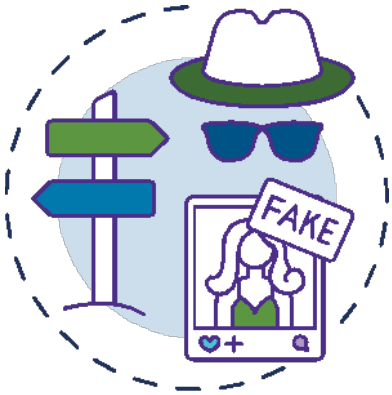
Tactics of Disinformation

Disinformation actors use a variety of tactics to influence others, stir them to action, and cause harm. Understanding these tactics can increase preparedness and promote resilience when faced with disinformation.

While this series discusses open-source examples of disinformation attributed by others to foreign governments, it does not represent the U.S. government confirming the accuracy of any such attribution.



What Are Disinformation Tactics?

Disinformation actors use a variety of tactics and techniques to execute information operations and spread disinformation narratives that pose risk to critical infrastructure. Each of these tactics are designed to make disinformation actors' messages more credible, or to manipulate their audience to a specific end. They often seek to polarize their target audience across contentious political or social divisions, making the audience more receptive to disinformation.

These methods can and have been weaponized by disinformation actors to generate threats to U.S. critical infrastructure. The Tactics of Disinformation series helps organizations understand and manage the risks posed by disinformation by breaking down common tactics, sharing real-world examples, and providing concrete steps to counter these narratives with accurate information. Any organization and its staff can be targeted by disinformation campaigns, and all organizations have a role to play in building a resilient information environment. This product, and others available in the CISA MDM Resource Library, supports critical infrastructure organizations in assessing their risk posture and building resilience in their communities.

Tactics Overview

Cultivate Fake or Misleading Personas and Websites: Disinformation actors create networks of fake personas and websites to increase the believability of their message with their target audience. Fake expert networks use inauthentic credentials (e.g., fake "experts", journalists, think tanks, or academic institutions) to lend undue credibility to their influence content and make it more believable.

Create Deepfakes and Synthetic Media: Synthetic media content may include photos, videos, and audio clips that have been digitally manipulated or entirely fabricated to mislead the viewer. Artificial intelligence (AI) tools can make synthetic content nearly indistinguishable from real life. Synthetic media content may be deployed as part of disinformation campaigns to promote false information and manipulate audiences.

Devise or Amplify Conspiracy Theories: Conspiracy theories attempt to explain important events as secret plots by powerful actors. Conspiracy theories not only impact an individual's understanding of a particular topic; they can shape and influence their entire worldview. Disinformation actors capitalize on conspiracy theories by generating disinformation narratives that align with the conspiracy worldview, increasing the likelihood that the narrative will resonate with the target audience.

Astroturfing and Flooding the Information Environment: Disinformation campaigns will often post overwhelming amounts of content with the same or similar messaging from several inauthentic accounts. This practice, known as astroturfing, creates the impression of widespread grassroots support or opposition to a message, while concealing its true origin. A similar tactic, flooding, involves spamming social media posts and comment sections with the intention of shaping a narrative or drowning out opposing viewpoints.

Abuse Alternative Platforms: Disinformation actors may abuse alternative social media platforms to intensify belief in a disinformation narrative among specific user groups. Disinformation actors may seek to take advantage of platforms with fewer user protections, less stringent content moderation policies, and fewer controls to detect and remove inauthentic content and accounts than other social media platforms.

Exploit Information Gaps: Data voids, or information gaps, occur when there is insufficient credible information to satisfy a search inquiry. Disinformation actors can exploit these gaps by generating their own influence content and seeding the search term on social media to encourage people to look it up. This increases the likelihood that audiences will encounter disinformation content without any accurate or authoritative search results to refute it.

Manipulate Unsuspecting Actors: Disinformation actors target prominent individuals and organizations to help amplify their narratives. Targets are often unaware that they are repeating a disinformation actor's narrative or that the narrative is intended to manipulate.

Spread Targeted Content: Disinformation actors produce tailored influence content likely to resonate with a specific audience based on their worldview and interests. These actors gain insider status and grow an online following that can make future manipulation efforts more successful. This tactic often takes a "long game" approach of spreading targeted content over time to build trust and credibility with the target audience.

