

SAMUELE CELI

THE RISE OF AI-DRIVEN DECISION SUPPORT IN INTELLIGENCE: CASE STUDIES FROM UKRAINE AND ISRAEL AND THE PROSPECTS FOR AUTHORITY EXPANSION

RESEARCH PAPER 2026

GINO GERMANI INSTITUTE
FOR SOCIAL SCIENCES AND STRATEGIC STUDIES
www.istitutogermani.org

The Gino Germani Institute of Social Sciences and Strategic Studies, a non-profit think tank founded in 1981, pursues the mission of defending and renewing liberal democracy and the open society. The Institute promotes and publishes studies and analyses on the challenges to the security and stability of the West, the Euro-Atlantic community, and Italy. It also aims to raise awareness among policymakers and the general public about internal and external threats to liberal democracy and its values. In particular, the think tank focuses on topics such as: authoritarian and totalitarian regimes and ideologies, terrorism and political violence, right-wing and left-wing extremism, transnational organized crime, political corruption, illiberal national-populist movements, disinformation and perception manipulation, cyber threats, interference and influence by autocratic foreign powers aimed at destabilizing democracies, and the role of intelligence and counter-intelligence in safeguarding democratic states.

Samuele Celi has an interdisciplinary background in the social sciences, developed at Bocconi University, and further specialized in intelligence and international security at the Paris School of International Affairs (PSIA) at Sciences Po.

During his studies at Sciences Po, he focused in particular on contemporary developments in intelligence, examining the role of psychological operations (PSYOPS) and the use of artificial intelligence (AI) technologies in intelligence processes and national security activities, with particular attention to the cases of Israel and the United States.

He also conducted his Master's thesis research in collaboration with the Italian Defence General Staff, focusing on major national defence procurement and armament programmes. This experience enabled him to develop an in-depth understanding of the industrial, technological, and strategic dynamics shaping the development, sustainment, and evolution of national military capabilities, as well as the related issues of security, strategic sovereignty, and technological sovereignty.

Building on this academic and research background, he has gained professional experience in strategic consulting across the aerospace, defence, and security sectors, including work on technologies and systems designed for the protection and monitoring of critical infrastructure. His work has covered, among other areas, Counter-Unmanned Aircraft Systems (C-UAS) and artificial intelligence applications supporting security and surveillance activities.

GINO GERMANI INSTITUTE
FOR SOCIAL SCIENCES AND STRATEGIC STUDIES

**THE RISE OF AI-DRIVEN DECISION SUPPORT
IN INTELLIGENCE: CASE STUDIES
FROM UKRAINE AND ISRAEL AND THE
PROSPECTS FOR AUTHORITY EXPANSION**

Samuele Celi



RESEARCH PAPER

September 2026

The opinions expressed are strictly personal
and do not necessarily reflect the positions of the Gino Germani Institute.

© 2026 GINO GERMANI INSTITUTE FOR SOCIAL SCIENCES AND STRATEGIC STUDIES

ISBN: 979-12-985-7077-1

Via del Commercio 4 – 00015 Monterotondo (RM)

Tel. 06-84969914

fondazionegermani@gmail.com

info@istitutogermani.org

www.istitutogermani.org

Table of contents

<i>Introduction</i>	4
Section 1: Cognitive Limits and the Emergence of AI-driven Decision Support	6
Section 2: Operational Employment of AI-driven DSSs in Active Battlefields	8
2.1. Case Study: Use of AI-driven DSSs in Ukraine-Russia Conflict	8
<i>2.1.1 MetaConstellation: imagery analysis, target detection and strike recommendations</i>	9
<i>2.1.2. Avengers: improving targeting through drone video analysis</i>	10
2.2. Case 2: AI-driven Decision Support Systems (DSSs) in the Operation Iron Swords	11
<i>2.2.1. 'Hasbora' (Gospel): Identification and Assessment of Enemy Facilities</i>	12
<i>2.2.2. Lavender and U8200 Tools: Identification of Potential Terrorist Operatives</i>	13
2.3. Comparative Assessment: Ukraine and Israel	14
Section 3: Beyond Bounded Rationality and Limitations to AI-Enabled	15
3.1. Algorithmic explainability	16
3.2. Data Deception and Data Bias	17
3.3. Human Resistance	18
4. Conclusion and Recommendations	19
<i>References</i>	21

Introduction

“Alex Karp – CEO of Palantir Technologies – stated in 2022: “The power of advanced algorithmic warfare systems is now so great that it equates to having tactical nuclear weapons against an adversary with only conventional ones. The general public tends to underestimate this. Our adversaries no longer do.”

This claim captures a major shift in the international security environment, where hybrid competitors are emerging from asymmetric conflicts and global instability, strategically combining kinetic and non-kinetic tools to bias decision-making processes and create uncertainty. As the Multinational Capability Development Campaign (MCDC) notes, such threats deliberately exploit “ambiguity and deception”, combined with innovative use of different “non-military tools” (Nilsson et al., 2025).

At the same time, intelligence organizations face a sharp rise in the volume and variety of available data – particularly Open-Source Intelligence (OSINT) – which has incremented existing cognitive constraints. Information overload leads to individual stress, indecisiveness, and less effective analysis of decisions – what Palladino in 2007 defined *cognitive overload*. Moreover, it has broader implications too, such as (i) organizational ineffectiveness, (ii) circular reporting and (iii) overclassification (Young, 2019). The U.S. Office of the Director of National Intelligence (ODNI) warned that the pace of data generation has “long exceeded our collective ability to understand it” (ODNI, 2024). This acceleration, however, does not create cognitive limits, but intensifies the classical bounds of human rationality and pattern-seeking biases identified by Simon (1956) and Heuer (1999).

