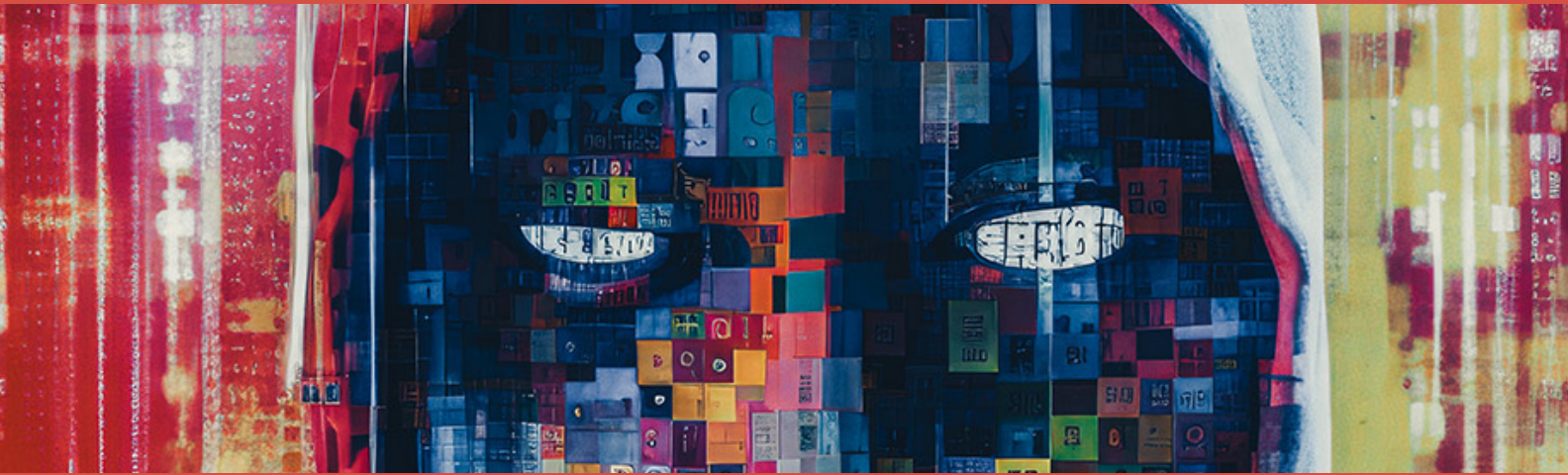


**M+E**

**JOURNAL**

# A SECURE



# AI WORLD?

How AI is being used both by and against the industry

## **SECURITY SOLUTIONS**

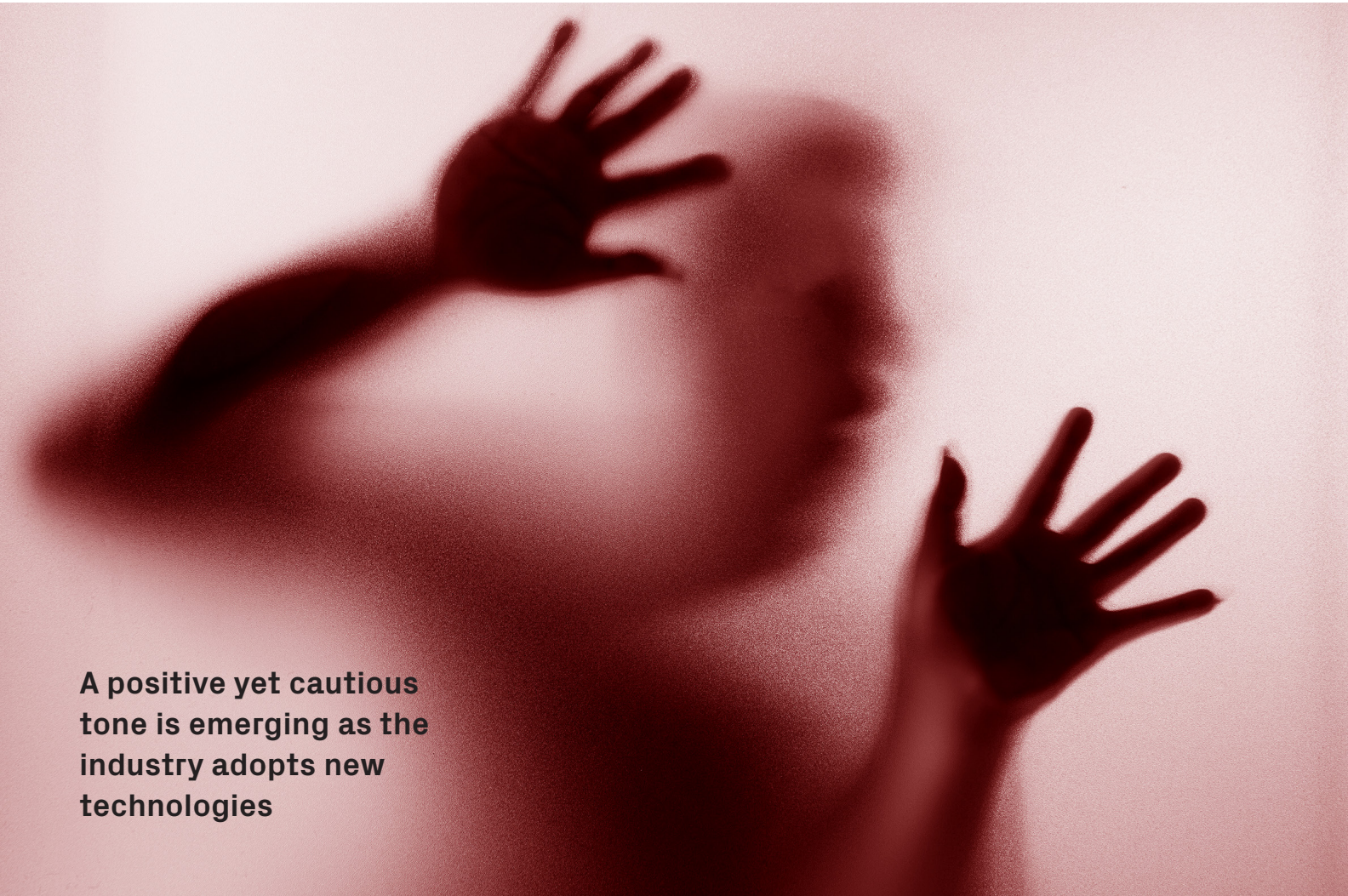
Where and how AI is being used to attack and protect M&E

## **SMART CONTENT**

Massive amounts of data now required new tools, including AI

# 23.02

# AI: THE NEXT BIG M&E CREATIVE ADVENTURE OR A FAST-APPROACHING SECURITY HEADACHE?



A positive yet cautious tone is emerging as the industry adopts new technologies

**ABSTRACT:** This article explores how AI is being used to create content that is realistic and easily blended with live-captured video. But aside from likeness protection, what about the wider security aspects and how could such technology be used for illicit gain?

**By Tim Pearson, VP, Global Solution Partner Marketing, NAGRA**

The M&E industry has been using AI in various forms for several years. Largely focused on data interpretation that detects anomalies and patterns around everything from security analytics to customer retention, its use is well documented. In the last year, however, its

use and application has left the labs to become more mainstream. One area in particular, generative AI, has caused a tempest of debate across the industry. Spearheaded by today's "go to" engines for tricky questions, such as ChatGPT and AI content creators such as

*WHETHER GENERATIVE AI WILL FORM the next content revolution and change established industry practices and business models remains to be seen.*

Midjourney, broader tools are also being used to create content that is realistic and easily blended into existing live-captured video.

At a recent NAGRA customer event, strategic partner AWS showed us how some of this technology is being used across the M&E industry — from sports telematics to creating new inserts for content production. Aside from likeness protection demanded by the recently striking actors, what about the wider security aspects and how could such technology be used for illicit gain and how does machine learning accelerate this adoption further?

