
Advanced Certificate in Digital Disinformation and Geopolitical Counter Narratives

Online Platform Manipulation Tactics

A/B Testing refers to a method of comparing two versions of a web page, online platform, or application to determine which one performs better in terms of user engagement, conversion rates, or other key metrics. This tactic is often used in online platform manipulation to identify the most effective ways to influence user behavior. Related terms include user experience, conversion rate optimization, and click-through rates. For instance, a social media platform may use A/B testing to compare the effectiveness of different ad formats, such as image-based ads versus video-based ads, to determine which one is more likely to engage users and increase click-through rates.

Account Takeover refers to the act of gaining unauthorized access to someone's online account, often through phishing or other types of cyber attacks. This tactic is commonly used in online platform manipulation to spread disinformation or propaganda. Related terms include password cracking, session hijacking, and identity theft. For example, an attacker may use account takeover to gain access to a social media influencer's account and use it to spread fake news or misinformation to their followers.

Ad Tech refers to the technology used to deliver, manage, and optimize online advertising campaigns. This includes tools for ad targeting, ad placement, and ad measurement. Related terms include programmatic advertising, real-time bidding, and data management platforms. For instance, an online publisher may use ad tech to deliver targeted ads to users based on their behavioral data, such as browsing history and search queries.

Affiliate Marketing refers to a form of online marketing that involves promoting products or services from another company and earning a commission on sales or referrals. This tactic is often used in online platform manipulation to promote fake or low-quality products. Related terms include influencer marketing, content marketing, and performance-based marketing. For example, an affiliate marketer may promote a fake weight loss supplement on social media, using fake testimonials and misleading claims to convince users to buy the product.

Algorithmic Biases refer to the biases that are built into algorithms used in online platforms, such as search engines or social media feeds. These biases can result in discriminatory or unfair outcomes, such as promoting certain types of content over others. Related terms include algorithmic transparency, data quality, and fairness metrics. For instance, a search engine's algorithm may be biased towards promoting established brands over smaller, independent websites, making it harder for new businesses to reach users.

Amplification refers to the tactic of using online platforms to amplify certain types of content or messages, often to manipulate public opinion or perception. This can include using bots or other types of automated accounts to spread content quickly. Related terms include disinformation campaigns, propaganda efforts,

and social media manipulation. For example, a state-sponsored actor may use amplification to spread fake news or propaganda on social media, using bots and other automated accounts to reach a large audience.

Anonymity refers to the ability to remain anonymous online, often through the use of VPNs, proxies, or other types of anonymization tools. This tactic is often used in online platform manipulation to hide one's identity or location. Related terms include online privacy, data protection, and cyber security. For instance, a whistleblower may use anonymity to leak sensitive information online, without revealing their identity or location.

Astroturfing refers to the tactic of creating fake or artificial online communities or movements, often to manipulate public opinion or perception. This can include using bots or other types of automated accounts to create the illusion of grassroots support. Related terms include disinformation campaigns, propaganda efforts, and social media manipulation. For example, a company may use astroturfing to create the illusion of public support for a controversial product or policy, using fake online accounts to create a fake grassroots movement.

Authentication refers to the process of verifying the identity of users or devices online, often through the use of passwords, biometrics, or other types of authentication methods. This tactic is often used in online platform manipulation to prevent unauthorized access or identity theft. Related terms include authorization, identity management, and access control. For instance, a social media platform may use authentication to verify the identity of users, using two-factor authentication to prevent account takeover.

Behavioral Targeting refers to the tactic of targeting online ads or content based on a user's behavioral data, such as their browsing history, search queries, or purchase history. This can include using cookies or other types of tracking technologies to collect data on user behavior. Related terms include personalization, ad targeting, and data driven marketing. For example, an online retailer may use behavioral targeting to deliver ads to users based on their browsing history, such as showing ads for products they have previously viewed.

