Deepfakes and Synthetic Media: The Emerging Threat to Large-Scale Public Gatherings

May 2026

Overview

Artificial intelligence (AI)-enabled synthetic media, including deepfake audio, video, imagery, and text, has emerged as one of the most consequential additions to the threat environment for large-scale public gatherings. Generative AI (GenAI)* tools capable of producing highly realistic but fabricated content have become widely accessible since 2020, sharply lowering the barrier to entry for sophisticated influence operations.[1, 2, 3] Since 2021, the Federal Bureau of Investigation (FBI) has assessed that malicious actors will almost certainly leverage synthetic content to conduct cyber and foreign influence operations, expanding on traditional tactics with greater speed, persuasiveness, and scale.[4, 5]

Large-scale mass gatherings, including concerts, festivals, political conventions, and sporting events, to include the FIFA World Cup 2026 (FWC26), present especially attractive targets. These venues concentrate large, emotionally charged audiences within compressed information environments where rapid perception shifts can generate disproportionate psychological, operational, and reputational effects. Initial threat reporting on the FWC26 indicates cyber threat activity is already underway, with deepfake and AI-generated content cited as primary vectors for false or misleading narratives, panic induction, and political influence, and in some cases the ability to inspire or facilitate real-world disruptive or violent activity, including swatting incidents and other hoax threats.[6] Threats may involve not only fully synthetic deepfakes, but also hybrid manipulations that alter authentic content in ways that may be harder to detect and easier to weaponize.[7]

This whitepaper characterizes the deepfake and synthetic media threat to large-scale events, including threat actors and motivations, observed tactics, techniques, and procedures (TTPs) across pre-event, event, and post-event phases, and provides operationally relevant mitigation guidance for event organizers, law enforcement, and security practitioners. The threat environment now includes the generation of synthetic content that can overwhelm information environments, crowd out trusted signals, degrade trust in legitimate communications, and increasingly target broadcast systems, financial markets, and high-visibility individuals in real time. The growing reliance on connected digital infrastructure, including mobile ticketing, high-speed venue connectivity, and Internet of Things (IoT)-enabled services, further expands the risk surface, creating additional pathways through which manipulated, misleading, or synthetic information can influence operational systems, public communications, and real-time decision-making.[8, 9]

* AI broadly refers to systems that analyze data and perform tasks requiring human-like intelligence, while GenAI is a subset of AI that produces new content, including synthetic text, images, audio, and video such as deepfakes.

Background: The Synthetic Media Threat Landscape

Deepfakes are a subset of synthetic media produced by trained AI models, most commonly generative adversarial networks (GANs)† or diffusion models, on reference content until the output is nearly indistinguishable from authentic imagery or audio.[10, 11] Techniques include face swapping, attribute editing, face re-enactment, and the generation of fully synthetic personas. Voice-cloning capabilities can replicate a target's voice from only a few seconds of reference audio, and multimodal models can generate coordinated video, audio, and text in near real time.[12, 13, 14] The rapid expansion of generative AI and synthetic media across sectors, including communications, marketing, and journalism, has increased both the accessibility and potential misuse of these technologies, making it more difficult for individuals and organizations to distinguish between authentic and manipulated content.[15, 16]

In 2023, the Department of Homeland Security (DHS) assessed the convergence of accessibility, affordability, and realism has transformed deepfakes from a niche technical capability into a mainstream tool for fraud, extortion, political manipulation, and influence operations.[17] The increasing adoption of “smart stadium” technologies, including AI-enabled surveillance, IoT-connected sensors, mobile applications, and real-time data analytics, further expands the risk surface surrounding large-scale events, creating additional pathways through which manipulated, misleading, or synthetic information can influence operational systems, public communications, and real-time decision-making.[18]

Google's 2024 Generative AI Misuse: A Taxonomy of Tactics and Insights from Real-World Data identified opinion manipulation as the single most common goal (approximately 27 percent of cases), with impersonation, appropriated likeness, sockpuppeting,‡ and falsification as the primary tactics used to conduct opinion-manipulation campaigns.[19] The operational maturity of the threat is illustrated by incidents including, deepfake videos of Ukrainian President Volodymyr Zelenskyy during the Russia-Ukraine conflict, AI-cloned voice robocalls impersonating political figures, such as former President Biden, and a $25.6 million corporate theft executed via a deepfake video conference.[20, 21, 22, 23]

This evolution, from isolated uses of synthetic media for information operations to more coordinated, targeted influence operations leveraging AI-generated content, reflects a broader shift to cognitive warfare, in which synthetic media is used not simply to misinform, but to shape perception, erode trust, and influence how individuals think, react, and make decisions.[24, 25] According to an April 2026 report from Sensity, the adoption of deepfakes and synthetic media in information operations is accelerating faster than expected, with content generation and dissemination scaling beyond verification capabilities, and trust itself emerging as a central battleground.[26, 27]

A Working Taxonomy of Synthetic Media Threats Relevant to Large-Scale Events

Synthetic-media threats span multiple related but distinct categories, from fabricated content and manipulated authentic media to coordinated influence operations and high-volume synthetic content designed to overwhelm information environments. The following frameworks provide a common structure for understanding these threats; first by categorizing major forms of synthetic-media risk, and second by illustrating how those forms relate to operational use and broader strategic effects to support planning and analysis.

Synthetic-media threats often operate through four overlapping mechanisms:

- **Fabricate**: create false content
- **Manipulate**: alter authentic content
- **Impersonate**: mimic trusted identities
- **Flood**: overwhelm information environments

† GANs are machine learning models in which two neural networks, comprising a generator that creates synthetic data and a discriminator that evaluates its authenticity, enabling the creation of highly realistic synthetic images, video, and audio.

‡ “Sockpuppeting” refers to the use of false or deceptive online personas, including AI-generated or stolen identities, to appear authentic while amplifying narratives, manipulating discourse, or obscuring the true source of influence activity.

Table 1. Functional Taxonomy of Synthetic Media Threats

The following categories are not mutually exclusive; threat actors may combine them in layered campaigns that span multiple event phases.

