Clingendael
Netherlands Institute of International Relations

JUNE 2025

ReArm Europe: A lack of a viable short-term strategy on the military use of Artificial Intelligence

Erik Stijnman

© AI generated

In December 2024 the Dutch military intelligence agency (MIVD) director, Rear Admiral Reesink, stated that 'despite heavy Russian losses in Ukraine, Russia's weapons and munitions supplies grow faster than compared to NATO'[1] and added that Moscow can be ready for an armed conflict with NATO before 2030, which is one of the scenarios he takes into consideration. Addressing the issue of limited European regeneration efforts as part of NATO, the EU drafted a White Paper *Rearm Europe Plan, Defence Readiness 2030* in March 2025. This alert argues that this plan lacks sufficient attention to which shorter-term military AI-strategy should be an integral part of expanding Europe's military capabilities. This alert is meant to inform Dutch and European policy makers and military experts.

Before addressing a shorter-term AI strategy that would better support European military capability development, this article will first outline what the Rearm Europe Plan and the White Paper intends to achieve. This section will also shortly discuss how military AI does – or does not fit – in the White Paper's claim

1 MIVD-directeur: 'Rusland kan binnen enkele jaren een groot conflict met de Navo aan'

on the importance of AI in military capability development. Secondly, it will propose a division in the military application on Artificial Intelligence (AI). Is AI automatically a disruptive innovation or technology as the White Paper suggests, or can it be understood in other ways too? The insights from these paragraphs will then be compared to contemporary AI-strategies of Ukraine and China. This article will conclude with recommendations on a viable, short- term AI strategy for Defence Readiness 2030.

White Paper Rearm Europe Plan/Defence Readiness 2030

Kaja Kallas – the EU's High Representative for Foreign Affairs and Security Policy – noted that 'to be able to live in peace, we need much greater investment in European defence to ensure the security of all EU citizens today and for the future'[2]. As such, the White Paper aims to provide a blueprint for action and aims to deliver more capable, fully ready European Defence by 2030.

To achieve this, the White Paper outlines 'three key areas of action'[3]:

- **Closing capability gaps and supporting the European defence industry**, including simplifying regulations and streamlining industrial programmes.
- **Enhancing European readiness for worst-case scenarios**, by improving military mobility, stockpiling, and fostering operational cooperation across the EU.
- **Deepening the single defence market** and accelerating the transformation of defence through disruptive innovations such as AI and quantum technology.

The Rearm Europe Plan aims to increase financial flexibility, allowing EU-member states to massively ramp-up defence spending with € 800 billion to close capability gaps and to support the European defence industry. Indeed, simplified regulations may facilitate faster procurements of EU-member states.

Increased budget will also directly contribute to the improvement of military mobility, the stockpiling and procurement of military equipment, and the enhancement of European readiness for worst-case scenarios, such as an open war with Russia.

However, to deepen the single defence market and accelerating the transformation of defence through disruptive innovations such as quantum technology and AI, more is needed than money alone. The White Paper argues that 'by attracting new players and supporting investments in disruptive innovations (for instance, AI and quantum technology), and by learning from the battlefield experiences of the Ukrainian defence industry, Europe will [be] better able to deter adversaries'[4].

Since the White Paper considers AI a *disruptive innovation* or *disruptive technology* one would therefore expect AI to play a central role in building capabilities. In contrast, AI is depicted just as one, decentral part, of a total of seven identified critical capabilities (see figure 1), giving rise to the assumption that the role and impact of AI in military capabilities is only partially understood.

2 White Paper for European Defence – Readiness 2030 | EEAS

3 Future of European defence - European Commission

4 White Paper for European Defence – Readiness 2030 | EEAS

Figure 1 'Critical Capabilities ReArm Europe'[5]

The next paragraph will explore to what extent AI is indeed a disruptive innovation or something else. Under the premises that understanding the role of AI in a military context, can help to eventually determine what a shorter AI-strategy for building military capabilities might be.

Artificial Intelligence (AI): a disruptive innovation or something else?

