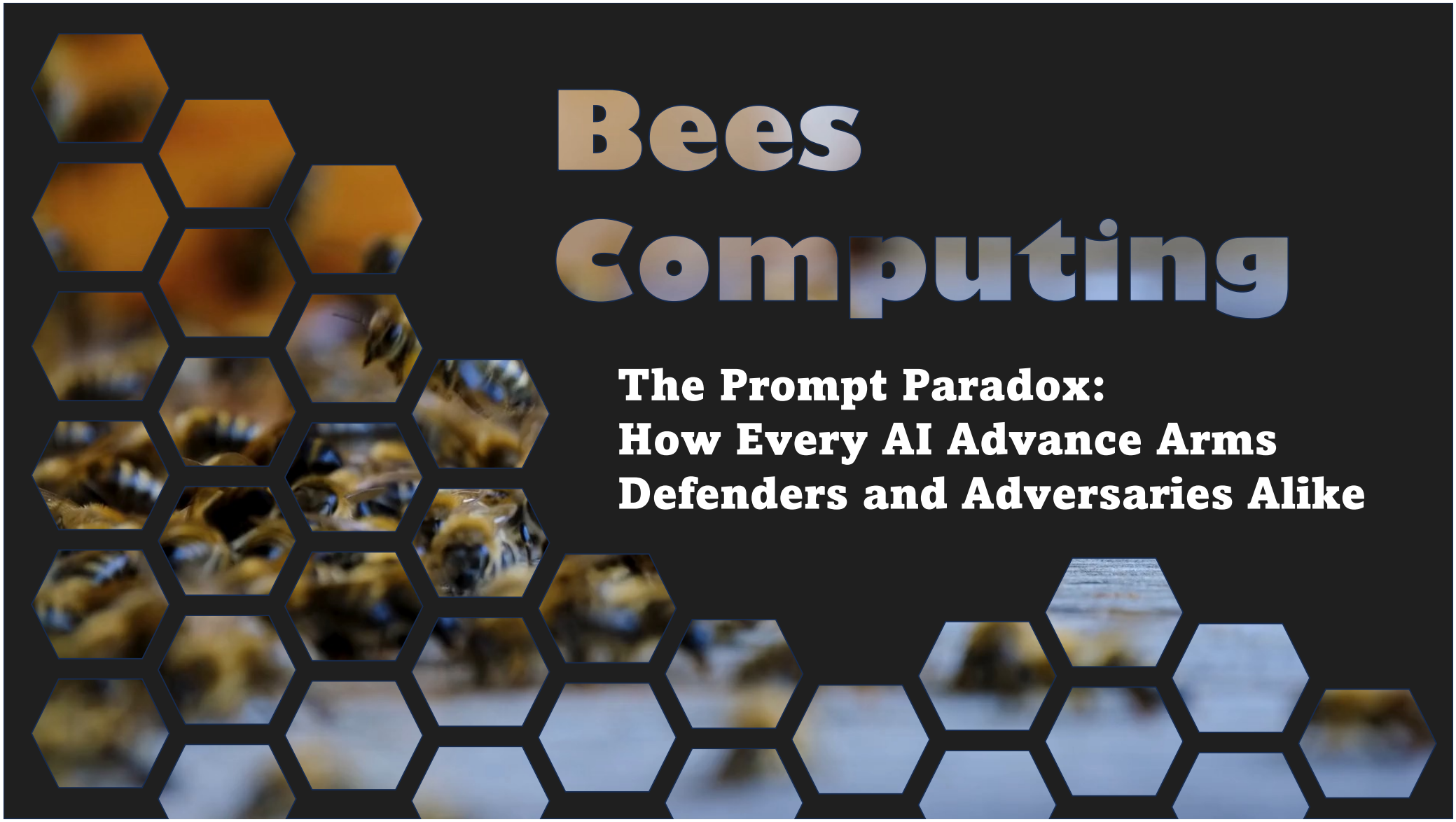

Bees
Computing
The Prompt Paradox:
How Every AI Advance Arms
Defenders and Adversaries Alike

