The 19th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 7th-8th 2024

HUMAN FACTORS IN MULTI-DOMAIN OPERATIONS: NAVIGATING THE BIVALENT DYNAMICS OF HUMAN TERRAIN AND MILITARY HUMAN CAPITAL WITH A HUMINT LENS

Alexandru Kis, PhD; Pavol Soltys

NATO HUMINT Centre of Excellence/ Oradea/ Romania

Abstract:
The Multi-Domain Operations (MDO) concept represents a comprehensive and integrated approach to modern warfare, reflecting the need for contemporary military organizations to address the increasingly complex and interconnected nature of global security challenges. To remain effective, intelligence agencies will need to adapt to a large array of changes, adopt new technologies (while increasing their digital competencies), integrate cross-cutting dimensions, align to operational approaches, and embrace evolving ethical constraints to navigate the complexities of modern societies while maintaining their ability to collect reliable intelligence.
Additionally, the imprint of societal transformation on the future "human terrain" leads to specific challenges and opportunities in the HUMINT tradecraft. The paper identifies the intrinsic relation between the civil consideration in the operational environment analysis and the main transformational directions for the human capital in HUMINT to meet the demands of the "right people, right skills" approach in the NATO MDO philosophy.
Disclaimer: This paper expresses the views, interpretations, and independent positions of the authors. It should not be regarded as an official document, nor expressing formal opinions or policies of NATO or the NATO HUMINT Centre of Excellence.
Key words: Multi-Domain Operations; HUMINT; skills; technology; human terrain

1. Introduction. A glimpse into the multi-domain operations

Multi-Domain Operations (MDO) is a modern military concept designed to address challenges from state and non-state actors by integrating and synchronizing actions across interconnected domains, including land, air, sea, space, and cyberspace, with a strong emphasis on emerging technologies. [1]

NATO defines MDO as the orchestration [2] of military activities, across all domains and environments, synchronized with non-military activities, enabling the Alliance to create converging effects at the speed of relevance. The philosophy of NATO's MDO concept is grounded in the recognition that future conflicts cannot be confined to a single domain - land, air, sea, cyber, or space. Instead, these conflicts will span multiple domains simultaneously and are intertwined with political, economic, and social factors, requiring a more holistic approach to warfare and synchronization of military efforts with non-military activities to achieve comprehensive effects.

MDO represents a pivotal shift in NATO's approach. This transformative concept replaces the joint operations [3] philosophy and empowers the Alliance to strategically influence events at the right time and place through military and non-military activities and synchronization of the efforts with external stakeholders (including partner nations, international organizations, and industry). This emphasizes the need for seamless

integration of NATO's capabilities and allied countries' military systems across all domains to achieve a decisive advantage over adversaries. Given the diverse nature of national capabilities at NATO level, the focus is on interoperability and ensuring that multinational forces can work together effectively. This approach places a significant weight on standardization and training to achieve this goal.

At the operational level, NATO's MDO approach advocates for a unified, agile, and flexible force structure capable of operating effectively in any environment, across any domain. This adaptability is vital for maintaining operational momentum and exploiting opportunities in a fluid battlespace. Furthermore, achieving decision superiority is a key principle of MDO. This involves the ability to collect, process, and disseminate information faster and more accurately than the adversary, enabling NATO commanders to make informed decisions that outpace the enemy's actions. In this context, leaders' creativity (enhanced by an ability to visualize context and settings) relies on the capacity to analyze situations from different viewpoints and turn complexity into simplicity.

Interconnectivity, as an MDO principle, enhances situational awareness, decision-making, responsiveness, and shared understanding across all Instruments of Power (IoP), partners, and stakeholders, and enables warfighting interoperability between force elements. It is challenged by differences between legacy and modern platforms (e.g. lack of technical interoperability), and by data classification. It must be resilient and requires standardized data to support user requirements.

