NINTH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

The Weaponization of Social Media

Mary Frantz, EKP LLC

October 28–30, 2019 | Minneapolis Convention Center

cybersecuritysummit.org | #cybersummitmn

I can make anybody pretty
I can make you believe any lie
I can make you pick a fight
With somebody twice
Your size
Well I've been known to cause a few breakups
And I've been known to cause a few births
I can make you new friends
Or get you fired from work.

~ Brad Paisley
or
the results of a retweeted Sock Puppet??

Mary Frantz

Enterprise Knowledge Partners, LLC
(952) 496-2460
maryf@ekpartner.com

ENTERPRISE KNOWLEDGE PARTNERS, LLC

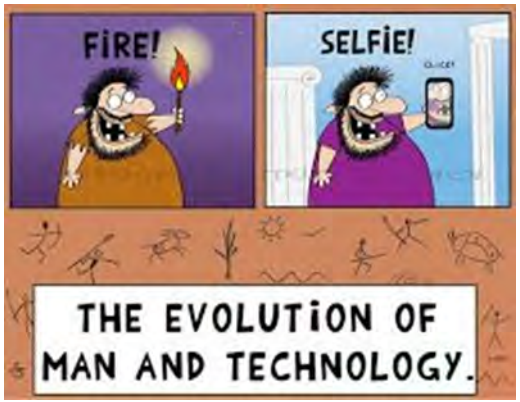
Because what you don't know, *can* hurt you

Weaponization of Social Media

- Use of social media as a means of attack is in multiple stages of the cyber kill chain
  - Reconnaissance
  - Weaponize
  - Delivery mechanism
  - Exploitation
  - Command and Control
- Motivation
- Desired Outcome
- Persistence

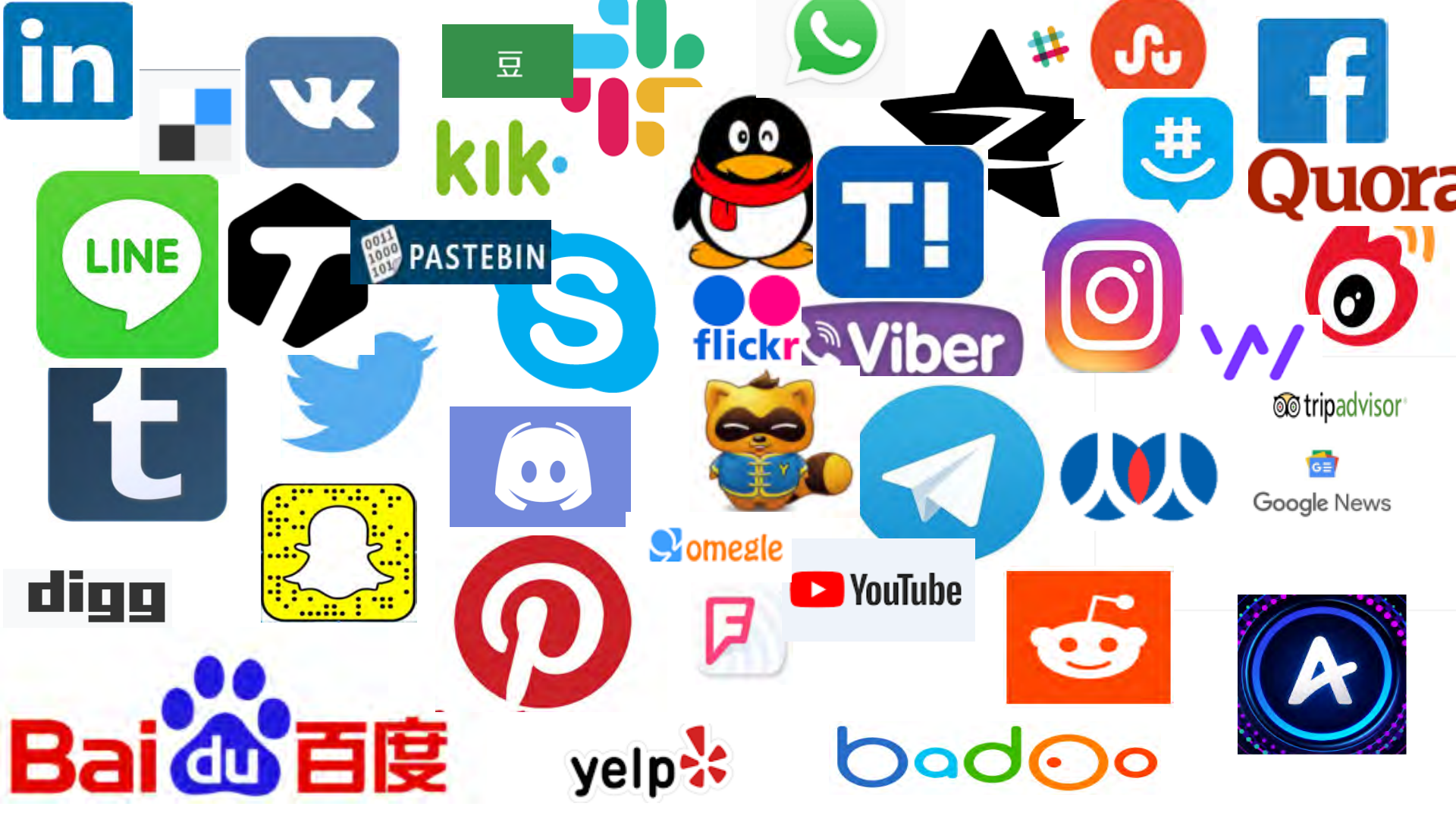
The information war is as old as war itself

