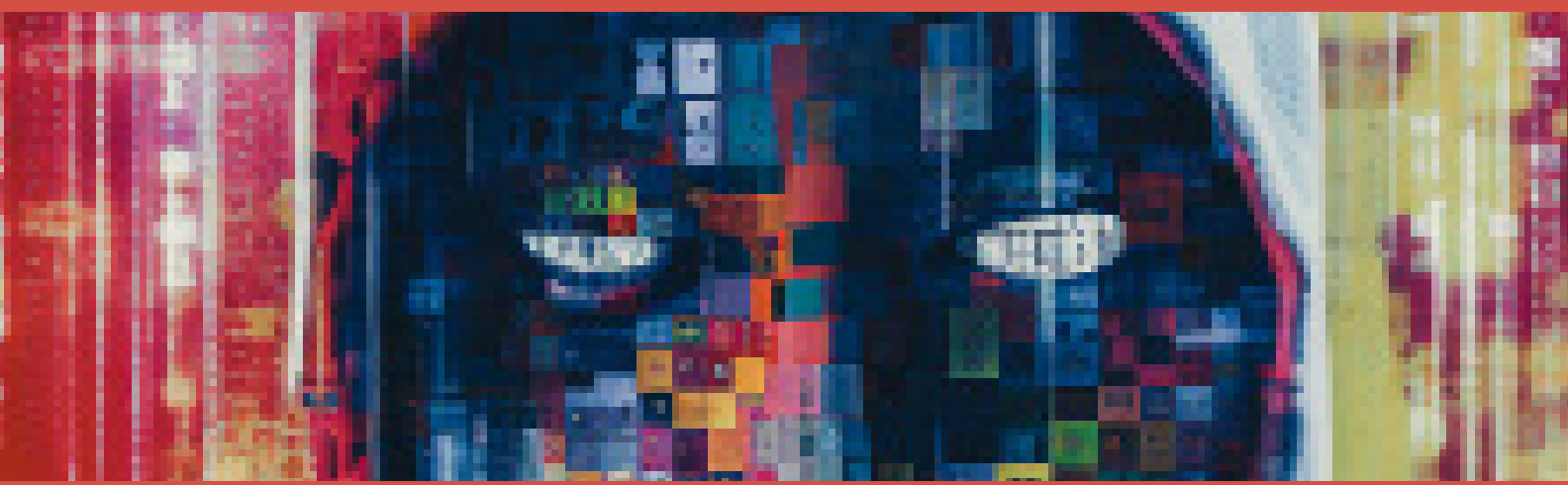
M+E JOURNAL

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 AND SECURITY CONVERGE

By Richard Atkinson, President, CDSA

***Richard Atkinson** is president of CDSA, and his experience covers more than 15 years in classified defense and 23 years in M&E senior leadership positions, driving profound business revenue and change for Northrop Grumman, Disney, EA, and Adobe.*
ratkinson@CDSAonline.org

"AI and Security Converge" is not just the theme of the Content Delivery & Security Association's (CDSA) Content Protection Summit. Artificial intelligence is also increasingly impacting every one of us in a multitude of ways. It is making things better and easier than was ever possible before.

When you can take large components of the world's information, index it and be able to assemble it in amazing ways, and link that with very simple and easy to use interfaces to access all this in seconds it's simply amazing. I don't mean doing things faster. I'm saying most things that AI is now enabling were literally not possible outside a lab and at scale before, and now it is not just possible, it is easy and almost instant.

When we then look at how AI is impacting security and aspects of fraud (in a broad context), there are both positive and negative aspects emerging, and here is a list of just a few categorical areas we were seeing AI impact today:

Cybersecurity:

- **Threat detection**: AI is used to detect and prevent cyber threats. Machine learning models can analyze large datasets to identify patterns and anomalies indicative of malicious activity.

- **Anomaly detection**: AI can identify unusual network or user behavior that might be a sign of a security breach.