MDO enablers include advanced data analytics and intelligence systems, which provide comprehensive situational awareness and support informed decision-making. Technological advancements play a significant role, in driving the development of cutting-edge weapons, communication networks, and cyber capabilities. The principle of having the "right people with the right skills" underscores the importance of highly trained personnel who can operate effectively in this complex, multi-domain environment. Capitalizing on education and individual training, collective training exercises ensure interoperability and seamless cooperation among different military branches and allied forces. Finally, cross-domain command structures are essential for maintaining strategic oversight and directing synchronized operations across all domains. Together, these enablers form the foundation for a flexible, adaptive, and highly effective MDO strategy.

We will further investigate how the society of the future will influence the transformation of the human intelligence (HUMINT) capability to meet the performance requirements in an MDO environment and what is expected at the individual level in terms of knowledge, skills, and attitudes.

2. A multi-domain society – the future human terrain of military operations

In the MDO context, HUMINT involves, invariably, the collection and analysis of information derived from human sources, providing critical insights into adversaries' intentions, capabilities, and vulnerabilities. As HUMINT heavily relies on interpersonal skills, cultural understanding, and human networks, the future battlespace, influenced by societal changes, will transform its nature, presenting both challenges and opportunities in collection activities and analysis, under the pressure of technological evolution, urbanization, demographics, and communication trends.

An evolving society under the MDO scoping can be characterized by its complexity and interconnectedness across multiple domains and layers that impact social, economic, political, and technological activities. These domains, often overlapping, influence each other and shape the dynamics of society in various ways.

HUMAN FACTORS IN MULTI-DOMAIN OPERATIONS: NAVIGATING THE BIVALENT DYNAMICS OF HUMAN TERRAIN AND MILITARY HUMAN CAPITAL WITH A HUMINT LENS

Physical and virtual spaces are deeply intertwined. Economic activities, social interactions, and even political processes occur simultaneously in both physical locations (e.g., cities, workplaces, institutions) and virtual environments (e.g., social media, online marketplaces, digital platforms). The boundaries between these domains are increasingly blurred as more aspects of daily life are conducted online, facilitated by digital infrastructures like cloud computing, the Internet of Things (IoT), and mobile networks.

The digital transformation of society has created a distinct cyber domain where information and data flow shape behavior, decision-making, and governance. Cybersecurity, data privacy, and the management of digital identities are critical issues. In the information domain, the flow of information, whether through traditional media, social media, or state-controlled outlets, plays a key role in influencing public opinion, economic trends, and geopolitical outcomes. Societal resilience in this domain requires strong digital literacy, critical thinking, and regulatory frameworks to prevent misinformation, cyberattacks, and digital manipulation.

Globalization has resulted in high levels of connectivity and mobility in modern societies, but also generates perspectives for a "world of disruption" [4]. People, goods, and information move quickly and across borders, linking diverse regions and cultures. Migration, international trade, and global communication networks contribute to the global nature of society, affecting its cultural diversity, economic strategies, and geopolitical positioning. This high degree of global integration also makes societies vulnerable to global crises, such as pandemics, cognitive polarization, exposure to climate change effects, or supply chain disruptions, which can impact multiple domains simultaneously.

Ecological factors like resource availability, global warming, and natural disasters increasingly influence social, economic, and political stability.[5] The intersection of climate issues with other challenges, such as migration, food security, and energy needs, demands that societies adopt holistic approaches to sustainability and resilience and integrate environmental considerations into urban planning, national security, and economic development strategies.

Ultimately, the governance of a multi-domain society requires frameworks that span across multiple sectors and areas of influence. This includes regulations on data privacy, cyber security, environmental protection, intellectual property, and global trade. Governments must coordinate with international organizations, private enterprises, and civil society to regulate these domains effectively, ensuring that societal needs are balanced with the protection of individual rights and national interests.

Norms surrounding ethics, privacy, and human rights will increasingly influence intelligence practices, including HUMINT. Growing awareness of privacy issues and human rights violations may place constraints on the methods and techniques used by intelligence agencies to collect information from human sources. Public scrutiny of intelligence operations, especially in democratic societies, may limit the ability of intelligence agencies to conduct covert operations. The demand for transparency and accountability in military and intelligence activities will require HUMINT operatives to balance operational effectiveness with ethical considerations, making recruitment and handling of sources more complex.

