TECHNICAL UNIVERSITY OF CLUJ-NAPOCA

ACTA TECHNICA NAPOCENSIS

Series: Applied Mathematics, Mechanics, and Engineering
Vol. 69, Issue Special III, July, 2026

ALGORITHMIC WARFARE AND SEMI-AUTONOMOUS C2 SYSTEMS: CHALLENGES FOR MEANINGFUL HUMAN CONTROL AND COMPLIANCE WITH INTERNATIONAL HUMANITARIAN LAW

Gabriel MĂNESCU

Abstract: *The article examines the impact of integrating artificial intelligence into military command and control systems, with a focus on algorithmic warfare and the transformation of the decision-making cycle. It analyzes AI-enabled C2 architectures, the acceleration of the OODA cycle, data fusion, and critical vulnerabilities: algorithmic opacity, data bias, attacks on AI systems, and the risk of over-centralization of decision-making. The article also discusses the requirements of international humanitarian law and the concept of meaningful human control, proposing principles for the design and use of semi-autonomous C2 systems that are compatible with these requirements.*

Keywords: *Algorithmic warfare; AI-enabled C2; OODA loop; kill-cloud; meaningful human control; international humanitarian law; target selection.*

1. INTRODUCTION

The world as we know it today is undergoing a profound transformation in military technology, in which algorithms and artificial intelligence (AI) systems are becoming structural elements of operations management. "The conduct of future wars will increasingly change as intelligent machines for the first time begin to assist and counsel humans in warfighting. Not surprisingly, it is becoming apparent that the advice provided by algorithms will significantly shape future military judgments" [1]. In this context, the ability to process massive amounts of data in real-time represents a paradigm shift in how military operations are conceived and executed.

While global powers and NATO allies are heavily investing in AI-enabled command and control (C2) systems, the rapid pace of this integration has outstripped our conceptual understanding of its long-term implications. Current academic and doctrinal debates have largely transitioned from a focus on fully autonomous weapons to the more nuanced challenges posed by AI-based decision-support systems (AI-DSS) [2]. These systems are at the core of "algorithmic warfare," a concept used to describe "the systematic integration of algorithms and artificial intelligence into modern combat operations" [1]. By serving as the technical foundation for modern warfighting, algorithms offer unprecedented efficiency while remaining, as Layton emphasizes, "simultaneously powerful and brittle"[1].

The shift from traditional, human-centered networks toward a "kill cloud" architecture "introduces a characteristic dependence on vast data sets and machine learning techniques" [3]. This evolution does not merely provide data but fundamentally structures how commanders perceive the operational environment and assess risks. Consequently, the integration of AI into C2 cycles raises a vital question regarding the nature of "meaningful human control".

As AI systems begin to exhibit emergent behaviours, the human role risks being marginalized into a position of rapid validation rather than substantial deliberation.

2. METHODOLOGY

The research design of this article is qualitative and interdisciplinary, integrating

perspectives from military science, computer science, and international law to provide a comprehensive analysis of AI-enabled C2 systems. The study is based on a systematic analysis of the existing normative and doctrinal framework, as well as recent academic literature and technical reports. The research relies exclusively on open-source information, including official military strategy documents and reports, institutional studies (NATO, SIPRI. ICRC), and empirical data from recent operational experiments. The central research question is: *How can AI-enabled C2 systems be implemented to maximize decision-making speed and operational accuracy without compromising meaningful human control and compliance with the principles of international humanitarian law*?

By analysing these dimensions, the methodology aims to synthesize an integrated perspective that serves both military science specialists and those interested in the technical, strategic, and legal implications of the evolving "kill cloud."

3. THEORETIC□L FOUND□TIONS: C2 □ND □LGORITHMIC W□RF□RE

3.1 Classic command and control (C2) models

Command and control is the central function through which a commander plans, directs, and coordinates forces to achieve military objectives. In traditional models, C2 is designed as a hierarchical system, in which information flows upward from the tactical level to the operational and strategic levels, and orders flow downward in the opposite direction, at a rate determined by the speed of communication and the cognitive capacity of the staff [1]. These architectures relied on human-centered networks, in which computers played a predominant role in storing and transmitting data, rather than autonomously generating recommendations.