Actions You Can Take

Although disinformation tactics are designed to deceive and manipulate, critically evaluating content and verifying information with credible sources before deciding to share it can increase resilience against disinformation and slow its spread. Share these tips:

- **Recognize the risk.** Understand how disinformation actors leverage these tactics to push their agenda. Be wary of manipulative content that tries to divide.
- **Question the source.** Critically evaluate content and its origin to determine whether it's trustworthy. Research the author's credentials, consider the outlet's agenda, and verify the supporting facts.
- **Investigate the issue.** Conduct a thorough, unbiased search into contentious issues by looking at what credible sources are saying and considering other perspectives. Rely on credible sources of information, such as government sites.
- **Think before you link.** Slow down. Don't immediately click to share content you see online. Check the facts first. Some of the most damaging disinformation spreads rapidly via shared posts that seek to elicit an emotional reaction that overpowers critical thinking.
- **Talk with your social circle.** Engage in private, respectful conversations with friends and family when you see them sharing information that looks like disinformation. Be thoughtful what you post on social media.

TACTICS OF DISINFORMATION:

Cultivate Fake or Misleading Personas and Websites

Disinformation actors use a variety of tactics to influence others, stir them to action, and cause harm. Understanding these tactics can increase preparedness and promote resilience when faced with disinformation.

While this document discusses open-source examples of disinformation attributed by others to foreign governments, it does not represent the U.S. government confirming the accuracy of any such attribution.

Description

Disinformation actors create networks of fake personas and websites to increase the believability of their message with their target audience. Such networks may include fake academic or professional "experts," journalists, think tanks, and/or academic institutions. Some fake personas are even able to validate their social media accounts (for example, a blue or gray checkmark next to a username), further confusing audiences about their authenticity. Fake expert networks use inauthentic credentials to make their content more believable.

Disinformation actors also increase the credibility of these fake personas by generating falsified articles or research papers and sharing them online. Sometimes, these personas and their associated publications are intentionally amplified by other actors. In some instances, these materials are also unwittingly shared by legitimate organizations and users. The creation or amplification of content from these fake personas makes it difficult for audiences to distinguish real experts from fake ones.

Adversaries have also demonstrated a "long game" approach with this tactic by building a following and credibility with seemingly innocuous content before switching their focus to creating and amplifying disinformation. This lends a false credibility to campaigns.

Examples

- Russia's military intelligence agency, the GRU, utilized fake experts in their influence efforts around the 2016 U.S. Presidential election. GRU operatives created fake think tanks and news sites populated with articles by inauthentic personas. They established dozens of public Facebook pages to post and amplify the content. Content ranged from expressing support for Russian interests in the Syrian and 2014 Ukrainian conflicts to issues of racial justice in the United States.[1]

- The Iranian-aligned network of fake websites and personas known as "Endless Mayfly" impersonates legitimate media outlets to spread disinformation narratives. They then use their fake personas to amplify content on social media.[2]

[1]DiResta, Renee, and Shelby Grossman. Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019. Stanford, CA: Stanford University, 2019.
[2]Lim et al. Burned After Reading: Endless Mayfly's Ephemeral Disinformation Campaign. The Citizen Lab, 2019.

Calls to Action

- In both traditional and social media communication activities, direct audiences to official websites and trusted sources of information.
- Ensure that your organization's website conveys clear, concise, and current information that people can turn to as a trusted source.
- Government organizations should transition websites to the .gov top-level domain to communicate to the public that the website is genuine and secure.
- Keep the organization's online information up to date and "validate" social media accounts for the organization, key representatives, and spokespeople.
- Verify the sources of articles, papers, and other resources before sharing them.

TACTICS OF DISINFORMATION:

Create Deepfakes and Synthetic Media

Disinformation actors use a variety of tactics to influence others, stir them to action, and cause harm. Understanding these tactics can increase preparedness and promote resilience when faced with disinformation.

While this document discusses open-source examples of disinformation attributed by others to foreign governments, it does not represent the U.S. government confirming the accuracy of any such attribution.

