SARA Law **R**esearch **C**enter
International **J**ournal of **L**egal and **S**ocial **O**rder, https://www.ccdsara.ro/ijlso
ISSN 2821 – 4161 (Online), ISSN 2810-4188 (Print), ISSN-L 2810-4188
N°. 1 (2025), pp. 231-248

UNDERSTANDING THE INSTRUMENTS OF POWER EFFECTS ON THE MILITARY INSTRUMENT OF POWER IN MULTI-DOMAIN OPERATIONS: A CASE STUDY FOR HUMAN INTELLIGENCE FROM A TRAINING PERSPECTIVE

A. KIS/A. MARZA

Received 24.11.2025; accepted 19.12.2025
First online publication: 20.12.2025
DOI: https://doi.org/10.55516/ijlso.v5i1.297

Alexandru KIS
PhD, associate lecturer at University of Oradea
E-mail: alexandru_kis@yahoo.com
ORCID: https://orcid.org/0009-0001-2780-5728

Andrei MARZA
NATO HUMINT Centre of Excellence[1]

Abstract

This paper investigates the effects of the diplomatic, informational, and economic instruments of power (IoPs) on the military IoP within Multi-Domain Operations (MDO), focusing on human intelligence (HUMINT) as a case study from a training perspective. It argues that HUMINT professionals must be trained not only in classical collection and influence skills but also in the ability to understand, navigate, and synchronize with other IoPs in a multi-domain environment. To this end, the study evaluates the conceptual foundations of IoPs in MDO, examines their interplay across the continuum of conflict, assesses the role of HUMINT in this context, and outlines training needs and approaches for HUMINT professionals. Ultimately, it seeks to contribute to the development of effective, future-proof training programs that enable NATO and partner personnel to operate effectively in the complex reality of modern conflict.

[1] **Disclaimer:** The presented content was built on available literature analysis, the authors' experience and consultations at a public level. The ideas and opinions expressed in this article are those of the authors and do not necessarily reflect NATO HUMINT COE, or NATO's policies.

Key words: *HUMINT, Instruments of Power, Multi-Domain Operations, hybrid warfare.*

INTRODUCTION

Warfare has become increasingly multidimensional, blending conventional military power with diplomatic maneuvering, economic coercion, information dominance, and technological disruption. This reality, often referred to as hybrid warfare, challenges the traditional distinction between peace and war, frontlines and home fronts, military and civilian spheres. Adversarial actors deliberately operate in the grey zone, exploiting vulnerabilities across political, informational, military, economic, social, and infrastructural domains to erode cohesion and resilience within target societies and alliances.

NATO and its member states have encountered repeated demonstrations of these hybrid tactics. Russia's use of disinformation campaigns and manipulation, cyberattacks, energy leverage, targeted assassinations, sabotage, and the instrumentalization of migration illustrate the deliberate orchestration of multiple Instruments of Power (IoPs) to achieve strategic objectives without triggering open war – all these while familiarizing its own public with the idea of an open conflict with the "collective occident" and NATO. Similar patterns can be observed in the Middle East, where state and non-state actors such as Iran and its proxies - Hamas, Hezbollah or Houthi - integrate military capabilities with informational and economic levers, and where groups such as ISIS have demonstrated mastery of narrative warfare and social mobilization alongside violent insurgency.

Against this backdrop, the concept of Multi-Domain Operations (MDO) has emerged as a doctrinal response, emphasizing the integration and synchronization of effects across all domains - land, air, maritime, cyber, and space - while also acknowledging the importance of cross-cutting enablers such as information and intelligence. MDO requires not only the coordination of military capabilities but also a comprehensive understanding of how military instruments interact with other national and allied IoPs. This interaction is bivalent: military operations are both enabled and constrained by diplomacy, economic measures, and informational campaigns. To tackle with this complexity, military professionals must be educated to perceive the broader strategic environment and to integrate their activities with other instruments effectively.

Within this framework, Intelligence, and Human Intelligence (HUMINT) in particular, plays a pivotal role. HUMINT serves as both a collector of insights on adversary intentions and perceptions, and as an active contributor to influence operations through engagement with human networks [2]. In MDO, where

[2] Alexandru Kis, *A projection of the cognitive warfare in Human Intelligence,* STRATEGIES XXI, vol. XIX, 27-28 June 2023, "Carol I" National Defence University Publishing House,

information is contested and perception is decisive, HUMINT professionals are uniquely positioned to provide context, nuance, and early warning. However, this role is increasingly demanding: adversaries employ artificial intelligence, cyber tools, and sophisticated disinformation to deceive, manipulate, or intimidate human sources. Consequently, HUMINT training must evolve, integrating digital literacy, cross-domain awareness, and resilience against manipulation alongside traditional tradecraft.

This paper investigates the effects of the broader IoPs on the Military IoP within MDO, focusing on HUMINT as a case study from a training perspective. It argues that HUMINT professionals must be trained not only in classical collection and influence skills but also in the ability to understand, navigate, and synchronize with other IoPs in a multi-domain environment. To this end, the study evaluates the conceptual foundations of IoPs in MDO, examines their interplay across the continuum of conflict, assesses the role of HUMINT in this context, and outlines training needs and approaches for HUMINT professionals. Ultimately, it seeks to contribute to the development of effective, future-proof training programs that enable NATO and partner personnel to operate effectively in the complex reality of modern conflict.