The Prompt Paradox: How Every AI Advance Arms Defenders and Adversaries Alike

"Who Controls the Context Controls the Battlefield: The Evolution of AI Prompting"

About Me

- Gary Whitsett, MBA, CISSP
- 35+ Years in IT, Cyber, AI
- Instead of fighting AI, I harnessed AI
- https://www.linkedin.com/in/garywhitsett/

The Stakes Today

"We're Living Through a Revolution"

4,151%

increase in phishing volume since ChatGPT launch (Nov 2022)

54%

AI phishing success rate vs. 12% traditional attacks

300,000+

FBI phishing complaints, $52M+ losses in 2025

March 2025: AI agents outperformed elite human red teams for first time

Our Journey Today

Six Stages of AI Evolution (2000-2030+)

Stage		
1	2000-2020	Keyword Era
2	2020-2023	Prompt Engineering
3	2023-2025	Contextual Prompting
4	2025-2027	Context Prompting
5	2027-2030	Autonomous Agents
6	2030-Beyond	Invisible AI

Stage 1 - The Keyword Era (Pre-2020)

"When Analysts Drowned in False Positives"

How We Prompted:

- Keywords, Boolean logic, regex patterns
- Rigid SIEM queries with limited sophistication

The Players:

- **Defenders:** Traditional log management, manual correlation
- **Compliance:** PDF searches, spreadsheet auditing
- **Adversaries:** "default router password" Google searches, Metasploit copy-paste

Case Study - The SIEM Struggle

Brief Example:

01

2005: Gartner coins "SIEM" term, promises centralized security

02

Reality: Analysts spending hours creating queries, drowning in alerts

03

Heavy reliance on manual processes made correlation nearly impossible

Stage 2 - Prompt Engineering (2020-2023)

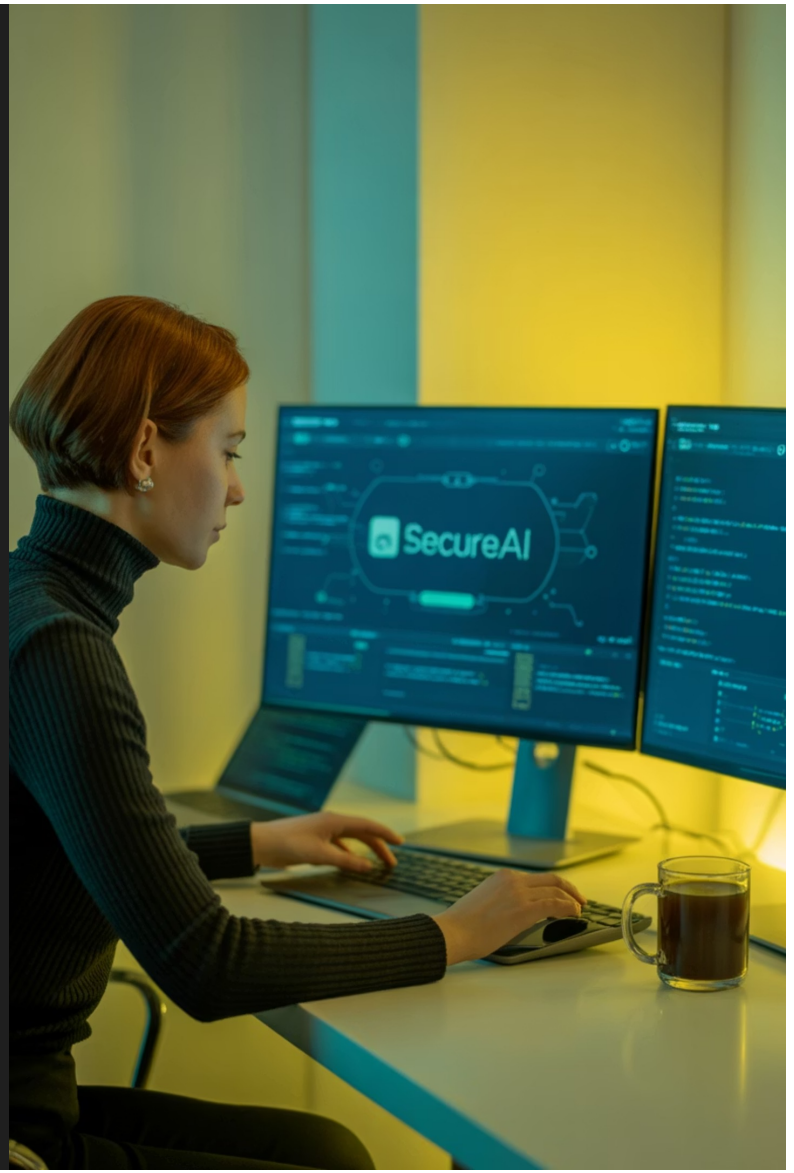
"The Magic Spell Era"

