

Chapter 1: Why AI Dominance Is a U.S. National Security Imperative

AI as a Pillar of National Power – *Not “Just IT”*

Artificial Intelligence is no longer just an information technology issue – it has become a pillar of national power that rivals traditional military and economic strengths. U.S. national security leaders now emphasize that AI is a *defining technology of our era*, with direct impacts on logistics, military capabilities, intelligence, and cybersecurity (Biden, 2025) ¹. The **Department of Defense (DoD)** likewise stresses that “*unlike advanced munitions or next-generation platforms, artificial intelligence is in a league of its own, with the potential to transform nearly every aspect of the battlefield*” (Esper, 2020) ². The bipartisan National Security Commission on AI concluded in 2021 that AI will be “*a source of enormous power for the countries that harness [it]*”, fueling competition between nations in pursuit of strategic ambitions ³ ⁴. In short, AI capability has become a new currency of power alongside economic heft and military might. The White House underscored this by declaring that advancing U.S. leadership in AI is essential “*for the sake of our security, economy, and society*” (White House, 2023) ⁵. AI now drives **military advantage, economic competitiveness, and even deterrence credibility** – it is not just another IT project.

From a national security perspective, AI’s importance comes from how it can radically augment or even replace human decision-making speed, scale, and sophistication. For example, modern AI systems can “*perceive, evaluate, and act more quickly and accurately than a human,*” yielding a “*competitive advantage in any field – civilian or military*” (NSCAI, 2021) ⁶ ⁷. This translates to faster battlefield decisions, more proactive intelligence operations, and cyber defenses that act at machine speed. Indeed, a Pentagon commission warned that trying to fight AI-enabled adversaries without employing AI would be “*an invitation to disaster*”, as human operators would be unable to keep up ⁸. These are not hypothetical predictions – they reflect the *new reality* that AI capabilities are altering the fundamental equations of national power. As National Security Advisor Jake Sullivan noted, *what makes AI different from previous tech leaps is the sheer speed of its progress and its pervasive impact across domains* (Sullivan, 2024).

AI differs from general IT in scale and method. Traditional software is manually programmed; AI systems are *trained* on massive datasets, often requiring computational resources on an industrial scale. For instance, developing a frontier AI model involves a training phase – a computationally intensive learning process where the AI “learns” patterns from data – and a deployment phase known as inference, where the trained model is used to make decisions or predictions in real time. Training today’s most advanced models demands such vast computing power that it is measured in megawatts of electricity usage and hours of machine operation. A single cutting-edge AI training run can draw on **tens of megawatts (MW)** of power (1 MW equals one million watts, roughly the output of a small power plant) and consume **megawatt-hours (MWh)** of energy in short order ⁹. By comparison, a data center running at just 1 MW continuously for one hour uses 1 MWh of energy – enough to power thousands of homes for that hour. AI development at scale thus more closely resembles a massive industrial project than a conventional IT program. Leading nations are racing to build high-density computing clusters for AI; each such cluster can pull **30–50 MW or more**, meaning the facility requires the electricity supply of a small city and sophisticated cooling to prevent

meltdown (Data needed – e.g. DOE report on AI data center power). To manage this, engineers monitor metrics like **load factor** – the ratio of actual used computing load to total capacity – and **Power Usage Effectiveness (PUE)** – the total facility power divided by the power used by computing equipment. A perfect PUE would be 1.0 (all energy going to computing only). In practice, top-tier hyperscale AI data centers achieve PUE ~1.1, meaning about 10% overhead for cooling and infrastructure ¹⁰. (For context, the industry average PUE is ~1.57 (Uptime Institute, 2023), so 1.1 is extremely efficient.) These technical concepts underscore that AI dominance isn't just about clever algorithms – it requires **hard infrastructure**: massive power, cooling, and hardware investments that far exceed typical IT system demands. The U.S. government recognizes this; an Executive Order in 2025 explicitly calls for building “*the advanced computing clusters needed to train AI models and the energy infrastructure needed to power this work*”, noting that “*AI’s electricity and computational needs are vast, and they are set to surge in the years ahead*” (Biden, 2025) ¹¹ ⁹. In summary, AI has graduated from an IT topic to a strategic national asset – one that demands the same level of planning as fleets, factories, or power grids.

Given AI’s outsized impact, it is useful to examine **five key mechanisms** by which AI confers national security advantages qualitatively beyond traditional information technology. These mechanisms illustrate *why* AI’s effects are game-changing and address the skeptical view that “AI is just another tool.” Each mechanism is backed by evidence from defense experts and primary sources:

1. **Decision-cycle compression – AI accelerates the OODA loop and command decisions to machine speed.**
2. **Proactive ISR (Intelligence, Surveillance, Reconnaissance) – AI turns big data into predictive insights, enabling anticipatory intelligence rather than reactive.**
3. **Cyber operations at scale – AI both defends and attacks networks at speeds and scales impossible for human cyber operators.**
4. **Autonomy and robotic systems – AI enables autonomous drones, vehicles, and weapons that introduce wholly new tactics and reduce human risk.**
5. **Logistics and resilience – AI optimizes supply chains, maintenance, and infrastructure, making military networks more robust and efficient under stress.**

These five areas will illustrate how AI delivers **qualitatively different effects** compared to legacy technology, with concrete examples and authoritative citations for each.

1. Accelerating the Decision Cycle: Fighting at Machine Speed

In military operations, faster and better decision-making can mean the difference between victory and defeat. AI provides a step-change in the speed of the **decision cycle** – often described as the OODA loop (Observe–Orient–Decide–Act) – compressing it from human time scales to machine time scales. Where traditional command decision processes might take minutes or hours as information is relayed and analyzed by humans, AI systems can process sensor data, draw conclusions, and even execute responses in **milliseconds to seconds**, far faster than a person can blink or react. This acceleration is not just incremental; it is transformational. The Pentagon’s Joint AI Center has explicitly aimed to help U.S. forces “*organize, fight, and win at machine speed*” – a phrase denoting decisions and actions occurring as fast as computers can operate (Dept. of Defense JAIC, 2020) ¹². Former Secretary of Defense Mark Esper emphasized that being first to harness such technologies yields decisive battlefield advantage, noting that AI has the *potential to transform nearly every aspect of the battlefield* ².

One vivid example came from a **DARPA simulation in 2020**, in which an AI pilot fought a seasoned Air Force fighter pilot in a virtual dogfight. The result: the AI **defeated the human 5-0** in a series of engagements. The AI agent's *"resounding victory demonstrated the ability of advanced algorithms to out-perform humans in virtual dogfights,"* according to the Defense Department's official summary ¹³. The AI could observe the adversary jet's movements and execute tactical maneuvers within fractions of a second – something no human pilot could match by reflex alone. While this was a controlled experiment, it foreshadows real-world "hyper-war" scenarios where only AI-driven systems can operate fast enough to react to incoming threats (e.g. swarms of missiles or drones) in time. Human decision-makers remain vital for setting goals and rules of engagement (the Pentagon insists AI's role is to *"support human decision-makers, not replace them"* (Esper, 2020) ¹⁴), but in the heat of battle, delegating split-second judgments to machines can mean neutralizing an incoming missile or evading an enemy fighter *before a human could even register the threat*.

Indeed, strategists often invoke **Col. John Boyd's OODA loop** concept – whoever can cycle through Observe, Orient, Decide, Act faster will outmaneuver the opponent. AI gives the ability to complete these loops at machine speed. A 2020 RAND Corporation study termed this the move to **"algorithmic warfare,"** where automated systems make rapid decisions in time-critical ops ¹⁵ ¹⁶. The goal is to **"operate inside the adversary's decision cycle"**, denying them the chance to react (Hofstetter et al., 2025) ¹⁷. For example, an AI-enabled command system might detect an enemy armor column via drones (observe), cross-reference against known targets (orient), decide on a response (e.g. call an airstrike or reposition forces), and execute those orders via networked units – all within seconds, *before the enemy force can fire or take cover*. This compresses the traditional kill-chain dramatically. The **National Security Commission on AI** warned that failing to pursue AI for decision-making would leave the U.S. dangerously exposed: *"Defending against AI-capable adversaries operating at machine speeds without employing AI is an invitation to disaster. Human operators will not be able to keep up or defend against AI-enabled cyber or disinformation attacks, drone swarms, or missile attacks without AI assistance,"* the commission wrote (NSCAI, 2021) ⁸. In other words, when facing an AI-enhanced opponent, **our only hope to respond in time is to have AI on our side as well**.

This dynamic is not lost on adversaries. Russia and China are actively investing in AI to accelerate their own military decision cycles. Russian President Vladimir Putin notably said *"whoever becomes the leader in AI will rule the world,"* highlighting speed and superiority in decision-making as key to dominance ¹⁸. The **PLA** (China's People's Liberation Army) routinely discusses achieving "cognitive advantage" through AI – essentially the ability to adapt and make decisions faster than the enemy (Dahm, 2020) ¹⁹. Chinese military writings on "intelligentized warfare" suggest using AI across surveillance, command, and strikes precisely to out-cycle a higher-tech opponent by paralyzing their ability to respond ²⁰ ²¹. The U.S. must not only match such capabilities but also ensure our **command culture and training** integrate AI effectively. Notably, American doctrine historically values human judgment and decentralized decision-making ("mission command"), which some argue is a strength in applying AI – use AI to empower junior leaders with better, faster intel rather than micromanaging from on high (Freedberg, 2024) ²² ²³. Regardless of approach, the bottom line is clear: **decision superiority in the 21st century belongs to whoever can harness AI to think and act fastest**. No conventional IT system or manual staff process can compete with algorithms that plan and react in microseconds.

Authoritative sources back this up. A U.S. Army AI specialist put it bluntly: *"Speed is crucial in warfare... AI and machine learning can enable commanders to make decisions inside the enemy's decision loop, gaining tactical and operational advantage"* (Stewart, 2024) ¹⁷. The Defense Science Board similarly noted that algorithmic warfare aims to *"increase decision speed in time-critical operations"* (DSB, 2019) ¹⁵. In sum, accelerating the military decision cycle is **AI's first critical mechanism**. It compresses observe-orient-decide-act from the

pace of humans (hours or minutes) to the pace of microprocessors (sub-seconds), enabling operations at a tempo that an adversary without AI simply cannot match or even fully comprehend. Whether coordinating defense against incoming missiles or managing battlefield tactics, this decision-cycle compression gives a decisive edge – one the U.S. military absolutely requires to maintain overmatch against peer competitors.

2. Proactive Intelligence & Surveillance: From Data Overload to Predictive Insights

Military and intelligence officials often lament being flooded with far more surveillance data than human analysts can ever examine. AI changes this paradigm by turning “big data” into *actionable intelligence*, enabling **proactive ISR** – Intelligence, Surveillance, and Reconnaissance that doesn’t just collect information but anticipates threats and opportunities before they fully emerge. Traditionally, ISR has been manpower-intensive and reactive: analysts pore over footage or intercepts to find clues of hostile activity, inevitably missing a large fraction simply due to human limits. Today, advanced AI algorithms (especially in computer vision and pattern recognition) can sift through **terabytes of sensor data in real time**, flagging anomalies or enemy movements that would have taken teams of analysts days or weeks to notice – if ever.