I. CONCEPTUAL FOUNDATIONS: HYBRID WARFARE, MULTI-DOMAIN OPERATIONS, AND THE INSTRUMENTS OF POWER

I.1 Hybrid Warfare and its characteristics

Hybrid warfare represents one of the defining paradigms of twenty-first century conflict. Unlike conventional wars, fought largely between uniformed forces with clear frontlines, hybrid warfare blurs distinctions between peace and war, state and non-state actors, and overt and covert actions[3]. It is designed to exploit the thresholds of international law and the vulnerabilities of open societies by combining multiple forms of pressure in a synchronized manner. Hybrid adversaries rarely rely on direct military confrontation alone; instead, they integrate political, economic, informational, and military measures into a comprehensive strategy of gradual erosion.

Bucharest, https://www.strategii21.ro/A/2023-06. STRATEGII XXI/CONFERINTA STRATEGII XXI 2023.pdf.

[3] Erik Reichborn-Kjennerud and Patrick Cullen, *What is Hybrid Warfare?*, Information Note January 2017, MCDC Countering Hybrid Warfare Project, https://assets.publishing.service.gov.uk/media/5b2904aded915d2cd5d01bfd/MCDC_CHW_Information_Note-Understanding_Hybrid_Warfare-Jan_2018.pdf.

In its tri-folded dimensions (figure 1), several characteristics distinguish hybrid warfare[4] [5] [6]:

- Interplay of military and non-military IoPs, inflicting kinetic and non-kinetic tools and tactics.
- Multi-vector pressure – exploiting weaknesses across political systems, media, infrastructure, and security institutions simultaneously.
- Ambiguity and deniability – operating in the grey zone through proxies, false-flag operations, or cyber anonymity.
- Speed and adaptability – tailoring campaigns dynamically to exploit emerging opportunities before adversaries can coordinate responses.
- Psychological and cognitive effects – seeking not necessarily physical destruction but erosion of trust, cohesion, and willpower within target societies.

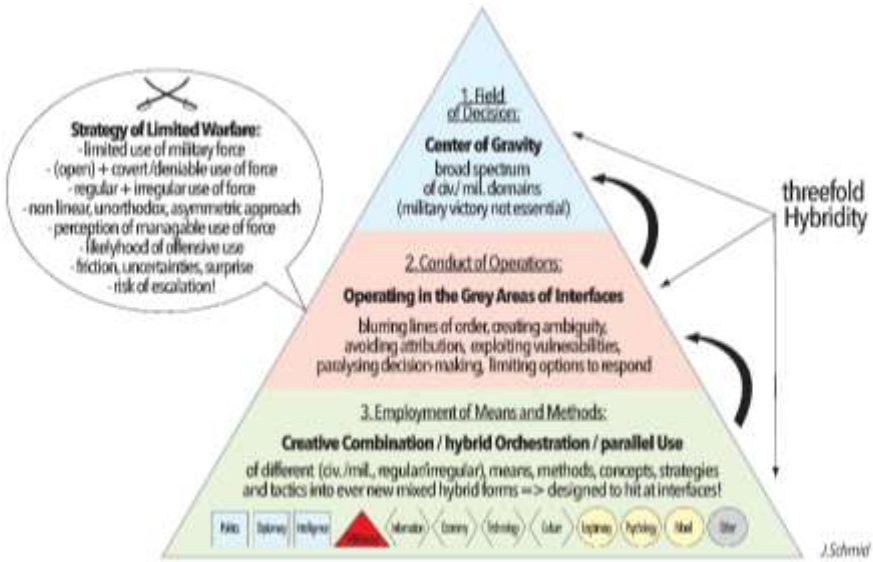

Figure 1 The Trinity of Hybrid Warfare[7]

[4] Arsalan Bilal, *Hybrid Warfare - New Threats, Complexity, and 'Trust' as the Antidote*, November 2021, NATO Review, https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.

[5] Johann Schmid, *Introduction to Hybrid Warfare – A Framework for comprehensive Analysis*, in: Thiele, R. (eds) Hybrid Warfare. Edition ZfAS. Springer VS, Wiesbaden, 2021, https://doi.org/10.1007/978-3-658-35109-0_2.

[6] K. Iskandarov and P. Gawliczek, *Hybrid warfare as a new type of war. The evolution of its conceptual construct*, in Miroslaw Banasik, Piotr Gawliciczek and Agnieszka Rogozinska (eds), *The Russian federation and international security*, Poland: Difin publishing house, 2020, pp. 96-107.

[7] Johann Schmid, *The Hybrid Face of Warfare in the 21st Century*, March 2019, https://www.maanpuolustus-lehti.fi/the-hybrid-face-of-warfare-in-the-21st-century/.

Russia's operations in Ukraine since 2014 illustrate these principles vividly. Prior to the full-scale invasion of 2022, Russia launched a hybrid campaign involving cyberattacks on energy infrastructure, disinformation targeting Ukrainian and Western audiences, economic leverage through gas exports, and covert paramilitary operations in Crimea and Donbas[8]. Similar hybrid approaches have been observed in Europe through interference in democratic elections, sabotage, and the weaponization of migration flows.

Hybrid warfare thus underscores the need to integrate responses across all IoPs, since military force alone is insufficient to counter threats that are simultaneously political, economic, and informational.

I.2 Multi-Domain Operations

Multi-Domain Operations represent NATO's and allied militaries' doctrinal answer to hybrid challenges. MDO seeks to achieve convergence: the simultaneous and synchronized employment of effects across all domains - land, air, maritime, cyber, and space - integrated with informational and cognitive dimensions.

