

DEFEATING ADVERSARY A2/AD SYSTEMS THROUGH THE SYNERGISTIC EFFECTS OF CROSS-DOMAIN FIRES

Iulian-Radu MONORANU

“Carol I” National Defense University, Bucharest, Romania
“Nicolae Bălcescu” Land Forces Academy, Sibiu, Romania
monoranu.radu@armyacademy.ro

Gheorghe MINCULETE

“Nicolae Bălcescu” Land Forces Academy, Sibiu, Romania
minculete.gheorghe@armyacademy.ro

ABSTRACT

A2/AD systems cannot be countered through the action of a single operational domain or a single platform, but rather through the disruption of the adversary's system-of-systems by means of synchronized cross-domain fires designed to generate systemic paralysis, operational shock, and “windows of superiority” that enable joint forces to regain freedom of maneuver. Based on a mixed qualitative and quantitative methodological design, this article highlights the quantification of the impact of multi-domain fires convergence on the effectiveness of engaging critical elements of A2/AD architectures, such as Integrated Air Defense Systems (IADS), Long-Range Precision Fires (LRPF) complexes, and command-and-control (C2) centers. The results demonstrate that defeating A2/AD systems requires a conceptual transition from sequential engagement models toward dynamic joint kill-webs, supported by artificial intelligence-enabled targeting automation and resilient, collaborative command-and-control (C2) architectures.

KEYWORDS: A2/AD, cross-domain fires, multi-domain operations, sensor-to-shooter, convergence.

Submission Received: 14 April 2026; **Revised:** 19 May 2026;
Accepted: 20 May 2026; **Published:** June 2026

1. Introduction

The return of large-scale conventional warfare and the intensification of competition among peer adversaries have fundamentally transformed the operational environment, particularly through the proliferation of anti-access/area denial (A2/AD) systems by China and the Russian Federation, the principal competitors of the Western powers. These systems are designed to prevent an adversary from

gaining access to a theater of operations (anti-access/A2) and to restrict freedom of maneuver within the theater itself (area denial/AD), primarily through integrated air and missile defense systems, long-range precision fires, electronic warfare, cyber operations, maritime denial capabilities, and reconnaissance systems supported by space-based assets (FM 3-0, 2025, p. 33).

Modern conflicts demonstrate that the battlespace has become increasingly

contested, congested, and highly transparent as a result of the proliferation of sensors, unmanned systems, satellite reconnaissance, and digital communications, all of which significantly accelerate the targeting cycle and increase the lethality of long-range fires (Black et al., 2024). The ongoing wars in Ukraine and the Middle East have highlighted the growing importance of long-range precision fires, unmanned systems, electronic warfare, and integrated targeting networks in modern warfare, emphasizing the inherently multi-domain character of contemporary operations. In response to these challenges, Western military doctrines place increasing emphasis on the concept of Multi-Domain Operations (MDO), which seeks to integrate land, air, maritime, cyber, space, electromagnetic, and even informational capabilities in order to generate convergent effects against adversary systems.

The objective of this research is to analyze the manner in which the synergistic effects generated by cross-domain fires can be exploited to counter adversary A2/AD systems, as well as to identify the doctrinal principles, capabilities, and integration mechanisms required for the conduct of such operations. To achieve this objective, the research was guided by two principal questions:

(1) Through which multi-domain mechanisms are synergistic effects generated against adversary A2/AD systems?

And

(2) What are the efficiency conditions of the sensor-to-shooter cycle necessary to ensure the successful countering of these integrated defensive systems?

The study employs a mixed methodology combining qualitative analysis of doctrinal documents and lessons learned from recent conflicts with quantitative data gathered through direct observation during the multinational exercise Dynamic Front 26. As a major U.S.-led artillery and fires interoperability

exercise, Dynamic Front 26 serves as a contemporary testing ground for NATO's ability to coordinate lethal and non-lethal effects, counter A2/AD challenges, and strengthen operational readiness in a multinational and multi-domain environment. Participation in the exercise provided direct insight into the relevant concepts and processes, while also enabling the collection of current, reliable, and operationally relevant data for the research.

The paper demonstrates that the decisive factor in countering A2/AD systems is not superiority within a single domain, but rather the synchronization and convergence of cross-domain effects aimed at restoring freedom of maneuver and facilitating the successful conduct of joint operations. The findings indicate that the synergistic integration of kinetic effects (precision artillery and missile fires, air support, First Person View/FPV drones, and loitering munitions) with non-kinetic effects (electronic warfare and cyber operations) produces an exponential, rather than linear, increase in the performance of the joint multi-domain force structure. Furthermore, the data reveal a substantial acceleration of the decision-making process, significantly reducing the "sensor-to-shooter" (S2S) cycle time against critical nodes of the adversary's A2/AD system, including IADS, LRPF systems, C2 networks, and operational logistics infrastructure. The ability to integrate fires and effects across all domains constitutes a decisive factor in modern warfare and an essential condition for restoring the freedom of maneuver of forces operating in contested environments.

2. Conceptual Framework of A2/AD Systems

A2/AD strategies were conceived as asymmetric response formulas developed by the principal anti-Western rivals, the Russian Federation and China, in reaction to the technological superiority and operational successes demonstrated by the armed forces of the United States and the

other members of the North Atlantic Treaty Organization/NATO in military engagements following the end of the Cold War. Seeking to re-establish themselves as peer competitors, these adversaries identified as such in Allied national defence strategies (US Department of War, 2026), have focused on developing integrated and multi-layered long-range engagement capabilities designed to deter approach and to establish so-called “A2/AD bubbles”. The ultimate purpose of these systems is to create, against NATO forces, the *“inability to come into direct contact with the enemy, destroy him, seize and secure terrain, and subsequently consolidate gains”* (Dwight, 2023, p. 2).

