



Influencing Meat Puppets Through Memes

Simon Howard
BSides Wellington
Friday 24th November 2017

Background



Presentation Overview

- NZ Election
- US Election
- Creating your own troll army
- Countermeasures

Election

- We had an election recently
- Most of the advertising was done via:
 - A piece of coloured card in you mail box
 - A terrestrial television advertisement
 - Newspaper
 - Billboards
 - Social media?
 - What's "direct marketing"

#AskJacinda



Jacinda Ardern

Auckland Central



Vote positive. Party vote  **Labour**
labour.org.nz

Authorised by Teo Barnett, 160 Willis St, Wellington

© New Zealand Herald

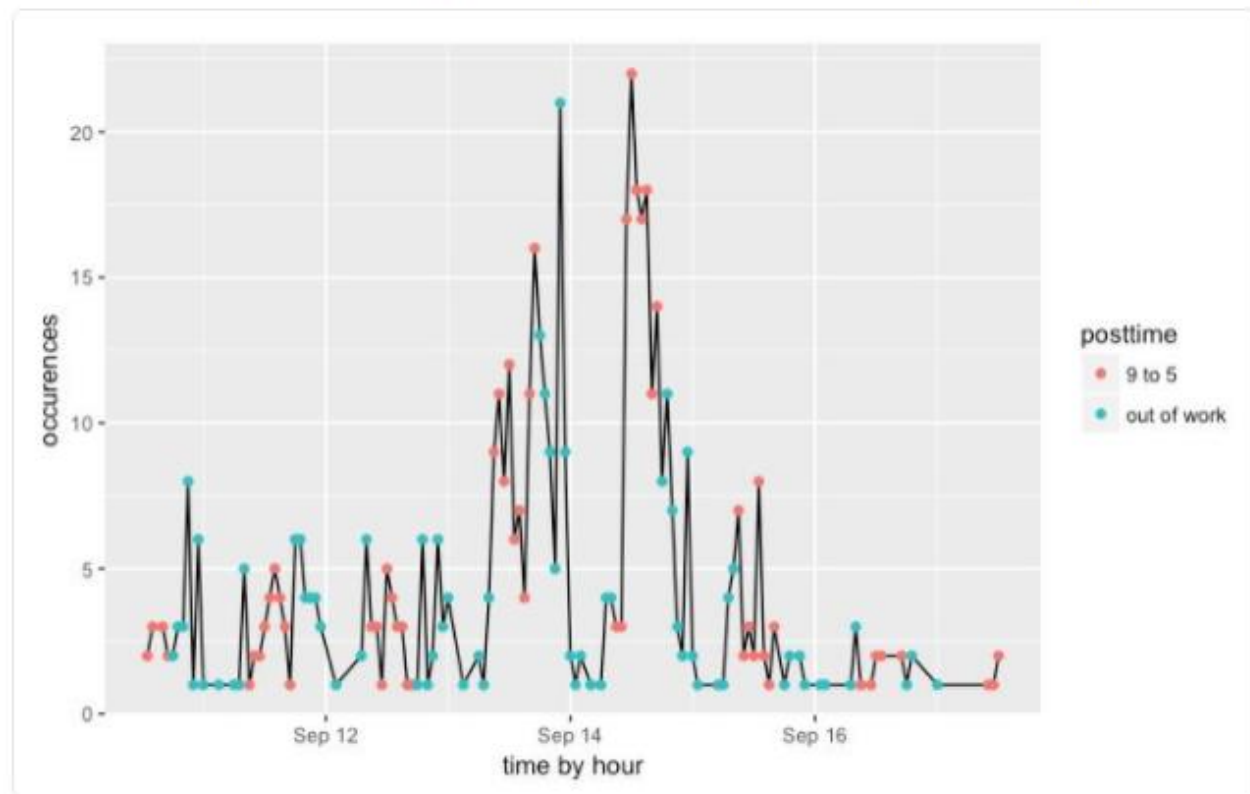
Social Media Impact

- Stuff.co.nz comments increased in volume for politically aligned articles
- A number of adverts appeared on Facebook – nothing untoward



David Hood @Thoughtfulnz · Sep 21

There was an unusual number of Twitter accounts using the phrase "tax" during business hours on Sep 13 and 14. Any PR people want to own up?



1



1



3

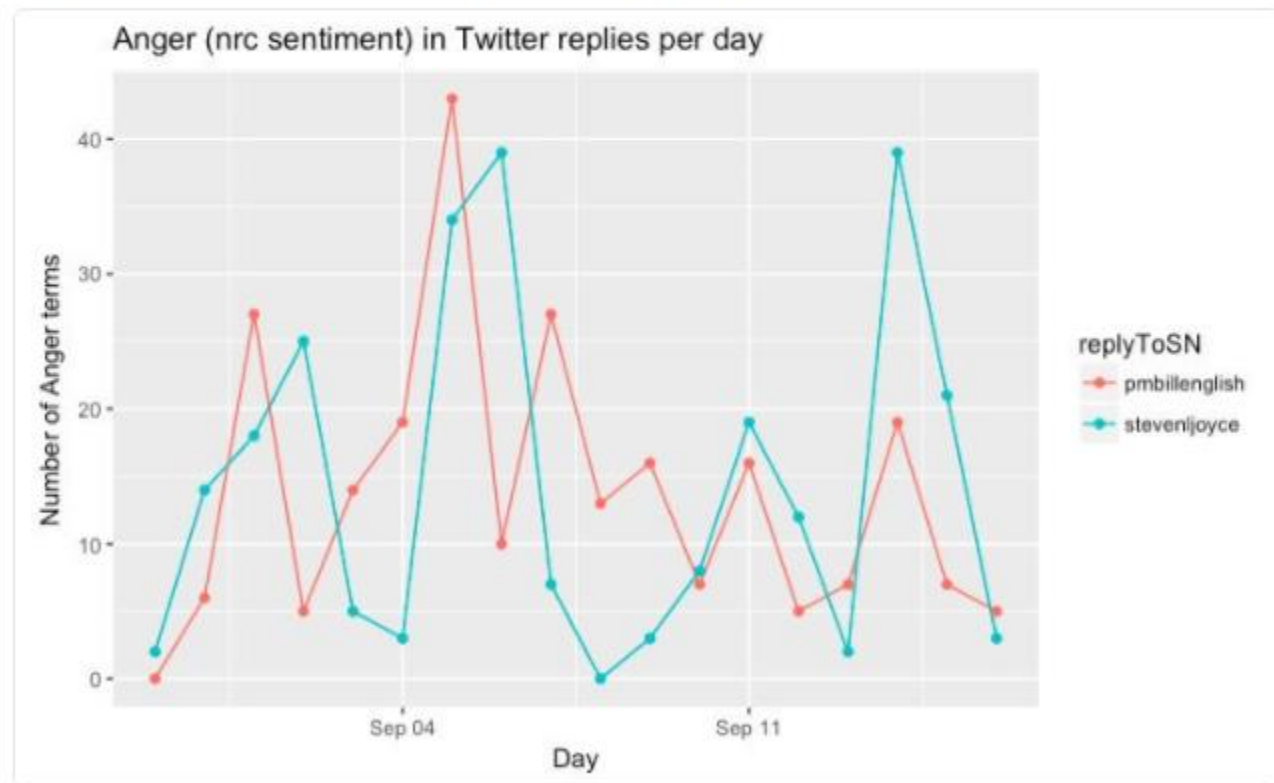




David Hood @Thoughtfulnz · Sep 17

Nerdrage quantified.

