



**MINISTÈRE
DES ARMÉES**

*Liberté
Égalité
Fraternité*



The Future of Defense

Thibaud Ehret



Generative AI : from research to general use product

ChatGPT

- ▶ Research paper introducing the transformer architecture in 2017 (Attention is all you need)
- ▶ ChatGPT public launch 2022
- ▶ One million users in **five days**
- ▶ Previous record for the iPhone (74 days)
- ▶ Twitter (2 years), Netflix (3.5 years)

New risks

- ▶ Deep fakes, fake news
- ▶ Plagiarism, IP theft

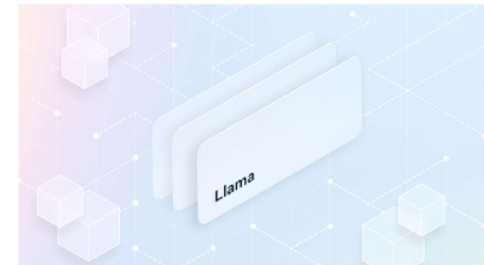
AI hijacking

- ▶ "We believe it is in both America and the wider democratic world's interest for American open source models to excel and succeed over models from China and elsewhere." (Meta)
- ▶ Chinese researcher used Llama 13B for military applications
- ▶ ChatBIT was fine-tuned and "optimised for dialogue and question-answering tasks in the military field" (Reuters)

Meta

Open Source AI Can Help America Lead in AI and Strengthen Global Security

November 4, 2024
By Nick Clegg, President of Global Affairs



Takeaways

- We're making Llama available to U.S. government agencies and contractors working on national security applications.
- Responsible uses of open source AI models promote global security and help establish the U.S. in the global race for AI leadership.
- Open source AI benefits the public sector by enabling discoveries and breakthroughs, driving efficiency and improving delivery of public services.

French Strategic Reviews



REVUE STRATÉGIQUE
DE DÉFENSE
ET DE SÉCURITÉ NATIONALE
2017



"The ongoing digital revolution, driven by public and business applications, is likely to yield the most significant disruptive technologies. Hyperconnectivity, big data technologies, the Internet of Things and robotics are examples of fields offering major opportunities for defence applications. Artificial intelligence, in particular, is expected to play a central role in defence systems, where it will make a significant contribution to operational superiority, while entailing new risks."
October 2017

"A meaningful AI implies that we know the way forward. This is the objective of the industrial policy presented in part 1 and structured around four strategic sectors: health, ecology, transport/mobility, and defence / security."
March 2018



French MoD's AI Master Plan



Minister's speech of April 5, 2019, with the main guidelines an AI Defence strategy

Publication of the report «**ARTIFICIAL INTELLIGENCE IN SUPPORT OF DEFENCE**» in September 2019

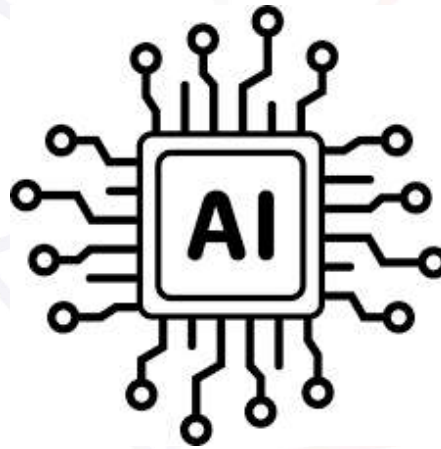
- ▶ Priority areas of application
- ▶ Ethics and AI in the defense field
- ▶ Trusted AI
- ▶ Ministerial action and the defense AI Ecosystem
- ▶ Data for the Ministry of the Armed Forces



