THE EVOLVING AI LANDSCAPE IN NATIONAL SECURITY

DAVID SPIRK

SENIOR COUNSELOR, PALANTIR TECHNOLOGIES

AI COMMISSIONER, GLOBAL TECH SECURITY COMMISSION

FORMER CHIEF DATA OFFICER, DEPARTMENT OF DEFENSE

WE MUST SPEED OUR ADOPTION OF AI IN NATIONAL SECURITY

- **The Digital Battlefield Demands Speed:** Events in Ukraine underscore the need for rapid AI integration across government and allies. Failure to adapt means ceding ground to adversaries building vast digital arsenals.
- **Information Warfare is Paramount:** Winning the narrative and dispelling misinformation are as vital as overwhelming force. AI will be pivotal for truth in an era of deepfakes and disinformation campaigns.
- **Data as the Strategic Asset:** Data fuels dominance in this new conflict landscape. AI-driven analysis and decision-making will determine who leverages data for decisive advantage.
- **A Whole-of-Nation Mobilization:** Meeting this existential challenge demands unprecedented mobilization of resources, talent, and partnerships across the US government and beyond.

AI COMPETITION WITH THE PRC: OUR LEADERS' WORDS

- "In this era of strategic competition with the [People's Republic of China], the advantage will always go to the country that uses AI and associated technologies better, faster, smarter and safer," Deputy Secretary of Defense Hicks said.

- "This competition ((with China)) also exploits technological advancements such as AI, biotechnologies and related biosecurity, the development and production of microelectronics, and potential quantum developments- to gain stronger sway over worldwide narratives affecting the global geopolitical balance, including influence within it," Director of National Intelligence Haines said.

- "China today poses a set of growing challenges to our national security…we believe there are three families of technologies that will be of particular importance over the coming decade: first, computing-related technologies, including microelectronics, quantum information systems, and artificial intelligence…we will continue to take action to protect our advantage and maintain as large a lead as possible in these foundational technologies," Secretary of Commerce Raimondo said.

Strengths

What do we need to capitalize on?

1. **Leading AI companies.** The US is home to most companies leading AI development (i.e., Nvidia, Alphabet, Amazon, Microsoft, Palantir, OpenAI, etc.). This provides access to an ecosystem of capable products and trusted partners for the government to leverage in solving national security challenges.
2. **World Class Academic Institutions**. The US has prestigious educational institutions, (i.e., MIT, Stanford, Carnegie Mellon, the University of Texas, Purdue, etc.) , which are at the cutting edge of AI research. These institutions draw leading talent from around the globe, which contribute to the domestic technology base while allowing the U.S. to directly influence the norms, priorities, and values for AI research.
3. **Start Up Ecosystem.** The US has a robust venture capital and private equity ecosystem that supports AI startups by incentivizing the rapid transition of new developments into commercially viable product lines that have dual-use implications with slight modifications for national security use in high consequence operations.
4. **Open and Collaborative Research Culture.** The US has an open and collaborative research culture that fosters sharing across disciplines, across institutions, and among nations that enable more rapid indentation of potential AI solutions and dissemination of effective approaches.
5. **Field Experience in AI Application.** Elements of the DoD and Intelligence Community, among others, are facilitating a campaign of learning in the adoption data-driven technologies at large scale in a variety of diverse, austere, and demanding circumstances.

Weaknesses

What do we need to overcome?

1. **Insufficient government investment in AI research and development (R&D).** The US needs to increase its investment—and outcome-based expectation/oversight--in AI R&D to maintain its competitive edge..
2. **Limited access to high-quality data.** Access to large, diverse, and high-quality datasets is crucial for training AI systems. The US has some data limitations due to privacy concerns, fragmented data sources, legacy tech infrastructure, and a lack of data sharing between organizations.
3. **Lack of investment in data and model protect.** At this time, AI models are inherently fragile and easily fooled by intentional actors and/or data slippage in real-world environments and operations, which requires significant investment in capabilities to monitor, identify, and protect algorithms employed in high consequence situations.
4. **Regulatory challenges.** The US needs to develop a clear regulatory framework for AI that addresses issues such as ethics, privacy, liability, and security. This framework must provide useful, predictable guardrails that uphold our values without being inflexible, onerous, or harmful to open innovation and competitiveness.
5. **Inadequate education and workforce development.** The US education system needs to be revamped to incorporate digital skills from the K-12 level to higher education, focusing on creating a growing and diverse talent pipeline. Many times we train our competitors by not providing international students with a visa to remain in the US. Additionally, there are few programs exist to increase data fluency of the current workforce throughout commercial and national security sectors

Opportunities

What do we need to leverage?

