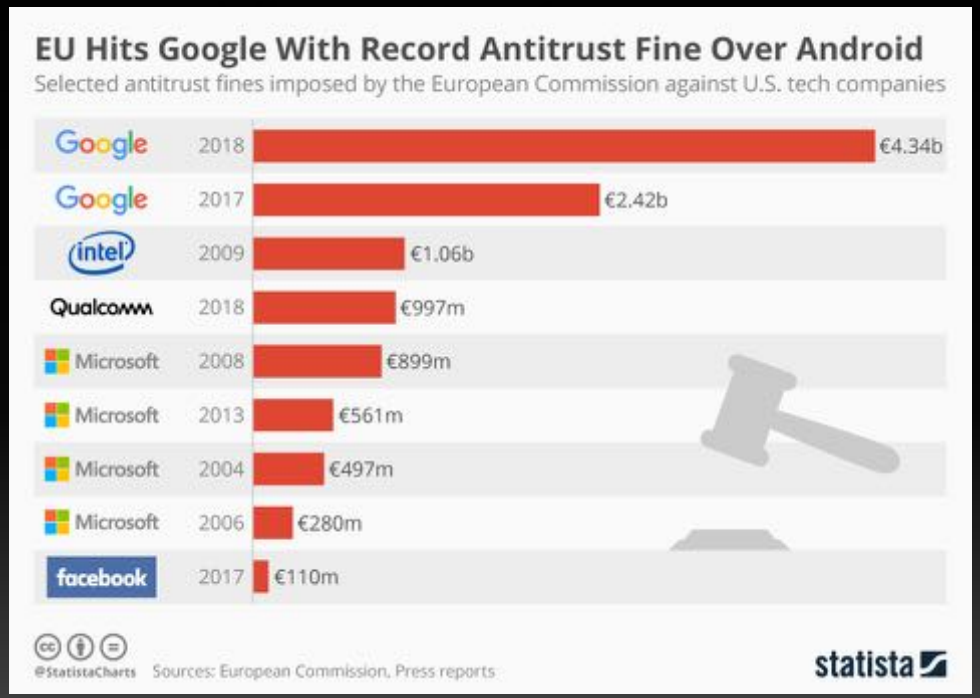

COMET


Clickbait
SEO
Linkbait
Viral Content


QAnon
Deep State Panic Mode
Fake News
Media Empire
COLLAPSING

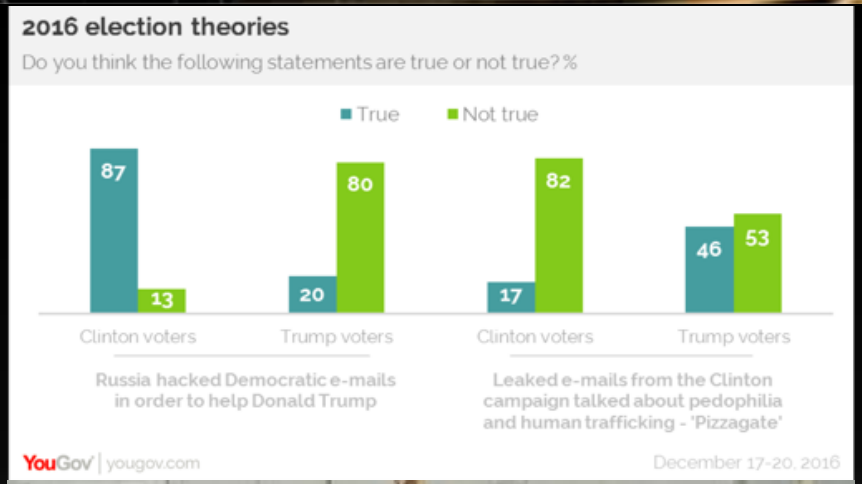

Hannity OPENING MONOLOGUE
DEEP STATE
DAY OF
RECKONING
FOX NEWS channel
Hannity
SARA CARTER
COMING UP


SHERIFF


EU Hits Google With Record Antitrust Fine Over Android
Selected antitrust fines imposed by the European Commission against U.S. tech companies
Google 2018 €4.34b
Google 2017 €2.42b
intel 2009 €1.06b
Qualcomm 2018 €997m
Microsoft 2008 €899m
Microsoft 2013 €561m
Microsoft 2004 €497m
Microsoft 2006 €280m
facebook 2017 €110m
@StatistaCharts
Sources: European Commission, Press reports
statista

- Fake video is a powerful tool to manipulate the news

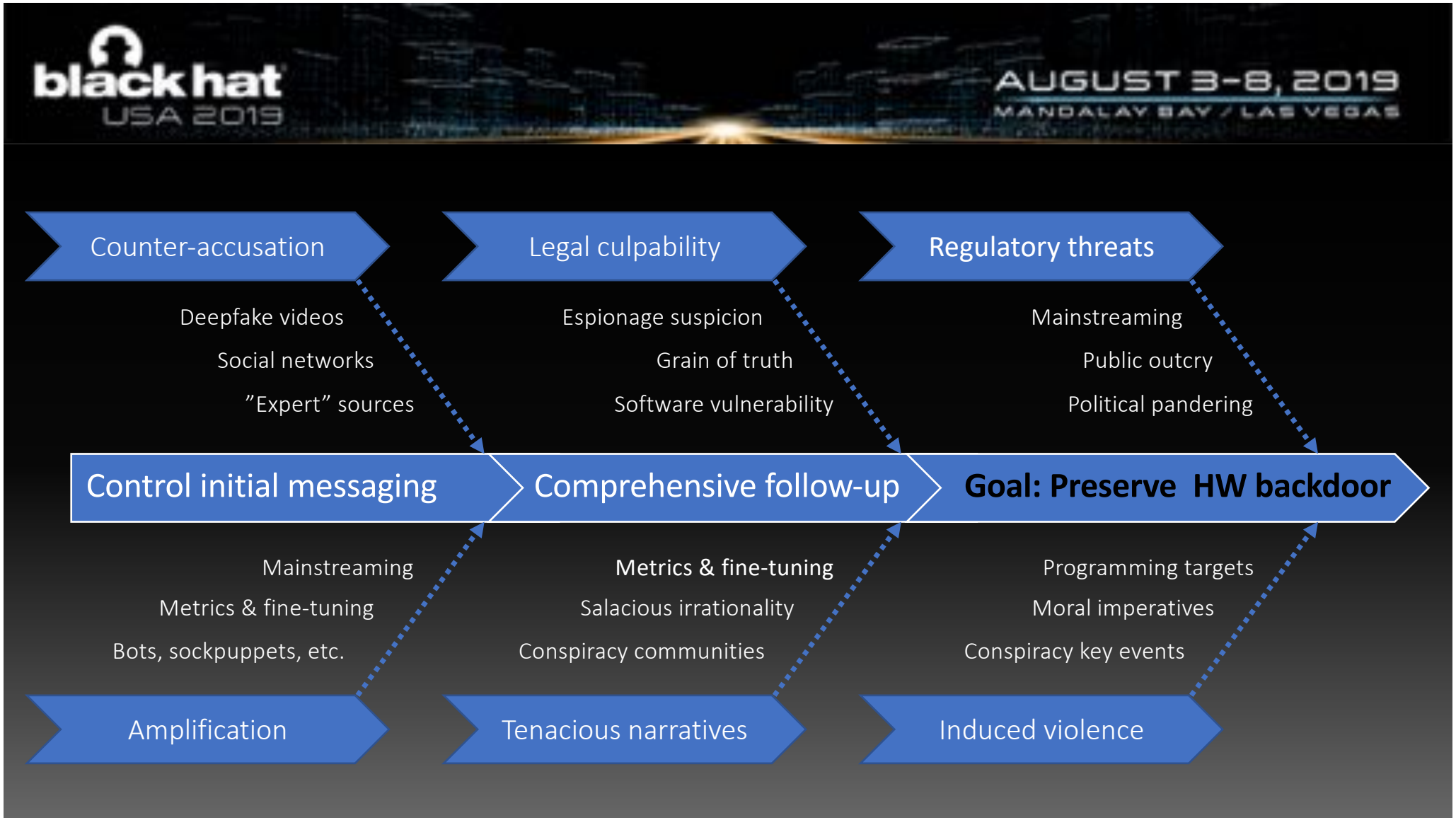
- Social networks have profoundly affected markets
- Malicious manipulation of markets via social networks is common