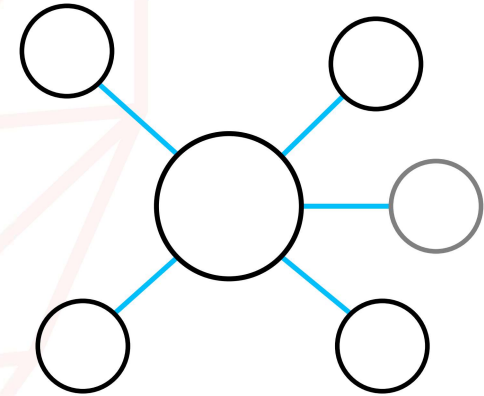
The Recipe for AI Adoption: Talent, Technology, and Transformation



Reinternalizing
Talents and
Competencies



Sovereign
Supercomputer for
Sensitive
Data-Based AI
Training



Developing internal
and external
collaborations (by
leveraging data)

AMIAD : a defense AI agency

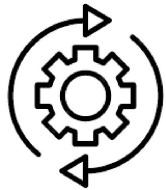
The Agency's Mandate

- ▶ Contribute to the transformation of armies, departments, and services.
- ▶ Accelerate the integration of AI into operations and organic processes.
- ▶ Enhance our operational superiority and daily efficiency for Ministry collaborators.



Our mission (short)

Bertrand Rondepierre, Director of AMIAD



Scaling up the use of Artificial Intelligence across various military applications.