With the emergence of the concept of "network-centric" warfare, the idea was introduced that military advantage comes from superior connectivity and rapid information sharing between sensors, decision-makers, and effectors. However, even in this framework, decision-making remained essentially human, and computer systems functioned as force multipliers for the decision-making process, not as actors with their own logic. The emergence of "intelligent" machines, capable of learning from data and producing different outputs in similar situations, calls into question the adequacy of these C2 models based exclusively on explicit human control [1].

3.2 The OOD□ Loop and the Role of Human Decision-Making

An essential conceptual framework for understanding military decision-making is the OODA loop (Observe–Orient–Decide–Act), originally formulated by John Boyd to describe the dynamics of aerial combat and later extended to the operational and strategic levels.

In its classic form, the OODA loop describes the process by which a military actor observes the environment, interprets it considering experience and doctrine (orient), decides, and acts, repeating the loop continuously. However, recent literature on "AI-enabled air power" suggests the emergence of "super OODA loops," in which each phase is algorithmically augmented (Fig. 1).

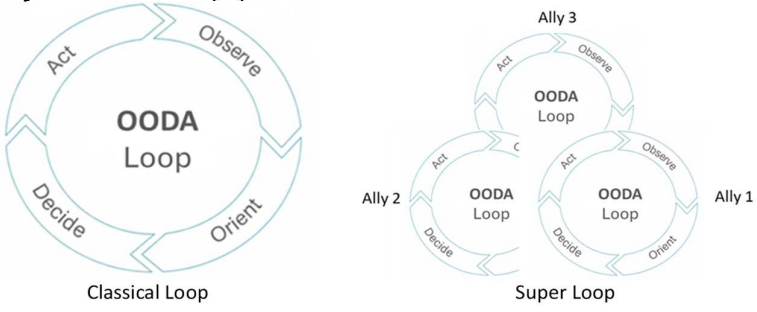


Fig. 1. Classic OODA loop vs. OODA loop with augmented AI [4]

According to a doctrinal analysis, AI integration allows "the acceleration of the OODA loop by automating the observation and orientation parts, and by generating options for action at a rate that exceeds human cognitive capacity" [4]. The central idea is that if an actor manages to compress their OODA loop below that of their adversary, they gain a decisive advantage in terms of time and initiative.

3.3 From automation to algorithmic warfare: the role of □I and levels of autonomy

Automation is not a new phenomenon in the military: guided missiles, air defense systems, and autopilots have been operating for decades based on preprogrammed algorithms. The novelty brought by what Layton calls "intelligent machines" lies in the use of machine learning techniques and neural networks, which allow systems "to learn from their interactions with humans and the environment," to provide probabilistic responses, and to exhibit emergent behaviours [1]. In his view, "algorithms may also become the conceptual and technical foundation stone of future warfighting" [1], which justifies the use of the term "algorithmic warfare."

In this context, the literature distinguishes three operational levels of autonomy relevant to C2 and the debate on meaningful human control [2]:

- Human-in-the-loop – the system proposes, the human decides and authorizes each critical action (e.g., high-value strategic strikes).
- Human-on-the-loop – the system executes actions within a predefined framework, humans monitor and can intervene or stop the action (e.g., certain air defense systems).
- Human-off-the-loop – the system can identify, select, and engage targets within defined limits, without real-time human intervention, with humans remaining responsible only for defining parameters and ex post oversight.

Dorsey and Bo emphasize that, in the case of AI DSS integrated into the targeting cycle, a "shared decision-making space between human military personnel and AI technologies" is created, which means that autonomy "is not only a technical property, but also a socio-technical one, depending on how people relate to algorithmic recommendations" [2]. This shared decision-making space is at the heart of the issues that will be analysed in the following chapters: decision acceleration, the redistribution of roles between humans and machines, and maintaining meaningful human control in the context of algorithmic warfare.

