How Artificial Intelligence is Transforming National Security

Dr. Jack Francis, AI Solutions Director, Davidson Technologies

Jason Kearns, Principal Enterprise Architect, Davidson Technologies

Agenda

- Traditional AI vs Generative AI
- AI for Decision Advantage
- AI-Enhanced Adversarial Capabilities
- Conclusion

AI isn’t new, but GenAI is

- **Traditional AI:** Analyze existing data to make predictions
  - **ISR:** Computer vision for automated target recognition (Project Maven)
  - **Command and Control:** Fuse sensor data into common operating picture (CJADC2)
  - **Predictive Maintenance:** Increasing equipment readiness (PANDA, CBM+)
- **Generative AI:** Create new, original content
  - **Large Language Model (LLM):** The core engine behind most GenAI today
  - **Agentic AI:** AI that can autonomously plan, reason, and execute complex tasks to achieve a goal, rather than just following a list of human-given commands.
  - **Task Force Lima:** 2023-24 CDAO Task Force to evaluate GenAI within DoD
  - **GSA Centralized Procurement:** LLM Access for $1 per agency (ChatGPT, Gemini)
  - **GenAI.mil:** LLM Access to top models for DoD
  - **AI Action Plan:** Significant focus on GenAI (LLM training, evaluation, infrastructure) [1]

Gemini

Claude

OpenAI

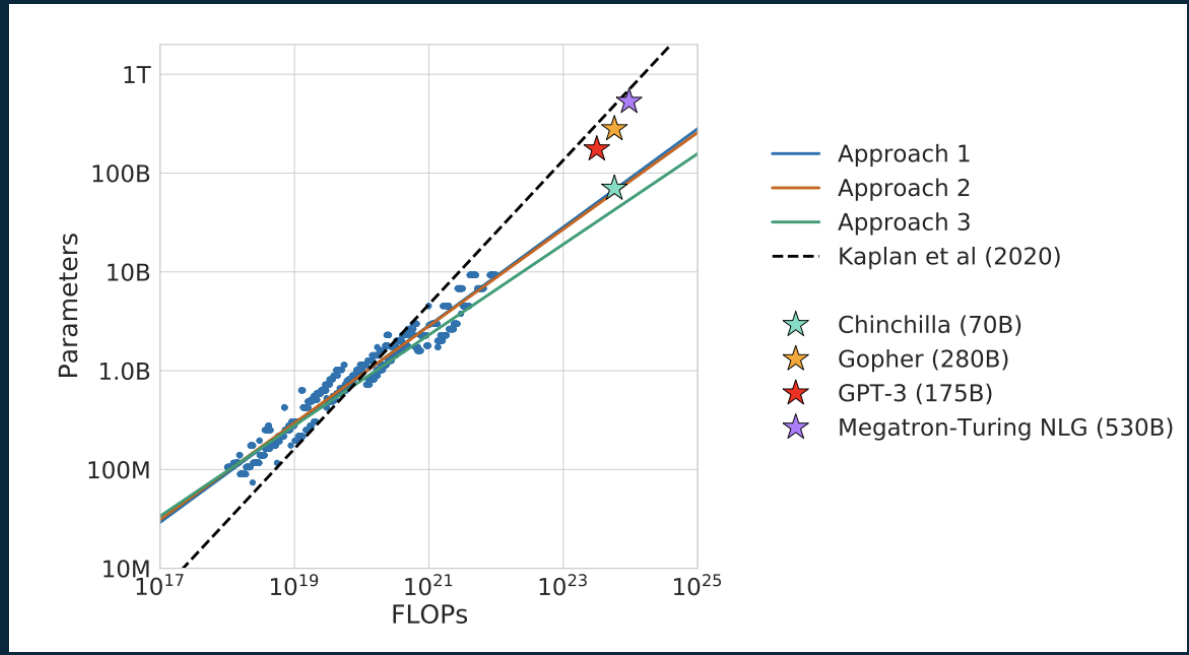
Grok

[1] https://www.ai.gov/action-plan

Davidson

Compute-to-Capability Pipeline

- LLM's are built on the transformer architecture
  - Ideal architecture for GPU training
  - More data + more parameters + more compute = better LLM (power law relationship)
- **The Compute-to-Capability Pipeline:** More compute *directly* leads to more capable LLMs. LLM scaling laws have guided top research organizations.
- A nation's ability to develop, train, and deploy the largest AI models is now a direct measure of its potential power on the global stage.