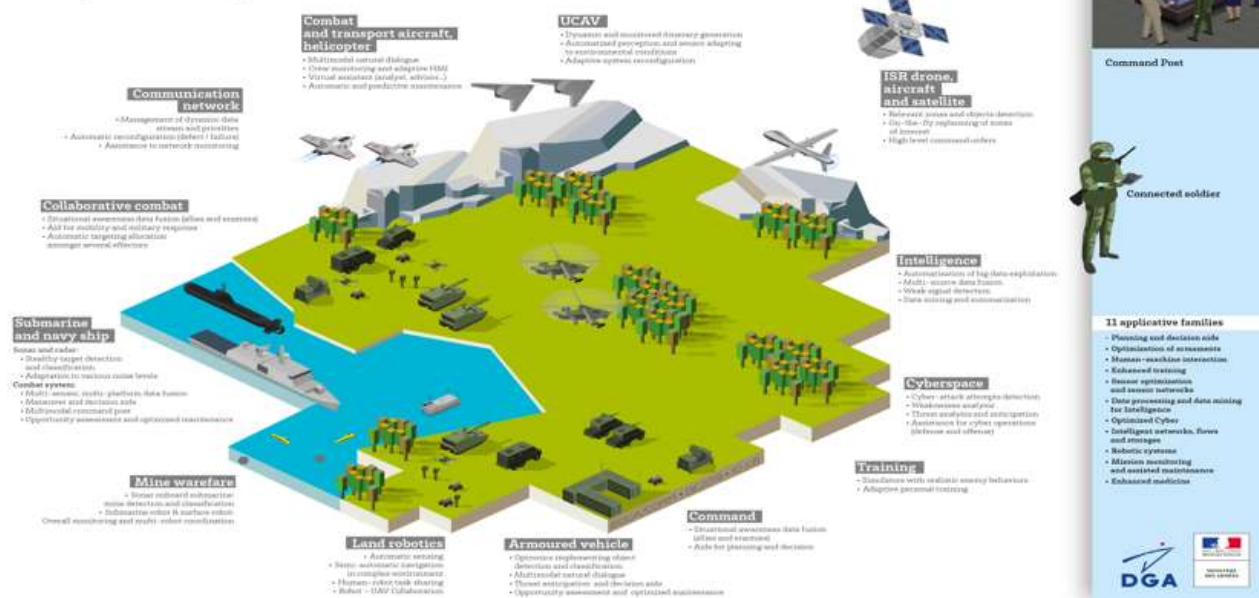
Review of Potential Applications

Three priority areas of application

1. Operational AI
2. Embedded AI
3. Organizational AI

Artificial intelligence

Serving the forces to boost the performance of operational systems

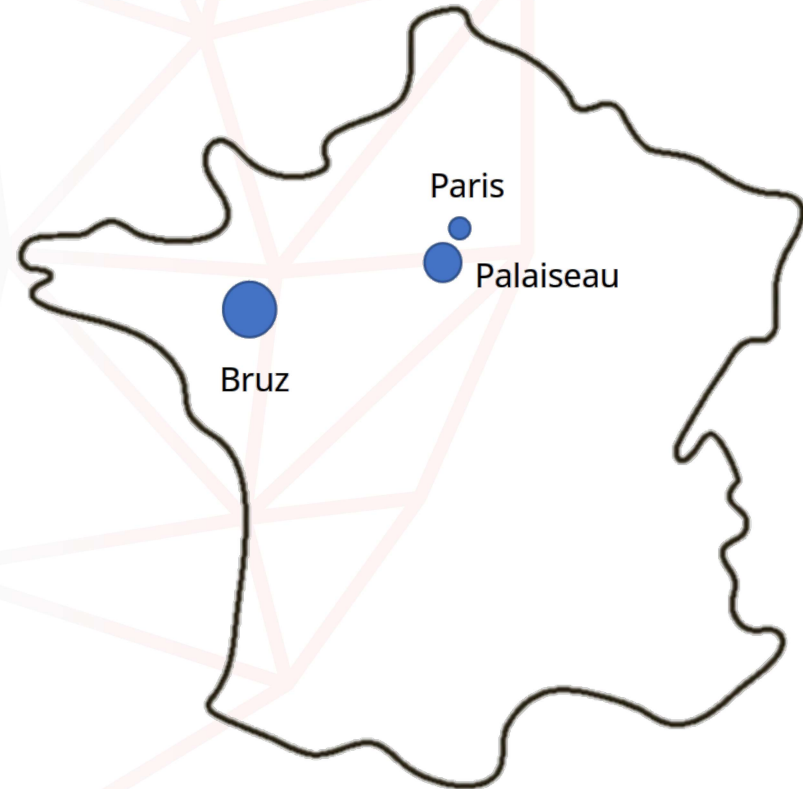


Organization of the agency

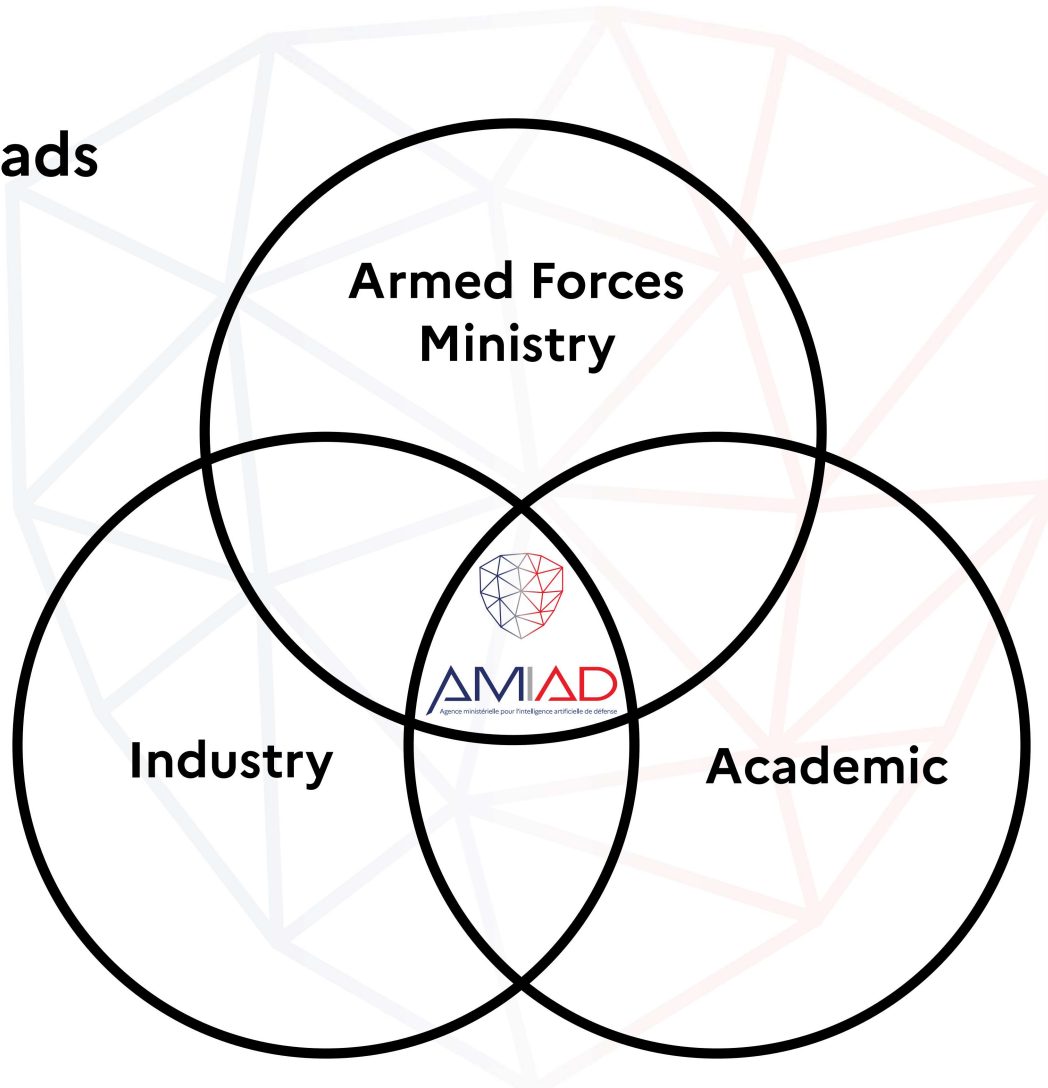
Recruiting 300 new talent professionals by 2026