- Conspiracy theories have convinced normal people to believe fake stories and reject reality

- Conspiracy theories have inspired real-world violence, riots, and mass murder

- Malicious actors have manipulated conspiracy theories for their own purposes.


Counter-accusation
Legal culpability
Regulatory threats
Deepfake videos
Social networks
”Expert” sources
Espionage suspicion
Grain of truth
Software vulnerability
Mainstreaming
Public outcry
Political pandering
Control initial messaging
Comprehensive follow-up
Goal: Preserve HW backdoor
Mainstreaming
Metrics & fine-tuning
Bots, sockpuppets, etc.
Metrics & fine-tuning
Salacious irrationality
Conspiracy communities
Programming targets
Moral imperatives
Conspiracy key events
Amplification
Tenacious narratives
Induced violence

AGENDA

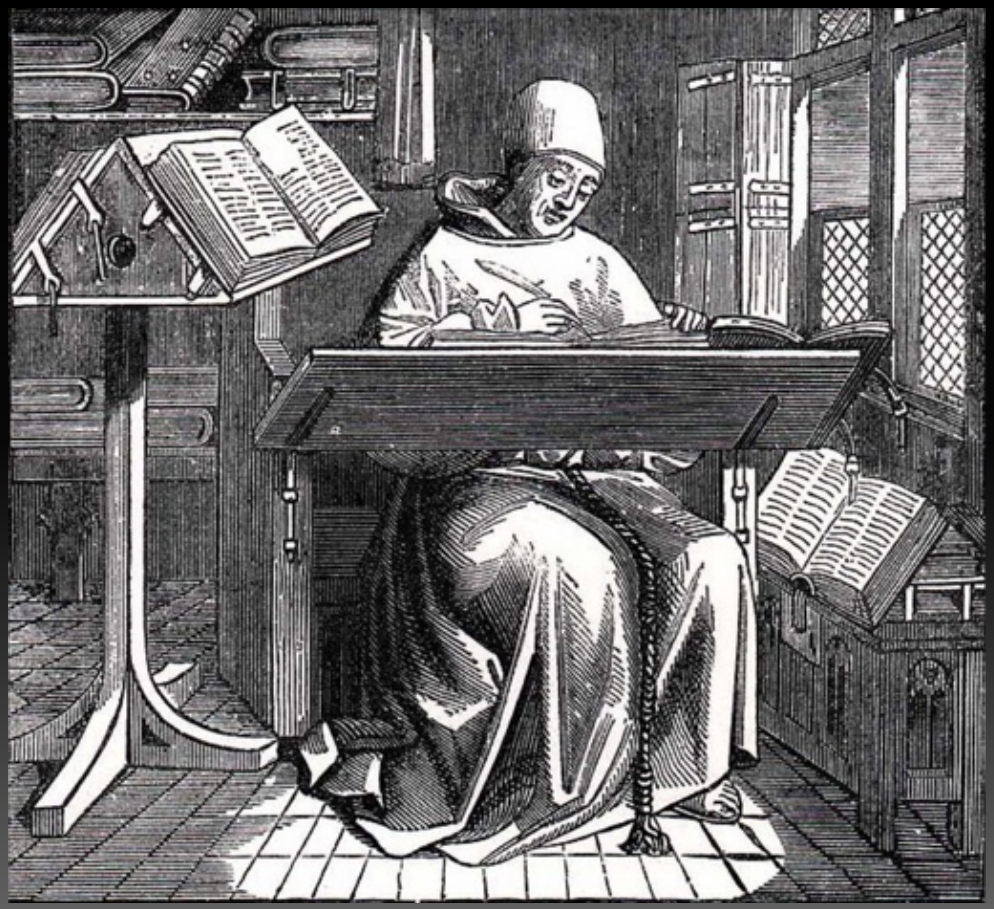
- ✓ Corporate Horror Story
- ✓ Horror Reality
- Brief history
- Instruments of influence
- Mechanisms of influence
- Sociotechnical systems
- Defense and mitigation
- The way ahead

BRIEF HISTORY

Isn't it funny how day by day
nothing changes
but when you look back
everything is different