1. **Strong innovation ecosystem.** The US has a robust innovation ecosystem, with world-class universities, research institutions, and a thriving technology industry; expanding collaboration and partnerships among these stakeholders will drive AI advancements and facilitate learning in the national security sector.
2. **Access to private capital.** The US has a mature venture capital and private equity investment environment that can provide financial resources for AI startups and research initiatives; facilitating access to this capital will fuel AI innovation and growth while incentivizing venture capital and private equity funds through favorable tax incentives for investment in data-driven technologies and its underlying compute and transport requirements.
3. **Access to Development Infrastructure.** The US should increase innovation amongst universities, not for profits, and startups by subsidizing significant portions of the cost of the leading cloud compute providers (e.g., Google Cloud Platform, Azure, Amazon Web Services, and Oracle); thereby lowering the barrier to experimentation and development.
4. **Diverse talent pool.** The US and its partners and allies have a diverse population with a wealth of expertise in various fields; this diversity can be harnessed to drive interdisciplinary AI research and applications, addressing complex challenges to accelerate the application of data-driven tech in the commercial and national security sectors.
5. **Leadership in key markets.** The US has already made significant progress in AI across various sectors such as healthcare, finance, and transportation. Building on these successes, the country can exploit AI's potential in other domains and industries.

Threats

What do we need to prepare for or mitigate?

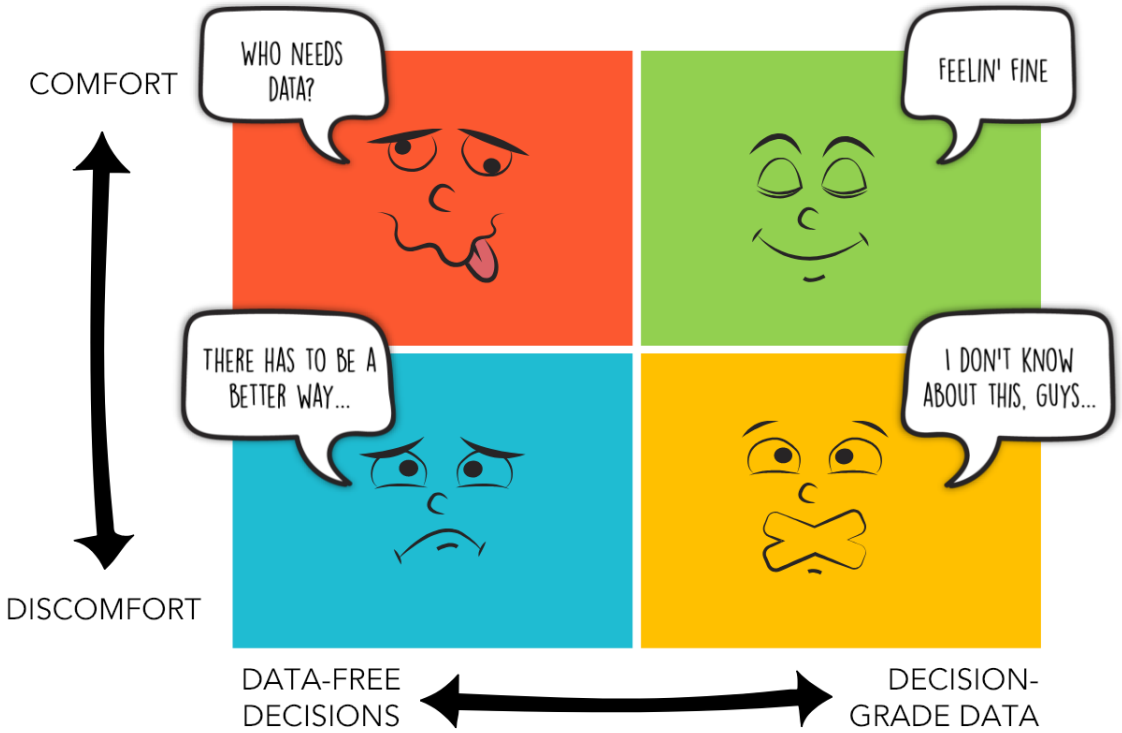
1. The Chinese Communist Party is distorting markets in its favor by **supporting the growth, development, and export of its domestic AI companies** (e.g., Baidu, Alibaba, Tencent, and Huawei), by providing them with favorable policies, financial incentives, and access to government resources for R&D with less concern of failure impacting bottom line.
2. The Chinese Communist Party is **investing in domestic and international universities and research institutions** to improve their AI research capabilities and attract top talent from around the world.
3. The Chinese Communist Party wages **an information operations campaign against the population of the US and its partners and allies to sow distrust in AI and force the overregulation of data and governance** slowing the adoption of data-driven technology across the commercial and national security sectors. They are also influencing international regulatory bodies to set standards consistent with their values.
4. The Chinese Communist Party **incentivizes intellectual property theft, state-sponsored espionage, and forced technology transfers** while expanding the footprint of their nationalized private sector around the globe with what appears to be comparable information technology at a discount rate.
5. The Chinese Communist Party leverages the **global proliferation of its domestic AI and defense related companies to gain—overt and covert—exclusive access** to additional large diverse data sets for AI training.

