AI-Powered Autonomous Weapon Systems Risk Geopolitical Instability and Threaten AI Research

Riley Simmons-Edler*[1], Ryan P. Badman*[1], Shayne Longpre[2], Kanaka Rajan[1]
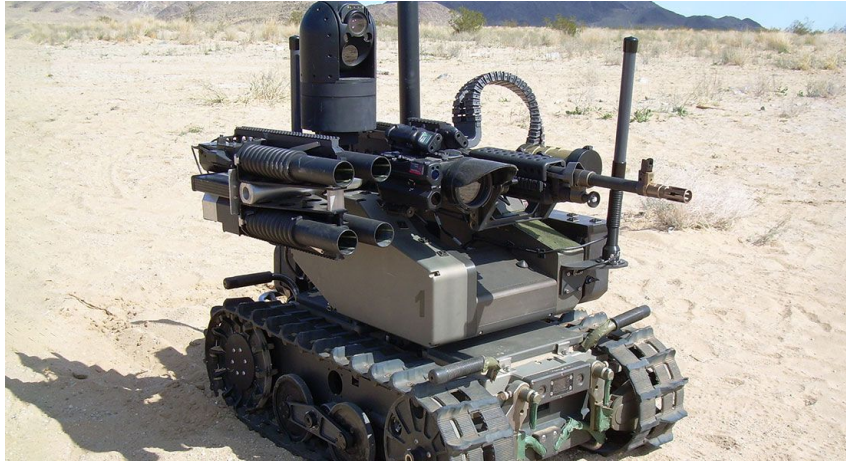
[1]Harvard Medical School, [2]MIT Media Lab

*Equal contribution

What are "Autonomous Weapon Systems" (AWS)?

ZALA Lancet-3

QinetiQ MAARS

STM Kargu-2

AWS Examples- Air

Kratos XQ-58 Valkyrie 🇺🇸

~2,500 kg

Shield AI V-Bat 🇺🇸

57 kg

AWS Examples- Ground

Milrem TheMIS 🇪🇪

Ghost Robotics Q-UGV 🇺🇸

AWS Examples- Sea

US Navy Sea Hunter USV 🇺🇸

Boeing Echo Voyager UUV 🇺🇸

Not a new idea

San Antonio Light, July 28, **1935**

Ghost Robotics Q-UGV, **2024**

Growing Relevance

AI's 'Oppenheimer moment': autonomous weapons enter the battlefield
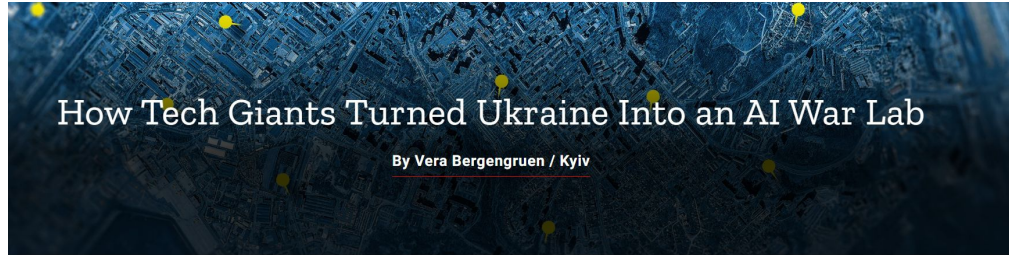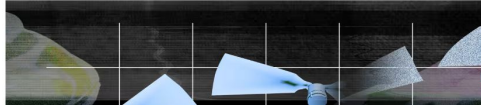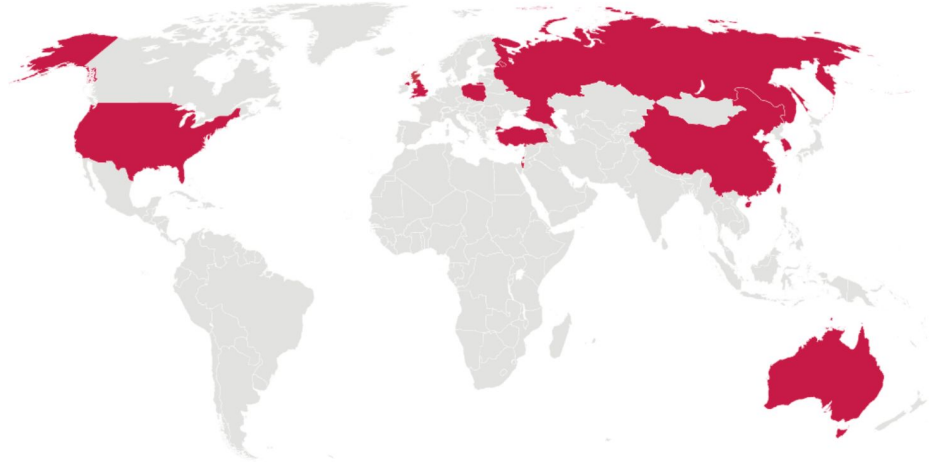
Nick Robins-Early