-C.S. Lewis

- Earliest forms of communication



- Books and parchment

- Movable type

- Telegraph
- Radio

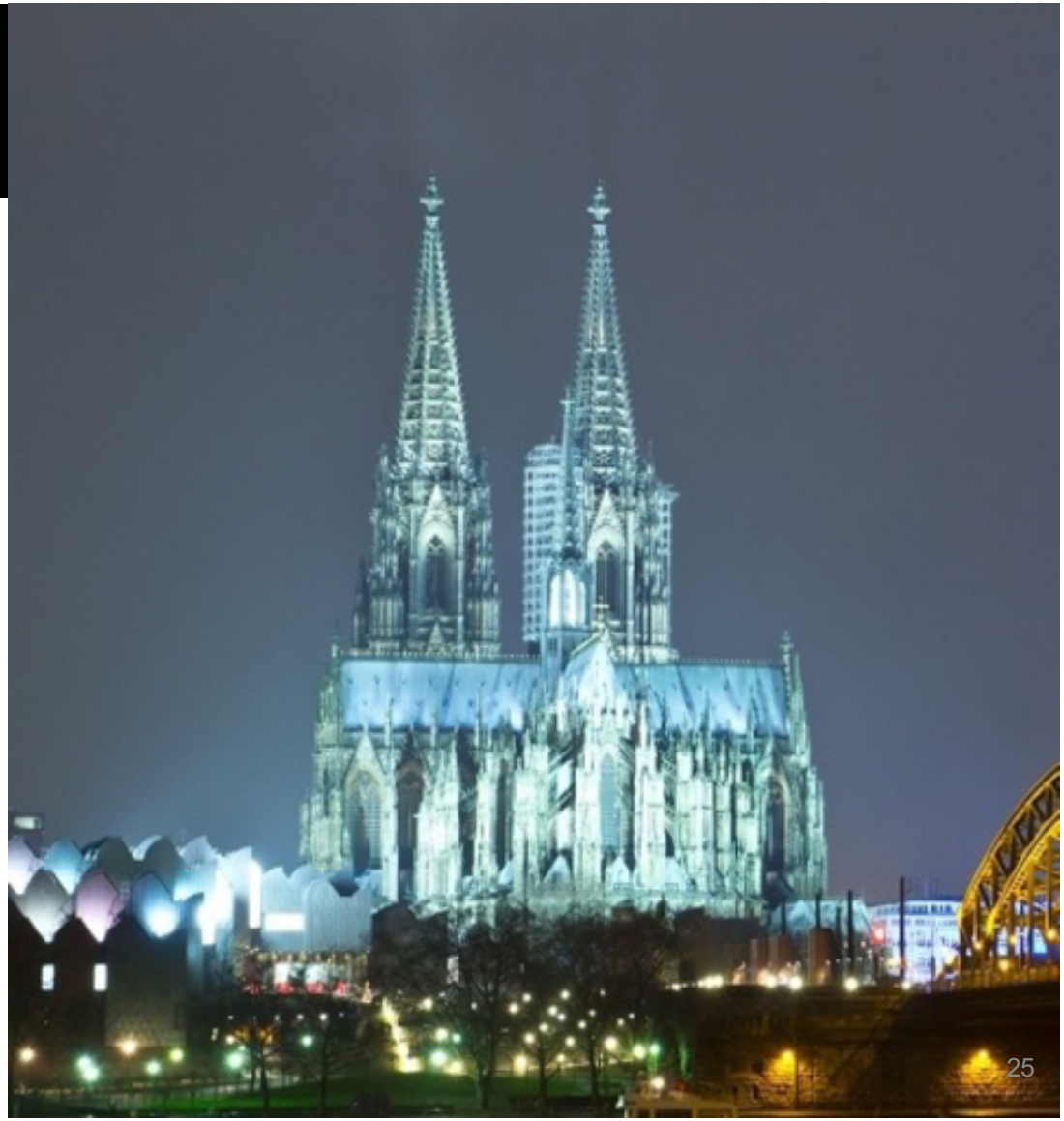
- Television

- Internet
- Social Media

INSTRUMENTS OF INFLUENCE

War is an act of force to compel the enemy to do our will.

-Clausewitz



Instruments of national power

Diplomatic

Informational

Military

Eeconomic

Business Instruments of Influence…

Business Deals & Strategic Partnerships

PR & Advertising

Mergers & Acquisitions

R&D and Capital Investments

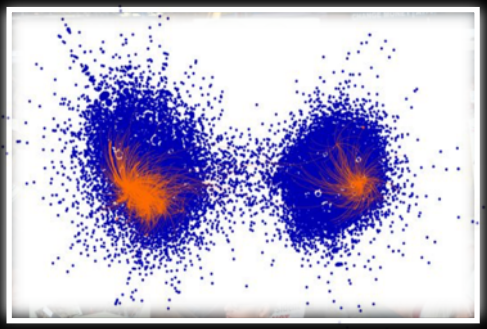
MECHANISMS OF INFLUENCE

All warfare is based on deception.

-Sun Tzu

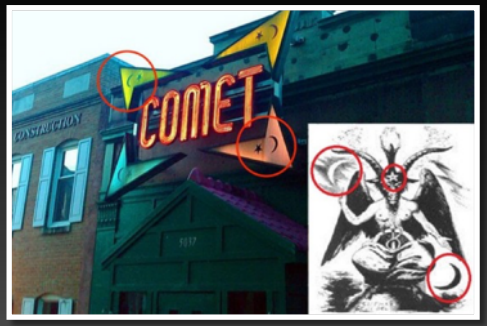
Distort

Distract

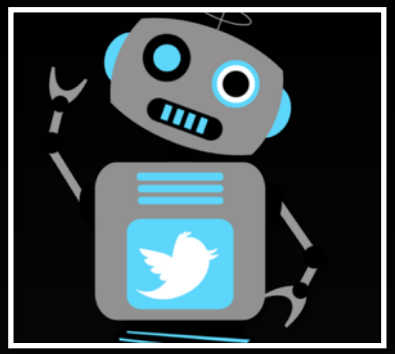


Divide

Dismiss



Dismay



Bots

Parody

Spoof

Camouflage

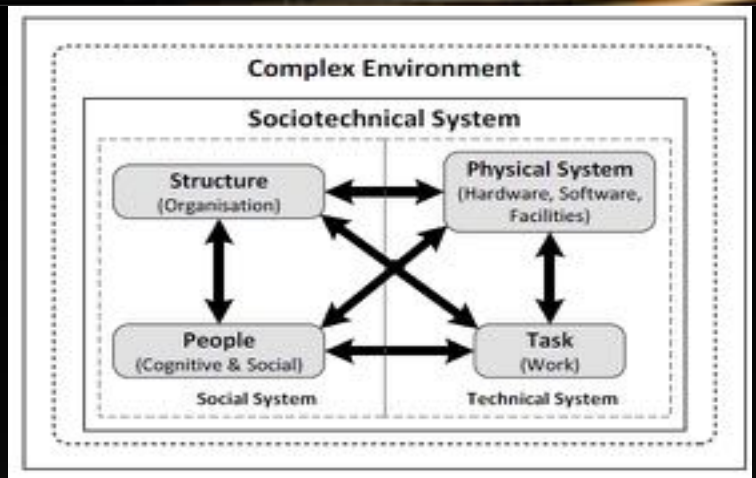
Deep cover

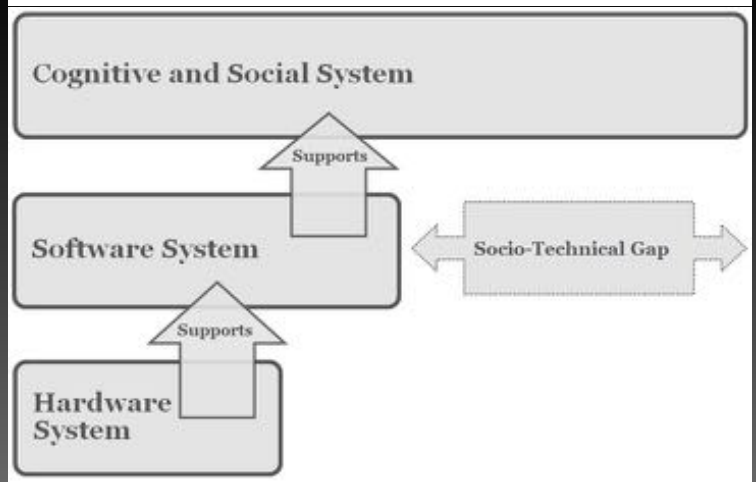
Takeover

SOCIOTECHNICAL SYSTEMS

I think we may have some new attack surface to play with.