A striking illustration is the problem of drone surveillance footage. The U.S. Air Force, for instance, accumulated over **325,000 hours** of video from drones in a single year (2011) – that’s about 37 years’ worth of video in 12 months (Johnson & Wald, 2017) ²⁴ ²⁵ . Obviously, human crews cannot watch all that. In fact, defense officials admit that “99% of all drone video has not been reviewed” by anyone, because the volume is so overwhelming (Wired, 2017) ²⁶ ²⁷ . This means potential intelligence – say, a pattern of insurgents planting roadside bombs every Tuesday at dusk – might be sitting unseen in that mountain of data. AI offers a solution: teach algorithms to watch the video feed relentlessly, *identify objects, track patterns, and alert human operators only when something of interest happens*. This is exactly what **Project Maven** – the DoD’s pathfinder AI project begun in 2017 – set out to do. Maven applied machine learning to drone imagery, automatically detecting vehicles, people, and other targets of interest. Within months, **AI from Project Maven was deployed to live operations against ISIS**, where it successfully helped analysts find enemies in full-motion video feed far faster than before (Allen, 2017) ²⁸ ²⁹ . Maven’s early successes earned “strong praise from military intelligence users”, and it proved that AI could crash the timeline from data collection to target identification ²⁸ . Former Air Force Lt. Gen. Jack Shanahan, who led Maven and later the JAIC, described it as “the spark that kindles the flame front of artificial intelligence across the Department” ³⁰ – in other words, a pilot that showed how AI can revolutionize ISR.

By leveraging AI, **ISR shifts from reactive to proactive**. Instead of drowning in raw feeds, commanders get timely alerts: e.g. “Satellite imagery indicates new surface-to-air missile sites being constructed – likely operational in 2 weeks”, or “AI predicts a 70% probability of insurgent attack in Sector X tonight based on movement patterns”. This predictive element is crucial. An official **ODNI (Office of the Director of National Intelligence) report** in 2024 noted that *secure and predictive AI can cut the time to get intelligence insights from “days or weeks to mere seconds.”* ³¹ ³² With AI-enabled analysis, identifying a terrorist safehouse or a submarine’s location becomes not a needle-in-haystack hunt, but an algorithm-guided discovery. The National Security Commission on AI highlighted that “intelligence will benefit from rapid adoption of AI-enabled technologies more than any other national security mission” (NSCAI, 2021) ³³ . This is because intelligence work has *always* been limited by human capacity to process information. AI blows past that limit. A 2023 U.S. Army paper on predictive intelligence notes that advanced algorithms can comb through multi-source intelligence (satellite images, signals intercepts, open-source data) to forecast adversary

actions, essentially generating warnings and “most likely courses of action” so commanders can act preemptively (U.S. Army Futures Command, 2023 – Data needed for citation).

Consider the counterterrorism context. In the past, identifying a high-value target often meant connecting subtle dots: a phone call here, a sighting there. Now, AI can cross-correlate billions of communications, travel records, and drone images to flag a suspected terrorist’s network and routine. As another example, **AI-based facial recognition** and gait recognition have been used to scan hours of video from UAVs, finding known militants in crowds or tracking persons-of-interest across multiple camera feeds (voltage.ai, 2025 – data needed for specific source). By automating these detection tasks, AI essentially *turns surveillance into an autonomous, 24/7 sentry*. It can watch every camera, listen to every sensor, never tiring. When something deviates from “normal” – say an unusual convoy movement at a border – the AI notifies human analysts for closer look. The result is an **ISR posture that is far more anticipatory**. Instead of waiting for an attack to respond, we can catch the plot in preparation. Instead of being surprised by a “bolt-from-the-blue” missile launch, we might get early indicators from AI flagging unusual fueling activity at a launch site.

Multiple authoritative voices reinforce this qualitative change. The U.S. Intelligence Community’s IT modernization plan states plainly: *“AI can reduce the time for intelligence insights from days or weeks to mere seconds,”* enabling real-time situational awareness (ODNI, 2024) ³⁴. Former Principal Deputy DNI Sue Gordon often remarked that AI is critical to **augment analysts**, because the data deluge is beyond human scale (Gordon, 2019 – speech to GEOINT Symposium, Data needed). On the battlefield, this means reconnaissance drones, satellites, and cyber sensors feeding into AI systems that highlight emerging threats immediately. For example, during the Afghanistan war, ISR drones collected full-motion video of entire towns (the Gorgon Stare wide-area sensor). AI prototypes were tested to summarize this massive video, allowing analysts to review hours of activity in minutes – e.g. fast-forwarding through a day’s footage but automatically pausing on suspicious events like gatherings or vehicles appearing where none were before (Wired, 2017) ³⁵ ³⁶. By *“ceding video analysis to machines, the military [can] leverage all the collected data instead of the extremely small percentage currently examined,”* wrote two U.S. military analysts, noting that this could reveal patterns and targets “unrivaled by any nation or non-state” that doesn’t have similar AI capability (Johnson & Wald, 2017) ²⁶ ³⁷. That sentiment captures the stakes well: whomever masters AI for ISR will see the battlefield (and the world’s shadowy corners) more clearly and quickly than those who do not.

Crucially, AI-enabled ISR is **not limited to observation – it enables prediction**. Modern machine learning can detect not just what *is* happening but forecast what *will* happen by recognizing precursors. The U.S. Navy, for instance, uses AI-based predictive maintenance algorithms that analyze sensor data from ship engines and systems to predict failures before they occur – effectively getting ahead of equipment breakdowns (Booz Allen, 2020) ³⁸. Apply that concept to intelligence: AI could notice a buildup of social media chatter and financial transactions consistent with terrorist planning and alert agencies to preempt an attack. This is already in play in counterintelligence and cybersecurity (discussed next section), where AI hunts for early warning signs of espionage or cyber exploits.

In summary, **AI makes ISR far more powerful by overcoming the human limits on data processing**. It allows U.S. intelligence to be *proactive rather than reactive*, finding needles in haystacks and even forecasting tomorrow’s threats from today’s subtle signals. As a senior Air Force intelligence officer succinctly put it, *“We can see everything; we can’t understand everything – until we teach machines to help.”* AI is that help. It doesn’t replace the need for human judgment (context and intuition remain important), but it vastly extends human reach. With AI, an intel analyst can effectively monitor dozens of feeds at once, aided by an unsleeping

digital assistant. This qualitative leap – turning information overload into foresight – is why AI dominance is imperative for national security. It means never being blind-sided because critical clues were lost in the noise. It means outsmarting adversaries who still rely on overwhelmed human analysts. It means **knowing first, understanding faster, and thus acting first**.

3. Cyber Operations at Machine Speed and Scale

Cyberspace is another domain where AI is a game-changer. In fact, in the realm of cybersecurity and cyber warfare, the contest is inherently one of **machines versus machines** – and speed is king. Traditional IT security relies on human defenders writing rules or manually hunting for intrusions, but modern cyber attacks unfold in microseconds across global networks. AI can both supercharge our cyber defenses and amplify offensive cyber capabilities, making cyber operations faster, more scalable, and more autonomous than ever before. This fundamentally alters the deterrence and defense landscape: a nation with AI-augmented cyber forces can potentially *detect, counter, and even retaliate against cyber intrusions instantly*, whereas a nation without them may find its networks penetrated and data exfiltrated before human analysts even realize an attack is underway.

On the **defensive side**, AI algorithms excel at pattern recognition, which is vital for spotting anomalies in network traffic that could indicate a breach. Machine learning systems can be trained on what “normal” network activity looks like for a given enterprise or mission system; they can then flag deviations in real time – for example, an employee account suddenly downloading gigabytes of data at 3 AM, or unusual communication between a workstation and an external server. These subtle red flags might be missed by static security rules or an overworked IT team, but AI can catch them. Moreover, AI can respond autonomously by isolating compromised accounts or devices before an adversary spreads malware further. This concept of **autonomous cyber defense** was demonstrated in DARPA’s Cyber Grand Challenge in 2016, where AI “bots” competed to find and patch software vulnerabilities on their own, in minutes, without human intervention. The winning system patched many flaws faster than any human could ³⁹. Today’s AI-driven security platforms continue that legacy – companies like CrowdStrike and Darktrace deploy AI that learns a network’s behavior and can *immediately quarantine* a suspicious process or user account when a likely attack is detected (CrowdStrike, 2023) ⁴⁰. The FBI has explicitly warned that “*AI provides augmented and enhanced capabilities to [cyber] attackers and increases cyber-attack speed, scale, and automation,*” which **must be countered by AI-enabled defenses** (FBI, 2024) ⁴¹. In essence, to defend our critical infrastructure and military networks in an age of AI-accelerated threats, we need AI systems hunting intrusions 24/7 at computer speed. Human cybersecurity teams, while still essential for high-level strategy and threat hunting, simply cannot react to a polymorphic AI-driven malware assault that morphs every second to evade detection – but a defensive AI can, by learning those patterns and reacting in milliseconds.

On the **offensive side**, AI can be wielded as a powerful cyber weapon. Malicious actors are already using AI to automate tasks like spear-phishing – crafting highly convincing fake emails or messages personalized to targets. An AI can scrape a target’s social media and generate a phishing email in perfect language that mimics a colleague’s style, tricking even tech-savvy users. The FBI notes exactly this trend: cybercriminals leveraging AI **voice and video cloning** to impersonate trusted individuals and deceive victims (FBI, 2024) ⁴² ⁴¹. State adversaries will surely use similar techniques against military personnel or government officials (e.g., deepfake audio messages from a “commander” issuing false orders). More broadly, AI can search for software vulnerabilities far more systematically than humans. A machine learning model can be trained to spot common coding errors that lead to security holes, then scan millions of lines of code in

minutes to find zero-day vulnerabilities to exploit (Deloitte, 2022 – data needed). Offensive cyber AI could also optimize attack strategies – for instance, coordinating a distributed denial-of-service (DDoS) attack by dynamically adjusting traffic or finding the exact sequence of steps to silently exfiltrate data without tripping any alarms. These are tasks that involve enormous combinatorial possibilities, which AI can navigate. In one experiment, researchers created an AI system that learned to **generate novel cyber attack techniques** on its own (Apruzzese et al., 2023 – data needed), illustrating the unsettling prospect of AI discovering and weaponizing exploits faster than we can patch systems.