Category	Description	Representative Techniques	Operational Risks at Events
Synthetic Fabrication (Fully AI-Generated)	Entirely fabricated media created by AI	Deepfake video/audio, GAN personas, synthetic personas, voice cloning	False emergency directives, impersonation, reputational attacks
Manipulated Authentic Media (Altered Reality)	Genuine content altered to mislead	Cheapfakes[§], edited clips, context manipulation, deceptive subtitling[28]	Panic induction, false misconduct claims, crowd disruption
Synthetic Impersonation and Identity Deception	Use of synthetic media to mimic trusted individuals or entities	Voice clones, avatar impersonation, synthetic executives, cloned officials	Fraud, unauthorized actions, swatting, operational deception
Synthetic Content at Scale ("AI Slop")	High-volume AI-generated content designed to flood information environments	Narrative flooding, bot amplification, synthetic spam, fake "highlights"	Information saturation, verification overload, trust erosion
Synthetic Influence and Narrative Operations	Coordinated synthetic media used as part of broader influence campaigns	Narrative pre-positioning, synthetic personas, multi-stage campaigns	Perception shaping, decision paralysis, protest/disruption mobilization
Hybrid Synthetic-Cyber/Physical Convergence	Synthetic media used to enable or amplify cyber or physical attacks	Spoofed alerts, synthetic threat reporting, cyber distraction, market manipulation	Real-world disruption, resource diversion, crisis escalation

Table 2. Synthetic Media Threats Can Be Understood Across Three Levels

The framework below provides a complementary way to view synthetic-media threats across three levels (what is manipulated, how it is used, and what effects it seeks to produce) helping connect tactics to security implications.

Level	Core Question	Examples	Primary Risks
Content Manipulation	*What is being falsified?*	Deepfakes; Cheapfakes; Synthetic personas; Voice/video cloning; AI slop	Deception, spoofing, false narratives
Operational Use	*How is it used?*	Fraud; Impersonation; Broadcast manipulation; Synthetic threat reporting; Swatting/hoax threats	Disruption, panic, operational interference
Strategic Effect	*What is it trying to produce?*	Decision paralysis; Crowd disruption; Influence over behavior; Mobilization or violence inspiration, Erode trust	Cognitive and real-world effects

§ "Cheapfakes" refer to manipulated or misleading media that do not rely on advanced AI techniques, but instead use simpler editing methods, such as altering context, splicing footage, or basic audio/visual manipulation, to create deceptive content.

Threat Actors and Motivations

A wide range of threat actors are positioned to employ synthetic media against large-scale events. Motivations and capability levels vary, but most share a common operational logic: exploit the compressed information environment to amplify disruption or shape the narrative at minimal cost.

- **State and state-aligned actors.** Russian, Chinese, and Iranian influence networks have repeatedly employed GAN-generated profile imagery and synthetic personas to amplify divisive narratives, according to multiple private-sector research reports reviewed by the FBI.[29] For example, an Iranian-linked group has been producing a series of viral AI propaganda videos mocking U.S. foreign policy and government officials, which have been shared by official Iranian government accounts.[30, 31] In 2022, Iran's Supreme Leader Ali Hosseini Khamenei's account also posted an AI-generated video depicting an assassination attempt against President Donald Trump. [32] More recently, pro-Iran networks have reportedly leveraged GenAI content and high-volume "AI slop" to amplify divisive narratives and saturate information environments, underscoring how synthetic media may be used not only for deception, but also to exacerbate tensions and shape perceptions of a host nation during a major event.[33, 34, 35] Additional examples include the Spamouflage Dragon network, a pro-Chinese communist party (CCP) online propaganda and influence operation, using AI-generated profiles to seed English-language cheapfake videos attacking U.S. policy, while Russian media promoted a deepfake video of Ukrainian President Zelenskyy in March 2022 that was briefly broadcast on hacked Ukrainian television.[36, 37] Host-country hostility, geopolitical tensions, and opportunities to exploit existing social or political tensions or contentious public narratives within a host nation make major international events attractive targets.[38]
- **Terrorist and violent extremist groups.** The National Counterterrorism Center (NCTC), DHS, and FBI jointly assessed that violent extremists are actively exploring use of GenAI for recruitment, radicalization, translation, and content creation. [39] Al-Qaida-supported and ISIS-aligned groups have published Arabic-language guides on using large language models (LLMs) and AI image generators.[40] Extremist use of deepfakes to fabricate atrocities, impersonate officials, or amplify grievances ahead of a symbolic target event remains a credible concern. Synthetic media may also be used to reinforce grievance narratives, validate perceived threats, or provide justification for mobilization, increasing the risk of individuals or small groups engaging in targeted violence.[41]
- **Transnational criminal organizations and fraud networks.** The FBI's Internet Crime Complaint Center (IC3), as well as the Financial Crimes Enforcement Network, have noted a steady rise in deepfake-enabled fraud, including real-time face-swapping in video calls, voice-cloning of executives, and synthetic identity creation to bypass Know Your Customer (KYC) checks.[42, 43] Criminal actors have also used synthetic media to amplify fear and perceptions of instability; in February 2026, Mexican cartels reportedly circulated AI-generated images portraying chaos and weakened government control following the killing of a cartel leader.[44, 45] Major events intensify commerce related to tickets, travel, and merchandise, expanding the victim pool, while also creating opportunities to exploit confusion and cause disruption.[46]
- **Hacktivists and issue-motivated actors.** Groups seeking to embarrass sponsors, delegitimize host governments, or advance specific causes have a low-cost, high-visibility tool set in GenAI. These actors may use synthetic media not only for narrative amplification and reputational attacks, but also to support protest mobilization, target sponsors, inflame grievances, or amplify disruptive activity tied to physical demonstrations.[47]
- **Opportunistic individuals**. Consumer-grade deepfake tools and commercial "deepfake-as-a-service" offerings lower the technical floor so individual actors, whether for clout, harassment, fraud, or protest, can produce convincing synthetic content in hours.

Observed and Anticipated Tactics, Techniques, and Procedures (TTPs)

Deepfake-enabled operations are increasingly designed as coordinated, multi-stage efforts to shape perception through repetition, emotional engagement, cumulative exposure, and increasingly hyper-personalized targeting that can inhibit timely decision-making.[48] These efforts often align individual pieces of content within a broader, evolving narrative rather than presenting them as isolated incidents.[49] Synthetic media threats to large-scale events can be organized by phases to support operational planning across an event lifecycle.[50, 51] Refer to *Appendix I: Risk Factors* for an overview of the operational impacts of synthetic-media threats on large-scale events.

