Pathways for Integration of Artificial Intelligence in the Defence Sector: A Comparative Study

Working Paper Series SOG-WP4/2024

Author: Domiziano Cristiani, Federico Deiana, Francesco Meriano May 2024

LUISS



Table of Contents

Abstract			3
1.	Intr	oduction	4
2.	Patl	hways for Integration of Artificial Intelligence in the Defence Sector	6
	2.1	The United States	6
	2.2	China	
	2.3	Russia	12
	2.4	Israel	15
3.	Con	nclusion	19

Abstract

The ever-faster spread of AI-powered technology opens new perspectives on the military applications of Artificial Intelligence. AI could revolutionise warfare by enhancing military technology in areas as diverse as geolocation and satellite imagery, strategic decision-making, logistics, cybersecurity, and autonomous and semi-autonomous systems. The main state players have already integrated – and continue to integrate – AI within their military apparatus, following integration models that often differ from case to case. In particular, an overview of the cases of the United States, China, Russia, and Israel reveals substantial differences in proceeding along this pathway, mainly because of the heterogeneity of the issues (ethics, threat structure, organization of armed forces, etc.). The purpose of this paper is to examine whether there are convergence points within these models, but above all, it tries to understand if they are really functional to the single player within a competitive context and therefore if they manage to provide a strategic advantage in the geopolitical competition.

Keywords: AI-powered Military Technology, Strategic Decision-Making, Geopolitical Competition

1. Introduction

Across the last decade, exponential progress in computational and storage capacities favoured the development of artificial systems that could simulate cognitive functions by elaborating ever-vaster datasets. The cross-cutting use of Artificial Intelligence (AI) in healthcare, logistics, entrepreneurship, finance, security, and defence has quickly become a key element of geopolitical developments. AI development drives the global competition for hegemony between the U.S. and China, while middle powers look at its asymmetric potential as a potential game-changer for their international positioning. Against the backdrop of the Sino-American confrontation, AI has become a crucial multiplier for the strategic scope of State actors.

The defence sector is no exception. Military integration of AI envisages transversal applications in geolocation, logistics, intelligence, autonomous and semiautonomous systems, and strategic decision-making. The upgrade of military hardware runs parallel to developing data analysis software to enhance command-and-control activities and produce realistic scenarios at reduced time and costs. Beyond practical issues, AI could also lead to significant changes in military balances and strategic thinking.

At the same time, the tendency to develop AI models in open innovation ecosystems – combined with the dual-use nature of several applications – blurs the line between civil society and the State security apparatus. Consequently, the analysis of AI military integration cannot overlook the political, institutional, and corporative framework in which national competitors operate. Depending on the orientation of decision-makers, overseeing the military integration of AI will entail striking a balance between technological sovereignty and State openness to international research and development (R&D) networks.

The research and implementation of AI technologies respond to the strategic interests of state actors, in a markedly shifting geopolitical landscape. The increase in international tensions and the deterioration of security in numerous regional contexts sharpens the actors' interest in developing strategies to restructure and modernize their armed forces. The current conflicts in eastern Ukraine and the Gaza Strip registered the germinal use of AI systems alongside conventional military means and tactics. Conflict scenarios represent potential incubators for the development and testing of AI-powered military applications. Moreover, geopolitical contingencies directly influence strategic priorities, public resource allocation and the orientation of national supply chains.

Building upon such considerations, the article aims to outline a comparative overview of the main pathways for the military integration of AI. To do so, it analyses the approaches taken by four players who have registered significant progress in the scramble for AI – namely the U.S., China, Russia, and Israel. Integration models were built through the cross-sectoral analysis of policy documents; finance laws and

available data on military transactions; the structural characteristics of R&D ecosystems; institutional and ethical frameworks; and geostrategic constraints informing the action of State actors.

On such a basis, the final section identifies points of divergence and traits d'union of these four pathways to the military integration of AI. While the fast pace of technological progress may limit the applicability of results to a given point in time, such results may still prove useful to develop an evolutive understanding of military integration strategies in the "age of AI".

2. Pathways for Integration of Artificial Intelligence in the Defence Sector

2.1 The United States

The United States remains the main forerunner for AI integration in the defence sector. The increasing hybridization of warfare and the proliferation of military automation systems, however, outline the erosion of the competitive advantage that the United States gained at the end of the Cold War.

The use of autonomous systems within the U.S. military equipment – strictly speaking, precursors to the integration of AI technologies – dates back to the early 1980s.¹ In this context, the case of the Aegis Ballistic Missile Defence System – an automated defensive system that allowed an operator to respond to immediate threats by alternating or combining a series of "doctrines" labelled as "Semi-Auto," "Auto SM," and "Auto-Special" – is emblematic. The first two were semi-autonomous with a "man in the loop" configuration, while the third provided solely human supervision of the activity cycle ("man on the loop") and was activated when the operator believed he could no longer handle the threat. Switching between these configurations was surprisingly easy by the standards of that period.²

Two programs promoted by the Defence Advanced Research Projects Agency (DARPA) in the 1990s in the field of planning and logistics also aroused significant interest. The first was the Joint Assistant for Deployment and Execution (JADE), which focused solely on planning the movements of units, primarily airborne, in conventional conflicts. The more challenging Survival Adaptive Planning Experiment (SAPE) generated actual war plans for nuclear conflicts. However, this experiment abruptly ended with the conclusion of the Cold War, as the threat posed by the existence of the Soviet Union was the rationale behind its implementation. With the collapse of the USSR, the U.S. establishment assessed that the risks of potential errors in nuclear planning systems outweighed the potential benefits deriving from the project.³

Recent U.S. history is not unfamiliar with such assessments. Many programs – some particularly disruptive and cutting-edge – have been interrupted prematurely or have not translated into operational plans. The case of the Northrop Grumman X-47B, whose program was initially cancelled by the U.S. Navy, is an example: this remotely piloted aircraft owned by the U.S. Navy successfully conducted the first unmanned take-off and landing on an aircraft carrier⁴ as well as the first in-flight refueling, respectively in 2013 and 2015.⁵

- ³ Ibid., pp. 51-52.
- "The USS George H. W. Bush.

¹ Work, R.O. e Brimley, S., 20YY: Preparing for War in the Robotic Age, pp. 31-36, Center for a New American Security, 2014.