How We Prompted:

- "Act as a SOC analyst..." style instructions
- Role-based prompting becomes standard practice

The Impact:

- **Defenders:** Paste logs into GPT, generate policy templates
- **Compliance:** AI-drafted audit checklists and security policies
- **Adversaries:** Clean phishing emails, polymorphic malware stubs
- **Key Shift:** Bar to entry dropped dramatically



Case Study - The 5-Minute Phishing Campaign

IBM Security Research:

AI: 5 prompts, 5 minutes = effective phishing campaign

Human experts: 16 hours for same quality

Result: Attackers could now iterate instantly, launch polymorphic campaigns

Stage 3 - Contextual Prompting (2023-2025)

"When AI Got Smart About Your Business"

How We Prompted:

- RAG systems with embeddings and vector databases
- Organizational context enriching every query

The Evolution:

- **Defenders:** AI correlating threat intel with SIEM context
- **Compliance:** Control mapping with curated evidence
- **Adversaries:** 76% of 2024 phishing attacks used polymorphic features
- **Key Shift:** 67.4% of phishing attacks utilized AI in 2024

Case Study - The Deepfake CEO Scam

Real-World Impact:

1. 2019: British CEO scammed out of $243,000

   AI-generated voice mimicked German accent and speech patterns

2. 2025: FBI confirms AI-generated voices impersonating senior US officials

Stage 4 - Context Prompting (2025-2027)