Increased global mobility and migration patterns influence HUMINT by expanding the reach of intelligence agencies beyond traditional national borders. The movement of populations, particularly refugees and migrants from conflict zones, offers new opportunities to collect intelligence from diverse human sources with firsthand knowledge of adversaries, hostile environments, or emerging threats.

However, the fluid nature of global migration also complicates HUMINT, as sources may be difficult to locate, transient, or less likely to establish long-term relationships with intelligence officers. Additionally, the transnational nature of many intelligence threats, including terrorism and organized crime, will require HUMINT officers to operate across cultural and national boundaries, necessitating a deeper understanding of the socio-political contexts in which sources operate.

Cultural values, social norms, and belief systems influence behavior and decision-making within a multi-domain society. Cognitive warfare - shaping the perceptions, beliefs, and behaviors of populations through propaganda, psychological operations, and information campaigns - becomes a more and more important factor. The digital age has amplified the relevance of the cognitive domain by allowing for widespread influence through social media and online platforms. Societal divisions, political polarization, and cultural shifts can be influenced or even exacerbated by the manipulation of information in these spaces. [6]

In the wake of cognitive warfare, the rise of digital societies and the ubiquity of online communication significantly impact HUMINT. Social media, encrypted messaging, and digital platforms are becoming integral parts of daily life, making them key arenas for intelligence operations. While the internet provides new avenues for identifying, recruiting, and communicating with human sources, it also creates challenges in terms of verifying information and steering the anonymity of online platforms. Moreover, adversaries can easily spread disinformation through these same channels, complicating efforts to obtain reliable information. [7] In addition, surveillance technologies and cybersecurity measures implemented by both state and non-state actors may make it harder to protect the identities of human sources or conduct discreet operations in the physical or digital spheres.

Social fragmentation is also fueled by ethnic, religious, or political tensions, which may create opportunities for HUMINT, as marginalized or disaffected groups could provide valuable intelligence. However, these same demographic shifts may also complicate intelligence operations, as competing narratives, misinformation, and distrust in institutions become more widespread. In many regions, generational divides could influence the willingness of individuals to cooperate with intelligence agencies. Younger generations, particularly those deeply embedded in digital and online communities, may be more resistant to traditional recruitment methods. HUMINT officers will need to adapt their approaches to account for these societal shifts, becoming experts in intersectional interactions [8].

In this context, military and defence strategies are no longer confined to traditional, physical battlefields. Cyber warfare, space-based technologies, and advanced surveillance have expanded the battlefield into new domains like cyber and space, with disruptive effects in the physical, virtual, and cognitive dimensions. Geopolitical competition is played out in these interconnected domains, with countries seeking to gain strategic advantages through technological superiority, cyber capabilities, and control over information flows.

The war in Ukraine highlights how urbanization is making densely populated cities central to conflicts, escalating risks of civilian casualties and humanitarian crises as a result of mass displacements due to essential services disruption. Urban warfare complicates military tactics by restricting mobility, targeting, and force concentration while blurring the line between combatants and civilians. It often involves non-state actors, insurgents, or irregular forces embedded within civilian populations, making HUMINT essential for distinguishing combatants from non-combatants. However, this also increases the risk of

misinformation and false reporting, as civilian populations may be coerced or influenced by adversaries. [9]

The urbanization tendency will complicate HUMINT activities, as collecting intelligence in heavily populated areas poses significant challenges. Dense populations provide cover for adversaries but also offer vast opportunities for intelligence gathering from civilians, local leaders, and social networks. Collecting reliable intelligence will require not only traditional HUMINT techniques but also deep cultural and social knowledge of urban societies.

Additionally, societal trends toward increased surveillance, often justified by concerns about security and crime prevention, affect HUMINT activities. Governments, corporations, and individuals have access to advanced surveillance technologies such as facial recognition, biometric tracking, and AI-driven monitoring tools. While these technologies may aid intelligence agencies in tracking individuals of interest, they also reduce the privacy of operatives and human sources, heightening the risk of exposure.

