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

Fire support

Anti-personnel

Anti-vehicle

"Weapons that can make decisions autonomously"
(in particular, using machine learning)
Many different shapes, sizes, capabilities

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 🇺🇸

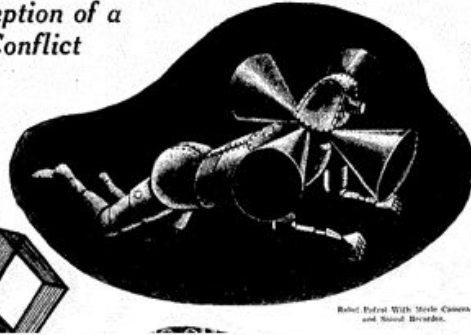Boeing Echo Voyager UUV 🇺🇸

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

How Tech Giants Turned Ukraine Into an AI War Lab
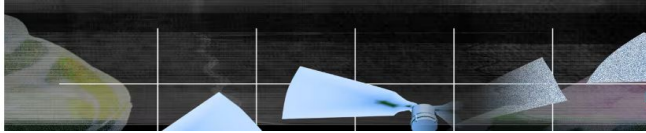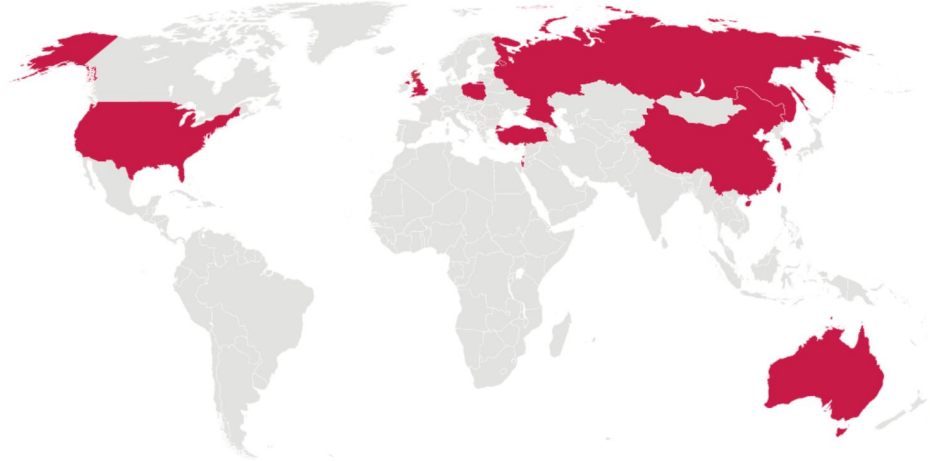
By Vera Bergengruen / Kyiv

Illustration by TIME

Large (and growing) # of AWS manufacturers

THE KYIV INDEPENDENT

Tuesday, April 16, 2024

...rn Europe · Video · Culture · Podcasts · Investigations · War Crimes · Explaining Ukra...

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

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

Share 🐦 👍 in ✉

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

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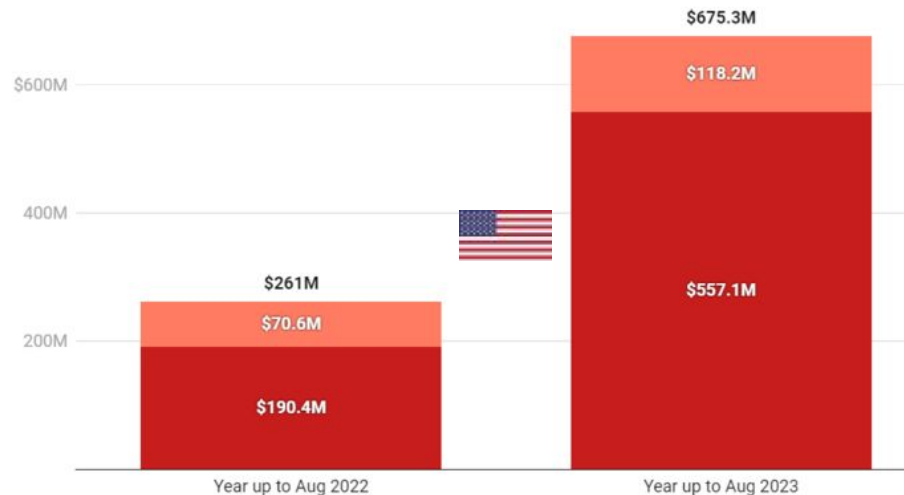Number of PLA AI Contracts by Application Area
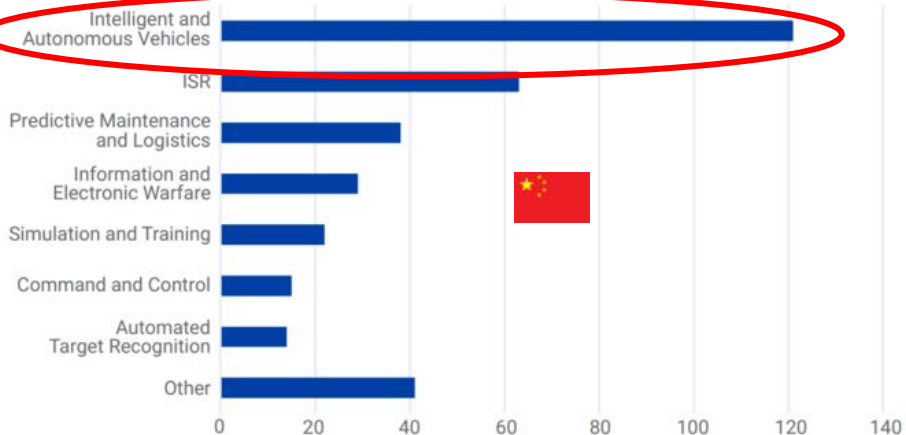
Source: CSET corpus of PLA procurement activity (343 AI contracts).