Pre-Event Shaping Operations

- **Narrative pre-positioning.** Fabricated audio, video, or imagery seeded weeks or months in advance can prime audiences around themes such as host-nation human-rights concerns, travel safety, venue corruption, or athlete or performer misconduct, potentially contributing to protest activity, demonstrations, or coordinated disruption. These narratives may be introduced in stages, with early content establishing context or emotional framing that subsequent content reinforces and amplifies over time. Narrative formation may also increasingly be influenced through AI-mediated information channels, including conversational tools used by the public to seek information on security, travel, or host-country conditions, creating additional opportunities for manipulation or bias.[52, 53, 54]
- **Synthetic persona cultivation.** Inauthentic social media accounts using GAN-generated profile photos build apparent grassroots credibility before pivoting to event-related narratives.[55, 56] Many accounts are "aged" for months to evade platform detection.
- **Infrastructure spoofing.** Fraudulent digital assets, such as websites, domains, or communication channels, can be created to mimic legitimate organizations to deceive users and enable fraud or data theft. More than 4,300 fake FIFA-related domains have been identified since August 2025, imitating official ticketing, streaming, and merchandise platforms.[57] Approximately 36 percent of FWC26 official partners were assessed by Proofpoint in February 2026 to lack sufficient Domain-based Message Authentication, Reporting and Conformance (DMARC) protections, increasing the risk of brand impersonation and email fraud.[58]
- **Deepfake-enabled credential harvesting.** AI-generated video or voice can be used to impersonate trusted personnel and trick individuals into revealing login credentials or sensitive information.[59] Fake "customer support" video agents and voice-cloned hotline operators are being reported in connection with FWC26 ticket scams.[60]

Event Exploitation

- **Impersonation of public officials, law enforcement, or event organizers.** Real-time deepfake video and voice-clone capabilities have matured to the point that live video calls and broadcast segments can be spoofed.[61] An impersonated official issuing false evacuation orders, security alerts, or all-clear messages could directly influence crowd movement and incident response.
- **Targeting of high-visibility individuals**. Deepfake audio, video, and synthetic social media content may be used to impersonate athletes, coaches, broadcasters, or other public-facing personnel to spread false statements, manipulate narratives, influence betting markets, or generate reputational harm during high-attention live events.[62, 63]
- **Fabricated incidents and emergency messaging.** AI-generated imagery, video, audio, or spoofed emergency communications may depict fires, explosions, violent incidents, or urgent public-safety

directives at or near event locations, creating confusion, inducing panic, misdirecting resources, or triggering unnecessary response actions such as evacuations or swatting-style incidents.[64] Synthetic content may also follow real-world events, leveraging existing incidents to amplify misleading narratives and increase credibility.

- **Synthetic threat reporting and swatting.** AI-generated audio, video, or text may be used to report fabricated threats, such as active shooters, explosives, or other emergencies, prompting large-scale law enforcement responses, venue disruptions, or panic among attendees.
- **Synthetic incitement and intergroup provocation.** AI-generated or manipulated content may be used to inflame tensions between fan groups, communities, or national constituencies by fabricating crimes, insults, provocations, or security abuses attributed to another group.[65] Such content could be used before, during, or after an event to incite hostility, trigger confrontations, or contribute to disorder and targeted violence. This may include fabricated content portraying supporters from a particular country or community as committing crimes or threatening others in order to provoke hostile reactions.[66]
- **Live-stream and broadcast manipulation.** Attackers may target social media platforms and the broader broadcast ecosystem to inject deepfake or AI-generated content during events.[67, 68] Such activity can disrupt transmission, undermine the credibility of live coverage, and rapidly amplify false content through trusted channels. During the 2025 Club World Cup, for example, fake AI-generated "highlight" clips amassed millions of views before moderation intervened.[69, 70, 71] Even if disproven, synthetic visual media can exert outsized persuasive effects during time-sensitive incidents.[72]
- **Voice-cloned workforce and business process compromise.** Attackers may exploit cloned voices of venue executives, security directors, or vendors to bypass financial controls, authorize transactions, grant emergency access, or elicit sensitive operational information, extending beyond traditional phishing into real-time, high-confidence deception.[73] This technique reflects a broader pattern observed by the FBI in the corporate sector and presents a direct risk to both operational decision-making and financial integrity during live events.[74, 75, 76, 77]
- **Market manipulation and betting fraud.** Synthetic content, including fake injury reports, fabricated insider commentary, or impersonated athlete statements, may be used to influence betting markets or financial decisions tied to event outcomes, as well as deceptive marketing practices that mislead consumers and influence purchasing behavior.[78]
- **Integration with physical or cyber activity.** Synthetic media can amplify real incidents (e.g., a minor disturbance presented as a coordinated attack) or provide cover for cyber activity by distracting public-affairs and incident-response resources.

Post-Event Exploitation

- **Fabricated incidents.** Synthetic imagery or video purporting to show injuries, misconduct by security, or failures of venue infrastructure can be published following the event, after attendees have dispersed.
- **Amplification of perceived failures.** Real operational friction (transit delays, weather, isolated crowd incidents) can be exaggerated through coordinated synthetic content to undermine public confidence in event security and host-government competence.
- **The "liar's dividend."** Defendants or accused parties increasingly claim that genuinely authentic audio or video is AI-generated, complicating accountability and investigations.[79] This phenomenon is expected to grow as public awareness of deepfakes expands.[80]

Lessons Learned from High-Visibility Events

- The 2026 Milano-Cortina Winter Olympics highlighted the potential use of deepfake and manipulated media to advance geopolitical narratives and distort perceptions during a high-visibility sporting event, reinforcing concerns that major events can serve as proving grounds for synthetic-media influence operations.[81]
- The 2024 Paris Olympic Games saw pre-event AI-generated false or misleading information, copycat ticketing sites, and state-linked influence operations attempting to delegitimize the host nation.[82]
- The Qatar FIFA World Cup 2022 generated reference data on ticketing and streaming fraud that cybersecurity and intelligence entities have used to forecast the 2026 environment, including the observation that approximately 299 malicious FIFA-branded domains were registered in a single five-day window in August 2025.[83]
- The 2022 Beijing Winter Olympics were accompanied by a covert influencer-recruitment campaign using Chinese state-linked public relations firms and AI-generated content to deflect human-rights criticism.[84]
- The Russia-Ukraine conflict produced widely observed wartime deepfakes (e.g., Zelenskyy surrender video), demonstrating the tactic's viability under live operational pressure, and as a coordinated psychological warfare campaign.[85, 86, 87]

Mitigation and Planning Considerations

Effective mitigation requires integrating synthetic-media scenarios into existing event security, crisis communications, and information-operations planning, supported by defined verification workflows, escalation procedures, communications protocols, and coordinated response mechanisms.[88, 89] The following considerations are drawn primarily from federal interagency guidance and operational best practices.