² Morgan, F.E. et al., *Military Applications of Artificial Intelligence. Ethical Concerns in an Uncertain World*, p. 49, RAND Corporation, 2020.

⁵ Ibid., p. 50.

Caution in the development of autonomous systems influences the U.S. approach to the evolution of AI military technologies and reflects both the widespread worries about errors and incidents – often fatal due to the very nature of the activities and particularly frequent over the past 20 years – and the national leadership's concerns for operational and ethical issues.

U.S. primacy cannot, therefore, be considered an immutable **status quo**, especially considering how other state actors, unencumbered by the procedural constraints of democratic systems, manoeuvre with extreme ease in AI technology procurement and military integration.

While the United States remains a global leader in private investments in AI, the public sector plays a crucial role in supporting its military application. The government is the leading national funder for basic research (41%), while approximately 40-60% of the federal budget for R&D is typically allocated to the defence sector. Notably, the "AI Next" campaign launched by DARPA in 2018 alone provided for the allocation of over 2 billion dollars in funding to initiate new R&D programs and complete the existing ones.⁶

Specifically, the program consisted of five functional pillars aimed at addressing the key needs of the Department of Defence (DoD). Firstly, the program aimed to expand the DoD's operational reach by increasing its capabilities and advancing AI technologies to enable the automation of critical business processes. Secondly, DARPA sought to achieve "robust" and resilient AI, addressing errors that could compromise in particular tactical operations. Another pillar of AI Next focused on Adversarial AI – a specific area of intervention where the goal was to consolidate the effectiveness of machine learning (ML) tools by minimizing the impact of biased input modifications. Staying within the domain of machine learning, DARPA had the objective of enhancing the efficiency of ML systems, both quantitatively and qualitatively, reducing the related energy consumption and increasing data processing speed. Lastly, the Next Generation AI pillar aimed to develop next-generation AI algorithms so that these could evolve from mere tools to problem-solving partners with advanced capabilities.⁷

When considering ML systems, it is impossible not to highlight the key AI project carried out by the DoD: the Algorithmic Warfare Cross-Functional Team (AWCFT). The AWCFT project, known as "Project Maven," fits within the perimeter of logistics and planning activities and was launched by the U.S. Department of Defence in 2017 with the goal of "accelerating the integration of big data and Machine Learning in the Department of Defence",⁸ in full compliance to the AI Next campaign guidelines. On a strictly technical level, Maven focuses on using computer vision software for automated analysis of images and videos collected during Intelligence, Surveillance, Target Acquisition, and Reconnaissance (ISTAR) operations. The amount of data acquired by drones often goes well beyond the threshold of material that can be analysed by humans, and, in addition, the algorithm is able to filter and sort it in a timely manner, according to pre-established priorities. The results were surprising: project Maven's successes led to its deployment in counter-IS operations just six months after its launch.

The speed of the AWCFT's deployment seems to confirm the theory that the U.S. establishment prioritizes AI projects with software-driven applications over the development of autonomous weapons systems.⁹

⁶ Currently, there are about 30 DARPA-funded programmes, in addition to hundreds of initiatives from the US academic environment.

⁷ Al Next Campaign (Archived), Defence Advanced Research Projects Agency.

⁸ <u>Il Pentagono si farà aiutare dall'intelligenza artificiale di Google</u>, AGI, 8th March 2018.

⁹ Morgan 2020, p. 55

However, Maven experienced a significant setback during its initial phase when Google employees, who were actively involved in the initiative, expressed their dissent towards their company's decision to contribute to the war industry. The Mountain View company thus decided to interrupt the activities with the Department of Defence for this project.

Upon closer examination, employees of the U.S. tech giant raised an ethical issue regarding "trust" in the use of AI technologies for military purposes. The U.S. leadership has placed this issue at the core of recent strategies for implementing AI in the defence sector. The concept of "trust," indeed, is a key part of the latest DARPA's initiative, called "AI Forward". This initiative shifts the focus of AI technology development towards ethical considerations and consists of three pillars: the Foundational Theory which aims to draft clear guidelines for the use of AI in the domain of national security; AI Engineering which aims to create technologies that work as intended in the real world, and not just in controlled laboratory settings; Human-AI Teaming which focuses on enabling new systems to act as effective, intelligent, and reliable partners for operators with different backgrounds.¹⁰ The Human-AI teaming pillar exemplifies the current trend of U.S. decision-makers. While initially, with the development of increasingly sophisticated technologies, the aspiration was to replace (almost entirely) human activities, there is now a tendency, following the occurrence of previously not adequately considered ethical issues, towards a scenario where humans and technology collaborate, leveraging each other's strengths.

The debate around Lethal Autonomous Weapon Systems (LAWS) has been highly contentious. These systems are weapons that use sensors and computer algorithms to independently identify a target and use an on-board system to engage and destroy it without direct human control. As previously discussed, so far the United States has not heavily invested in autonomous weapon systems, partly due to a preference for integrating AI in defensive rather than purely offensive applications. U.S. laws do not explicitly prohibit the development and use of these systems but require "commanders and operators to be capable of exercising appropriate levels of human judgment regarding the use of force".¹¹ This directive from the Department of Defence, which may initially seem to rule out the use of LAWS as "man out of the loop" systems, leaves two essential questions open. Firstly, the term "appropriate levels" is not clearly defined. The concept of "appropriateness" can vary depending on the specific weapon system, operational context, or type of conflict. Secondly, "human judgment regarding the use of force" does not necessarily imply manual control of each individual device but rather suggests a broader and unspecified human involvement that may occur before its use.¹² As this topic remains highly relevant, the Congress is expected to address the remaining issues in a reasonably timely manner.

The aforementioned directive imposes a fairly clear limit on the use of AI in autonomous or semiautonomous systems, requiring compliance with the DoD AI Ethical Principles¹³, which can be found in the Responsible Artificial Intelligence (RAI) Strategy and Implementation Pathway, released by the Department of Defence in June 2022. These principles are the basis of the six tenets driving the integration of AI into the US military system.

The tenets correspond to specific areas of intervention: RAI Governance, Warfighter Trust, AI Product and Acquisition Lifecycle, Requirements Validation, Responsible AI Ecosystem and AI Workforce. Specifically,

¹⁰ Al Forward, Defence Advanced Research Projects Agency.