Sun 14 Jul 2024 12.00 EDT

How Tech Giants Turned Ukraine Into an AI War Lab

By Vera Bergengruen / Kyiv

THE KYIV INDEPENDENT

Tuesday, April 16, 2024

rn Europe   Video   Culture   Podcasts   Investigations   War Crimes   Explaining Ukraine

NEWS FEED, WAR, UKRAINE, DRONES, DRONE PRODUCTION, WEAPONS

Deputy minister: Ukraine can produce 150,000 drones per month

Share

by Elsa Court and The Kyiv Independent news desk · March 5, 2024 3:17 PM · 2 min read

Major AWS manufacturers

Map from "Loitering Munitions and Unpredictability: Autonomy in Weapon Systems and Challenges to Human Control," Bode and Watts, 2023

Growing Investment in AWS R&D

FIGURE 2
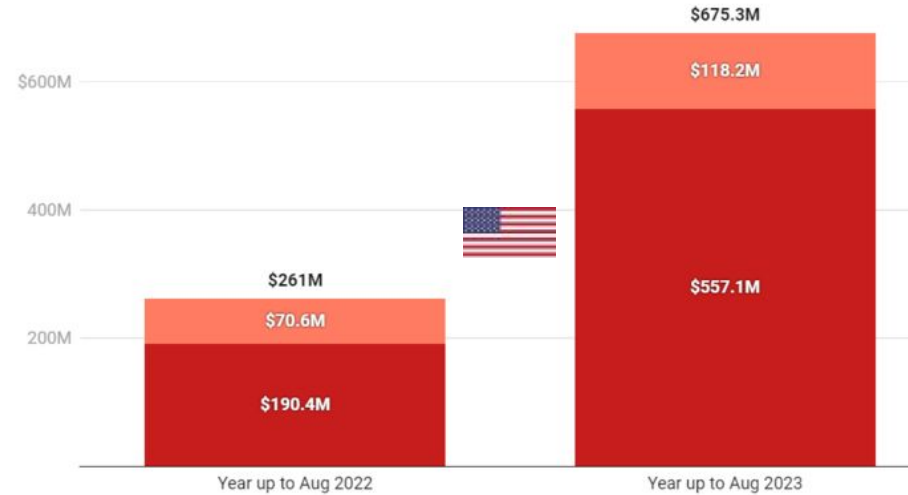Number of PLA AI Contracts by Application Area
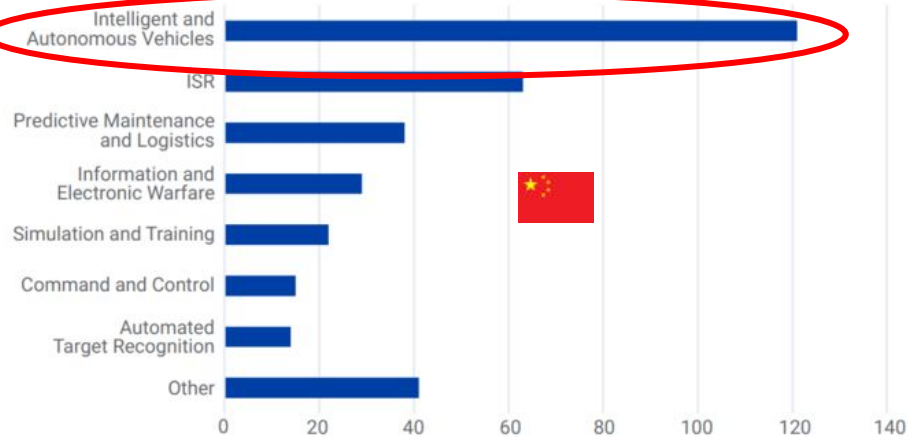
Source: CSET corpus of PLA procurement activity (343 AI contracts).

U.S. military AI spending nearly tripled from 2022 to 2023

Total dollars obligated from AI-related federal contracts, $M

■ Department of Defense   ■ Other agencies

Contracts classified as AI-related if they had the term "artificial intelligence" or "AI" in the contract description.