The arguments advanced by the Russian Federation are linked to the necessity of creating a buffer zone aimed at protecting its sphere of influence and countering the eastward expansion of

NATO (Chiorcea, 2024). Recognizing its limitations in competing NATO during a potential large-scale conventional conflict, the Russian Federation adopted a strategy oriented toward asymmetric compensation, investing significantly in the development and deployment of long-range strike systems. Consequently, capabilities such as Iskander ballistic missiles, S-400 air defence systems, and Kalibr cruise missiles are integrated into a complex A2/AD architecture designed to target and neutralize critical nodes of the adversary’s military and logistical infrastructure, including ports, airfields, and C2 centers (see Figure no. 1).

The primary purpose of this approach is to delay or disrupt the deployment of Allied reinforcements, thereby limiting NATO’s capacity for rapid reaction and force projection in strategically significant areas (Erdogan, 2018).



Figure no 1: Key Components of Russian and Chinese A2/AD Networks
(Source: Authors’ concept created using NotebookLM AI tool)

China justifies its A2/AD strategies, developed even prior to those of the Russian Federation, through the lessons learned from the Taiwan Strait Crisis (1995-1996), the Western operational successes of the conflicts of the 1990s, the objective of controlling the South China Sea, and the necessity of neutralizing aircraft carriers entering the Indo-Pacific region. The development of Chinese A2/AD capabilities has involved substantial investments in air platforms, advanced

surface-to-air systems, and naval modernization; however, the primary effort has focused on the advancement of precision-guided ballistic missiles. China is assessed as possessing one of the most advanced ballistic missile forces globally, capable of overwhelming U.S. missile defence systems. Systems such as the DF-41 (intercontinental ballistic missile), the DF-26, known as the “Guam killer” (intermediate-range missile), and the DF-21D, commonly referred to as the

“carrier killer” (anti-ship ballistic missile), directly support the objectives of the A2/AD strategy by enabling strikes against both land and maritime targets at extended ranges, thereby limiting the adversary’s capacity for power projection.

China also excels through the implementation of cutting-edge technologies in military equipment, including drones and autonomous systems, aerospace vehicles, anti-satellite weapons, and sophisticated electronic warfare and cyber capabilities. These capabilities complement one another in creating a layered A2/AD defence architecture and generating a significant decision-making advantage (see Figure no. 1). Simultaneously, the expansion of military infrastructure on artificial islands in the South China Sea strengthens China’s strategic posture and intensifies the operational challenges faced by the United States and its allies.

It is evident that the A2/AD architectures developed by these adversaries are based not only on ballistic and cruise missile systems, anti-ship strike capabilities, and modern integrated air and missile defence systems, but also on multi-layered ISR capabilities (largely supported

by the employment of UAS), advanced electronic warfare capabilities, and cyber-attack instruments relevant to the disruption of C2 systems and critical infrastructure (Dalsjo et al., 2019).

The electromagnetic and informational domains are becoming increasingly contested through interference operations and attacks against communication and data networks, spoofing activities, disinformation campaigns, and efforts aimed at undermining trust. Collectively, these actions are intended to reduce the speed and effectiveness of the detect–decide–engage–assess/D3A targeting cycle. (NATO.int, 2024).

A2/AD systems must therefore be understood as a “system of systems”, like an integrated architecture of sensors, C2 elements, kinetic and non-kinetic effectors, together with the necessary sustainment infrastructure. These are designed to delay, restrict, and deter the entry and freedom of action for an Allied force within a contested theater, rather than to create an impenetrable “layered bubble”. Each of the overlapping layers is designed to generate cumulative and mutually reinforcing effects (see Figure no. 2).



Figure no. 2: *Layered A2/AD Architecture: Capabilities and Purposes*
(Source: Authors’ concept created using NotebookLM AI tool)

Within the framework presented above, it is assessed that the effective countering of A2/AD systems cannot be reduced to a single “decisive strike”, for example against enemy air defence systems alone. Rather, it must involve the systematic disaggregation of the adversary’s entire *kill chain*, and the creation of temporary windows of superiority in which friendly air forces are able to operate, and project effects under controllable levels of risk. The lessons derived from NATO analyses and from the conflict in Ukraine converge toward a pragmatic conclusion: enemy IADS and A2/AD “bubbles” can only be penetrated through coordinated actions executed across multiple operational domains (Black et al., 2024).

3. Cross-Domain Fires and Operational Approach to Defeat A2/AD Systems

The emergence of increasingly sophisticated threats, which have generated ever more credible and dangerous warfighting scenarios for the United States armed forces and its NATO allies, has led to the development of the Western operational response concept known as Multi-Domain Operations (MDO), marking a return to the conduct of Large-Scale Combat Operations (LSCO). Within this new operational framework, the fires warfighting function is assigned an essential role in *“achieving success by defending critical objectives against a variety of complex air and missile threats, maintaining enemy forces under pressure from stand-off distances through long-range fires, and employing convergent lethal and non-lethal fires across multiple domains to create windows of superiority and enable their exploitation by the joint force”* (AFC, 2021, p. 11).

In MDO context, land-based fires must be integrated across time and space with the capabilities of other services and multinational forces to achieve convergence and generate synergistic cross-domain

effects greater than those produced by isolated actions. In this context, the concept of “fires” extends beyond traditional kinetic strikes to include non-kinetic effects delivered through electronic warfare, cyber operations, information activities, and actions in the electromagnetic and space domains. As a result, fires are redefined within MDO as an integrative tool for achieving operational objectives through synchronized and convergent effects across the modern battlespace. In U.S. doctrine ADP 3-19 *Fires* (2019), cross-domain fires are defined as those *“executed in one domain and producing effects in another domain”*, while multi-domain fires are those that *“converge effects from two or more domains against a target system”* (ADP 3-19, 2019, pp. 1-4).