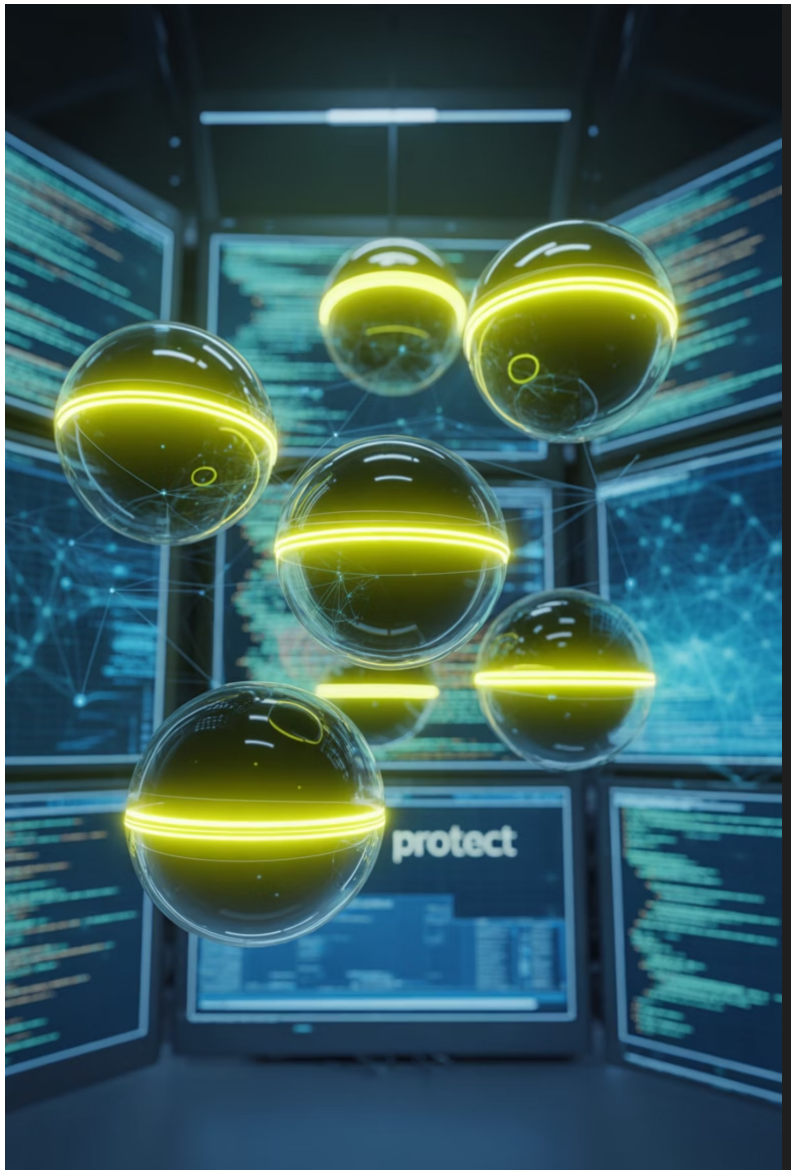
"AI That Knows Your Mission" *(Near Future)*

How We'll Prompt:

- AI pre-loaded with environmental awareness
- Mission-specific context driving autonomous decisions

Predicted Impact:

- **Defenders:** Auto-triaging copilots, attack path prediction
- **Compliance:** Full evidence packages assembled pre-audit
- **Adversaries:** Context-aware malware (knows contractor vs. DoD network)



Stage 5 - Autonomous Context Agents (2027-2030)

"Specialized AI Teams"

How We'll Prompt:

- High-level objectives: "Hunt lateral movement"
- Multi-agent systems and "agent swarms"

The Vision:

- **Defenders:** AI-led SOCs with human oversight
- **Compliance:** Real-time drift monitoring
- **Adversaries:** Multi-agent attack swarms sharing intel
- **Key Shift:** AI vs. AI battles inside networks

Stage 6 - Invisible AI (Beyond 2030)

"When We Stop Prompting"

How We Won't Prompt:

- Ambient AI woven into infrastructure
- Zero human intervention required

The Future:

- **Defenders:** Continuous, invisible monitoring
- **Compliance:** Always-on compliance, no point-in-time audits
- **Adversaries:** Nation-state "sleeper code" lying dormant for years
- **Ultimate Challenge:** The invisible insider threat

The Pattern We Can't Ignore

"Every Leap Armed Both Sides"

Stage 1: Basic tools for basic threats

Stage 2: Democratized phishing creation

Stage 3: Precision targeting with stolen data

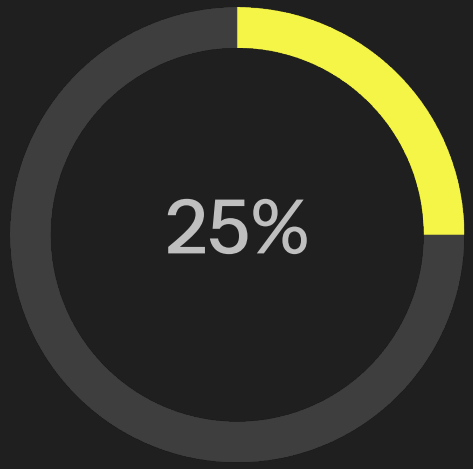
Stage 4-6: Autonomous warfare

The Trend: Escalating technological arms race between attackers and defenders

Current Reality Check

"Where We Stand Today"

of phishing emails bypassing filters are AI-generated



of CISOs experienced AI-generated network attack in past year

- Multi-agent systems emerging in 2025
- **Gap:** Many incidents go undetected without advanced metrics