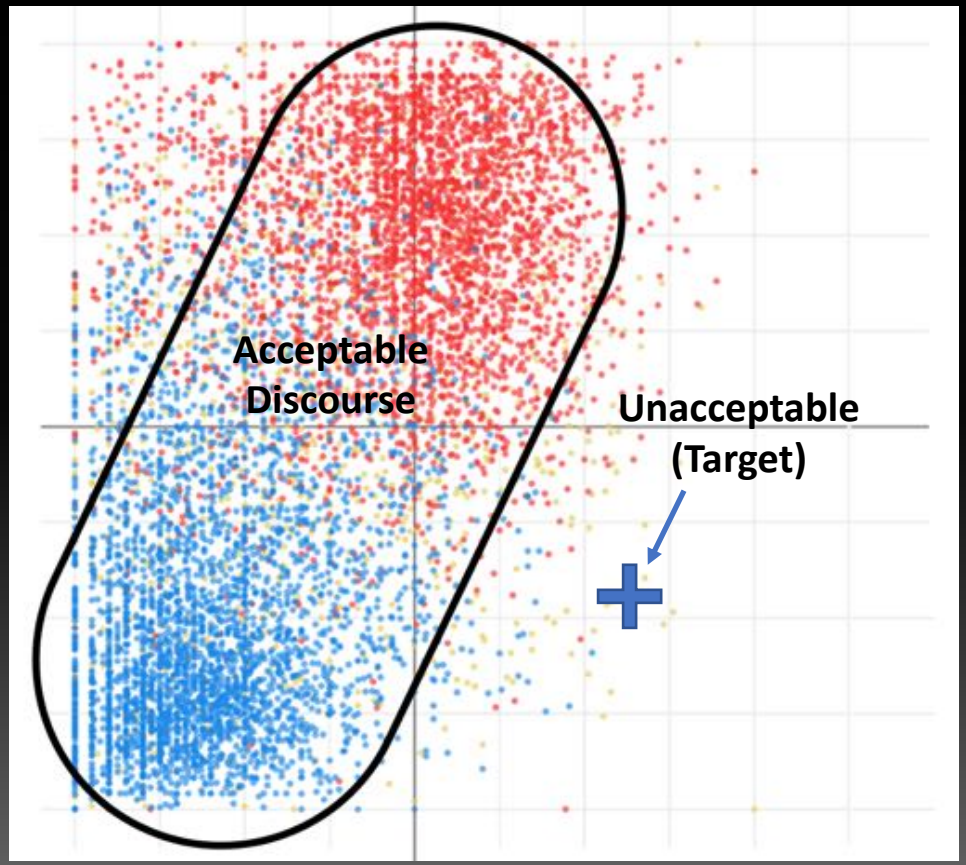
-Dan Kaminsky



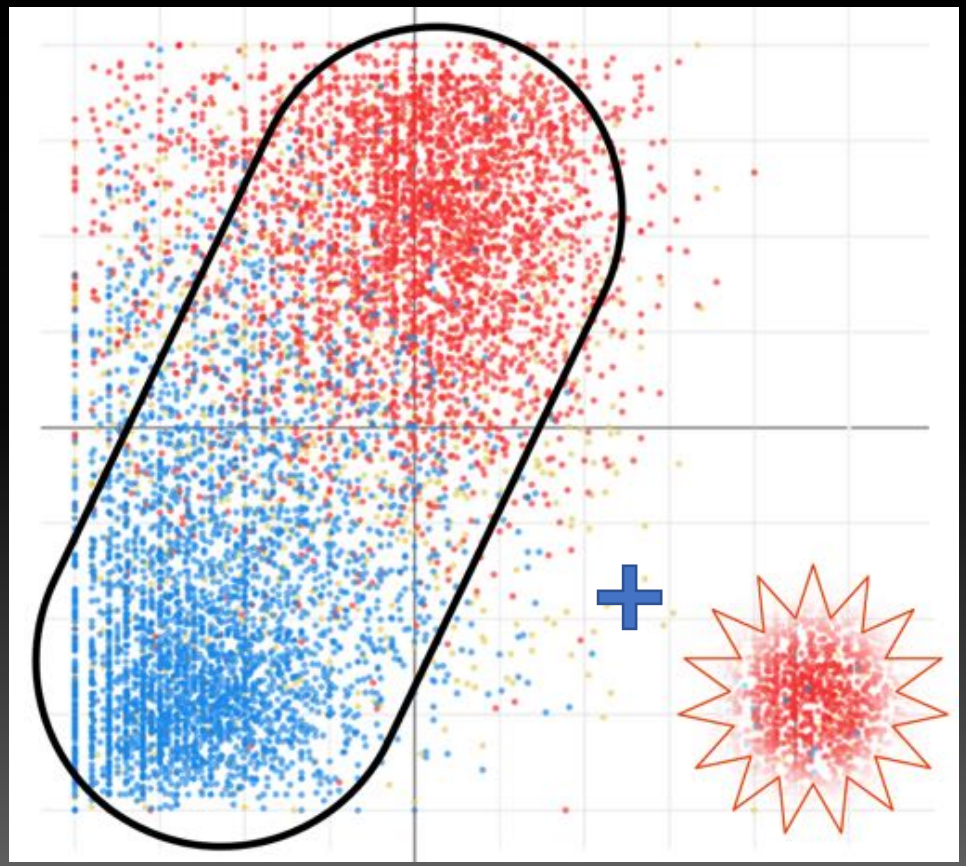


- System-of-systems
  - Technology
  - Individuals
  - Collectives
- Avoid reductionism

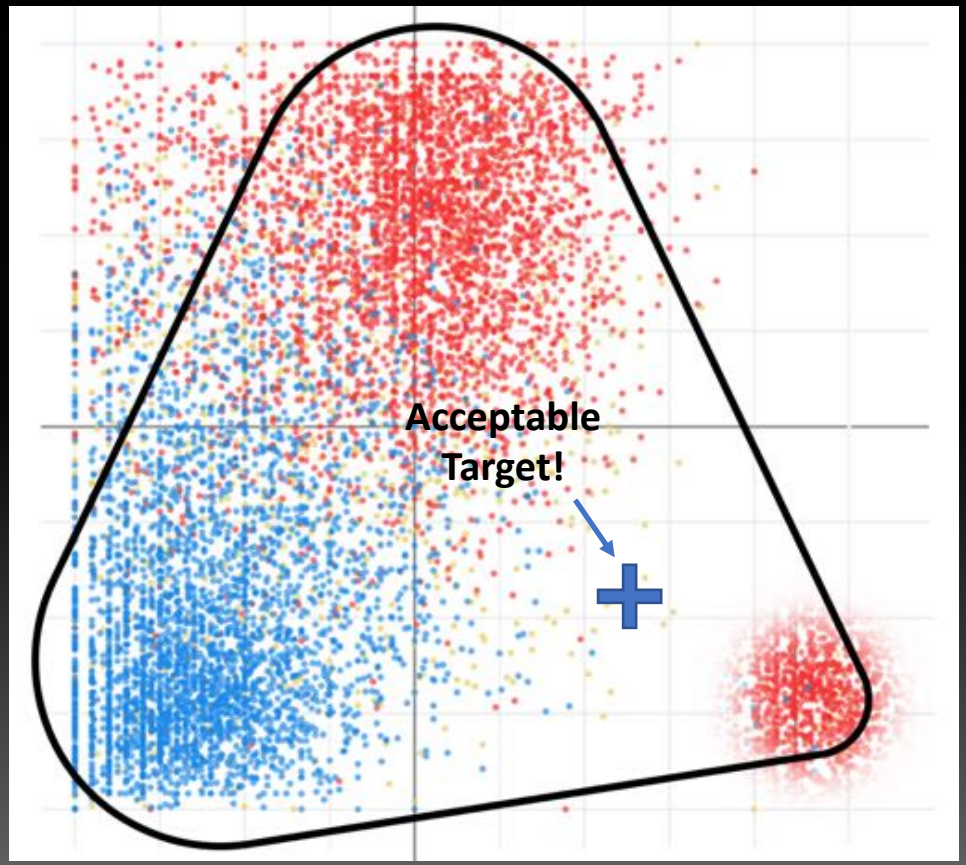
- Data science
  - High-dimensional
  - “Big Data”
- Political Economics
  - Preference Space
- Analysis and planning