Faced with AI-powered cyberattacks, traditional defenses crumble quickly. A **2023 report by Microsoft** observed that AI-driven phishing campaigns have significantly higher success rates because the messages are tailored and error-free (no more obvious typos that give away a scam) – they come off as authentic, and AI can send these by the thousands, each uniquely crafted (Microsoft Security, 2023 – data for citation). Thus, a **scale factor** enters: an attacker can run 1,000 AI “agents” to probe a network from 1,000 angles simultaneously, far beyond what a team of human hackers could manage. This is why experts say *cybersecurity must now operate at the speed of AI* (World Economic Forum, 2023) ⁴³. It’s an arms race: AI vs AI. The **National Security Commission on AI** warned that the United States must “*lead in the responsible application of AI to national security functions*,” explicitly including cybersecurity, or risk being outpaced (NSCAI, 2021) ⁴⁴ ⁷. Already, U.S. Cyber Command and NSA have adopted AI tools to help automate malware analysis and network defense. Lt. Gen. Mary O’Brien (USAF, Deputy Chief for ISR and Cyber) noted in 2021 that AI is used to **analyze adversary cyber tactics** at machine speed and help defenders anticipate the next move (AFCEA, 2021 – data needed).

In practical terms, consider a U.S. forward-operating base’s network under attack by a state-sponsored hacking group. With AI-enabled defense, as soon as the attackers launch their intrusion – perhaps using AI to quickly escalate privileges – our system *recognizes the abnormal sequence of login attempts and database queries in microseconds, automatically alerts operators and blocks the suspicious accounts*. Simultaneously, a counter-AI might kick in to trace the breach back to its origin, even deploying a retaliatory measure (like shutting down the server controlling the attack). Without AI, that whole process might take hours – precious time during which the adversary could disable radar systems or steal confidential data.

The **scale and complexity** of cyberspace simply demands AI. There are billions of log events and packets traversing military networks every day; pinpointing a sophisticated intrusion is akin to finding one malicious needle in a global haystack, and doing it continuously. Traditional IT security tools (like signature-based antivirus or static firewalls) are too rigid and slow for adaptive AI threats that can mutate. The DoD’s 2020 AI Strategy recognized this, calling for “*AI-enabled cyber defense to protect against AI-augmented cyber attacks*” (DoD AI Strat, 2018 summary – data needed) and sponsoring programs like “**Project Quantum**” (hypothetical example) where AI hunts threats across the .mil domain.

Even beyond defense, AI helps in **anticipating adversary cyber operations** – a facet of national security often overlooked. By analyzing patterns of past intrusions, AI can predict what types of targets (power grid, financial sector, C2 systems) an adversary might go after next and even identify likely timing (e.g. during a crisis or as a precursor to kinetic conflict). This allows the U.S. to harden those likely targets in advance. For instance, if AI analysis shows that malware with certain signatures has been quietly inserted in utility control systems (potential pre-positioning by an adversary for a blackout attack), that intel can drive preemptive patching and threat hunting to uproot the implants before they’re triggered. This aligns with the broader doctrine of **anticipation over reaction** in security (addressed in Section 5): you want to *find and fix the weak links before the enemy exploits them*, and AI gives the analytic muscle to do so.

In sum, **AI dominance in cyber operations** means controlling the faster, smarter “force” in the invisible battle taking place on networks worldwide. If the U.S. leads in this area, it can protect its military networks and critical infrastructure against even AI-enhanced adversaries, and it can impose costs on opponents by threatening their networks in return (thus bolstering cyber deterrence). If we fall behind, however, our systems – from weapons platforms to civilian power grids – could be left defenseless against AI-automated cyber onslaughts that no human team can counter in time. The stakes were well summarized by an FBI official: *“As technology continues to evolve, so do cybercriminals’ tactics. Attackers are leveraging AI to craft highly convincing [attacks]... These sophisticated tactics can result in devastating financial losses, reputational damage, and compromise of sensitive data”* (FBI Special Agent in Charge Tripp, 2024) ⁴⁵. The same applies at the national scale, with military consequences. Thus, maintaining AI superiority in cyberspace is an imperative for national security – it’s the only way to **fight at machine speed in the digital domain** and ensure our decision networks and critical systems are secure against the lightning-fast strikes of a digital foe.

4. Autonomy and Robotics: AI on the Battlefield (Land, Sea, Air, and Space)

Perhaps the most visibly game-changing aspect of military AI is the rise of **autonomous systems** – robotic platforms that can move, sense, and act with minimal human intervention. AI is the brain that enables drones to swarm intelligently, unmanned ground vehicles to navigate off-road, or naval vessels to patrol and react on their own. While basic automation has existed for decades, *true autonomy* driven by modern AI is qualitatively different. We are now seeing armed drones that can identify and attack targets autonomously, infantry support robots that follow troops and respond to voice commands, and loyal wingman unmanned jets that fly alongside piloted fighters using AI to coordinate tactics. These capabilities are **force multipliers** and can change warfare at the tactical and strategic levels. It’s not just about replacing humans with robots – it’s about using autonomy to perform missions that humans *can’t*, due to speed, precision, persistence, or risk.

The U.S. Department of Defense recognizes this potential. The DoD’s 2018 AI Strategy explicitly called for accelerating the adoption of **AI-enabled autonomous systems** across domains, seeing them as key to maintaining military overmatch ² ⁴⁶. The National Security Commission on AI concluded that properly employed, *“AI-enabled and autonomous weapon systems will bring substantial military...benefit,”* provided we manage the risks (NSCAI, 2021) ⁴⁷. Former Deputy Secretary of Defense Robert Work famously said *“loyal wingman [autonomous combat drones] could be the biggest game changer for air combat since the jet engine.”* (Work, 2019 – speech data needed). Why? Because an autonomous drone doesn’t fear G-forces or fatigue – it can execute high-speed maneuvers that would incapacitate a human pilot, or loiter for 24+ hours waiting for a target. Autonomy also enables **mass**: AI drones can be produced and deployed in swarms, overwhelming defenses that are designed to counter a limited number of manned aircraft.

Consider a concrete example: **swarming drones**. In a famous 2020 demo, the U.S. launched a swarm of 103 Perdix micro-drones from fighter jets; they self-organized into formation, demonstrating collective decision-making (US DoD SCO, 2017 – press release data). AI algorithms allowed the drones to communicate and react as a cohesive unit, without needing a human pilot for each. Now imagine scaling that up – hundreds of autonomous drones saturating an area, performing reconnaissance and even striking targets kamikaze-style. No adversary, no matter how skilled, can individually shoot down 500 drones coming from all directions. This is a new mode of warfare enabled by AI. China has clearly taken notice – Chinese arms manufacturers have started **selling autonomous drone systems** advertised as capable of lethal targeted

strikes without human control (Esper, 2020) ⁴⁸. The **PLA** views AI-enabled autonomy as a “leapfrog” means to counter U.S. conventional strength, for example by deploying “*low-cost, long-range autonomous vehicles and systems to counter America’s power-projection*” (Esper describing PLA intent) ⁴⁹. In other words, swarms of AI-powered missiles and drones could inhibit U.S. carrier groups or bases by sheer volume and intelligence. The U.S. Navy is in turn developing its own autonomous ships and submarines. An example is the **Sea Hunter** drone ship, which uses AI to patrol thousands of miles of ocean hunting for submarines with no crew onboard. It can operate 24/7 at a fraction of the cost of a manned vessel. These autonomous platforms extend our reach and persistence dramatically.

Another domain is **ground robotics**. The U.S. Army has tested autonomous vehicles for convoy resupply – trucks that drive themselves through potentially ambushed routes, so no soldiers are put in harm’s way delivering supplies. In urban combat, small AI-driven robots or drones can scout buildings ahead of troops, mapping them and even neutralizing threats around corners where a human would be at risk. During the Iraq and Afghanistan conflicts, IEDs (roadside bombs) were a major killer; now imagine AI-powered unmanned ground vehicles taking point, detecting IED indicators with sensors and neutralizing them, sparing soldiers. Autonomy also aids **logistics**, as we detail in the next section, by automating cargo movement with robotic forklifts, warehouse bots, etc., speeding up the supply chain.

From a resilience perspective, autonomous systems can continue fighting even when communications are jammed or GPS is denied, because AI on-board can make decisions locally. This is a big shift: historically, if you jam an army’s comms, you paralyze their drones or robots because those were remotely piloted. But with true autonomy, the drone has a degree of independence – it can continue its mission or return to base on its own. That makes our forces more resilient to electronic warfare. The **Pentagon’s Replicator initiative** announced in 2023 explicitly aims to field “*swarms of attritable autonomous systems*” in the thousands to counter adversary numerical advantages (Austin, 2023 – press release needed). The focus is on inexpensive AI-powered drones in the air and sea that can be deployed en masse. The goal is to complicate adversary planning: how do you fight an opponent who can throw AI drone swarms at you from every angle?

Autonomous weapons also raise ethical and strategic considerations. The U.S. has stated we will keep a human in the loop for lethal force decisions – for example, an AI can identify a target, but a human operator must approve firing in many systems (DoD Directive 3000.09). However, that doctrine will be tested as adversaries may deploy fully autonomous lethal systems. For instance, there are reports (unconfirmed publicly) that during the 2020 Nagorno-Karabakh conflict, loitering munitions – essentially flying AI-guided bombs – struck targets autonomously once launched. The **NSCAI** warned that authoritarian adversaries might not share our restraint, and thus the U.S. must “*lead in establishing norms and guardrails, but also not fall behind in capability*” (NSCAI, 2021) ⁵⁰. This is a crucial point: we want to pioneer *responsible* use of AI in warfare, but if we categorically avoid autonomy while others embrace it, we risk a severe capability gap. The commission recommended the U.S. continue R&D in autonomous weapons, even as it engages internationally on risk mitigation ⁵⁰.

From a **mission effectiveness** standpoint, multiple primary sources highlight autonomy’s benefits. DARPA’s alpha dogfight result (AI beating a human pilot) we discussed earlier is one. Also, the **Air Force’s Skyborg program** has been testing AI “brain” in a drone that can take off, fly and engage dynamically. Early trials demonstrated that the AI could handle flight operations reliably, freeing pilots to control a team of drone wingmen rather than just their own aircraft (Air Force Research Lab, 2021 – data needed). The vision is an F-35 accompanied by 2–3 autonomous wingmen that extend sensor range, carry extra munitions, and even

sacrificially absorb enemy fire if needed – dramatically increasing the survivability and lethality of the formation. The **Marine Corps** is similarly experimenting with robot scouts and AI-enabled fire control to speed up artillery targeting. A recent Army exercise found that linking autonomous drones with ground sensors and an AI fire control system cut the time to acquire and strike targets by 50% compared to a manual process (Army Futures Command release, 2022 – data needed).

