CyOP: Cyber-Enhanced Influence Operations and Propaganda

Cybersecurity in the world of psychology, political economics, and social choice theory

David M. Perlman, Ph.D.

SOFWERX 2018-12-04
How powerful of a weapon is a CyOP campaign?
2016

- Intel agencies report Russian attacks on US elections
- Senate hearing early December
- Widely reported
2016

- Outrageous, absurd "Pizzagate" appears
- First Twitter and Reddit posts Oct 30-Nov 4
- Widely propagated on known fake news sites & shows
- Spread by prominent far-right figures
December 2016 polls

- Poll numbers Dec. 17-20, 2016:
  - 54% believe "Russia hacked Democratic emails to help Donald Trump"
  - 32% believe "Leaked emails from the Clinton campaign talked about pedophilia and human trafficking, pizzagate"
- Less than 2 months:
  - 32% of America believes an obvious lie
  - 46% *disbelieve* truth from legitimate respectable sources
Even worse by party...
2016 election theories

Do you think the following statements are true or not true? %

<table>
<thead>
<tr>
<th>Statement</th>
<th>Clinton voters</th>
<th>Trump voters</th>
<th>Clinton voters</th>
<th>Trump voters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Russia hacked Democratic e-mails in order to help Donald Trump</td>
<td>87%</td>
<td>80%</td>
<td>82%</td>
<td>46%</td>
</tr>
<tr>
<td>Leaked e-mails from the Clinton campaign talked about pedophilia and human trafficking - 'Pizzagate'</td>
<td>13%</td>
<td>20%</td>
<td>17%</td>
<td>53%</td>
</tr>
</tbody>
</table>

Source: YouGov | yougov.com

December 17-20, 2016
Republicans — traditionally the party of national security — nearly unanimously rejected the wisdom of our own national security community.

More than half came to believe an outrageous lie after less than 2 months of CyOP
The objective of this campaign had nothing to do with "pizzagate" of course...
Republicans More Likely to See Russia as an Ally of, or Friendly Toward, the U.S.

For each of the following countries, please say whether you consider it an ally of the United States, friendly, but not an ally, unfriendly, or an enemy of the United States. How about Russia?

- Ally or friendly, but not an ally
- Unfriendly
- Enemy

YouGov

In the U.S., the partisan gap in views toward Russia has narrowed since 2017.

Favorable view of Russia
Republicans’ views of FBI turn far less positive

% who say they have a favorable opinion of the FBI

Pew

<table>
<thead>
<tr>
<th>Year</th>
<th>Total</th>
<th>Dem/Lean Dem</th>
<th>Rep/Lean Rep</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>67</td>
<td>71</td>
<td>68</td>
</tr>
<tr>
<td>2014</td>
<td>65</td>
<td>77</td>
<td>49</td>
</tr>
<tr>
<td>2018</td>
<td>49</td>
<td>71</td>
<td>68</td>
</tr>
</tbody>
</table>

PEW RESEARCH CENTER

Share of respondents who rate the job of the FBI as “excellent” or “good”

Gallup

Net Favorability of the CIA, By Party Affiliation

NBC

YouGov
Out with the old...

If there was a referendum on Britain’s membership of the EU, how would you vote? % responding

June 23rd EU referendum

Sources: “What UK Thinks”, NatCen; The Economist
The ongoing CyOP campaign has been extremely effective at manipulating public sentiment and beliefs in the US in ways favorable to Russia — and we can only expect this to get worse.
● Prolog on cognitive bias
● Sampling of techniques used in CyOP
● Government and private players (Domestic US-centric)
  ○ What can, can't, and should be done right now
● Comprehensive influence security framework!
  ○ Sara-Jayne Terp
Prolog: On Cognitive Bias

- Convenient heuristic for thinking and bias:
  - System 1 (fast, approximate)
  - System 2 (slow, careful) thinking

- Biases generally err towards ego and social consistency

- These biases affect everyone

- **Including you**
So, what can I do about my own bias?
So, what can I do about my own bias?

- Intuition won't de-bias you
- Willpower won't de-bias you
- Calling yourself a scientist/objectivist/rationalist won't de-bias you

"Bias Hygiene"
  - Learn types of bias
  - Assume you are biased
  - Use habits of pre-flight and debrief
Types of cognitive bias

- Biases generally err towards ego and social consistency:
  - Confirmation bias
  - Social conformity (Asch)
  - Availability heuristic
  - Framing effects
  - Self-serving/Superiority/Dunning-Kruger


- Many excellent, accessible books and articles
"I'm a scientist, so I'd better try as hard as I can to be rational and objective!"

... "Yeah I think I'm doing a pretty good job! Look at how objective I am! I'm a great scientist!"

Self-serving biases will trick you into thinking you are not biased.

