

Chapter 3: AI Compute Categorization Framework

Overview: *The U.S. AI strategy envisions a three-tier framework for allocating compute resources to different classes of AI use-cases. These notional categories are:*

- **Category A-1:** *Essential Warfighting & National Intelligence AI* – mission-critical defense and intelligence applications requiring privileged siting, assured compute/power, and low-latency integration with military operations (e.g. real-time battle management, autonomous weapons, multi-INT fusion, cyber defense).
- **Category A-2:** *Strategic National Advantage AI* – high-impact scientific and societal applications where U.S. compute and model access drive innovation or resilience (e.g. climate modeling, public health forecasting, advanced materials discovery, DOE science workloads, standards/testbeds, critical infrastructure simulations).
- **Category B:** *General Commercial & Consumer AI* – all other AI deployments in the broader economy (from enterprise software to consumer-facing AI services).

Below, we substantiate this framework by examining whether such distinctions appear in policy or scholarship, identifying representative workloads and responsible agencies for A-1 and A-2, and exploring how compute for each tier might be segregated or prioritized. We also compile authoritative language differentiating national security-relevant AI from commercial AI, and highlight voices advocating for (or against) special prioritization of AI compute in the national interest.

3.1 Recognition of a Tripartite Categorization in Policy & Literature

Is this 3-class model formally recognized? No single authoritative document explicitly lays out an “A-1/A-2/B” triad; however, **the concept of segregating AI/compute by mission-criticality is supported implicitly in several strategies and analyses.** For example, the DoD’s High Performance Computing Modernization Program (HPCMP) emphasizes *securely delivering a spectrum of HPC capabilities* to meet different priority needs – from “**Large-Scale Classified Computing**” for defense to “**Open Research**” for general science ¹. This echoes the idea that “**military and intelligence AI**” use cases demand dedicated, often classified infrastructure distinct from open commercial clouds. Likewise, recent U.S. export control frameworks differentiate **frontier AI compute for national security** from sub-frontier compute for broader use: the “**AI Diffusion Rule**” introduced in late 2024 created *tiers of access* to advanced GPUs by country, effectively reserving top-tier compute for the U.S. and close allies ². While that policy sorts *nations* into three tiers rather than domestic use-cases, it reinforces the notion that **access to the most capable AI computing is a strategic asset to be managed**, especially for security-related purposes.

Policy strategies do distinguish national security AI vs. commercial AI, even if not with the exact A-1/A-2 labels. The **National Security Commission on AI (NSCAI)** warned that “*America is not prepared to defend or compete in the AI era*” and urged a **whole-of-nation strategy** both to “*defend against AI threats*” and “*win the broader technology competition*” ³. This reflects an understanding that **government must prioritize AI resources for national security and critical missions**, beyond what the private sector pursues commercially. Consistently, White House strategy has framed leadership in AI as a *national security*

imperative in addition to an economic one. For instance, the 2025 “**America’s AI Action Plan**” states that as rivals race ahead, “*it is a national security imperative for the United States to achieve and maintain unchallenged technological dominance*” in AI ⁴. Such language differentiates AI endeavors that underpin **national power** from those that are simply market-driven.

Academic and think-tank literature also supports the spirit of this categorization. Analyses from organizations like CNAS and CSIS argue that control of **frontier compute** will determine AI leadership and thus geopolitical advantage ⁵ ⁶. They often implicitly carve out **military/intelligence AI** as a special class, given its requirements and risks, and **public-good AI** (scientific research, societal needs) as another priority class – leaving **general commercial AI** as the default remainder. In summary, *while the exact three-category taxonomy is novel*, it is **consistent with documented distinctions** between (1) **mission-critical national security AI**, (2) **strategic public-sector/innovation AI**, and (3) **widely distributed commercial AI** in U.S. strategy.

3.2 Category A-1 – Essential Warfighting & National Intelligence AI

Category A-1 encompasses **AI applications at the core of military operations and intelligence—those that provide a direct warfighting edge or intelligence advantage**. These use-cases are often classified or highly sensitive, require robust and dedicated compute/energy resources (potentially even in conflict zones or secure facilities), and must operate with minimal latency and maximal reliability under doctrinal timelines. **Key A-1 workloads and implementing agencies include:**

- **Intelligence, Surveillance & Reconnaissance (ISR) AI:** The U.S. has deployed AI to analyze the deluge of sensor data collected by drones, satellites, and other ISR platforms, augmenting human analysts. *Project Maven* is a flagship example – a DoD initiative (now operationally controlled by the NGA) that uses machine learning to process full-motion drone video and **automatically detect/classify potential targets** ⁷. NGA (with NRO) runs geo-intelligence AI services from Maven to flag objects of interest in imagery, accelerating target recognition for warfighters. Similarly, **facial recognition and pattern analysis AI** are being prototyped to sift intelligence feeds for persons or signals of interest ⁸. The NSA is applying AI in its SIGINT mission as well – NSA Director Gen. Nakasone noted “*we use artificial intelligence primarily within our signals intelligence mission*”, underscoring that NSA is leveraging AI/ML to triage vast intercepts and identify threats ⁹. These efforts, alongside **multi-INT fusion** (combining SIGINT, IMINT, MASINT), often fall under the purview of the **Intelligence Community (NSA, NGA, NRO, DIA)** in partnership with the DoD’s Joint AI efforts.
- **Autonomous Weapons & Combat Systems:** AI is being integrated into weapon systems to enable greater autonomy and faster reaction loops in combat. A prime example is DARPA’s **Air Combat Evolution (ACE)** program, which successfully demonstrated AI dogfighting in simulated aerial combat ¹⁰. ACE’s AI-driven autonomy allowed a fighter jet to perform within-visual-range maneuvers and engagements, a stepping stone to future “**loyal wingman**” drones that fight alongside human pilots. This feeds into DARPA’s “**Mosaic Warfare**” vision, where many expendable unmanned systems (air, land, sea) operate as a coordinated swarm using AI – overwhelming the enemy with distributed “tiles” rather than a few exquisite platforms ¹¹ ¹². The **U.S. Air Force and Navy** have likewise tested **robotic wingmen and autonomous ships**; for instance, the Sea Hunter drone ship uses AI to navigate and track submarines. Many such programs are funded by DARPA (STO/TTO offices) and executed with the Services (e.g. USAF). These systems place extreme demands

on compute during development (for simulation and training of AI models) and require specialized onboard inference hardware for real-time operation.