Anger directed at Steve Joyce and Bill English by day





David Hood @Thoughtfulnz · Sep 17



Replies to self as percentage of replies received by NZ political twitter accounts

Party <chr>	percent <dbl>	replies <int>	monitored_accounts <int>
United Future Party	0.47	215	2
Labour Party	0.59	3735	31
National Party	1.64	7364	39
Green Party	2.04	1910	13
ACT Party	2.15	885	3
Māori Party	2.61	575	3
NZ First Party	19.78	1158	7





David Hood @Thoughtfulnz · Sep 10

Very Preliminary, but might interest media, of the URLs in Twitter replies to NZ Pols I have processed (1481), that not to Twitter (156):

```
# A tibble: 61 x 4
  domain occurrences prop
  <chr>          <int> <dbl>
1 www.nzherald.co.nz      18 0.11538462
2 www.newshub.co.nz       17 0.10897436
3 www.youtube.com         16 0.10256410
4 www.radionz.co.nz       14 0.08974359
5 www.stuff.co.nz         11 0.07051282
6 i.stuff.co.nz           5 0.03205128
7 www.newsroom.co.nz      5 0.03205128
8 www.labour.org.nz       4 0.02564103
9 www.tvnz.co.nz          4 0.02564103
10 www.facebook.com        3 0.01923077
# ... with 51 more rows
```



1



1



In the US however

- Political advertising is a big thing
- Trump was mocked for not spending money on traditional TV ads (Hilary spent \$140mil).
- When "Trump TV" went live on Facebook, before and after the second debate, it raked in \$9 million in donations in 120 mins

Multi-pronged attack

- What we didn't realise at the time
- Trumps "team" was launching a multi-pronged attack
- A Blitzkrieg of sorts, breaking through the opponents line of defence
 - Short
 - Fast
 - Powerful
 - Dislocating the opposition, using speed and surprise to encircle them



VICELAND



HOW TO MAKE AMERICA



GREAT AGAIN
LIKE IF YOU AGREE



Screen Shot
2017-09-07 at
11.18.03 PM



Screen Shot
2017-09-07 at
11.18.42 PM



Screen Shot
2017-09-07 at
11.18.51 PM



Screen Shot
2017-09-07 at
11.19.14 PM



Screen Shot
2017-09-07 at
11.19.44 PM



Screen Shot
2017-09-07 at
11.21.21 PM



Screen Shot
2017-09-07 at
11.21.58 PM



Screen Shot
2017-09-07 at
11.22.43 PM



Screen Shot
2017-09-07 at
11.23.06 PM



Screen Shot
2017-09-07 at
11.23.21 PM



Screen Shot
2017-09-07 at
11.23.45 PM



Screen Shot
2017-09-07 at
11.24.03 PM



Screen Shot
2017-09-07 at
11.24.40 PM



Screen Shot
2017-09-07 at
11.25.11 PM



Screen Shot
2017-09-07 at
11.25.27 PM



Screen Shot
2017-09-07 at
11.25.42 PM



Screen Shot
2017-09-07 at
11.26.04 PM



Screen Shot
2017-09-07 at
11.26.20 PM



Screen Shot
2017-09-07 at
11.26.44 PM



Screen Shot
2017-09-07 at
11.27.11 PM



Screen Shot
2017-09-07 at
11.27.32 PM



Screen Shot
2017-09-07 at
11.27.55 PM



Screen Shot
2017-09-07 at
11.28.23 PM



Screen Shot
2017-09-07 at
11.28.45 PM



Screen Shot
2017-09-07 at
11.29.01 PM



Screen Shot
2017-09-07 at
11.29.18 PM



Screen Shot
2017-09-07 at
11.29.37 PM



Screen Shot
2017-09-07 at
11.29.56 PM



Screen Shot
2017-09-07 at
11.30.19 PM



Conspirador Norteño @conspir... · 1d ✓

Replying to [@conspirator0](#)

I searched through two recent datasets (propagators of [#FireMcMaster](#) and [#UniteTheRight](#) hashtags) and found 824 such accounts.



9



219



526





Conspirador Norteño @conspir... · 1d ▾

Searching their followers for similarly named accounts, and subsequently their followers' followers yielded 63099 accounts.

Marcus43751953	Maree71439592	Margare79641415
Marcus48216197	Marek43964167	Margare81639906
Marcus56156730	Marek96308039	Margare82503075
Marcus75809145	Maretta75339511	Margare86907051
MarcusA29588235	Marfan24708709	Margare87591469
MarcusA34629699	Marfo64557407	Margare90216013
MarcusA85394030	Margare00567021	Margare91112141
MarcusC22973194	Margare02122428	Margare94057847
MarcusH21186899	Margare03456100	Margare98070980
MarcusH71372471	Margare04323327	Margare98093014
MarcusJ05688311	Margare04973003	Margare98201545
MarcusJ33281449	Margare10184002	Margari00660072
MarcusJ37837973	Margare17266614	Margari06490855
MarcusJ80933550	Margare18140247	Margari16819759
MarcusJ81336519	Margare32712111	Margari28573338
MarcusS68779250	Margare35028932	Margari37295376
MarcusT85815320	Margare35031884	Margari53108294



19



293



691





Conspirador Norteño

@conspirator0



Let's look at the largest node in the network, DavidJo52951945. This account's been around for a while - since early 2013, 136K tweets.

David Jones
@DavidJo52951945
UK government have abandoned Brits. We need to exit EU, ECHR, stop all immigration + look after British people. Like UKIP. All my views. I follow back
© Southampton/ Isle of Wight
📅 Joined January 2013
[Tweet to David Jones](#)

Tweets 136K Following 95.5K Followers 102K Likes 13.5K

Tweets Tweets & replies Media

David Jones @DavidJo52951945 · 7h
RT Broken Britain-where Brits are treated like 2nd class citizens with crumbling public services & immigrants/refugees get everything free