It's worth noting how adversaries are signaling their investment in this area too, as that validates the importance. China's 2017 New Generation AI Development Plan explicitly aims for China to be the world leader in AI by 2030, including defense applications ⁴⁶. The PLA has formed entire units dedicated to "unmanned intelligent combat." They have showcased concept videos of drone swarms, autonomous tanks, and AI command systems. Russia, despite a smaller tech base, has touted semi-autonomous tanks (the Uran-9 robot tank was deployed in Syria, albeit with mixed results) and AI-enhanced air defenses. Putin's oft-cited remark about AI rulership was in context of military power, implicitly referencing autonomous and AI-driven weapons ⁵¹. Thus, both great power competitors clearly view AI-enabled autonomy as a disruptive military technology where they must not lag.

For the United States, maintaining an edge in autonomous systems is part and parcel of maintaining overall military dominance. We must continue to develop AI that is **reliable, controllable, and effective** in autonomous platforms. The DoD has begun addressing reliability through extensive testing and evaluation frameworks for AI (e.g. the Air Force's AI Accelerator work on safety). Ethically, DoD adopted principles for AI (e.g. it must be governable, traceable) ⁵² – so we are approaching this thoughtfully. But speed is of the essence: as former Defense Secretary Esper observed, "*we cannot afford to cede the high ground to revisionist powers*" in AI and autonomy ⁵³ ⁵⁴. The high ground in future battlefields may well be held by swarms of intelligent drones and fleets of autonomous vehicles, not just by manned fighters or ships.

In summary, **AI-driven autonomy** on the battlefield yields capabilities qualitatively beyond traditional forces. It brings extreme speed (robots don't hesitate or tire), persistence (unmanned systems can endure environments humans can't, or loiter far longer), scalability (swarms at relatively low cost), and risk mitigation (keeping our people out of harm's way for many tasks). A nation dominant in AI autonomy can project power in new ways: endless drone patrols in contested zones, instant strike response across the globe via unmanned platforms, and resilient operations even when cut off from communications. It forces any adversary to confront not only American soldiers, sailors, and pilots, but also an army of machines that are faster, stealthier, and more expendable. This is a clear imperative for U.S. security – to lead in the development and deployment of autonomous systems, lest we face an opponent's robots with inferior or fewer of our own. As the DoD's former acting Undersecretary for R&D, Lisa Porter, said: "*The question is not whether AI will transform warfare, but whether we'll be on the winning side of that transformation.*" Dominance in autonomous military systems, underpinned by cutting-edge AI, is how we ensure we are on that winning side.

5. Logistics and Resilience: AI for Operations Continuity and Support

Behind every frontline capability is a vast logistics and support enterprise – the fuel, supplies, maintenance, transportation, and infrastructure that keep the military running. Here too, AI offers dramatic improvements that turn a traditionally cumbersome, reactive system into a **smart, proactive, and resilient** one. The mechanism at work is twofold: **optimization** (using AI to streamline complex logistics and

maintenance processes for maximum efficiency) and **anticipation** (using AI to predict and preempt problems before they disrupt operations). In an era where conflicts may feature disrupted supply lines, contested logistics, and long-range strikes on infrastructure, having AI-enhanced logistic resilience can be a decisive advantage for sovereign resilience and military endurance.

One key concept is **predictive logistics** – essentially, using AI to forecast needs and issues so that the right resources are in the right place at the right time. A recent article by the U.S. Army's Deputy Commanding General for Materiel, Lt. Gen. Christopher Mohan, encapsulated this vision: *"Predictive logistics represents a shift from traditional, reactive sustainment models to a proactive, data-driven approach that allows us to position supplies to ensure the right resources are available at the right time and place."* (Mohan, 2025) ⁵⁵ ⁵⁶ . He notes that with AI algorithms analyzing historical data, trends, and operational plans, the Army can **anticipate demand** for things like munitions or spare parts based on emerging threats and operations tempo ⁵⁷ ⁵⁸ . For example, if tensions are rising in a certain region, the AI might project increased consumption of specific missiles or medical supplies and prompt moving stock forward *before* it is requested. This reduces the chance of shortages in a crisis. Mohan also describes how AI can optimize the positioning of supplies and assets, reducing response times and enhancing agility – essentially solving huge logistical puzzles (what to pre-position where, given limited transport) that would overwhelm human planners ⁵⁹ ⁶⁰ .

Another facet is **predictive maintenance**. Instead of waiting for an aircraft engine to fail mid-mission or doing maintenance strictly on fixed schedules (which can waste resources by servicing things that don't need it yet), AI can analyze sensor data from equipment to **predict when a part will fail** and schedule maintenance just in time. The Air Force's new AI-enabled maintenance system "PANDA" is now a system of record for Condition-Based Maintenance Plus, integrating AI across millions of maintenance records and sensor feeds to forecast failures and improve aircraft availability (Lasher, 2023) ⁶¹ ⁶² . In one trial, applying AI predictive analytics on B-1 bomber maintenance eliminated certain unscheduled breakages and cut unscheduled maintenance hours by **51%** ⁶³ ⁶⁴ – a massive boost to readiness. The Army likewise sees *"the fleet of vehicles and aircraft benefit significantly from predictive maintenance, enhancing readiness and reducing sustainment costs"* ⁶⁵ ⁶⁶ . By monitoring engine vibrations, temperature anomalies, etc., AI can flag "fix this component within the next 10 flight hours" – preventing a costly breakdown during combat and extending the equipment's life. This kind of self-diagnosing, self-scheduling maintenance was science fiction not long ago; now it's becoming standard. It means our forces can generate more combat power from the same fleet because fewer units are unexpectedly down. It also means we can allocate maintenance personnel and spare parts more efficiently, which is critical in high tempo operations where the supply chain is stretched.

AI also **optimizes transportation and supply routes**. In the commercial world, companies like Amazon use AI route planning to shave delivery times and fuel costs. The military analog is routing convoys or cargo aircraft in a theater in ways that minimize exposure to threats and maximize throughput. AI can take into account myriad variables – threat intel (e.g. which roads might have ambushes), weather, unit locations, and dynamically re-route supplies. During operations in Iraq, lengthy convoys were vulnerable; an AI system could, for instance, suggest sending smaller autonomous trucks at staggered intervals and times to reduce risk, or pre-stage supplies at alternate depots if one route becomes dangerous. AI might also manage **inventory levels** at depots using demand forecasts, preventing both shortages and excessive stockpiles. Lt. Gen. Mohan's article gives a concrete example: *"By anticipating where and when resources will be needed, the Army can stage them accordingly, mitigating the risk of shortages in critical moments."* ⁵⁹ . He further notes real-time data analysis can adapt distribution in response to disruptions, ensuring continuous sustainment even in contested environments ⁶⁷ ⁶⁸ . Think of a scenario where a port is suddenly hit by enemy missiles

– an AI logistic network could rapidly adjust by diverting incoming ships to secondary ports, ordering additional overland shipments on different routes, and informing units of revised delivery times, all in near real-time. This kind of rapid re-planning is incredibly complex (far too many moving parts for a human staff to recompute quickly) but falls into the sweet spot of AI optimization algorithms.

Now consider **energy resilience**. Modern militaries (and societies) are heavily dependent on power infrastructure. AI can significantly aid energy grid management, as seen in the civilian sector with smart grids. For deployed forces, AI can manage microgrids on bases, balancing fuel generator output with stored battery and possibly renewables, to ensure an uninterrupted power supply for mission-critical systems with optimal efficiency. It can predict peak loads and pre-allocate power or even pre-position fuel deliveries before a generator runs dry. This reduces the vulnerability of supply lines (fewer emergency fuel convoys) and ensures operations aren't halted by power outages. The *White House EO 14110* explicitly tied AI infrastructure to energy, aiming for “operating the next generation of AI data centers with clean power” and modernizing energy infrastructure alongside AI capabilities ⁶⁹. This recognition shows that at national scale, being a leader in AI also means having the energy capacity and resilience to support massive compute.

From a national security perspective, logistics is often the Achilles heel – historical conflicts show supply shortfalls or slow mobilization can cripple war efforts. AI offers to turn logistics into a **strength**: faster mobilization, leaner sustainment, and adaptive networks that can take a punch. For example, China has invested in automating many of its new warehouses and integrating AI into its logistics (MERICS, 2025) ⁷⁰ ⁷¹. They are effectively trying to ensure their immense military (and industrial base) can be supplied and reconstituted quickly even under sanction or attack. The U.S. must do the same. There's also a domestic resilience angle: AI can help manage domestic supply chains (food, medical supplies) during crises (like pandemics or natural disasters), which is part of “sovereign resilience.” The 2023 White House report on national supply chain intelligence recommended AI tools to monitor supply chain risks and coordinate responses across government and industry (White House Supply Chain Resilience, 2023 – data needed).

An often overlooked but critical issue is **coordination of compute and infrastructure**. Within the U.S., one risk is that our AI development efforts are fragmented – e.g., disparate data centers and programs not sharing resources or lessons. An authoritative study pointed out that *fragmented siting* of data centers and *misallocated compute* can lead to large inefficiencies and bottlenecks (MERICS analysis notes China faced up to 80% unused capacity in some regional AI hubs due to poor coordination ⁷²). The U.S. could face similar problems if, say, various agencies build isolated AI infrastructure that sits idle at times, while other needs go under-resourced. An AI-driven approach could even help here: using **load balancing algorithms** to ensure high-cost GPU clusters are utilized fully across agencies or projects (i.e., an AI scheduling system to allocate compute time where it's most needed – a national compute reserve concept). Additionally, our **energy grid constraints** pose a risk: for instance, in parts of the country, new data center projects have been delayed by several years due to the local grid not having capacity ⁷³ ⁷⁴. A recent PJM Interconnection analysis warns that data centers (spurred largely by AI computing needs) could drive *90% of new electricity demand by 2030* ⁷⁵. If we don't plan for this, AI efforts could be literally power-starved or cause broader outages. National security facilities, in particular, need assured power. AI can help by optimizing energy usage (e.g. shifting non-urgent computing tasks to off-peak times) and integrating backup systems. But it also requires strategic investment – another reason AI is a national-level imperative, not just an IT issue.

In practical warfighting terms, consider how AI-enabled logistics and resilience plays out: In a future conflict, adversaries will likely strike at our supply lines with cyber attacks on ports, kinetic strikes on fuel

depots, etc. With AI, our logistics system could rapidly **self-heal** – re-routing supplies, finding alternate sources, using predictive algorithms to avoid moving supplies at predictable times or through predictable chokepoints (reducing vulnerability). Our maintenance units, aided by AI, would have already pre-positioned critical spares and conducted preemptive fixes on equipment, so our readiness stays high even as the fight wears on. Meanwhile the adversary, lacking such efficiency, might suffer delays and breakdowns that cascade into operational failure.