- **Battle Management, Targeting, & C2 Decision Aids:** AI-driven decision support for command and control is a major A-1 focus. The Army's **FIRESTORM** system (FIRES Synchronization to Optimize Responses in Multi-Domain Operations) exemplifies this category: FIRESTORM ingests sensor data from multiple domains, uses terrain mapping, and then **recommends the optimal weapon system to engage each target**, all in seconds ¹³. In trials, prior systems took ~20 minutes to relay targeting data, whereas FIRESTORM did so in **32 seconds**, dramatically accelerating the kill-chain ¹⁴. This AI was the “megastar” of the Army's Project Convergence exercise and is envisioned to fundamentally change how commanders fight ¹⁵. It was integrated with the Air Force's Advanced Battle Management System (ABMS) during tests ¹⁶, showing how an AI-driven C2 node can plug into Joint All-Domain Command and Control (JADC2) networks. *Agencies involved:* Army Futures Command (NGCV CFT and others developed FIRESTORM with Army CCDC Armaments Center ¹⁷), the Air Force C2 enterprises (for ABMS), and the DoD CDAO. Likewise, NORTHCOM's Global Information Dominance Experiments (GIDE) applied AI to fuse data for **anticipatory command decisions**, and DARPA's ACE (noted above) also scales to **campaign-level battle management** with AI ¹⁸. All these efforts highlight the **C2 and targeting AI** work led by DoD entities like CDAO, DARPA, Army AI Task Force etc., often with Combatant Command involvement.
- **Cyber Defense AI:** Defending military networks and critical infrastructure from cyberattack is another essential warfighting application for AI. DoD and NSA are investing in AI to monitor networks, detect anomalies or intrusions, and respond at machine speed. Gen. Nakasone confirmed that U.S. Cyber Command (which he also leads) has a *five-year AI plan* for “**the realm of cyberspace operations**” ¹⁹. This likely includes AI tools for threat hunting (“hunt forward”) and automated cyber defense systems. The exact programs are mostly classified, but the DoD has prototyped things like “**Project HVAC**” (AI for network threat detection) under JAIC, and NSA's new AI Security Center will focus on securing AI and using AI for security ²⁰. *Agencies:* **NSA and USCYBERCOM** drive many of these efforts, with support from DARPA (which has run programs on AI for cybersecurity).
- **Other A-1 Use Cases:** Additional examples include **electronic warfare (EW)** and **sensor fusion** – AI that can recognize jamming or radar signals and adjust responses faster than human operators. The Air Force has experimented with AI for **EW signal classification**. The DoD is also applying AI to **predictive maintenance** on military platforms (to enhance readiness), which, while not direct combat, is critical to sustaining warfighting capability ²¹. Even logistics and wargaming are seeing A-1 AI applications (e.g., AI planning tools for mission logistics). While these may blur into broader DoD enterprise AI, the **National Defense Strategy** and DoD AI Strategy make clear that “*accelerating AI adoption to deliver tangible solutions for the warfighter*” is a top imperative ²² ²³. Indeed, over 1,000 AI projects were reportedly underway in DoD as of 2023 ²⁴, many aligned to A-1 needs.

Agencies running A-1 AI: The **Chief Digital and AI Office (CDAO)** is the DoD focal point for warfighter AI delivery, coordinating projects across the services ²⁵ ²⁶. Within the military services, organizations like **Army Futures Command (AFC)** and its AI Task Force, the **Air Force Life Cycle Management Center (for ABMS/C2)**, the **Navy's Project Overmatch**, and the Marine Corps Warfighting Lab all sponsor A-1 AI prototypes. The **Intelligence Community (ODNI, CIA, NSA, NGA, NRO)** similarly drive A-1 through their tech directorates – for instance, NGA's AI portfolio (which includes Maven's algorithms for GEOINT) and NSA's internal AI developments for SIGINT. **DARPA** remains a key engine for emerging warfighting AI

(Mosaic Warfare, ACE, OFFSET swarming, etc.), handing off successes to the Services. And not to be overlooked, the new **JAIC-derived** initiatives (under CDAO) and the service labs (e.g. Army Research Lab's AI projects, Air Force Research Lab's Skyborg autonomy) are implementing these technologies. In short, Category A-1 involves a **wide array of defense and intel agencies**, each focusing on the AI systems that give tactical advantage or safeguard national security. Many of these applications are still in R&D or early deployment – GAO notes that “*many AI capabilities that support DoD's warfighting mission are still in development*”, such as **AI for intelligence analysis, weapon system enhancement (drones, robotic ships), and battlefield decision aids for targeting** ⁸ .

3.3 Category A-2 – Strategic National Advantage AI

Category A-2 comprises **AI and HPC applications that, while not directly about combat, are vital to national well-being, economic strength, and sovereign resilience**. These are domains where leadership in AI **translates to strategic advantage** – for example, in scientific discovery, public health, energy, climate, and infrastructure. They typically require massive computing power (often provided by national labs or supercomputing centers) and are often government-funded or coordinated, since the outcomes benefit society or national capabilities broadly (beyond private ROI). **Prominent A-2 workloads and responsible agencies include:**

- **Climate and Earth System Modeling:** Accurate long-range climate forecasts and weather prediction are of immense strategic value (informing agriculture, disaster preparedness, military basing, etc.). AI-enhanced climate models are now running on the world's fastest supercomputers. Notably, the DOE's Oak Ridge National Lab unveiled *Frontier* (the first U.S. exascale supercomputer) which is being used to **run global climate simulations at unprecedented scale and resolution** ²⁷ . In 2023, Frontier enabled scientists to model worldwide cloud formation in 3D, shrinking “years of work into days” and yielding a “*new gold standard for climate modeling*,” according to Sandia's climate scientists ²⁸ ²⁹ . Such exascale-driven AI climate models (e.g. the E3SM Multiscale Modeling Framework) can integrate atmosphere, ocean, and ice data to project regional impacts decades out ³⁰ ³¹ . Agencies: **Department of Energy (DOE)** Office of Science funds much of this (the Exascale Computing Project and climate programs), in partnership with **NOAA** (which operates the National Climate-Computing Research Center at ORNL and runs climate/weather models on DOE machines) ²⁷ ³² . NASA and NSF also support climate AI research, but DOE's leadership computing facilities (like Frontier at ORNL and upcoming *El Capitan* at LLNL) are the flagship resources. Maintaining an edge in climate modeling is considered strategic – accurate climate insights can guide policy and infrastructure investments, and U.S. compute superiority ensures we aren't reliant on foreign models for critical forecasts.
- **Public Health Forecasting & Biosecurity:** The COVID-19 pandemic underscored the need for high-end computing and AI in epidemiology. DOE labs collaborated with NIH, CDC, and others to apply AI for drug discovery and to model disease spread. For example, **Lawrence Berkeley National Lab led a multi-lab effort to develop “ExaEpi,” an agent-based epidemic model that harnesses exascale supercomputers** to simulate pandemics for the CDC ³³ . ExaEpi, funded through DOE's Biopreparedness Research Virtual Environment (BRaVE), can use the full might of an exascale system to run city- or nation-scale disease spread scenarios in hours, helping public health agencies evaluate interventions ³⁴ . After success with COVID, DOE is now expanding this AI-driven tool to model other threats (influenza, cholera, etc.) with continued \$4M/year funding ³⁵ . The goal is a **generalized epidemic modeling AI** that can be rapidly adapted for new pathogens ³⁶ . Agencies:

This is a partnership between **DOE National Labs** (Berkeley, Argonne, Los Alamos, etc. all contributed) and the **CDC/HHS** for end-use. It highlights how **public health forecasting** using AI and HPC is treated as a strategic national capability, with DOE's compute enabling agencies like CDC to get faster, finer-grained forecasts for outbreak response. Similarly, DOE's AI was used to **optimize antibodies and drug candidates** during COVID (e.g. Oak Ridge's Summit supercomputer famously screened billions of molecules for potential antiviral drugs in 2020). Such efforts fall under A-2 because they bolster national resilience to biological threats through superior computing and AI.