**HOUSING, FREE MONEY,
FREE BENEFITS, FREE
SCHOOLS, FREE NHS, FREE
TRANSLATORS, FREE**

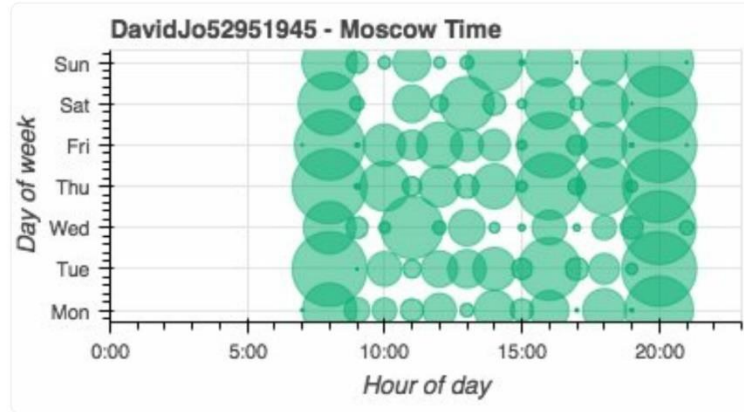
8:55 PM · 22 Aug 17



Conspirador Norteño
@conspirator0

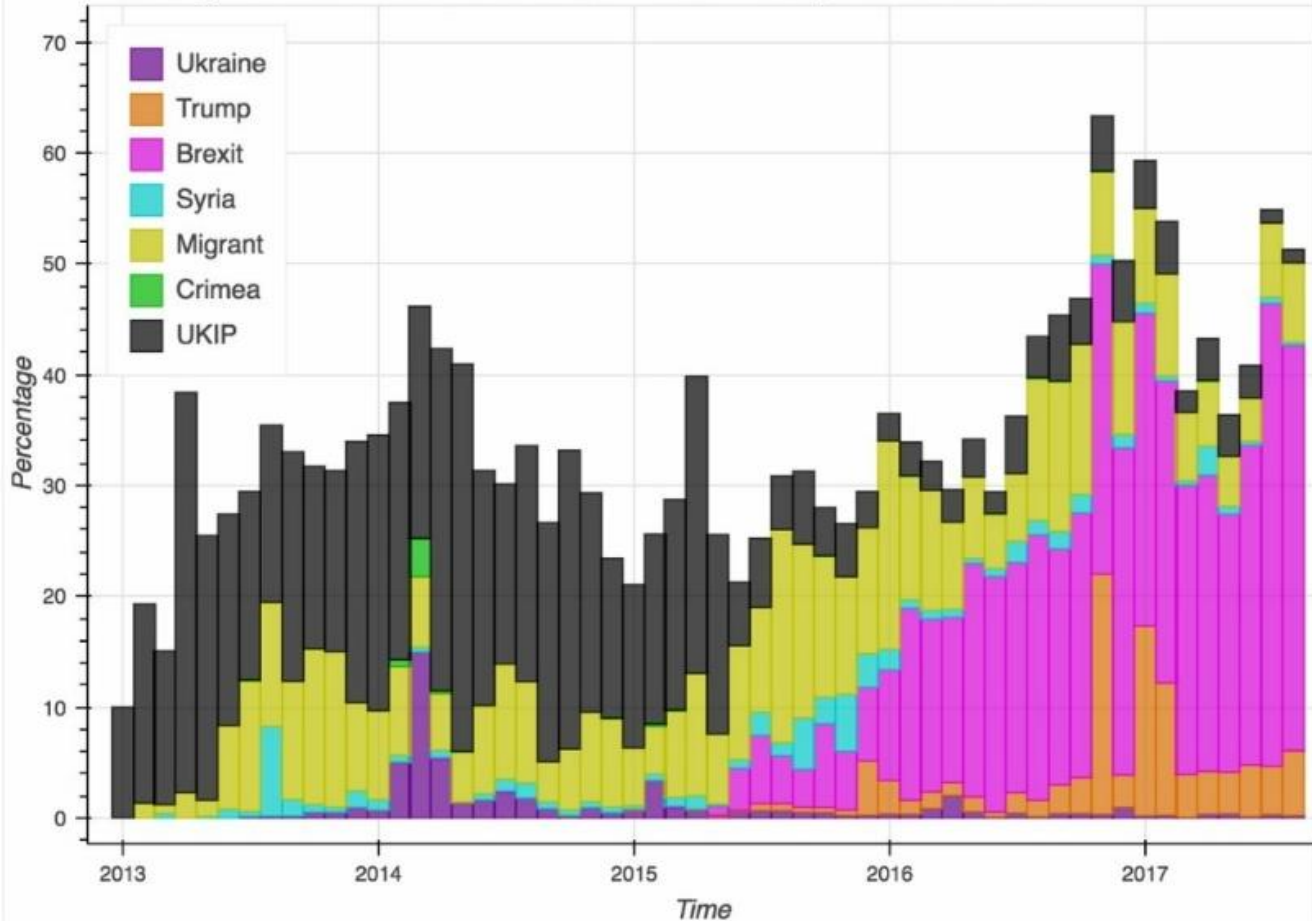


Here's an interesting observation
- David is posting 8 AM - 8 PM
every day, Moscow time. Almost
like it's his job or something.



8:56 PM · 22 Aug 17

Percentage of @DavidJo52951945 tweet volume containing terms of interest





The Troll Factory - Statistics

- Total US operational expenses: \$2.3mil
- Staff working on US Campaign: ~90
- Total Subscribers: 50 million +
- Page views per week: 100 million +
- Advertising budget: ~400k
 - Facebook: \$100,000
 - Twitter: \$274,000
 - Google Ads: \$4,700
 - Reddit Gold?

It's like a goddamn comedy sketch. A Russian troll sitting at his computer, "hmm, what would an American drink? Coca-cola of course! Let's give him a 6 pack, nice and overindulgent"

bratwurstbaby - /r/worldnews

It got me thinking

- What does it take to run something like this?
 - Start with a good lead-time
 - The Russians started a year and a half out from the campaign
 - Create a team
 - Creation of sock puppets
 - Tailoring of message
 - Delivery
 - Monitoring

- Can't be that hard eh?

Creating a team

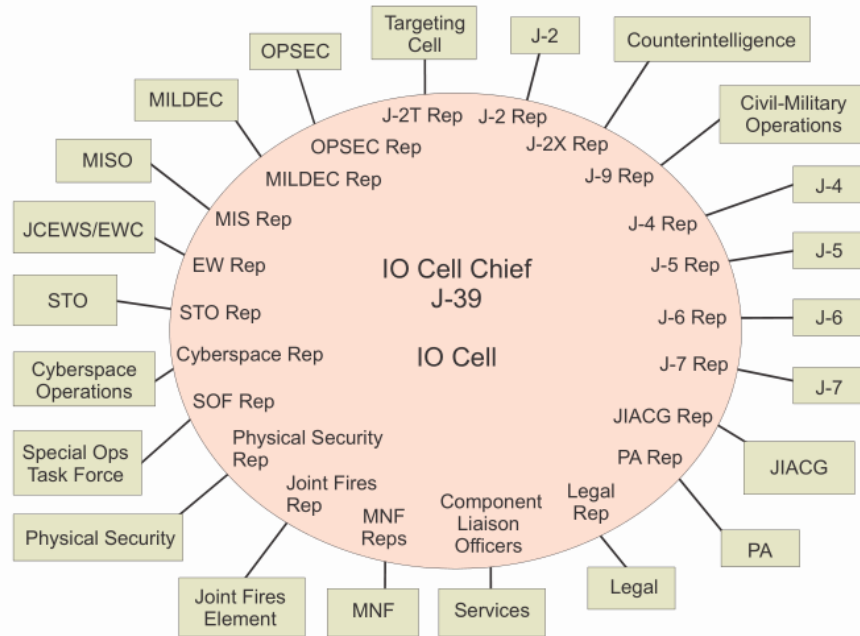
- Linguists
- Psychologists
- Designers / Artists / Cartoonists
- DevOps
- Machine Learning / Artificial Intelligence
- Hackers