Description

Synthetic media content may include photos, videos, and audio clips that have been digitally manipulated or entirely fabricated to mislead the viewer. *Cheapfakes* are a less sophisticated form of manipulation involving real audio clips or videos that have been sped up, slowed down, or shown out of context to mislead. In contrast, *deepfakes* are developed by training artificial intelligence (AI) algorithms on reference content until it can produce media that is nearly indistinguishable from real life. Deepfake technology makes it possible to convincingly depict someone doing something they haven't done or saying something they haven't said. While synthetic media technology is not inherently malicious, it can be deployed as part of disinformation campaigns to share false information or manipulate audiences.

Deepfake photos by disinformation actors can be used to generate realistic profile pictures to create a large network of inauthentic social media accounts. Deepfake videos often use AI technology to map one person's face to another person's body. In the case of audio deepfakes, a "voice clone" can produce new sentences as audio alone or as part of a video deepfake, often with only a few hours (or even minutes) of reference audio clips. Finally, an emerging use of deepfake technology involves AI-generated text, which can produce realistic writing and presents a unique challenge due to its ease of production.

Examples

- The pro-Chinese political spam network Spamouflage Dragon used AI-generated profiles to create a cluster of inauthentic profiles to spread its English-language cheapfake videos attacking U.S. policy in June 2020. Many videos featured selectively edited news coverage overlaid by awkward, automated voice-overs and captions.[1]
- In September 2020, Facebook took down thirteen accounts attributed to the Russian Internet Research Agency that used AI-generated profile pictures to appear more believable to unwitting audiences.[2]
- Russian media promoted a deepfake video purportedly showing Ukrainian President Volodymyr Zelenskyy telling Ukrainian troops to stand down in March 2022. Hackers managed to broadcast the video on live television news in Ukraine.[3]

Calls to Action

- Educate staff on how their personal information (such as public photos or videos on social media) could be used to generate synthetic media content and encourage good cyber hygiene practices across both personal and professional accounts.
- Utilize publicly available tools, like reverse image search, to verify the source of media content.
- Add disclaimers to content you share or create that includes synthetic media, even benign uses, to raise public awareness.
- Incorporate responding to deepfake videos or audio clips impacting your organization into your organization's incident response plan.
- Quickly identify any synthetic media impacting your organization or your message and debunk on official channels, offering evidence, if possible.

[1] Nimmo, Ben, Camille François, C. Shawn Eib, and Léa Ronzaud. "Spamouflage Goes to America." Graphika, August 2020. https://public-assets.graphika.com/reports/graphika_report_spamouflage_goes_to_america.pdf.

[2] Nimmo, Ben, Camille François, C. Shawn Eib, and Léa Ronzauc. "IRA Again: Unlucky Thirteen." Graphika, September 2020. https://public-assets.graphika.com/reports/graphika_report_ira_again_unlucky_thirteen.pdf.

[3] Allyn, Bobby. "Deepfake Video of Zelenskyy Could Be 'Tip of the Iceberg' in Info War, Experts Warn." NPR. NPR, March 17, 2022. https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia.

TACTICS OF DISINFORMATION:

Devise or Amplify Conspiracy Theories

Disinformation actors use a variety of tactics to influence others, stir them to action, and cause harm. Understanding these tactics can increase preparedness and promote resilience when faced with disinformation.

While this document discusses open-source examples of disinformation attributed by others to foreign governments, it does not represent the U.S. government confirming the accuracy of any such attribution.

Description

Conspiracy theories attempt to explain important events as secret plots by powerful actors.[1] Conspiracy theories not only impact an individual's understanding of a particular topic; they can shape and influence their entire worldview. Conspiracy theories often present an attractive alternative to reality by explaining uncertain events in a simple and seemingly cohesive manner, especially during times of heightened uncertainty and anxiety.

Disinformation actors capitalize on conspiracy theories by generating disinformation narratives that align with the conspiracy worldview, increasing the likelihood that the narrative will resonate with the target audience. By repeating certain tropes across multiple narratives, malign actors increase the target audience's familiarity with the narrative and therefore its believability. Conspiracy theories can also present a pathway for radicalization to violence among certain adherents. Conspiracy theories can alter a person's fundamental worldview and can be very difficult to counter retroactively, so proactive resilience building is especially critical to prevent conspiratorial thinking from taking hold.