This heightened surveillance environment could limit traditional HUMINT operations, as adversaries and other actors may be able to detect or monitor intelligence activities more easily. Human sources, especially in authoritarian or highly monitored societies, may be less willing to engage in intelligence activities due to fear of exposure or reprisal.

Another significant aspect of the conflict evolution is the peacetime contestation actions. Being not at war, as NATO Secretary General Jens Stoltenberg reiterated in his last official visit to Norway, on September 5, 2024, there are no immediate military threats [10] against NATO countries but there is a constant danger of terrorism, cyber-attacks, and sabotage that don't make our countries safer [11]. Since the war in Ukraine began, Russia has significantly escalated its cyberattacks across Europe, targeting critical sectors (government institutions, energy grids, financial systems, and transportation networks), has engaged in sabotage operations, directed towards the military industry, storage, and transportation infrastructure, and ramped up its information warfare by spreading disinformation and conspiracy theories through state-controlled media and social media platforms, and supporting radical groups to further undermine European stability. These efforts aim to polarize European societies, fuel division, and weaken democratic institutions. Countries like France, Germany, and those in Eastern Europe have been primary targets, intending to create internal discord and reduce Europe's unified response to Russia's actions. Russian intelligence services have also been linked to covert terrorist activities, including assassination attempts not only on dissidents, defectors, and critics of the Russian government but also on important figures in military organizations and industry.

Additionally, the rise of non-state actors and asymmetric warfare is accounted as a serious threat by NATO's strategic concept [12]. Non-state actors, including terrorist groups, insurgencies, and criminal organizations, play a significant role in peacetime contestation activities, or within the threat spectrum of the future battlefield. These groups often operate in decentralized networks and employ asymmetric warfare tactics, making traditional HUMINT approaches more difficult. Recruiting sources within these groups will require sophisticated cultural knowledge and a nuanced understanding of local loyalties, ideologies, and motivations. The proliferation of non-state actors also means that HUMINT activities will increasingly involve cooperation with a wide array of stakeholders, including local militias, private security firms, and even non-governmental organizations (NGOs). Intelligence agencies will need to navigate these complex networks to effectively gather and analyze human intelligence.

The ongoing conflict in Ukraine has reinforced the enduring importance of kinetic warfare principles – unity of command, territorial control, force protection, range, precision, and lethality – while highlighting the transformative role of emerging technologies like artificial intelligence (AI), global communication networks and space-based assets, and autonomous systems in situational awareness, decision-making, communication and coordination, and operational agility. [13]

Future expectation is that ever-changing conditions regarding the interactions among diverse actors, adaptable strategies, multiple operational domains, advanced capabilities, societal changes and trends, and the impact of global, regional, and local factors will transpose the societal features (the "human terrain") across the physical, cognitive, and virtual dimensions, presenting both challenges and opportunities for military forces, to include intelligence capabilities, which will need to adapt to a rapidly changing environment where traditional concepts of warfare are complemented by cyber capabilities, information operations, and the integration of emerging technologies.

To remain effective, intelligence agencies will need to adapt to these changes, adopt new technologies (while increasing their digital competencies), integrate cross-cutting elements [14], align to operational approaches, and embrace evolving ethical constraints, to navigate the complexities of modern societies while maintaining their ability to collect reliable intelligence from human sources.

3. The technological emphasis in multi-domain operations

The rapid pace of technological advancements, particularly in cyber, artificial intelligence (AI), and space environments, makes the MDO concept increasingly relevant in influencing military strategies. By integrating technologies in capability development and employing them in operations, military organizations can maintain a competitive edge over potential adversaries.

In a recent article [15], Bill Burns, Director of the US Central Intelligence Agency (CIA), and Richard Moore, Chief of the UK Secret Intelligence Service (SIS), pointed out the revolutionary impact of technology in the conflict in Ukraine, under the imperative to adapt, experiment and innovate facing a much stronger conventional enemy. As noted by the two prominent authors, this conflict represents the first one where open-source software is integrated with advanced battlefield technology, leveraging a combination of commercial and military satellite imagery, drone systems, unmanned aerial and maritime vehicles, a blend of sophisticated and rudimentary cyber warfare tactics, social media, open-source intelligence, and information operations, alongside human and signals intelligence, all at an unprecedented pace and scale.