Aligned with this approach, deep cross-domain fires become a critical capability for defeating the components of adversary A2/AD systems, more specifically through the disruption of command-and-control systems, degradation of integrated air defence systems, destruction of long-range fires capabilities, and isolation of enemy forces in depth. For example, cross-domain fires also involve the integration of effects generated from the cyber and space domains in order to disrupt command-and-control elements, particularly those associated with enemy IADS. The synergistic effects generated by cross-domain fires can readily produce disruption of enemy systems, operational paralysis, and windows of opportunity enabling joint forces to regain freedom of maneuver and subsequently achieve their operational objectives. To ensure success, however, U.S. doctrine identifies several critical requirements: echeloned fires capabilities, enhanced sensor-to-shooter linkages, the integrated planning of lethal and non-lethal effects within the targeting process, and the exploitation of joint, interagency, intergovernmental, and multinational capabilities (AFC, 2021, p. 13).

At the same time, defeating A2/AD strategies requires the enhancement of fires capabilities through the fusion of information technologies and sensor systems, materialized in increased range and precision, amplified lethality, improved mobility, and greater survivability and resilience of systems.

In order to ensure the echelonment of capabilities, we identify ongoing reorganizations and prepositioning efforts within the force structures of the Alliance and the armed forces of member states, adapted to the MDO doctrinal framework primarily centered on precision fires executed at extended ranges, with multi-domain capabilities allocated at each echelon. At the operational and strategic levels, the five Multi-Domain Task Forces (MDTFs) designed and operationalized by the United States Army represent theater-level force structures centered on cross-domain fires capabilities, including hypersonic systems. These formations have been deployed in strategic locations and specifically designed to support the penetration and disintegration of adversary A2/AD systems, predominantly within the Indo-Pacific and Euro-Atlantic regions (Feickert, 2025). Simultaneously, the Alliance established and prepositioned the NATO Response Force (NRF), consisting of eight multinational brigade-level battlegroups representing the Alliance's Enhanced Forward Presence (eFP) along the Eastern Flank (Elgin et al., 2024). At the tactical level, recent transformations within the U.S. Army include the reorganization and operationalization of infantry brigade structures into Mobile Brigade Combat Teams (MBCTs). This process has led to the reconfiguration of organic artillery battalions into Multi-Domain Effects Battalions (MDEBs), with towed artillery increasingly replaced by UAS, electronic warfare systems, mobile rocket launch systems, and loitering munitions ("kamikaze" drones) (Feickert &

M'Bai, 2025). Conversely, artillery and rocket systems are increasingly centralized at the division level within U.S. force structures, concentrating on deep-strike missions while providing support to forces in contact upon request. Similarly, the British Army has recently operationalized the Deep Recce Strike Brigade Combat Team (DRS BCT) concept within divisional structures – described as *"an innovative structure designed to bring together all the elements required to conduct deep battle for a division-level force, including artillery and rockets, ground reconnaissance, Signals Intelligence (SIGINT), and electronic warfare capabilities"* (Salerno-Garthwaite, 2023).

Within the MDO framework, the effectiveness of targeting and fires command depends heavily on the speed, continuity, and efficiency of the sensor-to-shooter connection, especially in dispersed operational environments involving diverse sensors and strike systems. The U.S. Army Futures Command Concept for Fires 2028 promotes the "any sensor – best shooter" paradigm, which enables rapid and precise target engagement through the integration of cross-domain capabilities (AFC, 2021). This integration relies on "kill web" architectures built around interconnected networks and digitally enabled command-and-control systems. Artificial intelligence further enhances these processes by compressing decision-making cycles and automating elements of the kill chain, reducing engagement timelines from minutes to seconds. Practical examples include Ukraine's DELTA and KROPYVA battlefield management systems (Bondar, 2024), as well as the U.S. Army's Integrated Battle Command System and the British Army's Project SCEPTRE (Shlesman, 2025).

A key innovation in MDO targeting is the early identification, prioritization, and planning of targets associated with adversary A2/AD systems during the phase of strategic competition. Achieving this

requires extensive coordination among military branches, allied forces, specialized agencies, and multinational structures to identify critical vulnerabilities within enemy systems. In this process, all available sensors must be integrated to support functions such as early warning, deep-target acquisition, and battle damage assessment.

Defeating A2/AD systems depends on the synchronized targeting of critical nodes in order to disrupt their functional coherence. Simultaneous attacks against these elements can generate cascading effects that degrade the adversary's decision-making cycle and operational effectiveness.

4. Research Methodology and Design

This study employs a mixed methodological design that combines qualitative documentary analysis with quantitative data derived from direct observation, and is intended to evaluate the manner in which cross-domain fires can generate synergistic effects against adversary A2/AD systems at the operational level.

The qualitative component is predominant and examines doctrinal documents, operational concepts, lessons learned from ongoing conflicts, as well as contemporary academic and military studies related to A2/AD, joint fires, deep fires, Multi-Domain Operations (MDO), convergence, and sensor-to-shooter integration. This component provides the conceptual and doctrinal foundation necessary for understanding both the functioning of adversary A2/AD systems and the manner in which cross-domain fires may be employed to disrupt them.

The quantitative component is based on structured observations of the sensor-to-shooter process conducted during the multinational exercise Dynamic Front 2026. This exercise is particularly relevant to the research because it focused on rehearsing NATO regional plans and strengthening the Alliance's capacity to integrate multi-domain fires and effects in support of counter-A2/AD capabilities.

4.1. Qualitative Analysis

The qualitative analysis examines adversary A2/AD architectures as "systems of systems" rather than as mere deployments of individual platforms. This important methodological distinction directed the analysis toward identifying the components of these systems and the manner in which interdependencies are established among them within the adversary's kill web interactions that collectively provide capabilities for detection, decision-making, engagement, protection, and logistical sustainment of adversary operations. At the same time, this analytical framework enables the identification of critical vulnerabilities within the adversary system. For example, the destruction of a launcher may produce only a temporary tactical effect; however, the simultaneous disruption of decision-making processes, C2 links, sensor coverage, or logistical sustainment capabilities may generate far broader operational effects. From this perspective, Table no. 1 presents the most relevant components of an A2/AD architecture, identified and grouped according to their functional roles, including representative categories of equipment.