What This Means for You

"Practical Implications"

For Defenders:

- AI will become essential for managing data volume and speed
- Unified data platforms will be critical

For Organizations:

- Privacy-preserving, on-device AI deployment
- Enhanced access controls and query validation

For the Industry:

- Prompt engineering skills increasingly valuable

The Coming Inflection Points

"What to Watch For"

1

2025-2026:

Widespread multi-agent system adoption

2

2027-2028:

Context-aware malware emergence

3

2029-2030:

Quantum-resistant encryption becomes standard

4

Beyond 2030:

True invisible AI integration

Your Action Items

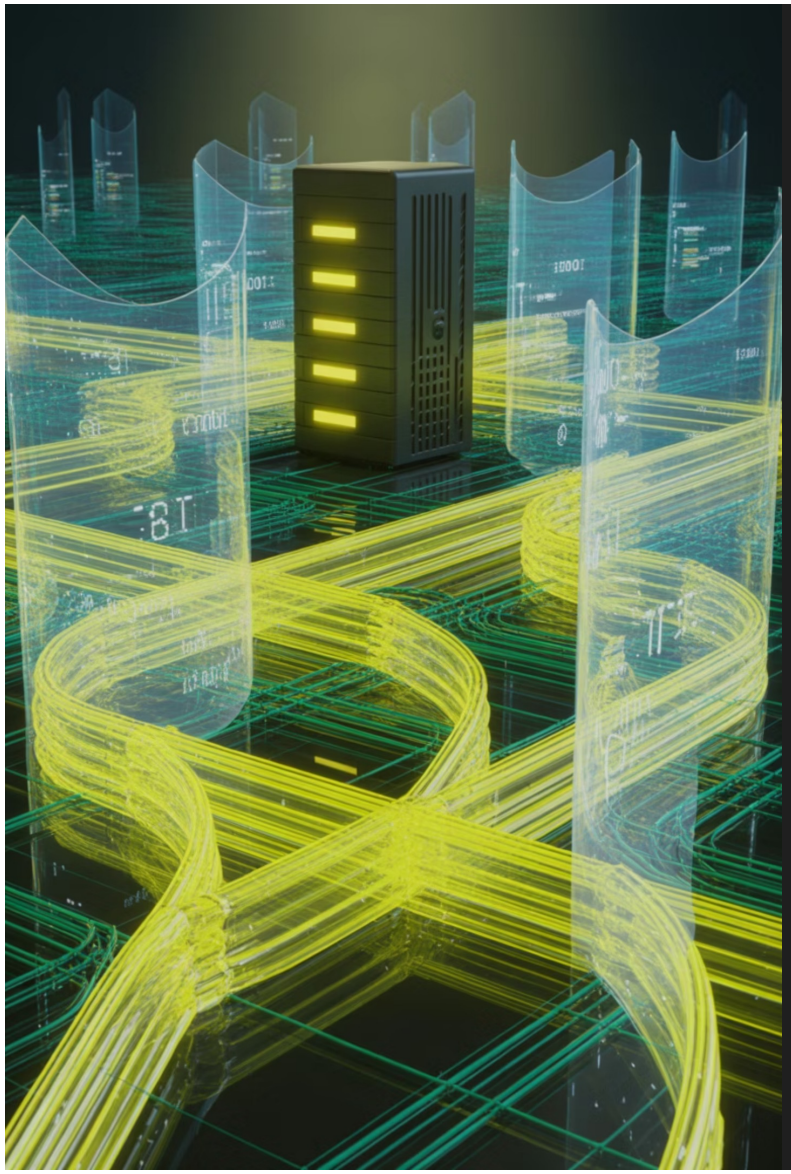
"Starting Tomorrow"

1. **Assess your prompting maturity:**
   Where are you on the 6-stage spectrum?

