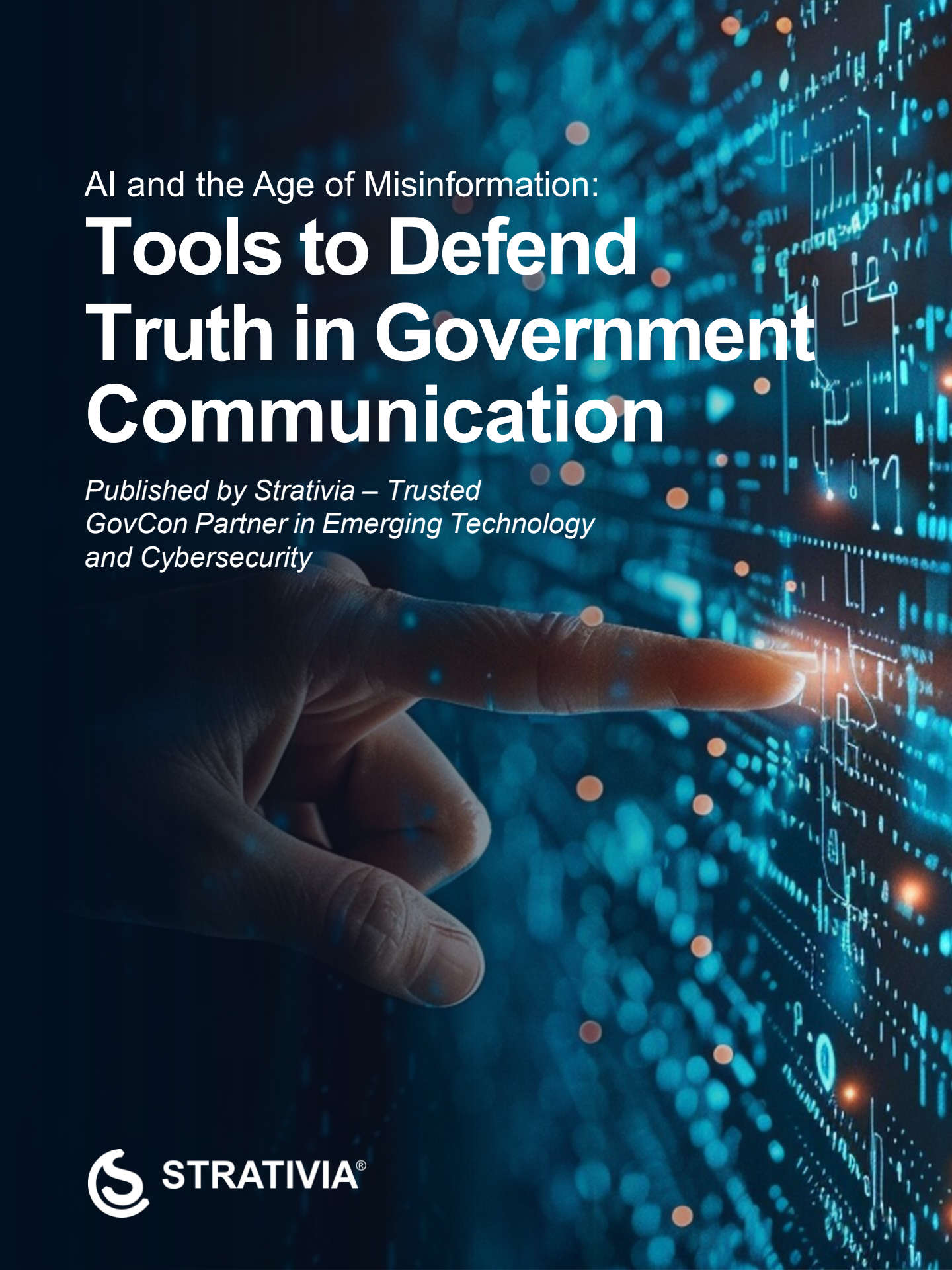

AI and the Age of Misinformation:

Tools to Defend Truth in Government Communication

Published by Strativia – Trusted GovCon Partner in Emerging Technology and Cybersecurity

STRATIVIA®

AI and the Age of Misinformation:

Tools to Defend Truth in Government Communication

Published by Strativia – Trusted GovCon Partner in Emerging Technology and Cybersecurity

In an era dominated by rapid information flow, the rise of artificial intelligence has ushered in a new age—one where disinformation is not only easier to create but harder to detect. This evolving threat landscape has introduced a national security risk that extends far beyond traditional cyber perimeters. At the intersection of technology, psychology, and governance, misinformation now has the potential to erode public trust, distort decision-making, and destabilize democratic institutions.