**PROTECTING THE PROTECTED**

In a world where computer generated moviemaking doesn't involve writers, crew, or talent, will today's structured production processes continue? Key to that production process is the protection of IP against illicit distribution. NAGRA is an industry leader in this charge by advocating solutions such as NexGuard Forensic Watermarking applied from the moment content leaves the camera to the point it is watched on a consumer's device. Along the distribution chain, further tools from the NAGRA Active Streaming Protection toolset are used to protect valuable content investments. This includes illicit activities such as pirate re-distribution, extended access through credential sharing or addressing broader cyber threats. Incorporated into production and distribution workflows, security is a firm fixture meaning it is protecting both studio revenues alongside the reputations, identities, and talents of those involved.

But how would this work in a pure generative AI landscape? For now, there is clearly a blend of both live and AI content working together as it passes through the existing secure workflows and processes. But with a pure AI landscape, where established processes, regulation and approaches are either in their infancy or

non-existent, innovation can spawn both new content genres and new content production approaches — and arguably quicker than their more traditional cousins. The adoption of machine learning technology can accelerate post-production through tools too. Examples include face ageing, changing clothing appearance and motion diffusion. But even before we get to that stage in the process, machine learning could also be used for concept ideation and reducing time spent on more time-consuming tasks such as animation, compositing, lighting, and optimizing localization.

But is that day already here? I recently came across an article on LinkedIn that discussed a new Netflix show where contestants guess whether their partners' actions are real or fake based on both live and deepfake content they review in the "chair of truth." Equally, Marvel Studios' new "Secret Invasion" TV series that has recently launched on Disney+ includes opening credits created with AI. Perhaps innocuous but creatives have reacted strongly about generative AI's role. In particular, the impact it could have on artists' careers going forward.

Evidently, this topic is generating much discussion across industry groups, regulators, and vendors.

**GENERATIVE AI AND PIRACY**

Teams across NAGRA and the wider Kudelski Group have been hot-housing technologies that can identify bogus media or unauthorized representation of individuals' likenesses created through AI-generated content. The aim being to ensure our solutions protect our customers' interests. In the same way conventional content and service piracy is outwitted by developments in technology, a new era is dawning where piracy is about both stealing content and creating content that to the unaware, is a "genuine fake." The ramifications of this are vast. With consumers already showing a voracious appetite for online content across both streaming

*Continued on page 4*



*Tim Pearson is VP of global solution and partner marketing at NAGRA. He drives various market development, solution, and partner marketing activities for the company. His areas of focus include next generation content protection, OTT streaming, watermarking, anti-piracy, broadcast, consumer engagement and user experience. marcom@nagra.com @NAGRAKUDELSKI*

**NAGRA** *Continued from page 3*

services and social media, production timelines will come under pressure, particularly at a time of industrial unrest. This can open the door to new original or variant generative AI content and/or content formats as seen in the Netflix example above.

However, existing technologies can help address some of these challenges. Those creating “human-intelligence” generated content use a variety of tools to identify whether AI-generated work has stolen their content — which can include likeness and speech/ tone. Some of these tools and techniques are the same as those used to track conventional content piracy and include watermarking both the video and/or audio so the source can be authenticated evidentially if required. In addition, investigative techniques are also used to identify entities posting or selling illicit AI-generated content.

Whether generative AI will form the next content revolution and change established industry practices and business models remains to be seen. While there is a positive yet cautious tone emerging,

history also tells us that not adopting new technologies such as generative AI for the reasons discussed here, may ultimately have a greater impact. As Paul Cramer from Veritone recently commented: “Gen AI won’t replace humans, but it will replace the humans who are not using AI.”

**NAVIGATE THE DISRUPTION. SECURE YOUR FUTURE**

NAGRA has been securing content in all its forms for more than 30 years. Our technologies extend across both content distribution and content production. As consumers start to interact and pay for a wider selection of content with their eyeballs (FAST, AdTech, loyalty rewards etc.) rather than their wallets, new security approaches, beyond just content security are required. NAGRA teams are actively working with new GenAI innovations to ensure our solutions remain robust in the face of attack and the benefits of AI and GenAI for our industry are maximized. 