Preparedness, Training, and Public Resilience

- **Integrate synthetic-media scenarios into tabletop exercises and incident-response plans.** Rehearse specific scenarios: a deepfake of a public-safety official ordering evacuation; a voice-clone call to the operations center; swatting-style false reports triggering emergency response; and fabricated or compromised livestream content injected into social or broadcast channels during a critical moment**,** supported by recurring exercises that reinforce pause, verify, and respond under stress.[90]
- **Prebunking.** Proactively educate attendees and the public about likely synthetic-media scenarios around the event. Research indicates prebunking is more effective than reactive debunking in reducing susceptibility to false or misleading narratives.[91]
- **Incorporate public awareness into resilience planning.** Pre-event messaging and media literacy awareness can help reduce susceptibility to synthetic-media deception and improve public response to false or manipulated content during an incident.[92, 93]
- **Identify high-value impersonation targets.** Assess which officials, executives, broadcasters, vendors, and trusted voices would be most attractive for impersonation or voice-clone abuse and prioritize protective measures accordingly.[94, 95]
- **Protect high-visibility individuals.** Provide targeted guidance and protective measures for athletes, broadcasters, and executives, including monitoring for impersonation, limiting exposure of high-quality voice/video data, and establishing rapid response protocols for reputational attacks.[96, 97]

Technical Security and Identity Protection

- **Secure smart-stadium systems and data flows.** Implement segmentation, monitoring, and integrity validation across IoT devices, AI-enabled analytics platforms, and operational systems to reduce the risk of manipulation, unauthorized access, or cascading system failures.[98]
- **Treat identity assurance as part of event security.** Verification of trusted identities, including senior officials, vendors, and operational partners, should be considered part of resilience against synthetic-media enabled deception.[99]
- **Harden impersonation-vulnerable surfaces**. Implement DMARC policies on official domains; enforce phishing-resistant multifactor authentication (MFA), including Fast IDentity Online (FIDO) -based methods, for all staff; and remove unnecessary executive voice and image samples from public-facing content.[100]
- **Adopt content authentication and provenance measures.** Use watermarking, cryptographic signing, C2PA-compliant content credentials,** or similar authentication approaches across official video, audio, and press materials, and encourage adoption by relevant vendors and media partners where feasible, to help distinguish trusted communications from manipulated content and enable rapid verification during high-tempo operations.[101, 102, 103, 104]
- **Deploy authentication codes and dual authorization**. Implement rolling passphrases known only to authorized personnel for real-time communications; require dual authorization for any access, transfer, or messaging decision that could be induced by an impersonation attempt.[105, 106] For voice-clone scenarios, organizations should consider layered human-authentication protocols, including out-of-band verification, pre-established challenge procedures, and dual-channel confirmation for high-consequence requests.[107]

Monitoring, Detection, and Verification

- **Centralize monitoring.** Maintain continuous open-source intelligence (OSINT) and social media monitoring for host-country, venue, executive, sponsor, and event-related synthetic-media content beginning well in advance of the event, integrating platform liaison channels and internal incident reporting into a single operations feed so that emerging synthetic content is triaged quickly. Monitoring efforts should also incorporate account-level analysis, including indicators such as recently created accounts, high-volume posting of similar content, and coordinated amplification patterns.
- **Shift verification earlier in the workflow.** Given the volume and sophistication of synthetic media, verification must increasingly occur at the point of ingestion rather than as a downstream analytic step.[108]
- **Use multimodal verification for suspected synthetic media.** Verification should combine content review, metadata analysis, behavioral indicators, contextual validation, and operational cross-checking through trusted channels to reduce reliance on any single detection method, while assessing authenticity as well as the potential intent and operational effect of the content.[109, 110]
- **Prioritize media verification workflows.** Establish dedicated processes to validate broadcast feeds, viral clips, and high-impact media content in real time, including coordination with broadcasters and platform trust/safety teams.
- **Integrate real-time deepfake detection capabilities.** Where feasible, incorporate automated detection tools into monitoring workflows to support rapid identification and triage of suspected synthetic media, enabling faster validation and response during high-tempo events.[111, 112]

** The Coalition for Content Provenance and Authenticity (C2PA) provides an open technical standard for publishers, creators and consumers to establish the origin and edits of digital content.

- **Do not rely solely on automated detection tools.** AI-detection technologies are often limited, platform-dependent, and susceptible to evasion; effective identification requires a layered verification process, combining technical analysis, human judgment, and source verification.[113]
- **Use caution with AI-assisted analytical outputs.** AI-generated or AI-assisted assessments may contain inaccuracies or unsupported correlations; outputs should be corroborated and treated as decision support, not decision authority.[114, 115]

Crisis Communications and Incident Response

- **Establish pre-event relationships with partners.** This includes social media platforms, broadcasters, fact-check organizations, Information Sharing and Analysis Centers (ISACs), and other relevant detection partners. Rapid assessment, verification, and takedown depend on pre-existing trusted channels.[116]
- **Establish rapid takedown procedures.** Pre-identify escalation paths for urgent platform reporting and removal of synthetic content that threatens safety, operational continuity, or public confidence.[117]
- **Pre-establish synthetic-media crisis communications protocols.** Develop pre-authorized messaging, pre-bunking and rumor-control procedures, rapid public clarification mechanisms, resilience-building communications that can be activated quickly to counter manipulated content before false narratives gain traction, and rehearse activation procedures during exercises.[118, 119, 120]
- **Develop a "trusted voices" network.** Identify and engage pre-designated spokespersons, community leaders, and media partners who can rapidly amplify verified information during an incident, reducing the audience share available to synthetic narratives.
- **Verify before amplifying.** Public-information officers should maintain standing protocols requiring secondary-channel verification of any unexpected directive, particularly those appearing to originate from senior officials via video or voice and regularly rehearse those procedures through exercises and scenario-based training.[121]
- **Counter-message with verified content.** Publish authenticated imagery or footage with content credentials and from verified .gov or official accounts to displace synthetic narratives before they dominate search and algorithmic feeds.