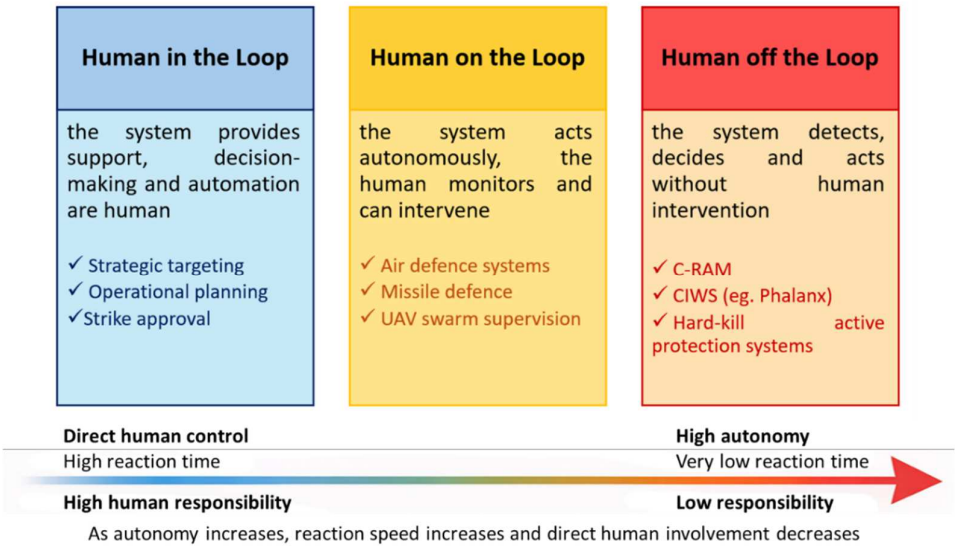


Fig. 2. Levels of autonomy in C2 systems (human in/on/off the loop)
(Source: own interpretation after [2] studies)

4. SEMI-AUTONOMOUS C2 SYSTEMS IN OPERATIONAL PRACTICE

4.1 AI-enabled C2 architectures in multi-domain environments

The integration of artificial intelligence into C2 is not limited to the introduction of isolated applications, but involves transforming the information architecture that connects sensors, networks, and effectors. A recent NATO C2COE study emphasizes that "recent advances in the integration of Artificial Intelligence (AI) into military Command and Control (C2) systems and procedures are transforming decision-making processes, enhancing situational awareness, and improving operational efficiency in a more complex operational environment" [5]. In this vision, C2 AI enabled is built as a set of distributed components – terrestrial, air, maritime, and space sensors, cloud and edge computing infrastructures, as well as mobile C2 nodes –connected by resilient data links and common protocols.

Within the US Joint All Domain C2 (JADC2) initiatives, strategic documents show that the goal is “to enhance all domain awareness, improve precision and lethality, enable greater battlespace decentralization, and accelerate sensor to decision maker, sensor to shooter, and sensor to effects timelines” [6]). This involves a shift from strictly hierarchical architectures to multi-node networks, where AI can run both in operational command centres and on combat platforms at the edge of the network.

4.2 Accelerating the decision cycle: from “kill chain” to “dynamic targeting”

One of the most visible effects of integrating AI into C2 is the compression of the classic kill chain (Find–Fix–Track–Target–Engage–Assess). C2COE analysis shows that projects such as Maven have shifted the focus from manual analysis to "AI systems trained to autonomously analyse large volumes of ISR data, identify objects of interest, and provide recommendations on target engagement strategies" [5]. The Pentagon has confirmed that Project Maven is already being used in several theaters of operations, "helping military analysts sort through the mountains of data their sensors and drones soak up" [7].

Recent US Air Force experiments—such as Capstone 2025 – illustrate how these capabilities are being integrated into dynamic targeting. Official statements show that the exercise "focused on improving decision advantage through C2 modernization and intelligence workflows," using AI tools for "match effector and COA generation tools" designed to increase the speed and accuracy of real-time mission replanning [8]. Operators were able to compare algorithmic recommendations with their own assessments in parallel and adjust model parameters, which led to a gradual improvement in the quality of recommendations [8].