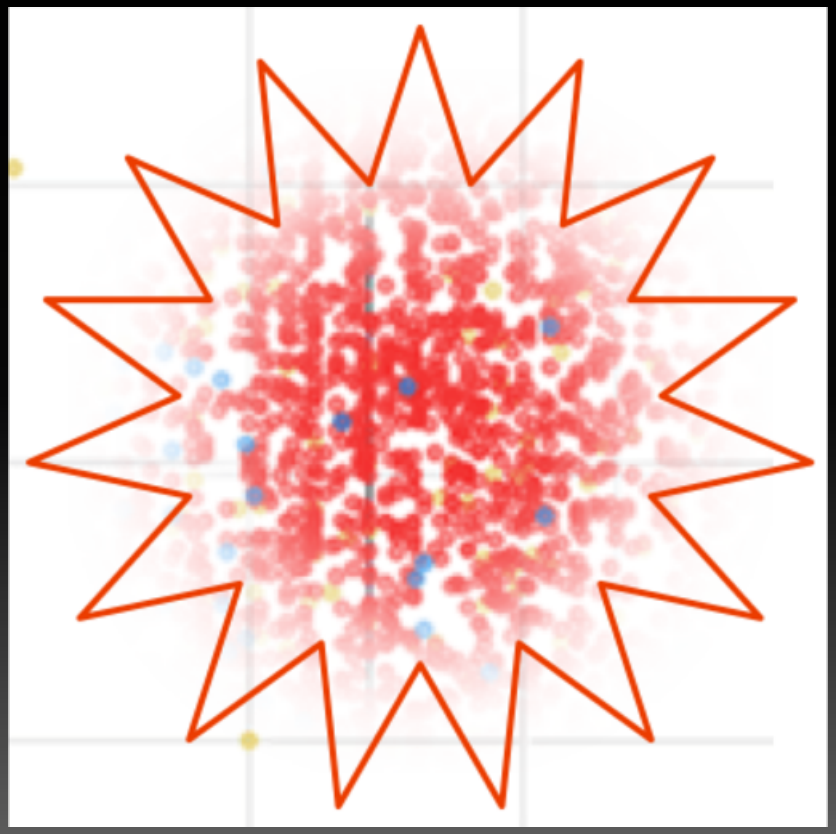
- Overton Window
  - Range of acceptable discourse
  - Left-Right spectrum
- Extend to more dimensions
  - Use with “big data”
  - Model populations



- "Door-in-the-face"
  - Sales technique
  - Start with crazy pitch
  - Real pitch seems more reasonable
- Small, vocal fringe group
  - Data science model helps target anchor message



- New Overton Window
  - Media reports crazy fringe
  - Target policy seems reasonable in comparison
- Easier than convincing the majority directly
  - Contrast “foot-in-the-door”

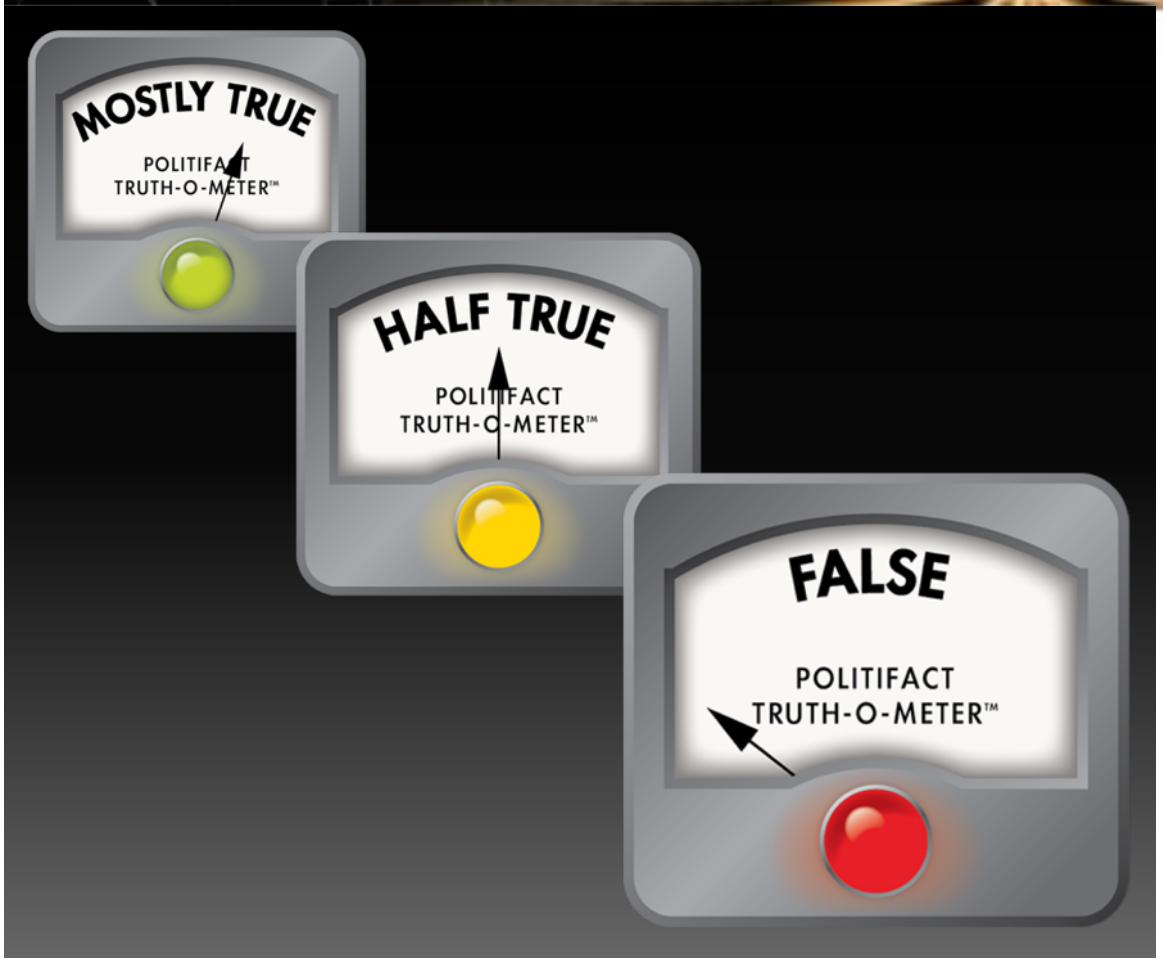


- "Ten Million Useful Idiots"
  - Soviet terminology
  - Unwitting participants in propaganda
- Gullible demographic
  - Compare to 419-scam emails