¹¹ U.S. Department of Defence Directive (DODD) 3000.09, November 2012 (update January 2023).

¹² Sayler, K. M., Defence Primer: U.S. Policy on Lethal Autonomous Weapon Systems, "In Focus", Congressional Research Service, update 1st February 2024.

¹³ DOD Adopts Ethical Principles for Artificial Intelligence, U.S. Department of Defence, 24th February 2020.

the document requires ensuring constant DoD oversight of the use of AI through cutting-edge governance structures and processes; providing operators with a standard level of familiarity and mastery of the systems; paying appropriate attention to the cycle of acquisition and use of AI technologies in order to mitigate the risks; undertaking a requirements validation process to ensure that capabilities leveraging AI are aligned with operational needs; promoting a common understanding of all phases of AI integration – i.e. design, development, deployment and use –; and ensuring that all Department staff members involved in activities related to the use of AI have adequately understood its functionality, risks, potential developments and operational methodologies.¹⁴

The ultimate goal of the Pathway is to cultivate among operators at all levels – and among U.S. citizens – the previously mentioned widespread sense of "trust". The concept of "trustworthiness" represents the "desired end state" of military integration of AI technologies, achieved through a meticulous process of risk assessment and risk management and through collaboration among democratic state actors.¹⁵

Furthermore, Responsible Artificial Intelligence serves as the cornerstone of the Data, Analytics, and Artificial Intelligence Adoption Strategy published by the DoD in 2023, providing insights into the U.S. trajectory of AI adoption. Developed by the Chief Digital and AI Office (CDAO), the strategy defines the approach to strengthening command-and-control chains in order to make them swift and well-supported by high-quality data, advanced analytics, and AI algorithms, providing a "lasting decision advantage". This advantage is characterized by a competitive condition marked by knowledge and deep understanding of the battlefield, agile and adaptive force planning and application, rapid and precise kill chains, resilient operational support, and efficient supply chains.¹⁶

To ensure this decision-making advantage, the Department of Defence has adopted an "agile approach" whereby authority is distributed throughout the entire chain of command, through a process of resource decentralization. The goal is to provide as much leeway as possible in decentralizing the creation, storage and management of AI assets, data and analytics. Obviously, the resulting infrastructure cannot be completely decentralized since some key decisions and technologies, due to their critical nature, must remain under the direct control of the Department.¹⁷

The 2023 Data, Analytics, and Artificial Intelligence Adoption Strategy builds upon two additional documents released by the DoD: the 2018 Artificial Intelligence Strategy and the 2020 Data Strategy. The first emphasized the need to build a decentralized infrastructure for AI development, cooperate with allies and commercial and academic partners, and exercise international leadership in AI military ethics.¹⁸ The second document significantly shifted the Department's focus towards data, aiming to use data to support activities and ensure greater operational efficiency. It also placed data management within the framework of the VAULTIS objectives – therefore aiming to make data increasingly visible, accessible, understandable, linked, trustworthy, interoperable, and secure.¹⁹ The 2023 Strategy builds upon these two

¹⁴ <u>Responsible Artificial Intelligence Strategy and Implementation Pathway</u>, U.S. Department of Defence, June 2022.

¹⁵ Ibid.

Nevertheless, it is still discussed among academia the way trust in institutions and their use of Al tools is produced. Cfr. Floridi, L., Cowls, J., King, T. C., Taddeo, M., *How to design Al for social good: Seven essential factors* in "Ethics, Governance, and Policies in Artificial Intelligence", pp. 125-151, Springer, 2021.

¹⁶ Data, Analytics, and Artificial Intelligence Adoption Strategy. Accelerating Decision Advantage, pp. 5-6, U.S. Department of Defence, 2023.

¹⁷ Ibid., p. 10.

¹⁸ Summary of the 2018 Department of Defence Artificial Intelligence Strategy. Harnessing AI to Advance Our Security and Prosperity, U.S. Department of Defence, 2019.

¹⁹ **DoD Data Strategy**, U.S. Department of Defence, 2020

previous documents and guides the DoD's activities related to data, analytics, and AI adoption towards an "AI hierarchy of needs."

This "hierarchy" is an ideal pyramid that envisions, at its base, the collection of high-quality data. The second level consists of in-depth analysis and metrics, including analytical models which are necessary for DoD operators to better understand the key variables that influence outputs in their areas of interest. At the top of the pyramid lies Responsible Artificial Intelligence, which includes the four-phase integration of AI – design, development, deployment, and use – consistently with the Department's ethical principles.²⁰

2.2 China

The People's Republic of China (PRC) considers AI as a key element in achieving global primacy. According to the 2017 strategic document "New Generation Artificial Intelligence Development Plan", Beijing intends to use AI to cement its status as a scientific and technological powerhouse, with equal implications for the civil and military spheres.²¹ Over the last decade, the Chinese establishment has invested significant resources in AI research and implementation, recruiting experts in the field and creating dedicated public-private coordination centres.²² The goal is to "overtake the West in Artificial Intelligence R&D by 2025" and "become the world leader in AI by 2030".²³

In the framework just described, the security and defence sectors play a key role. Internally, AI is used in the development of software for population monitoring or ostensibly control of ethnic and religious minorities. On the external front instead, AI is conceived as a force multiplier, necessary to address existing gaps in the military apparatus. To this end, the strategy involves the cross-sectional integration of civil and military development objectives through coordinated investments in the R&D sector. This concept, known as the Military-Civil Fusion Strategy (MCF), envisages more ambitious goals compared to *ad hoc* procurement policies in the civil sector.²⁴

In this regard, the Chinese strategy is articulated in three phases (*Mechanization – Informatization – Intelligentization*), aimed at comprehensively modernizing the Armed Forces by 2035 and developing a "world-class military" by mid-century.²⁵

Initiated in the 1980s and declared concluded in 2020, the **Mechanization** phase was characterized by the need to equip, with modern devices and platforms, a large but technologically backward military apparatus. The current phase of **Informatization** began in the 1990s and is expected to end in 2027. The latter involves integrating hardware tools with sensors and software to improve capabilities and expand operational use. Al takes over during phase three: first mentioned in 2015 and further elaborated in the 2019 Defence White Paper, **Intelligentization** involves the integration into the mechanized and

²⁰ Data, Analytics, and Artificial Intelligence Adoption Strategy. Accelerating Decision Advantage, p. 7, U.S. Department of Defence, 2023.

