

Disinformation & Propaganda

Research into Disinformation Operations and Methodology

Josh Martin

Index

Introduction	2
Breakdown	3
Examples	4
Operation Shocker	4
Russian Troll Farms	4
Deep Fakes	5
Mitigation Methods	6
Summary	6
References	7

Introduction

The Cambridge dictionary describes disinformation as “false information spread in order to deceive people.” (Cambridge Dictionary) The term disinformation come from the Russian word dezinformatsiya which is derived from the Soviet name for the KGB 1st Main Directorate, Department A, which was responsible for the Soviet Union’s external propaganda operations. (Rychlak, 2013) Depending on who you ask and how you are defining warfare, disinformation can fall under different categories of warfare when conducted by a nation state or non-state threat actor. The most common categories used will be: Political warfare, information warfare, intelligence warfare, psychological warfare, and unconventional warfare. Disinformation as we know it today is nothing new, it has taken place throughout history under different names, such as propaganda, psychological operations, information operations, influence operations, and political warfare.

Breakdown

Disinformation operations can generally be broken down into three categories:

- **White Propaganda:** White propaganda comes from a source that is real, and the information can be accurate. What the target audience hears is close to the truth, and it is presented in a way that convinces the audience that the propagator is on your side with the best ideas and political ideology. This type of propaganda is more what we are accustomed to seeing on social media and similar sites.
- **Black Propaganda:** Black propaganda is credited to a false source, and it is intended to spread lies, false stories, terror, fear, and mentally break down groups of people. A good example of black propaganda is the spread or attempted spread of beheading videos by the terrorist group Daesh.
- **Grey Propaganda:** Grey propaganda is somewhere between white and black propaganda. The source may or may not be real, and the accuracy of information is uncertain. A real world example of targeted disinformation would be Operation Shocker by the Federal Bureau of Investigations in the fifties targeting the Soviet KGB by getting a person the KGB thought was a traitor to U.S. to feed fake information to the KGB about the U.S.'s chemical and biological weapons programs.

There are many academic theories about cognitive processing, attitude formation and change, social influence, and persuasion that explain for people's attitudes, beliefs, or behaviors can be influenced. These theories become key when trying to understand how and why information operations work, below I will list a couple examples of these theories.

- **Expectancy-Value Theory:** This model suggests that meaning arises spontaneously and inevitably as people form beliefs about an object. Each belief a person has that associates with an attitude object with a specific attitude, and the person's overall attitude toward the object is determined by the opinion a person has to the value of the object's attributes in interaction with the strength of the associations. This method provides a framework to examine resistance to persuasion that focuses on message acceptance, second-order and third-order impacts on attitudes not directly addressed in messages. (Psychology Iresearchnet)
- **Cognitive Dissonance Theory:** This theory argues that a person who holds conflicting cognitions is motivated to reduce or stop the tension between these cognitions by trying to bring them back into alignment with each other. (McLeod, 2018) In regards to disinformation and information operations, this can be done by an individual only seeking out and looking at information or data that supports their cognitions and disregarding or attacking other information.

There are a few ways that disinformation can occur and proliferate. With the widespread use and reliance on the internet, it is only making it easier for threat actors to spread their influence and agenda. One-way disinformation can spread is by the selective release of information by organizations, like leaving out parts of an article, or purposely leaving out photos or videos that might add unwanted context. Another way disinformation can spread is through search engine optimization, preparing the fake or partially fake articles or information in such a way that it will appear at the top of Google searches. Another way this can be done is through using bots, fake organizations, or aliases to directly release disinformation to the target audience. A final possible way disinformation can be spread is through hacking targeted individuals or organizations to release select damning evidence on them.

Examples

Operation Shocker

Operation Shocker was a 23-year long operation in the late 1950s conducted by the U.S. Federal Bureau of investigations in an attempt to deceive the Soviet KGB. The operation involved replacing a US Army sergeant that the KGB already had contact with, with a fake defector to release unimportant and fake information on U.S. chemical and biological weapons manufacturing to the Soviets. The defector provided the Soviets with four thousand legitimate documents as well as countless fake documents on a nerve agent that the U.S. was able to create in a stable form in an attempt to waste Soviet resources. Allegedly the Soviets ended up creating the infamous Novichok nerve agent group from these documents.