LLM Scaling Laws [1]. Demonstrating relationship between number of parameters and compute

[1] https://arxiv.org/abs/2203.15556

Davidson

US vs China AI Philosophy

- **U.S. Strategy: Market-Led**
  - Our most powerful models (GPT-5.3, Gemini 3.1, Claude Opus 4.6) are incredibly capable, proprietary, and controlled by a few key industry partners.
  - AI Action Plan and Executive Orders
- **China Strategy: State-Led**
  - Military Civil Fusion -> Dual-use by design. AI Global Governance Action Plan
  - 15-30% of LLM usage today is with Chinese open-source models
  - Top open-weight models are globally available, easily modified, and can be weaponized by anyone from peer adversaries to non-state actors.
- **Implication for National Security:** We must be prepared to face adversaries using highly customized, unpredictable open-weight models that are not in our threat libraries and can evolve outside our visibility.

New Era of Power – Importance of Compute

- Training state-of-the-art models requires data centers at an unprecedented scale
  - OpenAI estimated to spend ~$12B in 2024 for training / inference [1]
  - xAI plans to expand Colossus to 1 million GPUs [2]
  - Nvidia shipped 3.76M data center GPUs in 2023 [2]
- Why does this matter? -> More compute leads to better models, with higher-quality outputs
  - Improved Decision Making to achieve Decision Advantage
  - Improved adversarial capabilities for cyber attacks

Nvidia H100

[1] https://www.arcade.dev/blog/ai-inference-economics
[2] https://www.datacenterdynamics.com/en/news/xai-elon-musk-memphis-colossus-gpu/

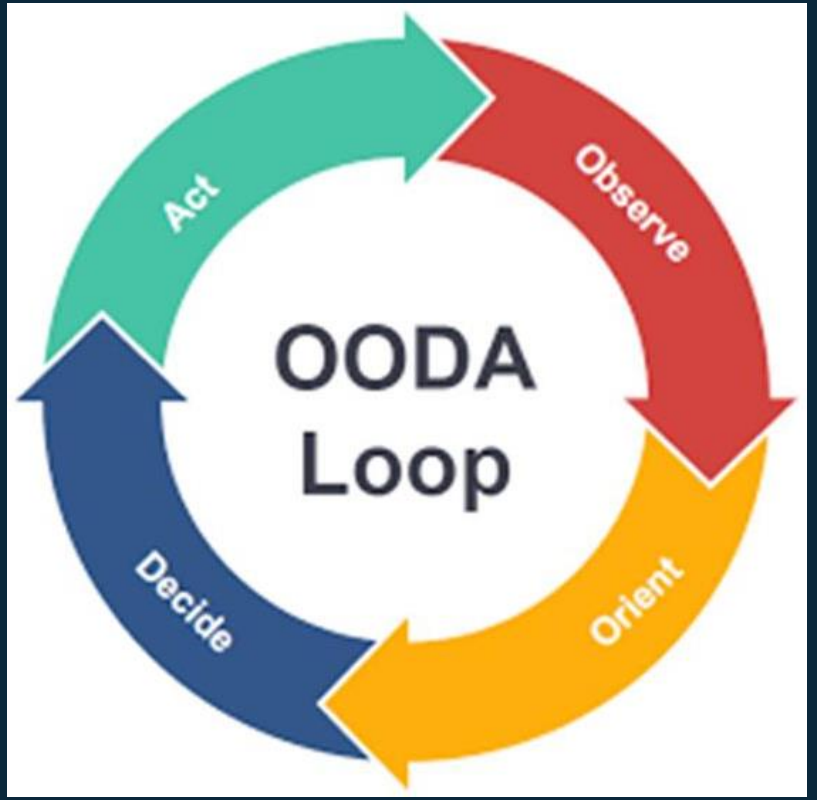
Davidson

Decision Advantage

- The product of situational understanding, the ability to assure and exchange information, make and communicate decisions by maintaining advantages in all domains. [AFDP 3-99]
  - Battlespace awareness and understanding
  - Adaptive force planning and application
  - Fast, precise, and resilient kill chains
  - Resilient sustainment support
  - Efficient enterprise business operations
- Decision advantage is a continuous process of transforming data into information, and information into decisions.