If you convince yourself you're not biased, when you really are, that's worse than baseline.
WRONG: IDENTITY

- "I'm a scientist, so I'd better try as hard as I can to be rational and objective!"
- "Yeah I think I'm doing a pretty good job! Look at how objective I am! I'm a great scientist!"
- Self-serving biases will trick you into thinking you are not biased
- If you convince yourself you're not biased, when you really are, that's worse than baseline

RIGHT: BIAS HYGIENE

- "I know I am biased!"
- Pre-flight checklist
  - Second opinion if possible
  - Which direction am I most likely to be biased?
  - Consciously edit decision/opinion
  - It will feel "wrong": but that's OK
  - "System 1" will adapt over time
- Debrief
  - Which direction did I err?
  - Is that consistent with my self-image?
  - How well did my pre-flight efforts work?
  - What could I do differently next time?
Always remember: YOU have cognitive bias
Execution: front line

- Two startups accidentally choose same name
- One has bigger budget
- Both have teams with similar reputations
- Underdog wants to own the namespace
Tactics: Large-scale political manipulation

- How to radically and rapidly shift public opinion en masse?
- No individual matters, only the demographics...
Overton Window

Originally defined on the left-right spectrum, Overton Window is the range that is socially acceptable in mainstream political and media discourse.
Overton Window

Originally defined on the left-right spectrum, Overton Window is the range that is socially acceptable in mainstream political and media discourse.

1-D left-right spectrum is inadequate:

Nolan Plot
Overton Window

Extend Overton Window to multiple dimensions:

K-Dimensional Overton Window (kDOW) or "Overton Blob"

Regions of high density in the population distribution
Not Out Here in the Fringe!

Somewhere In Here
Overton Window Convex Hull

Postulate: compromise positions are always socially acceptable

Example: Maybe all Americans are either pro-choice or anti-abortion with no moderates. However, a pundit who advocated compromise would be acceptable on TV.

Formalization: Overton convex hull
Security implications of Overton Hull

Gradually move the window.

"Foot-in-the-door" technique (FITD): Stretch it a little bit at a time

Time- and resource-intensive
Security implications of Overton Hull

Stretch the window rapidly?
Security implications of Overton Hull

Stretch the window rapidly?

"Door-in-the-face" (DITF) technique: Stretch the window immediately with an extreme position to make room for a less extreme position.
Security implications of Overton Hull

If one teenager eats a spoonful of cinnamon, it's crazy

But if enough do it then it's news…
Security implications of Overton Hull

If one teenager eats a spoonful of cinnamon, it's crazy

But if enough do it then it's news…

*TIDE PODS!!!*
Out Here in the Fringe is OK now!
Extreme political manipulation

Most people's beliefs are very hard to change.

"Lunatic fringe" of gullible individuals easier to manipulate. Sweep up the fringe.

Charismatic demagogue could cultivate a following of conspiracy theory believers

Unreasonableness guarantees community will consist only of the unquestioning (compare to 419 scams)

Cold War "useful idiots" but at a population level: Weaponized Demographic or WUID
Monitoring the "battlefield"

This tactic would be easy to see if you had a visualization of the battlefield.

"Big Data", social media allow passively sampling in near-real-time.

Signatures of organic and manipulated changes could be identified and then used as an early warning system.

Note that this is different from "microtargeting". Purely defensive and transparent.

Privacy-safe: only requires collective data, can be anonymous!
What tech companies can and can't do
"Why doesn't [tech company] just [ban/delete] all the [bots/Russians/troll farms]?"]
What the tech companies can and can't do

- Signals are too noisy for screening: problem of false positives in public health
- High cost for false positive enforcement
- Ranking algorithms: promote and demote content and users
  - Promote and demote content at the trend level after identifying campaigns
- Train models to identify campaigns:
  - need campaign-level signal
  - Not account-level or content-level
- Can incorporate input from e.g. Intel
What the government can and can't do

- Nationalize Facebook!
- Control content directly
- Counter-propaganda is propaganda: Smith-Mundt, posse comitatus, etc.
- **Can** provide intel to private companies
- Can do law enforcement activities: subpoenas, etc.
Private Defensive Security

"Dark Arts" Offensive Security: counter-operations

Tech Companies

Intelligence

Execution Law Enforcement
Thank you for your attention economy
Postscript: "Adversary" considered harmful

"Adversary" (based on identity) versus "Attacker" or "threat actor" (based on hostile actions) Attackers may not even have intention.

Citizens aren't "adversaries" but they may be "attackers".

Citizens can advocate for more or less military funding, but we don't let people steal fighter planes just because they're citizens.

Citizens can advocate for more or less electric generation, but we don't let people hack into the power grid just because they're citizens.

Citizens vote and campaign in elections. But we should not let people hack elections just because they're citizens. Need clarity in the law!
Postscript: "Adversary" considered harmful

As Peter Singer pointed out, hostile influence operations can hide behind e.g. domestic white supremacist groups.

Tribal framing blinds us to seeing the threat.