Russian Troll Farms

Troll Farms, also known as Russian Web Brigades or Troll Factories are groups comprised of political commentators, trolls, and bot herders that are allegedly sponsored by the Russian government to spread disinformation or pro-Kremlin propaganda to further the goals of Putin and the Kremlin. Probably the most famous instance of a Russian troll farm is the Internet Research Agency. The Internet Research Agency is a troll farm with links to the Russian oligarch Yevgeny Prigozhin who has extremely close ties with the Russian President Vladimir Putin, Wagner Group a Russian private military company that allegedly works on behalf of the Kremlin, and the Main Directorate of the General Staff of the Armed Forces of the Russian Federation otherwise known as the GRU. The Internet Research Agency has carried out many operations all over the globe, but probably their most infamous operation was during the United States 2016 Presidential Election where they: used thousands of bots to spread disinformation, and support for certain causes; created multiple political groups for varying and opposing political causes; spent hundreds of thousands of dollars on ad placements; and disseminated hundreds of thousands if not millions of pieces of disinformation including memes, videos, articles, and tweets.

Another fairly interesting operation conducted by the Internet Research Agency was a Columbian Chemicals plant explosion hoax. This event took place in September of 2014. Text, Twitter, and Facebook messages were sent to individuals living in Centerville, St. Mary Parish, Louisiana saying that there had been an explosion at the Columbian Chemicals plant and that ISIS had taken responsibility. At the same time a video was making rounds on YouTube claiming to be of the explosion, a screenshot of a news article claiming to be from CNN and Times-Picayune's website, and a Wikipedia article had been made. They also made clones for the Louisiana TV station and newspaper websites to further spread disinformation on the explosion. (Hill, 2015) Once authorities confirmed it was indeed a hoax, they began disseminating accurate information to residents. This entire incident was created and run by the Internet Research Agency.

Deep Fakes

While not what is expected when people think of disinformation, deep fakes present a very real threat. Deep fakes can be extremely useful tools to spread disinformation in a way that could be harder for a lot of people to differentiate from reality. With the right vocal and facial patterns combined, similar hand, eye, and body language, it becomes extremely hard for people to differentiate between reality and a manufactured video. Once you add those factors with audience targeting you could manufacture whatever disinformation you want to spread whether that be for a specific cause, to gain support for a person, or make people dislike that person. I have included a video below, demonstrating the dangers of deep fake videos.

In the video below you will see a deep fake of former president Barrack Obama. (Buzzfeed, 2018)



Mitigation Methods


Disinformation is interesting in that there are not a ton of ways to combat it, nor are any of them as quick as applying an update to a computer. The only true way to combat disinformation is through educating the masses on how to spot disinformation, even then some information can slip through the cracks and propagate. Some of the best ways to spot disinformation, misinformation, and mal-information are:

- Checking the source of the information
 - Look at the sources of information, who has published it, who shared it, what are their sources, where is it coming from? On social media such as Twitter, Facebook, or Instagram, check the account's username, if it has a lot of random letters and numbers, it could be a bot. If the content you are looking is coming from an unverified account posting content hundreds of times a day, that could be a bot.
- Check where the story is coming from and who is posting it.
 - Usually real news is covered by more than one news source. If mainstream media are not posting about the story, it could be fake, or it cannot be confirmed. By performing a Google search, you might find that independent fact-checkers have already debunked the story.
- Make sure you are not playing into your biases.
 - People are much less likely to identify disinformation if it aligns with their own biases. Before posting content, think about why you are doing so. Is because you know it's true or just because it fits with your ideas?

Summary

Disinformation is the false information spread in order to deceive people and has been used throughout history under different names and under different classifications. There are generally three categories of disinformation, black propaganda, white propaganda, and grey propaganda. There are many ways disinformation can be spread and used by threat actors to influence people's attitudes, beliefs, or behaviors. The only way you can truly combat the spread and influence of disinformation is to educate people on how to find and tell the difference between disinformation and real information.