Coordination, Governance, and Post-Incident Actions

- **Report to DHS, the FBI via local field offices, or IC3 (www.ic3.gov).** Real-time video deepfakes and voice-cloning impersonations should be reported even if financial loss is avoided.[122]
- **Document and preserve.** Capture suspected synthetic content with metadata intact for law enforcement referral, platform reporting, and potential prosecution. Chain-of-custody handling is essential given forensic and evidentiary implications.[123]
- **Coordinate with industry and sector partners**. Collaborate with ISACs (e.g., MS-ISAC, Sports ISAO, EI-ISAC) to contribute to broader threat picture and share lessons learned on emerging trends and tactics.[124]
- **Track legal and regulatory developments.** Monitor evolving federal, state, and host-country legal frameworks related to synthetic media and deepfakes, and engage policymakers on gaps in authorities, regulatory approaches, and operational coordination mechanisms. [125]
- **Conduct structured after-action reviews.** Treat synthetic-media incidents as learning events; update indicators, playbooks, and platform relationships based on observed TTPs.

Outlook

The trajectory of GenAI capability strongly suggests that the realism, speed, and cost of synthetic media will continue to favor offensive use in the coming years.[126, 127] Real-time deepfakes, multilingual voice cloning, and coordinated multi-platform influence efforts will likely be deployed against large-scale, high-visibility events, especially in light of current geopolitical environment. As these capabilities mature, the risk is not only that synthetic content will mislead audiences, but that it will increasingly be used to prompt real-world actions, including emergency responses, swatting incidents, and other similar threats, as well as acts of targeted violence.

At the same time, the scale and speed of AI-generated content, including high volumes of low-quality "AI slop," will increasingly challenge the ability of event operators to distinguish signal from noise, enabling false narratives to form and spread faster than they can be verified or countered.[128, 129]

Emerging standards, improved platform policies, detection tools, and greater public awareness offer real advantages, but adversaries continue to adapt, and detection remains technically challenging.[130] Because detection alone will remain imperfect, resilience will continue to depend more on disciplined verification and procedural controls than on technical detection alone.[131, 132] The most durable mitigation rests on process rather than technology: pre-established verification discipline, rehearsed response protocols, trusted-voice networks, and cross-sector information sharing.[133] Event planners should treat synthetic-media threats as a permanent feature of the operational environment, rather than as an episodic anomaly, to preserve event integrity, public safety, and public trust. As synthetic-media threats mature, trust increasingly functions as a critical element that requires active protection alongside physical, cyber, and information security measures.[134]

Additional Resources

- CIS An Examination of Generative AI and Physical Threat Planning
- CIS The Evolving Role of Generative Artificial Intelligence in the Cyber Threat Landscape
- CISA Risk in Focus: Generative AI and the 2024 Election Cycle
- CISA Stadium Spotlight: Connected Devices and Integrated Security Considerations
- CISA Tactics of Disinformation
- DHS Impacts of Adversarial Use of Generative AI on Homeland Security
- DHS Increasing Threats of Deepfake Identities
- EL PACCTO 2.0 Use of Artificial Intelligence by High Risk Criminal Networks
- Europol Facing Reality? Law Enforcement and the Challenge of Deepfakes
- FBI Malicious Actors Almost Will Leverage Synthetic Content for Cyber and Foreign Influence Operations
- FBI IC3 2025 Deep Fake Infographic
- FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions
- GAO Science and Tech Spotlight: Deepfakes
- INTERPOL Report Beyond Illusions: Unmasking the Threat of Synthetic Media for Law Enforcement
- NCSC Foreign Adversaries Could Use Deepfakes to Influence U.S. Elections
- NCTC Emerging Technologies and Possible Malign Uses by Terrorists
- NCTC Emerging Technologies May Heighten Terrorist Threats
- NCTC Violent Extremists' Use of Generative Artificial Intelligence

- NIST AI Risk Management Framework
- NSA, CISA, and FBI Contextualizing Deepfake Threats to Organizations
- Parliamentary Handbook on Disinformation, AI and Synthetic Media
- UNESCO Synthetic Content and its Implications for AI Policy A Primer

This whitepaper was developed by the Center for Internet Security (CIS) with review and input from the Institute for Strategic Dialogue (ISD), the National Fusion Center Association (NFCA) Cyber Intelligence Network (CIN), the National Real Time Crime Center Association (NRTCCA), the Major County Sheriffs of America, and the Arkansas State Fusion Center.

For additional support, or information regarding services, please contact CIS.