The rationale behind MDO is that modern adversaries operate seamlessly across domains, leveraging asymmetries and exploiting seams in allied structures. For instance, a cyberattack on communications may paralyze military command systems without a shot fired, while disinformation erodes public trust in defensive operations. To counter such tactics, NATO forces must integrate domain effects rapidly and flexibly, achieving superiority through coordination rather than mass.[9]

Key principles of MDO include:[10]

- Integration across domains – breaking down stovepipes between services and enabling joint effects.
- Cross-domain maneuver – using one domain to create opportunities in another (e.g., cyberattacks to disable air defense, enabling air operations).
- Tempo and decision dominance – outpacing adversaries in detecting, deciding, and acting.
- Resilience and adaptation – addressing vulnerabilities beyond the battlefield, including societal and political resilience.

[8] Sînziana Iancu, *Războiul hibrid al Rusiei împotriva Occidentului. Doctrina Gherasimov, forțe paramilitare și grupurile de voluntari*, in Defense Romania, September 2024, https://www.defenseromania.ro/razboiul-hibrid-al-rusiei-impotriva-occidentului-i-doctrina-gherasimov-forte-paramilitare-ipb-si-grupurile-de-voluntari-iv_630347.html.

[9] Andrea Gilli, Mauro Gilli and Gorana Grgić, *NATO, multi-domain operations and the future of the Atlantic Alliance*, in *Comparative Strategy*, *44*(1), 2025, pp. 73–91, https://doi.org/10.1080/01495933.2024.2445491.

[10] TRADOC, *The U.S. Army in Multi-Domain Operations 2028*, U.S. Army Training and Doctrine Command, 2018.

MDO is therefore not only a military framework but a whole-of-government and whole-of-alliance approach requiring synergy among all IoPs.

I.3 Instruments of Power: DIME and beyond. Instruments of Power across the continuum of conflict

The concept of IoPs provides the analytical framework through which states and alliances employ their resources to achieve strategic objectives. Traditionally expressed as DIME (Diplomatic, Informational, Military, Economic), the framework has been broadened at operational level in NATO and EU contexts to encompass PMESII (Political, Military, Economic, Social, Infrastructure, Information), reflecting the complexity of modern power[11]:

- Diplomatic: alliances, treaties, and shaping of norms; diplomacy constrains or enables military action.
- Informational: strategic communication, cyber, and cognitive operations; information has become both tool and domain.
- Military: deterrence, compellence, and defense; increasingly dependent on synergy with other instruments.
- Economic: sanctions, trade, finance, and energy leverage; economic measures weaken adversary resilience or strengthen alliance cohesion.

Other frameworks emphasize financial, intelligence, law enforcement ("DIMEFIL" IoPs) [12], or even cultural [13], or technological [14] instruments, highlighting the rise of lawfare, identity politics, and disruptive innovation.

The interdependence of these instruments is crucial: military success requires diplomatic legitimacy, informational superiority, and economic sustainability. In MDO, this interconnectedness is amplified, as adversaries deliberately exploit seams between domains and instruments.

Modern conflict is rarely a binary state of "peace" versus "war." Instead, it unfolds along a continuum (figure 2), with shifting intensities and modalities. In

[11] Dean S. Hartley, *The DIME/PMESII Paradigm*, in *Unconventional Conflict. Understanding Complex Systems. Springer*, Cham, 2017, https://doi.org/10.1007/978-3-319-51935-7_4.

[12] Cesar Augusto Rodriguez, Timothy Charles Walton, and Hyong Chu, *Putting the "FIL" into "DIME". Growing Joint Understanding of the Instruments of Power*, Joint Doctrine - JFQ 97, 2nd Quarter 2020, pp. 121-128, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-97/jfq-97_121-128_Rodriguez-Walton-Chu.pdf?ver=2020-04-01-095603-607.

[13] Nina Gorenc, *Cultural diplomacy – the instrument of power in American foreign and security policy*, in *The Review of International Affairs*, Vol. LXVI, No. 1158-1159, April–September 2015, pp. 18-31, https://thereviewofinternationalaffairs.rs/wp-content/uploads/RI/2015/1158-1159/RI-2015-1158-1159-article-2.pdf.

[14] Paola Fusaro, Nicolas Jouan, Lucia Retter and Benedict Wilkinson, *Science and technology as a tool of power. An appraisal*, RAND Europe, November 2022, https://www.rand.org/content/dam/rand/pubs/perspectives/PEA2300/PEA2391-1/RAND_PEA2391-1.pdf.

this spectrum, adversaries employ IoPs in calibrated sequences, exploiting ambiguity to pursue objectives without triggering full-scale military responses.

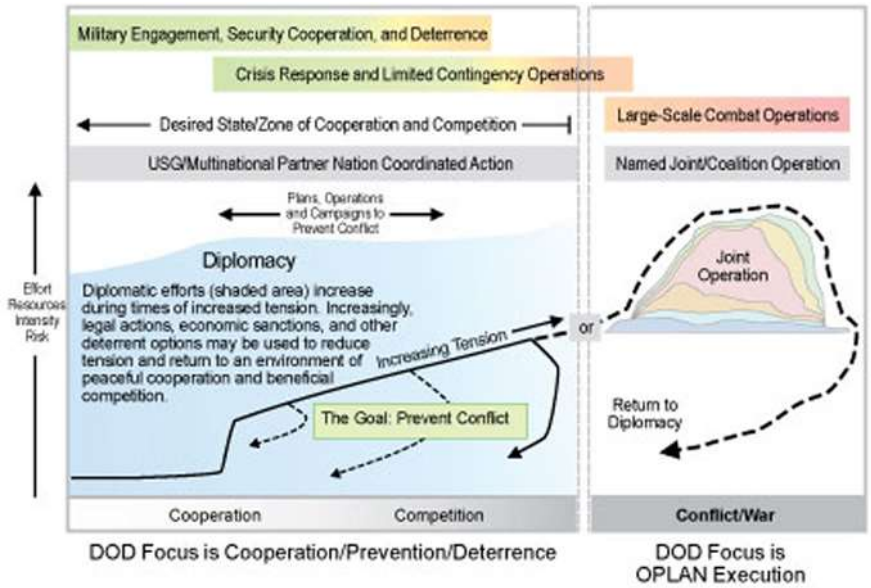

Figure 2 The conflict continuum[15]