- **Advanced Materials & Manufacturing Discovery:** The nation that can invent superior materials (for energy, defense, semiconductors, etc.) gains a competitive edge. AI is revolutionizing this discovery process by analyzing vast chemical/material datasets and guiding experiments. The DOE's programs in **"AI for Science"** explicitly target materials R&D: for instance, AI-driven *surrogate models* dramatically accelerate complex physics simulations, allowing scientists to explore materials' properties far faster ³⁷. This leads to breakthroughs in **battery materials, superconductors, alloys**, etc., which are essential for technology leadership ³⁸. DOE labs like Argonne and Oak Ridge have built **"self-driving labs"** where AI algorithms design and even conduct experiments autonomously to find optimal materials ³⁹. One DOE initiative (the Frontiers in AI for Science, Security and Technology program) is leveraging DOE's supercomputers to integrate AI into everything from **fusion energy research to high-energy physics** ³⁷. *Agencies: DOE Office of Science* and NNSA labs are primary, with partnerships in academia (Materials Genome Initiative) and NIST. NIST, while known for metrology, is involved in developing AI-driven standards for advanced manufacturing and in setting measurement benchmarks for new materials – effectively ensuring the U.S. sets the "ground truth" for next-gen tech. By investing in material-discovery AI, the U.S. secures its supply chains (e.g. discovering substitutes for critical rare elements) and maintains military-technological superiority (new armor, propulsion materials, etc.).
- **Energy Grid & Infrastructure Resilience Simulations:** Critical infrastructure (power grids, pipelines, transportation networks) can be modeled and enhanced with AI – a strategic need for both national security and economic stability. The Department of Homeland Security's **National Infrastructure Simulation and Analysis Center (NISAC)**, for example, develops *advanced analytic tools* to quantitatively assess risks to U.S. critical infrastructure ⁴⁰. These tools often use HPC and AI to simulate cascading effects of disasters (hurricanes, cyber-attacks, etc.) across interconnected systems ⁴¹ ⁴². By running such simulations, agencies can harden infrastructure and plan crisis responses. NISAC, managed by DHS's CISA with support from Sandia and Los Alamos National Labs, reflects an A-2 type mission: *applying big compute and AI to safeguard domestic infrastructure*. Similarly, DOE's national labs use HPC/AI to optimize the electric grid – for instance, AI models that can dynamically balance loads and integrate renewable energy, making the grid smarter and more resilient (DOE's Grid Modernization initiative). During extreme events, having superior predictive models (e.g. where will outages occur, how to reroute power) is vital. We also see NASA's use of AI for aerospace design or NIST's AI for building safety standards as A-2 examples – they enhance national capabilities indirectly tied to security and competitiveness.
- **Scientific Research & Innovation Platforms:** More broadly, **Category A-2 includes the AI workloads at national research facilities that drive American innovation forward**. This spans *NIH's biomedical AI* (for cancer genomics, etc.), *NASA's AI for space exploration*, *DOE's AI for high-energy physics* (e.g. *processing Large Hadron Collider data*), and more. The common thread is that **federal agencies treat compute for these AI-driven research areas as strategic resources**. The National

Science Foundation (NSF) and OSTP have proposed a **National AI Research Resource (NAIRR)** to democratize compute for academia, which can be seen as ensuring broad access to Category B compute for research, while **protecting truly critical workloads on separate infrastructure**. Even the Department of Defense engages in A-2 style work via the Defense Threat Reduction Agency (DTRA) and others for things like climate security or pandemic modeling, overlapping with civilian efforts.

Agencies and National Labs (A-2): Key players are the **DOE National Labs** (Oak Ridge, Lawrence Livermore, Argonne, Los Alamos, Sandia, etc.), which host the top supercomputers (Frontier, upcoming El Capitan, etc.) that power many A-2 projects. DOE's Office of Science sets priorities (e.g. Exascale Computing Project targets specific science grand challenges). **NOAA** operates major weather/climate computing (often in partnership with DOE – e.g. NOAA's *Gaea* supercomputer at ORNL runs climate models ⁴³). **NIH and NSF** fund AI-driven science on health and academia (the Covid19 HPC Consortium in 2020 brought DOE, NIH, NSF together with industry to grant researchers computing for pandemic solutions). **NIST** works on AI standards and has even solicited HPC support for AI testbeds ⁴⁴. **NASA** uses AI for Earth observation analysis and space tech (with its own supercomputers like Pleiades). The **DoD (DTRA, service labs)** cross over when national advantage AI overlaps with security (e.g. climate and stability, or materials for hypersonics). In all cases, **Category A-2 compute tends to reside in federally funded facilities or clouds**, not solely on commercial infrastructure, due to scale and often the sensitive or public-good nature of the work.

In summary, **Category A-2 covers the “strategic muscle” of national AI capacity beyond the battlefield** – ensuring the U.S. leads in the scientific and industrial domains that underpin long-term national power and resilience. The Frontier supercomputer's transformative impact on climate modeling ⁴⁵ ⁴⁶ and the multi-lab ExaEpi model speeding up epidemiological forecasts for CDC ³³ ³⁴ are concrete “receipts” of how dedicated compute in this category yields direct national benefits.

3.4 Category B – General Commercial and Consumer AI

Category B encompasses **all other AI applications** outside of the above privileged spheres. This is the vast domain of **commercial, academic, and consumer AI** that drives private sector products and everyday services. It includes everything from social media recommendation algorithms and e-commerce ranking systems, to enterprise AI tools (customer service chatbots, business analytics), to the current wave of **generative AI assistants (e.g. OpenAI's ChatGPT, Google's Bard)** that are available to the general public. It also spans academic research projects that aren't part of a national lab or mission program.

By definition, Category B is the “open” category – its compute resources are largely provided by commercial cloud providers or on-premises corporate data centers, and the location/operation of these resources is dictated by business considerations. Unlike A-1 and A-2, these AI workloads do *not* receive special prioritization or security restrictions beyond standard regulation. **Examples of Category B AI** would be:

- *Consumer-facing AI:* e.g. a virtual assistant on a smartphone, an AI music recommendation engine, or a vision model in a smartphone camera – typically developed by companies like Apple, Google, Meta, Amazon using their commercial AI infrastructure.