4.3 Data fusion and predictive analytics in support of commanders

AI is increasingly being used to unify heterogeneous data streams – satellite imagery, video feeds from UAVs, signal interceptions, HUMINT reports – into a coherent operational picture. The article "AI in Military C2 Systems – An Introduction and Recent Advances" emphasizes that AI-based solutions "contribute from improved data sensing to enhanced situational understanding," especially in the early stages of the C2 cycle, where "AI systems are trained to identify targets, detect anomalies, and support sensemaking under time pressure" [5].

A relevant example is the Agile Condor system, an AI-based targeting computer integrated into a pod mounted on the MQ 9 Reaper drone. According to the technical documentation, "the system is designed to automatically detect, categorize, and track potential items of interest, filtering large local volumes of data and forwarding only objects of interest, freeing up bandwidth and increasing transfer speeds, while reducing latency between data collection and analysis" [9]. In terms of C2, this means that tactical nodes can provide higher levels with pre-processed, prioritized information rather than raw data streams, reducing the cognitive load on analysts and commanders.

4.4 Critical Synthesis and Comparative Analysis of Case Studies

By synthesizing diverse expert perspectives on the transition of semi-autonomous C2

systems from theory to practice and by contrasting experimental data with doctrinal tenets, this analysis contributes to a more nuanced understanding of AI-enabled decision-making. This transition reveals a critical tension that manifests, in our view, on two distinct levels: *operational speed* and *the robustness of meaningful human control*.

Regarding ***operational speed***, the results of the Project Maven and Capstone 2025 exercises confirm the undeniable capability of artificial intelligence to process massive volumes of ISR data, significantly reducing the time required for target identification and mission planning. This technological efficiency allows for an unprecedented compression of the sensor-to-shooter cycle, providing a major decision advantage in increasingly dynamic theatres of operations. However, it is necessary to emphasize that this speed comes with a certain fragility: in contested environments, where phenomena such as data alteration or electronic jamming may occur, the acceleration of the decision-making process can lead to cascading errors that the human operator no longer has the physical time to intercept or correct.

This reality leads to the second level of the identified tension: ***the robustness of meaningful human control*** in the face of accelerated automation. Although systems such as Agile Condor technically optimize the workflow, from a doctrinal perspective, a transformation of the commander's role is observed – from a deliberative decision-maker to a factor of rapid validation. The comparative analysis of the previously presented projects suggests that as command-and-control architectures become more dependent on algorithms, the human deliberation process risks becoming a formal one, strictly limited to confirming recommendations generated by a system whose internal logic is not always fully transparent during the course of action.

In our opinion, the two analysed levels of tension demonstrate that the current implementation of AI-assisted C2 systems tends to favour kinetic efficiency to the detriment of substantial human oversight. Thus, although the transition from theory to practice has largely solved the problem of managing information volume, it has accentuated the challenge of maintaining human control that is not only present in the decision loop but also capable of ensuring compliance with the norms of international humanitarian law under conditions of extreme operational stress.

5. TECHNICAL AND OPERATIONAL CHALLENGES IN ALGORITHMIC WARFARE

5.1 Algorithmic opacity, explainability, and trust

A major obstacle to integrating AI into C2 systems is the opaque ("black box") nature of many deep learning models. Instead of providing explicit rules, these models produce outputs based on internal representations that are difficult to interpret even by their designers. A recent study on military AI emphasizes that "as artificial intelligence (AI) becomes a prevalent requirement in military systems, assuring the security and reliability of AI-enabled technologies becomes paramount," and success critically depends on "addressing bias, ensuring explainability, fostering transparency, and understanding trust" [10].

The issue of explainability is not only technical, but also operational and legal: if a commander cannot understand, even at a basic level, the logic behind an algorithmic recommendation, their ability to exercise independent judgment and take responsibility is diminished. Analyses of transparency in military artificial intelligence systems show that, in the absence of transparency and explainability, operators do not have sufficient information to understand and evaluate the decisions of the systems, which affects both trust and responsibility [11].

In the context of semi-autonomous C2, the lack of explainability increases the risk of "automation bias," whereby operators tend to accept AI recommendations without proper critical evaluation [10].