Thus, the continuum of conflict/ competition is characterized by:

- Competition below armed conflict – Diplomatic pressures, espionage, covert influence operations, economic pressure, sabotage, and disinformation.
- Hybrid confrontation – Combination of non-military and limited military tools, blurring attribution and legitimacy.
- Open armed conflict – Overt employment of conventional and unconventional military force, supported by the full spectrum of IoPs.

Russia's activities in Europe since 2014 exemplify this model. The annexation of Crimea, as well as the later invasion in Ukraine, were preceded and accompanied by disinformation campaigns, cyberattacks, political subversion, and economic leverage through energy supply manipulation. Similarly, in the Middle East, Iranian proxy operations illustrate how hybrid tactics are applied across the spectrum, from political influence in Iraq to drone and missile attacks by aligned militias in Liban, Syria, and Yemen.

What makes hybrid warfare effective is not any single instrument, but their synchronization, an interplay demonstrating that Military IoP cannot succeed in

[15] https://www.thelightningpress.com/wp-content/uploads/2018/06/Conflict-Continuum.jpg.

isolation. Its effectiveness depends on how it is influenced, enabled, or constrained by other IoPs. For NATO, the challenge is therefore to train military personnel to recognize and integrate these effects.

II. TOWARDS A CASE STUDY IN HUMINT

II.1 Intelligence in Multi-Domain Operations

Multi-Domain Operations (MDO) demand a comprehensive intelligence architecture capable of integrating data from multiple domains (land, air, sea, space, cyber, and cognitive). Intelligence must provide not only situational awareness but also predictive assessments, enabling commanders and policymakers to anticipate adversary actions across the continuum of conflict.

The traditional Intelligence Cycle (direction, collection, processing, dissemination) remains valid, but in the MDO environment it faces new pressures:

- Speed of decision-making – Information must be processed in near real-time to support dynamic operations.
- Volume of data – The exponential growth of open-source, cyber, and sensor-derived data strains analytical capacity.
- Ambiguity and deception – Hybrid adversaries deliberately inject false signals, requiring advanced analytical techniques to discriminate truth from deception.
- Cross-domain integration – Intelligence must break silos to integrate military, economic, diplomatic, and informational inputs.

The U.S. Army's concept of convergence, synchronizing effects across domains through intelligence-led targeting, exemplifies the centrality of intelligence in MDO[16]. NATO's equivalent, reflected in its Warfare Capstone Concept (NWCC), similarly emphasizes that intelligence is the connective tissue enabling coherent multi-domain responses[17].

In essence, intelligence in Multi-Domain Operations serves as the connective and predictive core of modern warfare, integrating data across all domains to enable rapid, informed, and synchronized decision-making against adaptive and deceptive adversaries.

II.2 HUMINT in the IoP-MDO Nexus

In this context, HUMINT faces a series of challenges brought by the evolving operational contexts, as we have shown in a previous paper.[18] Thus,

---

[16] TRADOC, Op. Cit.

[17] NATO Allied Command Transformation, The *NATO Warfighting Capstone Concept*, Norfolk, VA., 2021, https://www.act.nato.int/our-work/nato-warfighting-capstone-concept/.

[18] Alexandru Kis, Pavol Soltys, *Human factors in Multi-Domain Operations: navigating the bivalent dynamics of human terrain and military human capital with a HUMINT lens*, in the proceedings of the 19th International Scientific Conference "Defense Resources Management in the 21st Century", Braşov, 7-8 November 2024.

technological innovation in MDO both enhances and constrains HUMINT. AI, big data analytics, and NATO's digital backbone enable faster correlation of human reporting with technical intelligence and improve the timeliness of insights. AI tools can help identify influencers, detect anomalies, and verify reporting, yet they also bring risks of bias, misinterpretation, and adversarial exploitation. At the same time, pervasive surveillance technologies such as biometrics, facial recognition, and cyber monitoring limit discreet operations and increase risks for human sources, especially in authoritarian contexts. HUMINT must therefore integrate technological enablers without losing its unique value: understanding the adversary intent, motivation, and perception in ways machines cannot replicate.

This transformation also redefines the human capital in HUMINT. NWCC underscores the imperative of "*the right people with the right skills*,"[19] requiring HUMINT operators to blend traditional interpersonal expertise with digital literacy, cultural intelligence, and cognitive agility. They must be equally adept at engaging sources in fragmented, urbanized societies and at exploiting AI-driven data systems for operational advantage. Such adaptability can only be sustained through continuous education, interdisciplinary training, and concept experimentation that prepare practitioners for hybrid and multi-domain challenges.

In this context, HUMINT and broader intelligence functions must be engaged and cooperate with elements of other IoPs, thus needing specialized understanding on functions, terminology, legal and operational opportunities and limitations, cooperative expectations, employed technology/ systems, cultural aspects, working ethos and ethics.