Strativia, a trusted federal contractor with deep roots in cybersecurity, AI integration, and information assurance, is actively partnering with agencies to not only identify these threats—but to build the technological, analytical, and operational infrastructure needed to defeat them.

In an era where disinformation spreads faster than facts, federal agencies face a new kind of adversary—one that doesn't rely on weapons or malware, but on doubt, distortion, and distrust.

The rise of generative AI and synthetic media has added urgency to this challenge. Deepfakes, AI-generated social bots, and misinformation networks now influence everything from public health to national security. For government communicators, this means defending truth isn't just a communications issue—it's a mission-critical function.

What's Changed? The AI-Powered Misinformation Threat

Yesterday's misinformation campaigns relied on repetition and human labor. Today, disinformation is algorithmic, scalable, and disturbingly convincing.

Key drivers of the threat:

- Generative AI enables fake images, audio, and video to be created at scale.
- Bot networks amplify false narratives and manipulate public discourse.
- AI voice cloning mimics public officials to impersonate trust.
- Microtargeting tools allow for tailored disinformation, invisible to most watchdogs.

The Federal Response is Taking Shape

Agencies like CISA, NIST, and OSTP are mobilizing around AI and information integrity. Early-stage frameworks are forming that outline responsible AI use and content verification protocols.

Examples include:
- NIST's AI Risk Management Framework (AI RMF)
- OSCAL (Open Security Controls Assessment Language)
- CISA's Misinformation and Disinformation Toolkit

AI for Good: Tools to Protect Truth

AI Tool Category	Application in Government
Content Authenticity	Watermarking and digital signatures to verify official content
Anomaly Detection	Flagging false narratives or sudden spikes in disinformation activity
Natural Language Models	Identifying manipulated text patterns and sentiment drift
Synthetic Media Detection	Tools to spot deepfakes and altered videos
Threat Intelligence AI	Linking misinformation campaigns to threat actors

From Communication to Countermeasures

Agencies are beginning to view communications teams as frontline defenders. That means:

- Investing in AI-literate communication staff
- Training in misinformation triage
- Integrating AI tools with existing cybersecurity ecosystems
- Creating interagency playbooks for coordinated responses

Strativia's Commitment to Mission Integrity

At Strativia, we understand that truth is infrastructure. As a small business partner with Top Secret-cleared personnel, ISO 27001 credentials, and a growing portfolio in AI, cybersecurity, and data visualization, we support agencies at the intersection of trust and technology.

Whether helping federal teams deploy misinformation detection models, modernize NIST-aligned frameworks, or stand up real-time monitoring dashboards, Strativia brings the agility, security, and experience to help agencies protect the public narrative—and the public trust.

Strativia's Strategic Advantage

If your agency is exploring tools to navigate the AI-infused information environment, Strativia is ready to help. From Zero Trust cybersecurity to AI-enabled communications support, we are your partner in clarity, confidence, and national integrity.

Strativia's commitment goes beyond simply supplying tools—we architect ecosystems for digital trust. As a CMMI Level 3, ISO 27001–certified, Top Secret–cleared small business, Strativia operates at the frontline of cybersecurity, AI integration, and mission assurance for civilian and defense agencies alike.

From implementing Zero Trust policies that extend to communications systems, to embedding AI-driven threat analytics into agency operations, we combine deep technical expertise with mission fluency.

Let's secure the truth. Let's secure the mission—together.

Strativia (HQ)
1401 Mercantile Lane, Suite 501, Largo, MD 20774
P: 301-362-6555 | F: 301-362-6557 | www.strativia.com

Strativia Regional Offices:
Arlington, VA | Atlanta, GA | Denver, CO

STRATIVIA®
TECHNOLOGY | CONSULTING | SERVICES