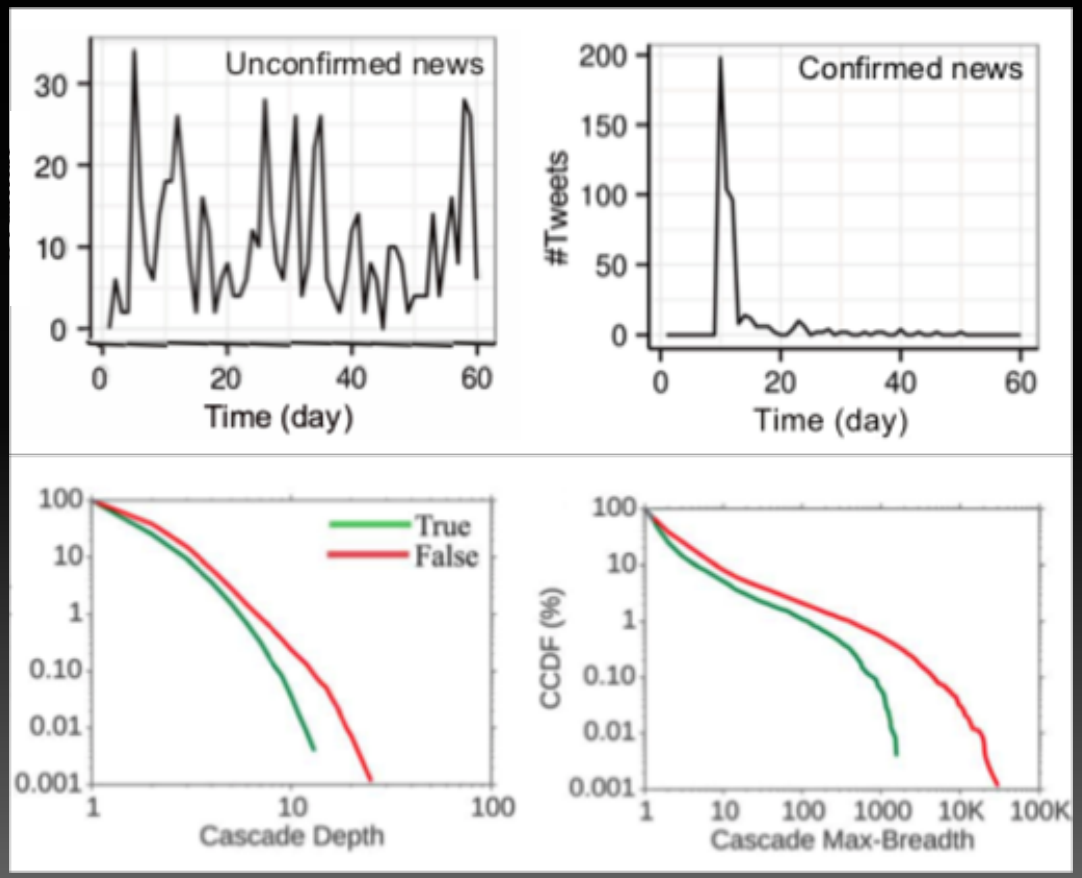
DEFENSE AND MITIGATION

The only defense against the world is a thorough knowledge of it.

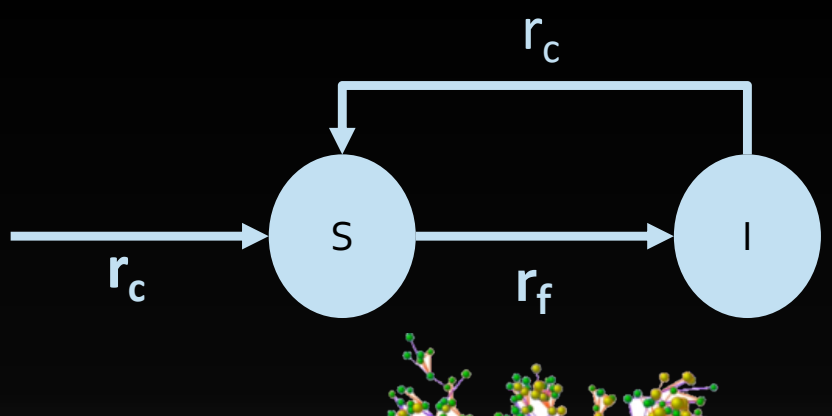
-John Locke

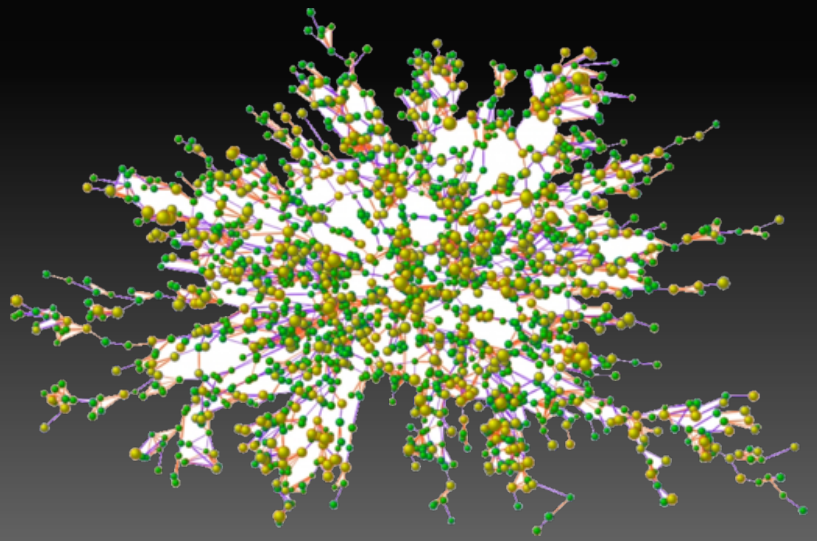


- Fact Checking
  - Manual
  - Automatic
    - Open-world
    - Closed-world
    - Can't handle satire, editorials, etc.



