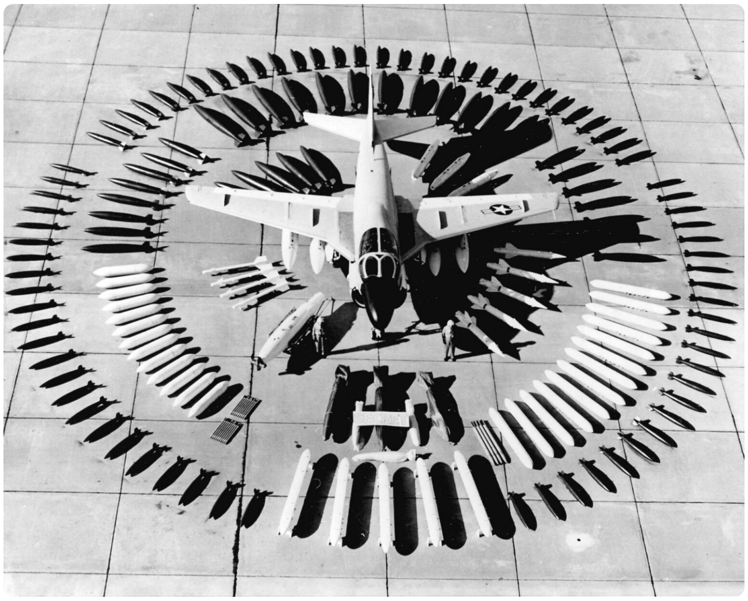
AINOW

Research Oct 22, 2024

New AI Now Paper Highlights Risks of Commercial AI Used In Military Contexts



Research Areas:
Safety & Security

READ PAPER ON ARXIV

Mind the Gap: Foundation Models and the Covert Proliferation of Military Intelligence, Surveillance, and Targeting examines urgent national security risks posed by AI systems used in military contexts. The paper finds that while the policy discussion about AI and national security has largely focused on the risks of AI serving to proliferate chemical, biological, radiological and nuclear weapons (CBRN), these concerns are not most pressing. Instead, policymakers must widen the aperture and focus much more attention on AI systems already in wide deployment for military intelligence, surveillance, targeting, and reconnaissance, as such systems pose current dangers, and with the introduction of foundation models into these contexts, address their significant future risks.

The paper examines systems currently in use in military contexts, such as Gospel, Lavender, and Where's Daddy, which are deployed in Gaza and contributing to a significant civilian death toll. Such systems rely on significant personal data, and raise urgent questions on their own. And currently plans are being made to integrate foundation models into these systems, further exacerbating the risks they already pose. Risks that have at their heart the reliance on personal data, which can be exfiltrated and weaponized by adversaries, and the vulnerabilities that are present in such systems, and currently have no remedy.

The report concludes that in order to secure military systems and limit the harms of AI-based armaments to national security, creating military AI systems that are separate from commercial systems, and addressing the security risk posed by the use of personal data within commercial AI models, will be necessary.

Outlining the limitations of currently proposed policy interventions such as compute thresholds and export controls for addressing these harms, the report recommends a novel approach to addressing the national security concerns posed by AI systems: in particular, the necessity of insulating military AI and personal data from foundation models as necessary protections for national security.

RESEARCH AREAS

Safety & Security