For NATO, inter-agency cooperation is not only vertical (between national and Alliance structures) but also horizontal, requiring collaboration between intelligence, cyber defense, information operations, and strategic communication. HUMINT, situated at the intersection of human engagement and broader intelligence processes, plays a crucial bridging role.

II.3 Military HUMINT in MDO - from crisis response operations to collective defense

Narrowing down to the military intelligence organizations, HUMINT practitioners need a clear understanding of possible tasks and the operating environment in different phases or manifestations of the hybrid warfare. These elements should be considered in a wide spectrum of reference, from the

[19] NATO Allied Command Transformation, *The NATO Warfighting Capstone Concept*, Norfolk, VA., 2021.

management of crowd-sourced intelligence to military liaison and advanced source and non-source operations.

Another critical aspect is represented by the HUMINT ascendent in Force Collection Activities, where oversight may include specialized support (guidance, mentorship, training) to the formation of expert interviewers. Moreover, the HUMINT access to specific informational ecosystems positions it at the forefront of collection on details relevant for human security (as an emerging imperative in areas of operations, alongside other cross-cutting topics[20]), or in relation with Law Enforcement Intelligence (LEINT)[21].

Training in military HUMINT must therefore prepare practitioners at all levels (collection, analysis, operational management, logistic & technological support) to perceive these dimensions for accurately answering intelligence requirements and produce effective influence.

Considering this approach for HUMINT in Article 5 context, we identify two major challenges. The first issue is represented by **the spectrum of activities where military HUMINT is involved in time and space** (the expectation is that requirements would emerge from technical agreements signed by SHAPE with the interested nations). As it is validated in stabilization, counterinsurgency, or crisis-response operations where the adversary and the host nation are distinct, the operating environment in collective defense is no longer "foreign soil with host-nation dynamics" but own or allied territory. Here, military power is not applied to influence or stabilize a host state but to defend sovereignty. This creates a stalemate for HUMINT: traditional collection from civilian sources in host societies may be restricted, as those societies are already part of NATO/allied structures, governed by national security laws, and heavily integrated with other instruments of power.

In any case, HUMINT remains critical across the stages of the conflict, but its role evolves. In early phase (hybrid/ pre-article 5 threshold), HUMINT may provide indications and warnings of adversary subversion, disinformation campaigns, infiltration of political movements, sabotage of infrastructure, or manipulation of minority groups. Here, HUMINT complements other collection assets by accessing human intentions and motivations, often hidden from technical means. In this context, operating in the virtual space (active collection through social media channels) would be a great benefit (although it needs the

[20] Alexandru Kis, *Subiecte transdisciplinare în NATO și reflectarea lor la nivelul disciplinei HUMINT – securitatea umană, considerațiile de gen și consolidarea integrității*, in INFOSFERA, Year XVI no. 2/2024, pp. 72-81, https://www.mapn.ro/publicatii_militare/arhiva_infosfera/documente/2024/2_2024.pdf.

[21] David L. Carter, *Law Enforcement Intelligence Guide 3.0*, Michigan State University, August 2021, https://www.researchgate.net/publication/353720175_CARTER_Law_Enforcement_Intelligence_Guide_30.

necessary legal framework, as it was the case for shooting down Russian-linked drones overflying NATO territory).

In the transition to high-intensity conflict, HUMINT supports intelligence collection and force protection in various operational and tactical contexts, reflected across the HUMINT spectrum of activities in the area of intelligence interest. In this regard, the development of the HUMINT tactics, techniques, and procedures to leverage emerging and disrupting technologies (e. g. facilitating Intelligence crowd-sourcing) must be considered to ensure depth and width of collection (as lessons from the war in Ukraine demonstrate)[22].

The second focus is understanding the operational environment throughout the extent and relevance of PMESII (a reference standard for assessing an operating environment) on the national/ NATO soil. HUMINT continues to exploit local populations' perceptions, resilience, and vulnerabilities. Even on allied soil, societies under attack experience stress (displacement, shortages, propaganda, economic coercion) that can affect posture's expectations. HUMINT can measure morale, map influence networks, and advise commanders on non-kinetic vulnerabilities. HUMINT's center of gravity shifts from "knowing the host population" to "safeguarding allied populations and exposing adversary manipulation", protecting and understanding the dynamics of the home environment. PMESII remains valid as an analytical tool, but its relevance in the continuum of conflict is found in prevention, resilience, and counter-subversion, requiring close integration with the non-military instruments of power. HUMINT thus becomes a bridge between military defense and national/Alliance-wide resilience.

In sum, HUMINT in hybrid and collective defense contexts must transform into a resilience-oriented, technologically enabled, and interagency-integrated discipline (coordination with relevant entities across non-military IoPs), bridging military defense with societal awareness to detect, prevent, and counter human-centered threats across the continuum of conflict.

III. INTEGRATION OF THE INSTRUMENTS OF POWER AND IMPLICATIONS FOR TRAINING

Understanding and applying IoPs interplay is not intuitive. Military officers often lack familiarity with diplomacy, economics, or information operations in the military education and training. Conversely, civilian actors may

[22] Laviniu Bojor, *Tehnologie dual în război: rolul telefoanelor inteligente în conflictul din Ucraina*, in *Impactul tehnologiilor emergente asupra securității internaționale,* coord. Alin Cîrdei and Laviniu Bojor, pp. 21-54, Editura Academiei Forțelor Terestre "Nicolae Bălcescu", Sibiu, 2025.

underestimate the constraints of military operations. Hybrid adversaries exploit these institutional silos by operating seamlessly across instruments.