Bot Farms refer to networks of bots or other types of automated accounts that are used to manipulate online platforms, often for malicious purposes such as spreading disinformation or propaganda. Related terms include botnets, scripted attacks, and automated threats. For instance, a state-sponsored actor may use a bot farm to spread fake news or propaganda on social media, using thousands of automated accounts to reach a large audience.

Clickbait refers to online content that is designed to attract attention and encourage clicks, often through the use of sensational or mysterious headlines. This tactic is often used in online platform manipulation to drive traffic to a website or landing page. Related terms include native advertising, content marketing, and social media optimization. For example, a website may use clickbait to attract users to a fake news article, using a sensational headline to encourage clicks.

Content Marketing refers to the tactic of creating and distributing valuable or relevant content to attract and engage with a target audience. This can include using blog posts, videos, or social media posts to build

brand awareness or drive traffic to a website. Related terms include inbound marketing, native advertising, and storytelling. For instance, a company may use content marketing to create a series of educational videos on a topic related to their product or service, using social media to promote the videos and attract new customers.

Cookie Tracking refers to the tactic of using cookies or other types of tracking technologies to collect data on user behavior, such as their browsing history or search queries. This can include using first-party cookies or third-party cookies to track user behavior across multiple websites. Related terms include data collection, behavioral targeting, and online privacy. For example, a website may use cookie tracking to collect data on user behavior, using cookies to track which pages users visit and how long they stay on the site.

Crisis Mapping refers to the process of identifying and analyzing potential crises or threats to an organization or individual, often using data analytics or social media monitoring tools. This tactic is often used in online platform manipulation to anticipate and respond to crises or threats. Related terms include risk assessment, crisis communication, and reputation management. For instance, a company may use crisis mapping to identify potential crises or threats to their reputation, using social media monitoring tools to track conversations about their brand.

Crowdsourcing refers to the tactic of soliciting ideas or contributions from a large group of people, often through online platforms or social media. This can include using crowdfunding platforms to raise money for a project or cause. Related terms include open innovation, participatory culture, and collaborative problem-solving. For example, a company may use crowdsourcing to solicit ideas for a new product or service, using social media to engage with customers and gather feedback.

Cyber Attack refers to a type of malicious activity that is designed to compromise or disrupt online systems or infrastructure. This can include using viruses, worms, or other types of malware to infect computers or steal data. Related terms include hacking, phishing, and cyber security. For instance, a state-sponsored actor may use a cyber attack to disrupt a country's critical infrastructure, such as their power grid or financial systems.

Data Brokers refer to companies that collect, analyze, and sell data on individuals or organizations, often for use in targeted advertising or marketing campaigns. This can include using publicly available data or proprietary data sources to build detailed profiles of individuals or organizations. Related terms include data collection, data mining, and privacy concerns. For example, a data broker may collect publicly available data on individuals, such as their social media profiles or online search history, to build detailed profiles for use in targeted advertising campaigns.

Deepfakes refer to fake or manipulated digital content, such as videos, audio recordings, or images, that are designed to deceive or mislead users. This can include using artificial intelligence or machine learning algorithms to create realistic but fake digital content. Related terms include disinformation, propaganda, and media manipulation. For instance, a state-sponsored actor may use deepfakes to create fake videos or

audio recordings that appear to show a public figure or official saying or doing something that they did not actually say or do.

Digital Footprint refers to the trail of data or information that an individual or organization leaves behind online, often through their online activities or behavior. This can include using cookies or other types of tracking technologies to collect data on user behavior. Related terms include online privacy, data collection, and identity management. For example, an individual's digital footprint may include their search history, browsing history, or social media activity, which can be used to build a detailed profile of their online behavior.

Disinformation refers to false or misleading information that is spread intentionally, often to manipulate or deceive users. This can include using fake news articles, propaganda, or other types of manipulative content to influence public opinion or perception. Related terms include misinformation, propaganda, and media manipulation. For instance, a state-sponsored actor may use disinformation to spread fake news or propaganda on social media, using bots or other automated accounts to reach a large audience.