- Propagation-based detection
- Time-based cascades detection





- Other Models
  - Epidemic Diffusion
  - Scale-free networks

- Analysis Challenges
  - Computational power
  - Speed of propagation
  - Lack of framework
  - Emergent behaviors
  - Cognitive dissonance
  - Cognitive friction

The Washington Post

Special Edition

Democracy Awakens in Action

MAY DAY • WEDNESDAY, MAY 1, 2019 • FREE

UNPRESIDENTED

TRUMP HASTILY DEPARTS WHITE HOUSE, ENDING CRISIS

Celebrations break out worldwide as Trump era ends

Entire globe breathes sigh of relief at end of dark period

"BLAME CROOKED HILLARY & HFIOR"

Surge of protests proves too much for Trump

BY LISA CRUWG

THE CAPITAL — On May 1, barely six months after the midterm elections, Donald Trump appears to have abandoned the White House and abdicated his role as president. He issued no formal statement, though four White House aides — who spoke on the condition of anonymity — claim they found a napkin on the president's desk in the Oval Office on the evening of April 30, scrawled in

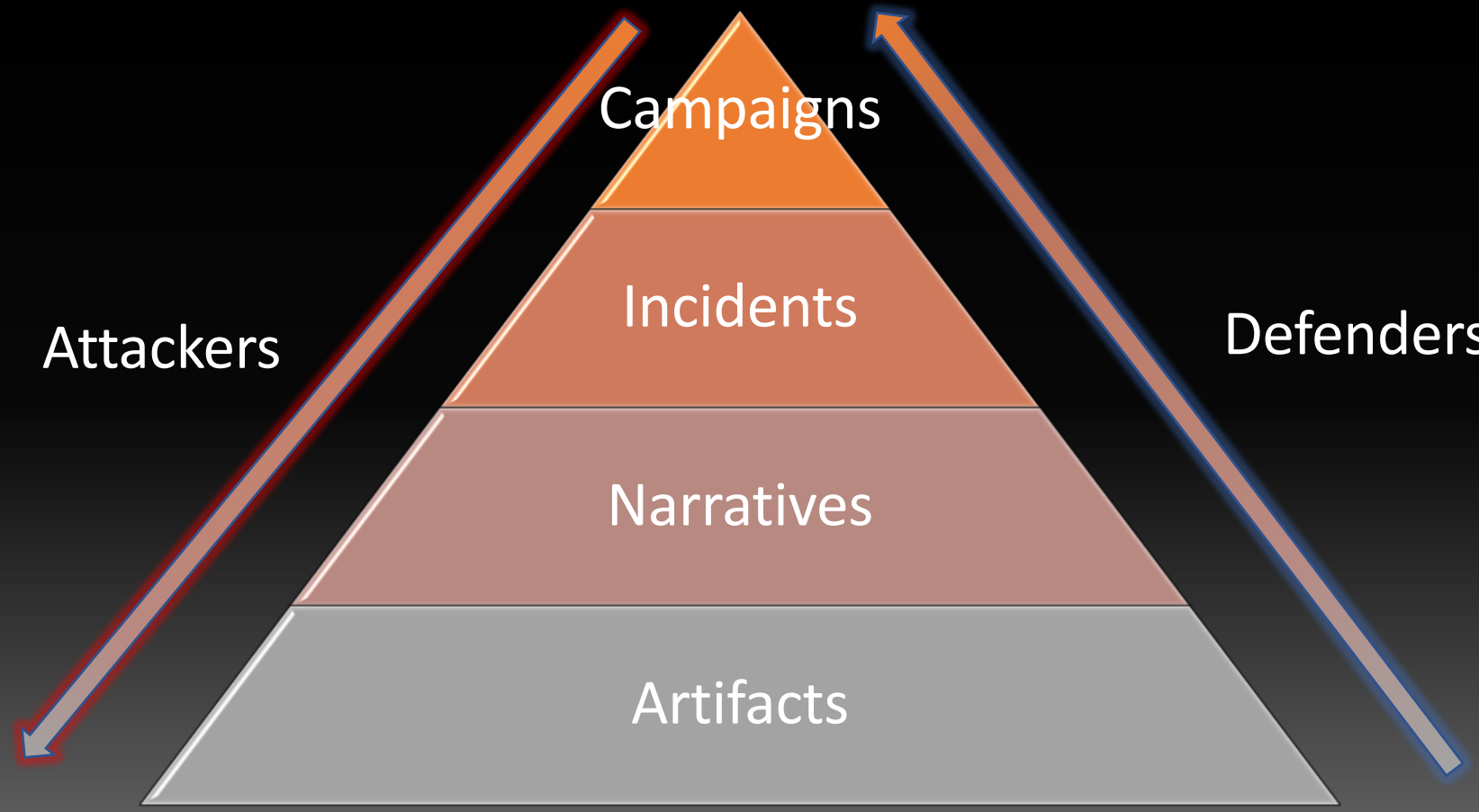
- Convincing messages
- Cognitive bias
- Lack of dissent
- Authoritative source

