

Disinformation & Manipulation

AnnexVault LLC
Groundhog Research Group™

Original publication: April 2025
Revised: 26 October 2026

Cyber Threat Intelligence (CTI) is critical for identifying and mitigating cyber threats. However, malicious actors use disinformation (deliberately false information) and manipulation tactics to compromise CTI systems, mislead analysts, and disrupt defense mechanisms. Understanding these risks is essential for improving the integrity of CTI operations.

Why this matters to AnnexVault

This report focuses on information integrity, source trust, and influence risk. Those conditions affect how analysts interpret evidence and confidence.

Tactics of Disinformation and Manipulation in CTI

Disinformation Techniques

1. **False Indicators of Compromise (IOCs):** Misleading data to mask attackers or misdirect investigations.
2. **Fake Attribution:** Assigning responsibility to incorrect groups, often to stir geopolitical tensions.
3. **Misinformation Campaigns:** Spreading rumors or inaccurate analysis to erode trust in legitimate intelligence.

Manipulation Methods

1. **CTI Feed Tampering:** Compromising intelligence feeds to insert misleading information.
2. **Data Poisoning:** Infiltrating machine-learning systems to reduce detection accuracy.
3. **Noise Amplification:** Overloading CTI platforms with irrelevant data to obscure real threats.

Impacts of Disinformation and Manipulation

- **Erosion of Trust:** Organizations may lose confidence in CTI platforms and providers.
- **Resource Wastage:** Responding to false alarms or investigating fabricated threats diverts resources from real issues.
- **Disruption of Collaboration:** Shared intelligence networks are less effective when disinformation spreads.

Case Studies:

- **2016 U.S. Election Interference:** Cyber campaigns amplified by disinformation on social media platforms.
- **False Flag Operations:** Advanced Persistent Threat (APT) groups framing others to avoid detection and mislead investigations.

Defensive Strategies

- **Source Verification:** Cross-check intelligence with multiple trusted sources to ensure accuracy.
- **Automated Validation Tools:** Use AI/ML systems to assist anomaly detection, with human validation and checks for false positives.
- **Collaborative Intelligence Sharing:** Engage in trusted forums like ISACs to validate information.
- **Awareness Training:** Educate teams to identify and mitigate disinformation tactics.

Disinformation in financial systems refers to the intentional spread of false information to influence market behaviors, destabilize economies, or achieve strategic objectives. Manipulation involves deliberate actions, such as exploiting market inefficiencies or leveraging misinformation for financial gain or geopolitical advantage. Both tactics threaten financial stability and investor trust.

Key Example

- **Market Manipulation:** Dissemination of false reports about corporate performance or economic policies to influence stock or currency prices.
- **Social Media Campaigns:** Coordinated false or misleading investment claims, including pump-and-dump schemes. Social-media interest or a short squeeze alone does not establish misinformation. [2]
- **Algorithmic Manipulation:** Spoofing and layering can create a false appearance of trading interest. High-frequency trading is not inherently manipulative. [1]
- **State-Sponsored Disinformation:** Countries engage in economic warfare by spreading propaganda targeting rival economies or currencies.

Impacts

- **Market Instability:** Loss of investor confidence, rapid devaluation of assets, and liquidity crises.
- **Economic Destabilization:** Systemic risks to financial institutions and markets, exacerbating economic downturns.
- **National Security Risks:** Disinformation campaigns can undermine sovereign debt markets or currency stability.

Defense Mechanisms

1. **Regulation and Oversight:**
 - Securities laws such as the U.S. **SEC** rules and the EU's **Market Abuse Regulation (MAR)** combat disinformation and manipulation.

2. Technological Countermeasures:

- **AI-driven monitoring** systems detect and flag anomalies in trading and online narratives.
- **Blockchain technology** can make recorded transactions traceable, but does not by itself establish that off-chain claims are true.

3. Public Awareness:

- Education initiatives promote media literacy and awareness of financial scams.