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

$675.3M
$118.2M

$600M

400M

$261M
$70.6M

200M

$190.4M

$557.1M

Year up to Aug 2022   Year up to Aug 2023

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
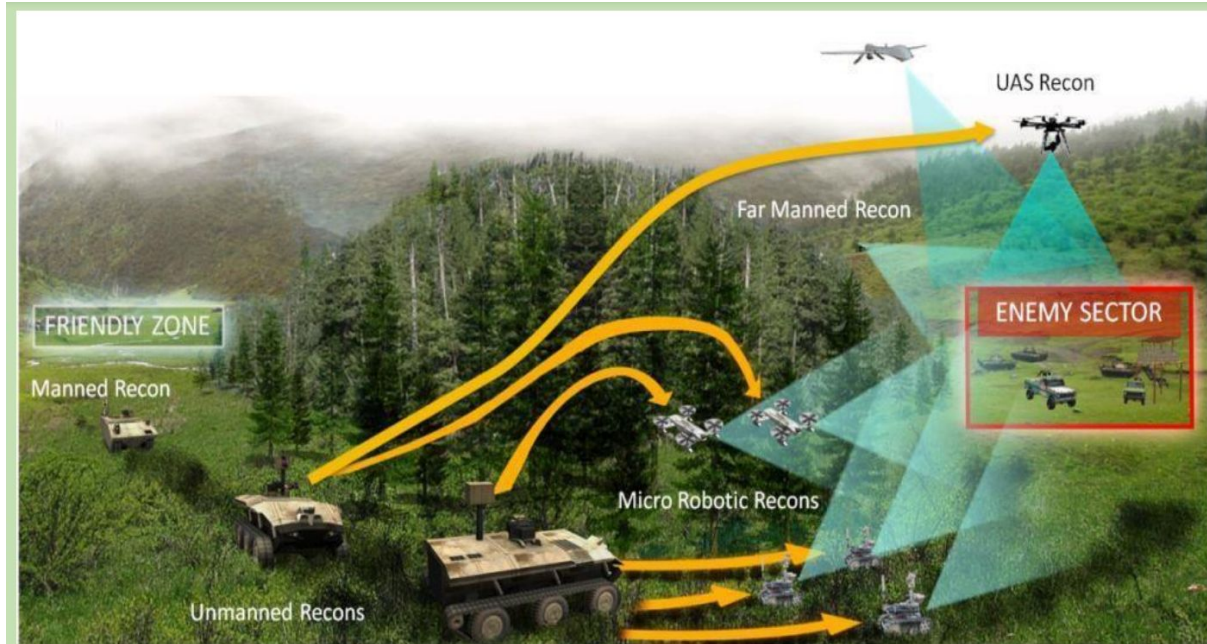
Geopolitical Implications

Say this vision works out- what are the implications?

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

- 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

- Invites asymmetric and inhumane tactics to deter

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

Academic Implications

- ML advances have major national security implications

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

  - Incentive to encourage non-public ML research (closed source, even classified)

- Current trends look like e.g. cold war nuclear science:

  - Visa restrictions on ML researchers are already in some countries (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)

  - Military funding for dual-use research is already a thing (and there will be more)

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

Can we do anything about it?

There's <u>no simple solutions</u>, but some ideas to start:

- Reject software/hardware restrictions as a solution
  - 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
- Create clear 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/use
  - 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)

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

Thank You!

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 ban buy-in

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

AWS are not innately either of those (compared to other weapons)

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)