- *Enterprise AI services*: e.g. an insurance company's ML model for fraud detection or a bank's algorithmic trading AI. These often run on public cloud platforms (AWS, Azure, etc.) or corporate servers, and while important economically, they are not treated as national security assets.
- *Advertising and personalization AI*: a huge portion of commercial AI optimizes ads and content feeds (Facebook's newsfeed ranking, Google's ad placement AI). This category arguably consumes significant compute, but it falls under normal market-driven allocation rather than government prioritization.
- *Academic and open-source AI research*: universities training models on general research clouds, or open-source communities developing AI models (e.g. Stability AI's Stable Diffusion image generator). These efforts use Category B compute, unless they partner into NAIRR or other programs.

Regulation and oversight for Category B is generally light compared to A-1/A-2. Government's role here is setting broad policies (e.g. AI ethics guidelines, privacy laws, or forthcoming licensing requirements for very large models) that apply to industry. But the government does not, for the most part, control *where* or *how much* compute companies devote to their AI – that's driven by the market and user demand. In fact, the **largest AI compute clusters in the world are currently in the private sector** (e.g. OpenAI's supercomputer in Microsoft Azure, or Google's TPU v4 pods) built to train frontier commercial models. These would fall under Category B usage (unless/until they are tapped for A-2-like collaborations, as sometimes happens with companies offering compute for scientific research).

It's worth noting that **the boundaries between Category B and A-2 can sometimes blur**: for instance, a tech company could develop an AI model for drug discovery in a commercial context, which has strategic value (healthcare) but was not government-directed. Generally, though, what distinguishes Category B is *the absence of a direct government or national security driver in provisioning the compute*. Category B compute can be located globally wherever economical – indeed, big cloud providers place data centers based on cost and market reach, which might be **in regions not aligned with U.S. security priorities** ⁴⁷. (For example, an AI training center might be built in a country for cheap energy, whereas Category A-1 compute would almost certainly be kept on U.S. or allied soil for security).

In summary, Category B is the “everything else” bucket: **the open, commercial AI sector that thrives on market forces and global infrastructure**. It is the largest category by volume of deployments and users. However, it is *not* prioritized for special protections or government support the way A-1 and A-2 are, except indirectly through initiatives like workforce development or basic R&D funding. The **national strategy challenge** is ensuring that breakthroughs and resources from Category B (largely private) continue to feed into U.S. advantage without compromising security – and conversely, that prioritizing A-1 and A-2 doesn't stifle the innovation engine of commercial AI. Leading figures have stressed that *America's AI strength comes from its vibrant private sector*, and thus even national security policy must keep Category B healthy.

3.5 Segmentation of Compute for Each Category

A crucial question is whether the compute infrastructure for these categories can – or should – be **segmented physically or contractually** to reflect their different sensitivities. The framework implies a hierarchy of needs: A-1 at the top (most sensitive), then A-2, then general. In practice, we **do see efforts to segregate computing environments** for these classes:

- **Physical & Network Segregation (Secure Enclaves)**: Category A-1 workloads often run on **classified networks or air-gapped systems**, separate from the internet and commercial clouds. The

U.S. government has partnered with cloud providers to create *government-only cloud regions* to host sensitive AI. For example, Amazon Web Services operates **Secret and Top-Secret cloud regions** exclusively for U.S. defense and intelligence customers ⁴⁸ ⁴⁹. In June 2025, AWS announced a second “Secret” region, explicitly noting it will improve performance for **AI and other intensive workloads at the Secret level** ⁵⁰ ⁵¹. This new region (and existing GovCloud/Top-Secret regions) allows classified AI development to occur in a segregated cloud, with data stored closer to users for low latency ⁵². DoD and IC clients can deploy multi-region architectures that keep mission AI redundant and isolated from commercial traffic ⁵³. The U.S. Army CIO welcomed this, saying it *“enhance[s] support for critical warfighting IT systems... safeguarding combat-essential applications and improving force readiness.”* ⁵⁴. This is a prime example of **contractual and physical segmentation**: a commercial vendor provides cloud capacity, but in a dedicated enclave that meets government siting and security requirements (U.S. soil, U.S.-cleared personnel, etc.). Similarly, Microsoft’s Azure has **Government Secret and Top Secret clouds** used by the IC. These enclaves effectively create a **Category A-1 compute pool** separate from general commercial data centers.

Within DoD’s on-premises infrastructure, segmentation is longstanding: the **Defense Research & Engineering Network (DREN)** and classified networks like SIPRNet and JWICS host DoD supercomputers and AI clusters that serve only authorized users. The DoD HPCMP, for instance, has been pursuing “*Large-Scale Classified Computing*” as a strategic initiative ¹, including building HPC systems accredited for higher classification and even **deployable containerized supercomputers (like ARL’s SCOUT system)** for tactical AI needs ⁵⁵ ⁵⁶. Meanwhile, it also supports “*HPCMP Commercial Cloud and Open Research*” for unclassified work ⁵⁷. This mirrors an A-1 vs. A-2/B split in compute: tightly controlled capacity for classified/warfighting vs. leveraging commercial cloud for broader research. **Secure enclaves** (whether cloud-based or on-prem) are thus a key mechanism to segment A-1 compute.

- **Geographic and Siting Controls:** Location matters for segmentation. The government typically requires that A-1 compute (and often A-2) be located in the United States or in allied territories, with supply chain-secure hardware. For example, the Pentagon’s upcoming Joint Warfighting Cloud Capability (JWCC) contracts mandate cloud data centers on U.S. soil for classified data. In export control, the U.S. now restricts where advanced AI chips can be deployed internationally; *even U.S. firms must avoid placing cutting-edge GPUs in certain countries* (Tier 3 in the diffusion framework) ⁵⁸ ⁵⁹. This is effectively a **global segmentation of compute by location** for security reasons. Domestically, states like **Idaho, Tennessee, Texas** host large new AI data centers (for companies), but if those facilities were to be used for A-1 or A-2 workloads, additional government oversight or designation as critical infrastructure might apply.
- **Power Supply Prioritization:** The question of **power priority tiers** for data centers is emerging as AI’s energy appetite grows. While we did not find explicit policy naming “power tiers” for AI, one can analogize to how hospitals and emergency services get priority in grid restoration. It’s conceivable that **A-1 compute facilities (e.g. a NORAD AI data center or NSA cluster)** would be designated as *priority load* in power emergencies. There has been concern that commercial AI farms might strain energy goals, but some argue national security AI should override such constraints. Indeed, former Google CEO Eric Schmidt controversially suggested “*we should go all in on building AI data centers*” even if it complicates climate targets ⁶⁰. This implies a viewpoint that **certain AI uses are important enough to justify high energy allocation**, effectively a prioritization. However, formalizing “power priority tiers” would likely require critical infrastructure legislation – which, to date, data centers have only loosely been part of. (There is movement: e.g., DOE’s grid strategy

includes ensuring **defense-critical missions** have resilient power, which could extend to their compute sites.)