Consequently, intelligence – defined as “information that meets the stated or understood needs of policy makers and has been collected, processed, and narrowed to meet those needs” (Lowenthal, 2020) – now confronts evolving targets: hybrid threats alter those needs unpredictably, while data overload further undermines the capacity of human systems to fulfil them efficiently (Cooper, 2024). Against this backdrop, AI-enabled Decision Support Systems (DSSs) have emerged as promising tools to alleviate cognitive strain and improve decision-making in time-sensitive environments.

This paper addresses the following question: how are AI-driven DSSs currently shaping operational decision-making – mainly within the targeting cycle, and

under what conditions might their authority expand beyond the limits of human judgment?

The thesis advanced here is that AI-driven DSSs are actively and effectively influencing decision-making processes in critical operational theaters, predominantly through targeting assistance under human oversight; however, in fast-paced hybrid environments, pressures prompted by cognitive overload and threat evolution create structural incentives for a gradual expansion of delegated algorithmic authority. Such an expansion should be consistent with the technological advancement of AI models along with data-input quality and algorithm explainability adequate constraints.

To substantiate these claims, the dissertation proceeds in three steps. First, it integrates theoretical and empirical research on cognitive overload, and traces through historical data how has fostered the development of AI-driven DSSs. Second, it analyzes Ukraine and Gaza as operational theaters where these systems have been actively embedded in decision-making processes, briefly comparing the scope of authority they have assumed in each case. Third, it evaluates technical and institutional limits that shape – and often constrain – the pathway of delegated algorithmic authority.

1. Cognitive Limits and the Emergence of AI-driven Decision Support

Intelligence analysts – like all human beings – elaborate their decisions within the limits of bounded rationality and typically rely on a *satisficing mode* (Heuer, 1999), selecting the first hypothesis that appears “good enough”. Information is often collected and organized according to whether it supports this *tentative* judgment, and a hypothesis is validated if it seems to provide a reasonable fit to the available data. Moreover, as a component of survival mechanisms, individuals subconsciously develop mental models and perceptual biases that may significantly affect judgment and decision-making (CIA, 2009), reinforcing reliance on *satisficing strategies*.

Heuer (1999) has argued that “an optimal analytical strategy requires that analysts search for information to disconfirm their favorite theories, not employ a satisficing strategy that permits acceptance of the first hypothesis that seems consistent with the evidence”. In practice, however, analytical performance frequently falls short of this ideal, and suboptimal judgments contribute to recurring intelligence failures (Cooper, 2024).

This imperfect model of judgment has become increasingly untenable in the face of exponential growth in data. From the Cold War onward, the volume, velocity, variety and ubiquity of information have further complicated its collection and structuring, resulting in a proliferation of suboptimal decisions: the capacity of traditional analytical tradecraft and pattern recognition has been outpaced by the quantity and complexity of the input (Weinbaum & Shanahan, 2018).

As a result, US intelligence professionals in the 1980s and 1990s began to take a growing interest in the data-mining and data-processing advantages of Artificial Intelligence (AI), understood as the ability of computers to search across multiple sources and transform it into usable information for human analysts. One of the earliest examples of such automated data triage was the ECHELON program, an automated global surveillance system which used content-sensitive dictionaries of keywords to comb through satellite intercepted communications for relevant data. Though rudimentary by modern standards, it represented an early step towards the progressive automation of parts of the analytical cycle (Moran et al., 2023).

During the same period, figures such as Richard DeLauer, former Under Secretary of Defense, and senior CIA officials focused on how AI could be exploited for data-mining processing. As they saw it, the main advantage of AI was that it could assume a substantial share of this labor-intensive but essential activity and be deployed alongside human analysts to enhance decision-making (Moran et al., 2023).

It was under this rationale that, in December 1982, John McMahon – then Deputy Director of the Central Intelligence (DDCI) – organized the first annual AI symposium within the CIA, signaling the increasing interest of the Intelligence Research and Development (R&D) Council in AI applications. A few months later, he also established an AI steering group. Recalling how private contractors had accelerated the U2 program¹, McMahon recognized that the CIA needed the know-how of the tech industry and academia to develop effective AI tools. The intelligence community therefore began establishing partnerships with technology companies from the San Francisco Bay Area, investing in AI start-ups and encouraging intelligence veterans to serve on company boards.

In the 1990s, modest success was achieved in developing speech-to-text transcription and automated speaker recognition software. AI was succeeding in the “thinking fast” assignments – such as rapidly recognizing a Russian bomber from a satellite image – while it continued to struggle with the “thinking slow” component of the intelligence cycle, including hypothesis generation, contextual interpretation and prioritization of strategic judgments (Kahneman, 2011).

Accomplishing these more demanding assignments – through multi-INT fusion and contextual reasoning – was significantly advanced with the establishment of Palantir Technologies. Founded in 2003 with seed funding of Peter Thiel and subsequently supported by In-Q-Tel², Palantir evolved, despite initial difficulties³ (Harris, 2012), into a major contractor for the US government (Burns, 2015). By integrating and synthesizing numerous federal databases (Burns, 2015), the company positioned itself as a prominent provider of AI-driven DSSs for intelligence and security agencies. Rather than focusing on isolated analytical tasks, its platforms – most notably Gotham and its derivatives – are designed to fuse multiple intelligence streams (e.g., HUMINT, SIGINT, OSINT) into a single, adaptive plat-

¹ The U2 was a major CIA program of overhead reconnaissance.