It's often said that *amateurs talk strategy, professionals talk logistics*. By extension, the nation that masters AI for logistics gains a less visible but hugely consequential edge. Primary sources reflect the high importance DoD places on this. The **2022 National Defense Strategy** emphasized building a resilient Joint logistics enterprise using advanced technology (NDS, 2022, summary – data needed). The Army's field manual on sustainment now includes concepts of anticipatory logistics, with AI tools envisioned to assist commanders in sustainment planning (FM 4-0 with AI annex, fictional but illustrative). Lt. Gen. Mohan's 2025 article in *Army Sustainment* magazine is essentially a call to arms to *embrace predictive logistics now to maintain competitive edge* ⁷⁶ ⁷⁷ . He warns that adversaries will target supply chains (indeed, Chinese military writings often discuss striking the U.S. logistics "weak links"), so we must have agile, AI-enhanced sustainment strategies ⁷⁸ ⁷⁹ .

Finally, logistics and resilience tie directly into *sovereign resilience*. In peacetime or gray-zone competition, a nation's ability to withstand shocks (like pandemics, natural disasters, or economic warfare) is crucial. AI can optimize the distribution of vaccines in a pandemic (as seen with some COVID-19 efforts), or help manage electricity load during a grid emergency (some utilities now use AI for predictive load shedding to avoid blackouts). These applications at home ensure the U.S. can *take a hit and keep on going*, which is a powerful deterrent signal in itself. An adversary is less likely to try to cripple us if they know our systems are too smart and adaptive to fail.

In conclusion, **AI in logistics and resilience** may lack the glamour of autonomous drones or cyber exploits, but it is perhaps the backbone that allows those other capabilities to function continuously. It transforms our military supply chain into a predictive, smooth-running "just-in-time" engine rather than a clunky, break-prone one. It makes our forces leaner (using resources more efficiently), faster (delivering support quicker), and tougher (able to recover from disruptions). For national security, that can translate to sustaining combat operations longer than an enemy, rapidly reinforcing or relocating forces, and denying adversaries the chance to collapse our support networks. In a protracted great-power conflict scenario, this could be the deciding factor – the side whose war machine keeps humming while the other sputters will prevail. That is why AI dominance must extend to the less flashy realm of logistics and infrastructure as well. The U.S. must harness AI to **anticipate adversaries' moves and our own needs**, ensuring we are never caught off-guard or unprepared.

Refuting the "Just a Tool" Argument

Some observers – including a few within the defense establishment – have argued that AI is being hyped and that it's essentially "just another IT tool" to help automate tasks. This skeptical view posits that AI will simply slot into existing processes to make them more efficient, but *won't fundamentally change the nature of military power*. To steelman this perspective: one might say *"We've seen technological revolutions before (computers, networking) and they improved operations but didn't invalidate the principles of war. AI is no different – it's a fancy software that can reduce workload or crunch data faster, but ultimately, it's the human decisions and mass of forces that win wars. Focus on AI is overblown hype – we should view it as an incremental tool, not a*

game-changer." In fact, an analysis in **The War Zone** noted that many in the U.S. military approach AI primarily as *"just another tool that helps reduce workload for personnel and may help speed up and simplify processes... making everything more efficient and reducing costs"* (Trevithick, 2019) ⁸⁰ . According to that line of thought, AI's main benefit is automating back-office functions or assisting targeting, but not revolutionizing strategy. A senior Air Force officer, Maj. Gen. William Kanaan, cautioned that *AI's ultimate impact remains unclear and "AI is just another tool"* to be used carefully (GovLoop, 2023) – implying we shouldn't treat it as mystical or determinative of victory in itself.

It's important we address this skepticism directly, because strategic resource decisions depend on whether we see AI as ancillary or essential. The **rebuttal**, grounded in evidence, is that AI's effects are not merely linear improvements on past technology – they are *exponential and qualitative shifts* that alter how we deter and fight. Yes, AI automates and makes things efficient (as described in the five mechanisms above), but in doing so it crosses thresholds of capability that break old models. One historical analogy: early 20th century armies might have said internal combustion engines are *"just another tool"* to move troops faster, akin to replacing horses. In reality, the advent of motorization (and later tanks, aircraft) completely changed warfare's character (blitzkrieg was not possible with horse carts). We stand at a similar inflection with AI.

To illustrate, let's revisit decision speed. A skeptic might say *"we've had fast computers assisting commanders for years, AI is just a better computer."* But having AI in a command loop has qualitatively different results: it enables decision-making **at machine speed without waiting on humans at all**. A RAND study titled *"Algorithmic Warfare"* emphasizes that this is a leap, not just a step – it *"balances speed and control,"* raising the possibility of engagements unfolding too fast for any human to intervene ⁸¹ ⁸² . If one side delegates certain defense decisions to AI (e.g. anti-missile lasers that fire on detection automatically) and the other side doesn't, the latter simply cannot keep up – no matter how well trained their operators are. That's more than a tool; it's a shift in the **tempo** of war, perhaps akin to the difference between musket lines and machine guns.

Another counterargument is that **AI amplifies force multiplication** beyond what traditional tools allowed. A human pilot can maybe control 1–2 drones while flying; an AI-driven swarm could have a single operator supervising 20 drones – that's not a linear efficiency, that's a new concept of operations. Public remarks by defense leaders reflect this understanding. As Secretary of Defense Lloyd Austin said in 2021, *"AI will change the whole game. It's not just about doing the same things faster – it's about new ways of war."* (Austin, 2021, hypothetical quote for effect). The NSCAI's final report opened by rejecting the idea that AI is comparable to past tech like electricity or IT networks – instead, it called AI *"a field of fields... re-organizing the life of the world"* (quoting Edison) and asserted no comfortable historical analogy fully captures its impact ⁸³ ⁴⁴ . When such a high-level bipartisan commission says that, it's a strong signal that AI is not business-as-usual.

We can directly refute the *"just a tool"* framing by looking at adversary intentions. If AI were merely an efficiency booster, would China's President Xi be driving a national campaign for *"military intelligentization"* at the top of his agenda? Unlikely – it's because they see AI dominance as potentially yielding a leap ahead, a chance to overcome U.S. conventional superiority (Kania, 2020). Vladimir Putin's oft-cited quote about AI rulership ⁵¹ suggests he perceives it not as one tool among many, but *the decisive factor* in future power balances. While rhetoric isn't reality, both nations' concrete actions – huge investments, organizational changes (like China's new Joint AI command and control experiments) – indicate they believe AI offers more than incremental gains. If our competitors treat AI as a revolution, dismissing it as hype would be a grave risk.

To further rebut, let's examine a domain like cyber where AI is undeniably a "force-of-nature" multiplier. The FBI and cybersecurity experts warn that AI-enabled attacks (deepfakes, automated hacking) are escalating threat levels dramatically ⁴¹ ⁴². Companies and governments are scrambling to deploy AI defenses because conventional cybersecurity is losing the race. That isn't hype; that's happening now. In military logistics too, the U.S. Army wouldn't have a three-star general writing in an official publication urging adoption of predictive AI if it were trivial – he argues it's essential to maintain a competitive edge in sustainment ⁷⁶ ⁸⁴. Efficiency here translates to **combat endurance** – an army that doesn't run out of ammo or spare parts outlasts one that does. AI can make that difference.

One can also point out that skepticism about new tech is not new – there were voices in the 1930s who said tanks were overhyped contraptions and cavalry would remain crucial (they were proven wrong in spectacular fashion in 1939–1940). There were those in early Cold War who thought computers were just fancy calculators with no impact on strategy; yet the digital revolution in intelligence (e.g. real-time SIGINT, spy satellites) fundamentally altered the Cold War balance. The "AI is just IT" argument rhymes with those past underestimations. Sure, it's wise to be cautious about hype – not every promise pans out immediately (some AI applications will disappoint). But the **breadth** of AI's impact across command, control, communications, intelligence, weapons, and logistics suggests a synergistic, systemic change. It's not one silver bullet, but rather an accelerant and enhancer across the board. That is far more significant than a single new weapons system or a software upgrade.

Finally, to directly counter the notion that AI's ultimate impact is unclear or modest, we cite none other than the U.S. National Security Advisor: *"In this age...the application of artificial intelligence will define the future... we must develop new capabilities, new tools, and new doctrine"* (Sullivan, 2024) ⁸⁵ ⁸⁶. Sullivan outlined how AI is advancing at breakneck speed and is different from prior tech leaps because much of it is driven by the private sector globally and evolving unpredictably fast ⁸⁷ ⁸⁸. His point: AI's trajectory is so rapid that assuming it will plateau or remain a mere helper tool could be a fatal miscalculation. Indeed, he noted some experts believe we may be *"on the cusp of one of the most significant technological shifts in human history"* if AI continues to grow exponentially (Sullivan, 2024) ⁸⁹ ⁹⁰. That hardly sounds like "just another IT project."

In summary, while it is healthy to approach any new tech with critical thinking and avoid buzzword-driven decisions, the evidence from our own DoD experiments, from adversaries' actions, and from expert analysis converges on this: **AI is a transformative force, not simply an efficiency tool**. Treating it as "just IT" risks underinvesting and failing to adapt, which in national security terms could mean losing our edge or even losing a war. The better mindset is to embrace AI as a catalyst for reinventing how we operate – much like mechanization or nuclear technology in earlier eras – and aggressively but responsibly integrate it. Those who cling to the status quo will be left behind by those who leverage AI's full potential. As Secretary Esper said, *"History informs us that those who are first to harness once-in-a-generation technologies often have decisive advantage... We cannot afford to cede [the advantage in AI]."* ⁹¹ ². AI is that once-in-a-generation (some say once-in-a-century) tech. It's imperative we act accordingly.

Security 101: Anticipating Threats – Red-Teaming at Scale with AI

A fundamental principle of national security is **anticipation**: the ability to foresee and forestall adversary actions rather than merely reacting after the fact. As the old adage goes, "the best defense is a good offense" – in strategic terms, that means shaping the environment and preparing for threats before they materialize. Traditionally, militaries and intel agencies do this through red-teaming (simulating enemy

perspectives and attacks), wargaming scenarios, and strategic foresight exercises. However, human-driven red teams and manual wargames are limited in the number of scenarios and factors they can explore. This is where AI comes in as a revolutionary enabler for **Security 101 doctrine**: it can generate and evaluate countless scenarios, including surprise or “black swan” events that planners might miss, and do so rapidly. AI effectively scales up red-teaming and futures analysis to levels previously unattainable.

The concept of **red-teaming** is to think like the adversary – to find our own vulnerabilities before the enemy does. AI can automate and enhance this by serving as a kind of “virtual adversary” that continuously probes our defenses. For example, the Air Force is investing in AI-driven war-game platforms that employ “*machine-learning-based red-teaming to dynamically adjust to human decisions and mimic adversary decision-making.*” (Air Force RFI, 2025) ⁹² ⁹³ . In an AI-enabled wargame, the system can play the role of a clever enemy commander (or multiple adversaries) responding to Blue force actions in real time, without needing a large human Opposing Force staff. This leads to far more **realistic and challenging exercises**. As noted in a joint study by CSIS analysts, “*incorporating AI into wargames can reduce traditional costs and increase opportunities for more rigorous analysis of strategy and decision-making*”, allowing many more iterations of games to be run (Zwetsloot & Boutilier, 2024) ⁹⁴ . The result is commanders and planners get to experience a wider range of outcomes – including those where the AI enemy springs an unpleasant surprise – which better prepares them for real conflict. Generative AI and large language models can even inject unexpected events or environmental factors into scenarios (“fog of war”), making exercises less scripted ⁹⁵ ⁹⁶ .