- **Licensing and Contractual Restrictions:** Another way to segment compute is via **licensing or service agreements** – only allowing certain models or workloads on particular infrastructure. For Category A-1, the government often uses contractual provisions: e.g. cloud contracts for classified work stipulate strict controls and allow government inspection. There's also the concept of **software licensing** to restrict model usage (for instance, a powerful model trained on a government system might be export-controlled or released only to certain users). While we did not find an existing *domestic* licensing regime that maps to A-1/A-2/B, the Biden Administration's recent Executive Order on AI (Oct 2023) does call for **developing standards and potentially requiring licenses for advanced AI model development** in certain critical areas. If implemented, that could function as a segmentation tool – e.g., require a license (and thus government awareness/control) to train models above a certain scale or in certain sectors. Congress has also discussed whether **foundation models used in national security** should have special accreditation. This is still in formative stages.
- **Priority Access and Pre-emption:** In times of crisis, one could imagine the government invoking the Defense Production Act or similar to redirect compute resources. For example, if a war or pandemic required sudden massive AI compute, **Category B resources might be temporarily commandeered** for A-1 or A-2 purposes. This is not routine segmentation, but it speaks to the hierarchy: A-1 tasks would outrank others if push came to shove.

In practice, **segmentation is imperfect**. *Commercial cloud providers still undergird a lot of A-2 and even some A-1 work*. For instance, DOE labs sometimes use commercial cloud for unclassified science workloads, and smaller DoD programs might train AI on commercial GPUs. Conversely, big tech companies may have more raw compute than national labs, which raises the question of whether the government should tap or even prioritize those resources for A-2 goals (public-private partnerships). One challenge noted by CSIS is that **hyperscalers (cloud companies) make decisions based on cost and market, not national security**, and they “gravitate toward locations where power is cheap [and] hurdles are minimal,” which “may not always be aligned with [U.S.] priorities”⁴⁷. This suggests a need for policy to **align and tether commercial compute to national aims** – essentially segmentation by incentives or mandates.

To illustrate segmentation with an example: **AWS's new Secret-West region** was explicitly justified as “strengthen[ing] U.S. AI leadership” by giving defense users dedicated capacity⁵¹. Simultaneously, tech companies like Anthropic and Palantir are introducing **special “Gov” AI models** for national security use (e.g., Anthropic's Claude Gov AI⁶¹). These moves create a *de facto* segmented ecosystem where **the most sensitive AI runs in special environments with privileged access and safeguards**, whereas the mass of AI runs in general environments.

Bottom line: It is **feasible and, in many areas, already happening** that A-1 compute is segmented via classified clouds and on-prem secure centers, and A-2 compute is concentrated in national supercomputing facilities or mission-specific platforms. Category B compute remains broadly distributed, but may be indirectly segmented by export controls or potential future licensing for frontier models. The effectiveness of segmentation will depend on robust implementation – and there are trade-offs (siloeing too much could reduce synergies with commercial innovation, for example). So far, the U.S. approach is to **carve out enclaves for what truly must be protected**, while encouraging open innovation elsewhere.

3.6 Policy Language Differentiating National Security AI vs. Commercial AI

U.S. officials and policy documents frequently draw a line between AI for **national security / defense** and AI for **general or commercial use**, underscoring why certain AI efforts need special focus. Some relevant quotes:

- **NSCAI Final Report (2021):** *“We will not be able to defend against AI-enabled threats without ubiquitous AI capabilities and new warfighting paradigms. We want the men and women in national security agencies to have access to the best technology in the world to defend themselves and us....”* ⁶² . – Schmidt & Work, NSCAI Chair/Vice Chair. This highlights that AI for national security must be cutting-edge and ubiquitous, distinctly prioritizing defense use above status quo commercial availability.
- **Jake Sullivan (Nat’l Security Advisor, 2024):** *“President Biden has signed a National Security Memorandum on Artificial Intelligence... This is our nation’s first-ever strategy for harnessing the power and managing the risks of AI to advance our national security.”* ⁶³ . – Sullivan’s remark at NDU stresses that AI in national security warrants its own strategy (separate from broader AI initiatives), implicitly separating it from commercial AI governance.
- **DoD Secretary Mark Esper (2020):** *“The real question is whether we let authoritarian governments dominate AI, and by extension the battlefield, or whether industry, the United States military and our partners can work together to lead the world in responsible AI...”* ⁶⁴ . – Esper, at an NSCAI public conference, contrasts *military AI leadership* with the risk of adversaries dominating, and notably includes industry as a partner, implying a delineation: the military’s needs vs. private sector’s role in meeting them.
- **America’s AI Action Plan (2025), Trump foreword:** *“...transformative technologies such as artificial intelligence... have the potential to reshape the global balance of power... As our global competitors race to exploit these technologies, it is a national security imperative for the United States to achieve and maintain unquestioned and unchallenged global technological dominance.”* ⁴ . – This explicit linking of AI to global power competition and the call for “dominance” reflects a mindset applied to defense and strategic domains, not how we talk about AI in, say, consumer apps.
- **Congressional Research Service (2020):** *“AI is a rapidly growing field of technology with potentially significant implications for national security. ... DoD has recognized that AI applications – from autonomous systems to decision support – could fundamentally change warfighting and intelligence.”* ⁶⁵ ⁶⁶ . – A typical CRS briefing note to Congress distinguishes AI’s national security implications from general advances, underscoring DoD’s focus on warfighting AI transformation.

The consistent theme: **when discussing national security, leaders emphasize AI’s role in military superiority, strategic competition, and the need for special measures** (strategies, investments, ethical guidelines) that go beyond the considerations of commercial AI deployment. Meanwhile, in documents about commercial AI (like OSTP’s AI Bill of Rights or FTC guidelines), the language centers on innovation, fairness, and civil aspects – a very different focus. This bifurcation in language supports treating the national security subset of AI (our Category A-1, and to an extent A-2) as something of a **separate class in policy**.