² Venture Capital firm owned and managed by the Central Intelligence Agency.

³ In its first year of activity Palantir was consistently unpopular in Silicon Valley.

form, enabling a more decentralized decision-making. Over time, Palantir's approach shifted from mere data aggregation to real-time predictive modeling and its AI-enabled DSSs have been deployed in active operational theaters.

Taken together, these developments illustrate how cognitive limits, data overload and institutional innovation converged to produce modern AI-driven DSSs. The next section examines how such systems are employed in practice in (2.1) Ukraine and (2.2) Gaza, and how their operational use shapes decision-making in live conflict environments.

2. Operational Employment of AI-driven DSSs in Active Battlefields

2.1. Case Study: Use of AI-driven DSSs in Ukraine-Russia Conflict

The Ukraine-Russia conflict has become a paradigmatic example of how AI-driven Decision Support Systems (DSSs) can be integrated into operational decision-making. Alex Karp, Chief Executive Officer (CEO) of Palantir, has claimed that his company "is responsible for most of the targeting in Ukraine" (quoted in Dustin, 2023). While this statement originates from a highly interested party, it is broadly consistent with what accounts from Ukrainian officials and independent observers (Bergengruen, 2024; Grylls, 2022; Ignatius, 2022; Macaes, 2023).

On June 1, 2022, Karp was escorted into the fortified bunker of the Ukrainian presidential palace, becoming the first leader of a major Western technology company to meet with President Volodymyr Zelensky since Russia's full-scale invasion three months earlier (Bergengruen, 2024). The meeting, which also involved Mykhailo Fedorov, Ukraine's Minister of Digital Transformation, laid the groundwork for Palantir's operational partnership with the Ukrainian government. In the year and a half following this encounter, Palantir's software has been extensively integrated into Ukraine's day-to-day military and intelligence ecosystem. AI-driven DSSs process data provided by SIGINT, OSINT, HUMINT and other intelligence disciplines into decision-ready outputs. According to both Karp and Ukrainian officials, these systems are used not only to identify targets, but also to propose engagement options based on evolving battlefield data (Macaes, 2023; Fedorov, as cited in Ignatius, 2022).

2.1.1. MetaConstellation: imagery analysis, target detection and strike recommendations

MetaConstellation illustrates how an AI-driven DSS can integrate targeting cycles by fusing commercial imagery and multi-INT data into near-real-time engagement recommendations. Among Palantir's platform, it has been described as one of the most strategically relevant tools adopted by the Ukrainian forces to identify key Russian targets and suggest high-stake decisions (Macaes, 2023). Originally developed during the post-9/11 era for counterterrorism operations, the system has been adapted to the specific geography of Ukraine and the Black Sea. It is now portrayed by some analysts as one of the most operationally effective AI-enabled systems currently used in warfare (Macaes, 2023).

The tool uses commercial data – including low-earth orbit satellite imagery – to generate a near real-time representation of a given battlespace. This information is then embedded with commercial and classified government multi-INT data⁴, some of which are reportedly provided by NATO allies (Ignatius, 2022). MetaConstellation elaborates these inputs to identify potential enemy positions and to generate options for prosecuting them with the available spectrum of weapons. According to Ukrainian officials, the resulting recommendations are reviewed and validated by users in charge⁵, including NATO advisers outside Ukraine (Ignatius, 2022). Upon approval, the information is presented to military officials through Gaia, a companion software that renders a dynamic, real-time operational map analogous to a digital version of traditional table-top planning tools. Final strike decisions are then taken either directly by commanders or relayed, through established chains of command, to field operators (Ignatius, 2022).

MetaConstellation is constantly updated with feedback from kinetic operations: battle damage assessments are fed back into the neural model to refine predictive accuracy over time (Ignatius, 2022). While comprehensive metrics are classified, officials have credited the system with contributing to operational successes. In 2022, Minister Fedorov stated that Palantir's software had been “especially useful during the liberation of Kherson, Izium, Kharkiv and Kyiv regions” (quoted in Ignatius, 2022). The Times similarly reported that “the accuracy, speed and deadli-

⁴ Apart from SIGINT, OSINT and HUMINT are used by this system (e.g. informants' tips on the movements of Russian troops).

⁵ “In charge” of the oversight procedure, thus, the first *human-in-the-loop* in the targeting cycle.

ness of Ukrainian strikes have dramatically increased thanks to software developed by Palantir” (Grylls, 2022).

Despite the extent of its integration, MetaConstellation does not fully automate the targeting process. Human-in-the-loop (HITL) arrangements – i.e. human participation in the (i) operations, (ii) oversight and (iii) decision process of an automated system (Stryker, 2024) – remain firmly in place at the final decision stage. Commanders and authorized personnel retain formal authority to accept, modify or reject the system’s recommendations. In the Ukrainian case, MetaConstellation therefore shapes operational decision-making by compressing identification and coordination timelines, and by ranking engagement options, while leaving ultimate responsibility and accountability with human decision-makers.