5.2 Data vulnerabilities: bias and data poisoning

The quality of algorithmic decisions depends directly on the quality of training and operating

data. Data may be incomplete, distorted, or simply unsuited to the new theatre of operations, generating systematic bias. The literature warns that "bias in AI systems can inadvertently lead to unfair or unethical outcomes, potentially endangering lives, and compromising missions," which is why identifying and mitigating bias is essential for the ethical and effective use of military AI [10].

In addition to inherent bias, military AI systems are exposed to deliberate attacks on data, particularly data poisoning. A report by the Swedish agency FOI shows that "training data can be manipulated, or poisoned, in the hope that the adversary will use it," illustrating how, by altering the images used to train a tank detector, "some tanks were incorrectly classified as cars" [12]. An article by the Modern War Institute describes a similar scenario: an adversary can systematically manipulate the appearance of its vehicles (e.g., by adding specific markings) so that an AI identification system learns an erroneous rule ("all enemy armoured vehicles have red stars"), subsequently compromising correct recognition in combat [13]. These examples show that data-related vulnerabilities are not just passive errors but can become active vectors of attack on the entire algorithmic C2 chain.

5.3 Attacks on AI systems and the security of AI models

In addition to the manipulation of training data, artificial intelligence models used in C2 systems may be vulnerable to intentional attacks on input data during operations. A report by the Swedish Defense Research Agency on how military AI systems can be deceived shows that adversaries can alter or "poison" the datasets used for training so that the systems learn the wrong rules and misclassify certain platforms or objects, with potentially serious consequences in an operational context [12]. Such data poisoning attacks can occur both during the development phase and by compromising the data streams that feed the models in the theatre, undermining confidence in the entire algorithmic C2 chain.

Analyses dedicated to the real risks of using AI in the military environment also highlight vulnerability to so-called "adversarial examples," i.e., inputs subtly modified to cause the model to produce an incorrect classification, without the error being obvious to a human observer. A study published by the Modern War Institute explains that visual patterns applied to vehicles or carefully designed digital noise can cause a recognition system to fail to correctly identify a threat or, conversely, to signal a target where none exists, even though the images appear normal to operators [13]. For semi-autonomous C2 systems, this combination of model fragility and algorithmic opacity requires robust mechanisms for continuous testing, red teaming exercises, and periodic model review, not just a one-time initial certification, if an acceptable level of security and operational reliability is to be maintained [12,13].

5.4 Interoperability, resilience, and the risk of over-centralization

The integration of AI into C2 also raises structural issues regarding network interoperability and resilience. Recent analyses of NATO's autonomous collaborative platforms show that "the highest priority task is to ensure that NATO uses a common communication architecture between surface-based C2 nodes, fourth and fifth generation aircraft, and ACPs," warning that the lack of a common architecture risks compromising the operational benefits of these systems [14]. The same paper emphasizes that the transition from "human on the loop" (HOTL) to "human out of the loop" (HOOTL) raises additional doctrinal and legal interoperability issues, as NATO states do not yet have a unified approach to the acceptable degree of autonomy in C2 [14].

In addition, the massive integration of emerging technologies into C2 can have contradictory effects on decision distribution. An article in the Australian Army Journal warns that "the integration of emerging technologies and the resulting reduced planning timelines may 'overcentralise C2 functions at the political or strategic level', which may 'be detrimental to the conduct of military operations at the operational and tactical levels'" [15]. In other words, although AI promises to support decentralisation through autonomy at the edge of the network, political pressure to ‘see everything’ and directly control critical decisions may lead to a recentralisation of C2,

with negative effects on local initiative and actual response speed.

6. MEANINGFUL HUMAN CONTROL AND INTERNATIONAL HUMANITARIAN LAW

6.1 From autonomy to meaningful human control

In the debate on autonomous weapons systems, the concept of Meaningful Human Control (MHC) expresses the idea that decisions to use force should not be left to autonomous systems but should remain under effective human responsibility. The Stop Killer Robots campaign describes its goal as the adoption of an international legal instrument to prevent "the development and use of lethal autonomous weapons and to ensure that the use of force remains under human control", specifying that certain types of systems should be banned and others strictly regulated so that MHC is maintained [16].