JP13 – Information Operations

- This publication provides joint doctrine for the **planning, preparation, execution, and assessment** of information operations across the range of military operations



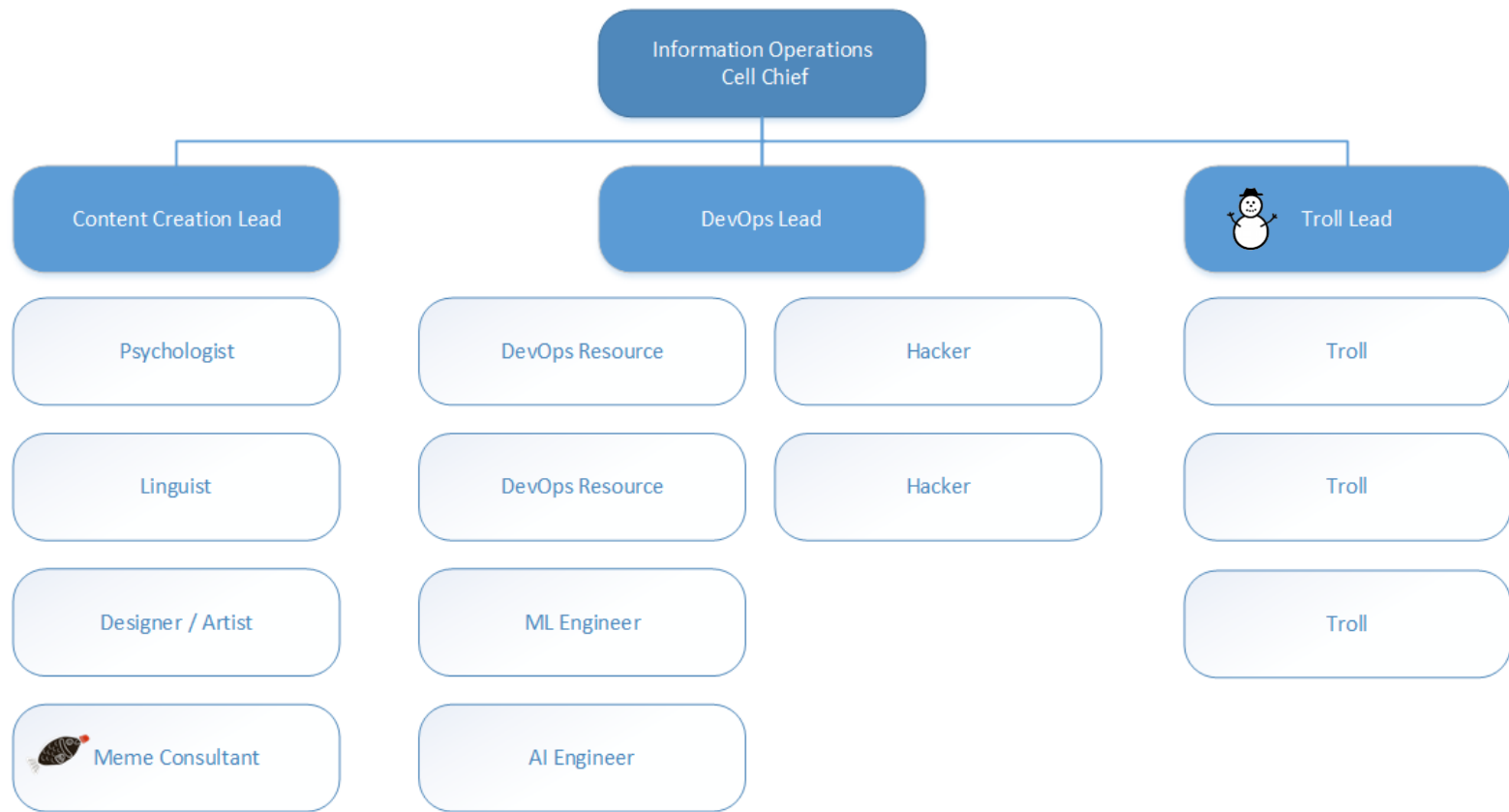
Notional Information Operations Cell



Legend

EW	electronic warfare	JCEWS	joint force commander's electronic warfare staff
EWC	electronic warfare cell	JIACG	joint interagency coordination group
IO	information operations	MILDEC	military deception
J-2	intelligence directorate of a joint staff	MIS	military information support
J-2T	deputy directorate for targeting	MISO	military information support operations
J-2X	joint force counterintelligence and human intelligence staff element	MNF	multinational force
J-39	information operations staff	Ops	operations
J-4	logistics directorate of a joint staff	OPSEC	operations security
J-5	plans directorate of a joint staff	PA	public affairs
J-6	communications system directorate of a joint staff	Rep	representative
J-7	force development directorate of a joint staff	SOF	special operations forces
J-9	civil-military operations directorate of a joint staff	STO	special technical operations

Figure II-3. Notional Information Operations Cell





CHAOS CITY

SOUTH PARK
ALL NEW NEXT WED 10PM



Outsourcing

- Build the team from contractors (\$10-20 USD per hour)
- Conduct online interviews
- Pay everyone in Bitcoin
 - xbtfreelancer.com
 - cryptogrind.com

"Position: Internet operator (night)"

The salary of 40-50 thousand rubles with the schedule of work (from 21:00 to 09:00) in the office in the Primorsky district. Job duties include writing "on the given topic", "news information and analytical". Employee skills required are "free English", including "confident possession" of written language, and creativity.

SuperJob.ru advert for Internet Research Agency



Sock Puppet Accounts - Creation

- OPSEC countermeasures
 - Fakenamgenerator.com
 - School / Education
 - Workplace
 - Address
 - Birthdate (that isn't 1/1/xx or 31/12/xx)
 - Backstop some family members too
 - Depends on how deep your cover will be investigated
 - Consider the purpose for which your profile photograph is being used and the source of the photograph.
 - Remember to flip that profile pic



Sock Puppet Accounts - Creation

- OPSEC countermeasures
 - Proxy
 - Burner phones for 2FA
 - You can use Twilio
 - Doesn't support SMS to NZ numbers
 - Why not create your own SMS service?
- Base accounts
 - Outlook (feeder account)
 - Facebook
 - Twitter
 - etc

Sock Puppet Accounts – 2FA

- USB GSM Modem (E1552) \$4.5 ea
- SIM Card ~\$.50 cents
 - No identification required in NZ to purchase one
- Powered USB Hub (mbeat USB-M13HUB 3A) ~\$30-40
- Bonus: Can be used to spam your friends