The future battlespace will be shaped by pervasive technology, with enhanced surveillance, monitoring, and automation becoming key features in convalescing lethality, mobility, and concealment. Technological advantage is a critical enabler for the readiness and adaptability of the Military Instrument of Power (MIoP).[16] While nations advancing the MDO approach in their military strategies (e.g. USA [17] [18] and UK [19]) invest heavily in research and development to maintain a technological edge, with a focus on integrating cutting-edge technologies into operational planning and execution, NATO's approach is more focused on ensuring that member states can integrate and use these technologies within a collective framework, contributing effectively to MDO through interoperability and shared systems: AI-driven predictive analytics enhance situational awareness, enabling rapid response to dynamic threats; machine learning algorithms process vast amounts of data, identifying patterns and anomalies that human operators might miss; bio-human enhancements, such as wearable sensors and neural interfaces,

empower soldiers with real-time health monitoring and cognitive augmentation, enhancing their performance across domains.[20]

The impact of technology can be yet more dramatic if legal, procedural, or ethical barriers are flexible. AI's involvement in social media is revolutionary not only for information operations but also for intelligence activities. With access to vast amounts of social media data, AI systems can analyze behaviors, identify and profile key influencers and human networks, craft personalized messages designed to retrieve information, and even more, manipulate opinions and decisions up to influencing larger populations (based on human predisposition toward quick, emotional decision-making [21]). Advanced AI avatars or personas can interact with social media users, mimicking human behavior and gaining trust as part of social engineering and deep fake attempts.

A critical role of AI in HUMINT is its capacity to manage vast amounts of data, alleviating the challenge of information overload. AI systems can monitor social media applications and informational platforms in real-time, flagging critical discussions, shifts in public opinion, information of intelligence interest, or security vulnerabilities. However, the complexity of AI systems introduces risks, such as the potential for misinterpretation of data, biases in algorithms, or a lack of transparency, which could lead to faulty conclusions or misguided decisions.

Anyway, as technology becomes central to warfare, adversaries may resort to low-tech, asymmetric strategies to counter these capabilities and ensure comparable assets. Both state and non-state actors will utilize advanced tools such as sensors, satellite networks, AI, and real-time data analytics for greater precision, requiring adapted countermeasures.

MDO demands a data-centric [22] approach that recognizes data as a strategic asset. In practical terms, this involves empowering people to derive maximum value from data, establishing coherent policies and processes for data exploitation, and creating a secure and governed environment for data within NATO. [23]

MDO needs a stronger digital infrastructure (“digital backbone” [24]) to link Alliance forces across various domains and command levels, as well as with non-military stakeholders. This network must ensure real-time data collection, storage, and analysis, while also enhancing NATO's collaboration with national systems and non-military expertise. Additionally, it must be flexible enough to incorporate emerging technologies that support MDO execution. Additionally, digital transformation plays a vital role in achieving this objective, allowing NATO to appreciate, share, exchange, and exploit data effectively. [25]

HUMINT can leverage NATO’s digital backbone, which aims to enhance connectivity and data transport across domains. By integrating with this backbone, HUMINT can seamlessly share information across military and non-military domains, ensuring timely and relevant intelligence dissemination. By adopting standardized data formats and procedures, HUMINT can ensure that its insights are easily accessible and usable by other domains, enhancing overall situational awareness and operational coherence. Additionally, HUMINT must engage in continuous collaboration and information exchange with other intelligence disciplines, to enrich and corroborate its findings. This interconnected approach allows for a more comprehensive understanding of the operational environment, enabling military forces and commanders to anticipate and respond to threats more effectively.

By embedding itself within the multi-domain framework, HUMINT ensures that its valuable human-centric insights contribute to a unified and agile operational strategy.

