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

#Hack10M

Pablo Breuer @Ngree_H0bit
David Perlman @CoPsyCon
KEEP CALM
IT'S BUSINESS AS USUAL
Vignette 1
EU Hits Google With Record Antitrust Fine Over Android

Selected antitrust fines imposed by the European Commission against U.S. tech companies

<table>
<thead>
<tr>
<th>Company</th>
<th>Year</th>
<th>Fine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>2018</td>
<td>€4.34b</td>
</tr>
<tr>
<td>Google</td>
<td>2017</td>
<td>€2.42b</td>
</tr>
<tr>
<td>Intel</td>
<td>2009</td>
<td>€1.06b</td>
</tr>
<tr>
<td>Qualcomm</td>
<td>2018</td>
<td>€997m</td>
</tr>
<tr>
<td>Microsoft</td>
<td>2008</td>
<td>€899m</td>
</tr>
<tr>
<td>Microsoft</td>
<td>2013</td>
<td>€561m</td>
</tr>
<tr>
<td>Microsoft</td>
<td>2004</td>
<td>€497m</td>
</tr>
<tr>
<td>Microsoft</td>
<td>2006</td>
<td>€280m</td>
</tr>
<tr>
<td>Facebook</td>
<td>2017</td>
<td>€110m</td>
</tr>
</tbody>
</table>

Sources: European Commission, Press reports
• 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.
Control initial messaging
- Counter-accusation:
  - Deepfake videos
  - Social networks
  - "Expert" sources

- Amplification:
  - Mainstreaming
  - Metrics & fine-tuning
  - Bots, sockpuppets, etc.

Comprehensive follow-up
- Legal culpability:
  - Espionage suspicion
  - Grain of truth
  - Software vulnerability

- Tenacious narratives:
  - Metrics & fine-tuning
  - Salacious irrationality
  - Conspiracy communities

- Induced violence:
  - Conspiracy key events
  - Programming targets
  - Moral imperatives

Regulatory threats
- Mainstreaming
- Public outcry
- Political pandering

Goal: Preserve HW backdoor
AGENDA

- Corporate Horror Story
- Horror Reality
  - Brief history
  - Instruments of influence
  - Mechanisms of influence
  - Sociotechnical systems
  - Defense and mitigation
  - The way ahead
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
• Television
- Internet
- Social Media
War is an act of force to compel the enemy to do our will.

-Clausewitz
Instruments of national power

Diplomatic  
Informational  
Military  
Economic
Business Instruments of Influence...

- Business Deals & Strategic Partnerships
- PR & Advertising
- Mergers & Acquisitions
- R&D and Capital Investments
All warfare is based on deception.

-Sun Tzu
STRATEGIES

Distort

Distract

Divide

Dismiss

Dismay
TYPES OF ACCOUNTS

Bots
Parody
Spoof
Camouflage
Deep cover
Takeover
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
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
• Convincing messages
• Cognitive bias
• Lack of dissent
• Authoritative source
• Content challenges
• Deepfake Video
Perfection is the enemy of progress.
-Winston Churchill
TYPES OF ACCOUNTS

- Campaigns
- Incidents
- Narratives
- Artifacts

Attackers

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

Strategic Planning
- SDs

Facilitate State Propaganda
- Center of Gravity Analysis

Leverage Existing Narratives
- Create Master Narratives

Competing Narratives
- Create fake Social Media Profiles / Pages / Groups

Preparation

Develop People
- Create fake or imposter news sites

Develop Networks
- Hijack legitimate account

Microtargeting
- Promote online funding

Develop Content
- Trial content
- "Backstop" personas

Channel Selection
- Paid targeted ads [e.g., Facebook]

Generate information pollution
- Memes

Manipulate online polls
- YouTube

Execution

Pump Priming
- "Bait Legitimate Influencers"

Exposure
- "Muzzle Social Media as a Political Force"

Go Physical
- Organize Remote Rallies and Events

Persistence
- Legacy Web Content

Evaluation

Measure Effectiveness

Adversarial Misinformation Influence & Tactics Techniques Framework

misinfosec.org
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
...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

misinfosec.org
References


Epilogue: recommendation systems

Qanon on eBay | Seriously, We Have Qanon
[Ad] www.ebay.com/ ▼
★★★★★ Rating for ebay.com: 4.5 - Order accuracy: 95–100%
Electronics · Fashion · Business & Industrial · Gift Cards · Toys · Trending on eBay