- **Predictive analysis**: Machine learning models can predict future threats based on historical data and trends.

- **Malware detection**: AI-powered antivirus and anti-malware tools can quickly identify and mitigate new and evolving malware strains.

THE EVOLVING NATURE of video security threats means an "on your toes" approach is inevitable if an organization seeks to remain one step ahead of the bad guys.

Network security:

- **Intrusion detection and prevention**: AI helps in identifying and responding to network intrusions in real-time, protecting sensitive data.

- **Firewall management**: AI can optimize firewall rules and configurations, reducing vulnerabilities.

Physical security:

- **Facial recognition**: AI-driven facial recognition systems are used for access control, video surveillance, and identifying individuals in real-time.

- **Object detection**: AI can be used to identify objects or anomalies in security camera footage.

Biometric security:

- AI plays a crucial role in biometric security, such as fingerprint recognition and voice authentication.

Fraud detection:

- AI algorithms can analyze financial and transaction data to detect fraudulent activities in banking and e-commerce.

Continued on page 3

ATKINSON *Continued from page 2*

Security automation:
■ AI and machine learning can automate routine security tasks, allowing security professionals to focus on more complex threats.

Vulnerability assessment:
■ AI can identify vulnerabilities in software and infrastructure, helping organizations patch weaknesses before they are exploited.

Phishing detection:
■ AI-driven email security tools can identify phishing emails and other forms of social engineering attacks.

Security analytics:
■ AI can process and analyze large datasets to provide security professionals with insights into potential risks and trends.

Threat intelligence:
■ AI can help organizations gather, process, and analyze threat intelligence data from various sources to anticipate and prepare for emerging threats.

Autonomous security systems:
■ AI-powered security systems can make real-time decisions and take actions to mitigate threats without human intervention.

Privacy concerns:
■ AI's capabilities can also be a threat to privacy when used for surveillance, data mining, or profiling. There are ongoing debates about balancing security with privacy concerns.

With AI development moving so fast and so broadly, with such potential impact, what should we be doing as AI leaders to just keep up ... much less get ahead of this revolution?

Recognize that you are not alone. In fact, pretty much every one of us is being eclipsed by this revolution. What this means is that we can leverage each other in learning, sharing, and trying. Be a part of a community that has a culture of sharing (such as CDSA and MESA) and get involved with your experiences and importantly your perceptions.

Don't fear AI: it is simply a tool. Incredibly powerful and amazing, but still just a tool. So, the more we can keep this perspective, the more we can see it as an enabler and force-multiplier and keep our thinking in context, the easier it will be to keep AI in context.

Try using it, in safe ways. Getting real-world experience with AI-based tools (and seeing what you can do that maybe you could not prior) builds perspectives. For example, try ChatGPT (openai.com/chatgpt) by asking it some questions, and getting its formatted and curated answers in moments. Try things you wonder, but also try things that you know very well. You might see that the AI engine is interpreting the sources it has and might be getting things right...or maybe very wrong.

Understand that these AI engines are interpretive, by design. Different from the types of queries/results that we are used to from computer systems for the past 20 years. This is more like asking another person, and getting a response that could be delivered with confidence and passion but could be fundamentally wrong. But this ability to "interpret" is exactly what also makes them extremely powerful. Adobe's ability to simply request their AI systems to "create" imagery that did not exist before is a great example where this type of function is fueling a new revolution.

Look on the bright side, cautiously. Yes, AI is being leveraged for fraudulent means. Bad guys have always used whatever tools are available. But AI-enabled tools are changing our lives for the positive too.

AI and security are colliding, in many ways. And while it feels like this has come out of nowhere and is hitting us from all angles (and it is), this is also a revolution of tools that has been in vision and development for many years and will take many years to mature. Don't panic. Learn to drive, in a context, and let's all work together as a community to deal with this — and grow — together. ⊞