Table no. 1
A2/AD Architecture Components and Capabilities

COMPONENT	CAPABILITIES	OPERATIONAL PURPOSE
“The SHIELD” Integrated Air and Missile Defense Systems (IADS)	– long-range surface-to-air missile systems; – medium- and short-range air defense systems; – early warning radars; – command and control nodes; – fighter aircraft and interceptor aircraft; – electronic warfare systems.	• Protection of A2/AD infrastructure; • Denial of adversary air superiority.
“The FIST” Long-Range Precision Fires (LRPF)	– ballistic and cruise missiles; – rocket artillery; – hypersonic weapons.	• Strike: air bases, ports, logistics hubs, command posts, troop concentrations, critical infrastructure.
“The EYES” Intelligence, Surveillance, Reconnaissance (ISR)	– satellites and space-based sensors; – reconnaissance units and UAVs; – radar systems; – electro-optical / infrared sensors; – electronic and signal intelligence (ELINT / SIGINT); – cyber intelligence,	• Detection and tracking of targets at long range without which the rest of the system cannot function.
“The BRAIN” Command and Control (C2)	– command and control (C2); – communication networks; – integration of ISR data with strike systems.	• Rapid decision-making; • Synchronization of fires; • Target allocation and distribution.
“The SHADOW” Electronic Warfare, Cyber and Space	– electronic warfare; – cyber operations; – space denial capabilities; – communications jamming; – GPS denial; – network attacks.	• Degrading adversary ISR and C2; • Concealing own systems and operations.
“The GATEKEEPER” Maritime Denial	– anti-ship missiles; – submarines; – naval mines; – coastal defense systems; – maritime patrol aircraft; – unmanned maritime systems.	• Deny access to key maritime routes, ports, and littoral areas.
“The LIFELINE” Logistics and Sustainment	– missile storage depots (hardened or underground); – munitions distribution hubs and supply points; – logistics support areas; – railheads and military transport terminals; – fuel storage depots; – forward arming and refueling points.	• A2/AD logistics is not centralized, but: – distributed (to avoid targeting); – mobile (to survive strikes); – redundant (to ensure continuity).

(Source: Authors' concept)

The most recent version of the US Army MDO doctrine, FM 3-0, *Operations* (2025), identifies Integrated Air Defense Systems (IADS) and the adversary's integrated fires complexes as “essential components of both anti-access (A2) and area denial (AD), assessed as

resilient and adaptive capabilities that cannot easily be defeated through strikes against a single decisive point or through attacks conducted within a single domain” (FM 3-0, 2025). In parallel, US fires doctrine, FM 3-09 *Fire Support and Field Artillery Operations* (2024), clarifies the

role of fires in MDO as consisting of the “*rapid and continuous integration of ground-to-ground indirect fires, target acquisition assets, attack aircraft, and other lethal and non-lethal strike systems that converge against targets across all domains*” (FM 3-09, 2024). Convergence constitutes a fundamental principle of MDO doctrine, also applicable to cross-domain fires, explaining the manner in which capabilities from different domains may be synchronized in order to generate exploitable effects against decisive points within enemy systems.

The lessons learned from ongoing conflicts validate the relevance of these doctrinal and conceptual provisions. Both the war in Ukraine and the conflicts in the Middle East demonstrate the growing importance of drones, commercial and military sensors, electronic warfare, long-range precision fires, and the acceleration of targeting cycles. RAND analyses concerning the lessons of the war in Ukraine emphasize the unprecedented transparency of the battlefield, the extensive use of unmanned systems, the role of satellite imagery, and the necessity for the dispersion, concealment, protection, and continuous movement of forces in order to increase survivability (Black et al., 2024). These conflicts also demonstrate the continuing operational relevance of deep fires capable of generating effects beyond the tactical level. Ground-based missile systems (e.g., HIMARS/MLRS), complemented by loitering munitions and “one-way attack drones”, have enabled Ukraine to strike command posts, ammunition depots, troop concentrations, and critical infrastructure targets located deep within the Russian territory (Svartman et al., 2024). Similarly, precision missiles launched by the United States and Israel from maritime and air platforms have successfully engaged operationally and strategically high-value targets in Iran.

At the same time, the analysis of conclusions derived from recent exercises and experiments focused on cross-domain fires highlights the fact that solely long-range strike systems are insufficient for the effective countering of A2/AD strategies. The exercises *Dynamic Front 2026* and *Cross-Domain Fires Concept Focused Warfighting Experiment 2026* demonstrated the necessity of integrating multi-domain effects and accelerating the synchronization of detection, data transmission, and target engagement processes. In the context of the proliferation of ballistic missiles, cruise missiles, and long-range drones, *Dynamic Front 2026* represented a significant milestone for NATO in testing fires capabilities and the integration of multi-domain strikes through the rehearsal of targeting processes conducted at a high operational tempo and within extremely compressed timelines (Mustață, 2026). Complementarily, *Cross-Domain Fires 2026* assessed the capacity of force structures and emerging technologies to deliver synchronized effects in contested, degraded, or intermittent environments. The experiment integrated a fires command element with helicopters and Air-Launched Effects (ALE) systems employed as advanced sensors within a simulated contested area, with the purpose of locating and identifying high-value targets and generating essential targeting data (Miller, 2026). Overall, the conclusions of these exercises confirm that the effectiveness of fires depends on the ability to detect targets, transmit targeting data, validate targets, allocate the optimal strike asset, generate effects, and assess results. Consequently, sensor-to-shooter integration becomes an essential condition in which ISR, C2, targeting processes, data links, and fires platforms form an operational chain whose speed, resilience, and interoperability determine the effectiveness of cross-domain fires.

Building upon the analysis of the investigated sources, it may be proposed a phased operational algorithm designed to reflect both the process and the conditions required for the disintegration and destruction of adversary A2/AD system components, with the objective of regaining

and maintaining access to geographically significant areas (see Figure no. 3). This model represents an adaptation of the deliberate targeting algorithm D3A to the MDO operational cycle (Compete – Penetrate and Disintegrate – Exploit – Return to Competition).