4. Right people, right skills. Emergent requirements for the human capital in HUMINT

The NATO Warfighting Capstone Concept, endorsed in 2021, aims to guide NATO's military adaptation over the next 20 years, focusing on maintaining an advantage against adversaries [26]. Central to its implementation is the Alliance Warfare Development Agenda (WDA), which aligns NATO's warfare development activities around five key imperatives: Cognitive Superiority, Layered Resilience, Influence and Power Projection, Cross-domain Command, and Integrated Multi-Domain Defence. [27]

A crucial aspect of the WDA is the "right people with the right skills" dimension. NATO recognizes that technological advancement alone is insufficient without skilled personnel to utilize and manage these capabilities effectively. The agenda emphasizes improving workforce connectivity and ensuring that the right talents are in place to enable multi-domain operations. These skilled professionals are essential enablers, alongside data, technology, and agility, to maintain NATO's competitive edge.

The integration of HUMINT into MDO ensures that human-driven intelligence is utilized effectively to anticipate and counter complex, multi-domain threats, thereby enhancing the decision-making process and operational outcomes in a highly interconnected and dynamic battlespace.

HUMINT requires creativity in both collection methods and analytical approaches. HUMINT operators must employ innovative techniques to gather intelligence from diverse sources, including leveraging technology, social networks, and cultural understanding. Similarly, analysts must apply creative thinking and analytical skills to derive actionable insights from raw intelligence data, identifying patterns, trends, and anomalies that may not be immediately apparent.

In a multi-domain environment, military personnel must possess a diverse skill set [28], with competencies spanning the military specialty, as well as technological proficiency, cross-domain coordination, and cultural intelligence. For instance, in the realm of HUMINT collection, a professional must not only excel in traditional interpersonal skills - such as building rapport and assessing human behavior - but also be adept in digital literacy, including analyzing social media patterns, utilizing AI tools, and interpreting cyber vulnerabilities. Additionally, HUMINT professionals must develop cognitive flexibility to operate seamlessly across domains - whether in physical combat environments, cyberspace, or within psychological and information operations.

Besides cultural awareness and sensitiveness, effective training in data analysis, cybersecurity, and AI integration (as part of an enhanced digital literacy [29]) will ensure that HUMINT professionals are not only collecting but also correctly interpreting information from multi-layered environments. Adaptability, quick learning, and collaboration with tech specialists are critical for these roles, highlighting the growing necessity for interdisciplinary, customized teams that combine traditional military expertise with modern technological insights.

This requires rigorous and continuous training programs that are updated to reflect the latest technological advancements and emerging threats. Hands-on training with various platforms and technical devices becomes a must, and concept development and experimentation are at the spearhead of adapting emerging technologies to the evolving needs of HUMINT.

Moreover, interdisciplinary collaboration and cross-cutting training are vital to foster a comprehensive understanding of how various domains intersect and influence each other. Collective training is a vital enabler of MDO, as it ensures that forces from various branches and member nations can operate seamlessly and effectively together. Collective

training must be enhanced to include scenarios that incorporate a higher level of complexity. The creation of blended live-synthetic training to generate multi-domain realism is essential to the development of an MDO-enabled force. It is also applicable to HUMINT, where modeling the "human terrain" should mirror the technical dimensions, communication patterns, and trends of modern society.

The future combat soldier will require a versatile mindset and technological literacy, seamlessly integrating technology with human capabilities. In MDO - where conflicts span land, sea, air, space, and cyberspace - situational awareness and operational agility will be paramount; it will be the result of processing vast amounts of real-time data across multiple platforms, requiring cognitive agility and the ability to make rapid decisions under pressure.

Based on current trends in research, soldiers will be equipped with enhanced body armor and smart uniforms, night vision goggles and augmented reality headsets, advanced weapon systems, and communication devices, enhancing survivability and effectiveness. Robotic technology will enhance combat capabilities, with soldiers collaborating alongside autonomous systems like drones, ground robots, and exoskeletons. This synergy will extend soldiers' operational range and allow for advanced reconnaissance, targeting, and logistical support. Wearable for HUMINT operators would also aim to improve protection, communication, human engagement support, data collection and retention, in a more discreet manner. Understanding and managing these technologies will be crucial, as soldiers would have to control, maintain, and cooperate with robotic systems in dynamic environments.