References

- AI, W. F. (2019, June 8). *Imagine Sung by Trump, Putin & Other World Leaders (John Lennon Song)*. Retrieved from Youtube: <https://youtu.be/OmB7fmi8JwY>
- Bagge, D. P. (2019). *Unmasking Maskirovka Russia's Cyber Influence Operations*. Defense Press.
- Buzzfeed, M. P. (2018, April 17). *You Won't Believe What Obama Says In This Video!*  Retrieved from Youtube:
https://www.youtube.com/watch?v=cQ54GDm1eL0&feature=emb_logo&ab_channel=BuzzFeedVideo
- Cambridge Dictionary. (n.d.). *Disinformation*. Retrieved from Cambridge Dictionary:
<https://dictionary.cambridge.org/dictionary/english/disinformation>
- Canadian Security Intelligence Service. (2017, Feb). *WHO SAID WHAT? The Security Challenges of Modern Disinformation*. Retrieved from Government of Canada:
https://www.canada.ca/content/dam/csis-scrs/documents/publications/disinformation_post-report_eng.pdf
- Conley, H. A. (2016, October 6). *Kremlin Playbook*. Retrieved from CSIS.org:
<https://www.csis.org/analysis/kremlin-playbook>
- Cummins, D. (2019, May 6). Timesuck | The Brutal KGB and Russia's Long History of Secret Police. Bad Magic Productions.
- Cummins, S. T. (2019). *The Ultimate Art of War A Step-by-Step Illustrated Guide To Sun Tzu's Teachings*. Watkins Media Limited.
- Dorogan, A. S. (2010). *The New Nobility The Restoration of Russia's Security State and the Enduring Legacy of the KGB*. PublicAffairs.
- Fridman, O. (2018). *Russian Hybrid Warfare: Resurgence and Politicization*. Oxford University Press.
- Gangware, C. N. (2019, March). *Weapons of Mass Distraction: Foreign Disinformation in the Digital Age*. Retrieved from U.S. Department of State: <https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf>
- Hill, J. (2015, June 2). *The Agency*. Retrieved from NY Times:
https://www.nytimes.com/2015/06/07/magazine/the-agency.html?_r=0
- Krogerus, H. G. (2017, December 2). *fake-news-botnets-how-russia-weaponised-the-web-cyber-attack-estonia*. Retrieved from theguardian.com:
<https://www.theguardian.com/technology/2017/dec/02/fake-news-botnets-how-russia-weaponised-the-web-cyber-attack-estonia>
- Mcleod, S. (2018, Feb 5). *Cognitive Dissonance*. Retrieved from Simply Psychology:
<https://www.simplypsychology.org/cognitive-dissonance.html>

- McReynolds, J. (2015). *China's Evolving Military Strategy*. Jamestown Foundation.
- Mitrokhin, C. A. (2000). *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*. Basic Books.
- Mitrokhin, C. A. (2018). *The Mitrokhin Archive: The KGB in the World*. Penguin Press.
- New York Times. (2018, Nov 25). *Operation InfeKtion: How Russia Perfected the Art of War*. Retrieved from New York Times / Youtube:
https://www.youtube.com/watch?v=tR_6dibpDfo&ab_channel=TheNewYorkTimes
- Psychology Iresearchnet. (n.d.). *Expectancy-Value Theory*. Retrieved from Iresearchnet:
<http://psychology.iresearchnet.com/sports-psychology/sport-motivation/expectancy-value-theory/>
- Purcell, L. M. (n.d.). *EXERCISE/EXERCICE New Horizons Core Requirements for the Successful Development of a Psychological Operations*. Retrieved from Canadian Forces College:
<https://www.cfc.forces.gc.ca/259/290/293/287/purcell.pdf>
- Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. (2019, March). Retrieved from justice.gov: <https://www.justice.gov/storage/report.pdf>
- Rhysider, J. (2020, May 12). Ep 65: PSYOPS. *Darknet Diaries*. Darknet Diaries.
- Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux; Illustrated edition.
- Rychlak, I. M. (2013). *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*. WND Books.
- Sawyer, R. D. (2007). *The Tao of Deception: Unorthodox Warfare in Historic and Modern China*. Basic Books.
- Stengel, R. (2019). *Information Wars: How We Lost the Global Battle Against Disinformation and What We Can Do About It*. Atlantic Monthly Press.
- White, S. P. (2018, March 20). *understanding-cyberwarfare-lessons-russia-georgia-war*. Retrieved from mwi.usma.edu: <https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/>
- Xiangsui, Q. L. (2017). *Unrestricted Warfare*. Shadow Lawn Press.