A research and development organization:

- ▶ A technical department
- ▶ A research department



At the crossroads



The research department

Three main objectives:

1. Promote the development of defense AI in conjunction with the civil ecosystem, particularly the academic world.
2. Host young talents who will eventually join the operational department of the AI agency or the armed forces, directions, and services.
3. Enhance the credibility of the Ministry's actions by publishing at an international level.

Collaboration at a national level...

Located at the heart of Paris-Saclay research-intensive cluster

- ▶ National research institutions



- ▶ Prestigious schools and universities



- ▶ Industry research labs

...but also at a European level

AI Factories



- ▶ Health and life sciences
- ▶ Manufacturing
- ▶ Climate and environment
- ▶ Finance
- ▶ Automotive and autonomous systems
- ▶ Cybersecurity
- ▶ Agri-tech and agrifoods
- ▶ Education, arts and culture
- ▶ Green economy
- ▶ Space
- ▶ Defense

Generative AI in Defense and Security (1)

Project managed by AMIAD

Generative Adversarial Networks (GANs) and Transformers

- ▶ Detection of disinformation
- ▶ Creation of malicious content

Signal Processing and Data Security

- ▶ Critical for Defense Systems : Ensuring integrity and confidentiality
- ▶ Key Aspects : Reliability, Integrity, Transparency, Security of systems using generative AI

Data Integrity

- ▶ Particularly for Training Models
- ▶ Ensuring the accuracy and reliability of data used in training models

Generative AI in Defense and Security (2)

Project managed by AMIAD

Robustness to Attacks

- ▶ Developing mechanisms to detect and resist attacks
- ▶ Ensuring the resilience of generative AI systems against malicious activities

Explainability and Transparency

- ▶ To explain and make transparent decision-making processes
- ▶ Enhancing trust in generative AI models by making their operations understandable

Risks Related to Hallucinations

- ▶ Developing mechanisms to detect and reduce the risk of hallucination
- ▶ Ensuring that generative AI outputs are accurate and reliable

Generative AI in Defense and Security (3)

Project managed by AMIAD

Model Security

- ▶ Protection Against Unwanted Dissemination : Safeguarding models and training data
- ▶ Preventing unauthorized access or misuse of sensitive information

Control and Regulation

- ▶ European Approach : Horizontal regulation of AI application development and dissemination in member states
- ▶ Impact on National Defense and Security : Analyzing the effects of this regulation on defense systems