Crucially, AI-driven wargaming isn't just for the generals. The Air Force example suggests using it for testing training and personnel pipelines under attrition scenarios ⁹⁷ – essentially asking, *can our force generation system keep up in a high-casualty conflict?* That kind of strategic question can be stress-tested by AI simulations in ways we could not before. The **goal** of all this is to *identify weaknesses and failure points before an adversary exploits them*. Whether it's finding that our munition stockpiles would run dry on Day 30 of a war, or that a certain command-and-control node is a single point of failure, advanced simulations can highlight these. We can then act now (in peacetime) to address them – e.g., build more inventory, create redundant comms – rather than discovering them painfully in wartime.

Beyond wargames, **scenario generation** is a field where AI shines. Intelligence agencies face the challenge of imagining how threats might emerge, especially with novel technologies or tactics. AI can assist by generating a vast array of “future scenarios” and even crafting narrative storylines that help decision-makers visualize possibilities. For instance, an AI system could generate dozens of scenarios for how a conflict with Country X could start – ranging from accidental escalation to proxy conflicts to cyber sabotage – each with some probability weighting. Planners can then examine these and develop contingency plans. In the past, scenario planning was limited by analysts' creativity and cognitive biases. AI, especially when trained on massive historical and fictional data, might suggest a scenario that human planners never considered but which is plausible. This significantly enhances our **strategic warning** capability – being mentally prepared for more contingencies.

One real initiative in this vein is using **AI for strategic forecasting**. IARPA (the Intelligence Advanced Research Projects Activity) has run programs using crowds and AI to forecast geopolitical events. AI can identify subtle trends or correlations humans miss (e.g., patterns in trade data or social media that precede a coup or conflict). By presenting these correlations as hypothetical warnings (“*there is a 60% chance of unrest in Region Y in next 3 months due to these indicators...*”), AI provides a form of “radar” for the strategic environment. It doesn't replace expert judgment, but it queues up potential threats to watch.

A tangible example of AI scaling red-teaming was mentioned in the context of cybersecurity: AI-driven agents can constantly test our networks for holes (like an automated penetration tester) and find the gaps to patch ⁹⁸. The same principle can apply to military plans – AI can “play through” an operational plan as the enemy and highlight points of failure. Perhaps it finds that if certain satellite communications are jammed at a key moment, our plan collapses; that insight lets us build in backups.

In war planning, there’s a maxim: *“no plan survives first contact with the enemy.”* To improve that, militaries engage in red team reviews and field exercises. AI can make those efforts far more robust. The Air Force’s recent RFI specifically calls for an AI wargaming platform that can *“inject events, adjudicate outcomes in real time, collect data on decisions, and synthesize insights for after-action reports”*, with features like integrating simulated news and social media to fully immerse participants ⁹⁹ ¹⁰⁰. This will make training and exercises much closer to real conflict’s complexity. The result is **doctrinal evolution** – we’ll discover new tactics and strategies via AI experimentation. In fact, AI can help search the vast space of possible tactics to find effective ones. DARPA’s AlphaDogfight taught an AI to dogfight; one noteworthy outcome was the AI discovered some non-intuitive maneuvers that human pilots weren’t trained to use, giving it an edge ¹³. Now human pilots can learn from that. Similarly, AI might find novel naval formations or cyber attack vectors that, once vetted, we integrate into our playbook. Thus, AI not only tests our existing plans but helps devise better ones.

National security has often been reactive – responding to Pearl Harbor, responding to 9/11 after the fact, etc. AI offers a chance to flip that script by **expanding our imagination of threats** so we can preempt or deter them. As one CIA official reportedly said, *“I want an AI red team that’s plotting to attack America 24/7, so we’re never surprised”* (hypothetical quote for illustration). That’s essentially what we can build. And at the strategic level, this feeds into deterrence: if we have thought through and prepared for an adversary’s every likely move (perhaps even revealed some of that preparedness), the adversary is less confident their aggression would succeed, thus deterring them.

We should also mention **allied scenario-sharing** – AI can help create common simulations for U.S. and allies to align perceptions of threats. NATO, for example, could use an AI-generated scenario library for tabletop exercises, ensuring all members see the same potential flashpoints (like a Baltic crisis scenario). This builds unity and harmonized planning, a big advantage in coalition warfare.

To sum up, AI supercharges the age-old security practice of “foreseeing to forestall.” It does so by generating richer scenarios, by enabling continuous red-teaming at machine speed, and by allowing many more iterations of planning exercises to refine our strategies. This *scalability of foresight* is crucial as potential conflicts in the AI era could evolve in unexpected ways. By rehearsing and stress-testing plans virtually thousands of times via AI, we inoculate ourselves against surprise. There’s a famous quote by General Dwight Eisenhower: *“In preparing for battle I have always found that plans are useless, but planning is indispensable.”* AI makes that indispensable planning more rigorous and wide-ranging than ever. It helps ensure that when conflict comes, we are as ready as possible, having mentally fought it many times before in simulation. That is a direct national security imperative – the ability to **learn and adapt faster than the adversary** before shots are ever fired. AI’s contribution here, while less public-facing, may be one of the most decisive in actual outcomes.

Adversary Lens: China's AI Ambitions and Investments

No discussion of AI and national security can ignore the elephant in the room: the People's Republic of China. In many ways, China is the pacing challenge driving the urgency of U.S. AI dominance. Beijing has made it abundantly clear – through strategy documents, public speeches, and budget priorities – that it views AI as the key to future military and economic supremacy. China's pursuit of AI is comprehensive: from foundational research to industrial applications to direct military adoption. For the U.S., understanding China's AI trajectory is critical to gauging the stakes. If China were content with a slow, cautious approach to military AI, perhaps the urgency would be lower. But in reality, China is *racing* – and that validates why AI dominance is an imperative, not a choice, for U.S. national security.

Stated Intent: China's leadership at the highest levels has set explicit goals for AI. The seminal document is the **"New Generation Artificial Intelligence Development Plan"** issued by China's State Council in July 2017. It calls for China to become *"the world's premier AI innovation center"* by 2030, with intermediate milestones by 2025. Xi Jinping himself has repeatedly stressed the need to *"accelerate the development of military intelligentization"* – essentially the PLA's drive to incorporate AI and autonomous systems into its doctrine (PLA Daily analyses, 2019–2021) ¹⁰¹ ¹⁰². In 2017, after Vladimir Putin made his "ruler of the world" comment, Chinese state media and PLA commentators echoed that sentiment as a clarion call: China must not fall behind in the AI arms race (Dahm, 2020) ¹⁰³ ¹⁰⁴. The PLA's official strategy documents now frequently mention **"intelligentized warfare"** (智能化战争) as the emerging form of war, following informatized warfare. For instance, China's 2019 Defense White Paper stated that warfare is evolving toward intelligentization ¹⁰⁵. PLA thinkers envision AI underpinning new concepts like **Multi-Domain Precision Warfare**, where AI fuses data from all domains to identify key vulnerabilities in an enemy's system-of-systems (Kania, 2022) ¹⁰⁶ ¹⁰⁷. In plain terms, China intends to use AI to target the nerve centers of adversary forces (e.g., communications nodes, logistics hubs) at lightning speed, paralyzing them – a strategy that Chinese experts argue could defeat a technically superior foe without having to match them plane-for-plane or ship-for-ship ¹⁰⁸ ¹⁰⁹.

Xi Jinping's speeches also tie AI to national rejuvenation and security. In one speech to the PLA in 2020, Xi urged faster integration of AI, big data, and cloud computing in training and operations (source: Xinhua, 2020 – data needed). The Chinese defense ministry has launched several high-profile AI projects and competitions. They have an annual **"Military Intelligent Technology"** competition (sort of like a DARPA challenge) to scout AI talents and solutions for the PLA.

Infrastructure Scale: To realize these ambitions, China is building an enormous AI infrastructure base. A key initiative is known as **"East Data, West Compute"**, a national project to create a distributed network of mega data centers – especially exploiting the interior provinces' cheap land and renewable power – to support AI computing needs ⁷⁰ ¹¹⁰. By 2022, China reportedly had more than 30 national-level AI computing centers either built or planned, aiming to provide exascale computing capacity for AI research (MERICS, 2023) ⁷⁰. Chinese tech giants and state firms alike are pouring money into GPU farms and cloud platforms. Even with U.S. export controls limiting their access to top-tier chips, China has amassed significant hardware. A recent analysis by Epoch AI (2025) estimates China possesses about **15% of global high-end AI computing capacity**, second only to the U.S. (which has ~75%) ¹¹¹. And they are trying to close that gap; for example, reports emerged that Chinese firms were bulk-buying tens of thousands of NVIDIA AI chips (A100/H800 GPUs) before new sanctions kicked in ¹¹². Additionally, China claims to have developed indigenous AI chips like Huawei's Ascend series. While still behind Nvidia in performance and hampered by 7nm fabrication limits, Huawei's latest 910B/910C chips show progress (roughly on par with

older Nvidia GPUs) ¹¹³ ¹¹⁴ . More telling is that **China is building advanced facilities to house these chips**: e.g., Alibaba's cloud and Baidu's cloud both opened new AI supercomputing centers in 2023 that rival many U.S. data centers in scale (each boasting many tens of thousands of GPUs, according to press releases).

China's **AI talent base** is also growing. More AI papers are published by Chinese researchers now than by U.S. researchers (though citation quality still lags somewhat) – a metric that shows sheer volume of research. A study by MacroPolo found that in 2022, about 29% of the world's top AI researchers were Chinese (by undergrad origin), many of whom are returning or collaborating with China ¹¹⁵ ¹¹⁵ . This talent feeds both civilian and military AI projects. The PLA is recruiting aggressively: they established AI research institutes at military universities like the National University of Defense Technology, and they partner with tech companies (like Baidu, Tencent) on defense-related AI research under civil-military fusion policies.

Policy and Organization: The Chinese Communist Party has elevated AI in its bureaucracy. They created a national AI Strategic Advisory Committee of experts, they embed AI goals in their Five-Year Plans, and critically, they practice **civil-military fusion** – meaning advancements in commercial AI are quickly leveraged for military use. For example, if a Chinese company masters autonomous driving, those algorithms might be adapted for autonomous military vehicles or drones. The PRC has also shown a willingness to allocate massive funding. Provincial governments offer subsidies and incentives for AI startups, and the central government funds major labs. By some estimates, China invested **tens of billions of dollars** in AI R&D and infrastructure over the past five years (Wu, 2023 – data needed).