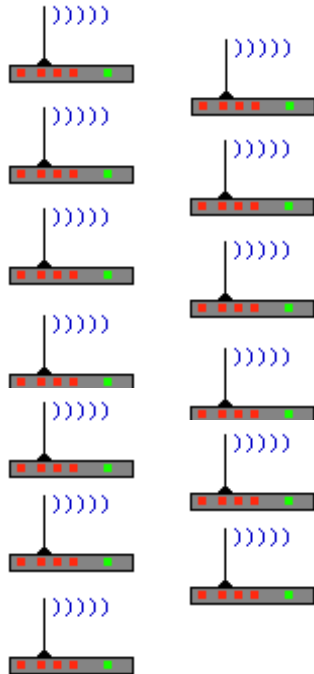


SMS Server Tools 3

Incoming Folder



GSM Modems



Sock Puppet Accounts - Creation

- Creating lots of accounts?
 - Use the mobile version of the site
 - Selenium/greasemonkey for automation
 - Steal existing accounts from dumps
 - Prone to being shutdown though

Sock Puppet Accounts – Management

- Managing lots of social media accounts is a PITA
- There are some tools you can use however
 - Hootsuite
 - Buffer
- These companies are probably compliant with law enforcement requests

Sock Puppet Accounts – Management

MonsterSocial

- Bot management platform
 - Facebook
 - Instagram
 - Pinterest
 - Tumblr
 - Twitter

Sock Puppet Accounts – Management

- When your Facebook activity looks dodgy you will get challenged
 - Account will be locked
 - Asked to send a recent pic
 - This is when you send the original (un-flipped) pic
- Using 2FA will also provide validity to your profile

You can't log in at the moment

We'll get in touch with you shortly after we've reviewed it. You'll now be logged out of Facebook as a security precaution.

Security check

A code was sent to [REDACTED]. Please enter the code here when it has arrived.

Confirmation code [Submit](#) [Send code again](#)

[I'm having trouble with this step](#)

[Continue](#)

How does the Troll Factory deal with it?

- When Facebook blocks accounts of trolls, the IT department of the organisation buys a proxy server, issues new IP-addresses, virtual "OSes", and the work begins anew
- Also new SIM cards or cloud numbers are purchased, new payment accounts are opened.

Sock Puppet Accounts – Tailoring of Profiles

- Match your profiles to personality types, someone who will resonate with their “new friends”
- OCEAN personality test
 - Based on what you like & post

O	Openness to Experience	Low	←————→	High
			<i>Imaginative</i> <i>Conventional</i>	
C	Conscientiousness	Low	←————→	High
			<i>Organised</i> <i>Spontaneous</i>	
E	Extraversion	Low	←————→	High
			<i>Outgoing</i> <i>Solitary</i>	
A	Agreeableness	Low	←————→	High
			<i>Trusting</i> <i>Competitive</i>	
N	Neuroticism	Low	←————→	High
			<i>Prone to Stress</i> <i>Emotionally Stable</i>	

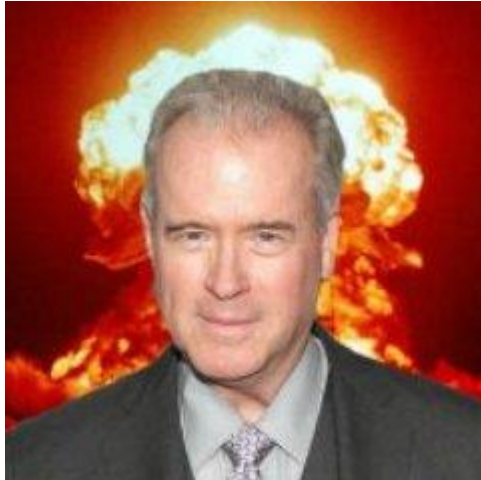
But Bogan...

- The OCEAN personality test is rubbish
- It only caters for 56% of the population
- It doesn't measure
 - religiosity
 - manipulativenness/machiavellianism
 - honesty
 - sexiness/seductiveness
 - thriftiness
 - conservativeness
 - masculinity/femininity
 - snobbishness/egotism
 - sense of humour, or
 - risk-taking/thrill-seeking



Cambridge Analytica

- A "global election management agency"
- Offshoot of parent company SCL Group
- Part owned by the billionaire Robert Mercer who funds Steve Bannon and Breitbart



Cambridge Analytica

- Has as many as 3,000 - 5,000 data points on each American
 - Age, income, debt, hobbies, criminal histories, purchase histories, religious leanings, health concerns, gun ownership, car ownership, homeownership.
 - Collected by the company, and purchased from consumer-data giants
- “Assisted with” Brexit and Trump campaigns
- Currently under investigation by the House Permanent Select Committee on Intelligence

Profiling Yourself - Apply Magic Sauce

- University of Cambridge API
 - CA staff were originally from hired from the uni
- Obtain a list of your profiles likes and posts and process them
- Once your profile type is known, friend people with similar types
- Keep this method for later as we will apply it to each person to deliver “dark ads”

OCEAN Test Results

Average (50%)



Working

the world

isting

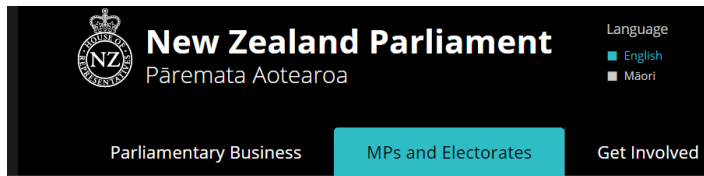
motional

Centres of influence

- Pulling numbers on New Zealanders social media usage is hard
- Facebook (~2.9million users)
 - Visiting 14 times a day
 - Spending on average 50 minutes rotting their brain
- Twitter (~500k)
- Instagram
- Stuff comments 😊

Profiling of electorates

- Parliament.nz website already has done some for us



Clutha-Southland Electorate Profile

[Home](#) » [MPs and Electorates](#) » [Electorate profiles](#)

Published date: 26 Jun 2015

[> View related Documents and downloads](#)