Figure no. 3: *A2/AD Defeat Operational Cycle*
(Source: Authors' concept created using NotebookLM - AI tool)

During the competition phase, preceding the outbreak of hostilities, the prepositioning of forces is essential in order to preserve terrain and facilities necessary for the subsequent introduction of additional forces and for reducing the distances to objectives and targets. Within this same phase, as previously emphasized, the targeting process also begins through the identification, prioritization, and planning of targets associated with adversary A2/AD system components. This process must pursue the progressive isolation and destruction of the most exposed components, beginning with those belonging to LRPF and IADS complexes, which constitute the adversary's center of gravity.

In competition phase, the first three stages are to be conducted:

- **SENSE** – involves the integration of multi-domain sensors (satellites, UAVs, Signals Intelligence/SIGINT, Electronic Intelligence/ELINT, Human Intelligence/HUMINT, Special Operations Forces/SOF) for the identification and localization of system components;
- **UNDERSTAND** – encompasses the analysis of the collected information in order to understand the system architecture, its interconnections, and operational functioning;
- **DECIDE** – consists of conducting the decision-making and targeting process regarding target prioritization, effects planning, and the allocation of engagement systems and ISR assets.

During the conflict phase, the first three stages continue while the actual degradation of the designated A2/AD target elements is executed through:

- **STRIKE** – aims at engaging targets through synchronized cross-domain lethal and non-lethal fires and effects:

- Electronic and cyber-attacks intended to disrupt communications and data networks;
- Preliminary multi-vector attacks (UAVs, loitering munitions);
- Decisive strikes employing long-range precision missile systems launched from land, air, and maritime platforms.

- **ASSESS** – consists of monitoring and evaluating the effects generated on targets, analyzing the results, and issuing guidance for re-engagement when necessary.

- **EXPLOIT** – ensures the creation of favorable conditions that can subsequently be exploited by friendly forces in order to accomplish operational objectives (e.g., reducing the enemy air defence bubble to enable the approach and freedom of action of friendly air forces, or destroying anti-ship capabilities in order to enable naval penetration and maneuver toward designated maritime areas or coastlines).

The qualitative analysis clarifies why cross-domain fires are relevant for defeating A2/AD systems by aiming to disrupt this architecture through the simultaneous or sequential targeting of multiple functional nodes across different domains. Cyber and electronic effects may disrupt C2 systems and communications; space and ISR capabilities may identify critical targets; land-based fires may engage long-range fires systems and logistical nodes; air-delivered fires may execute Suppression of Enemy Air Defenses (SEAD) and Destruction of Enemy Air Defenses (DEAD) missions and deep strikes; while maritime fires may engage

coastal defence and maritime interdiction systems. The overall objective is not merely the attrition of the adversary, but rather the degradation, disruption, and ultimately the disintegration of the adversary's operational system.

Additionally, the quantitative component that follows does not serve merely a descriptive purpose, but rather provides the analytical framework through which the data derived from structured observations of the sensor-to-shooter process conducted during the Dynamic Front 2026 exercise will be interpreted.

4.2. Quantitative Analysis

Direct involvement, as a fire support specialist, within the tactical- and operational-level command structures of the multinational exercise Dynamic Front 26 has provided the practical and analytical framework necessary for observing and evaluating the effectiveness of the sensor-to-shooter process across multiple target categories through the use of a structured observation instrument. To support this data collection process, a total of nine observers were selected from among the evaluators, observer-controllers, and mentors provided by Allied and national structures. These individuals were specialists possessing a considerable level of expertise regarding both the conduct of the observed sensor-to-shooter (S2S) process and the operational scenario adopted for the exercise. They were distributed across distinct locations in order to observe the conduct of the process within tactical- and operational-level fires support structures.

The observation of the S2S process was conducted in two distinct phases:

- Phase 1 – Computer Assisted Exercise (CAX);
- Phase 2 – Live Fire Exercise (LFX).

In both cases, the observations focused on target categories representing components of A2/AD systems, such as:

- a. Long-Range Artillery and missile systems (LRA);
- b. Integrated Air and Missile Defense Systems (IADS);
- c. ISR elements (radars, ground-based UAS platforms, etc.);
- d. Command posts and command-and-control (C2) elements;
- e. Logistics nodes/hubs (LOG).

Within the observation forms, observers were required to record the execution times associated with each stage of the S2S process (initial target detection – confirmation/identification – complete targeting process – approval/decision – transmission of the fire mission – actual engagement – initial battle damage assessment/BDA), as well as to calculate

the total elapsed time for each target category, separately for each exercise type.

By comparatively analyzing the data extracted from the observation forms and illustrated through the diagrams presented in Figure no. 4, it was identified in both phases of the exercise a differentiation in process duration according to target category that remains relatively constant (e.g., LRA: 3.5–5.5 min.; IADS: 6–7.5 min.; ISR: 4–5.5 min.; C2: 11–13.5 min.; LOG: 16.5–18.5 min.). These differences result from target prioritization according to their operational importance, the time sensitivity associated with their appearance on the battlefield, the allocation of sensors and direct S2S connectivity, as well as the maximization of decision-making speed for engagement approval.