2. **Invest in context:**
   RAG systems are critical for 2025

3. **Prepare for agents:**
   Multi-agent systems are coming fast

4. **Control your context:**
   Your data = your competitive advantage



The Ultimate Question

"Who Will Control the Context?"

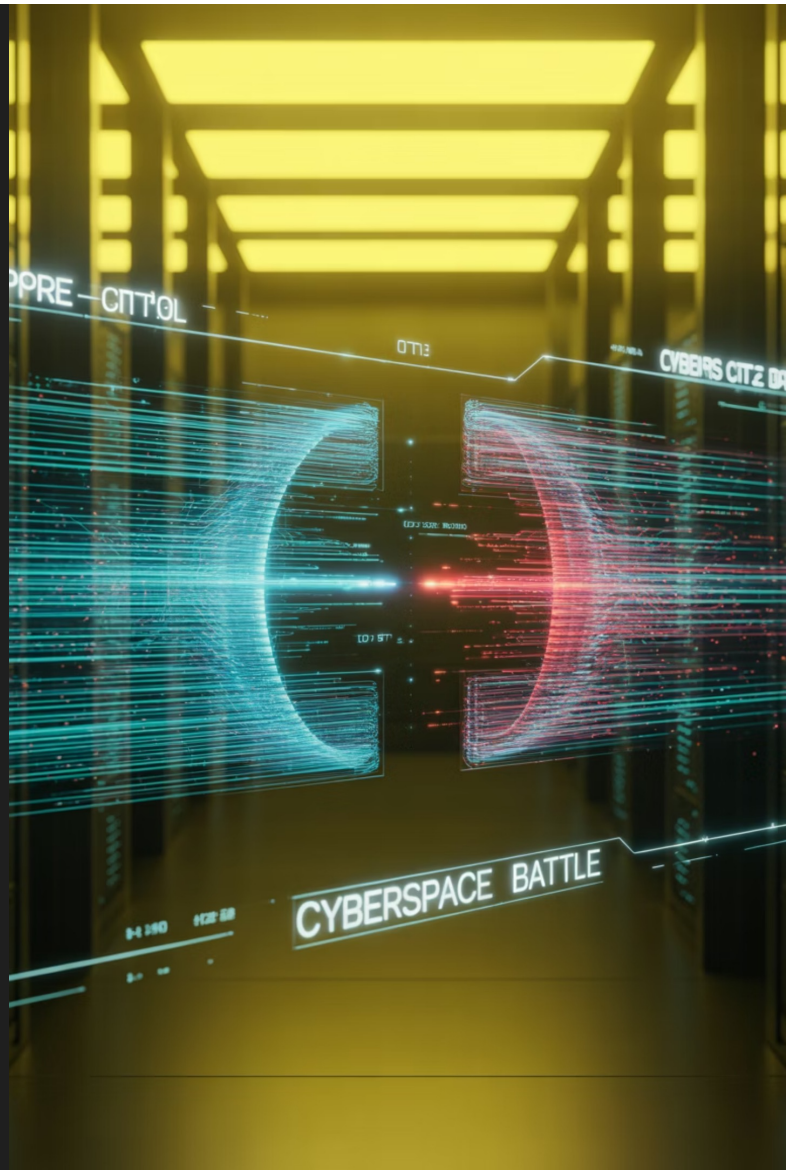
- Your organization's proprietary data
- Your threat intelligence feeds
- Your operational environment
- Your response playbooks

Remember:
Context-driven AI isn't just relevant in 2025—it's critical

Every leap in prompting gave defenders new tools—but it also gave adversaries sharper weapons.

The future of AI in cyber isn't about who can prompt better, it's about who can control the context.

Because whoever controls the context, controls the battlefield.



Thank You & Questions

gary.whitsett@beescomputing.com

https://www.linkedin.com/in/garywhitsett/

https://beescomputing.com

Questions?

Contact Info