²¹ Webster, G. et al., *Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)*, Stanford University, 2017; Kania, E., *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*, Center for a New American Security, 2017; Kania, E., *Chinese Military Innovation in Artificial Intelligence*, Center for a New American Security, 2017; Kania, E., *Chinese Military Innovation in Artificial Intelligence*, Center for a New American Security, "Testimony before the US Senate U.S.-China Economic and Security Review Commission at the Hearing on Trade, Technology, and Military-Civil Fusion", 7th of June 2019.

²² Peterson, D., Luong, N., Feldgoise, J., Assessing China's Al Workforce: Regional, Military, and Surveillance Geographic Job Clusters, Center for Security and Emerging Technology, 2023.

²³ Military and Security Developments Involving the People's Republic of China, US Department of Defence, 2023.

²⁴ Kania, E. e Laskai, L., *Myths and Realities of China's Military-Civil Fusion Strategy*, Center for a New American Security, 2021.

²⁵ Dossi, S., La Modernizzazione delle Forze Armate cinesi, in AA.VV. Andornino, G., Cina: prospettive di un paese in trasformazione, 11 Mulino, 2021.

informatized military apparatus of intelligent and autonomous systems based on artificial intelligence, in order to improve the effectiveness of current tactics and tools (both hardware and software) and achieve entirely new capabilities.²⁶

The operational integration of AI within the People's Liberation Army reflects the broader restructuring of China's strategic thinking around the concept of System Warfare. Given the proliferation of high-precision and lethal weaponry that makes it challenging to defeat a technologically advanced adversary using conventional means, Chinese doctrine aims to disrupt or inhibit the system guiding the adversary's actions. Consequently, the ultimate objective is to structurally compromise the opponent rather than defeat it on the field.²⁷ In the context of systemic confrontation, the cross-sectional use of AI should enhance the superiority of the military apparatus by optimizing interoperability and response speed, processing large quantities of data, connecting geographically distant units, and harmonizing multiple combat domains.²⁸

However, the specific methods and timelines for realizing this process remain unclear. Recent academic literature focuses on the modernization process in general terms, and even official proclamations do not provide clearly defined integrative practices. Therefore, efforts have been made to reconstruct the Chinese integration path through the analysis of military procurement data, collected from independent sources.

The major investments in this regard seem to be concentrated in the areas of ISTAR sensors, Cyber, Electronic Warfare, Decision Support Systems (DSS), Logistics, Predictive Maintenance, and Robotics, although – with respect to the latter area – doubts remain about the level of autonomy integrated into the different devices.²⁹ For example, regarding the development of LAWS and Swarm Drones of Chinese production, a considerable part of the academia suggests that these are not yet fully autonomous devices, but rather human operators continue to exercise a considerable control.³⁰ This choice would be a deliberate instruction by the Communist Party to maintain control over the various components of the military apparatus. It's noteworthy, however, that the degree of autonomy of such AI-driven systems can be modified **ex post**, potentially reaching the complete exclusion of human intervention (no man in the loop). Yet, for the moment, it seems that the path decided by the PRC is different. The pervasiveness of the Party's control over the armed forces is reflected in the relatively lower emphasis on AI in the command-and-control activities.

From what has been discussed, it appears that China has a greater inclination to exploit AI in "soft activities", which involve enhancing monitoring, data collection and analysis capabilities, cyber activities,

²⁸ Fedasiuk, R., Chinese Perspectives on Al and Future Military Capabilities, Center for Security and Emerging Technology, 2020; Morgan, 2020.

²⁶ Stokes, J., Sullivan, A., Greene, N., U.S.-China Competition and Military AI: How Washington Can Manage Strategic Risks amid Rivalry with Beijing, Center for a New American Security, 2023; Pollpeter, K. e Kerrigan, A., The PLA and Intelligent Warfare: A Preliminary Analysis, CNA Corporation, 2021.

²⁷ Cozad, M. et al., Gaining Victory in Systems Warfare. China's Perspective on the U.S.-China Military Balance, RAND Corporation, 2023; Engstrom, J., Systems Confrontation and System Destruction Warfare. How the Chinese People's Liberation Army Seeks to Wage Modern Warfare, RAND Corporation, 2018.

²⁹ Konaev, M. et al., U.S. and Chinese Military AI Purchases, An Assessment of Military Procurement Data between April and November 2020, Center for Security and Emerging Technology, 2023; Fedasiuk, R., Melot, J., Murphy, B., Harnessed Lightning, How the Chinese Military is adopting Artificial Intelligence, Center for Security and Emerging Technology, 2021.

³⁰ Stokes, J., *Military Artificial Intelligence, the People's Liberation Army, and U.S.-China Strategic Competition*, Center for a New American Security, "Testimony before the US Senate U.S.-China Economic and Security Review Commission at the hearing 'Current and Emerging Technologies in U.S.-China Economic and National Security Competition'', 1st February 2024; Beauchamp-Mustafaga, N., *Exploring the Implications of Generative AI for Chinese Military Cyber-Enabled Influence Operations*, RAND Corporation, "Testimony before the US Senate U.S.-China Economic and Security Review Commission at the hearing 'Current and Emerging Technologies in U.S.-China Economic and National Security Competition'', 1st February 2024; Beauchamp-Mustafaga, N., *Exploring the Implications of Generative AI for Chinese Military Cyber-Enabled Influence Operations*, RAND Corporation, "Testimony before the US Senate U.S.-China Economic and Security Review Commission at the hearing 'Current and Emerging Technologies in U.S.-China Economic and National Security Competition'', 1st February 2024.

cognitive domain operations, and decision-making support for operators. Conversely, some resistance remains towards fully relying on AI for matters of strategic importance.³¹

In this context, AI is currently perceived as a perfect tool at the tactical and operational levels, capable of improving effectiveness and efficiency on the field. Meanwhile, where a broader level of decision-making is necessary, human operators remain fundamental. This is particularly evident in the case of nuclear weapons. Nevertheless, it cannot be excluded that the current situation may change in the near future, especially if the advantages of automatization provide Beijing with a higher degree of success or reliability in warfare.