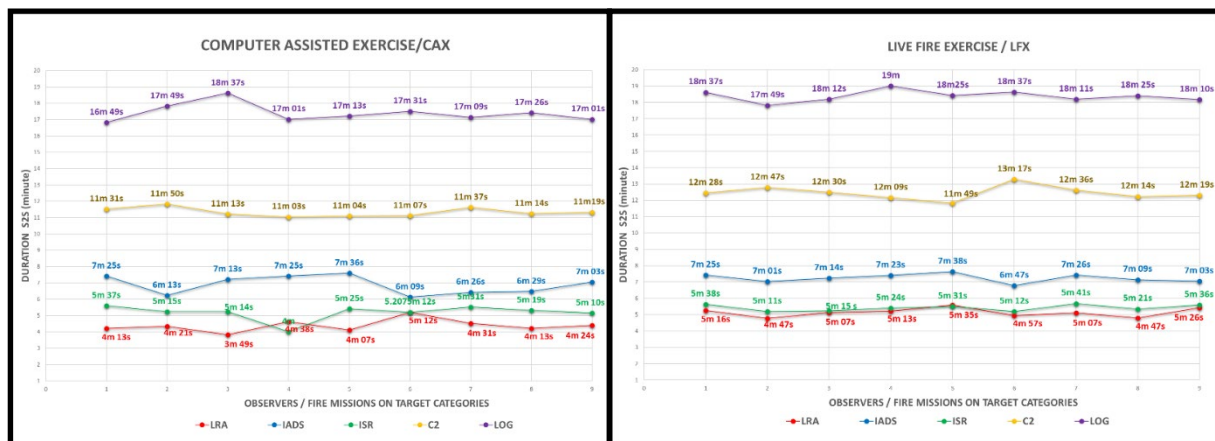


Figure no. 4: *Time of S2S Process on targets during CAX and LFX*
(Source: Authors' conception)

At the same time, the observations indicate that the duration of the S2S process is shorter during simulation exercises (CAX, using J-CATS) compared to live-fire exercises (LFX), because the simulated environment eliminates a significant portion of real operational frictions, such as firing safety constraints, technical limitations of systems, physical preparation and firing execution times, supplementary verification procedures, as well as communication and electromagnetic environment disruptions.

Conversely, live-fire exercises more accurately reflect the actual latencies of the S2S chain by incorporating all technical, procedural, and organizational constraints associated with the execution of fires in a real operational environment.

In interpreting the times obtained from the nine observations of the S2S process for each exercise type, consideration was given to the factors that could have influenced process duration, namely: delays within the decision-making chain, communication issues, the rules of

engagement (ROE) and collateral damage assessment (CDA) considerations during deconfliction procedures, electromagnetic jamming, and even human errors. Consequently, both measures of central tendency and measures of dispersion were employed in the statistical analysis of the S2S process times, as presented in Table no. 2.

The median was used as the principal indicator of operational timing because the distribution of S2S times is asymmetric and influenced by the delaying factors

mentioned above. The arithmetic mean may be used complementarily for mathematical modeling purposes; however, it is less relevant operationally because it is strongly influenced by extreme values. The minimum and maximum times reflect the fastest and most delayed target engagements, respectively. The variability of the process was evaluated through the interquartile range (IQR) and the standard deviation (σ), indicators that reflect both the stability of the process and the level of operational friction.

Table no. 2
The values of the main statistical indicators for the observed S2S times

Target Cat.	Exercise Type	Obs.	MIN Time	Q1	MEDIAN	Q3	MAX Time	Average	STD. DEV. (σ)	IQR
LRA	CAX	9	3m 49s	4m 13s	4m 21s	4m 31s	5m 11s	4m 23s	23s	(18s) 0.307
	LFX	9	4m 47s	4m 57s	5m 07s	5m 16s	5m 35s	5m 08s	16s	(19s) 0.310
IADS	CAX	9	6m 09s	6m 26s	7m 03s	7m 25s	7m 36s	6m 53s	34s	(59s) 0.981
	LFX	9	6 m 47s	7m 03s	7m 14s	7m 25s	7m 38s	7m 14s	16s	(22s) 0.365
ISR	CAX	9	4m	5m 12s	5m 14s	5m 25s	5m 37s	5m 11s	28s	(13s) 0.211
	LFX	9	5m 11s	5m 15s	5m 24s	5m 36s	5m 41s	5m 25s	12s	(21s) 0.355
C2	CAX	9	11m 03s	11m 07s	11m 14s	11m 31s	11m 50s	11m 20s	16s	(14s) 0.400
	LFX	9	11m 49s	12m 14s	12m 28s	12m 37s	13m 17s	12m 28s	25s	(23s) 0.381
LOG	CAX	9	16m 49s	17m 01s	17m 13s	17m 31s	18m 37s	17m 24s	33s	(30s) 0.490
	LFX	9	17m 49s	18m 11s	18m 25s	18m 37s	19m	18m 23s	21s	(26s) 0.434

The IQR values ≤ 0.5 and $\sigma < 1$ min presented in the table indicate a highly stable and predictable S2S process, without significant operational frictions, decision-making delays, or interoperability issues between capabilities, even though these capabilities belonged to multiple NATO member states participating in the exercise and could therefore have potentially influenced the execution of the S2S chain.

By comparing the median temporal values obtained through observation in the context of employing multi-domain capabilities with the known benchmark values established in doctrinal documents for conventional capabilities, it can be concluded that the duration of the S2S process is significantly reduced by approximately 60-80% when operating within multi-domain capability configurations (see Figure no. 3).



Figure no. 5: *Comparative Time of S2S Process: Conventional vs MDO*
(Source: Authors' conception created using NotebookLM - AI tool)

Complementary to the collection of quantitative data, the observation activity also pursued the acquisition of qualitative findings by asking the observers' opinions regarding the identification of potential frictions and delays affecting the S2S process, the efficiency of multi-domain capability integration, and the operational effects generated, as assessed on the basis of the observed outcomes during the analyzed activities. Likert-type scales (1-5) were employed in order to rank the responses. The multi-domain capabilities whose integration was subject to observer evaluation included:

- Multi-platform ISR sensors (UAS, radars, EW systems, deep reconnaissance patrols, SOF);
- Long-range precision artillery and missile systems;
- Electromagnetic jamming or spoofing;
- Air and maritime support integrated with land-based fires;
- FPV attack drones and loitering munitions;
- Simulated cyber-attacks;
- Automation of the decision-making/targeting process (MAVEN Smart System).