Clutha-Southland: Electoral Profile

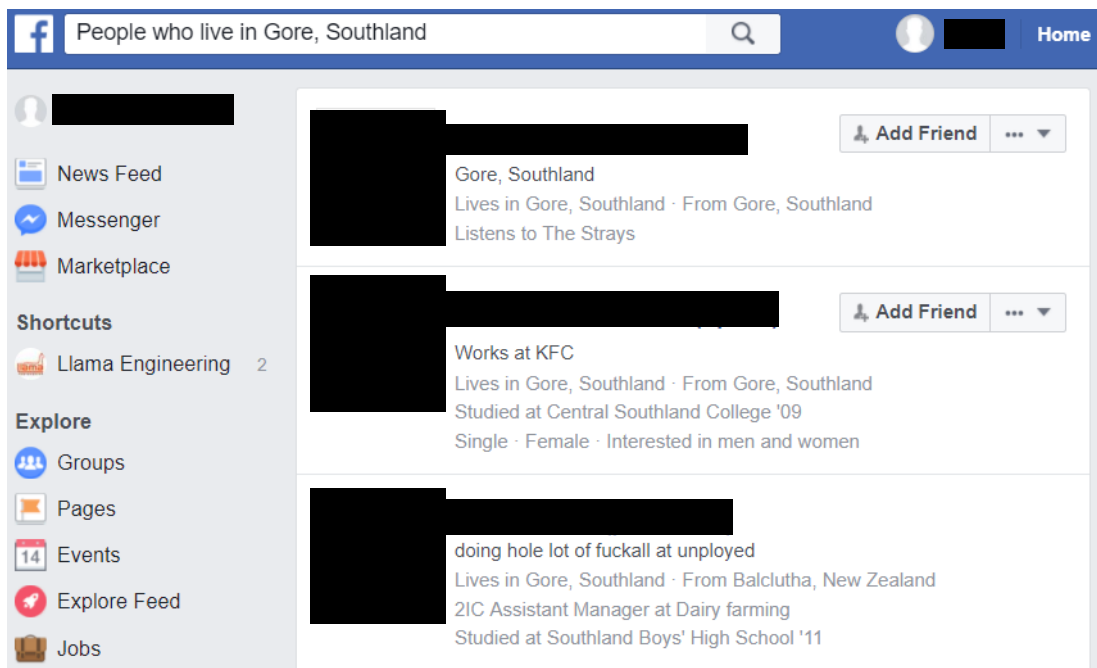
- General notes
- Election results
- 2014 General election results – electorate candidate votes
- 2011 General election results – electorate candidate votes
- 2008 General election results – electorate candidate votes
- General election results – party vote 2008-2014
- Voter enrolment and turnout 2011 and 2014

Clutha-Southland: People

- Population summary
- Age groups of the usually resident population
- Ethnic groups of the usually resident population
- Birthplace of usually resident population
- Birthplace and years since arrival in New Zealand, for overseas born
- Languages spoken
- Highest qualifications of the population aged 15 years and over
- Ethnic group of school pupils July 2014
- Iwi affiliations
- Religious affiliations
- Cigarette smoking behaviour of the population aged 15 years and over

Getting some friends

- Facebooks location search is more restricted than it once was
- You can't use the API, instead of have to scrape the Web UI



The screenshot shows a Facebook search results page for the query "People who live in Gore, Southland". The page features a blue header with the Facebook logo, a search bar containing the query, and a "Home" button. On the left side, there is a navigation menu with options like "News Feed", "Messenger", "Marketplace", "Shortcuts", and "Explore". The main content area displays three search results, each with a profile picture (blacked out), a name (blacked out), and an "Add Friend" button. The first result is located in Gore, Southland, lives in Gore, Southland, and listens to The Strays. The second result works at KFC, lives in Gore, Southland, studied at Central Southland College '09, and is single and interested in men and women. The third result is doing a lot of fuckall at unemployed, lives in Gore, Southland (from Balclutha, New Zealand), and is a 2IC Assistant Manager at Dairy farming, having studied at Southland Boys' High School '11.

Hitting your straps

Respond to Your 228 Friend Requests

[View sent requests](#)



Confirm

Delete Request



Rustam Kurbanov

 Works at Almaty, Kazakhstan

Confirm

Delete Request



خميس عوض فايد



Confirm

Delete Request



خالد سحاق



Confirm

Delete Request



الحارس الشخصي



Confirm

Delete Request

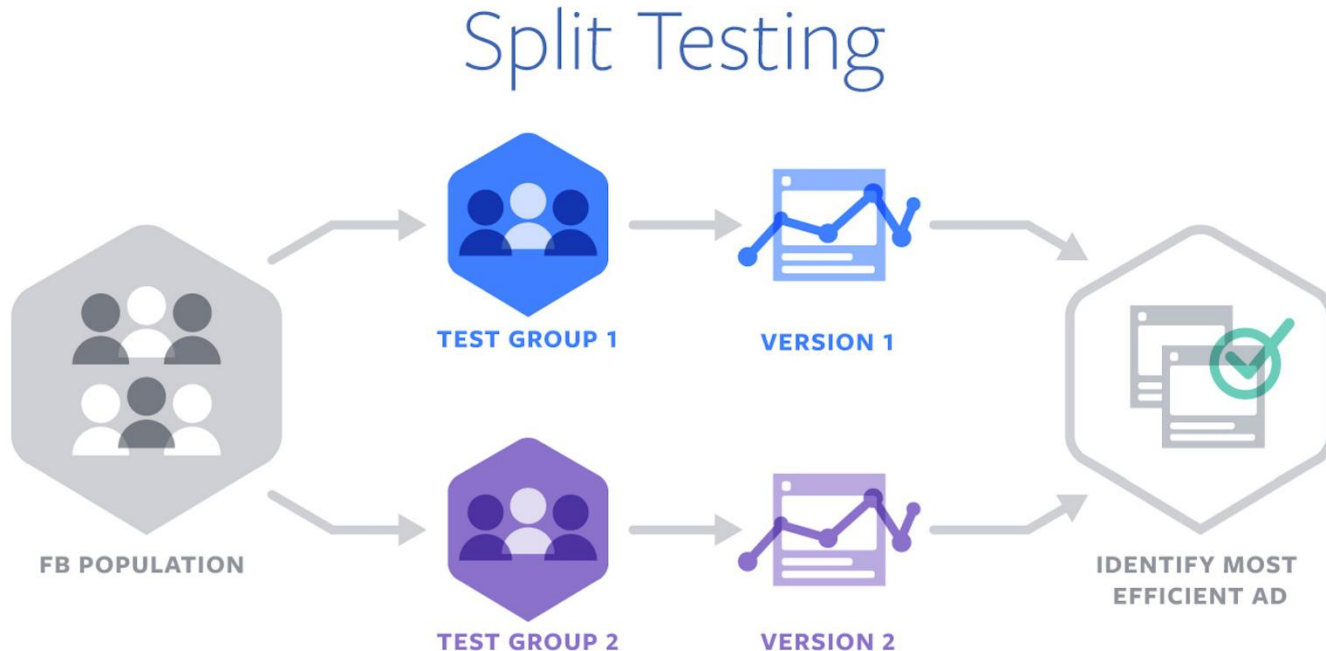
Creation of Content

A pro-gun voter whose Ocean score ranks him high on neuroticism could see storm clouds and a threat: The Democrat wants to take his guns away