2.3 Russia

Trailing the wake of US-Chinese competition, the Russian Federation is emerging as a notable outsider in the global scramble for AI. Relying upon the legacy of the Soviet military industry, Russia looks at artificial intelligence as a potential disruptor to bridge the growing technological gap **vis-à-vis** the West. On the other hand, the spread of AI-enhanced military technology threatens to erode the advantages of Russia's extensive production of conventional arms and must therefore be mastered to avoid lapsing into obsolescence. This was the gist of Vladimir Putin's oft-cited 2017 televised address, according to which "Whoever becomes the leader in this sphere will become the ruler of the world".³²

Russia's pursuit of AI is thus shaped first and foremost by hard security concerns. Moscow's research and development strategy adopts a top-down, State-led focus on the military industry with added incentives for civilian enterprises to cooperate with the defence sector. The focus on military applications as opposed to general-purpose AI is prompted by both the traditional influence of the military and the pressing issue of hostilities in Ukraine, where AI could be employed to enhance automation and reduce battlefield losses. As the war enters its third year and frontlines become entrenched, AI might also improve command-and-control capabilities to reduce attrition and improve the allocation of resources.

Consequently, while State policy documents envision a variety of ambitious applications that include communications, high-precision and nuclear weapons, electronic warfare, space-based systems, logistics and manufacture, actual plans for integrating AI into the Russian armed forces seem to have focused mainly on developing autonomous aerial and ground robotics to conduct mapping, reconnaissance, demining and combat support. Urad-6 and Urad-9 UGVs – used respectively for demining operations and as an anti-tank platform – were reportedly tested during Russia's campaign in Syria.³³ The much-touted Marker platform, which possesses anti-tank payloads and can operate drone swarms for reconnaissance and protection against enemy UAVs, reportedly employs neural network technology to identify enemy targets by comparing feedback from drones and satellite imagery.³⁴ The Lancet-3 loitering munition system, according to combat footage registered in Ukraine, also possesses object recognition capabilities. Similar allegations concern KUB-LA kamikaze drones as well as several others of the uncrewed vehicles produced by Russia in the last five years.³⁵

³³ Morgan 2020.

³¹ Kania, E., "AI Weapons" in China's Military Innovation, Brookings Institution, 2020;

³² Путин: лидер по созданию искусственного интеллекта станет властелином мира, TASS Russian News Agency, 1st September 2017.

³⁴ Bendett, S., *The State of Autonomy, AI & Robotics for Russia's Ground Vehicles*, European Security and Defence 2023.

³⁵ Zysk, K., **Struggling, Not Crumbling: Russian Defence AI in a Time of War**, Royal United Service Institute, 2023.

Another priority focus concerns the development of AI-powered data analysis and decision support systems, accounting for respectively 33% and 16,5% of the 2020 R&D budget.³⁶ Known projects in the area highlight a drive towards enhancing command-and-control operations as well as improving the performance of defensive systems. Russia's new Afghanit APS – the ideal descendant of the first 1979 Drozd Soviet model – is reportedly able to identify up to 40 ground targets and 35 aerial targets.³⁷ Moreover, AI could bolster Russia's extensive A2D2 system through platform integration. Several reports indicate that Russia is currently working on an automated control system meant to unify S-300 and -400 missile batteries, as well as the Pantsir anti-aircraft emplacements, under a single domain.³⁸

It is unclear, however, to what degree modern Russian systems possess true learning capacity or merely high-level autonomy. Much like in the U.S., Russian semiautonomous weapon systems date back to the Cold War. While such systems can choose between preselected courses of action, they cannot elaborate or compare data to evaluate a given situation. In the case of the Marker – four of which were deployed in Ukraine as of February 2023 – more information would be needed on the role of its remote human operators to gauge the degree of intellectualization reached by the platform. While the head of the Russian Ministry of Defence's AI Directorate, Vasily Yelistratov, stated in 2022 that AI as a cross-cutting technology was "present in all weapons, especially high-precision ones and ground-, air-, and sea-based weapons systems", ³⁹ its actual integration in the Russian armed forces seems to follow a slower pace compared to U.S., Chinese or Israeli counterparts. With the notable exceptions of drones, UVs have been employed to a relatively limited extent in the Ukraine theatre, while the Urad-9's performance in Syria was deemed unsatisfying.⁴⁰ Moreover, the analysis of downed or captured Lancet-3 UAVs has revealed that their image processing capabilities are powered by a NVIDIA Jetson module of Western production, highlighting the relative disadvantage of Russian industry in the field and raising questions as to Russian ability to circumvent Western-imposed supply chain constraints.⁴¹

In keeping with Soviet inclinations, Russia favours a State-dominant approach over private innovation models. In 2018, 67% of R&D financing came from the federal budget, while in China and the U.S. private initiatives accounted for 79% and 77% of total investment.⁴² Commercial, academic, and industrial cooperation ultimately fall under the purview of the Russian Ministry of Defence, which opened its AI Directorate in April 2022 and manages roughly 1200 partnerships with universities, financial institutions, governmental entities, and research centres.⁴³ Mirroring U.S. and Israeli initiatives, Russia also launched a series of State-sponsored technology parks – chief among them the 2018 ERA and the Skolkovo centres – which aim to foster public-private sector partnerships. Still, pervasive State control usually blurs the line between public and private initiatives. Major corporate investors – such as Sberbank, Yandex, Gazpromneft and VKontakte – are either majority State-owned or directed by close associates of the Russian political leadership. Sberbank, which has been entrusted with the drafting of State AI policy

³⁶ Ibid.

³⁷ Morgan 2020.

³⁸ Ibid., p.86.

³⁹ Russian defence ministry introducing AI technologies in army, TASS Russian News Agency, 25th August 2022.

⁴⁰ Brown, D., *Russia's Uran-9 robot tank reportedly performed horribly in Syria*, Business Insider, 9th July 2018.

⁴¹ Faragasso, S., <u>Russian Lancet-3 Kamikaze Drone Filled with Foreign Parts: Western Parts Enable Russian Lancet-3 Drone to Have Advanced Targeting and Anti-jamming</u>

<u>Capabilities</u>, Institute for Science and International Security, 18th December 2023.