In this regard, the data collected through the observation sheets indicate an excellent level of performance (score 5) associated with the integration of multi-domain ISR platforms, particularly

unmanned aerial systems (UAS), the automation of the targeting process, the integration of effects generated by cyber capabilities, and the high degree of interoperability of command-and-control systems. At the same time, a moderate increase in performance (score 3) was identified in situations involving the integration of kinetic engagement assets from different domains (land, air, and maritime), as well as regarding the speed of obtaining battle damage assessment (BDA) results. The most significant impact on the generation of effective operational effects was associated with the employment of long-range precision artillery and missile systems, FPV drones and loitering munitions, as well as with the integration of various categories of sensors into a common system for target detection, identification, and engagement. Furthermore, the automation of the targeting process proved to be a determining factor in reducing reaction times and increasing the effectiveness of target engagement within the multi-domain operational environment.

It may be inferred that the analysis of the observational data provides a consolidated answer to the second research question established in this study by offering detailed insight into the manner in which multi-domain fires capabilities are integrated, while highlighting aspects such as the quality of the targeting process, the

interoperability of C2 systems, and the speed of the feedback loop for re-engagement.

From quantitative perspective this research has several limitations. First, exercises such as, Dynamic Front 2026 are experimentation environments, not combat environments; therefore, their results cannot be directly equated with wartime performance. Second, some data related to sensor-to-shooter timelines, targeting accuracy, network performance, and cross-domain effects may be restricted or classified. Third, quantitative observations may be influenced by exercise design, scenario assumptions, available systems, training objectives, and the maturity of participating units.

Despite these limitations, the combination of doctrinal analysis, lessons from ongoing conflicts, and exercise-based observations provides a relevant methodological basis for assessing how cross-domain fires can contribute to defeating adversary A2/AD systems.

5. Operational and Doctrinal Implications

The operational implications of the study highlight the fact that the defeating of A2/AD systems can no longer be achieved through sequential engagements or through supremacy within a single operational domain, but rather through the convergent integration of effects generated simultaneously across the land, air, maritime, cyber, electromagnetic, and space domains. The article demonstrates that the effectiveness of A2/AD architectures disintegration depends decisively on the ability of joint forces to disrupt the adversary's kill web through the synchronized targeting of sensors, C2 networks, IADS, LRPF capabilities, and logistical infrastructure. In this context, MDO requires the development of flexible, dispersed, and highly digitally interconnected force structures capable of

generating rapid and coordinated effects within contested environments. The results of the observations conducted during the Dynamic Front 2026 exercise confirm that the integration of ISR capabilities, precision fires, and targeting process automation significantly reduces the duration of the S2S cycle, thereby providing decision superiority and the ability to exploit temporary "windows of superiority" necessary for regaining freedom of maneuver.

From a doctrinal perspective, the study's insights support the necessity of transitioning from traditional fires support models toward operational architectures based on multi-domain convergence and dynamic joint kill webs. This transformation requires the re-thinking of the concept of "fires," which no longer encompasses exclusively kinetic effects, but also non-kinetic effects generated through electronic warfare, cyber operations, and actions conducted within the electromagnetic and informational spectrum. At the same time, doctrine must prioritize the integration of targeting processes beginning in the phase of strategic competition through the early identification of vulnerabilities within A2/AD systems and the synchronization of ISR, C2, and engagement capabilities within a common combat network. Within the same logic, the doctrinal experiences of the United States and NATO highlight the necessity of developing specialized multi-domain structures, such as MDTFs and MDEBs, capable of integrating sensors, fires systems, electronic warfare, and cyber capabilities into a single coherent operational mechanism.

In terms of military transformation, the doctrinal and operational implications indicate that the success of future joint operations will depend on the resilience and interoperability of C2 architectures, the automation of the decision-making process, and the integration of artificial intelligence

into the targeting cycle. The study demonstrates that the speed of target detection, validation, and engagement becomes a determining factor of operational effectiveness, and that military forces capable of efficiently implementing the “any sensor – best shooter” paradigm will possess the capacity to systemically disintegrate adversary A2/AD architectures. Consequently, future doctrines must emphasize multinational interoperability, decentralized execution, the resilience of communications within electromagnetically contested environments, and the accelerated integration of emerging technologies such as autonomous drones, loitering munitions, artificial intelligence, and distributed ISR systems as essential elements for achieving operational superiority in high-intensity conflicts.

6. Conclusions

The value of this qualitative and quantitative approach lies in the fact that it connects doctrine, theory, and operational practice. Doctrinal documents establish the conceptual vocabulary, and operational concepts explain how capabilities should be integrated. Lessons learned from ongoing conflicts and exercises demonstrate how these concepts function under real combat conditions, while specific research reports provide the analytical interpretation and supporting arguments required. Collectively, these sources establish the foundation for understanding adversary A2/AD systems as integrated operational architectures and for explaining how cross-domain fires may be employed for their systematic disruption.

In a complementary manner, the observation method served as an anchor to battlefield reality, transforming complex operational processes into quantifiable indicators (S2S times), highly relevant for substantiating one of the essential conditions for the effective countering of A2/AD systems, specifically, the significant

reduction of the detect–decide–engage cycle through the employment of cross-domain fires capabilities.

The outcomes of the research highlight the fact that the mechanisms through which cross-domain fires generate synergistic effects against A2/AD systems are based on the simultaneous integration of ISR capabilities, precision fires, electronic warfare, cyber operations, and digital C2 architectures within a convergent targeting process. Decisive effects against enemy’s A2/AD architectures do not result from the isolated destruction of individual platforms, but rather from the progressive disintegration of the adversary’s kill web and the generation of cumulative effects capable of producing operational paralysis and reducing the adversary’s capacity to react.

The research also confirms that the efficiency of the sensor-to-shooter cycle represents the critical condition for the success of counter-A2/AD operations. The data resulting from observations conducted during the Dynamic Front 2026 exercise demonstrate that the integration of multi-domain capabilities and the automation of the targeting process enable a significant reduction in D3A timelines, increasing both the speed of operational reaction and the capacity to exploit tactical and operational opportunities. In this regard, the convergence of sensors, data networks, command-and-control systems, and lethal or non-lethal strike systems becomes the principal force multiplier within the contemporary operational environment.

