Hybrid Threats and the Amplifying Power of AI: Five Strategic Scenarios

Organizations today face an evolving landscape of hybrid threats—coordinated, multi-vector attacks that exploit vulnerabilities across digital, operational, and information environments. These threats go beyond traditional cybersecurity concerns, integrating social engineering, economic pressure, and AI-enhanced deception to manipulate decision-making and erode institutional trust.

The AI-Driven Threat Multiplier

The rapid advancement and democratization of generative AI have amplified these risks. Malicious actors leverage AI to create scalable, highly personalized attacks, from synthetic identity fraud to AI-generated disinformation campaigns. As the accessibility of these tools increases, so does the sophistication of threats across sectors, impacting businesses, governments, and civil society.

Five Strategic Risk Scenarios

To help organizations navigate this evolving threat landscape, we introduce a model of five AI-driven risk scenarios, each reflecting critical challenges faced by industries today. These scenarios highlight how hybrid threats—enabled by generative AI—can manifest in financial markets, corporate operations, public affairs, and beyond.

Understanding and mitigating these risks requires a proactive approach. Organizations must enhance their monitoring, detection, and response capabilities to stay ahead of AI-enabled threats.

Understanding The AI Hybrid Threat Multiplier

At their core, hybrid threats are designed to exploit vulnerabilities across multiple sectors simultaneously. Their goal isn't simply to breach systems – it's to shake confidence in institutions, distort decision-making processes, and ultimately destabilize markets or entire societies.

The actors behind these threats exhibit two key characteristics:

- **They operate below detection thresholds, exploiting delays in response systems**
- **They actively avoid attribution through technical sophistication, proxy use, or by manipulating unwitting third parties (often called "useful idiots")**

Our approach to understanding these threats involves carefully mapping how these characteristics intersect with AI capabilities, with particular attention to the information domain where generative AI has had such a transformative impact. AI has fundamentally reshaped the hybrid threat landscape by enabling attacks that are more scalable, automated, and customized than ever before. Through our analysis of open-source AI model availability, we've observed these tools becoming increasingly accessible to non-state and criminal actors, and this evolution is particularly evident in two areas:

1

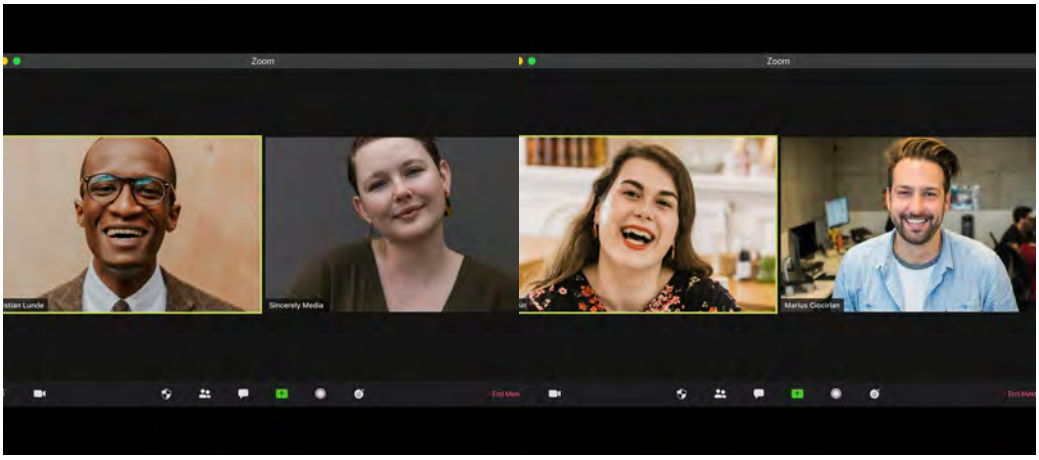
Automated Cyber and Social Engineering Operations

AI now enables highly personalized phishing attacks and malware development, significantly reducing operational costs for attackers

2

Generative AI and Sophisticated Deception

Generative AI has revolutionized how false narratives are created through realistic deepfakes, synthetic identities, and fabricated interactions



Realistic identities are increasingly being generated by AI (Source: Unsplash)

