SHIFT5

Testimony by Dr. Josh Lospinoso
To the Senate Armed Services Committee
Subcommittee on Cybersecurity
Outside perspectives to inform understanding of the state of Artificial Intelligence and Machine Learning (AI/ML) applications to improve Department of Defense operations.

Chairman Manchin, Ranking Member Rounds, members of the subcommittee, it is my honor to have the opportunity to testify before you today on the state of Artificial Intelligence and Machine Learning applications to improve Department of Defense operations.

While AI research is well over 60 years old, development seems to be accelerating at a dizzying pace. Recent AI-powered technologies ranging from ChatGPT to self-driving cars have again captured the public imagination. The subcommittee is correct to treat this accelerating development with renewed urgency. Additionally, given the DoD's foundational role in artificial intelligence research, it's fitting that the National Security Commission on Artificial Intelligence has taken up the challenge of considering how the US can continue taking a central role in AI, responsibly employ AI for national security and defense, and protect against AI threats.

In this testimony, I want to bring to the subcommittee's attention two key facts about our weapon systems, AI, and cybersecurity:

1. Most major weapon systems are not AI ready
2. We cannot solve weapon system cybersecurity without AI

Today, the Department of Defense lacks the ability to collect, translate, enrich, store, and process weapon system data. Without these basic, fundamental elements, our major weapon systems cannot benefit from AI-powered technologies including cybersecurity, maintenance, and operational applications. They are and will continue to be stuck in the last century, and there is a real risk that our adversaries will leapfrog over us as a result.

The NSCAI made two important claims: (a) AI will exceed humans in a wide range of tasks, and that this will have world-altering impacts; (b) that AI wielded by our adversaries, especially China, will challenge America's technological predominance.

I wish I could disagree, but I wholeheartedly share the NSCAI's convictions. I would like to take the opportunity to emphasize and sharpen several key recommendations within the NSCAI report: manage risks associated with AI-enabled and autonomous weapons; establish justified confidence in AI systems; and present a democratic model of AI use.

Most major weapon systems are not AI ready

As data scientists are quick to say, "garbage in makes garbage out." Data allows us to investigate, train, and monitor novel AI-enabled techniques. Without high-quality data, we cannot build effective AI systems.

If military weapon systems are going to benefit from the rapid expansion of AI-power technology, Congress must levy requirements for every major weapon system that they collect, translate, enrich, and disseminate their data. These systems are designed with nervous systems that carry tremendous volumes of extremely valuable data. We must extract this data and make it broadly available across the Department to achieve the four top priorities outlined by the 2022 National Defense Strategy. Congress must also fund the requirements. This funding should go towards procuring readily available technology solutions across industry, not to merely study the problem, but to address the problem. This is how we will deter or win the next major conflict. We cannot wait a decade.

AI-powered technology is only as good as the data used to train it. Getting this wrong on weapon systems could put the warfighter at risk or result in mission failure. Today, the Department of Defense does not have anywhere near sufficient access to weapon system data. We do not – and in some cases due to contractual obligations, the Department cannot -- extract this data that feeds and enables the AI capabilities we will need to maintain our competitive edge. The Department of Defense must be empowered to holistically collect, assess, and manage data particular to those capabilities responsible for the defense of the Homeland. Ensuring that the Department not just has access to weapon systems data but can own that data will be a paradigm shift in the way the Department of Defense can truly assess total formation readiness. Enabled by AI technologies, commanders/operators/maintainers must have unparalleled visibility into not just the platforms but the fleets of weapon systems – without which, JADC2 cannot be achieved.

The DoD and the US have played a formative role in advancing the field of AI. The NSCAI's report provides a roadmap for how the US can retain AI preeminence, how the DoD must prepare for AI's potential impact on modern warfare, and how the world order could easily change if we misstep.

Each of these recommendations require the difficult, unglamorous work of laying strong foundations: clean, labeled, enriched, comprehensive data; sound, simple, decentralized, scalable data architectures; and straightforward, unambiguous metrics for measuring AI-empowered systems' effectiveness. Ask data scientists where they spend most of their time, and you'll hear that it's 90% data engineering, data cleaning, and data shaping. Obtaining and preparing the right data for a particular AI application is, by a wide margin, the least appreciated and resourced part of the process. Without robust, pristine, well-curated data sets, we must significantly reduce our expectations about the efficacy of AI applications built without this foundation.

I believe that three of the reports key recommendations -- managing risks associated with AI-enabled weapons, establishing justified confidence in AI systems, and presenting a democratic model of AI use -- require the unglamorous but essential work of laying strong foundations. This involves clean, labeled, enriched, and comprehensive data, sound and scalable data architectures, and straightforward and unambiguous metrics for measuring AI system effectiveness. This foundational work is crucial in ensuring weapon system cybersecurity, and the proposed solutions need to be implemented through funding and requirements. Ultimately, the successful deployment of AI in national security and defense requires a collaborative effort among government, academia, and industry to lay the groundwork and build on the progress made so far.

<u>We cannot address weapon system cybersecurity without AI</u>

As evidenced by the NCSAI report's length – over 750 pages – defense's role in AI is an enormous topic. I'd like to focus your attention on one specific and extremely consequential AI-enabled technology of great importance to the warfighter: weapon system cybersecurity. The FY2016 NDAA Section 1647 required DoD to complete cybersecurity vulnerability assessments for individual weapon systems. My colleagues and I spent considerable time studying these systems, and what we found unsettled us deeply. By comparison to weapon systems, IT systems like cell phones seem like impregnable fortresses. The Government Accountability Office arrived at the same conclusions, and in 2018 published its sobering "Weapon Systems Cybersecurity" report.