Examples

- In 2020, Chinese state media channels and government officials claimed that COVID-19 had originated in the United States and had been brought to China by a member of the U.S. military. Such narratives were present earlier among conspiracy theory communities online, but China's extensive information operations networks legitimized and amplified these narratives broadly across traditional and social media in an effort to redirect criticism from China's own handling of the outbreak and to attempt to discredit its geopolitical rivals.[2]
- Russia's Defense Ministry deployed the disinformation narrative that the U.S. government is funding military programs in Ukraine to produce bioweapons. Further amplified by the Chinese Foreign Ministry, these narratives seek to justify Russia's invasion as a mission to neutralize the alleged bioweapons and to provide grounds for blaming the U.S. or Ukraine in potential false-flag operation.[3]

Calls to Action

- Utilize CISA's MDM Planning and Incident Response Guide to prepare your team for responding to potential narratives.
- Ensure that your organization's website is up-to-date with clear, accurate information, including an FAQ or Rumor Control page addressing common points of confusion about your work.
- Establish both online and offline channels to share information with your peers and partners and collaborate as an amplifying network for trusted information.
- Proactively educate audiences about how conspiracy theories work and common tropes they may encounter.

[1] Douglas, Karen M, Robbie M Sutton, and Alexandra Cichocka. "The Psychology of Conspiracy Theories." Current Directions in Psychological Science 26, no. 6 (December 2017): 528–42. https://doi.org/10.1177/0963721417718261.

[2] DiResta, Renée. "For China, the 'USA Virus' Is a Geopolitical Ploy." The Atlantic. Atlantic Media Company, May 14, 2020. https://www.theatlantic.com/ideas/archive/2020/04/chinas-covid-19-conspiracy-theories/609772/.

[3] Rising, David. "China Amplifies Unsupported Russian Claim of Ukraine Biolabs." AP News. Associated Press, March 11, 2022. https://apnews.com/article/russia-ukraine-covid-health-biological-weapons-china-39eeee023efdf7ea59c4a20b7e018169.

TACTICS OF DISINFORMATION:

Astroturfing and Flooding the Information Environment

Disinformation actors use a variety of tactics to influence others, stir them to action, and cause harm. Understanding these tactics can increase preparedness and promote resilience when faced with disinformation.

While this document discusses open-source examples of disinformation attributed by others to foreign governments, it does not represent the U.S. government confirming the accuracy of any such attribution.

Description

Disinformation campaigns will often post overwhelming amounts of content with the same or similar messaging from several inauthentic accounts, either created by automated programs known as bots or by professional disinformation groups known as troll farms. By consistently seeing the same narrative repeated, the audience sees it as a popular and widespread message and is more likely to believe it. This practice, known as astroturfing, creates the impression of widespread grassroots support or opposition to a message, while concealing its true origin.

A similar tactic, flooding, involves spamming social media posts and comment sections with the intention of shaping a narrative or drowning out opposing viewpoints, often using many fake and/or automated accounts. Flooding may also be referred to as "firehosing." This tactic is used to stifle legitimate debate, such as the discussion of a new policy or initiative, and discourage people from participating in online spaces. Information manipulators use flooding to dull the sensitivity of targets through repetition and create a sense that nothing is true. Researchers call these tactics "censorship by noise," where artificially amplified narratives are meant to drown out all other viewpoints. Artificial intelligence and other advanced technologies enable astroturfing and flooding to be deployed at speed and scale, more easily manipulating the information environment and influencing public opinion.

Examples

- In 2016, Russian agents, part of the Internet Research Agency, impersonated activists on both sides of the political spectrum to flood social media channels with inflammatory content, as well as to call for activists to attend events.[1]
- The Chinese government has been suspected of hiring as many as two million people, known as the "50 Cent Party," to flood the web in China with pro-regime messaging. The 50 Cent Party drowns out critics and distracts from policy issues by sharing an overwhelming amount of positive news on online platforms.[2]

[1]Keller et al. It's not easy to spot disinformation on Twitter. Here's what we learned from 8 political 'astroturfing' campaigns. The Washington Post, 2019.

[2]King, Gary, Jennifer Pan, and Margaret E. Roberts. How the Chinese government fabricates social media posts for strategic distraction, not engaged argument. Harvard University, 2017.