- Propaganda – pre-Roman times to present (and future)
- Morse code (Samuel Morse, 1838)
- Telegraph (Morse, 1858)
  - Hacking
  - Yellow Journalism
- Telephone (1876, Bell & Watson)
  - Long distance/over ocean – 1927
  - Degrees of Separation – 1929
- Television
- Internet –clear, deep and dark



The information "war" is constantly evolving

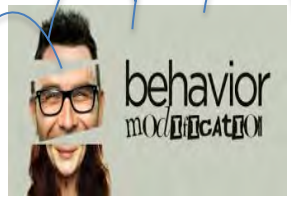
- Engagement and attention is power
- Speed - virality
- Authenticity and/or shock value
- Anonymity
- Social default – into mainstream news, bury legitimate news


豆
kik
PASTEBIN
LINE
flickr
Viber
Quora
tripadvisor
Google News
omegle
YouTube
digg
Baidu 百度
yelp
badoo

scrape/steal/sell

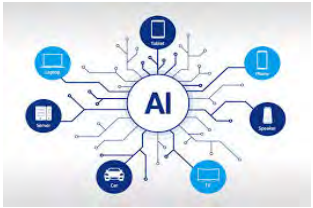
IoTSM - apps

Subscriptions	*Demographic data*	*Time Spent/Stickiness*	*Surveys*
Comments	*Likes*	*Clicks*	*Public Records*
Text Messages	*Emails*	*Shares*	*Census*
Photos	*Videos*	*Contact Info/Phone*	*Searches*
Location	*Biometrics*	*Purchases*	*Language*
Payment Card Stats	*Demographic data*	*Relationships status*	*Relatives*
Tokens/cookies	*Chats*	*App Links*	*Device and IP*
Age	*Gender*	*Sexual preference*	*Work history*