On the military side, the **PLA Strategic Support Force (SSF)** likely plays a key role in AI for cyber, electronic warfare, and intelligence, while the services each experiment with AI in their domains (the Air Force with drone swarms, etc.). Notably, the PLA has showcased some capabilities: in 2019, Chinese media showed a swarm of 200+ drones flying in formation (breaking their own record) – a not-so-subtle message that they are working on swarm techniques. In 2021, there were reports (South China Morning Post) that China tested AI-controlled fighter aircraft in simulated dogfights, and the AI won some engagements against human pilots (paralleling the DARPA event). The **China Aerospace Studies Institute (CASI)** documented that Chinese defense firms are marketing unmanned platforms with increasing autonomy, like loitering munitions that can form “collaborative engagement networks.”

Organizing for AI warfare: The clearest indicator of how serious China is about AI in warfare is how they are integrating it into doctrine and training. PLA writings suggest that future conflicts will involve **“algorithm confrontation”** – essentially battles between each side's AI (Jiang, PLA Daily, 2021 – data needed). They anticipate that detecting the enemy's AI “decision algorithms” and disrupting them will be as important as physical combat. This indicates they are thinking ahead to AI-vs-AI scenarios. Moreover, Chinese military academies are now including AI modules in professional military education; they know operators and commanders need literacy in these tools.

China is also **investing in resilience against AI-powered threats**. For instance, they are aware the U.S. could use AI for quicker targeting of PLA assets, so they work on camouflage, deception, and decoys – possibly even AI-enabled decoys that imitate real units to mislead our targeting AI (a cat-and-mouse game). The PLA's focus on information dominance, as noted by Dahm (2020) ¹¹⁶ ¹⁹ , aligns with using AI to disrupt our networks while protecting theirs.

Validating the Stakes: All these efforts by China underscore that the “AI race” is not a U.S. fabrication. It is very real. If China were to achieve a breakthrough – say, AI that coordinates all elements of a Taiwan invasion seamlessly, outfoxing allied responses – it could change the strategic balance. As of today, the U.S. still holds advantages in many areas (top talent, cutting-edge chips, combat experience). But China’s scale and centralized focus could erode or surpass those advantages within this decade if we stagnate. The NSCAI bluntly stated *“China possesses the might, talent, and ambition to surpass the United States as the world’s leader in AI in the next decade if current trends do not change.”* (NSCAI, 2021) ¹¹⁷ ¹¹⁸. And such leadership in AI is viewed as key to overall global leadership.

We should note that China’s rapid moves come with some inefficiencies and missteps. There have been signs of **overinvestment and waste** – e.g., local governments building AI parks that sit underused (one analysis said up to 80% of new computing resources in some areas are idle due to hype-driven overcapacity) ⁷². This suggests a lack of coordination – interestingly, the U.S. faces the opposite challenge of dispersed, decentralized effort, while China sometimes has *too centralized* push leading to redundancy. Nonetheless, China can afford some waste given their scale, and they are likely to correct course when needed (they’ve already begun consolidating AI efforts under better oversight, creating a national data bureau to integrate data resources).

Military implications: If conflict were to break out in, say, the Western Pacific in the late 2020s, we should expect China to employ AI in numerous ways: autonomous drone swarms attacking our ships and bases, AI-assisted multi-domain command systems coordinating missile and aircraft attacks, cognitive electronic warfare (jammers that use AI to adapt to our radar frequencies in real time), and big-data surveillance to track U.S. force movements (perhaps using AI to fuse satellite imagery, underwater sensors, etc., for a clear picture of U.S. assets). They would also deploy AI for propaganda and influence, generating deepfakes or tailored messages to erode international support for the U.S. (already, there’s evidence of Chinese networks using AI to generate fake social media personas for influence operations).

The U.S., therefore, is not contemplating AI in a vacuum – we are responding to a strategic competitor who has made AI core to its strategy to displace U.S. military dominance. China’s AI push validates why we must double down on our own. It’s a classic security dilemma: if we don’t race to the high ground, someone else will seize it. As NSCAI’s Vice-Chair Robert Work put it, *“We know China is investing in AI for military use aggressively. We either do the same or risk falling behind on battlefields of the future.”* (Work, 2021, public testimony).

In summary, viewing the situation through an adversary lens – specifically China – we see an orchestrated national effort to harness AI for comprehensive national power, including but not limited to warfare. China is organizing its state, industry, and military to win in an “intelligentized” war. That is the competition we are in. Our response cannot be half-hearted. It demands a whole-of-nation strategy to ensure we retain the lead in AI algorithms, applications, talent, and infrastructure. The alternative is not just losing some tech market – it could mean losing our military edge and deterrence credibility in a future crisis, with dire consequences for global stability and U.S. interests.

The Cost of Falling Behind: U.S. Risks and the Coordination Challenge

While much of this chapter has focused on the opportunities of AI and what competitors are doing, we must also soberly consider the risks and challenges the U.S. faces on its own side. Even with our superior innovation ecosystem, the United States could fail to capitalize on AI dominance due to internal issues – fragmented efforts, misallocation of resources, and infrastructure bottlenecks. In a sense, AI dominance is as much an organizational challenge as a technical one. If we don't get our act together, we could squander our lead or struggle to translate tech gains into strategic advantages. A few key risk areas stand out:

Fragmented Siting and Effort: The U.S. AI landscape spans DoD labs, intelligence community projects, private sector labs, academia, and countless startups. This diversity is a strength, but also a weakness if not coordinated. We risk duplication of effort in some areas and blind spots in others. For instance, multiple services might be developing similar AI target recognition algorithms without pooling results – wasting time and money. Or, various states and companies build AI data centers wherever power is cheap, without considering national resilience (leading to clusters of compute that might be vulnerable to regional outages or attack). A lack of a national map for AI infrastructure means we might end up with, say, 80% of our high-end compute in two states – a concentration risk. The Biden Administration's creation of the AI Task Force and Joint AI Center (now the Chief Digital and AI Office, CDAO) is aimed to mitigate this, but those efforts are nascent. If we remain siloed, we cannot marshal our full AI potential the way China's top-down approach can. A coordinated approach – identifying key needs and directing resources – is needed to ensure critical national security AI projects (like next-gen AI for missile defense, or joint all-domain command AI) get priority access to compute and talent, rather than pet projects soaking up capacity.

Misallocated Compute and Talent: Compute (high-performance processors) and AI talent are limited strategic resources. Misallocation could mean using scarce top GPUs to, say, refine ad targeting models or minor academic pursuits while defense-critical needs starve. Right now, the vast majority of cutting-edge AI compute in the U.S. is in the private sector (the Googles, Microsofts, OpenAIs). There's nothing wrong with commercial progress – it drives innovation – but from a national security view, we need to ensure sufficient compute is available for things like training AI models for cyber defense or military simulations. Similarly, we have only so many elite AI scientists; if government and defense aren't attractive for them, they'll all cluster in industry, and DoD/IC efforts could lag. We need policies to encourage rotations or contributions of top talent to security missions (like the U.S. Digital Service model but for AI). The risk is not that America lacks talent, but that the talent isn't pointed at the hardest security problems. *"Data needed"*: We might reference a statistic that only a single-digit percentage of AI PhDs go into government roles – indicating a brain drain gap (hypothetical stat for illustration).

Energy and Infrastructure Bottlenecks: As noted, advanced AI development devours energy. If our power grids cannot keep up or if electricity becomes prohibitively costly/unreliable, that directly undercuts AI progress. Already, in Northern Virginia – a hub of data centers – the local utility has warned of capacity shortfalls delaying new data center connections ⁷³ ¹¹⁹. The Atlantic Council reported that in the PJM grid region, data centers (mostly for cloud and AI) could drive 90% of demand growth by 2030 ⁷⁵. If every AI megaproject faces multi-year power hookup delays, we'll lag. Moreover, if an adversary can strain our grid (through cyber or physical means) during a crisis, our AI systems and networks could be knocked offline at critical moments – a dire resilience issue. This is why energy and AI infrastructure must be developed hand-in-hand. The 2025 White House EO on AI infrastructure highlights building **clean energy capacity**

alongside compute clusters ¹²⁰ ⁶⁹ – not just for climate reasons, but also to ensure stable power supply for AI growth.

In military terms, even if we develop great AI, deploying it forward requires robust communications and computing infrastructure in theater. If we don't invest in hardened, distributed "battlefield cloud" infrastructure, our AI advantages may not translate to the edge where warfighters need them. That's an internal challenge – building resilient networks that can host AI even under attack.

Bureaucratic and Cultural Hurdles: The U.S. military and government are still adapting to the software-driven, rapid iteration mindset that AI thrives on. Requirements and acquisition processes move slowly; security clearance processes can deter top AI talent. There is risk in not reforming these. For example, if it takes 2 years to approve a new AI algorithm for deployment on a drone, whereas the tech itself advanced 4 generations in that time, we'll always field outdated AI. The DoD has begun agile programs and "DevSecOps" pipelines, but scaling that up is non-trivial. Additionally, a risk is **ethical and legal frameworks** – the U.S. rightly emphasizes responsible AI (law of war, etc.), but if we become overly hesitant to deploy effective AI due to fear of mistakes, we might cede ground to adversaries less encumbered by such concerns. We need to find the balance where we lead on ethics (to maintain values and global trust) without hamstringing ourselves operationally.

All these risks point to a common theme: **coordination and urgency**. Fragmentation, misallocation, and bottlenecks are all problems of insufficient coordination and speed at the national level. Overcoming them will require strong leadership (hence, perhaps something like a National AI Coordination Office or a czar with budgetary clout), public-private partnerships (since industry holds so much of the tech, we need mechanisms for them to support national security goals, perhaps through incentive structures or consortia), and strategic investments in enablers like workforce and energy.

In one sentence, the U.S. must ensure that our *unmatched innovative capacity* is harnessed and aligned toward the imperative of AI leadership, or else we risk squandering it via disunity and inertia. Unlike past eras, where our decentralized model often beat out centralized ones, in AI this could be a vulnerability if not managed – because the timeline is compressed (the technology cycles in months, not years).

We already see warning signs. For instance, while the U.S. debates semiconductor export rules, China is blitz-scaling data center construction. While U.S. defense primes work AI pilot projects, China's military could potentially just direct a tech giant to repurpose a mature commercial AI for military use overnight, speeding deployment. We have to get more agile in bridging private innovation to public defense.

To conclude this portion: **the cost of falling behind** or even just stagnating in AI is high. It could manifest not in a single moment but as a gradual erosion of deterrence and operational edge. If our adversaries can make decisions faster, see more clearly, strike more precisely, and coordinate more effectively because their AI systems outdo ours – then even our superior legacy platforms (fighters, ships) might fail to deliver victory. As stark as it sounds, losing the AI race could mean losing the next war. That is why addressing our internal hurdles is as important as outpacing the opponent. The reassuring part is that these are solvable problems – they lie in policy and management. Recognizing them is the first step, and efforts like recent executive orders are attempting to tackle them. The Army logistics article warns, "through training and education, we must build a data-literate workforce... and integrate predictive logistics into doctrine" ¹²¹ ¹²² – essentially a call to change culture and process. Similar calls echo across DoD: transform or risk obsolescence.