Calls to Action

- If you suspect an account is inauthentic, check details such as the account creation date, profile picture, bio, followed accounts, or posting activity.
- Consider whether content is posted by suspected bot or troll accounts before sharing.
- Develop a network of trusted communicators in your area to amplify authoritative, accurate information.
- Communicate with your audience through more than one channel, so you have alternate ways to share information if your organization is targeted by an astroturfing or flooding campaign.
- Encourage discussion, debate, and feedback from your constituents through both online and offline. forums.

TACTICS OF DISINFORMATION:

Abuse Alternative Platforms

Disinformation actors use a variety of tactics to influence others, stir them to action, and cause harm. Understanding these tactics can increase preparedness and promote resilience when faced with disinformation.

While this document discusses open-source examples of disinformation attributed by others to foreign governments, it does not represent the U.S. government confirming the accuracy of any such attribution.

Description

Disinformation actors often seek opportunities for their narratives to gain traction among smaller audiences before attempting to go viral. While alternative social media platforms are not inherently malicious, disinformation actors may take advantage of less stringent platform policies to intensify belief in a disinformation narrative among specific user groups. These policies may include fewer user protections, less stringent content moderation policies, and fewer controls to detect and remove inauthentic content and accounts than some of the other social media platforms.[1]

Alternative platforms often promote unmoderated chat and file sharing/storage capabilities, which is not inherently malicious but may be appealing for actors who want to share disinformation.* While some alternative platforms forbid the promotion of violence on public channels, they may have less visibility into private channels or groups promoting violence. Disinformation actors will recruit followers to alternative platforms by promoting a sense of community, shared purpose, and the perception of fewer restrictions. Groups on alternative platforms may operate without the scrutiny or detection capabilities that other platforms have. Often, groups focus on specific issues or activities to build audience trust and disinformation actors can, in turn, abuse this trust and status to establish credibility on other platforms.

Examples

- The Russian government has encouraged users to turn to specific platforms for pro-Kremlin content from state-affiliated media, including Sputnik and RT News. These channels spread disinformation concealed as fake "war correspondents" or fake "fact-checking" about Russia's invasion of Ukraine.[2]
- Foreign terrorist organizations sometimes leverage disinformation tactics to abuse alternative platforms as well. Terrorist organizations like ISIS have leveraged the platforms to spread malign content, recruit new followers, and coordinate activities. Research shows that communications by ISIS on alternative platforms played a role in the uptick in terrorism attacks in Europe between 2015 and 2016.[3]

Calls to Action

- Encourage questions, feedback, and dialogue from your followers and constituents across communication channels.
- Train staff on responding to external questions and feedback with clear, accurate information and empathy.
- Rotate responsibilities for responding to external audiences to avoid burnout among staff.
- Work with your team to develop community guidelines and expectations for behavior on social media channels and communicate these to your followers.
- Where possible, work with partners who have a presence across different communication channels to enable rapid information sharing and amplification.

[1]Greenhalgh, Spencer, Daniel G. Krutka, and Shannon M. Oltmann. "Gab, Parler, and (Mis)educational Technologies: Reconsidering Informal Learning on Social Media Platforms." *The Journal of Applied Instructional Design* 10, no. 3 (2021).

[2]Alazab, Mamoun and Kat Macfarlane. "Why Telegram became the go-to app for Ukrainians—despite being rife with Russian disinformation." *The Conversation* (2022).

[3]Walther, Samantha and Andrew McCoy. "US extremism on Telegram: Fueling disinformation, conspiracy theories, and accelerationism." *Perspectives on Terrorism* 15, no. 2 (2021).

*Note: The misuse of social media by a disinformation actor should not be attributed to the social media platform, absent specific articulable facts tending to show the platform is acting at the direction or under the control of a disinformation actor.

TACTICS OF DISINFORMATION:

Exploit Information Gaps

Disinformation actors use a variety of tactics to influence others, stir them to action, and cause harm. Understanding these tactics can increase preparedness and promote resilience when faced with disinformation.

While this document discusses open-source examples of disinformation attributed by others to foreign governments, it does not represent the U.S. government confirming the accuracy of any such attribution.