⁴² Zysk, K., <u>High Hopes Amid Hard Realities: Defence AI in Russia</u>, Defence AI Observatory 2023.

⁴³ Zysk 2023(a).

documents and is attempting conversion into a fully-fledged technology company, is controlled through a 50%+1 stake acquired by the Russian government in 2020.⁴⁴

Meant to favour power concentration and technological protectionism, such arrangements may also translate into weaker integration in international networks, lower levels of direct investment and ultimately smaller data pools. Within the R&D ecosystem, the problem is reflected in the long-standing issues of brain drain, an ageing workforce and the deteriorating performance of Russian universities and research centres in the production of AI-related papers and patents.⁴⁵ Within this context, the war in Ukraine channels priority investments into the military sector, but also increases inflationary pressures and may divert resources to replenish battlefield losses in equipment and machines, to the detriment of production and research.

Available policy documents suggest a tendency towards the latter option. In November 2023, the Russian State Duma approved a budget law allocating roughly 29% of federal State funding to national defence for 2024, for an estimated 10,700 billion rubles. Within this sum, 324.966 million roubles are allocated to overall research and development for military technology.⁴⁶ By contrast, Prime Minister Mikhail Mishustin announced in September that Russia would allocate 5,2 billion rubles (about 500 million euros) to the development of AI technologies in 2024.⁴⁷ Likewise, the current national AI strategy, which was published in December 2022, cut spending estimates on AI to approximately 346 million euros, as compared to the 800 million recommended by the 2019 Sberbank-drafted roadmap.⁴⁸ It should be kept in mind, however, that much of the federal budget is classified, a tendency which has grown more pervasive with the 2024-7 iteration. Moreover, the last two years of the budget plan usually tend to be provisional in nature and subject to the high discretional power of the Russian authorities. As such, figures related to AI spending might not mirror the government's full commitment to AI development.

A final variable influencing the effectiveness and pace of AI integration in the Russian armed forces pertains to cooperation with China. Chinese President Xi Jinping's announcement of an "unlimited partnership" with Russia, aired on the occasion of Putin's visit to Beijing days before the invasion of Ukraine, came on the backdrop of a decade of deepening political, economic, and military ties between Russia and the People's Republic. Joint high-level consultations and military exercises have intensified since the start of Russian 2014 operations in Crimea and the subsequent deterioration of Moscow's relations with the West, which has forced Russia to reorient its procurement strategy towards its Chinese neighbour. Consequently, Russian imports of Chinese electronics and semiconductors key to AI R&D have surged since the outbreak of hostilities in mainland Ukraine.⁴⁹ Under this view, Sino-Russian cooperation also benefits from strategic alignment upon Moscow and Beijing's mutual anti-NATO stance.

The last years have consequently seen the expansion of multidimensional Sino-Russian partnerships, including in the field of artificial intelligence. At the close of a Beijing summit held in February 2024, Russia and China agreed to strengthen coordination mechanisms on the military application of AI, a move the Russian leadership said reflected the consolidation of bilateral ties.⁵⁰ In the last few years China invested

⁴⁸ Zysk 2023(b).

⁴⁴ Korsunskaya, D. e Tétrault-Farber, G., **Russian finance ministry buys 50% of Sberbank from central bank**, Reuters, 10th April 2020.

⁴⁵ Talanova, D., <u>Следите за уходом мысли</u>, Novaya Gazeta Europa, 19th August 2023.

⁴⁶ Cooper, J., Another Budget For A Country At War: Military Expenditure In Russia's Federal Budget For 2024 And Beyond, Stockholm Institute of Peace Research, 2024.

⁴⁷ Russia to spend over 5 bln rubles to support development of AI technology in 2024 – Mishustin, Interfax, 27th September 2023.

⁴⁰ Garlauskas, M. et al., China's support for Russia has been hindering Ukraine's counteroffensive, Atlantic Council, 15th November 2023.

⁵⁰ *China and Russia forge AI military alliance*, Digwatch, 6th February 2024.

300 million dollars in the Skolkovo research centre, set up a joint research fund with an annual budget of 1 billion dollars and opened a Sino-Russian technology hub in Shaanxi province.⁵¹ Such initiatives run parallel to Huawei's deepening presence in Russia, where the Chinese group ranks – alongside the South Korean Samsung – as one of the only major foreign companies investing in the Russian tech sector.⁵²

The relative unattractiveness of the Russian tech market for corporate investors, troubled by potential Western sanctions and pervasive State control, further cement Huawei's influence on Russian R&D. Joint projects undertaken by the group and Russian enterprises, such as VisionLab and Kaspersky, have focused on AI-powered surveillance in the civil sphere but could expand into purely military applications.⁵³ In this view, Chinese backing could quicken the pace of AI integration by partially offsetting issues related to low foreign investment and weak integration into Western research networks.

While there is probably space to further upgrade AI cooperation, Sino-Russian relations are hampered by several factors. The emphasis on technological sovereignty cultivated by both partners may make it difficult for them to enable technology transfers beyond autonomy at rest, especially given past instances of Chinese reverse engineering on Russian arms exports.⁵⁴ Moreover, China's increasing self-sufficiency in technological development may limit its interest in AI partnerships with a lagging Russia in favour of simply exporting components to its northern neighbour. The consolidation of Chinese technological advantage also mirrors the limits of Sino-Russian geopolitical alignment: as China expands its sphere of influence deeper into post-Soviet Central Asia and the global South, its support of Russian AI research and development may be limited to ensuring that the Federation saps Western resources away from anti-Chinese containment.

2.4 Israel

Compared to its U.S., Chinese and Russian counterparts, Israeli national security is more uniquely shaped by its geopolitical determinants. Presiding over a narrow territory surrounded by historically hostile States, Israel's defence strategy focuses primarily on offsetting its lack of strategic depth. Building upon tenets first laid out by David Ben Gurion, Israel's traditional approach fosters a hard-security culture based on qualitative superiority and the maintenance of a constant, high-alert defensive posture enhanced by targeted preemptive strikes. The issue of border depth consequently enhanced the role of national intelligence in providing early warning against security threats: notable examples include the 1967 Israeli bombing of the Egyptian air force and the destruction of the Syrian missile bases on the contested Golan Heights. The heavy toll exacted by purported deviations from the doctrine – such as the 1982 Israeli thrust into southern Lebanon – contributed to reinforcing the public perception of Israel's defence strategy as an existential matter.