AI for Decision Advantage

- CJADC2
  - Proliferation of data and sensors (HUMINT, CYBINT, GEOINT, OSINT, SIGINT)
  - Main challenge: Data integration, sensor fusion, and interoperability
- AI applications
  - Sensor fusion to build a Common Operating Picture
  - Predictive analytics to anticipate adversary actions
  - Autonomous systems
- Main objective: Increase speed of OODA loop

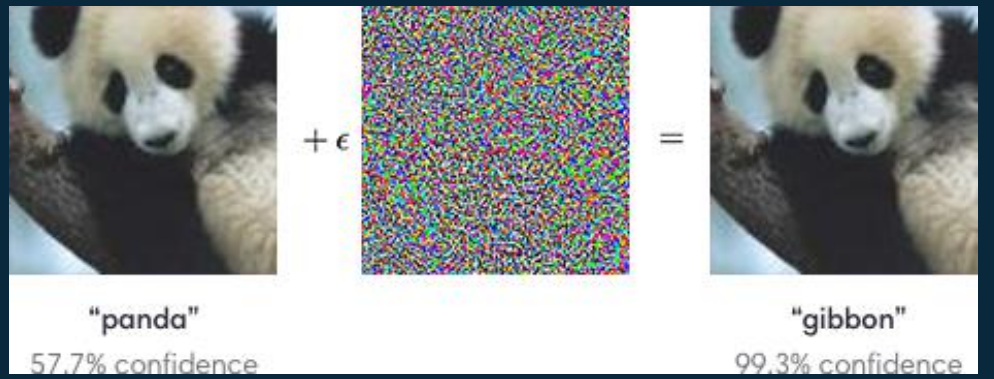


AI Applications

- Project Maven
  - Computer vision to identify and classify objects of interest from imagery and full-motion video
  - 18th Airborne targeting cell achieved same time performance with 20 people compared to 2000 people during Operation Iraqi Freedom [1]
- PANDA: Predictive Analytics and Decision Assistant
  - AFLCMC Program of Record for Condition-Based Maintenance
  - Predict maintenance issues -> Saves thousands of maintenance hours per year
- Navy Task Force 59
  - Unmanned vehicles (UUV / USV / UAV) equipped with variety of sensors
  - Identify suspicious maritime behaviors and cue manned ships to investigate
- Commercial solutions such as Palantir AIP, Anduril Lattice, LM DIAMONDShield, and others focused on using and enabling AI to improve decision advantage

[1] https://cset.georgetown.edu/wp-content/uploads/CSET-Building-the-Tech-Coalition-1.pdf

AI Shortfalls



- AI has different failure modes than humans
  - AI can be brittle to changing inputs.
    - Maven was primarily trained for desert environments and did worse in non-desert environments [1]
    - For LLM applications, changing a single word can alter the output
  - AI explainability is a hard problem
  - AI is vulnerable to adversarial attacks
    - Slight modifications to input data can be engineered to cause AI misclassification
- Why does this matter? -> Reduction in AI Trust

If a commander does not trust AI, how can we expect them to use the recommendations when soldier's lives are on the line?

[1] https://www.deeplearning.ai/the-batch/maven-a-system-that-analyzes-satellite-data-to-identify-targets-in-real-world-conflicts/

Warfare Transformation: Decision Advantage

- **Major Focus:** Get AI in hands of users to gain trust in system over time.
  - Human in the loop, with slow gradient towards true autonomous control
  - Some applications require AI due to volume or current lack of manpower (Computer Vision)
  - Use AI when risk level is appropriate
- Decision Advantage use cases include Intelligence (ISR), Command and Control, Autonomy, and Predictive Maintenance among many others
- **The Ultimate Objective: Decision Advantage.** Using AI to sense, make sense, and act faster and more effectively than any adversary, giving commanders a decisive edge.

- **Cybersecurity:** AI is a force multiplier for offensive and defensive cyber operations, autonomously processing vast amounts of data to enhance threat intelligence, threat hunting, and offensive capabilities.

AI Reconnaissance & Intelligence Gathering

- **Reconnaissance is the precursor that shapes offensive cyber operations.**
- AI accelerates OSINT and CYBINT processing beyond human limits
  - China is accelerating this as shown in CrowdStrike Global Threat Report; highlighting a 150% surge in China state-sponsored espionage attacks [1]
  - Chinese spy services have invested heavily in artificial intelligence to create new tools to speed analysis [2]
- **Iran Utilizes GenAI for Vulnerability Research and Exploitation.**
  - In 2024, Iran-nexus actors increasingly explored GenAI for vulnerability research and exploit development [1]
- Primary goal is to improve efficiency and sophistication of espionage, propaganda, and offensive cyber efforts.