Description

Data voids, or information gaps, occur when there is insufficient credible information to satisfy a search inquiry, such as when a term falls out of use or when an emerging topic or event first gains prominence (e.g., breaking news). When a user searches for the term or phrase, the only results available may be false, misleading, or have low credibility. While search engines work to mitigate this problem, disinformation actors can exploit this gap by generating their own influence content and seeding the search term on social media to encourage people to look it up.

Because the specific terms that create data voids are difficult to identify beforehand, credible sources of information are often unable to proactively mitigate their impacts with accurate information. Disinformation actors can exploit data voids to increase the likelihood a target will encounter disinformation without accurate information for context thus increasing the likelihood the content is seen as true or authoritative.[1] Additionally, people often perceive information that they find themselves on search engines as more credible, and it can be challenging to reverse the effects of disinformation once accepted.

Example

- In 2015 as part of its effort to undermine opponents in the Syrian Civil War, Russia exploited data voids to falsely associate a Syrian humanitarian organization with terrorism. A small number of Russia-backed sources, including state media outlets, generated hundreds of articles that were further amplified by Russian disinformation networks on social media, overwhelming search engines with influence content. Individuals searching for information about the organization were met with many narratives pushing Russia's agenda, which overwhelmed accurate authoritative information sources that appeared lower down in search results.[2]

Calls to Action

- Review website analytics to see what terms people use to surface your organization's website on search engines.
- Proactively consider hashtags and trending topics on social media to identify emerging narratives that may be exploited by data voids.
- Transition official government websites to the .gov top-level domain and seek verification of official social media accounts to communicate to your audience that your organization is a credible source of information.
- Utilize search engine optimization techniques to raise the visibility of your website in search results.

[1] Golebiewski, Michael, and Danah Boyd. "Data Voids: Where Missing Data Can Easily Be Exploited." Data & Society, October 29, 2019. https://datasociety.net/wp-content/uploads/2018/05/Data_Society_Data_Voids_Final_3.pdf.

[2] Sohn, Olivia. "How Syria's White Helmets Became Victims of an Online Propaganda Machine." The Guardian. Guardian News and Media, December 18, 2017. https://www.theguardian.com/world/2017/dec/18/syria-white-helmets-conspiracy-theories.

TACTICS OF DISINFORMATION:

Manipulate Unsuspecting Actors

Disinformation actors use a variety of tactics to influence others, stir them to action, and cause harm. Understanding these tactics can increase preparedness and promote resilience when faced with disinformation.

While this document discusses open-source examples of disinformation attributed by others to foreign governments, it does not represent the U.S. government confirming the accuracy of any such attribution.

Description

Disinformation campaigns target prominent individuals and organizations to help amplify their narratives. These secondary spreaders of disinformation narratives add perceived credibility to the messaging and help seed these narratives at the grassroots level while disguising their original source. Targets are often unaware that they are repeating a disinformation actors' narrative or that the narrative is intended to manipulate. The content is engineered to appeal to their and their follower's emotions, causing the influencers to become unwitting facilitators of disinformation campaigns.

Examples

- In 2016, the Russian Internet Research Agency conducted a campaign to spread divisive content and covertly recruited U.S. persons across the political spectrum to unknowingly amplify this content. Then again in 2020, the Russian Internet Research Agency deployed a campaign to covertly recruit unwitting journalists to write freelance for fabricated news outlets.[1]

- In August 2021, Facebook removed several accounts connected to a UK marketing firm for its Russian-linked operations. Starting in 2020, several fake accounts were created and began posting memes and comments claiming the AstraZeneca COVID-19 vaccine would turn recipients into chimpanzees. The hashtags and petitions associated with these accounts were then shared by several health and wellbeing influencers. The UK firm allegedly also contacted influencers on YouTube, Instagram, and TikTok to ask them to push anti-vaccine content for payment.[2]

- Following the United States' "diplomatic boycott" of the 2022 Winter Olympics in Beijing, China hired a U.S.-based public relations firm to discreetly recruit social media influencers in the U.S. to amplify positive messaging, including disinformation, about China and the competition. Influencers were chosen to reach target audience segments with content that deflects from allegations of human rights abuses in China. Many posts did not properly attribute their sponsorship, a violation of platform requirements that increased the seemingly organic content's credibility.[3]

Calls to Action

- Educate organization leadership on how their personal and professional social media presence may be targeted to spread disinformation.
- Inoculate audiences against grassroots disinformation campaigns by proactively debunking or "prebunking," potential disinformation narratives related to your work.
- Encourage followers to verify sources and assess before sharing content further on social media.