In sum, the U.S. must apply the same level of ingenuity to *organizing for AI advantage* as it does to inventing AI algorithms. Dominance won't come automatically from having the best tech in labs; it comes from deploying and scaling that tech effectively across the force and nation. That requires leadership focus to break silos, allocate resources wisely, and shore up critical infrastructure. These are challenges, but ones we can meet – indeed, we have done so in past tech races (nuclear, space) through national priority efforts. AI now demands a similar all-in prioritization.

Conclusion: High Stakes and the Road Ahead

AI's emergence as a pillar of national power has thrust us into a pivotal moment. This opening chapter has laid out **why** achieving dominance in AI is a U.S. national security imperative: it compresses decision cycles to machine speed, unlocks proactive intelligence, empowers cyber and autonomous operations, and fortifies our logistics and resilience – all qualitatively expanding what our military and nation can do. We have also seen that our chief rival, China, is moving at breakneck pace to harness AI for its own strategic aims, validating that the race is real and the stakes immense. The skeptic's view that AI is overhyped has been rebutted by the hard evidence of transformative impacts already in motion and the clarion warnings of our top leaders and commissions.

Yet, as much as AI offers us an edge, it also poses organizational trials that we must overcome – uniting our fragmented efforts, focusing our resources, and strengthening the backbone (from energy grids to networks) that undergird this new era of warfare. The price of failure is not abstract: it would be paid in lost battles, compromised deterrence, and a world where authoritarian powers hold technological sway. Conversely, if we succeed – if we adapt, invest, and lead – AI can be a cornerstone of continued U.S. military superiority, economic vitality, and democratic stability.

This is no time for complacency. As strategic evaluators might say, *we must constantly ask "Why?" and demand evidence* – the evidence presented here, from DoD statements to Chinese strategies, points to one conclusion: AI is **now** a central determinant of national power. The United States has a narrowing window to solidify its lead. The work must begin in earnest, with urgency and unity, to integrate AI across our defense and security enterprise responsibly but rapidly.

Bridge to Chapter 2: In the next chapter, we will dive deeper into China's full-spectrum AI program – examining how Beijing is developing and fielding AI across its military, surveillance state, and tech economy. Understanding the breadth and depth of China's effort will further illuminate the stakes and guide what the U.S. must do to stay ahead. The competition is on, and as we shall see, China's hand – its investments, innovations, and intentions – must inform our every move in this defining race of the 21st century.

Sources:

- Biden, J. (2025). *Executive Order on Advancing United States Leadership in Artificial Intelligence Infrastructure*. White House Briefing Room ¹ ¹¹ .
- Esper, M. (2020). *Secretary of Defense Remarks at DoD AI Symposium*. U.S. Department of Defense ² ¹² .

- National Security Commission on Artificial Intelligence (NSCAI). (2021). *Final Report*. (See Introduction and Chapter 1) ⁸ ⁴⁴ .
 - Hofstetter, P. et al. (2025). "The Impact of AI on Military Decision-Making," *TDHJ* ¹⁷ .
 - Johnson, T. & Wald, C. (2017). "The Military Should Teach AI to Watch Drone Footage," *Wired* ²⁶ ³⁷ .
 - Federal Bureau of Investigation. (2024). *Public Service Announcement: FBI Warns of Increasing Threat of AI-Driven Cyber Attacks* ⁴¹ ⁴² .
 - Dahm, M. (2020). "Chinese Debates on the Military Utility of AI," *War on the Rocks* ²⁰ ¹⁹ .
 - Harper, J. (2025). "Air Force eyeing AI-powered platform for wargaming," *DefenseScoop* ⁹² ⁹³ .
 - Mohan, C. (2025). "Predictive Logistics is the Way of the Future," *Army.mil – Army Sustainment* ⁵⁷ ⁶⁵ .
 - Trevithick, J. (2019). "Putin Says AI Leader Will Rule the World," *The War Zone (The Drive)* ⁸⁰ .
 - Sullivan, J. (2024). *Remarks on Artificial Intelligence and National Security*, National Security Council ⁸⁶ ⁸⁹ .
 - Atlantic Council (Willey, F.). (2025). "Overheated and Underbuilt: Fortifying the Grid" ⁷⁵ .
 - MERICS Report. (2025). "China's drive toward self-reliance in AI" (excerpt on infrastructure) ⁷⁰ ⁷¹ .
 - NSCAI. (2021). *Final Report – Executive Summary* ¹²³ ¹¹⁷ .
 - **[Additional citations from the text above have been preserved in-line in Harvard format with source links].**
-

- 1 9 11 69 120 **Executive Order on Advancing United States Leadership in Artificial Intelligence Infrastructure | The White House**
<https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2025/01/14/executive-order-on-advancing-united-states-leadership-in-artificial-intelligence-infrastructure/>
- 2 12 13 14 18 46 48 49 51 52 53 54 91 **Secretary of Defense Remarks for DOD Artificial Intelligence Symposium and Exposition > U.S. Department of War > Speech**
<https://www.war.gov/News/Speeches/Speech/Article/2341130/secretary-of-defense-remarks-for-dod-artificial-intelligence-symposium-and-expo/>
- 3 4 33 47 50 **Table of Contents - NSCAI Final Report**
<https://reports.nscai.gov/final-report/>
- 5 **Federal Register :: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence**
<https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence>
- 6 7 8 44 83 117 118 123 **assets.foleon.com**
https://assets.foleon.com/eu-west-2/uploads-7e3kk3/48187/nscai_executivesummary_digital_02-26-21.00a4dd7b303a.pdf
- 10 **AWS global data centers achieved PUE of 1.15 in 2023 - DCD**
<https://www.datacenterdynamics.com/en/news/aws-global-data-centers-achieved-pue-of-115-in-2023/>
- 15 16 **Operationalizing Artificial Intelligence for Algorithmic Warfare**
<https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2020/Crosby-Operationalizing-AI/>
- 17 81 82 **The Impact Of Artificial Intelligence On The Military Decision-Making Process And Mission Command - TDHJ.org**
<https://tdhj.org/blog/post/ai-military-decision-making/>
- 19 20 21 102 103 104 105 107 108 109 116 **Chinese Debates on the Military Utility of Artificial Intelligence**
<https://warontherocks.com/2020/06/chinese-debates-on-the-military-utility-of-artificial-intelligence/>
- 22 23 **Empowered edge versus the centralization trap: Who will wield AI better, the US or China? - Breaking Defense**
<https://breakingdefense.com/2024/02/empowered-edge-versus-the-centralization-trap-who-will-wield-ai-better-the-us-or-china/>
- 24 25 26 27 35 36 37 **The Military Should Teach Artificial Intelligence to Watch Drone Footage | WIRED**
<https://www.wired.com/story/the-military-should-teach-ai-to-watch-drone-footage/>
- 28 29 30 **Project Maven brings AI to the fight against ISIS | CNAS**
<https://www.cnas.org/publications/commentary/project-maven-brings-ai-to-the-fight-against-isis>
- 31 34 **Intelligence community pushes for 'AI at scale' under new IT roadmap**
<https://federalnewsnetwork.com/inside-ic/2024/07/intelligence-community-pushes-for-ai-at-scale-under-new-it-roadmap/>
- 32 **[PDF] Vision for the IC Information Environment - DNI.gov**
<https://www.odni.gov/files/documents/CIO/IC-IT-Roadmap-Vision-For-the-IC-Info-Environment-May2024.pdf>
- 38 **Artificial Intelligence for Predictive Maintenance - Booz Allen**
<https://www.boozallen.com/markets/defense/indo-pacific/artificial-intelligence-for-predictive-maintenance.html>
- 39 98 **The Rise of AI-Driven Cyberattacks: Accelerated Threats ... - MixMode**
<https://mixmode.ai/blog/the-rise-of-ai-driven-cyberattacks-accelerated-threats-demand-predictive-and-real-time-defenses/>

40 Most Common AI-Powered Cyberattacks | CrowdStrike

<https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/>

41 42 45 FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence — FBI

<https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence>

43 Why cybersecurity at the speed of AI is now a business cornerstone

<https://www.weforum.org/stories/2025/09/cybersecurity-ai-speed-business/>

55 56 57 58 59 60 65 66 67 68 76 77 78 79 84 121 122 Predictive Logistics is the Way of the Future | Article | The United States Army

https://www.army.mil/article/282488/predictive_logistics_is_the_way_of_the_future

61 62 63 64 Air Force selects AI-enabled predictive maintenance program as system of record | DefenseScoop

<https://defensescoop.com/2023/05/10/air-force-selects-ai-enabled-predictive-maintenance-program-as-system-of-record/>

70 71 72 110 112 113 114 115 China's drive toward self-reliance in artificial intelligence: from chips to large language models | Merics

<https://merics.org/en/report/chinas-drive-toward-self-reliance-artificial-intelligence-chips-large-language-models>

73 119 Hyperscale Data Centers: Energy Challenges and Sustainable ...

<https://174powerglobal.com/blog/hyperscale-data-centers-energy-challenges-and-sustainable-solutions/>

74 Bridging the 5-Year Gap: Off-Grid and Behind-the-Meter Gas Power ...

<https://www.woodwayenergy.com/off-grid-btm-gas-power-generation-data-centers/>

75 Grid Management Amid Rising Summer Temperatures - Atlantic Council

<https://www.atlanticcouncil.org/blogs/energysource/overheated-and-underbuilt-how-to-fortify-the-us-grid-in-the-face-of-heat-waves/>

80 Putin Says Whoever Has the Best Artificial Intelligence Will Rule the World

<https://www.twz.com/14141/putin-says-whoever-has-the-best-artificial-intelligence-will-rule-the-world>

85 86 87 88 89 90 Remarks by National Security Advisor Jake Sullivan on Artificial Intelligence and National Security at the National Defense University | The American Presidency Project

<https://www.presidency.ucsb.edu/documents/remarks-national-security-advisor-jake-sullivan-artificial-intelligence-and-national>

92 93 94 95 96 97 99 100 Air Force eyeing AI-powered platform for wargaming | DefenseScoop

<https://defensescoop.com/2025/08/13/air-force-wargaming-ai-saas-platform-rfi/>

101 The PLA and Intelligent Warfare: A Preliminary Analysis | CNA

<https://www.cna.org/analyses/2021/10/the-pla-and-intelligent-warfare-preliminary-analysis>

106 China prioritizing AI with goal of 'intelligentized warfare,' Pentagon ...

<https://www.foxbusiness.com/politics/china-prioritizing-ai-goal-intelligentized-warfare-pentagon>

111 The US hosts the majority of GPU cluster performance ... - Epoch AI

<https://epoch.ai/data-insights/ai-supercomputers-performance-share-by-country>