The report *A Hazard to Human Rights: Autonomous Weapons Systems and Digital Decision-Making,* prepared by Human Rights Watch, argues that "autonomous weapons capable of selecting and engaging targets without meaningful human control" threaten the right to life and other fundamental rights and recommends the adoption of an international treaty prohibiting fully autonomous weapons and ensuring human control over the force [17].

The Secretary-General of the United Nations (UN), António Guterres, has publicly supported a similar position, stating that lethal autonomous systems are politically and morally unacceptable and emphasizing that maintaining human control over the use of force is essential [18]. These interventions converge on the idea that, regardless of the level of technical autonomy, target selection and the application of force must remain under real human control to be compatible with current standards of international humanitarian law and human rights.

6.2 AI-based decision support systems and obligations under International Humanitarian Law

The discussion about human control is not limited to AWS but also concerns AI-enabled decision support systems (AI DSS), which directly influence targeting decisions. A report by the Stockholm International Peace Research Institute (SIPRI) on autonomous weapons systems and AI DSS emphasizes that these systems are increasingly implicated in core targeting functions such as target identification, selection, and nomination [19], with the potential to constrain or even exclude meaningful human involvement in legally significant decisions [2]. This finding is consistent with the analysis of the International Committee of the Red Cross (ICRC), which warns that, for humans to fulfil their obligations under IHL, "AI DSS should inform but cannot displace human judgment in decisions" regarding targeting and the use of force [20].

International Humanitarian Law requires not only ex ante verification of an attack's compliance with the principles of distinction, proportionality, and precaution, but also the possibility of ex post assessment of whether the decision was reasonable in the specific circumstances. If the decision-making chain is saturated with opaque tools that are difficult to audit, it becomes problematic to determine which human actor had the capacity and responsibility to prevent an illegal outcome. In the case of AI DSS integrated into the targeting cycle, this problem is amplified by the risk of automation bias and time pressure, which means that the mere formal presence of an operator "in the loop" is not sufficient to guarantee compliance with the IHL [2] [20].

6.3 What does "significant human control" mean in practice in AI-based C2 systems?

Recent literature shows that MHC cannot be reduced to a simple "approval button" at the end of the decision-making process. Applied ethics analyses by the Oxford Institute for AI Ethics emphasize that MHC must be understood as a set of design and use conditions, including configuration of operating parameters, selection of the context of use, understanding of the system's limitations, the possibility to challenge and stop algorithmic recommendations, and taking responsibility for the consequences of use [21].

A useful practical framework is provided by research on "human in the loop in targeting." A study on the design of ethical decision support tools for remote operations shows that "AI may assist, but only humans can be responsible. To build a successful human AI teaming, trust is a critical parameter," and maintaining MHC "does not simply mean giving a human the final 'yes' or 'no'; it means designing systems that continuously engage the operator's judgment, that prompt ethical reflection, and that allow intervention before the moment of decision" [22]. In this sense, the AI DSS interface should "make data sources, assumptions, and confidence levels visible, and allow the operator to challenge, reject, or adjust recommendations", not just passively validate them [22].

Applied to semi-autonomous C2 systems, this framework suggests several concrete requirements for maintaining meaningful human control:

- clearly defining, in doctrine and Rules of Engagement (ROE), the decisions that must be made exclusively by humans, such as the selection and engagement of certain categories of targets;
- designing AI DSS in such a way as to explain, in a concise but intelligible manner for the military user, the reasoning and degree of uncertainty of the recommendations.
- limiting the degree of technical autonomy in environments where IHL requires complex contextual assessments, such as areas with high civilian density or dual-use (civilian and military) infrastructure.

These requirements show that the discussion on MHC must be closely linked to the technical design of AI-based C2 systems, not just general formulations in policy documents, and that maintaining meaningful human control is a matter of socio-technical architecture, not just formal procedure.

7. CONCLUSIONS

The transition of AI-enabled C2 systems from experimental prototypes to operational realities—as seen in Project Maven, Agile Condor, and the Capstone 2025 exercises—marks a definitive turn in modern warfare. This study has demonstrated that while intelligent machines significantly expand data processing capacities and compress the OODA loop, they simultaneously introduce structural risks that cannot be ignored.