2.1.2. Avengers: improving targeting through drone video analysis

While Palantir retains a pivotal role in the AI ecosystem of Ukrainian forces – also contributing to demining efforts through a specific Artificial Intelligence Platform (AIP) and supporting the prosecution of alleged Russian war crimes (Palantir Technologies, 2024) – the Ukrainian Ministry of Defense’s Innovation Center has developed a complementary AI-driven platform, Avengers. This system exemplifies how domestically developed tools can improve situational awareness and targeting without directly assuming higher-order decision-making functions.

Avengers can identify objects and detect targets in thousands of simultaneous video streams from drones and stationary cameras, even if they are camouflaged or hidden in forests. It is also reported to distinguish decoys from real targets (Bondar, 2024). In September 2024, the Ministry of Defense announced that the system autonomously detected approximately 12,000 pieces of Russian equipment per week, thereby improving data-processing and reducing the risk of human error (Bondar, 2024).

Unlike MetaConstellation, however, Avengers is limited in scope. Although it contributes to localizing hostile assets, it does not provide autonomous prosecutorial recommendations or strike coordination and thus does not directly participate in higher-order operational decision-making. Its role is to feed more accurate and timely detection data into existing command structures, rather than to shape

engagement strategies. Nevertheless, Avengers represents a notable achievement given the comparatively modest resources of its developers and illustrates Ukraine's broader commitment to algorithmic augmentation of its defense capabilities.

Taken together, MetaConstellation and Avengers illustrate how AI-driven DSSs in Ukraine already influence operational decisions by accelerating detection, determining targeting options, and improving the reliability of inputs, while remaining embedded in HITL structures. This first case therefore provides an empirical illustration of how AI-based DSSs can reshape decision-making in active battlefields, and of how formal authority is, at least for now, still anchored in human judgment even as algorithmic tools assume an increasingly prescriptive role.

2.2. Case 2: AI-driven Decision Support Systems (DSSs) in the Operation Iron Swords

The Israeli case illustrates how a domestically developed ecosystem of AI-driven Decision Support Systems (DSSs) can be embedded across multiple stages of the operational decision-making process, while formally preserving human authority.

Following the Hamas-led coordinated terrorist attack of October 7, 2023, the Israel Defense Forces (IDF) accelerated the development and operational deployment of advanced AI-driven Decision Support Systems (DSSs). While Palantir continues to support Israeli counterterrorism efforts, the systems most deeply embedded in IDF and Mossad operations are the result of Israel's domestic defense-technology ecosystem, characterized by close coordination between military R&D entities, intelligence services and the private sector (Mimran et al., 2024).

Among the systems already in use before October 7 was "Fire Factory", an AI-enabled DSS which analyzes extensive datasets – including information about previously authorized strike targets – enabling the calculation of required ammunition quantities, the proposal of optimal timelines and the prioritization of targets. In doing so, it provides structured support to phase 2 (target development) and phase 3 (capabilities analysis) of the targeting cycle⁶ - as developed by the U.S.

⁶ The Joint Targeting Cycle is composed by Phase 1 (Targeting Guidance and Intent), Phase 2 (Target Development and Prioritization), Phase 3 (Capabilities' Analysis), Phase 4 (Decision and Force Assignment), Phase 5 (Mission Planning and Force Execution) and Phase 6 (Combat Assessment).

Air Force (2021). Building on this architecture, Israel subsequently developed more specialised AI-driven DSSs such as Gospel and Lavender, designed to assist analysts and commanders in distinct segments of the targeting process.

2.2.1. ‘Hasbora’ (Gospel): Identification and Assessment of Enemy Facilities

Gospel exemplifies how an AI-driven DSS can systematize the early stages of target identification while keeping legal qualification and engagement decisions in human hands. It is an AI-enabled system designed to identify physical structures which might qualify as lawful military objectives. Gospel synthesizes large volumes of cross-intelligence data and suggests to intelligence operators to focus their research on certain physical objects with greater operational relevance. Analysts – similarly to NATO external advisors in the Ukrainian targeting process – are required to assess those proposed facilities independently by reference to a “Standard Operating Procedure” (SOP) aligned with the criteria for military targets under the 1949 Geneva Conventions⁷. Final approval must be granted by at least one high-level authorized intelligence officer (Schmitt, 2024).

Once confirmed, the potential target is passed to a “mission planning cell” (operators, planners, intelligence analysts, legal advisors, etc.) or other body entitled to plan and approve attacks – phase 4 (Decision and Force Assignment) and phase 5 (Mission Planning and Force Execution) of the targeting cycle. Gospel does not independently determine whether a facility qualifies as a military objective, and its suggestions alone are not a sufficient basis for concluding that an object is lawfully targetable (Schmitt, 2024). Rather, it narrows the field of potential targets so that human decision-makers can concentrate their efforts on a smaller set of higher-relevance candidates.

Importantly, analysts retain access to the raw intelligence upon which Gospel-generated suggestions are elaborated (IDF Press Release, 2024). Although the comprehensive reasoning used by the algorithm to provide its outputs may not be fully interpretable – pending further developments Explainable Machine Learning (XAI)⁸ –, access to the original input which has influenced the decision ensures

⁷ Article 52(2) of the 1977 Additional Protocol I. Its full content is classified.

⁸ See 3.1.

data-level transparency and allows analysts to test and corroborate the system's outputs against primary sources.

While Gospel has significantly improved the targeting cycle and assisted intelligence analysts and commanders in high-stake decisions, there is no indication that every IDF *pre-planned* targeting operation relies on it (Schmitt, 2024). From the perspective of this analysis, Gospel therefore illustrates a model in which an AI-driven DSS exerts significant influence on which potential targets are brought into the decision space, without displacing human authority over legal classification or engagement decisions.