3.7 Arguments For and Against Compute Prioritization & Segmentation (Quote Bank)

To shed light on the debate around prioritizing and segmenting compute for national interest, we present a quote bank from leading figures. These “receipts” capture both **advocacy for** ensuring key AI uses get privileged access to compute, and **cautions against** over-segmentation or misallocation:

- **Eric Schmidt (NSCAI Chair, ex-Google CEO) – For prioritization:** *“We should go all in on building AI data centers... [because] the AI boom... comes at a price [in energy]... [Some think] climate goals are too lofty to reach anyway.”* (Paraphrased from an AI summit) ⁶⁰ ⁶⁷ . **Context:** Schmidt argued that investing heavily in AI infrastructure is so critical that it outweighs concerns like energy use. This reflects a hard-nosed stance that *compute for AI = strategic priority*, even if it conflicts with other policy goals (like carbon reduction). It underscores the view that **U.S. must not throttle compute growth**, especially not for A-1/A-2 needs, even if trade-offs are involved.
- **Lt. Gen. Jack Shanahan (ret., former JAIC Director) – For prioritization:** (As summarized by an interviewer) *The Pentagon’s AI lead stressed delivering AI to warfighters is a “strategic imperative” to preserve the nation’s military advantage, and requires accelerating adoption* ²² . **Context:** Shanahan often argued that DoD needed significantly more compute and faster acquisition to field AI – implicitly calling for priority funding and perhaps preferential allocation of resources to defense AI projects. This aligns with creating Category A-1 as a protected slice.
- **Jake Sullivan (NatSec Advisor) – For segmentation:** *“On the one hand, the U.S. needs to prevent diversion of advanced GPUs to China... On the other hand, the exponential growth in compute demand makes it impractical to limit AI infrastructure to U.S. soil... U.S. firms gravitate to locations with cheap power... which may not be reliably aligned with our priorities nor insulated from Beijing’s reach.”* ⁶⁸ ⁴⁷ . **Context:** Sullivan (via the NSM-Export framework analysis) acknowledges the **tension**: we want to **segregate top compute away from adversaries**, but our own companies might distribute compute globally for cost reasons. This justifies policy intervention – essentially an argument for segmentation via regulation (as seen in the three-tier export rule).
- **Army CIO Dr. Raj Iyer (paraphrased) – For segmentation:** *By establishing secure cloud regions (like AWS Secret-West), we ensure combat systems and data stay resilient and available, improving force lethality and readiness* ⁵⁴ . **Context:** The Army CIO’s statement on the new secret region highlights the benefits of having **dedicated infrastructure** for warfighting IT – a clear endorsement of segmentation to protect and prioritize those workloads (Category A-1) for reliability and security.
- **Peter Eckersley (EFF technologist) – Caution against overreliance on AI hype in military:** *“AI technologies have made exciting progress... but they remain brittle... There’s much to be done with ML, but plenty of reasons to keep it away from target selection, fire control... in the near future.”* ⁶⁹ ⁷⁰ . **Context:** In an EFF whitepaper, Eckersley advises militaries not to rush AI into critical kill-chain roles. This is a voice urging *restraint*, implying that perhaps pouring compute into those A-1 applications or prioritizing them could be dangerous if the tech isn’t mature. It’s not directly about compute allocation, but it’s an argument **against the assumption that more AI (and by extension more compute for A-1) is always better**.

- **General emphasis from Industry on Open Innovation:** Several tech leaders have argued that **restricting compute or data too tightly for national security could stifle innovation**. For example, an oft-cited dynamic is that *“the government needs the commercial sector’s AI advancements, so it should avoid segregating too much or it will fall behind.”* While we don’t have a pithy quote here, this sentiment is reflected in initiatives like the DIU and public-private partnerships – they argue **leveraging commercial AI (Category B) is as important as building exclusive defense AI**. This acts as a counterpoint to total segmentation: it’s more about **bridging** categories than isolating them.
- **DoD Ethical AI Principles (Defense Innovation Board) – Against indiscriminate use:** *“The Department will design and engineer AI capabilities to fulfill their intended functions while possessing the ability to detect and avoid unintended harm...”* (DIB Principle of Reliability). **Context:** While not directly about compute, this principle (adopted by DoD) implicitly says not all AI that *can* be built (with unlimited compute) *should* be built or deployed without constraint. It’s a caution that perhaps counters a pure “race for dominance” narrative and suggests careful prioritization (quality and safety over just quantity of compute).

Overall, **most leading voices favor giving national security and critical fields special focus and resources**, sometimes to the point of advocating massive investments and controls. Yet, there is also a chorus advising balance – warning of technical pitfalls, ethical ramifications, and the need to keep America’s broader AI ecosystem open and innovative. This underscores that **compute prioritization is not just a technical or strategic choice, but also a policy balancing act**.

3.8 Examples of Each Category in Action (with Sources)

The following table compiles **real-world examples for Categories A-1, A-2, and B**, including the use-case or system, the agency or organization involved, and a citation to corroborating information:

Category & Example	Agency / Organization	Description & Relevance	Source
A-1: Project Maven (Algorithmic Warfare AI)	NGA / DoD (Joint AI Center/ CDAO)	AI analyzes drone imagery (full-motion video) to automatically detect/track targets for intel & targeting support. Flagship warfighting AI tool transitioned to NGA in 2022 ⁷ ⁷¹ . Enables faster ISR analysis for combat ops.	⁷ ⁷²
A-1: FIRESTORM Targeting System	U.S. Army Futures Command / CCDC	AI-enabled C2 system that ingests multi-domain sensor data and recommends optimal fires (weapon-target pairings) in seconds, massively speeding up battlefield targeting ¹³ . Demonstrated in Project Convergence, integrated with Joint force networks ¹⁶ .	¹³ ¹⁶

Category & Example	Agency / Organization	Description & Relevance	Source
A-1: DARPA ACE (Air Combat Evolution) / “Mosaic Warfare”	DARPA / U.S. Air Force	Autonomous dogfighting AI that shifts pilot to a mission commander role while AI maneuvers aircraft ¹⁰ . Part of DARPA's Mosaic Warfare concept of distributed, AI-coordinated combat ¹⁸ . Demonstrates lethal autonomous systems for air combat.	¹⁰
A-1: NSA SIGINT & Cyber AI	NSA / U.S. Cyber Command	NSA employs AI/ML in signals intelligence processing and Cyber Command has a 5-year AI plan for cyberspace ops ⁹ ¹⁹ . AI helps filter vast signal data and aids cyber defense (anomaly detection, etc.) for national security networks.	⁹
A-2: Frontier Exascale – Climate Model	DOE Oak Ridge + NOAA/Sandia	Frontier (ORNL) runs the E3SM climate model at exascale, resolving global clouds in 3D. Achieved “ <i>years’ worth of simulations in days,</i> ” enabling high-fidelity long-range climate forecasts ²⁷ ²⁸ . Strategic for climate resilience and policy.	²⁷ ²⁸
A-2: ExaEpi Pandemic Simulation	DOE Labs (LBNL, etc.) + CDC	DOE’s multi-lab team built ExaEpi, an exascale AI-driven epidemiological model to simulate disease spread for CDC in near-real-time ³³ ³⁴ . Used in COVID-19 response and now expanding to other diseases, boosting U.S. public health preparedness.	³³ ³⁴
A-2: AI-Driven Materials Discovery	DOE (Multiple Nat’l Labs)	DOE “AI for Science” initiatives use AI to accelerate materials and drug discovery. E.g., AI surrogate models speed up simulations in materials science, leading to breakthroughs in batteries, fusion materials, etc. ³⁷ . Maintains U.S. innovation lead in critical tech sectors.	³⁷
A-2: NISAC Critical Infrastructure Sim	DHS CISA (Sandia/Los Alamos Nat’l Labs)	The National Infrastructure Simulation and Analysis Center develops advanced analytic tools (often using HPC/AI) to model risks to U.S. critical infrastructure ⁴⁰ . Helps anticipate impacts of disasters or attacks on interdependent systems (energy, telecom, etc.), guiding protective measures.	⁴⁰