Generic training for MDO must therefore prepare personnel to recognize IoPs effects across the conflict continuum, understand synergies and tensions between instruments, and incorporate cross-domain and cross-instrument perspectives into planning. Furthermore, interoperability is a point not just between services and nations, but across civilian-military agencies.

Given the lingering role of HUMINT in MDO, dedicated training programs must focus on tailoring performance objectives through the lenses of multiple IoPs: **cross-domain literacy** (HUMINT practitioners must understand how diplomatic, economic, informational, and military instruments interact), **intercultural competence** (essential for source engagement in any environment) [23] , **digital proficiency** (mastery of cyber hygiene, OSINT exploitation, AI-assisted analytics, and secure digital communication) [24] , **resilience and ethics/ integrity** (ability to withstand manipulation, cognitive warfare, and moral dilemmas).

The integration of IoPs has several implications for HUMINT training:

1. **Comprehensive Situational Awareness** – HUMINT operators must be trained to understand the effects of diplomatic, informational, and economic instruments in their areas of operation. These aspects are contextual and must be part of the training scenarios, while preserving an educational value.
2. **Cross-instrument coordination** – Training should emphasize cooperation with civilian agencies (e.g., diplomats, economists, cyber experts). It has to start from deciphering their specific role and access to information of intelligence interest. Military intelligence liaison has a specific stake, and its output can be injected in exercises as training vignettes. Also, sharing of awareness/ educational materials and participation in drills carried on by other elements
3. **Resilience against hybrid threats** – Operators must learn to detect disinformation, resist cognitive manipulation, and protect their sources from hostile propaganda. NATO HUMINT COE is very active in shaping the necessary skills and developing adequate educational solutions (e.g. the ADL "Information assessment – a HUMINT perspective").
4. **Application of emerging technologies** – The **transformational potential of Emerging and Disruptive Technologies (EDTs)** on HUMINT lies in their capacity to **augment human performance, expand operational reach, and enhance analytical precision**, while simultaneously

[23] Alexandru Kis (coord.), *Webbing leadership and communication in human engagement*, Centrul Tehnic-Editorial al Armatei, București, 2024.

[24] Alexandru Kis (coord.), *Turning Digital. Probing emerging competences for HUMINT professionals*, Centrul Tehnic-Editorial al Armatei, București, 2025.

redefining the nature of human–machine collaboration within intelligence. Specifically, EDTs can: [25]

- **Revolutionize HUMINT collection** by integrating advanced sensors, autonomous platforms, and AI-driven analytics that enable real-time validation, fusion, and interpretation of human-derived data.
- **Enhance operator performance** through bio and cognitive augmentation technologies (BHET), wearable systems, and smart interfaces that increase resilience, awareness, and decision-making under stress.
- **Transform education and training** via modeling and simulation (M&S), immersive virtual environments, and adaptive learning platforms that replicate complex human engagement scenarios (e.g., QUESTIX platform developed at NATO HUMINT COE, based on the QUESTIFY framework[26]).
- **Strengthen interoperability** by linking HUMINT with other C5ISR components, ensuring seamless cross-domain intelligence integration in MDO contexts.
- **Support ethical and legal compliance** by developing frameworks for responsible use of AI and automation, ensuring data protection and safeguarding human dignity.

In essence, **EDTs transform HUMINT from a purely interpersonal discipline into a hybrid human-machine enterprise**, where technology amplifies - not replaces - the human capacity for understanding motivation, intent, empathy, and perception. This evolution positions HUMINT as both **a cognitive and technological bridge** within NATO's multi-domain intelligence architecture, enabling smarter, faster, and more resilient decision-making across the continuum of operations and in connection with other IoPs.

Training ensures that HUMINT officers are not only technically proficient but also able to interpret and act within a system of interconnected domains. This requires moving from **domain-centric training models** to a **multi-domain learning framework integrated across IoPs**, emphasizing interoperability, adaptability, and cross-disciplinary literacy.

While HUMINT awareness for staff and commanders is a prerequisite for the discipline's seamless integration in the bigger picture of Intelligence and operations, a series of generic tasks/ performance statements can emerge into the

[25] Alexandru Kis, *HUMINT și tehnologiile emergente și disruptive din perspectiva operațiilor multidomeniu*, in *Impactul tehnologiilor emergente asupra securității internaționale*, coord. Alin Cîrdei și Laviniu Bojor, pp. 279-302, Editura Academiei Forțelor Terestre "Nicolae Bălcescu", Sibiu, 2025.

[26] https://www.natohcoe.org/nato-humint-coe-at-hackathuso/.

HUMINT training requirements analysis to reflect the complexity of MDO. The training requirements' sources are represented, on one hand, by top-down transformation expressed in policies and doctrines, or the implementation of various technologies, and on the other hand, by bottom-up initiatives inspired by best practices and lessons learned (a reactive process), or concept development and experimentation (a proactive process). Additionally, contextual training vignettes can also support the purpose of enlarging the vision and the practice of the HUMINT professionals.

In establishing a multi-domain HUMINT competence framework - an Alliance-wide reference for skills, knowledge, and attributes required at tactical, operational, and strategic levels, understanding how military operations intersect with political, economic, and informational activities is very important.