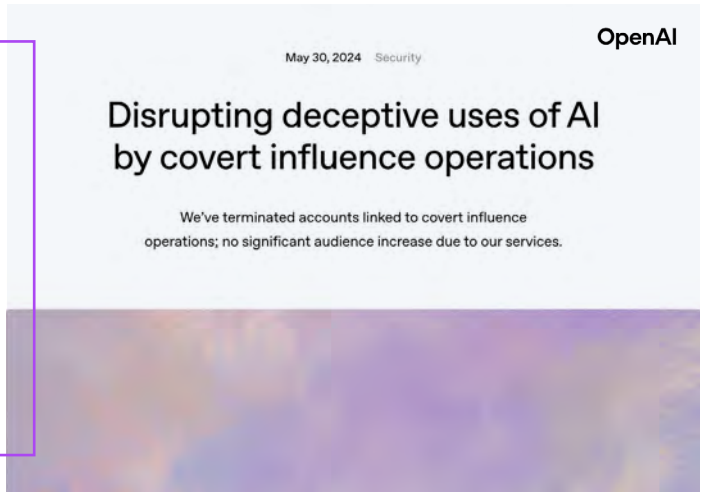
The Deepfake Dimension

The term “deepfake,” while non-technical, has become widely understood to describe AI-generated videos, audio, and images that convincingly depict individuals saying or doing things they never did. The implications for privacy, reputation, and commercial integrity are profound. The evolution of this threat has been rapid:

2017 marked the emergence of deepfake videos through “face-swap” content involving celebrities, seeing significant early usage in the creation of explicit pornographic and adult content.

By 2023-2024, major regulatory bodies including the FTC, NSA, FBI, and CISA had issued formal warnings about synthetic media threats, following a joint NSA/FBI/CISA advisory in September 2023 that highlighted how these tools were becoming accessible even to low-capability malicious actors.

In February 2024, OpenAI reported on efforts to disrupt covert influence operations using AI, revealing that deceptive actors were leveraging its models for propaganda and disinformation, though with limited sophistication, and emphasizing the company’s commitment to monitoring and mitigating such misuse.



Understanding Deepfake Threat Scenarios: Key Risks and Challenges for Organizations

Our research has identified five critical scenarios where deepfakes pose significant threats across industries. Each scenario was evaluated using a comprehensive seven-dimension framework: victim, actor, scheme, attack type, technique, digital channel, and monitoring capacity. These seven key dimensions define the primary deepfake threat scenarios organizations face today, as outlined in the tables below. In many cases, detection and threat actor attribution remain challenging, making escalation a major concern for security, operations, risk, and reputation management teams.

7 Attack Dimensions

Potential Victim
Individuals, companies, markets, and governments.

Attack Actor (motivation)
State, criminal, hacktivists, or mercenaries.

Illicit Scheme
Existing or Novel; Identity theft, fraud, disinformation, and market manipulation.

Type of Attack
Segmented (Spear) or Broad (Mass)

Attack Technique
Synthetic audio, video, fabricated identities, or text.

Digital Channel
Private, restricted, and public platforms with varying levels of monitoring.

Ability to Monitor Digital Channel
Monitored – Partially Monitored - Unmonitored

5 Deepfake Threat Scenarios

Individual Victims

Identity Theft for Access or Payment

Fraudulent Impersonation for Extortion

Companies Markets Governments Victims

Falsified Events for Stock or Market Manipulation or Bank Run

Disinformation for Brand or Project Manipulation

Fake Official Government, Regulatory or Law Enforcement Intervention

Convergence of Individual- and Organization-Focused Threat Scenarios Relevant to Financial Services Today

1

Identity Theft for Access or Payment

Attackers use synthetic video or audio to impersonate high-net-worth individuals or corporate executives, authorizing fraudulent transactions or gaining access to sensitive systems.

2

Fraudulent Impersonation for Extortion

Synthetic media is used to coerce payments through threats of exposure to fabricated compromising content, such as synthetic pornography or blackmail attempts.

3

Falsified Events for Market Manipulation

Deepfakes of corporate executives making false statements or fabricated crisis events can manipulate investor sentiment, trigger stock price volatility, or fuel mass withdrawals in financial institutions.