GLOBAL TECH SECURITY COMMISSION

US-CHINA SWOT ANALYSIS

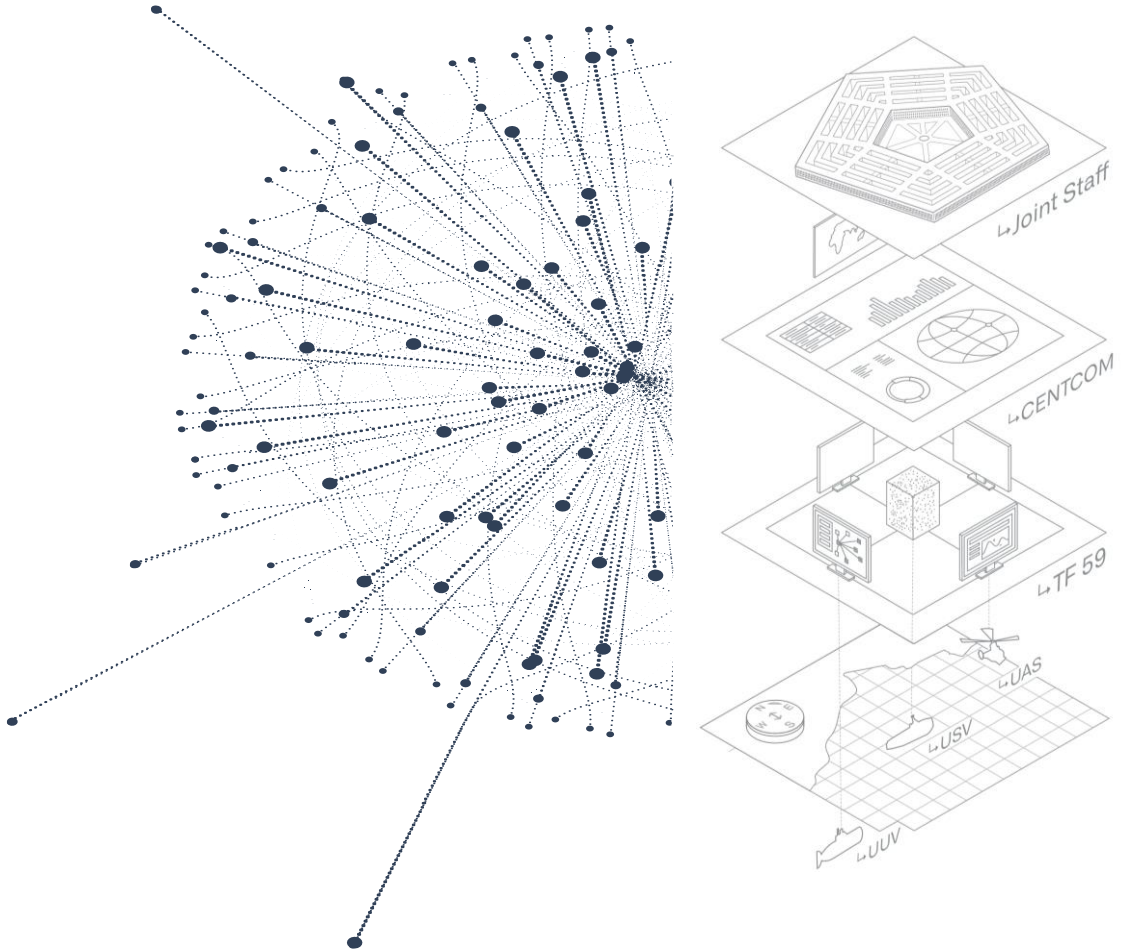
FOCUS ON TALENT, NOT TOOLS

- **Prioritize People Over Tech:** Data fluency in operators and analysts is the key to long-term success. "Relentless incrementalism" empowers them to drive innovation and doctrinal shifts.
- **Tap the Widest Talent Pool:** USG needs to forge non-traditional partnerships across industry, academia, and civil service to attract the best minds.
- **Data Fluency as a Core Competency:** Every person in the USG should build data literacy as a vital part of their expertise. Leaders should champion data-driven decision-making.
- **Change Starts at the Top:** A "Data and AI Day" alongside executive-level data education signals the importance across the board. Data skills should factor into training and promotions.



RESOURCE AND PROCURE A FLEXIBLE DATA ARCHITECTURE

- **Outdated Data Architecture Impedes Progress:** Legacy data systems with rigid standards put the USG behind the innovation curve. A flexible, open-standard architecture is essential for adapting to the commercial data landscape.
- **Cloud Compute Power at the Edge is the Future:** True compute power must be accessible in disconnected environments. Data-driven tactics developed at the edge will drive wider doctrinal change.
- **IT as an Operational (aka, Warfighting) Domain:** CIOs need the resources and authority to procure and deploy IT solutions rapidly, just like other operational/battlefield necessities. Outdated cybersecurity protocols hinder progress.