Appendix I: Key Risk Factors

Risk Factors	Operational Impacts
Compressed decision windows	Live events demand minute-scale decisions on evacuations, access, and communications. Deepfakes exploit this by inserting false inputs before verification is possible, particularly under conditions of information overload.
Narrative velocity advantage	The increasing prevalence of AI-generated content further accelerates narrative spread, as such clips are cheaper to produce, easier to distribute, and more difficult to verify in real time. Synthetic content can establish dominant narratives within minutes, often outpacing verification processes and official communications during time-sensitive operations.[135]
High audience emotional salience	Fans, attendees, and distant viewers process information under heightened arousal, reducing critical evaluation and increasing sharing velocity.
Dense media and broadcast ecosystems	Hundreds of authorized broadcasters, livestreamers, and social accounts provide many vectors for spoofing and many sources whose authenticity audiences cannot easily verify.
Geopolitical attention to host nations	Host-country disputes, sanctions regimes, and diplomatic frictions create motive for state-aligned information operations targeting event legitimacy, including potential misuse of platform amplification features to increase reach and intensify tensions.
Commercial and financial exposure	Ticketing, hospitality, betting, and merchandise flows create fraud opportunities where deepfake customer support, cloned executive voices, or impersonated sponsors drive direct monetary loss.
Detection asymmetry	Generative models continue to evolve faster than detection tools, including adversarial techniques designed to evade detection, reinforcing the need for layered verification, procedural resilience, and continuous adaptation.[136] Effective detection also increasingly depends on integration into operational workflows rather than standalone analysis.
Confidence–capability gap	Organizations and individuals may overestimate their ability to recognize or counter synthetic-media deception, creating false confidence that can undermine preparedness, verification discipline, and response effectiveness.
Information saturation ("AI slop")	High volumes of AI-generated content, ranging from convincing deepfakes to low-quality synthetic media, can overwhelm monitoring systems, delay verification, and erode trust in legitimate communications during time-sensitive operations. These risks may be exacerbated when malicious actors exploit platform features, paid amplification mechanisms, or algorithmically curated feeds to boost reach, crowd out trusted signals, and accelerate false narratives.[137]
Authenticity uncertainty ("liar's dividend")	The proliferation of synthetic media allows authentic evidence, official messaging, or legitimate reporting, including evidence of incidents, misconduct, or policy violations, to be dismissed as AI-generated or fabricated, degrading trust, delaying response, degrading situational awareness, complicating crisis decision-making, and reducing confidence in legitimate evidence.[138]
Sensor and data integrity manipulation	Smart stadium systems rely on AI-enabled analytics and IoT sensor data to monitor crowd movement, security risks, and operational conditions. Manipulation, spoofing, or corruption of data, whether through cyber intrusion, deceptive signals, or synthetic inputs, could distort situational awareness, trigger inappropriate responses, or degrade decision-making.[139, 140, 141]
Decision paralysis through uncertainty	Synthetic-media campaigns may be designed not just to persuade, but to induce hesitation or delayed action, creating decision paralysis during time-sensitive incidents.
Synthetic-triggered real-world disruption	Deepfake and AI-generated content may prompt real-world actions, including protests, demonstrations, or emergency responses. This includes swatting and other hoax threats, where fabricated reports of violence (e.g., active shooters or explosives) trigger law enforcement deployment, venue disruption, or public panic, even when the underlying information is false.
Cumulative exposure and cognitive fatigue	Repeated exposure to synthetic content across multiple platforms can degrade critical thinking over time, creating cognitive fatigue and increasing susceptibility to misleading or false narratives.

References

[1] https://www.dhs.gov/sites/default/files/2025-01/25_0110_st_impacts_of_adversarial_generative_ai_on_homeland_security_0.pdf
[2] https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf
[3] https://www.csis.org/analysis/crossing-deepfake-rubicon
[4] https://www.ic3.gov/CSA/2021/210310-2.pdf
[5] https://www.security.org/resources/deepfake-statistics/
[6] https://linden-nj.gov/fifa-world-cup-2026-cyber-threat-and-risk-outlook/
[7] https://link.springer.com/content/pdf/10.1007/s10462-023-10679-x.pdf
[8] https://www.secureworld.io/industry-news/cyber-risks-tech-sports-entertainment
[9] https://www.sportsvenue-technology.com/articles/inside-smart-stadiums-how-ai-is-changing-the-future-of-security
[10] https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf
[11] https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes
[12] https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes
[13] https://www.isaca.org/resources/isaca-journal/issues/2025/volume-1/the-rise-of-deepfakes-a-deep-dive-into-synthetic-media-and-its-implications
[14] https://help.kits.ai/hc/en-us/articles/40742972060435-How-is-Instant-Voice-Cloning-different-from-Professional-Voice-Cloning
[15] https://competition-bureau.canada.ca/en/how-we-foster-competition/education-and-outreach/publications/canadian-digital-regulators-forum-synthetic-media-digital-landscape
[16] https://buffett.northwestern.edu/documents/buffett-brief_the-rise-of-ai-and-deepfake-technology.pdf
[17] https://www.dhs.gov/sites/default/files/2023-06/23_0630_st_digital_forgeries_report_signed.pdf
[18] https://www.sportsvenue-technology.com/articles/the-rise-of-smart-stadiums-how-ai-and-iot-are-transforming
[19] https://arxiv.org/pdf/2406.13843
[20] https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
[21] https://www.cisa.gov/sites/default/files/2024-10/PSA_Just%20So%20You%20Know_Foreign_Threat_Actors_Likely_to_Use_a_Variety_of_Tactics.pdf
[22] https://www.reuters.com/world/us/fcc-finalizes-6-million-fine-over-ai-generated-biden-robocalls-2024-09-26/
[23] https://www.mcafee.com/ai/news/was-the-fake-joe-biden-robocall-created-with-ai/
[24] https://lieber.westpoint.edu/deepfake-technology-age-information-warfare/
[25] https://5865987.fs1.hubspotusercontent-na1.net/hubfs/5865987/SODF%202024.pdf
[26] https://sensity.ai/blog/the-role-of-deepfakes-in-cognitive-warfare/
[27] https://hai.stanford.edu/assets/files/2020-11/HAI_Deepfakes_PolicyBrief_Nov20.pdf
[28] https://www.forbes.com/sites/lanceeliot/2024/06/25/cheap-fakes-and-rescuing-humankind-via-generative-ai/
[29] https://www.ic3.gov/CSA/2021/210310-2.pdf
[30] https://time.com/article/2026/04/02/when-virality-is-the-message-the-new-age-of-ai-propaganda/
[31] https://apnews.com/article/iran-war-images-misinformation-russia-israel-9e495017dc5c4bf24a0b6152863dbfb1
[32] https://nypost.com/2024/09/25/us-news/iranian-animation-targeting-trump-on-golf-course-resurfaces-after-assassination-attempts-revenge-is-definite/
[33] https://www.lemonde.fr/en/les-decodeurs/article/2026/04/25/how-tehran-s-propaganda-lures-the-west-into-distraction_6752815_8.html
[34] https://www.isdglobal.org/digital-dispatch/how-pro-iran-networks-gained-a-billion-views-on-war-propaganda/
[35] https://www.isdglobal.org/digital-dispatch/irans-diplomats-launch-a-meme-war/
[36] https://www.cisa.gov/sites/default/files/2024-10/PSA_Just%20So%20You%20Know_Foreign_Threat_Actors_Likely_to_Use_a_Variety_of_Tactics.pdf
[37] https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia
[38] https://www.expertisefrance.fr/sites/expertise/files/2026-02/ai-and-hrncs_elpaccto2.0_en_compressed.pdf
[39] https://www.dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team/first-responder-toolbox/technology/violent-extremists-use-of-generative-artificial-intelligence
[40] https://www.dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team/first-responder-toolbox/technology/violent-extremists-use-of-generative-artificial-intelligence
[41] https://www.dni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/151s_First_Responders_Toolbox-Violent_Extremists_Use_of_Generative_Artificial_Intelligence.pdf
[42] https://www.ic3.gov/PSA/2024/PSA241203
[43] https://www.fincen.gov/system/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf
[44] https://www.reuters.com/business/media-telecom/after-killing-top-drug-lord-cartels-use-fake-news-spread-fear-mexico-2026-02-24/
[45] https://www.kxan.com/news/texas-politics/artificial-intelligence-contributes-to-spread-of-misinformation-amid-mexican-cartel-violence/
[46] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf
[47] https://www.cbc.ca/news/canada/british-columbia/anti-olympics-rioters-smash-vancouver-store-windows-1.870509
[48] https://www.cia.gov/resources/csi/static/de26d97e60d513780f9763afaf0d31a6/Review-Routledge-Disinformation-National-Security-Studies-68-1-March-2024.pdf
[49] https://www.cpahq.org/media/sphl0rft/handbook-on-disinformation-ai-and-synthetic-media.pdf
[50] https://sensity.ai/blog/the-role-of-deepfakes-in-cognitive-warfare/
[51] https://www.hstoday.us/featured/perspective-deepfakes-and-the-erosion-of-trust-in-homeland-security/
[52] https://www.brookings.edu/articles/how-to-deal-with-ai-enabled-disinformation/
[53] https://arxiv.org/abs/2312.13096
[54] https://www.theguardian.com/technology/2025/feb/11/ai-chatbots-distort-and-mislead-when-asked-about-current-affairs-bbc-finds
[55] https://www.ic3.gov/CSA/2021/210310-2.pdf
[56] https://arxiv.org/pdf/2406.13843
[57] https://www.cisometric.com/articles/4300-fake-fifa-domains-and-counting-the-cybercrime-behind-world-cup-2026
[58] https://www.proofpoint.com/uk/newsroom/press-releases/fifa-world-cup-2026-more-one-third-official-partners-expose-public-risk
[59] https://www.huntress.com/resources/2026-cyber-threat-report
[60] https://www.globalrescue.com/common/blog/detail/2026-fifa-world-cup-scams

