3. Influence Techniques

TL;DR Influence Techniques

- A common description language helps us share information about disinformation incidents.
- Describing disinformation behaviours helps us mitigate and counter those behaviours.

Describing Influence

Disinformation isn't always obvious misinformation, e.g. "Covid-19 isn't real". To track it, we need to look for its components, and traces of its creators' activities.

Strategies

The social strategies for mass population influence.

The Four Ds: Distort, Distract, Dismay, Dismiss

Ben Nimmo created the "4Ds": Distort, Distract, Dismay, Dismiss[1].

- Distort the facts. We're not invading Ukraine; we're rescuing/protecting ethnic Russians.
- Dismiss: Critics and uncomfortable facts. Make counter-accusations. We've seen this one used often by China. Every time the U.S. accuses China of stealing our intellectual property via illicit hacking, China retorts by first dismissing the accusation and then stating that they're the targets of U.S. hacking.
- Distract from the main issue. MH-17 was a tragedy. Why is a commercial airliner flying over a war zone?
- Dismay: Ad-hominem – make personal attacks, insults and accusations. This one is particularly interesting because by even addressing these attacks, you lend them credence. Think about Pizzagate. Making a preposterous claim suggesting that political elites have a secret sex dungeon full of kids is very hard to defend against without lending the accusations credence.

CogSecCollab added a fifth D:

- Divide: Reduce trust, create confusion, and provoke populations. It's not an accident when two groups at polar opposite ends of the political spectrum "magically" have competing events at the same time and place.

Hack and Leak

Obtain documents (eg by theft or leak), then release either the real documents, or altered versions of them, possibly among factual documents/sources.

[1] Ben Nimmo, described in "Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter it", StopFake.org, 2018

Unsurmountable Proof

Campaigns often leverage tactical and informational asymmetries on the threat surface, as seen in the Distort and Deny strategies, and the "firehose of misinformation". Specifically, conspiracy theorists can be repeatedly wrong, but advocates of the truth need to be perfect. By constantly escalating demands for proof, propagandists can effectively leverage this asymmetry while also priming its future use, often with an even greater asymmetric advantage. The conspiracist is offered freer rein for a broader range of "questions" while the truth teller is burdened with higher and higher standards of proof.

Fake (and real) Content

Misinformation

Misinformation is fake content. This might be false messages, photoshopped images, or deepfakes: fake text, images, and videos created by computers.

Misinformation doesn't have to be sophisticated, so deepfakes are used more for things like creating fake profile pictures. Some hybrid infosec/disinformation attacks use deep faked voices exist, but these are relatively rare.

Fake but Credible "Research"

Plandemic is an example of credible-seeming research output through videos and reports with high production values.

Grain of Truth

Wrap lies or altered context/facts around truths. Many successful disinformation campaigns work with true information, or information that is mostly true, with a small percentage of misinformation embedded in it: a rough rule of thumb is 90% true to 10% misinformation.

Influence campaigns pursue a variety of objectives with respect to target audiences, prominent among them: 1. undermine a narrative commonly referenced in the target audience; or 2. promote a narrative less common in the target audience, but preferred by the attacker. In both cases, the attacker is presented with a heavy lift. They must change the relative importance of various narratives in the interpretation of events, despite contrary tendencies.

When messaging makes use of factual reporting to promote these adjustments in the narrative space, they are less likely to be dismissed out of hand; when messaging can juxtapose a (factual) truth about current affairs with the (abstract) truth explicated in these narratives, propagandists can undermine or promote them selectively. Context matters.

Narratives

Narratives are the stories that we base our beliefs on: “identity narratives” about who we are, “in-group” and “out-group” narratives about the groups that we do and don’t belong to, and other narratives about what’s happening in the world around us. Examples of narratives include that midwesterners are generous, and that Russia is under attack from outside.

Narratives form the bedrock of our worldviews. New information is understood through a process firmly grounded in this bedrock. If new information is not consistent with the prevailing narratives of an audience, it will be ignored. Effective campaigns make extensive use of audience-appropriate archetypes and meta-narratives throughout their content creation and amplification practices. Examples include using or distorting narratives that already exist in targeted communities, or creating competing narratives connected to the same issue, e.g. deny an incident, and at the same time dismiss it.

Fake (and real) Accounts

To implement strategies using the power of social networks, we need accounts with access to social groups, and personas. These types of accounts can be broken into six categories.