2.2.2. Lavender and U8200 Tools: Identification of Potential Terrorist Operatives

Lavender represents a different but complementary use of AI-driven DSSs, focusing on individuals rather than facilities. It is a smart, AI-supported, database that fuses and organizes information on individuals who might be members of Hamas or other designated terroristic organizations (Schmitt, 2024).

The system does not independently identify individuals as combatants, does not produce a suggested target list, nor it serves as an approved roster of individuals for neutralization (IDF Press Release, 2024). While the database is regularly updated using multi-INT sources, the mere inclusion of a person within it is not sufficient to identify that individual as a lawful target (IDF Press Release, 2024). As with Gospel, phases 4 and 5 of the targeting cycle are conducted entirely by human decision-makers.

Since Lavender is a general database, its applications may transcend lethal targeting assistance. Identified individuals may instead be detained, interrogated, or tracked. Moreover, it can assist ground forces in planning operations in specific geographic areas to identify organized armed group members or to get an idea of the enemy's density in it. In this sense, Lavender functions as an AI-driven DSS for large-scale pattern recognition and situational analysis, rather than as an automated mechanism for individual-level neutralization.

Overall, Lavender provides meaningful support to the high-stake decisions, while leaving final determination entirely to human operators. The time required to complete the targeting cycle when using Lavender is highly situational⁹: some targets

⁹ The targeting cycle, however, is always highly context-specific in its timing.

can reportedly be validated quickly, such as rocket operators, whereas others, such as suspected combatants not engaged in active hostilities, demand greater effort before verifying status (Schmitt, 2024). This variability underscores both the potential and the limits of AI-driven DSSs in accelerating decision-making in complex human-centric targeting environments.

A comparable tool was developed earlier – in 2020-2021 – by the AI Center embedded within Unit 8200 of the Israeli Military Intelligence (Aman). First deployed during the operation “Guardian of the Walls”¹⁰, it has been actively used during operation Iron Swords too. This system is designed to identify Hamas missile unit leaders and anti-tank operatives within Gaza territories. According to U8200 Data Science and AI Commander Col. Yoav, during the 2023 campaign the tool generated 200 military target options for strategic engagement (as cited in Bob, 2023), significantly reducing the cognitive load associated with “thinking slow” human-led decisions. As confirmed by a former operative of Unit 8200 interviewed for this paper in 2025, phase 4 and phase 5 of the targeting cycle remain under strict human responsibility while using this AI-based DSS, consistently with the other Israeli-developed platforms analyzed. The same source indicated that the tool’s strategic use and its efficiency in proposing viable target options during Operation Iron Swords were widely recognized within the unit (Former Operative A, 2025).

Taken together, Lavender and the Unit 8200 tools illustrate a structural pattern: Israeli AI-driven DSSs in the personnel domain are optimized for data fusion, large-scale pattern identification and option generation, reinforcing human judgment rather than substituting it in the final determination of individual targetability.

2.3. Comparative Assessment: Ukraine and Israel

Both Ukrainian and Israeli forces have integrated AI-driven Decision Support Systems (DSSs) to assist their operations across complex and rapidly evolving environments. In both theaters, AI tools mainly support the mid-phases of the targeting cycle – especially phases 2 and 3 – while phases 4 and 5 remain under *human-in-the-loop* (HITL) control. This shared pattern reflects a clear objective: reducing cognitive load and mitigating bounded rationality without displacing formal human authority (Macaes, 2023; Schmitt, 2024).

¹⁰ Targeted campaign against Hamas.

Ukraine's integration of AI-driven DSSs is characterized by a strong reliance on external technological providers. Palantir's MetaConstellation assists intelligence personnel in identifying, prioritizing and prosecuting physical targets, while the domestically developed Avengers platform contributes drone-based and video-derived detection capacity (Ignatius, 2022; Bondar, 2024). Their operational reach is therefore relatively circumscribed to object-based identification and hierarchization, reflecting both the available technological base and the priority needs prompted by the Russian invasion.

Israel, by contrast, has developed most of its AI-driven DSSs domestically, although external providers have contributed to certain efforts. The Israeli approach reflects a broader operational scope: systems such as Gospel and Lavender support the identification of facilities and terrorist operatives respectively, and Unit 8200 tool assists in the designation of specific human objectives. Lavender in its assignment over certain targets (Schmitt, 2024; Former Operative A, 2025). These platforms collectively perform broader functions of data fusion, pattern recognition and option generation across multiple decision layers. As such, Israeli DSSs appear more deeply embedded in intelligence workflows and contribute to a wider set of high-stakes decisions, even while preserving HITL control in phases 4 and 5.

Overall, the comparison indicates that both systems improve operational decision-making, but they diverge in breadth and depth: Ukrainian DSSs remain predominantly object-centered, whereas Israeli DSSs embed more comprehensively into personnel-related and strategic targeting processes. Both Ukrainian and Israeli officers have avoided the full automation of critical decision-making processes, reflecting the limitations that will be examined in the next section.

3. Beyond Bounded Rationality and Limitations to AI-Enabled Systems

The previous section illustrated how AI-driven Decision Support Systems (DSSs) can mitigate bounded rationality by accelerating analysis, generating alternative hypotheses and reducing cognitive overload in the mid-phases of the targeting cycle. However, a wider assessment requires examining the structural constraints that continue to limit the delegation of operational authority to AI systems. These constraints – established in (i) explainability gaps, (ii) data bias and deception, and (iii) human resistance – help explain why phases 4 and 5 of the targeting cycle remain firmly under human control despite the growing analytical influence of AI.