Some scholars already warned that 'the traditional categorization of innovation as either incremental or radical is incomplete and potentially misleading. 'There is growing evidence that there are numerous technical innovations that apparently involve modest changes to existing technology but have quite dramatic competitive consequences'[6].

Given the theoretical foundation of Architectural Innovation, AI is the perfect tool to alter 'the overall architecture of the product [which] lays out how the components will work together'[7], even in cases where there are only minor or no technological changes. When used in this way, AI is not a *disruptive technology* but can create a *disruptive effect*, making AI the tool that facilitates a change of the overall architecture. Examples are the integration of separate air-missile defence, artillery systems, drones and ammunition resupply using AI (see visualization figure 2). Put differently, AI can help to boost how existing weapon systems connect and can operate in greater harmony, which can generate a hugely positive effect in warfare situations without changing the weapon systems themselves.

In contrast, generative AI uses underlying patterns and structures of training-data to generate new content and does not intend to change the overall architecture of existing military components. It can therefore create new content and provide a commander with new services. Examples can be automated invoice orders and the distribution of artillery shellsbased on generative AI-models prognosing mission demands, or a push of amended battlefield plans based on a real-time, automated intelligence analysis. In this case, AI is a *disruptive technology* (see visualization figure 3), as it has the potential to create whole new systems or unlock new services.

5 White Paper for European Defence – Readiness 2030 | EEAS

6 https://www.researchgate.net/publication/200465578_Architectural_Innovation_The_Reconfiguration_of_Existing_Product_Technologies_and_the_Failure_of_Established_Firms

7 https://www.researchgate.net/publication/200465578_Architectural_Innovation_The_Reconfiguration_of_Existing_Product_Technologies_and_the_Failure_of_Established_Firms

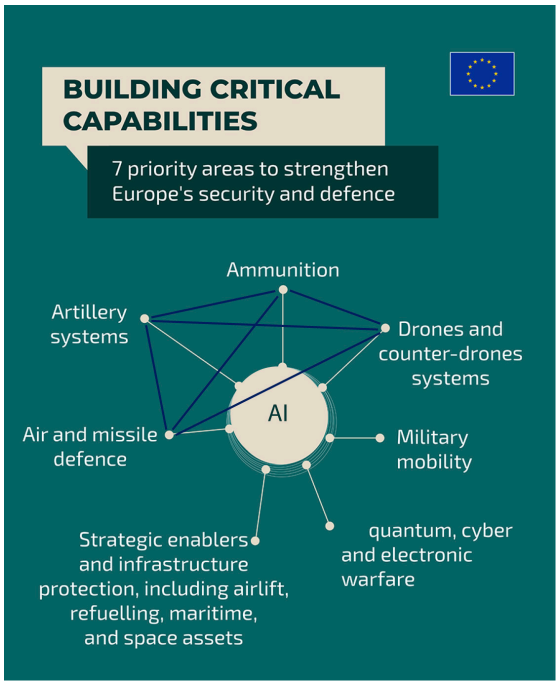

Figure 2 "AI as a disruptive effect, integrating existing components components by changing the overall architecture"

Figure 3 "AI as a disruptive technology, creating new components and unlocking new AI-services"

Therefore, viewing AI as either a *disruptive technology* or a *disruptive effect* will result in a different relative positioning of AI when rebuilding military capabilities. Using two contemporary examples, the question then is to what extent the powers of AI are currently harnessed as either a *disruptive effect or a disruptive technology*?

Ukraine and China: AI as disruptive effect or disruptive technology?

Disruptive Effects

The war in Ukraine shows that AI already has a profound impact in warfighting, particularly when it comes to the deployment of drones. 'The Ukrainian defense industry is pursuing an approach of training small AI models on small datasets'[8] for specific equipment, such as drones. This is supplemented with Ukraine's unique DELTA communication system, which 'is the largest Ukrainian integration platform and national data lake that operates in the cloud'[9].