Training must include modules/ teaching points on hybrid warfare case studies, focusing on how non-military instruments shape the operational environment. Particularly, HUMINT operators, collators and analysts, operational managers, or technical support staff need to discover horizontal connections with elements of other IoPs, to enable:

- Crowd-sourcing – integration in the intelligence spectrum and harmonization with HUMINT operational process;
- Analytical integration – ability to fuse HUMINT with cyber, OSINT, and technical intelligence into coherent assessments that inform commanders across domains.
- Operational adaptability – capacity to shift seamlessly and secure between physical, informational, and cognitive domains during engagements.
- Enhanced source management – source validation and protection under hybrid threats, as they are increasingly exposed to risks from biometrics, pervasive surveillance, and adversary counterintelligence technologies.
- Narrative sensitivity – recognition of adversary influence operations and capacity to provide counter-narratives informed by cultural insight.
- Digital literacy – proficiency in secure digital platforms, AI-assisted tools, and data analytics relevant to HUMINT.
- Active collection on social media platforms – legal background, procedures and security for HUMINT.
- Cross-functional cooperation – ability to work effectively with diplomats, law enforcement, cyber experts, and other key persons.
- Resilience, ethics, and decision-making under pressure – HUMINT practitioners often face morally ambiguous situations, balancing operational necessity with ethical constraints.

In the assessment of correspondent performance objectives indicators such as speed and accuracy in recognizing deception cues, effective use of AI-enabled HUMINT tools in simulated environments, demonstrated resilience in ethical

decision-making during exercise vignettes, or capacity to integrate HUMINT contributions into multi-domain planning documents should be adjusted to the desired depth of knowledge and integrated into multi-disciplinary training.

Exercises remain the most powerful vehicle for preparing HUMINT professionals for MDO, and key elements include the realism of scenarios, replicating adversary hybrid tactics, and integration of cross-domain injects - HUMINT tasks should not be isolated but linked with cyber disruptions, diplomatic signaling, and economic sanctions.

Ultimately, HUMINT training in MDO is not just about producing technically skilled operators. It is about shaping multi-domain intelligence leaders capable of navigating uncertainty, integrating across instruments of power, and strengthening NATO's resilience in an era of hybrid conflict.

CONCLUSION

HUMINT and the Instruments of Power in Multi-Domain Operations

This study set out to explore how the interaction between the IoPs — diplomatic, informational, and economic — shapes the military IoP in the context of MDO, with a focus on HUMINT. The purpose was not only descriptive, but prescriptive: to identify training implications that ensure NATO and partner forces remain agile, adaptive, and resilient in the face of hybrid and multi-domain threats.

The analysis shows that while hybrid adversaries have blurred the lines between peace, crisis, and war, nations and security organizations must leverage the coordinated effects of all IoPs to respond effectively. In this continuum, HUMINT emerges as a bridge capability, linking the human dimension to the broader operational picture. While technical collection may show "what happened," HUMINT explains the "why" - the rationale behind adversary actions, the likelihood of escalation, or the vulnerabilities that can be exploited. In hybrid warfare, HUMINT also provides the cultural and contextual depth to interpret signals correctly.

Case studies like Russia's cyber-attacks, targeted crimes, disinformation campaigns, exploitation of migration flows, and the air penetrations over Europe illustrate the multi-layered use of IoPs. Each case potentially reaffirms that:

- *The Diplomatic IoP may rely on HUMINT to understand negotiations, adversary posturing, and informal channels.*
- *The Informational IoP may depend on HUMINT both as a collector of ground-truth narratives and as a counterweight to disinformation and psychological manipulation.*
- *The Economic IoP can be sharpened by HUMINT insights into corruption networks, sanctions evasion, or supply-chain vulnerabilities.*

- *The Military IoP is directly enabled by HUMINT through targeting, force protection, and operational decision support.*

Thus, in certain conditions, HUMINT may act as an enabler and amplifier of all IoPs, ensuring that decisions are grounded in human realities rather than abstract models. Given its expanded role, HUMINT professionals require training that extends beyond classical debriefing and source operations, to include digital competencies (e.g. AI-assisted analysis, social media exploitation), cultivate cross-domain literacy to understand how HUMINT interacts with diplomacy, economics, and strategic communication, strengthen resilience and ethical judgment to operate in high-pressure, morally ambiguous hybrid scenarios, and enhance cognitive agility to detect manipulation, biases, and adversarial use of disruptive technologies (e.g., deepfakes, AI-generated personas).

The integration of innovative platforms like QUESTIX and the emphasis on psychological self-regulation training are examples of how NATO HUMINT COE is already adapting to these imperatives. The Centre's academic outreach is also meant to increase understanding and interaction with other actors from the non-military IoPs with the aim to discover common denominators and foster operational synergies.

BIBLIOGRAFIE

1. NATO Allied Command Transformation, The *NATO Warfighting Capstone Concept*, Norfolk, VA., 2021, https://www.act.nato.int/our-work/nato-warfighting-capstone-concept/. ;

2. TRADOC, The U.S. Army in Multi-Domain Operations 2028, U.S. Army Training and Doctrine Command, 2018, https://www.army.mil/article/243754/the_u_s_army_in_multi_domain_operations_2028;

3. Bilal, Arsalan, *Hybrid Warfare - New Threats, Complexity, and 'Trust' as the Antidote*, November 2021, NATO Review, https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html;

4. Bojor, Laviniu, *Tehnologie dual în război: rolul telefoanelor inteligente în conflictul din Ucraina*, in *Impactul tehnologiilor emergente asupra securității internaționale,* coord. Alin Cîrdei and Laviniu Bojor, pp. 21-54, Editura Academiei Forțelor Terestre "Nicolae Bălcescu", Sibiu, 2025;