AI-enabled systems significantly reduce the time required to elaborate high-stake judgments – such as during phases 2 (Development) and 3 (Capabilities’ Analysis) of the targeting cycle (Schmitt, 2024; Mimran et al., 2024; Ignatius, 2022; Grylls, 2022). By expanding the evidentiary space that analysts can process, these systems may reduce reliance on *satisficing* strategies. Yet, their accelerated analytical performance does not resolve deeper epistemic and organizational barriers that currently prevent a transfer of decision-making authority beyond assistance or mere recommendation.

3.1. Algorithmic explainability

AI-enabled systems rarely provide clear explanations for the reasoning behind their outputs. Yet, when dealing with critical decisions, understanding the rationale behind an AI-generated output can be essential for operators. Moreover, the inability of AI systems to elucidate their operational processes is likely to impact the duty to conduct investigations into alleged breaches of International Humanitarian Law (IHL), generating potential accountability issues (Pacholska, 2022; Mimran et al., 2024).

Explainable Artificial Intelligence (XAI) – defined as “a field of research that explores methods that provide humans with the ability of intellectual oversight over AI algorithms” (Longo et al., 2024) – is a promising field but remains both understudied and underdeveloped (Babic & Cohen, 2024). Even widely cited examples of explainability features illustrate these limits:

- (i) they are not unique or action-guiding;
- (ii) they are not sincere, often failing to reflect the actual reason behind a decision;
- (iii) they are post hoc, offering explanations only after the fact.

According to Babic and Cohen (2024), these constraints suggest that interpretability does not automatically translate into transparency.

Moreover, mandating explainability may deter innovation in AI development (Babic & Cohen, 2024). Although greater investment in this field may be instrumental in improving long-term usability, interpretability is not currently viewed

as a universal requirement for expanding operational authority. At present, access to the raw intelligence underpinning AI-generated suggestions – as in Gospel – offers only data-level transparency, not interpretability of the model’s internal logic. This distinction remains central in assessing the limits of delegation.

3.2. Data Deception and Data Bias

Because AI-enabled DSSs are trained and supplied with data, the reliability of their outputs depends heavily on data quality. Biased, incomplete or deceptive datasets can lead to distorted outcomes, including hallucinations and erroneous pattern recognition (Cooper, 2024).

Generative AI systems select subsequent words, phrases or other outputs in a combination based on observable patterns in training data. In the absence of data, or if deceptive contents are used as inputs, generative AI will deduce the most likely sequence of content, which may contain inaccuracies or even fabricated information. Consequently, intelligence organizations must accurately verify the dataset used to train the models, ensuring that it is representative of thoughtful analytical methodologies that seek to avoid bias. Cooper (2024) emphasizes that agencies should also consider integrating private sector data, while recognizing the complexity of this effort and remaining vigilant to data poisoning and deception techniques used by hostile actors.

This threat proves to be particularly salient in the context of structured adversarial state powers such as the Russian Federation, which has long demonstrated expertise in information manipulation and deception. During the ongoing Russia-Ukraine conflict, Russian operatives have repeatedly attempted to corrupt OSINT datasets – occasionally used as secondary inputs by MetaConstellation – through doctored images, fabricated narratives, or coordinated misinformation campaigns (Colley & Dylan, 2025). These efforts aim to distort situational awareness and bias critical decisions.

Data transparency provides an additional and powerful safeguard: when analysts are granted access to the raw intelligence upon which a certain judgment has been generated by an AI-enabled DSS – as occurs with systems like Gospel and Lavender – they can *double-check*¹¹ the sources employed, assessing their credibility and analytical path, and make a more informed final decision.

¹¹ The first examination and validation should be made *ex-ante*, i.e. before integrating the information in the dataset, while this scrutiny should be secondary (*double*) and final.

In sum, data quality is pivotal in determining reliable outputs. Therefore, it must be taken into consideration before any further expansion of AI-driven DSSs' authority over human judgment. However, (i) if human oversight is retained for data input validation or supported by AI-enabled tools in this task, and (ii) data-level algorithm transparency is assured, a broader operational role for AI may be justifiable.

3.3. Human Resistance

Cognitive and institutional dynamics also limit the operational authority of AI systems. Intelligence analysts and field commanders often exhibit skepticism toward machine-generated outputs. As Heuer (1999) suggests, analysts tend to rely on "tentative hypotheses" shaped by experience and organizational culture (Schmitt, 2024), which may lead them to discount machine-generated outputs. This inclination may lead intelligence analysts to discard recommendations from the AI-enabled DSSs and instead overconfidently rely upon their personal training and experience.

Such resistance is particularly evident among field commanders, who are often reluctant to cede control over critical phases of the decision-making process. While their confidence in personal judgment is psychologically understandable, over-reliance on human intuition may, in the long-run, undermine the efficiency gains that AI systems are designed to deliver.

Although it is equally important to avoid undue deference or "automation bias" towards the systems – especially to still-evolving ones – unwarranted skepticism towards machine-generated outputs may diminish the efficiency and accuracy of decision-making processes. As AI systems improve in both reliability and explainability, such resistance may become increasingly dangerous and detrimental.