As noted in 2019 by former Israeli Chief of Staff Gadi Eisenkot, however, such tenets have since reckoned with both geopolitical and technical developments⁵⁵. After the 1973 Yom Kippur War and the signing of peace accords with both Egypt and Jordan, conventional military threats against Israel largely gave way

⁵¹ Linke, S., *Russia-China Relations in AI*, Eastern Circles, 2023.

⁵² Ibid., pp. 16-23.

⁵³ Ibid.

⁵⁴ Gorenburg, D. et al., *How Advanced Is Russian-Chinese Military Cooperation?*, War On The Rocks, 26th June 2023.

⁵⁵ Samaan, J., 'Decisive Victory' and Israel's Quest for a New Military Strategy, Middle East Policy Council, 2023.

to non-State armed groups, often serving as proxy actors financed and supported, to varying degrees, by the Islamic Republic of Iran and its supporters across the Middle East. The impossibility of eradicating such opponents by directly engaging on the field is compounded by their growing asymmetric capabilities: the proliferation of relatively cheap dual-use hardware (such as commercial drones), as well as the increasing access of insurgent groups to missile weapons and rocketry supplied through Iran, Syria, and Iraq, have rapidly increased the threat posed by such "diffuse rocket-based terror armies".⁵⁶

Against this backdrop, Chief of Staff Kochavi's "Decisive Victory" concept, first launched as part of the 2020 "Momentum" Multiyear Plan, has prioritized AI integration to enhance the offensive capacity of the Israeli military in asymmetric warfare and remedy the issue of border depth. More specifically, the Concept calls for "overwhelming destruction of enemy capabilities using intelligence assets, precise fire capabilities, and offensive autonomous systems".⁵⁷ Subsequent implementation of AI within the Israeli Defence Forces (IDF) and in the Israeli military apparatus brings several areas of focus in relief.

First, AI is being used as a key enhancer of area denial capabilities. While the level of integration is unclear, AI can improve the performance of automated air defence systems such as Iron Dome, the interlinked set of batteries which became operational in 2011 to intercept missiles fired from beyond Israeli borders. Within this context, AI can increase interception rates vis-à-vis the growing firepower of Israel's adversaries. However, AI can also be used to rationalize assets by improving automated threat assessment to only intercept rockets set to fall in populated areas. While interception rates have reportedly reached 90%, each interceptor missile can cost over 100.000 dollars compared to the much cheaper munitions (such as 300-dollars Katiusha rockets or artisanal projectiles) employed by Hamas or Hezbollah.⁵⁸ In a state of constant military threat, AI can therefore be crucial in reducing the weight of automated defence systems on the Israeli economy.

Second, AI can enhance military intelligence through faster and more accurate data gathering and elaboration. The integration of machine learning techniques into Israeli military intelligence aims to allow faster early warning responses and increase the granularity of targeted strikes. The Habsora (Gospel) system, in use by the Israeli Defence Forces during the current operations in Gaza, uses AI to determine priority targets from available datasets: according to an IDF February statement, the strike is then authorized or denied by a human operator.⁵⁹ Israel is also employing AI for a more granular surveillance of its territory through CCTV and facial recognition technology.⁶⁰

Third, the Israeli strategy aims to use AI to improve IDF responsiveness, mobility, and precision in the field. AI-powered advances in sensing, satellite imagery and mapping aim to enhance IDF freedom of movement to allow quicker mobilisation against multi-front threats. The Fire Factory system currently employed by the IDF analyses datasets to calculate the required ammunition and firepower to engage with a given target, as well as allocating and prioritizing optimal engagements.⁶¹ In short, Israeli strategy seemingly uses AI to streamline and rationalize its limited assets in line with a quality-over-quantity

⁵⁶ Eisenkot, G. e Siboni, G., Guidelines for Israel's National Security Strategy, The Washington Institute for Near East Policy, 2019.

⁵⁷ Samaan, J., 2023.

⁵⁸ Nagel, J. e Schanzer, J., <u>Assessing Israel's Iron Dome Missile Defence System</u>, Foundation for Defence of Democracies, 2019.

⁵⁹ Mimran, T. et al., Israel - Hamas 2024 Symposium - Beyond The Headlines: Combat Deployment of Military AI-Based Systems by the Idf. Lieber Institute West Point, 2024.

⁶⁰ Ibid.

⁶¹ IDF's "Fire Factory", Defence Redefined, 14th October 2024.

approach, with integration aiming to enhance C2 capabilities, manoeuvring and firepower to conduct strikes against a diffuse and increasingly active enemy.

Israel's drive towards AI integration is supported by a vibrant R&D ecosystem. While 91% of research and development is financed by the private sector,⁶² Israel also profits from the close interrelation between academia and the industrial-defence complex. The IDF itself is a leading contributor to defence AI and cyber, with academics hailing from its ranks allowed to work 20% of their time off university according to current legislation. ⁶³ By contrast, the Israeli government is virtually absent, financing just 9% of investments in the hi-tech sector despite the latter's crucial contribution to the national economy.⁶⁴

This trend, however, shows signs of abating. 2023 saw investments in Israeli start-ups decline by 55% on average, with the IT and data sector registering a 58% decrease.⁶⁵ This followed a previous 50% decrease in overall funding for 2022, which the Israeli Innovation Agency attributed to the global economic slowdown in the wake of the Ukraine conflict.⁶⁶ The outbreak of hostilities in Gaza between Israel and Hamas is set to weigh more heavily on the Israeli R&D ecosystem, disrupting daily research and production as an estimated 8% of the workforce is called to serve.⁶⁷ On the backdrop of a growing budget deficit (+6,6% at the end of 2023),⁶⁸ the economic downturn will likely be deepened by a spike in military spending: the revised 2024 State budget (which the Israeli parliament approved early in January) includes an additional 15 billion dollar mostly destined to the defence and internal security sector.⁶⁹ In the longer term, another issue for AI military integration concerns the absence of progress in integrating growing segments of the Jewish ultra-Orthodox and Arab population in the tech sector.