4

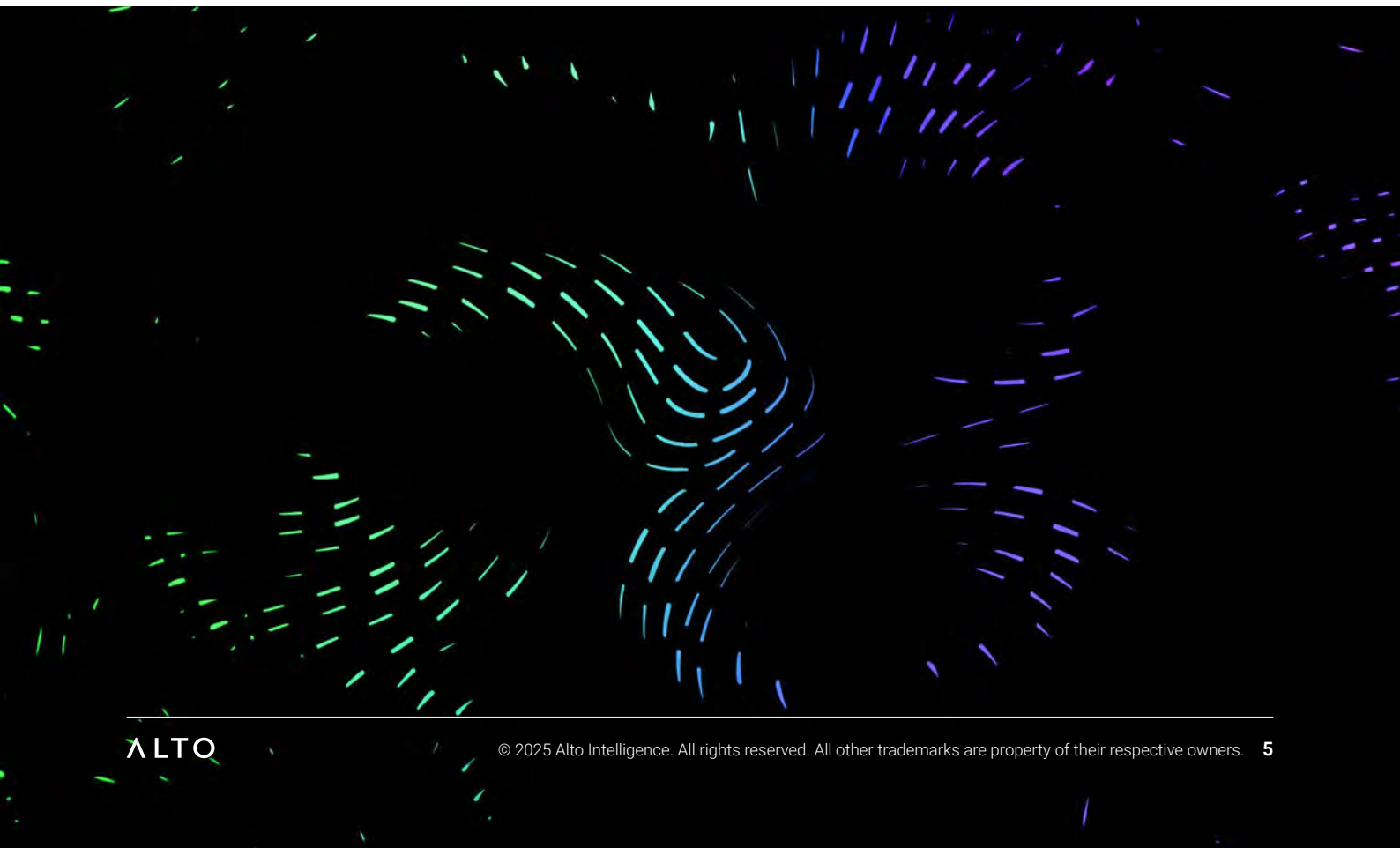
Disinformation Targeting Brands and Projects

Synthetic media campaigns create artificial grassroots movements, alter public perception, and damage brand reputation by spreading false narratives.

5

Fake Government or Regulatory Announcements

Fabricated official statements or interventions can trigger panic, compliance responses, or operational disruptions across industries.



Implications and Path Forward

How Hybrid Threats and AI-Driven Deception Through Synthetic Media and Identities Are Already Reshaping Risk for Global Financial Institutions

Market Instability – Fabricated Events Manipulating Prices

AI-generated **misinformation** is already **destabilizing financial markets**. In 2023, a **fake image** of an explosion near the **Pentagon** spread on social media, briefly causing **panic** and a **U.S. stock market dip** before being debunked. This incident underscores how **synthetic media** can trigger **volatility**, as **financial algorithms** and **investor sentiment** react to **false signals** before verification catches up.

Source: AP News

Operational Disruption – Synthetic Identity & Fraud Risks

AI-powered deepfakes are **bypassing traditional security measures**. In 2024, a Hong Kong company lost **$25 million** when an employee, believing they were on a **video call** with the **CFO and colleagues**, was deceived by **deepfake-generated faces and voices**. Fraudsters are increasingly using AI-driven identity manipulation to commit **new account fraud**, **hijack existing accounts**, and execute **unauthorized transactions**. Regulatory bodies, including FINRA, have issued warnings about **synthetic identities**, **deepfake credentials**, and **AI-enhanced account takeovers**.

Source: BBC News, Financial Industry Regulatory Authority (FINRA).