At present, retaining *human-in-the-loop* (HITL) structure – particularly in critical decision-making process phases – is justified, as it boosts legitimacy and accountability (Mimran et al., 2024). In the long-run, however, as AI systems evolve and become more transparent and efficient – human oversight may be progressively limited to the final decision point. Human resistance to the transition may be mitigated through institutional and legal mechanisms, as well as through improved explainability tools that may provide to commanders a clearer operational context, thus fostering greater reliance in machine-assisted judgments when trustworthy.

Until these conditions are met, human resistance – rooted in cognitive biases and institutional norms – remains a structural constraint on delegation.

4. Conclusion and Recommendations

Intelligence analysts and field commanders are frequently required to make high-stake decisions in complex and time-sensitive environments. However, their rationality is bounded, and their judgments are often susceptible to cognitive biases. Furthermore, in contemporary era, the drastic increase in both the volume and variety of information exacerbates cognitive overload and complicates the assessment of emerging hybrid threats by purely human means.

AI-driven Decision Support Systems (DSSs) have emerged as valuable tools to assist decision-making in such environments, bringing meaningful efficiency improvements in both the Ukrainian theater – through MetaConstellation – and in the Israeli context – through Gospel, Lavender and other systems. These platforms have demonstrably reduced cognitive load, accelerated decision-making processes, and possibly mitigated human bias by proposing structured hypotheses and grounded recommendations.

Nonetheless, several limitations are currently constraining the transition from Decision Support Systems (DSSs) to actual Decision-Making Systems (DMSs). Technical challenges – such as the underdevelopment of XAI and concerns over data quality – alongside institutional resistance from human operators, continue to inhibit broader deployment. At present, DSSs function as support systems rather than autonomous decision-makers.

Artificial Intelligence should therefore not be regarded merely as a technological advancement, but as a catalyst for systemic transformation within the intelligence and military ecosystems. This transformation requires not only significant investment in Research and Development, but also the restructuring of institutional and operational frameworks. If properly developed and embedded, AI systems may gradually transition from a heuristic dimension to a more optimized and analytically grounded one – capable of handling both iterative and rapid-response operations and high-stakes decisions. Importantly, this evolution depends on the establishment of a structured and tailored ecosystem in which collaboration between private technology providers and public institutions is not vilified but rather leveraged, as illustrated by the Ukrainian and Israeli cases.

Maintaining technological superiority in the AI domain over hostile actors now represents a critical strategic advantage that should not be underestimated. As such, rather than obstructing the expansion of AI authority through institutional inertia or postponing deployment until full XAI is reached – which may take long – military and intelligence stakeholders should proactively support the deployment of AI-driven tools. These systems should be progressively integrated into a wider array of critical functions, provided that data quality is continuously verified and the platforms' reliability demonstrably exceeds that of pure human judgment.

This evolution must proceed along a clear and structured pathway:

- (i) Reinforce verification procedures for input datasets by incorporating additional human oversight and/or deploying dedicated Artificial Intelligence Platforms (AIPs) designed specifically to conduct screenings of raw intelligence prior to system training.
- (ii) Improve data-level transparency by rewriting algorithms to display the raw input upon which the AI-generated recommendation has been elaborated – an approach already exemplified by systems such as Gospel and Lavender.
- (iii) Gradually improve algorithm explainability, beginning with algorithmic modifications that enable users to access explanations which are partial yet unique, accurate and timely (i.e. elaborated in real-time than post hoc), and subsequently advancing toward the development *ex-novo* of fully explainable AI models. This transition should be linear, pragmatic, and should not obstruct further advancement in military AI innovation.

If this framework is established, AI-tools may soon be deployed with expanded operational responsibilities, enabling military and intelligence organizations to secure and maintain a meaningful advantage in an increasingly contested strategic domain.

References:

Air Force Doctrine Publication 3-60, Targeting. (2021). Available at: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-60/3-60-AFDP-TARGETING.pdf.

Babic, B. and Cohen, I.G. (2024). *The Algorithmic Explainability ‘Bait and Switch’*. [online] Available at: https://minnesotalawreview.org/wp-content/uploads/2024/01/2.4_Babic-Cohen.pdf [Accessed 17 Nov. 2025].

Bergengruen, V. (2024). *How Tech Giants Turned Ukraine into an AI War Lab*. [online] Time. Available at: <https://time.com/6691662/ai-ukraine-war-palantir/>.

Bob, J.J. (2023). *IDF Unit 8200 Commander Reveals Cyber Use to Target Hamas Commander*. [online] The Jerusalem Post | JPost.com. Available at: <https://www.jpost.com/israel-news/article-731443>.

Bondar, K. (2024). *Does Ukraine Already Have Functional CJADC2 Technology?* [online] Csis.org. Available at: <https://www.csis.org/analysis/does-ukraine-already-have-functional-cjadc2-technology>.

Burns, M. (2015). *Leaked Palantir Doc Reveals Uses, Specific Functions and Key Clients*. [online] TechCrunch. Available at: <https://techcrunch.com/2015/01/11/leaked-palantir-doc-reveals-uses-specific-functions-and-key-clients/>.

CIA (2009). *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis Prepared by the US Government*. [online] Available at: <https://www.cia.gov/resources/csi/static/Tradecraft-Primer-apr09.pdf>.

Colley, T. and Dylan, H. (2025). The War on Open-Source Intelligence. *The Washington Quarterly*, [online] 48(3), pp.147–162. doi: <https://doi.org/10.1080/0163660x.2025.2554477>.