Category & Example	Agency / Organization	Description & Relevance	Source
B: Generative AI Chatbots (e.g. ChatGPT)	OpenAI / Microsoft (Commercial)	Large-scale language model deployed as a consumer-facing chatbot. Trained on vast data via commercial cloud compute. Represents general-purpose AI available to millions, with no special government restrictions (aside from emerging safety guidelines). Category B uses drive private investment in AI compute.	N/A (Common knowledge)
B: Social Media Recommendation Algorithms	Meta, Google, ByteDance (Commercial)	AI models sort and recommend content/ads to users (e.g. Facebook News Feed, YouTube suggestions, TikTok's For You page). These algorithms are trained on commercial data center GPUs/TPUs, tuned for engagement and revenue. They exemplify Category B: high-volume AI compute directed by market incentives, not national security needs.	N/A (Market reports)

Table: Examples of AI Compute Use-Cases by Category. Sources indicate verification for the described use-cases (for A-1 and A-2, which are tied to government/mission contexts; Category B examples are widely documented in industry). Each example illustrates how the category's compute is deployed and managed (e.g., A-1 on secure networks, A-2 on national supercomputers, B on global commercial clouds).

3.9 Data Gaps and Further Research Needs

In compiling this research, certain areas lacked authoritative data or remain **open questions**, where policy is still evolving:

- **Formal Endorsement of 3-Category Framework:** We did not find any official U.S. strategy document that explicitly codifies a tripartite division exactly as A-1/A-2/B. The framework is an analytical construct supported by analogous distinctions in multiple sources, but **no single policy uses these labels or a direct three-tier scheme**. Future strategies (e.g. an updated National AI Strategy) might benefit from clarifying such categories.
- **Power Priority and Energy Policy for AI:** There was scant explicit evidence of “**power priority tiers**” for AI data centers in public documents. While critical facilities (hospitals, command centers) have priority in emergencies, *whether dedicated AI infrastructures like HPC centers are formally on such priority lists is unclear*. This is a gap: as AI compute gobbles power, planning for assured energy supply (perhaps via microgrids or backup generation for A-1 facilities) is needed. More data is needed on any ongoing initiatives (DOE or DoD) to secure power for critical AI infrastructure (one related item: DoD's experiments with small nuclear reactors for bases could support compute resilience).

- **Licensing of Domestic AI Compute/Models:** Outside of export controls, **mechanisms to license or restrict who can use top-tier compute domestically were not evident**, aside from procurement controls for government projects. The idea of licensing AI models (like how nuclear material is licensed) is nascent. The recent Exec Order asks for reports on possible measures, but **no concrete licensing regime exists yet** for, say, training a GPT-5-level model in a private data center. Monitoring the implementation of the EO and any Congressional action (e.g. forthcoming AI regulations) is needed to fill this gap.
- **NIST's Role in A-2 (Standards Development):** The narrative included "NIST standards development" as an A-2 example. We found NIST actively working on **AI standards and test frameworks** (like the NIST AI Risk Management Framework) and even piloting an "AI standards incubator" ⁴⁴, but not an explicit case of NIST using heavy compute for a standards *use-case*. Possibly this referred to NIST using simulation/AI to develop e.g. smart manufacturing standards. This was not well documented in connected sources. Further research could clarify NIST's compute-intensive AI projects (if any) or its needs for HPC in setting technology standards (perhaps the **NIST RFQ for HPC services** in 2023 suggests a growing need ⁷³).
- **Complete Inventory of A-1 Projects:** While we identified many known A-1 programs, **the full inventory of defense/IC AI efforts is classified or scattered**. GAO reported DoD had 600+ AI projects in 2021; by now over 1000 ⁷⁴. We cited prominent examples, but there are surely more (e.g. Navy's Project Overmatch for maritime AI networking, Air Force's ACTS for targeting, classified IC projects like NRO's Sentient analysis program). An authoritative list is not publicly available. A recommendation is a **CDAO-maintained public summary of major AI programs** (where releasable) to improve transparency and coordination – currently evidence was partial from news and speeches.
- **Effect of Segmentation on Innovation:** Little hard data is available on **whether segmenting compute harms or helps innovation**. It's a theoretical concern raised by experts. One could study, for instance, the utilization of GovCloud vs. commercial cloud by DoD – is DoD missing out on latest GPU generations if stuck in enclaves? Or conversely, does dedicating compute (like a supercomputer for climate) yield better results than relying on scattered commercial resources? This **impact assessment of segmentation** is a gap that could be explored via case studies or metrics (e.g. time to model training in segregated vs open environments).
- **International Analogues:** Our focus was U.S., but it's worth noting if allies or adversaries use similar categorization. China and EU strategies often talk about "*AI for defense*" vs "*for society*", etc. We didn't delve deeply due to scope, but comparative research could validate if this tripartite concept holds globally (and if, say, China informally prioritizes military AI compute in a similar fashion or not).
- **Emerging A-2 domains:** Some A-2 use-cases (like **NIST's role, or AI for infrastructure like smart cities**) were harder to find concrete examples for. There may be pilot projects (DOE using AI to simulate supply chains, etc.) not well-publicized. Further evidence-gathering is needed to flesh out **all "strategic advantage" AI domains** – e.g., *agricultural AI for food security, education AI for workforce development* could arguably be A-2 if viewed through a strategic lens, but we found no policy labeling them as such.
- **Verification of Compute Allocation Policies:** Finally, a data gap exists in verifying **how compute is actually allocated in practice**. We have policies and anecdotal examples, but, for instance, if a

shortage of AI chips occurred, does the U.S. have a mechanism to route them to A-1/A-2 first? Not clearly. Tracking investments (like the CHIPS Act funding for DoD labs or AI research infrastructure) could serve as a proxy – indicating prioritization. However, a more direct accounting (perhaps via the Chief AI Officers Council or OSTP) of compute distribution would enhance confidence in this framework's real implementation.

In conclusion, the tripartite framework is a useful lens that aligns with many strategic directives, but it is not yet formally consolidated in one policy. The evidence gathered **supports the validity of distinguishing AI compute by national importance**, and highlights both the moves made to secure Categories A-1 and A-2 and the areas requiring more development. As the U.S. implements its AI National Strategy, we anticipate clearer articulation of these categories and stronger measures to ensure that *essential warfighting and strategic AI* are adequately and efficiently provisioned – without unduly hampering the broader AI ecosystem that ultimately feeds innovation to all three categories.