- Bots: Bulk purchase, mostly amplifiers, little-to-no original content
- Parody: Clearly counterfeit account used to satirize or diminish image
- Spoof: Counterfeit account which closely copies real account.
- Camouflage: False account which mimic community of real accounts
- Deep Cover: False account accepted as real for long periods of time
- Takeover: Real account controlled by someone who isn't its owner

It's easy to get caught up in the technology: hacking accounts, identity theft, botnets, and so on, but it's important to remember that the technology is only one aspect of the integrated problem space.

Ignorant Agents

Cultivate propagandists for a cause, the goals of which are not fully comprehended, and who are used cynically by the leaders of the cause. Independent actors use social media and specialised web sites to strategically reinforce and spread messages compatible with their own. Their networks are infiltrated and used by state media disinformation organisations to amplify the state's own disinformation strategies against target populations. Many are traffickers in conspiracy theories or hoaxes, unified by a suspicion of Western governments and mainstream media. Their narratives, which appeal to leftists hostile to globalism and military intervention and nationalists against immigration, are frequently infiltrated and shaped by state-controlled trolls and altered news items from agencies such as RT and Sputnik. Also known as "useful idiots" or "unwitting agents".

Fake Experts

Stories planted or promoted in computational propaganda operations often make use of experts fabricated from whole cloth, sometimes specifically for the story itself.

Fake Groups

Computational propaganda depends substantially on false perceptions of credibility and acceptance. By creating fake users and groups with a variety of interests and commitments, attackers can ensure that their messages both come from trusted sources and appear more widely adopted than they actually are.

Botnets

Bots are automated/programmed profiles designed to amplify content (ie: automatically retweet or like) and give appearance it's more "popular" than it is. They can operate as a network, to function in a coordinated/orchestrated manner. In some cases (more so now) they are an inexpensive/disposable assets used for minimal deployment as bot detection tools improve and platforms are more responsive.

Disinformation Websites

Disinformation websites range from sites created to attract clicks and advertising money, to sites created to spread disinformation. Tertiary sites create content/news/opinion web-sites to cross-post stories. Tertiary sites circulate and amplify narratives. Often these sites have no masthead, bylines or attribution.

Pink Slime Networks

A network of websites that are amplifying misinformation, often whilst purporting to be something else, including a network of local newspapers. A prominent case from the 2016 era was the Denver Guardian, which purported to be a local newspaper in Colorado and specialized in negative stories about Hillary Clinton.

Other dedicated channels

Some nationstate backed news outlets specialise in publishing and amplifying disinformation.

Fake (and real) Sharing

Amplification

Use trolls and bots to amplify narratives and/or manipulate narratives. Fake profiles/ sockpuppets operating to support individuals/narratives from the entire political spectrum (left/right binary). Operating with increased emphasis on promoting local content and promoting real Twitter users generating their own, often divisive political content, as it's easier to amplify existing content than create new/original content.

Hashtag Jacking

Use a dedicated hashtag - either create a campaign/incident specific hashtag, or take over an existing hashtag.

Microtargeting (including SMS, Whatsapp, targeted ads)

Create or fund advertisements targeted at specific populations, or use messaging services to target them individually.

Manipulate Online Polls

Create fake online polls, or manipulate existing online polls. Data gathering tactic to target those who engage, and potentially their networks of friends/followers as well.

Search Engine Optimisation

Manipulate content engagement metrics (ie: Reddit & Twitter) to influence/impact news search results (e.g. Google), also elevates RT & Sputnik headline into Google news alert emails. aka "Black-hat SEO".

Organising Real-World Events

Coordinate and promote real-world events across media platforms, e.g. rallies, protests, gatherings in support of incident narratives.

Astroturfing and Information Pollution (fill the zone with shit)

Firehose of misinformation. Flooding and/or mobbing social media channels feeds and/or hashtag with excessive volume of content to control/shape online conversations and/or drown out opposing points of view. Bots and/or patriotic trolls are effective tools to achieve this effect. Flood social channels; drive traffic/engagement to all assets; create aura/sense/perception of pervasiveness/consensus (for or against or both simultaneously) of an issue or topic. "Nothing is true, but everything is possible." Akin to astroturfing campaign.

Further Reading

- AMITT TTP Guide
- https://medium.com/@timboucher/adversarial-social-media-tactics-e8e9857fede4
- Kate Starbird's social graphs