- Content challenges
- Deepfake Video

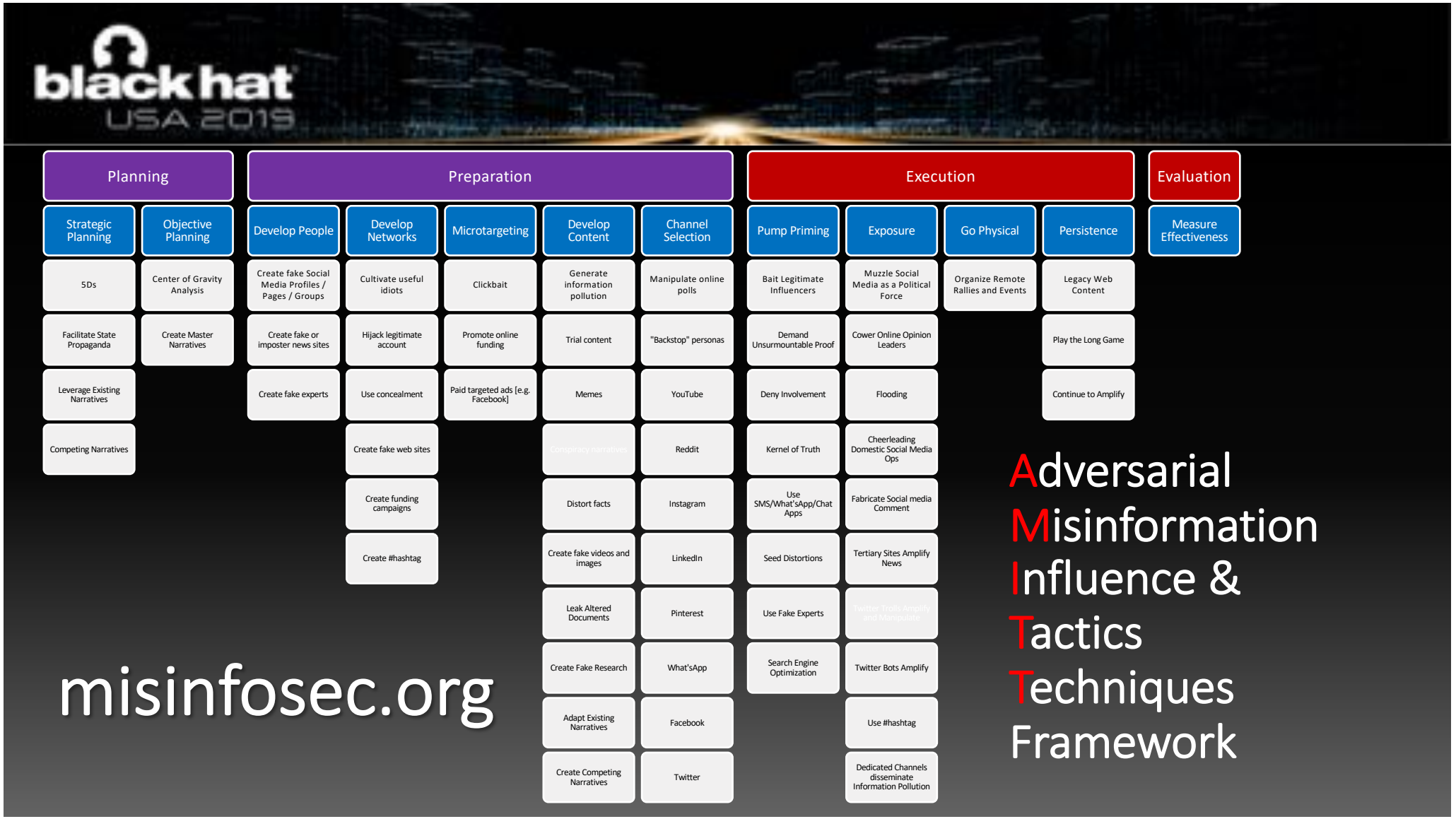
THE WAY AHEAD

Perfection is the enemy of progress.

-Winston Churchill


Campaigns
Incidents
Narratives
Artifacts
Attackers
Defenders

- Misinfosec Communities
  - Industry
  - Academic
  - Media
  - Community
  - Government
  - Infosec


black hat
USA 2019
Planning
Preparation
Execution
Evaluation
Strategic Planning
Objective Planning
Develop People
Develop Networks
Microtargeting
Develop Content
Channel Selection
Pump Priming
Exposure
Go Physical
Persistence
Measure Effectiveness
5Ds
Facilitate State Propaganda
Leverage Existing Narratives
Competing Narratives
Center of Gravity Analysis
Create Master Narratives
Create fake Social Media Profiles / Pages / Groups
Create fake or imposter news sites
Create fake experts
Cultivate useful idiots
Hijack legitimate account
Use concealment
Create fake web sites
Create funding campaigns
Create #hashtag
Clickbait
Promote online funding
Paid targeted ads [e.g. Facebook]
Generate information pollution
Trial content
Memes
Conspiracy narratives
Distort facts
Create fake videos and images
Leak Altered Documents
Create Fake Research
Adapt Existing Narratives
Create Competing Narratives
Manipulate online polls
"Backstop" personas
YouTube
Reddit
Instagram
LinkedIn
Pinterest
What'sApp
Facebook
Twitter
Bait Legitimate Influencers
Demand Unsurmountable Proof
Deny Involvement
Kernel of Truth
Use SMS/What'sApp/Chat Apps
Seed Distortions
Use Fake Experts
Search Engine Optimization
Muzzle Social Media as a Political Force
Cower Online Opinion Leaders
Flooding
Cheerleading Domestic Social Media Ops
Fabricate Social media Comment
Tertiary Sites Amplify News
Twitter Trolls Amplify and Manipulate
Twitter Bots Amplify
Use #hashtag
Dedicated Channels disseminate Information Pollution
Organize Remote Rallies and Events
Legacy Web Content
Play the Long Game
Continue to Amplify
misinfosec.org
Adversarial
Misinformation
Influence &
Tactics
Techniques
Framework

Blue Team - Red Team

- Blue Team
  - Secure by design
  - SecDevOps
  - Centralized monitoring
  - Assume a breach
- Red Team
  - Threat modeling
  - Security testing
  - Code review

SUMMARY

- Misinformation is a sociotechnical security problem
- Physical and financial consequences for businesses
- Technology cannot solve it alone
- Every new product must consider how it will be abused
- We need to share threat information across communities

PARTING THOUGHT

…You may already be the target of a nation-state's attempts to influence the economic instrument

CALLS TO ACTION

- Tell your CxO to care!
- Contribute to AMITT
- Follow @misinfosec
- Join cognitive security ISAO

References

- Kwon, Sejeong, Cha, Meeyoung, Kyomin Jung, Wei Chen, and Wang Yajun. “Prominent features of Rumor Propagation in Online Social Media.” *Microsoft Research.* 26 December 2018. <https://www.microsoft.com/en-us/research/uploads/prod/2016/06/icdm13-rumors.pdf>.
- Vosoughi, Soroush, Roy, Deb, and Aral, Sinan. “The Spread of True and False News Online.” *Science*. 09 March 2018: Vol 359, Issue 6380, pp 1146-1151. https://science.sciencemag.org/content/359/6380/1146/tab-pdf
- Boucher, Tim. "Adversarial Social Media Tactics." 10 August 2018. Medium. 26 December 2018. <https://medium.com/@timboucher/adversarial-social-media-tactics-e8e9857fede4 >.
- Bruce, Schneier. "Information Attacks Against Democracy." 21 November 2018. *Schneier on Security.* 15 January 2019. <https://www.schneier.com/blog/archives/2018/11/information_att.html?fbclid=IwAR3l6zYAWUmzdkPwWbX6Kl-mbKPRG2gS25E5sSch_5celRUHfEaNTGerIRU>.
- Nimmo, Ben. 19 May 2015. “Anatomy of an Info-War: How Russia’s Propaganda Machine Works , and How to Counter it.” StopFake.org 01 December 2018<https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/>
- Xinyi Zhou and Reza Zafarani. 2018. Fake News: A Survey of Research, Detection Methods, and Opportunities. ACM Comput. Surv. 1, 1 (December 2018), 40 pages.
- YouTube Video. “I Wish I could….” 14 June 2019. *YouTube.* 02 July 2019. <https://www.youtube.com/watch?v=3f66kBwfMto>
- Visual Capitalist. *Visual Capitalist*. 14 May 2018. 25 January 2019. <https://www.visualcapitalist.com/wp-content/uploads/2018/05/internet-minute-share2.jpg >.
- Zou, Xinyl and Zafarani, Reza. "Fake News: A Survey of Research, Detection Methods, and Opportunities." 2 December 2018. *Cornell arXiv.* Document. 20 January 2019. <https://arxiv.org/pdf/1812.00315.pdf>.

Epilogue: recommendation systems

Qanon on eBay | Seriously, We Have Qanon

Ad www.ebay.com/

★★★★½ Rating for ebay.com: 4.5 - Order accuracy: 95–100%

Free Shipping Available. Buy **Qanon** on eBay. Money Back Guarantee! Fill Your Cart With Color. Make Money When You Sell. Fast 'N Free Shipping. Huge Savings. Top Brands. World's Largest Selection. We Have Everything. Under $10. Returns Made Easy. >70% Items Are New.

Electronics · Fashion · Business & Industrial · Gift Cards · Toys · Trending on eBay