4. Corporate Defenses:

- Rapid response teams address misinformation, while cybersecurity controls reduce breach risk.

Emerging Threats

- **Deepfake Technology:** AI-generated media could simulate executives' voices or videos to spread false financial announcements.
- **Cryptocurrency Manipulation:** Decentralized finance (DeFi) platforms can face misinformation and manipulation risks.
- **Hybrid Warfare:** State-sponsored campaigns target financial systems as a component of broader geopolitical conflicts.

Healthcare and pharmaceutical communication can be affected by false or misleading claims. In a randomized UK/US study, exposure to COVID-19 vaccine misinformation reduced stated vaccination intent relative to factual information. This finding concerns intentions in that study, not a direct measure of real-world vaccination or health outcomes. [9]

Relevant risks include false vaccine claims and misleading communications about medicines. Drug pricing and the opioid crisis should not be classified wholesale as disinformation without evidence about a specific claim or practice.

Critical infrastructure, encompassing sectors such as energy, healthcare, transportation, and communication, is increasingly vulnerable to disinformation and manipulation. These tactics exploit societal, technical, and operational vulnerabilities to disrupt essential systems and erode public trust.

Key Areas of Impact

Public Trust and Perception

1. **Erosion of Trust:** Disinformation undermines confidence in infrastructure reliability (e.g., vaccine logistics during COVID-19).
2. **Panic Inducement:** False narratives about outages or contamination create unnecessary fear, such as during natural disasters.

Cyber Manipulation

1. **False Alarms:** Cyber attackers use fake warnings or ransom claims to amplify impact.
2. **Operational Data Alteration:** Manipulated data misleads operators, causing potentially harmful decisions (e.g., water treatment settings).

Election Infrastructure

1. **Confidence Undermining:** False claims of voter fraud compromise trust in results.
2. **Voter Suppression:** False information about polling logistics can obstruct participation; this report does not quantify its effect on turnout.

Energy Sector Disinformation

1. **Pipeline Attacks:** The 2021 Colonial Pipeline disruption illustrates the need for accurate emergency communication. DOE advised rumor control and discouraging panic buying; this does not establish a coordinated disinformation campaign as the cause. [3]
2. **Climate Narratives:** Misinformation about energy sources hampers critical advancements.

Social Engineering

- **Phishing and Influence Campaigns:** Manipulating insiders through targeted communication.

Tactics and Tools

- **Bots and Trolls:** Amplify disinformation on social platforms.
- **Deepfakes:** Convincing yet false content targeting stakeholders.
- **Fake News Websites:** Dissemination of fabricated reports.
- **Data Breach Exploitation:** Leaked or altered data misused to incite distrust.

Case Studies

- **2016 U.S. Election:** The Senate Intelligence Committee documented the Internet Research Agency's social-media campaign to sow discord and influence the 2016 election. This is distinct from a claim that voting systems were altered. [4]

Mitigation Strategies

- **Public Awareness:** Educating citizens to verify sources and identify disinformation.
- **Rapid Response Protocols:** Addressing misinformation in real time.
- **Technological Solutions:** AI-assisted screening of possible fake content, bots, and deepfakes, followed by validation.

- **Collaborative Efforts:** Coordination between governments, private sectors, and international bodies.

Scope and evidence

This is a qualitative background report, not an original empirical study, a validated prediction method or a product-performance evaluation. Sector examples describe possible risks unless a named source is cited. Recommended controls require contextual assessment; they do not guarantee prevention. Updated 26 October 2026 from the report originally dated 1 April 2025.

References

- [1] SEC staff, Algorithmic Trading in U.S. Capital Markets (2020)
- [2] SEC, Social Media and Investment Fraud (2022)
- [3] DOE, State Resources for Colonial Pipeline Disruption (2021)
- [4] U.S. Senate Intelligence Committee, Russia's use of social media (2019)
- [9] Loomba et al., COVID-19 vaccine misinformation and vaccination intent (2021)
- [13] NIST SP 800-53 Rev. 5, Security and Privacy Controls