[61] https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-impersonated-in-malicious-messaging-campaign
[62] https://tiaki.ai/from-the-white-house-to-the-worldcup-deepfakes-expose-sports-datavulnerability/
[63] https://www.brabners.com/insights/sport/deepfakes-ai-powered-cybercrime-in-sport-how-can-athletes-clubs-protect-themselves
[64] https://unesdoc.unesco.org/ark:/48223/pf0000392181
[65] https://www.expertisefrance.fr/sites/expertise/files/2026-02/ai-and-hrncs_elpaccto2.0_en_compressed.pdf
[66] https://www.espn.co.uk/football/story/_/id/39279661/brazil-argentina-fined-fan-brawl-world-cup-qualifier
[67] https://insights.nccgroup.com/annual-cyber-security-research-report-2025
[68] https://www.hstoday.us/featured/perspective-deepfakes-and-the-erosion-of-trust-in-homeland-security/
[69] https://tiaki.ai/mitigating-al-powered-deepfake-cyberserity-attacks-in-sport/
[70] https://www.broadcastnow.co.uk/broadcasting/why-deepfakes-are-the-next-big-threat-to-broadcast-credibility/5204196.article
[71] https://fuseint.com/club-world-cup-how-fake-highlights-are-beating-moderation-and-amassing-millions-of-views/
[72] https://www.nawj.org/uploads/files/annual_conference/2024-annual-conference/fri845a-sgipsonrankinnawjhandout.pdf
[73] https://www.business.com/articles/deepfake-threats-study/
[74] https://www.fbi.gov/investigate/cyber
[75] https://www.ic3.gov/PSA/2024/PSA241203
[76] https://tiaki.ai/from-the-white-house-to-the-worldcup-deepfakes-expose-sports-datavulnerability/
[77] https://www.isaca.org/resources/isaca-journal/issues/2025/volume-1/the-rise-of-deepfakes-a-deep-dive-into-synthetic-media-and-its-implications
[78] https://competition-bureau.canada.ca/en/how-we-foster-competition/education-and-outreach/publications/canadian-digital-regulators-forum-synthetic-media-digital-landscape
[79] https://www.brennancenter.org/our-work/research-reports/deepfakes-elections-and-shrinking-liars-dividend
[80] https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security
[81] https://www.bbc.co.uk/news/videos/cr45nnlv2ewov
[82] https://cloud.google.com/blog/topics/threat-intelligence/cyber-threats-2024-paris-olympics
[83] https://www.cisometric.com/articles/4300-fake-fifa-domains-and-counting-the-cybercrime-behind-world-cup-2026
[84] https://www.cisa.gov/sites/default/files/2024-10/PSA_Just%20So%20You%20Know_Foreign_Threat_Actors_Likely_to_Use_a_Variety_of_Tactics.pdf
[85] https://www.cisa.gov/sites/default/files/2024-10/PSA_Just%20So%20You%20Know_Foreign_Threat_Actors_Likely_to_Use_a_Variety_of_Tactics.pdf
[86] https://www.brookings.edu/wp-content/uploads/2023/01/FP_20230105_deepfakes_international_conflict.pdf
[87] https://www.kyivpost.com/post/74576
[88] https://genai.owasp.org/download/41043/?tmstv=1727108189
[89] https://www.zerofox.com/blog/how-to-create-a-deepfake-incident-response-plan-a-practical-framework-for-security-teams/
[90] https://www.adaptivesecurity.com/blog/deepfake-protection-risk-management-guide
[91] https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide
[92] https://www.researchgate.net/profile/Jan-Mark-Garcia/publication/389593259_Exploring_Deepfakes_and_Effective_Prevention_Strategies_A_Critical_Review/links/67ca895fcc055043ce6ec42d/Exploring-Deepfakes-and-Effective-Prevention-Strategies-A-Critical-Review.pdf
[93] https://www.ncsc.gov.ie/pdfs/Cybersecurity_Guidance_on_Generative_AI_for_PSBs.pdf
[94] https://www.adaptivesecurity.com/blog/deepfake-protection-risk-management-guide
[95] https://www.cdse.edu/Portals/124/Documents/perserec/perserec-deepfakes-research-note.pdf
[96] https://www.brabners.com/insights/sport/deepfakes-ai-powered-cybercrime-in-sport-how-can-athletes-clubs-protect-themselves
[97] https://tiaki.ai/from-the-white-house-to-the-worldcup-deepfakes-expose-sports-datavulnerability/
[98] https://www.secureworld.io/industry-news/cyber-risks-tech-sports-entertainment
[99] https://static-content.regulaforensics.com/PDF-files/0831-Regula-Deepfake-Research-Report-Final-version.pdf
[100] https://www.cisa.gov/sites/default/files/2024-01/Risk-in-Focus-Generative-A.I.-and-the-2024-Election-Cycle-508c.pdf
[101] https://www.researchgate.net/profile/Jan-Mark-Garcia/publication/389593259_Exploring_Deepfakes_and_Effective_Prevention_Strategies_A_Critical_Review/links/67ca895fcc055043ce6ec42d/Exploring-Deepfakes-and-Effective-Prevention-Strategies-A-Critical-Review.pdf
Review.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
[102] https://cnti.org/issue-primers/synthetic-media-deepfakes/
[103] https://c2pa.org
[104] https://www.cpahq.org/media/sphl0rft/handbook-on-disinformation-ai-and-synthetic-media.pdf
[105] https://www.cisa.gov/sites/default/files/2024-01/Risk-in-Focus-Generative-A.I.-and-the-2024-Election-Cycle-508c.pdf
[106] https://www.fbi.gov/investigate/cyber
[107] https://genai.owasp.org/download/41043/?tmstv=1727108189
[108] https://5865987.fs1.hubspotusercontent-na1.net/hubfs/5865987/SensityAI%20How%20Is%20Deepfake%20Detection%20Changing%20Forensic%20Analysis.pdf
[109] https://www.researchgate.net/profile/Jan-Mark-Garcia/publication/389593259_Exploring_Deepfakes_and_Effective_Prevention_Strategies_A_Critical_Review/links/67ca895fcc055043ce6ec42d/Exploring-Deepfakes-and-Effective-Prevention-Strategies-A-Critical-Review.pdf
[110] https://www.zerofox.com/blog/how-to-detect-deepfakes/
[111] https://alethea.com/insights/bringing-deepfake-detection-into-artemis-alethea-partners-with-reality-defender
[112] https://news.skrew.ai/alethea-deepfake-partnership-influence-defense/
[113] https://deepstrike.io/blog/deepfake-statistics-2025
[114] https://www.fbi.gov/investigate/counterintelligence/emerging-and-advanced-technology/artificial-intelligence
[115] https://www.expertisefrance.fr/sites/expertise/files/2026-02/elpaccto2-iaycrimen-en_compressed.pdf
[116] https://www.cisa.gov/sites/default/files/2024-01/Risk-in-Focus-Generative-A.I.-and-the-2024-Election-Cycle-508c.pdf
[117] https://genai.owasp.org/download/41043/?tmstv=1727108189
[118] https://www.globsec.org/sites/default/files/2024-12/Regulating%20Deepfakes%20-%20Global%20Approaches%20to%20Combatting%20AI-Driven%20Manipulation%20policy%20paper%20ver4%20web.pdf
[119] https://cnti.org/issue-primers/synthetic-media-deepfakes/