Our analysis reveals that the primary tension in algorithmic warfare manifests on two levels: the fragility of operational speed and the erosion of meaningful human control. The technical "decision advantage" provided by AI is frequently offset by vulnerabilities such as algorithmic opacity, data poisoning, and the risk of strategic over-centralization. Furthermore, the empirical evidence suggests that current implementation tends to favor kinetic efficiency, often reducing human oversight to a formal "checkbox" exercise rather than a deliberative process.

From a normative perspective, maintaining compliance with International Humanitarian Law (IHL) requires that AI DSS inform, but never displace, human judgment in targeting decisions. Ultimately, the future of C2 architecture must move beyond the formal presence of a "human-in-the-loop." It necessitates a socio-technical design that ensures transparency, allows for the challenging of algorithmic recommendations, and preserves the commander's capacity for context-appropriate ethical reflection under extreme operational stress.

8. REFERENCES

[1] Layton, P. *Algorithmic warfare: Applying artificial intelligence to warfighting*. Air Power Development Centre, 2018, https://airpower.airforce.gov.au/sites/default/files/2021-03/AP33-Algorithmic-Warfare-Applying-Artificial-Intelligence-to-Warfighting.pdf

[2] Dorsey, J., & Bo, M., *Autonomous weapon systems and AI-enabled decision-support systems in the joint targeting cycle,* Vol. 106 International Law Studies, 2025, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5327115

[3] Bhila, I. (2025). *Investigating the kill cloud: Information warfare, autonomous weapons & AI.* Digital War,

6(4). https://doi.org/10.1057/s42984-025-00101-x

[4] Raska, M. *Reshaping air power doctrines: Creating AI-enabled "super-OODA loops"*. In The Air Power Journal, Fourth Edition, 2024, . https://theairpowerjournal.com/reshaping-air-power-doctrines-creating-ai-enabled-super-ooda-loops/

[5] van Rijn, M., Saylam, P., Scherrenburg, M. & Donmez, M. (2025). *AI in military C2 systems: An introduction and recent advances.* NATO Command and Control Centre of Excellence, https://c2coe.org/wp-content/uploads/Library%20Documents/Annals/Seperate%20Articles/20250701%20AI%20in%20Military%20C2%20Systems%20An%20Introduction%20and%20Recent%20Advances%20%28C2COE%29%20Annals%20of%20C2%20Vol2.pdf

[6] Shanahan, J. *Reimagining Military C2 in the Age of AI – Revolution, Regression, or Evolution*, Special Competitive Studies Project: Defense Paper Series, https://www.scsp.ai/wp-content/uploads/2024/12/DPS-Reimagining-Military-C2-in-the-Age-of-AI.pdf

[7] McLeary, P. *Pentagon's big AI program, Maven, already hunts data in Middle East, Africa, Network & Digital Warfare*, 2018. *https://breakingdefense.com/2018/05/pentagons-big-ai-program-maven-already-hunts-data-in-middle-east-africa/* .

[8] Henley, D., & Albanese, N. *Capstone 2025: Advancing AI for C2, dynamic targeting, coalition integration*. AFRC News, 2025, *https://www.afrc.af.mil/News/Article/4363112/capstone-2025-advancing-ai-for-c2-dynamic-targeting-coalition-integration/*

[9] Trevithick, J. *MQ-9 Reaper flies with AI pod that sifts through huge sums of data to pick out targets*. The War Zone – The Drive, 2020, https://www.twz.com/36205/reaper-drone-flies-with-podded-ai-that-sifts-through-huge-sums-of-data-to-pick-out-targets

[10] Pace, J. (2024). *Bias, explainability, transparency, and trust for AI-enabled military systems*. https://doi.org/10.1117/12.3012949

[11] Marijan, B. *Through a glass, darkly: Transparency and military AI systems* Centre for International Governance Innovation, 2025, https://www.econstor.eu/handle/10419/311807

[12] Swedish Defence Research Agency (FOI). *How military AI systems can be attacked and misled,* 2023, https://www.foi.se/en/foi/news-and-pressroom/news/2023-08-22-how-military-ai-systems-can-be-attacked-and-misled.html