Another critical line of development for improving the soldier’s capacity is represented by Bio and Human Enhancement Technologies (BHET), in the areas of Gene Editing, Bio-Engineering, Cognitive Enhancement, and Human-Machine Symbiosis [30]. Wounds care, disease prevention, performance drugs, regeneration, cognitive health and enhanced function, well-being and behavioral responses monitoring are just several dimensions supporting the soldier's physiological performance in operation, with a due application at the level of the HUMINT personnel.

5. Conclusions

MDO is a paradigm shift and a forward-looking approach to modern warfare that allows NATO to operate seamlessly across domains and environments, synchronizing military activities within multinational joint forces and integrating non-military elements (diplomatic, informational, economic instruments of power) in the continuum of conflict, from enhanced deterrence [31] to maintain a strategic advantage over adversaries [32]. Through MDO integration, NATO demonstrates its commitment to maintaining its strategic edge in a rapidly evolving global security environment.

The growing digitization of society (and warfare) will transform objects, individuals, and areas into entities with digital footprints, expanding conflict into virtual and augmented spaces. As a consequence, digital infrastructure, identities, and public perception become a target for cyber warfare, with significant implications for information manipulation, and intelligence collection and processing. Emerging technologies, such as AI, quantum sensors, and robotics, will reshape the battlefield and expand the scope of cyber operations, creating a more complex, densely interconnected digital battlespace.

Technological advancements are crucial in shaping MDO and enhancing military strategies. Integrating commercial and military technologies, as seen in the war in Ukraine, is key to maintaining a competitive edge. AI-driven analytics, machine learning, and bio-enhancements boost surveillance, decision-making, and soldier performance. To

orchestrate the instruments of power, MDO demands a data-centric approach and robust digital infrastructure to link military and non-military stakeholders.

HUMINT's view of the future must include the integration of collection, analytical, management, and support assets with technological networks, ensuring timely and relevant performances. Starting from a projection of the future HUMINT team's profile, the supporting toolset and systems have to keep pace with the technological evolution. From this perspective, concept development and experimentation are paramount in determining the way ahead in technological investments. In any context, besides performance objectives correlated with new capabilities, adapted education and training should focus on the HUMINT professionals' digital literacy - proficiency in utilizing digital tools and platforms for information gathering, data analysis, cybersecurity awareness (including adversaries' low-tech, asymmetric strategies), and social media engagement, enhancing their effectiveness in a complex, technology-driven environment.

MDO also considers the transformation of the human dimension (sociocultural, psychological, and behavioral aspects of populations) in the future operational environment. The future human terrain of military operations is complex, being shaped by societal, technological, and environmental changes. HUMINT will face new challenges and opportunities as it adapts to urbanization, migration, and the rise of digital societies. The interconnectedness of physical and virtual domains complicates intelligence collection, as disinformation, surveillance, and societal fragmentation increase. Cognitive competencies, cultural sensitiveness, intersectional engagement skills, cross-cutting awareness, self-regulation and optimization techniques will drive the future performance of the HUMINTers engaged in continuous development programs, as part of the mindset adaptation to MDO and a comprehensive understanding of the operational environment [33].

The MDO approach in the HUMINT tradecraft will parallel top-down capability integration and organizational adaptation and interconnection, being centered on human capital enhancement, where relevant organizations – like the NATO HUMINT Centre of Excellence from Oradea, Romania – have a major stake.

References:

[1] Ionela Cătălina Manolache, *The role of multi-domain operations in modern warfare*, Revista Academiei Forţelor Terestre nr. 3 (111)/2023, https://www.armyacademy.ro/reviste/rev3_2023/Manolache_RAFT_3_2023.pdf.

[2] Orchestration is the arrangement and coordination of military activities across domains – and affecting all levels – that align with the commanders' intent to achieve converging effects in support of military objectives. (Allied Command Transformation, *Next Generation Command and Control*, December 6, 2023, https://www.act.nato.int/article/next-generation-c2/).