Sources:

- GAO – DOD Warfighting AI Examples ⁸ ; DARPA ACE program description ¹⁰ ; Army FIRESTORM targeting AI ¹³ ¹⁶ ; NGA takeover of Project Maven ⁷ ; NSA use of AI for SIGINT ⁹ .
- DOE/ORNL – Frontier supercomputer enabling exascale climate modeling ²⁷ ²⁸ .
- LBNL/DOE – ExaEpi epidemiological modeling for CDC ³³ ³⁴ .
- DOE – “AI for Science” impacts on simulations (materials, etc.) ³⁷ .
- DHS CISA – NISAC infrastructure risk analysis tools ⁴⁰ .
- DoD HPCMP – Strategic initiatives for classified HPC vs. open research ¹ .
- CSIS – Discussion of hyperscaler vs. natsec priorities for data centers ⁴⁷ .
- Nextgov – AWS Secret Region launch for defense AI workloads ⁵⁰ ⁵¹ .
- NSCAI Report – Chair’s warning on AI competition and need for action ⁶² .
- White House – AI Action Plan (Trump quote) on AI as natsec imperative ⁴ .
- DoD – Sec. Esper remarks on military AI vs. adversaries ⁶⁴ .

¹ ⁵⁵ ⁵⁶ ⁵⁷ arl.devcom.army.mil

https://arl.devcom.army.mil/wp-content/uploads/sites/3/2020/09/ARL-HPCReview18_19-Section-508.pdf

² ⁴⁷ ⁵⁸ ⁵⁹ ⁶⁸ The AI Diffusion Framework: Securing U.S. AI Leadership While Preempting Strategic Drift
<https://www.csis.org/analysis/ai-diffusion-framework-securing-us-ai-leadership-while-preempting-strategic-drift>

³ ⁶² Chair and Vice Chair Letter - NSCAI Final Report
<https://reports.nscai.gov/final-report/chair-and-vice-chair-letter>

⁴ America’s AI Action Plan
<https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>

⁵ ⁶ Global Compute and National Security | CNAS
<https://www.cnas.org/publications/reports/global-compute-and-national-security>

⁷ ⁷¹ ⁷² Intelligence agency takes over Project Maven, the Pentagon’s signature AI scheme
<https://www.c4isrnet.com/intel-geoint/2022/04/27/intelligence-agency-takes-over-project-maven-the-pentagons-signature-ai-scheme/>

8 21 **How Artificial Intelligence Is Transforming National Security | U.S. GAO**

<https://www.gao.gov/blog/how-artificial-intelligence-transforming-national-security>

9 19 **NSA 'recently completed' AI strategic study, director says - Defense One**

<https://www.defenseone.com/defense-systems/2023/09/nsa-recently-completed-ai-strategic-study-director-says/390032/>

10 18 **ACE: Air Combat Evolution | DARPA**

<https://www.darpa.mil/research/programs/air-combat-evolution>

11 12 **DARPA Tiles Together a Vision of Mosaic Warfare**

<https://www.darpa.mil/news/mosaic-warfare>

13 14 15 16 17 **Soldiers and Commanders to Assess FIRESTORM AI Technology | AFCEA International**

<https://www.afcea.org/signal-media/technet-augusta-22-coverage/soldiers-and-commanders-assess-firestorm-ai-technology>

20 **National Security Agency is starting an artificial intelligence security ...**

<https://apnews.com/article/nsa-artificial-intelligence-security-deepfakes-f9b19dd64890884cc2b0700ddf66e666>

22 **Delivering AI to Warfighters Is Strategic Imperative - DoD CIO**

<https://dodcio.defense.gov/In-the-News/News-Display/Article/2347200/delivering-ai-to-warfighters-is-strategic-imperative/>

23 **DOD CDAO Defines AI Goals For Warfighter Support**

<https://govciomedia.com/dod-cdao-defines-ai-goals-for-warfighter-support/>

24 74 **'Kind of Like Electricity'—Where DOD Stands With AI - GovCon Wire**

<https://www.govconwire.com/articles/where-dod-stands-with-ai>

25 26 **Organization**

<https://www.ai.mil/About/Organization/>

27 28 29 30 31 32 45 46 **Pulling clouds into focus: Frontier simulations bring long-range climate forecasts within reach**

<https://www.ornl.gov/news/pulling-clouds-focus-frontier-simulations-bring-long-range-climate-forecasts-within-reach>

33 34 35 36 **Epidemiological Modeling in the Exascale Era - Computing Sciences – Computing Sciences**

<https://cs.lbl.gov/news-and-events/news/2023/epidemiological-modeling-in-the-exascale-era/>

37 38 **Artificial Intelligence for Science | Department of Energy**

<https://www.energy.gov/topics/artificial-intelligence-science>

39 **Scaling Materials Discovery with Self-Driving Labs | IFP**

<https://ifp.org/scaling-materials-discovery-with-self-driving-labs/>

40 41 42 **National Infrastructure Simulation and Analysis Center (NISAC) | CISA**

<https://www.cisa.gov/resources-tools/groups/nisac>

43 **ORNL and NOAA launch new supercomputer for climate science ...**

<https://sciencesprings.wordpress.com/2023/04/15/from-the-does-oak-ridge-national-laboratory-and-the-national-oceanic-and-atmospheric-administration-ornl-and-noaa-launch-new-supercomputer-for-climate-science-research/>

44 **NIST Launches Pilot Project to Propel AI Innovation, Accelerate ...**

<https://www.ansi.org/standards-news/all-news/3-27-25-nist-launches-pilot-project-to-propel-ai-innovation>

48 49 50 51 52 53 54 61 **AWS launches second secret cloud region for defense, intel customers - Nextgov/FCW**

<https://www.nextgov.com/acquisition/2025/06/aws-launches-second-secret-cloud-region-defense-intel-customers/405951/>

60 67 Former Google CEO Eric Schmidt says we should go all in on building AI data centers because 'we are never going to meet our climate goals anyway' : r/Futurology

https://www.reddit.com/r/Futurology/comments/1g1yyia/former_google_ceo_eric_schmidt_says_we_should_go/

63 Remarks by APNSA Jake Sullivan on AI and National Security | The White House

<https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2024/10/24/remarks-by-apnsa-jake-sullivan-on-ai-and-national-security/>

64 Remarks by Secretary Esper at National Security Commission on Artificial Intelligence Public Conference > U.S. Department of War > Transcript

<https://www.war.gov/News/Transcripts/transcript/article/2011960/remarks-by-secretary-esper-at-national-security-commission-on-artificial-intell/>

65 [PDF] Artificial Intelligence and National Security - Congress.gov

https://www.congress.gov/crs_external_products/R/PDF/R45178/R45178.8.pdf

66 [PDF] 2022 National Defense Strategy, Nuclear Posture Review ... - DoD

<https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf>

69 70 The Cautious Path to Strategic Advantage: How Militaries Should Plan for AI | Electronic Frontier Foundation

<https://www.eff.org/wp/cautious-path-strategic-advantage-how-militaries-should-plan-ai>

73 NIST RFQ: High Performance Computing (HPC) Services

<https://orangeslices.ai/nist-rfq-high-performance-computing-hpc-services/>