Chart: Will Henshall for TIME · Source: Brookings Institute · Get the data · Created with Datawrapper

Left: "Harnessed Lightning: How the Chinese Military is Adopting Artificial Intelligence," Fedasiuk et al, 2021

Right: "The U.S. Military's Investments Into Artificial Intelligence Are Skyrocketing," Will Henshall, 2024

The Vision
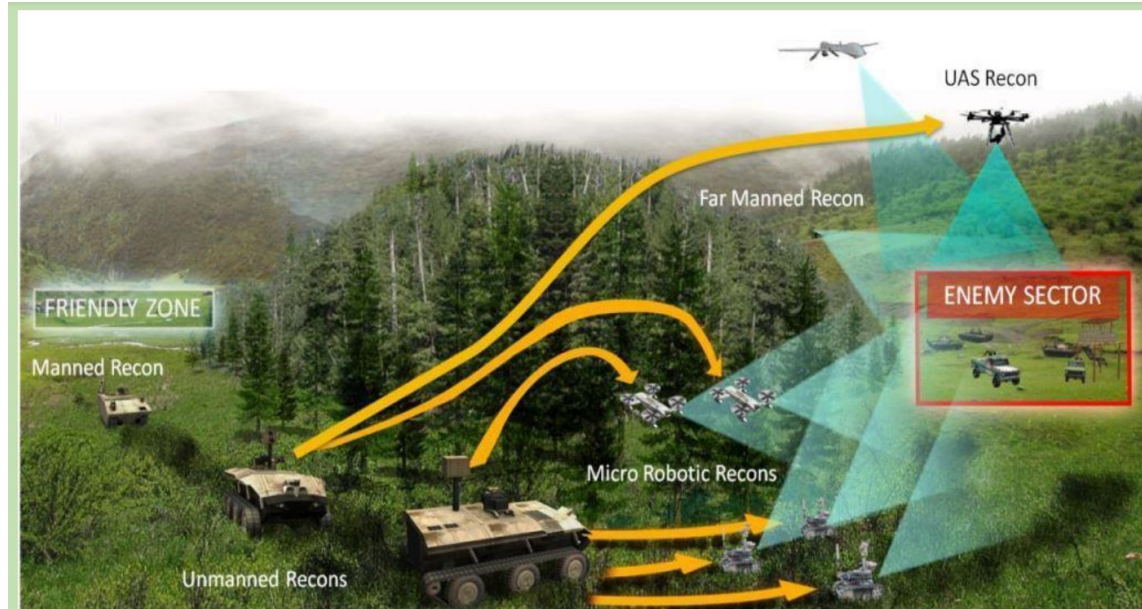
AWS remove human soldiers from the active battlefield

Geopolitical Implications

- Starting wars costs treasure, not blood (for invaders)

- Countries can shoot at each other's robots "casually," risking escalation

- Easier to start wars ("~~boots~~ bots on the ground"), but maybe not to finish them

- Easier to cover up atrocities, hide realities of war from the public

  - Limited human battlefield presence means limited visibility into how the war's going

- Invites asymmetric and inhumane tactics

  - If attacking their robots won't deter your rival, maybe attacking their civilians will

Academic Implications

If the primary weapon of war is robots running ML models, AI/ML research has major national security implications

If you have better ML models than rival nations, you will have an edge in war

We've been here before: Rocket science and nuclear physics in the cold war

Academic Implications

Visa restrictions on ML researchers are already a thing (and will get worse)

ML hardware export controls are already in place (and will get tighter)

Military-civil fusion programs are already happening (and will be more widespread)

Publication restrictions? Restrictions on open-source code?

Security clearances to do civilian AI research?

Increased funding/push for "dual use" research is very likely

AI companies will also be potential defense companies, with all that entails

Can we do anything about it?

- Software/hardware restrictions are unlikely to help
  - AWS don't need big models or datacenter compute, can rely on embedded processors
  - Russia fields numerous AWS in the Ukraine war despite heavy sanctions
- Define and maintain boundaries between civil and military AI R&D
  - Universities need to treat military funding the way they treat corporate funding
  - How much military R&D should civil-focused AI companies do?
- Advise policymakers about consequences of AWS development
  - We have a spotlight right now as a field, let's use it
  - Raise public awareness of the realities and risks of militarized AI (short of AGI)

AWS are coming, but the role they take can still be influenced, and the risks mitigated

Thank You!

Check out the paper!

Coauthors:

Riley Simmons-Edler
@SimmonsEdler

Ryan P. Badman
@RyanPaulBadman1

Shayne Longpre
@ShayneRedford

Kanaka Rajan
@KanakaRajanPhD

Alternate Viewpoint: What about a ban?

It would be best if "killer robots" were never developed

Sadly, there's too many of them already and they are too useful to get buy-in

Weapons that get banned tend to be both inhumane and not very effective

Thus, limits on use, development, autonomy, to stave off the worst consequences

AWS should augment, but not replace, human-operated weapons

Note: All of this is independent of "human in the loop" ethical concerns or the risk of increased collateral damage (which also matter)