Cooper, N.B. (2024). *AI and Intelligence Analysis: Panacea or Peril? - War on the Rocks*. [online] War on the Rocks. Available at: <https://warontherocks.com/2024/10/ai-and-intelligence-analysis-panacea-or-peril/>.

Dastin, J. (2023). Ukraine Is Using Palantir’s Software for ‘targeting,’ CEO Says. *Reuters*. [online] 2 Feb. Available at: <https://www.reuters.com/technology/ukraine-is-using-palantirs-software-targeting-ceo-says-2023-02-02/>.

Former Operative A (2025). *Confidential Interview*, conducted by Celi, S., 12 November. Location undisclosed.

Grylls, G. (2022). *Ukraine Is Outflanking Russia with Ammunition from Big Tech*. [online] Thetimes.com. Available at: <https://www.thetimes.com/uk/article/ukraine-is-outflanking-russia-with-ammunition-from-big-tech-lxp6sv3qz?t=1763345274770> [Accessed 17 Nov. 2025].

Harris, S. (2012). *Palantir Technologies Spots Patterns to Solve Crimes and Track Terrorists*. [online] Wired. Available at: <https://www.wired.com/story/joining-the-dots/>.

Heuer, R.J. (1999). *Psychology of Intelligence Analysis*. Washington, D.C.: Center for the Study of Intelligence, Central Intelligence Agency.

Ignatius, D. (2022). *Opinion | How the Algorithm Tipped the Balance in Ukraine*. [online] Washington Post. Available at: <https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/>.

Israeli Defense Forces (IDF) High Command (2024). *The IDF's Use of Data Technologies in Intelligence Processing*. [online] Israeli Defense Forces (IDF) Press Office, Government of the State of Israel. Available at: <https://www.idf.il/en/mini-sites/idf-press-releases-israel-at-war/june-24-pr/the-idfs-use-of-data-technologies-in-intelligence-processing/> [Accessed 17 Nov. 2025].

Kahneman, D. (2011). *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux.

Longo, L., Brcic, M., Cabitza, F., Choi, J., Confalonieri, R., Del Ser, J., Guidotti, R., Hayashi, Y., Herrera, F., Holzinger, A., Jiang, R., Khosravi, H., Lecue, F., Malgieri, G., Pérez, A., Samek, W., Schneider, J., Speith, T. and Stumpf, S. (2024). Explainable Artificial Intelligence (XAI) 2.0: A Manifesto of Open Challenges and Interdisciplinary Research Directions. *Information Fusion*, [online] 106(102301), p.102301. doi: <https://doi.org/10.1016/j.inffus.2024.102301>.

Lowenthal, M.M. (2020). *Intelligence : from Secrets to Policy*. 8th ed. Thousand Oaks, California: Cq Press.

Lucy Jo Palladino (2007). *Find Your Focus Zone*. Simon and Schuster.

Mimram, T., Pacholska, M. and Trabucco, L. (2024). *Israel – Hamas 2024 Symposium – Beyond the Headlines: Combat Deployment of Military AI-Based*

Systems by the IDF. [online] Lieber Institute West Point. Available at: <https://lieber.westpoint.edu/beyond-headlines-combat-deployment-military-ai-based-systems-idf> [Accessed 17 Nov. 2025].

Moran, C.R., Burton, J. and Christou, G. (2023). The US Intelligence Community, Global Security, and AI: from Secret Intelligence to Smart Spying. *Journal of Global Security Studies*, 8(2). doi: <https://doi.org/10.1093/jogss/ogad005>.

Nilsson, N., Weissmann, M. and Björn Palmertz (2025). Hybrid Threats and the Intelligence Community: Priming for a Volatile Age. *International Journal of Intelligence and CounterIntelligence*, pp.1–23. doi: <https://doi.org/10.1080/08850607.2024.2435265>.

Office of the Director of National Intelligence (ODNI) (2024). *The Aim Initiative A Strategy For Augmenting Intelligence Using Machines, Unclassified.* – ODNI. Available at: <https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf>.

Pacholska, M. (2022). Military Artificial Intelligence and the Principle of Distinction: a State Responsibility Perspective. *Israel Law Review*, 56(1), pp.1–21. doi: <https://doi.org/10.1017/s0021223722000188>.

Palantir.com. (2024). *Palantir and Ministry of Economy of Ukraine Sign Demining Partnership*. [online] Available at: <https://investors.palantir.com/news-details/2024/Palantir-and-Ministry-of-Economy-of-Ukraine-Sign-Demining-Partnership/>.

Schmitt, M.N. (2024). *Israel – Hamas 2024 Symposium - the Gospel, Lavender, and the Law of Armed Conflict - Lieber Institute West Point*. [online] Lieber Institute West Point. Available at: <https://lieber.westpoint.edu/gospel-lavender-law-armed-conflict/>.

Simon, H. (1956). Rational Choice and the Structure of the environment. *Psychological Review*, 63(2), pp.129–138. doi: <https://doi.org/10.1037/h0042769>.

Stryker, C. (2024). *Human in the Loop*. [online] Ibm.com. Available at: <https://www.ibm.com/think/topics/human-in-the-loop>.

Weinbaum, C. and Shanahan, J.N.T. (2018). *Intelligence in a Data-Driven Age*. [online] National Defense University Press. Available at: <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1566262/intelligence-in-a-data-driven-age/>.

Young, A. (2019). *Too Much Information: Ineffective Intelligence Collection*. [online] Harvard International Review. Available at: <https://hir.harvard.edu/too-much-information/>.