

Chapter 3 Influence techniques

TL;DR Influence Techniques	1
Describing Influence Techniques	1
Strategies	1
Resources	2

TL;DR Influence Techniques

Describing Influence Techniques

The big ideas here are:

- if we have a common description language, we can share information about disinformation incidents in real time.
- if we describe the moves disinformation creators use, especially if they're reused moves, we can mitigate or block those moves

Strategies

The social strategies for mass population influence can be divided into five categories: Distort, Distract, Dismay, Dismiss, and Divide.

- **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?
- **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.
- **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.

References:

- Ben Nimmo, 19 May 2015. "Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter it." StopFake.org 01 December 2018, <https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/>
- Social graph: Kate Starbird, via <https://twitter.com/katestarbird/status/954805298652332032>

Resources

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 in control of adversary

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.

References:

- <https://medium.com/@timboucher/adversarial-social-media-tactics-e8e9857fede4>