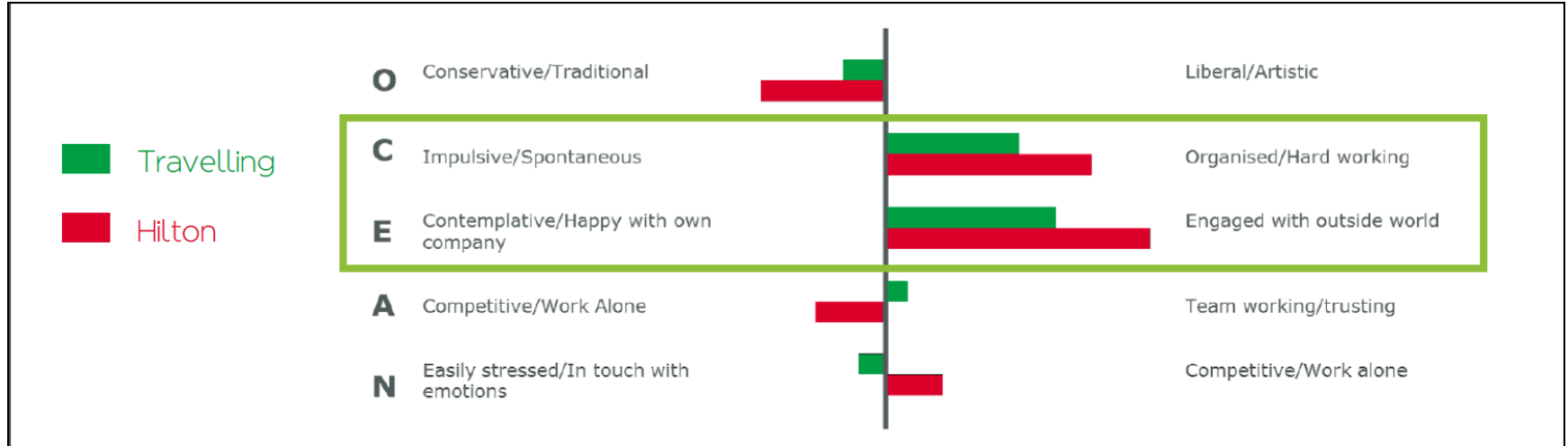
McKenzie Funk - Nytimes

Creation of Content

- Facebook Split testing



Creation of Content



HIGH EXTRAVERSION



Hilton HHonors

23 June at 01:27 · 🌐

Summer's here, so it's time for fun times and good vibes. With more than 300 hotels and up to 33% off rooms across Europe, the Middle East and Africa, those good times are closer than you might think. So, what are you waiting for? Press play on summer!



Hilton Summer Sale

MAKE THIS SUMMER SENSATIONAL with UP to 33% OFF AT OVER 300 HOTELS IN EUROPE, THE MIDDLE EAST & AFRICA.

WWW.HILTONWEEKENDS.CO.UK/SUMMERSALE

[Book Now](#)

HIGH AGREEABLENESS



Hilton HHonors

23 June at 01:27 · 🌐

School's out for summer! That means it's time to corral the family for the annual trip. With more than 300 hotels and up to 33% off room rates across Europe, the Middle East and Africa, you'll be able to find a great place to pitch your wagons.



Hilton Summer Sale

MAKE THIS SUMMER SENSATIONAL with UP to 33% OFF AT OVER 300 HOTELS IN EUROPE, THE MIDDLE EAST & AFRICA.

WWW.HILTONWEEKENDS.CO.UK/SUMMERSALE

[Book Now](#)

Publishing Content

- We don't want to leave a financial trail
- Free advertising campaigns (e.g. AdWords)
- Direct marketing via posting of content
- Using our follower base to push the message

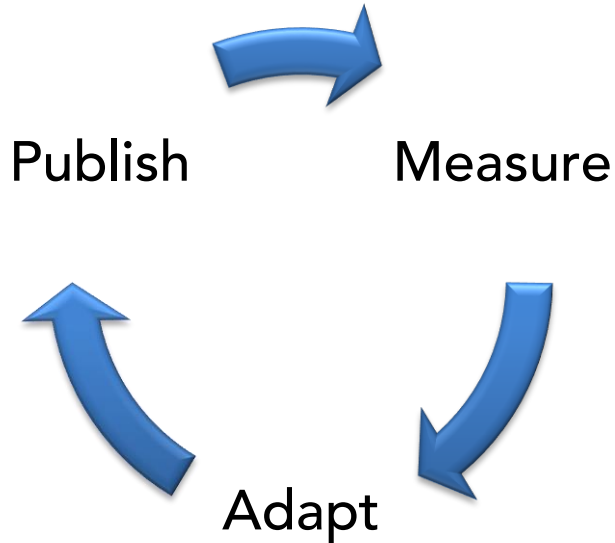


Dark Advertising

- Send different adverts to different target audience groups where it would be disadvantageous for the audience of one target group to see the adverts intended for another
- To do this:
 - Harvest targets likes via scraping
 - Plug into Magic Sauce
 - Target advert directly

Then we wait

- Measure
 - IBM Watson Natural Language (NLP)
 - Sentiment, emotion, keywords, entities
- Adapt
- Publish (Troll)





We are building these Silicon Valley
platforms that are setup to optimise for
self radicalisation

Matt Tait (@pwnallthethings)

The way forward is for us as citizens of the internet, and that's what we all are, to educate ourselves and our families that what we're seeing through that Facebook newsfeed is curated - whether it's by human or computer - and to understand the difference between an ad and an organic story from your friends and sometimes it's hard to tell.

Matt Tait (@pwnallthethings)



Regulators like the Electoral Commission would always be playing catch-up when it came to regulating emerging technology

Val Hooper - Lecturer in marketing, research methodology, consumer and buyer behaviour and information systems management at Victoria University

"Long term maybe this is something we need to look at as a society and say 'well, if this is our view of the world and it's being controlled by some publicly listed company in California, do we want some control or some transparency round that?'"

Vaughn Davis - The Goat Farm's

Facebook made 44 billion in Ad revenue
in the past 2 years.

They have replaced human curation with automated curation. To fix this you need to fundamentally change the model.

Patrick Gray on Risky.biz (RB476)

You can still be super wealthy, but not minting at the current speed. They have been minting at this speed by not paying for the externalities. You wouldn't let a company do something just because they are used to making a lot of money. Maybe they aren't meant to be this profitable.

Zeynep Tufekci on Risky.biz (RB476)

Monitoring - Whotargets.me

- Who Targets Me tells you which political campaigns use Dark Ads and Micro-Targeting to influence your vote.
- Installing the browser extension lets them monitor election campaigns and call for greater digital transparency.
- <https://whotargets.me/en/>
- Feature Request: auto submission of dodgy ads to Facebook

Monitoring – German Marshall Fund

- GMF - Alliance for securing democracy
 - Tracks activity from 600 Twitter accounts linked to Russian influence operations
 - Document URLs, domains, topics and hashtags



Facebook Ad Police

- Facebook have hired 250 people to police adverts on the site
- They are notifying 10s of millions of users who liked / followed the 290 Russian influencers
- Also implementing mechanisms to detect fake news (AI and manual fact checking)