5. Carter, David L., *Law Enforcement Intelligence Guide 3.0*, Michigan State University, August 2021, https://www.researchgate.net/publication/353720175_CARTER_Law_Enforcement_Intelligence_Guide_30;

6. Fusaro, Paola; Jouan, Nicolas; Retter, Lucia and Wilkinson, Benedict, *Science and technology as a tool of power. An appraisal*, RAND Europe, November 2022,

https://www.rand.org/content/dam/rand/pubs/perspectives/PEA2300/PEA2391-1/RAND_PEA2391-1.pdf;

7. Gilli, Andrea; Gilli, Mauro and Grgić, Gorana, *NATO, multi-domain operations and the future of the Atlantic Alliance*, in *Comparative Strategy*, *44*(1), 2025, pp. 73–91, https://doi.org/10.1080/01495933.2024.2445491;

8. Gorenc, Nina, *Cultural diplomacy – the instrument of power in American foreign and security policy*, in *The Review of International Affairs*, Vol. LXVI, No. 1158-1159, April–September 2015, pp. 18-31, https://thereviewofinternationalaffairs.rs/wp-content/uploads/RI/2015/1158-1159/RI-2015-1158-1159-article-2.pdf;

9. Hartley, Dean S., *The DIME/PMESII Paradigm*, in *Unconventional Conflict. Understanding Complex Systems. Springer*, Cham, 2017, https://doi.org/10.1007/978-3-319-51935-7_4;

10. Iancu, Sînziana, *Războiul hibrid al Rusiei împotriva Occidentului. Doctrina Gherasimov, forțe paramilitare și grupurile de voluntari*, in Defense Romania, September 2024, https://www.defenseromania.ro/razboiul-hibrid-al-rusiei-impotriva-occidentului-i-doctrina-gherasimov-forte-paramilitare-ipb-si-grupurile-de-voluntari-iv_630347.html;

11. Iskandarov, K. and Gawliczek, P., *Hybrid warfare as a new type of war. The evolution of its conceptual construct*, in Miroslaw Banasik, Piotr Gawliciczek and Agnieszka Rogozinska (eds), *The Russian federation and international security*, Poland: Difin publishing house, 2020, pp. 96-107;

12. Kis, Alexandru (coord.), *Turning Digital. Probing emerging competences for HUMINT professionals*, Centrul Tehnic-Editorial al Armatei, București, 2025.

Kis, Alexandru (coord.), *Webbing leadership and communication in human engagement*, Centrul Tehnic-Editorial al Armatei, București, 2024;

13. Kis, Alexandru and Soltys, Pavol, *Human factors in Multi-Domain Operations: navigating the bivalent dynamics of human terrain and military human capital with a HUMINT lens*, in the proceedings of the 19th International Scientific Conference "Defense Resources Management in the 21st Century", Brașov, 7-8 November 2024;

14. Kis, Alexandru, *A projection of the cognitive warfare in Human Intelligence*, STRATEGIES XXI, vol. XIX, 27-28 June 2023, "Carol I" National Defence University Publishing House, Bucharest, https://www.strategii21.ro/A/2023-06. STRATEGII XXI/CONFERINTA STRATEGII XXI_2023.pdf;

15. Kis, Alexandru, *HUMINT și tehnologiile emergente și disruptive din perspectiva operațiilor multidomeniu*, in *Impactul tehnologiilor emergente asupra securității internaționale*, coord. Alin Cîrdei și Laviniu Bojor, pp. 279-302, Editura Academiei Forțelor Terestre "Nicolae Bălcescu", Sibiu, 2025;

16. Kis, Alexandru, *Subiecte transdisciplinare în NATO şi reflectarea lor la nivelul disciplinei HUMINT – securitatea umană, consideraţiile de gen și consolidarea integrităţii*, in INFOSFERA, Year XVI no. 2/2024, pp. 72-81, https://www.mapn.ro/publicatii_militare/arhiva_infosfera/documente/2024/2_2024.pdf;
17. Reichborn-Kjennerud, Erik and Cullen, Patrick, *What is Hybrid Warfare?*, Information Note January 2017, MCDC Countering Hybrid Warfare Project, https://assets.publishing.service.gov.uk/media/5b2904aded915d2cd5d01bfd/MCDC_CHW_Information_Note-Understanding_Hybrid_Warfare-Jan_2018.pdf;
18. Rodriguez, Cesar Augusto; Walton, Timothy Charles and Chu, Hyong, *Putting the "FIL" into "DIME". Growing Joint Understanding of the Instruments of Power*, Joint Doctrine - JFQ 97, 2nd Quarter 2020, pp. 121-128, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-97/jfq-97_121-128_Rodriguez-Walton-Chu.pdf?ver=2020-04-01-095603-607;
19. Schmid, Johann, *Introduction to Hybrid Warfare – A Framework for comprehensive Analysis*, in: Thiele, R. (eds) Hybrid Warfare. Edition ZfAS. Springer VS, Wiesbaden, 2021, https://doi.org/10.1007/978-3-658-35109-0_2.;
20. Schmid, Johann, *The Hybrid Face of Warfare in the 21st Century*, March 2019, https://www.maanpuolustus-lehti.fi/the-hybrid-face-of-warfare-in-the-21st-century/;
21. https://www.natohcoe.org/nato-humint-coe-at-hackathuso/.
22. https://www.thelightningpress.com/wp-content/uploads/2018/06/Conflict-Continuum.jpg.