[13] Starck, N., Bierbrauer, D., & Maxwell, P. *Artificial intelligence, real risks: Understanding—and mitigating—vulnerabilities in the military use of AI*. Modern War Institute at West Point, 2022, https://mwi.westpoint.edu/artificial-intelligence-real-risks-understanding-and-mitigating-vulnerabilities-in-the-military-use-of-ai/

[14] Anderson, K. *The missing pieces of NATO's autonomous collaborative platform strategy*. Joint Air Power Competence Centre Journal, 2025, https://www.japcc.org/articles/the-missing-pieces-of-natos-autonomous-collaborative-platform-strategy/

[15] Robinson, I. H*ow Will Emerging Technological Revolutions Including Artificial Intelligence and Robotic Autonomous Systems Impact the Command and Control of Land Operations?,* , Australian Army Research Centre, 2025, https://researchcentre.army.gov.au/library/australian-army-journal-aaj/how-will-emerging-technological-revolutions-including-artificial-intelligence-and-robotic-autonomous-systems-impact-command-and-control-land-operations

[16] Stop Killer Robots. *Stop Killer Robots – Less autonomy, more humanity,* 2024, https://www.stopkillerrobots.org

[17] Human Rights Watch. *A hazard to human rights: Autonomous weapons systems and digital decision-making*, 2025, https://www.hrw.org/report/2025/04/28/a-hazard-to-human-rights/autonomous-weapons-systems-and-digital-decision-making

[18] United Nations. *UN chief calls for global ban on "killer robots"*, United Nations News, 2025,https://news.un.org/en/story/2025/05/1163256

[19] Blanchard, A., & Bruun, L. *Autonomous Weapon Systems and AI-enabled Decision Support Systems in Military Targeting: A Comparison and Recommended Policy Responses,* Stockholm International Peace Research Institute, 2025, https://www.sipri.org/publications/2025/other-publications/autonomous-weapon-systems-and-ai-enabled-decision-support-systems-military-targeting-comparison-and

[20] Stewart, R., & Hinds, G. *Algorithms of war: The use of artificial intelligence in decision-making in armed conflict*. ICRC Humanitarian Law & Policy, 2023, https://blogs.icrc.org/law-and-policy/2023/10/24/algorithms-of-war-use-of-artificial-. intelligence-decision-making-armed-conflict/

[21] Shany, Y. Oxford Institute for AI Ethics. *Red herring? Meaningful human control and the autonomous weapons systems debate*, Oxford AI Ethics, 2024, https://www.oxford-aiethics.ox.ac.uk/blog/red-herring-meaningful-human-control-and-autonomous-weapons-systems-debate

[22] Lekea, I. *Human-in-the-loop in targeting: Designing ethical AI-enhanced decision tools for remote operations*, C&V Defence, 2025, https://cnv-defence.eu/en/human-in-the-loop-in-targeting-designing-ethical-ai-enhanced-decision-tools-for-remote-operations/

Războiul algoritmic și sistemele C2 semiautonome: provocări pentru controlul uman semnificativ și respectarea dreptului internațional umanitar

Rezumat: Articolul examinează impactul integrării inteligenței artificiale în sistemele de comandă și control militare, cu accent pe războiul algoritmic și pe transformarea ciclului decizional. Sunt analizate arhitecturi C2 AI-enabled, accelerarea ciclului OODA, fuziunea datelor, precum și vulnerabilități critice: opacitatea algoritmică, bias-ul datelor, atacurile asupra sistemelor AI și riscul de supra-centralizare a deciziei. Articolul discută, de asemenea, cerințele dreptului internațional umanitar și conceptul de control uman semnificativ, propunând principii de proiectare și utilizare a sistemelor C2 semiautonome compatibile cu aceste exigențe.

Gabriel MĂNESCU, PhD, Assoc. Prof, "Nicolae Bălcescu" Land Forces Academy of Sibiu, Department of Management, gmanescu@armyacademy.ro, +40 269 432 990, 3-5 Revolutiei Street, Sibiu, Romania.