In this application, the components of the drone, such as rotors, batteries, airframes, sensors or added weaponry, have altered only incrementally and continue to rely on the same working principles. Still, the simple, small AI-models combined with a cloud-based network have resulted in a different architecture, allowing for fast and seamless integration of the different components, such as sensors, operator controls, command and control systems. The result is a profoundly shortened sensor-to-shooter-time. Pre-2022 , identifying and engaging a newly identified target took Ukrainian armed forces between 12 and 48 hours. Currently, that timeframe has been reduced to 3 to 15 minutes.

In the Ukrainian case, by using the idea of Architectural Innovation, AI is not a *disruptive technology*, but instead has a *disruptive effect* on military operations.

8 Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare

9 Battlefield Innovation: Ukraine's DELTA System Paves the Way for Allied Interoperability at CWIX24 - NATO's ACT

Disruptive technologies

Both Ukraine and China invest in small AI models changing the existing architecture, aimed to shorten the sensor-to-shooter-time. However, China also explores using Large Language Models (LLMs), potentially allowing for the creation of entirely new, generative services. By using big data, among others, China seeks to provide a 'virtual assistant interface to provide intelligent interaction and task-planning' [10]with existing command information systems, which accelerates decision-making speed and quality. A military commander will be provided with near-real-time, automatically generated, operational or tactical military templates. This should even allow commanders to conduct near-real time psychological operations, thereby unlocking the possibility to quickly and deliberately engage an adversary in the cognitive domain to degrade its will to fight.

Looking at China's military AI strategy, the algorithms directing the Large Language models are therefore in fact the new components, generating new content. AI in this application is not aimed at merely altering the interaction of existing components but are designed to unlock new services. In contrast to Ukraine, China actively seeks to pursue an AI-strategy involving AI both as a *disruptive effect* and as *disruptive technology*.

Revisiting Rearm Europe's 2030 AI-strategy

This alert shows that military AI can both create *disruptive effects* and can be a genuine *disruptive technology*. Ukraine's drone-warfare demonstrates that AI already creates a disruptive effect. China on the other hand, is also developing a strategy to introduce generative AI as a military disruptive technology to provide completely new services, improving on and accelerating military decision-making.

Unfortunately, even when Rearm Europe's effort to simplify regulations will lead to successful procurement of military equipment, much equipment will nevertheless enter service *after* 2030. Based on the intelligence estimates of the Dutch Military Intelligence Agency (MIVD) on Russian aggression, this might be too late. Set against this timeframe, merely procuring more equipment will not increase our military capabilities in event of a Russian attack.

After 2030, as a longer-term AI-strategy, generative AI can be used as a *disruptive technology*. A sound, shorter-term AI-strategy, however, would be to focus on AI as a *disruptive effect*. Changing the overall architecture of existing military equipment will greatly improve the effectiveness of our current and near-future military arsenal. Differences in military conceptual, technological and organizational interoperability will have to be bridged if Europe wants to implement such an AI-strategy.

Ukraine has successfully achieved interoperability and integrated Soviet-era equipment with Western ones. It took an existential war to incentivise a push towards interoperability. If we truly want to rearm Europe, entities such as the European Defence Agency (EDA) should play a role in both the coordination of interoperability issues and the successful implementation of AI as a disruptive effect. Individual defence contractors cannot be expected to resolve these issues independently by just deepening the defence market. Outside coordination is crucial with just little time left on our hands.

10 New products show China's quest to automate battle - Defense One

About the Clingendael Institute
Clingendael – the Netherlands Institute of International Relations – is a leading think tank and academy on international affairs. Through our analyses, training and public debate we aim to inspire and equip governments, businesses, and civil society in order to contribute to a secure, sustainable and just world.

www.clingendael.org
info@clingendael.org
+31 70 324 53 84

@clingendaelorg
The Clingendael Institute
The Clingendael Institute
clingendael_institute
Clingendael Institute
Newsletter

About the author

Erik Stijnman is an Army Lieutenant Colonel in active Dutch Service and has been seconded to Clingendael as Senior Research Fellow with Clingendael's Security Unit. He focusses on security-related topics with a geographical focus on Russia and Ukraine and with a thematical focus on Combat and Peacekeeping Operations, Intelligence, Decision-making and Military Innovation and Adaptation and the use of Artificial Intelligence.