Domain Manipulation refers to the tactic of manipulating domain names or websites to deceive or mislead users, often for malicious purposes such as phishing or cyber attacks. This can include using typosquatting or domain squatting to create fake websites that appear to be legitimate. Related terms include cyber security, domain name system, and website security. For example, a hacker may use domain manipulation to create a fake website that appears to be a legitimate online banking site, using typosquatting to trick users into entering their login credentials.

Echo Chambers refer to online communities or groups that are characterized by a lack of diversity and a homogeneous view of the world, often resulting in the amplification of certain ideas or beliefs. This can include using social media algorithms to create filter bubbles that reinforce a user's existing beliefs or views. Related terms include social media manipulation, disinformation, and propaganda. For instance, a social media platform may create an echo chamber by using algorithms to show users content that reinforces their existing beliefs or views, rather than exposing them to diverse or contrarian viewpoints.

Fake News refers to false or misleading news articles or reports that are spread online, often to manipulate or deceive users. This can include using satirical or parodic content to mock or criticize certain individuals or groups. Related terms include disinformation, propaganda, and media manipulation. For example, a website may publish fake news articles that appear to be legitimate, using sensational headlines and misleading information to attract attention and engagement.

Geotargeting refers to the tactic of targeting online content or ads based on a user's geographic location, often using IP addresses or GPS data to determine a user's location. This can include using geofencing or location-based targeting to deliver content or ads to users in a specific area or region. Related terms include location-based marketing, mobile advertising, and context-aware targeting. For instance, a company may use geotargeting to deliver ads to users in a specific city or region, using IP addresses or GPS data to

determine a user's location.

Hactivism refers to the use of hacking or other types of cyber activism to promote social or political change, often through the use of online protests or campaigns. This can include using DDoS attacks or website defacement to draw attention to a cause or issue. Related terms include cyber protest, online activism, and hacktivism. For example, a group of hacktivists may use DDoS attacks to protest against a government or corporation, using online platforms to coordinate their efforts and draw attention to their cause.

Identity Theft refers to the act of stealing or misusing someone's identity or personal data, often for financial or personal gain. This can include using phishing or other types of cyber attacks to steal sensitive information such as passwords or credit card numbers. Related terms include data breach, identity fraud, and cyber security. For instance, a hacker may use identity theft to steal someone's login credentials, using phishing or other types of cyber attacks to gain access to their online accounts.

Influencer Marketing refers to the tactic of partnering with influencers or content creators to promote products or services to their followers or audience. This can include using sponsored content or product placements to reach a target audience. Related terms include content marketing, social media marketing, and influencer relations. For example, a company may partner with a social media influencer to promote their product or service, using sponsored content or product placements to reach their followers.

Information Operations refers to the use of information or disinformation to influence or manipulate public opinion or perception, often for strategic or competitive advantage. This can include using propaganda or disinformation to shape public opinion or influence decision-making. Related terms include psychological operations, information warfare, and strategic communication. For instance, a state-sponsored actor may use information operations to spread disinformation or propaganda on social media, using bots or other automated accounts to reach a large audience.

Malware refers to malicious software or code that is designed to harm or exploit online systems or infrastructure, often for financial or personal gain. This can include using viruses, worms, or other types of malware to infect computers or steal data. Related terms include cyber attack, hacking, and cyber security. For example, a hacker may use malware to infect a computer or steal sensitive information, using phishing or other types of cyber attacks to gain access to the system.

Microtargeting refers to the tactic of targeting online content or ads to specific individuals or groups, often using data analytics or machine learning algorithms to identify and reach target audiences. This can include using cookies or other types of tracking technologies to collect data on user behavior. Related terms include behavioral targeting, personalization, and data-driven marketing. For instance, a company may use microtargeting to deliver ads to specific individuals or groups, using data analytics to identify and reach their target audience.

Native Advertising refers to the tactic of using native ads or sponsored content to promote products or services online, often in a way that is seamless or integrated with the surrounding content. This can include

using sponsored content or product placements to reach a target audience. Related terms include content marketing, influencer marketing, and branded content. For example, a company may use native advertising to promote their product or service, using sponsored content or product placements to reach their target audience.