Trust Erosion – Financial Institutions as Targets of AI-Driven Deception

Synthetic media is being **weaponized** to **erode institutional trust**. The 2023 collapse of **Silicon Valley Bank** demonstrated how social media-fueled panic can accelerate bank runs, a dynamic reinforced by subsequent crises. In 2024, a deepfake video of Federal Reserve Chair Jerome Powell briefly spread false information about interest rates. Regulators warn that **AI-powered campaigns** are being used to **simulate market consensus**, **manipulate investor sentiment**, and **undermine financial stability**. Reports from **Microsoft** and the **SEC** highlight **synthetic media** as a **growing threat vector**, reinforcing the urgency for **detection and mitigation strategies**.

Source: New York Times, Bloomberg, SEC Investor Alert, Microsoft Digital Defense Report 2024.

- **Strengthening Detection Capabilities to Counter AI-Enabled Hybrid Threats**

  AI-Driven Deception is Reshaping Risk—Organizations Must Evolve

  The increasing sophistication of AI-powered synthetic media and hybrid threats demands a fundamental shift in how organizations approach risk detection and mitigation. Traditional security and monitoring tools are no longer sufficient in an era where deception can be automated, scalable, and highly personalized.

- **Alto Intelligence's Recommendation: Enhance Detection Capabilities**

  To stay ahead of emerging AI threats, organizations must strengthen their early-stage detection capabilities. This means integrating AI-powered risk monitoring, cross-domain intelligence, and proactive anomaly detection into their security strategies. Key focus areas include:

  Expanding Real-Time Monitoring and Detection → Going beyond conventional cybersecurity to detect AI-generated threats across hard-to-reach sources in digital, operational, and public information spaces.

  Automating Threat Intelligence → Leveraging AI to identify synthetic content, misinformation, and coordinated manipulation before escalation.

  Cross-Sector Collaboration → Strengthening industry-wide and regulatory cooperation to align detection efforts and mitigate evolving risks.

SEE IT IN ACTION

Alto Intelligence has developed advanced detection and early-warning solutions designed to help organizations navigate this new threat landscape.

Request a demo today

Explore how Alto monitors and detects synthetic threats at scale

Annex: 5 potential scenarios - 2 focused on individuals and 3 on organizations

Scenario	Description	Potential Victim(s)	Attack Actor(s) (motivation)	Illicit Scheme	Type of Attack	Attack Technique(s)	Digital Channel	Ability to monitor Digital Channels
Identity Theft for Access or Payment	Impersonation of a wealthy individuals or corporate officials to initiate fraudulent transactions or gain digital (or physical) access which can enable larger-scale operation.	**Individuals**	**Criminal** **Mercenaries**	**Existing & Novel**	**Segmented** (Spear)	Synthetic Synchronized Video and/ or Audio for Full Identity Impersonation (Vishing)	Private Peer to Peer (Private Comms or Messaging incl. Social Networks)	**Unmonitored** channels
Fraudulent Impersonation for Extorsion	Impersonation of individuals (incl. family members) for extorsion - Scenarios include Synthetic pornography of the victim for blackmail or coercion for fraudulent payment	**Individuals**	**Criminal** **Mercenaries**	**Existing & Novel**	**Segmented** (Spear)	Synthetic Synchronized Video and/ or Audio for Full Identity Impersonation (Vishing)	Private Peer to Peer (Private Comms or Messaging incl. Social Networks)	**Unmonitored** channels
Falsified events for Stock or Market manipulation or Bank Run	Influence investor sentiment through defamation or fabrication of endorsements of corporate officials. Spreading or amplification of fabricated rumors of a market-moving event or market weakness to fuel cash withdrawal.	**Companies** **Markets**	**State** **Criminal** **Mercenaries**	**Existing & Novel**	**Broad** (Mass)	Synthetic Synchronized Video and/ or Audio for Full Identity Impersonation (Vishing) Synthetic Fabricated New Identity Synthetic Text | Documents	Restricted Public	**Monitored** channels **Partially monitored** channels
Disinformation for Brand or Project manipulation	Human-like digital activity that attack or promote a brand or project altering perception of consumer or civil society sentiment in order to manipulate decision making process.	**Companies** **Governments**	**State** **Criminal** **Mercenaries** **Activism or Hackactivism**	**Existing**	**Broad** (Mass)	Synthetic Fabricated New Identity Synthetic Images or Videos Synthetic Text | Documents	Restricted Public	**Monitored** channels **Partially monitored** channels
Fake Official Government, Regulatory or Law enforcement Intervention	Fake imminent action from Government, Regulation or Law Enforcement.	**Companies** **Markets** **Governments**	**State** **Criminal** **Mercenaries**	**Existing & Novel**	**Broad** (Mass)	**S**ynthetic Synchronized Video & Audio for Full Identity Impersonation Synthetic Audio for Voice Impersonation (Vishing) Synthetic Fabricated New Identity Synthetic Images or Videos Synthetic Text | Documents	Public	**Monitored** channels