- **The Result: Seamless Coalition Data at the Speed of War:** A zero-trust approach with advanced encryption is crucial. This enables real-time, secure data sharing with allies, outpacing adversaries in the decision-making cycle.



From strategic leaders through operational leaders to tactical operators

ENCOURAGE A CONTINUOUS CAMPAIGN OF LEARNING

- **The Virtuous Cycle of Learning:** Persistent integration of cutting-edge tech in real-world operations fuels talent growth, uncovers IT gaps, and reveals the precise policy changes needed for accelerated data-driven decision-making.
- **Success Stories Drive Progress:** DoD/IC/DOS examples showcase the transformative power of data-driven tech for warfighter missions. This model must be expanded across the USG.
- **Partnership for Precision:** Industry-operator collaboration enables real-time refinement of capabilities and the surgical removal of outdated policies, aligning the USG with industry's adaptability.
- **Beyond Tech: It's About People:** Emphasize that this campaign prioritizes data fluency across the USG workforce, empowering them to drive the adoption of data-driven decision-making for global competitiveness.

CONCLUSION

- **Our national security professionals are moving out**
- **It is an ongoing competition with the nation-state competitors who want AI dominance**
- **America and our partners and allies citizens and their creativity is a true advantage we must continue to enable**
- **We must resource the modernization of our information technology and data architecture to build a modern future-proof base across our commercial and government sectors**
- **Learn by doing and don't over regulate your way out of the virtuous learning cycle**

THANK YOU!