More immediately, the Gaza crisis may constitute a watershed for Israel's AI integration strategy. Following the 2023 drop in domestic and foreign financing, military AI could benefit from the governmental increase in defence spending. On the other hand, the deteriorating security outlook in the Middle East and the growing risk of regional spillovers may impact foreign investment in Israeli research and development. On this note, Israel will likely benefit from continued U.S. financial support for R&D as well as arms and technology transfers, which will partially offset the costs of ongoing military operations and currently reach 3,8 billion dollars per year.⁷⁰ US-Israeli technology cooperation has historically been tighter than the Russo-Chinese one, which is slowed down by a mutual drive towards technological protectionism and by the shifting balance of power alongside their shared Central Asian border. The relationship is mirrored by the activity on Israeli soil of U.S. players such as IBM, NVIDIA, Amazon, and Google. However, the magnitude of U.S. support will likely be conditioned by the growing political cost of endorsing Israel's campaign in the Gaza Strip in the eyes of the international community.

Finally, while Israeli authorities seem to be touting the extensive use of AI software in Gaza (and less publicly in the West Bank), the devastating toll of a prolonged campaign in the Strip seems to directly

⁶² Israel's State of Climate Tech 2023 Report, Israel Innovation Authority, 2023.

⁶³ Scheer, S., The State of Artificial Intelligence in Israel, Ministry of Foreign Affairs of Denmark - Innovation Centre, 2019.

⁶⁴ Israel Innovation Authority 2023.

⁶⁵ 2023 Israeli Tech Annual Report, Startup Nation Central, 2023.

⁶⁶ Israel Innovation Authority 2023

^{er} Dietrich, M., Economic fallout of Israel's Gaza Strip operation threatens growth prospects, International Institute for Strategic Studies, 2024.

⁶⁸ Altstein, G., *Israel War Budget Exposes Rifts and Leaves Markets on Edge*, Bloomberg, 16th January 2024.

⁶⁹ Bar Eli, A., Israeli Government Approves Wartime 2024 State Budget; Five Ministers Vote Against, Haaretz, 15th January 2024.

⁷⁰ Magid, J., Biden signs \$1.7 trillion spending bill, including \$3.8 billion for Israel, into law, The Times of Israel, 30th December 2022.

contradict the assumptions at the core of the Momentum plan. It is not unlikely, therefore, that the Israeli leadership might seek to reassess its AI integration strategy.

3. Conclusion

While favouring a software-driven approach to ISTAR activities, the U.S. and China have conceived multidimensional integration pathways, in which operational concerns are couched within a broader medium- and long-term strategic outlook. End goals include consolidating the technological edge over competitors, upgrading current military capabilities, and developing entirely new ones.

Despite having adopted similar multi-year strategies on paper, both Russia and Israel prioritise tactical and operational advantage over long-term development plans. This is largely due to the urgency of addressing regional scenarios and threats that require the immediate fielding of available assets. Israel must therefore address its lack of strategic depths, given its small geographical size, combined with the activity of hostile proxies across the broader region, while Russia needs to keep up production of conventional arms to supply the ongoing war theatres.

Another key point concerns the efficacy of the military-industrial complex in powering AI-related technological advances in the four different contexts. AI has emerged as a strong recipient of R&D funding: while the U.S. and Israel maintain a technological edge, uncertainty remains with regard to China and Russia's ability to act as effective technological forerunners. However, China is working to rapidly close the distance with its geopolitical rivals. To this end, Beijing's Military-Civil Fusion strategy aims to bypass Chinese technological dependence on Western competitors by reducing industrial and knowledge gaps in the hi-tech sector.

Pathways to the military integration of AI are likewise conditioned by differences in political and institutional arrangements. While the U.S. seemingly aim to regulate AI use through institutional safeguards, in addition to allowing easier scrutiny of official documents, the vertical power structure adopted by China and Russia seems to favour a less stringent system of checks and balances. All four actors, however, still display the intention to maintain firm control over certain components linked to Artificial Intelligence. This is the case of key sectors – such as Lethal Autonomous Weapons Systems – in which all four countries seemingly intend to exclude the use of technologies based on the "man out of the loop" principle. However, this condition could be rescinded with relative ease, as AI can be integrated **expost** into several hardware and software instruments.

It is worth noting how Chinese and Russian technological protectionism contrasts with the prevalence of open innovation systems as incubators for AI development. Strategically, the Sino-Russian approach allows for greater input control at the potential expense of dataset quality and variety, which directly impact the efficacy and versatility of AI applications. At the operational level, finally, China and Russia's interest in centralizing decision-making procedures strengthen their historical proclivity for direct control over command structures, while the U.S. and Israel look with greater interest at implementing AI to decentralize and streamline command-and-control operations.

Acknowledgements

Il presente paper è stato realizzato nell'ambito del progetto "Geopolitica del Digitale", promosso dalla Fondazione Med-Or, in collaborazione con il Center for International and Strategic Studies (CISS) della Luiss Guido Carli, grazie al sostegno della Fondazione Compagnia di San Paolo all'interno del bando "Geopolitica e tecnologia".

About Luiss School of Government

The Luiss School of Government (SoG) is a graduate school training high-level public and private officials to handle political and government decision-making processes. It is committed to provide theoretical and hands-on skills of good government to the future heads of the legislative, governmental and administrative institutions, industry, special-interest associations, non-governmental groups, political parties, consultancy firms, public policy research institutions, foundations and public affairs institutions. The SoG provides its students with the skills needed to respond to current and future public policy challenges. While public policy was enclosed within the state throughout most of the last century, the same thing cannot be said for the new century. Public policy is now actively conducted outside and beyond the state. Not only in Europe but also around the world, states do not have total control over those public political processes that influence their decisions. While markets are Europeanised and globalised, the same cannot be said for the state.

The educational contents of the SoG reflect the need to grasp this evolving scenario since it combines the theoretical aspects of political studies (such as political science, international relations, economics, law, history, sociology, organisation and management) with the practical components of government (such as those connected with the analysis and evaluation of public policies, public opinion, interests' representation, advocacy and organizational leadership).

For more information about the Luiss School of Government and its academic and research activities visit. www.sog.luiss.it

Luiss School of Government

Via di Villa Emiliani 14 00197 Roma T +39 85 225052 sog@luiss.it