Overall, the study demonstrates that future confrontations against adversaries possessing A2/AD system architectures will be determined less by numerical superiority or the isolated performance of individual platforms, and more by the capacity to rapidly integrate multi-domain effects at an operational tempo superior to that of the adversary.

Author Contributions

Conceptual framework and operational approach, I.-R.M. and G.M.; methodology, I.-R.M. and G.M.; qualitative analysis, I.-R.M. and G.M.; quantitative analysis, I.-R.M.; operational and doctrinal

implications, I.-R.M. and G.M.; resources, I.-R.M. and G.M.; writing – original draft preparation, I.-R.M. and G.M.; writing – review and editing, I.-R.M. Both authors have read and agreed to the published version of the manuscript.

REFERENCES

- ADP 3-19. (2019). *U.S. Army Doctrine Publication/ADP 3-19 Fires*.
- AFC. (2021). *Pamphlet 71-20-6 Army Futures Command Concept for Fires 2028*. USA: U.S. Army Futures Command.
- Black, J., et al. (2024). *Russia's War in Ukraine Emerging Insights for UK and NATO Joint Doctrine*. Santa Monica, Calif., and Cambridge, UK: RAND Corporation. Available at: <https://www.rand.org/randeurope/research/projects/2024/russias-war-in-ukraine-insights-for-uk-and-nato.html>.
- Bondar, K. (2024). *Understanding the Military AI Ecosystem of Ukraine*. Center for Strategic and International Studies. Available at: <https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine>, accessed on March 21, 2026.
- Chiorcea, I. (2024). The A2/AD (Anti Access/Area Denial) Concept between Theory and Practice. *Romanian Military Thinking*, 1, 96-109. Available at: <https://engmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20reviste/RMT/2024/1/CHIORCEA.pdf>.
- Dalsjo, R., et al. (2019). *Bursting the Bubble: Russian A2/AD in the Baltic Sea Region: Capabilities, Countermeasures, and Implications*. FOI, Swedish Defence Research Agency. Available at: <https://www.diva-portal.org/smash/get/diva2:1410288/FULLTEXT01.pdf>, accessed on March 24, 2026.
- Dwight, P. (2023). *Multi-Domain Operations: Passing the Torch*. Hague: The Hague Centre for Strategic Studies. Available at: <https://hcss.nl/report/multi-domain-operations-passing-the-torch/>, accessed on March 15, 2026.
- Elgin, K., et al. (2024, 05 20). *Understanding NATO's Concept for Deterrence and Defense of the Euro-Atlantic Area*. Center for Strategic and Budgetary Assessments. Available at: <https://csbaonline.org/research/publications/understanding-natos-concept-for-deterrence-and-defense-of-the-euro-atlantic-area/publication/1>, accessed on March 11, 2026.
- Erdogan, A. (2018). Russian A2AD Strategy and Its Implications for NATO. Modern Air & Space Power. *Political & Hybrid Warfare, Research*. Available at: <https://behorizon.org/russian-a2ad-strategy-and-its-implications-for-nato/>, accessed on February 23, 2026.
- Feickert, A. (2025). *The Army's Multi-Domain Task Force (MDTF)*. Congressional Research Service. Available at: <https://www.congress.gov/crs-product/IF11797>, accessed on April 2, 2026.
- Feickert, A., & M'Bai, E. (2025). *The U.S. Army's Mobile Brigade Combat Team (MBCT)*. Congressional Research Service. Available at: <https://www.congress.gov/crs-product/IF13128>, accessed on April 2, 2026.
- FM 3-0. (2025). *Operations*. Washington, DC: Headquarters Department of the Army.
- FM 3-09. (2024). *Fire Support and Field Artillery Operations*. Washington, DC: Headquarters Department of the Army.

Impson, N. (2020). *The Next Warm War: How History's Anti-Access/Area Denial Campaigns Inform the Future of War*. Small Wars Journal. Available at: <https://archive.smallwarsjournal.com/comment/62423>, accessed on March 20, 2026.

Miller, D. (2026). *CDF CFWE tackles DDIL, Interoperability to execute Fires*. US Army. Available at: https://www.army.mil/article/291397/cdf_cfwe_tackles_ddil_interoperability_to_execute_fires, accessed on April 7, 2026.

Mustață, R. (2026). *Dynamic Front 26 la Cincu: NATO testează integrarea loviturilor multidomeniu, artileria aliată și dronele de recunoaștere*. Mediafax. Available at: <https://www.mediafax.ro/social/dynamic-front-26-la-cincu-nato-testeaza-integrarea-loviturilor-multidomeniu-artileria-aliata-si-dronele-de-recunoastere-23684671>, accessed on April 2, 2026.

NATO.int. (2024). *NATO's approach to counter information threats*. Available at: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/10/18/natos-approach-to-counter-information-threats>, accessed on April 3, 2026.

Salerno-Garthwaite, A. (2023). *Agile approach: British Army Deep Recce Strike*. Global Defence Technologies. Available at: <https://defence.nridigital.com/global-defence-technology-aug23/revolutionising-nato-s-land-forces-the-british-armys-agile-approach-with-deep-re>, accessed on March 30, 2026.

Shlesman, V. (2025). *Connecting Every Sensor to Every Shooter: Why Software is the New Decisive Domain*. Hadean.com. Available at: <https://hadean.com/blog/connecting-every-sensor-to-every-shooter-why-software-is-the-new-decisive-domain/>, accessed on April 3, 2026.

Svartman, E.M., et al. (2024). *Deep fires and the British strategic posture: does the war in Ukraine validate it?* *Revista Brasileira de Política Internacional*, 67(1). DOI:<http://dx.doi.org/10.1590/0034-7329202400103>.

US Department of War. (2026). *2026 National Defense Strategy. SUA*. Available at: <https://media.defense.gov/2026/Jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSE-STRATEGY.pdf>.