[1] CrowdStrike 2025 Global Threat Report
[2] https://www.recordedfuture.com/research/artificial-eyes-generative-ai-chinas-military-intelligence
[3] https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/#:~:text=Forest%20Blizzard's%20use%20of%20LLMs,TTPs%20using%20the%20following%20descriptions

Offensive Cyber Autonomy

- Recent benching of generative AI models in security challenges showed problem success rate of 61.4% [1]
- **HexStrike AI:** New AI orchestration framework dramatically accelerates threat actor capabilities, reducing complex exploit times from **days to minutes.**
- Within hours of non-trivial Citrix vulnerability release, HexStrike was used with success in exploit [2]
- **China's approach**: Per FBI Cyber leadership, Chinese operators are actively experimenting with AI across the **entire attack chain,** not always perfect, but **efficiency and speed gains matter**.[4]

Real-World Performance

Operation	Traditional Manual	HexStrike v6.0 AI	Improvement
Subdomain Enumeration	2-4 hours	5-10 minutes	**24x faster**
Vulnerability Scanning	4-8 hours	15-30 minutes	**16x faster**
Web App Security Testing	6-12 hours	20-45 minutes	**18x faster**
CTF Challenge Solving	1-6 hours	2-15 minutes	**24x faster**
Report Generation	4-12 hours	2-5 minutes	**144x faster**

HexStrike AI Performance benchmarks [3].
Demonstrating improvement in pentesting operations

[1] https://arxiv.org/pdf/2506.14682
[2] https://blog.checkpoint.com/executive-insights/hexstrike-ai-when-llms-meet-zero-day-exploitation/
[3] https://github.com/0x4m4/hexstrike-ai
[4] https://www.theregister.com/2025/04/29/fbi_china_ai/

Davidson

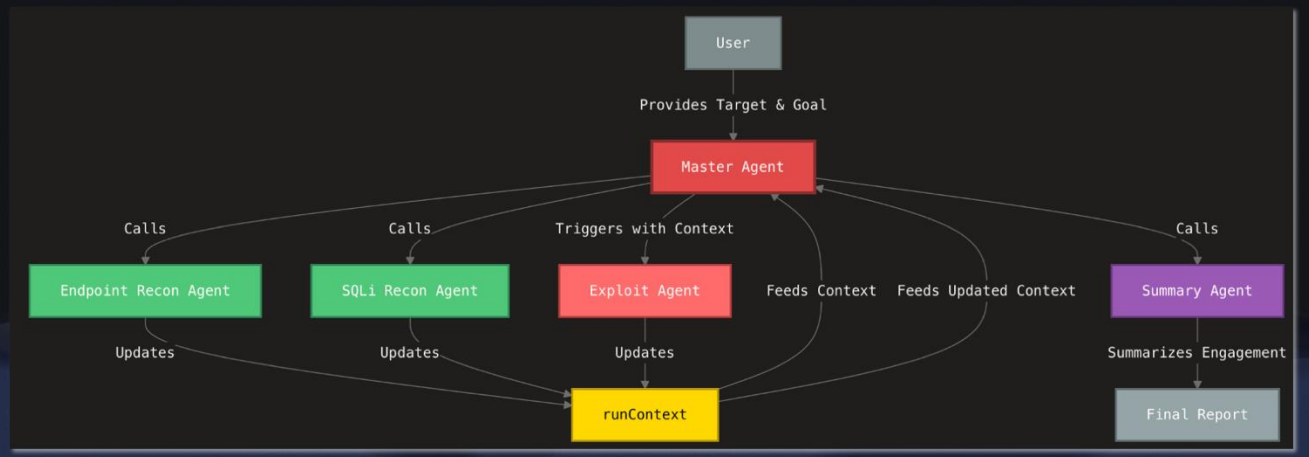
Offensive Cyber Autonomy

Automating Exploitation with Agentic Systems

2026 AI Symposium
Jason Kearns | Principal Enterprise Solutions Architect
Davidson Technologies

Automating Exploitation

Engagement: E-Commerce db exfiltration



AI Driven Attack Development

- **Largely focused around dual-use and open-source technologies.**
- **Weaponizing:** China's open-sourced DeepSeek model is found to be trivial in breaking safety mechanisms, easily supporting development of functional malware, including ransomware code from scratch [1]
- **Intelligence:** China's PLA fine-tuned Meta's open-sourced Llama language model into tool called "ChatBIT", optimized for military intelligence analysis and possible strategic planning [2]
- Voice phishing (vishing) attacks, where adversaries call victims to amplify their activities with persuasive social engineering techniques, saw explosive growth, up 442% between the first and second half of 2024. [3] Russian cyber gangs demonstrate repeat success with this method, posing as IT staff.