Twitter Policing



MashableAustralia ▾

VIDEO

ENTERTAINMENT

CULTURE

TECH

SCIENCE

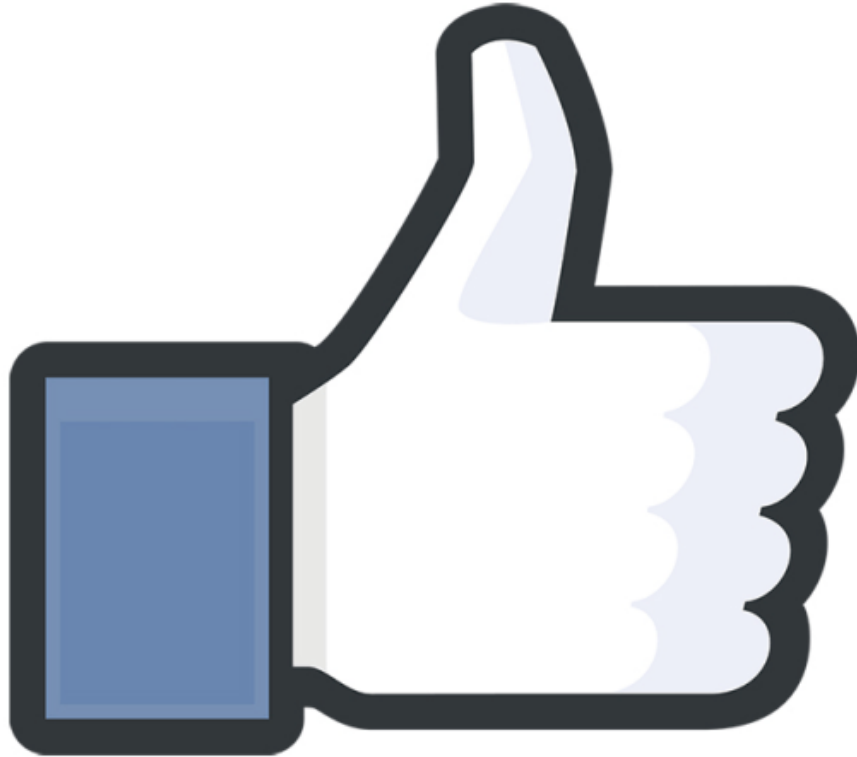
BUSINESS

SOCIAL GOOD

Culture

While everyone celebrated 280 characters, Twitter verified another white supremacist

Delete Facebook



Delete Twitter

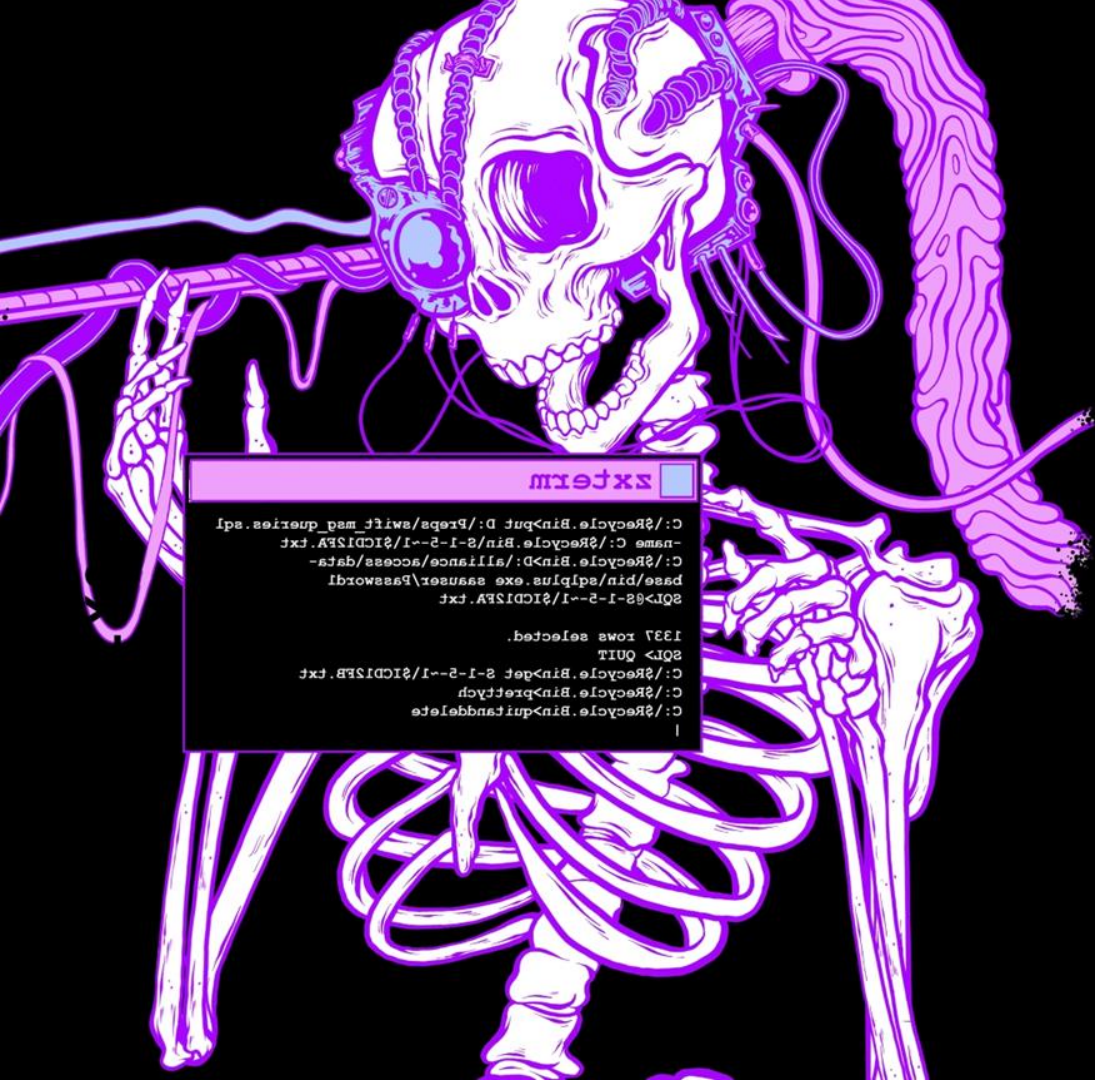


There is a war out there, old friend - a World War. And it's not about whose got the most bullets; it's about who controls the information.

Cosmo – Sneakers (1992)



HOPE



Thanks

simon@zxsecurity.co.nz

References

- https://np.reddit.com/r/worldnews/comments/7a6znc/russia_organized_2_sides_of_a_texas_protest_and/dp7wnoa/
- https://en.wikipedia.org/wiki/Dark_advertising
- <https://www.nytimes.com/2016/11/20/opinion/the-secret-agenda-of-a-facebook-quiz.html>
- <https://risky.biz/RB476/>
- https://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads
- <https://qz.com/1104195/russian-political-hacking-the-internet-research-agency-troll-farm-by-the-numbers/>
- <http://www.rbc.ru/magazine/2017/11/59e0c17d9a79470e05a9e6c1>
- <http://mashable.com/2017/11/08/twitter-verification-white-supremacist/#xOd9IiiZkqX>
- <http://smstools3.kekekasvi.com/>
- <http://securingdemocracy.gmfus.org/>