[120] https://www.gov.uk/government/publications/cdei-publishes-its-first-series-of-three-snapshot-papers-ethical-issues-in-ai/snapshot-paper-deepfakes-and-audiovisual-disinformation
[121] https://unesdoc.unesco.org/ark:/48223/pf0000392181
[122] https://www.fbi.gov/investigate/cyber
[123] https://www.dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team/first-responder-toolbox/technology/violent-extremists-use-of-generative-artificial-intelligence
[124] https://www.cisa.gov/sites/default/files/2024-01/Risk-in-Focus-Generative-A.I.-and-the-2024-Election-Cycle-508c.pdf
[125] https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=2012&context=bjil
[126] https://www.expertisefrance.fr/sites/expertise/files/2026-02/elpaccto2-iaycrimen-en_compressed.pdf
[127] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf
[128] https://www.reuters.com/sports/global-sports-face-challenges-ai-slop-misinformation-2026-01-17/
[129] https://brandequity.economictimes.indiatimes.com/amp/news/digital/global-sports-face-challenges-from-ai-slop-misinformation/126608273
[130] https://media.defense.gov/2023/Sep/12/2003298925/-1/-1/0/CSI-DEEPFAKE-THREATS.PDF
[131] https://genai.owasp.org/download/41043/?tmstv=1727108189
[132] https://www.ncsc.gov.uk/blog-post/preserving-integrity-in-age-generative-ai
[133] https://www.linkedin.com/pulse/deepfakes-digital-twins-fan-trust-ethical-tightrope-synthetic-j9vge
[134] https://www.unesco.org/en/articles/deepfakes-and-crisis-knowing
[135] https://digitalcommons.odu.edu/covacci-undergraduateresearch/2023fall/projects/4/
[136] https://www.ncsc.govt.nz/insights-and-research/insights-reports/quarter-one-cyber-security-insights-2025/insights-deepfakes-seeing-isnt-always-believing/
[137] https://www.isdglobal.org/digital-dispatch/how-pro-iran-networks-gained-a-billion-views-on-war-propaganda/
[138] https://5865987.fs1.hubspotusercontent-na1.net/hubfs/5865987/SensityAI%20How%20Is%20Deepfake%20Detection%20Changing%20Forensic%20Analysis.pdf
[139] https://www.secureworld.io/industry-news/cyber-risks-tech-sports-entertainment
[140] https://pmc.ncbi.nlm.nih.gov/articles/PMC11219349/
[141] https://stadiumtechreport.com/editorial/building-the-ai-ready-stadium/