The DoD spends trillions of dollars fielding major weapon systems. Each one contains dozens – sometimes hundreds – of special purpose computers that perform every conceivable function. From the control surfaces on an aircraft to data radios on submarines, these systems are highly digitized. This digitization happened gradually over the latter half of the 20th century. Modern weapon systems are both profoundly digitized and highly interconnected. Many have radio frequency connections including to satellites and other weapon systems. Virtually all systems interconnect with IT systems such as maintenance laptops for routine upkeep. Some older systems were designed with the assumption that they would remain air gapped once they rolled off the assembly line. This assumption simply no longer holds in the modern military.

It is deeply unfortunate that we never architected cybersecurity requirements into these systems, their communications, or their interoperability layers. The result is that we have trillions of dollars of major weapon systems that are profoundly vulnerable to cyberattack. It is conceivable that the next major military conflict will be decided with the click of a mouse. Imagine the effect of a cyberattack against a satellite constellation, prepositioned defense stock, or a fleet of fighter aircraft positioned to response to crisis. The cyberattack doesn't have to be dramatic to be devastating; the enemy just needs to ensure that those fighters cannot get off the ground to respond to an attack.

Today, the IT cybersecurity community aspires to concepts such as "zero trust," where all system interactions are suspect and should not be trusted. Unfortunately, major weapon systems are several decades behind. They are complete trust systems. Regrettably, we cannot redesign these systems with secure electronics and protocols because of the long timelines and astounding costs involved.
All is not lost, however. We can draw strength from the tremendous progress that the cybersecurity community has made in securing IT systems. We do not need to reinvent the wheel. We can learn from thirty years of best practices to accelerate weapon system cybersecurity. Well known concepts like defense in depth, patch management, access controls, and incident planning are highly applicable to weapon system cybersecurity. This is far too big a job for one organization to solve. It will take a village – including government, academia, and industry – to get there. Each best practice reinforces the other.

In the world of major weapon systems where there is virtually no cybersecurity aside from obscurity, observability is the first step. Not only does it help you to design the other control measures, but it ensures that you are keeping up to date with the latest threats. To observe weapon systems – or any

digital system for that matter – you need data collection. Weapon systems have data networks that connect all their electronic components. You can think of them like nervous systems. These nervous systems generate enormous amounts of extremely valuable data every second. Unfortunately, in 2018 no weapon systems collected all – or anywhere near all – of this data. These platforms were talking, but no one was listening.

Industry has tackled the weapon system cybersecurity observability problem by building the foundational tools first. The military now has readily-available, certified hardware capable of real-time edge computing and software capable full-take data capture from every bus. Frameworks exist for normalizing, translating, and enriching the data into a common format. Technologies and processes for liberating this data from the weapon systems can be fed into cloud environments. This took years, but the military should be proud that it successfully completed its first full-fleet deployment last year and has already democratized many terabytes of critical data from that fleet. The services have begun many more initial deployments since.

Armed with this foundation widely deployed across the DoD – pristine, full, high-quality digital data streams from every weapon system – we would have the platform to build AI-enabled applications that can scale and integrate across platforms to support all domain operations. Intrusion prevention is a canonical example. In AI parlance, intrusion prevention is a "classification problem." Given a stream of data, you must detect anomalous/malicious traffic from normal/benign traffic. There are several algorithms that are very good at detecting many kinds of cyberattacks against weapon systems. No need to reinvent the wheel.

But we're only able to unleash these algorithms once we build the data foundation.

We Are Out of Time

In very short order, we must aggressively expand this foundational work across our major weapon systems. There is remarkable work on enterprise architectures to promote ready, decentralized, self-service access to wide ranges of data, algorithms, and applications. We must expand the scope of these foundational efforts to include the trillions of dollars of major weapon systems that the warfighter relies on in both combat and training missions.

The extensive NSCAI report comprehensively addressed some very critical issues regarding the state of the AI ecosystem and produced an extensive series of key recommendations to change the paradigm of AI adoption. However, we do not have the luxury of time for drawn-out policy and budgetary cycles; if the U.S. does not take the lead on establishing and formalizing standards and responsible use of AI, our adversaries will.

Recent legislative activity highlights the congressional commitment to addressing the issue, but we must be mindful of the speed in which we consider the role of AI in defense. While our adversaries are developing and employing AI technologies at speed of requirement, we must be faster – we must consider how to deliver at the speed of action. As data continues to flow off weapon systems and associated sensors, the Department must consider the resource limitations it faces with sensemaking; there will never be enough DoD civilians or servicemembers to manage the biblical deluge of data – AI models must be employed to ensure a postured, ready, and resilient formation where the unnecessary risk of known vulnerabilities is addressed with smart models that can distinguish between anomalous alerts as maintenance issues or cyberattack.

While the Department defends their FY24 budget requests, Congress must ask – are these budgets representative of change necessary to truly develop and posture a ready force? Does the Department consider readiness in terms of threats borne of the 21st century, or are they still articulating ability to fight through outdated, outmoded practices of failed history? Are the right steps being taken to buy down unnecessary risk based upon known vulnerabilities, or does emphasis remain upon those capabilities which might be useful today but useless tomorrow?

America's preeminence as a military superpower derives from several key inputs including the world's best trained and highest quality people, its robust budget, its global reach, and our tremendous allies and partners. But its technological superiority, especially manifested in our major weapon systems, is where we derive the greatest advantage. If, as the NSCAI's report warns, the United States doesn't retain its AI dominance and empower its major weapon systems with AI-enabled technology, we face the real prospect that an adversary could surpass us.

We must act now to prepare our major weapon systems for the era of AI. We are decades behind and there's not a moment to lose.