BIG DATA

Algorithms

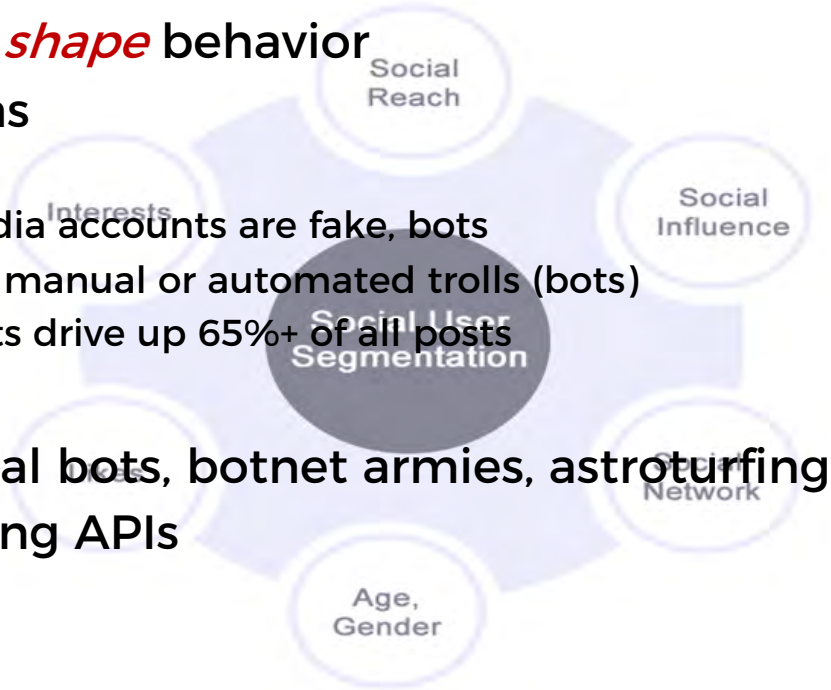


Deep Learning

Data informed content creation

Methods

- Addiction, then measure and *shape* behavior
- Trolls and fake online personas
  - Create discord, controversy
  - Up to 15% of all online social media accounts are fake, bots
  - Up to 28% of online personas are manual or automated trolls (bots)
  - Fake accounts, paid personas, bots drive up 65%+ of all posts
- Click farms
- Automated bots/botnets, social bots, botnet armies, astroturfing
- Information Delivery – Ads using APIs
- Stolen data
- Data laundering

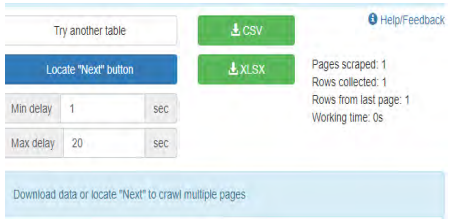


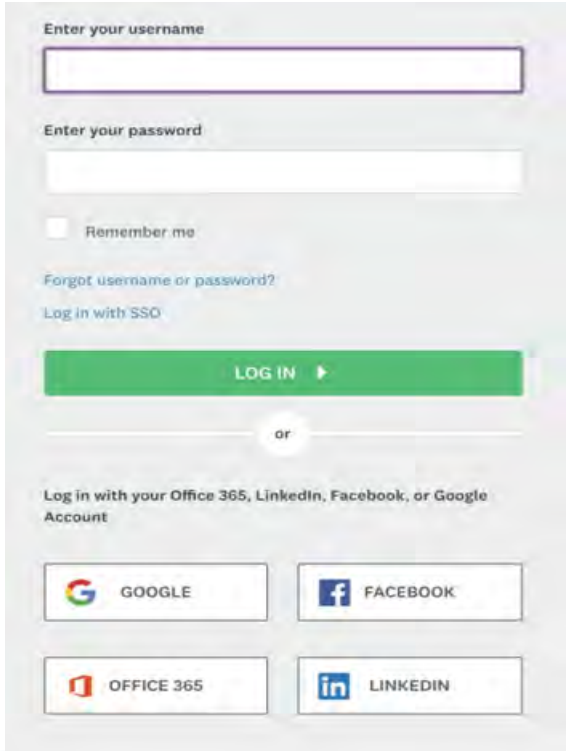
Social media botnets

- Social bots
  - Engage or like troll content
  - Sock Puppets
- Click farms
- Automated bots, bot armies, astroturfing bots
- (mis)Information delivery automation
- Malware
- Darknet stolen data (data laundering)

Ads, APIs, Apps, OAuth, oh my…

- Both parties receive consumer information/profile data
- Enables stickiness
- Integrate friends/contacts
- Easily scrape likes, clicks, shares, retweets, copies, etc.
- APIs allow targeting by user, profile type, etc.





How to Weaponize Behavior

1. Obtain user profile data (gather, buy, or create a fake)
2. Email account, burner phone, proxy, vpn
3. Scrape a site - or create a developer account - or steal
   - DOM manipulation, scraper API, headless chrome/puppeteer, SET, BurpPro, Octoparse, third party and SM APIs, self infect

   - OR create an developer account for an app, ad, etc.;

   - use built-in targeting
1. Spread
   - Virality
   - Seek-and-Infect
2. Learn and adapt