[1] Nimmo, Ben, Camille Francois, C. Shawn Eib, and Lea Ronzaud. Rep. IRA Again: Unlucky Thirteen: Facebook Takes Down Small Recently Created Network Linked to Internet Research Agency. Graphika, 2020.
[2] Elizabeth Culliford, Facebook removes Russian network that targeted influencers to peddle anti-vax messages. Reuters, 2021
[3] Seitz, Amanda, Mike Catalini, and Eric Tucker. "China Used TV, TikTok Stars in Discreet Olympics Campaign." AP NEWS. Associated Press, April 8, 2022. https://apnews.com/article/entertainment-technology-business-sports-travel-ebd23980015ffa35b60dbb0348e9ca62.

TACTICS OF DISINFORMATION:

Spread Targeted Content

Disinformation actors use a variety of tactics to influence others, stir them to action, and cause harm. Understanding these tactics can increase preparedness and promote resilience when faced with disinformation.

While this document discusses open-source examples of disinformation attributed by others to foreign governments, it does not represent the U.S. government confirming the accuracy of any such attribution.

Description

Disinformation actors surveil a targeted online community to understand its worldview, interests, and key influencers and then attempt to infiltrate it by posting tailored influence content likely to resonate with its members. By starting with entertaining or non-controversial posts that are agreeable to targeted communities, disinformation actors gain "insider" status and grow an online following that can make future manipulation efforts more successful. This tactic may be used in combination with cultivating fake experts, who spread targeted content over time, taking a "long game" approach that lends false credibility to the campaign. Targeted content often takes highly shareable forms, like memes or videos, and can be made to reach very specific audiences by methods such as paid advertising and exploited social media algorithms.

Examples

- In its effort to sow division within the United States during the 2016 presidential election, the Russian Internet Research Agency (IRA) deployed a vast network of inauthentic social media accounts, pages, and groups to target specific American communities, including racial and ethnic groups and adherents to specific political movements or ideologies. For example, the IRA attempted to discourage participation among Black Americans in the electoral process by creating an ecosystem of connected fake accounts posing as media outlets. The network of fake accounts pushed repetitive narratives and sometimes manipulated legitimate influencers into amplifying its content, lending it the appearance of insider status within the community.[1]
- An extensive, pro-China network of inauthentic online accounts has expanded efforts to target global audiences in recent years. The operation has spread to dozens of social media platforms and websites, including alternative forums catering to niche audiences, and has deployed disinformation content in at least seven languages, including Russian and Spanish. Like the IRA efforts, many of the accounts in the pro-China network shared the same content and linked to in-network accounts on other platforms. The targeted content often seeks to spur real-world action. For example, in April 2020, content targeting Asian Americans sought to mobilize protests within the U.S. against findings that COVID-19 originated in China.[2]

Calls to Action

- Understand how your audience receives their information, including platforms and trusted sources.
- Assess prior disinformation that has affected your sector and other potential vulnerabilities.
- Clearly and creatively communicate accurate information through channels and media that are likely to appeal to specific segments of your audience.
- Invest in clear and concise content on official websites to serve as accurate and verified reference information. Direct users to this content if disinformation campaigns emerge and ensure key stakeholder questions are addressed in user-centered language and framing.
- Develop an incident response plan to mitigate the impacts of significant disinformation narratives.

[1]DiResta, Renee, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson. "The Tactics & Tropes of the Internet Research Agency." DigitalCommons@University of Nebraska - Lincoln, October 2019. https://digitalcommons.unl.edu/senatedocs/2/.

[2] Serabian, Ryan, and Lee Foster. "Pro-PRC Influence Campaign Expands to Dozens of Social Media Platforms, Websites, and Forums in at Least Seven Languages, Attempted to Physically Mobilize Protesters in the U.S." Mandiant. Mandiant, September 7, 2021. https://www.mandiant.com/resources/pro-prc-influence-campaign-expands-dozens-social-media-platforms-websites-and-forums.