Online Harassment refers to the act of harassing or intimidating someone online, often through the use of abusive language or threats. This can include using social media or other online platforms to stalk or harass someone. Related terms include cyberbullying, online abuse, and digital harassment. For instance, a person may use online harassment to stalk or intimidate someone, using social media or other online platforms to harass or abuse them.

Phishing refers to the act of tricking or deceiving someone into revealing sensitive information such as passwords or credit card numbers, often through the use of fake emails or websites. This can include using social engineering tactics to manipulate or deceive users. Related terms include cyber attack, identity theft, and online security. For example, a hacker may use phishing to trick someone into revealing their login credentials, using fake emails or websites to deceive them.

Propaganda refers to the use of information or disinformation to influence or manipulate public opinion or perception, often for strategic or competitive advantage. This can include using propaganda or disinformation to shape public opinion or influence decision-making. Related terms include information operations, psychological operations, and strategic communication. For instance, a state-sponsored actor may use propaganda to spread disinformation or propaganda on social media, using bots or other automated accounts to reach a large audience.

Psychological Operations refers to the use of psychological tactics or techniques to influence or manipulate public opinion or perception, often for strategic or competitive advantage. This can include using propaganda or disinformation to shape public opinion or influence decision-making. Related terms include information operations, psychological warfare, and strategic communication. For example, a state-sponsored actor may use psychological operations to spread disinformation or propaganda on social media, using bots or other automated accounts to reach a large audience.

Search Engine Optimization (SEO) refers to the tactic of optimizing websites or online content to rank higher in search engine results pages (SERPs), often through the use of keywords, meta tags, and other optimization techniques. This can include using black hat SEO tactics to manipulate or deceive search engines. Related terms include digital marketing, online advertising, and search engine marketing. For instance, a company may use SEO to optimize their website for certain keywords, using meta tags and other optimization techniques to improve their ranking in search engine results pages.

Social Engineering refers to the tactic of using psychological manipulation or deception to influence or manipulate individuals or groups, often for malicious purposes such as identity theft or financial fraud. This can include using phishing or other types of cyber attacks to trick or deceive users. Related terms include

cyber attack, identity theft, and online security. For example, a hacker may use social engineering to trick someone into revealing sensitive information, using phishing or other types of cyber attacks to deceive them.

Social Media Manipulation refers to the tactic of using social media platforms to manipulate or influence public opinion or perception, often for strategic or competitive advantage. This can include using bots or other automated accounts to spread disinformation or propaganda on social media. Related terms include information operations, psychological operations, and strategic communication. For instance, a state-sponsored actor may use social media manipulation to spread disinformation or propaganda on social media, using bots or other automated accounts to reach a large audience.

Spear Phishing refers to the act of targeting specific individuals or groups with phishing attacks, often using personalized or tailored emails or messages to trick or deceive them. This can include using social engineering tactics to manipulate or deceive users. Related terms include cyber attack, identity theft, and online security. For example, a hacker may use spear phishing to target a specific individual or group, using personalized emails or messages to trick or deceive them.

SQL Injection refers to the act of injecting or inserting malicious code into a database or website, often to extract or manipulate sensitive data. This can include using SQL injection attacks to compromise or disrupt online systems or infrastructure. Related terms include cyber attack, hacking, and cyber security. For instance, a hacker may use SQL injection to inject malicious code into a database or website, using SQL injection attacks to extract or manipulate sensitive data.

Troll Farms refer to networks of trolls or other types of automated accounts that are used to manipulate or disrupt online discussions or conversations, often for malicious purposes such as spreading disinformation or propaganda. Related terms include disinformation campaigns, propaganda efforts, and social media manipulation. For example, a state-sponsored actor may use troll farms to spread disinformation or propaganda on social media, using trolls or other automated accounts to manipulate or disrupt online discussions.

URL Redirection refers to the act of redirecting or <