Minimal computing power
Minimal network noise
Hide source

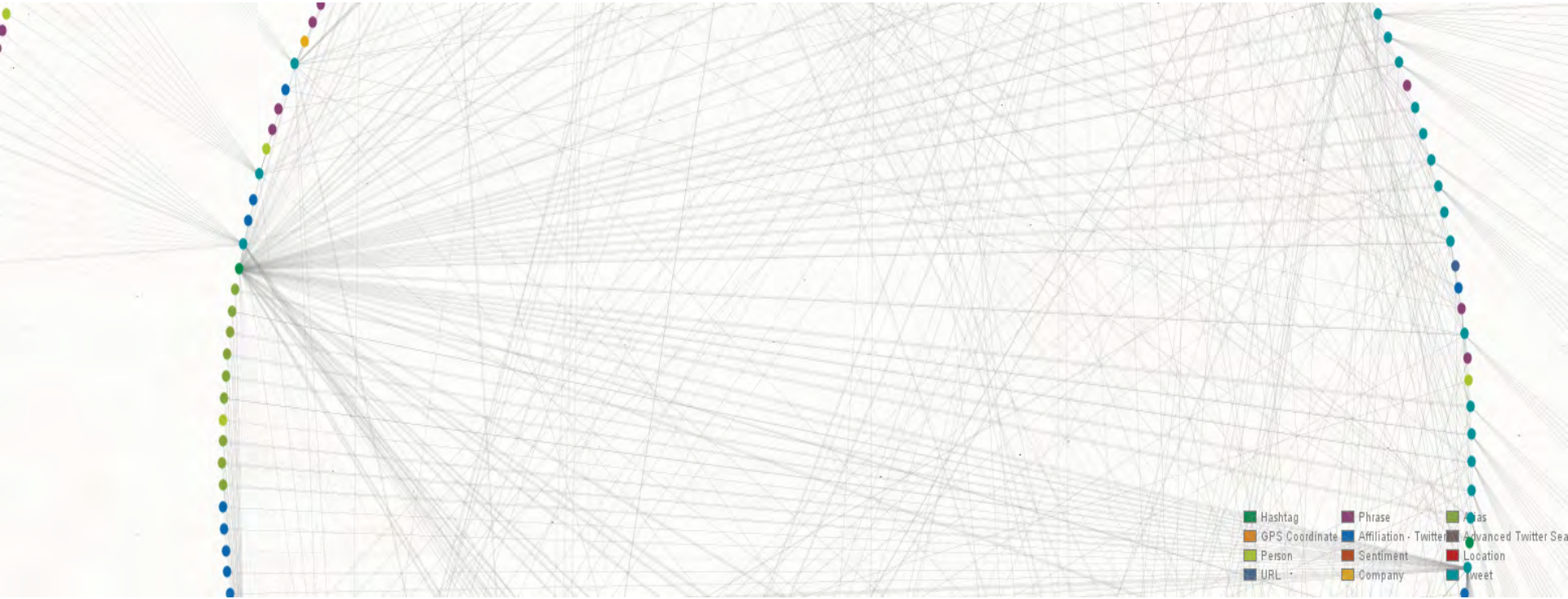
Ad Fraud - by hashtag

1. Buy or rent a botnet (easy) or ….
2. Register for developer account on social media site
   - Phone/text number, email account
3. Create an app, set access level
4. Get the API, access token and secret key
5. Create a post, add an array of userids, hashtags or use infected devices
6. For every click
   - ✓ Money (clicks)
   - ✓ Vote (change polling stats)
   - ✓ Auto add followers / following

Minimal computing power
Minimal network noise
Hide source

MethBot – Ad Fraud

- Created 6,000+ domains
- 250,267 distinct URLs
  - big-name publishers, from ESPN to Vogue
  - Only hosted a video ads
  - Used 100K+ IP addresses large regional internet registries
  - Hosted on major US internet providers
- Tricked automated algorithms to bid on ad space in pay per click
- Created a bot farm to watch video ads (up to 570K bots) @ $13.04 per thousand video views
- $3M - $5M per day



10/28/2019 – followed tweet from @cs_summit (Women in Cyber Lunch)

Twitter Bots

Enter your Twitter Apps Keys:

Consumer Key	xKcO1xkLSiaLAx1x1G1yCDEF7	Consumer Secret	nFGefOdJkM8YGMBEbobW0MGjU
Access Token	26723204-xwX25YRCzX4uqJ2iVJ9:	Access Secret	pQ3mAaeV7g9J4dSj1Y2LP366Gmj

What will your Twitter bots do?

Bot #1	Search phrase	Select Action	Text	Start at	End at
Bot #2	Search phrase	Select Action	Text	Start at	End at
Bot #3	Search phrase	Select Action	Text	Start at	End at
Bot #4	Search phrase	Select Action	Text	Start at	End at
Bot #5	Search phrase	Select Action	Text	Start at	End at

Create Twitter Bots

Show Logs

STOP

Automated Trolls, Bots

1. 82% of users said they'd consider trying a new product if someone in their social network recommended it
2. 65% of users said they might change their mind on who to vote for if their friend base was supporting another candidate
3. 72% of users will respond to surveys if their friends do
4. Over 80% of users have connected to a bot, troll or a other false persona
5. Over 90% of those under the age of 25 clicked on a sock puppet
6. 30% face online personas in popular gaming apps and services

Mary Frantz

Enterprise Knowledge Partners, LLC
(952) 496-2460
maryf@ekpartner.com

ENTERPRISE KNOWLEDGE PARTNERS, LLC

Because what you don't know, *can* hurt you