[1] https://www.csis.org/analysis/delving-dangers-deepseek
[2] https://www.reuters.com/technology/artificial-intelligence/chinese-researchers-develop-ai-model-military-use-back-metas-llama-2024-11-01/
[3] CrowdStrike 2025 Global Threat Report

DarkGPTs

- Malicious GenAI variants marketed on darknet/hacker forums that remove safety filters and produce harmful outputs (malware, phishing, obfuscation).
- **Evil-GPT and WolfGPT:** Described as a cheap “Malware factory” particularly appealing to low-skilled hackers, drawing on extensive datasets of existing malware. [1][2]
- **Operational Impact:** Lowers the skill barrier, shortens development time, and contributes to attribution blur.

Example output of WolfGPT for process injection in C++ language.

[1] https://www.qsolit.com/evil-gpt-the-enemy-of-chatgpt/#:~:text=In%20the%20ever%2Devolving%20landscape,task%20ChatGPT%27s%20ethics%20would%20block.
[2] https://blog.barracuda.com/2025/08/28/wolfgpt-upgraded-dark-ai-malware

Davidson

Lowering the Bar

- GenAI lowers the technical expertise needed for cyber attacks.
  - Readily available open-source tools accelerate attack development and dissemination.
  - Malware-as-a-Service offering subscription-based AI services for creating hacking tools and executing attacks.
- Accelerated reconnaissance and attack development using agents
  - Adds ability to prioritize and build cyber kill chains and operational security actions without technical depth

The gap between an Advanced Persistent Threat and a capable, resource-constrained actor is narrowing.

Davidson

Force Multiplier

- Agentic offensive systems greatly enhance and scale threat actor capability
  - Making every malicious actor more efficient
  - Why does this matter? -> Active paradigm shift threat landscape
  - Autonomous AI agents performing multiple steps of an attack from initial research to vulnerability exploitation
- Recent Anthropic report on 'Disrupting the first AI-orchestrated espionage campaign'
  - Targeted 30 organizations through orchestration agents

The gap between an Advanced Persistent Threat and a capable, resource-constrained actor is narrowing.

Davidson

AI-Informed Threat Hunting (Proactive Defense)

- Threat hunting is a proactive method that looks for signs of compromise or indicators of compromise (IOCs)
- **Traditional Threat Hunting**
  - Data overload with sheer volume of information generated by modern networks
  - Manual log & telemetry review leading to difficult event correlation
- **AI / Agentic AI Threat Hunting**
  - Autonomy in routine data correlation and enrichment tasks
  - Enhances ability to detect subtle patterns missed by human analysts
- US Cyber Command seeking innovative solutions on challenge sets to include AI-assisted Cyber Threat Hunting, Defensive Cyberspace ops and continuous monitoring [1]

[1] https://www.cybercom.mil/Portals/56/Documents/Cyber%20Command%20Problem%20Set%203rd%20Edition.pdf?ver=peIH1oSQMl5uvPQxB4Cs-g%3D%3D

AI Transformation on National Security

- **Geopolitics:** Active race for algorithmic superiority, fueled by compute.
- **Warfare:** The battlespace is accelerating to machine speed, making the vision of CJADC2 unachievable without an AI backbone.
- **Adversary Capabilities enhanced by AI:** GenAI is enabling accelerated development of increasingly sophisticated and autonomous offensive capabilities while amplifying information warfare and disinformation.
- **Infrastructure:** With the rise of GenAI, large data centers are now key targets for adversaries that must be defended due to national security implications

Key Takeaways

- **The Strategic Landscape Has Fundamentally Changed.** The AI competition with our pacing threat is a defining element of our national security.
- **AI-Enabled attacks are increasing in sophistication, speed, and scale.** Defensive postures that worked yesterday won't hold tomorrow. AI shifts the tempo of conflict to machine speed.
- Our ability to securely develop, deploy, and adapt AI faster than our competitors will define our strategic position for the coming decades.

Q&A

- Contact Info
  - Jack Francis: jackfrancis@davidson-tech.com
  - Jason Kearns: jasonkearns@davidson-tech.com

Thank You!

February 26, 2026

LONE STAR
NCMS CHAPTER 28

Davidson