[3] Many military forces within the NATO ecosystem have "Joint" military capabilities. In the post-World War II restructuring of military forces, the emergence of integrated command structures that cut through inter-service rivalries was common throughout the militaries of NATO members. These "Joint" capabilities are associated with a collective focus and cooperation between traditional military services. However, "Joint" command structures promote coordination with other armed services, while a "Multi-Domain" mindset must go beyond that to include military and non-military assets, which is the key differentiating factor between "Joint" and "Multi-Domain" Operations and also became a feature of modern national military forces. (Allied Command Transformation,

Multi-Domain Operations in NATO – Explained, October 5, 2023, https://www.act.nato.int/article/mdo-in-nato-explained/).

[4] McKinsey Global Institute, *Navigating a world of disruption*, January 22, 2019, https://www.mckinsey.com/featured-insights/innovation-and-growth/navigating-a-world-of-disruption.

[5] UN SC, 8923RD Meeting SC/14728, People, *Countries Impacted by Climate Change Also Vulnerable to Terrorist Recruitment, Violence*, open debate, 9 December 2021, https://press.un.org/en/2021/sc14728.doc.htm.

[6] Cornelis van der Klaauw, *The 21st-Century Game Changer. Cognitive Warfare*, The Three Swords Magazine, 39, Joint Warfare Centre, Stavanger, 2023, p. 97.

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

[8] Alexandru Kis (coordinator), *Webbing leadership and communication in human engagement*, under revision for publication by the Army Technical-Publishing Center, Bucharest, 2024.

[9] Alexandru Kis, *The Intelligence importance in the war in Ukraine – a HUMINT perspective to the Human Terrain*, under publication in EUROLIMES, University of Oradea Publishing House, 2024.

[10] Not minimalizing the threat posed by Russian rockets and unmanned air systems penetrating the national airspace of NATO Eastern countries.

[11] Gwladys Fouche, *Ukraine has achieved 'a lot' in Kursk offensive, NATO's Stoltenberg says*, September 5, 2024, https://www.reuters.com/world/europe/ukraine-has-achieved-a-lot-kursk-offensive-natos-stoltenberg-says-2024-09-05/.

[12] NATO 2022 Strategic Concept Adopted by Heads of State and Government at the NATO Summit in Madrid, 29 June 2022, pp. 4-5, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

[13] Franklin D. Kramer, Ann Marie Dailey, Joslyn Brodfuehrer, NATO multidomain operations: Near- and medium-term priority initiatives, *Atlantic Council, Scowcroft Center for Strategy and Security, Washington DC, 2023, https://www.atlanticcouncil.org/wp-content/uploads/2024/03/NATO-multidomain-operations-Near-and-medium-term-priority-initiatives.pdf.*

[14] Alexandru Kis, *Subiecte transdisciplinare în NATO şi reflectarea lor la nivelul disciplinei HUMINT – securitatea umană, consideraţiile de gen şi consolidarea integrităţii (Cross-cutting topics in NATO and their reflection in HUMINT – human security, gender, and building integrity)*, in INFOSFERA, Year XVI no. 2/2024, pp. 72-81, https://www.mapn.ro/publicatii_militare/arhiva_infosfera/documente/2024/2_2024.pdf.

[15] Bill Burns, Richard Moore, *Intelligence partnership helps the US and UK stay ahead in an uncertain world. Technological advantage is key to ensuring the special relationship maintains its lead*, in The Financial Times, September 7, 2024, https://www.ft.com/content/252d7cc6-27de-46c0-9697-f3eb04888e70.

[16] Allied Command Transformation, *Empowering NATO's Multi-Domain Operations Through Digital Transformation*, October 16, 2023, https://www.act.nato.int/article/empowering-nato-mdo-through-digital-transformation/.

[17] Jen Judson, *US Army adopts new multidomain operations doctrine*, October 2022, https://www.defensenews.com/land/2022/10/10/us-army-adopts-new-multidomain-operations-doctrine/.
[18] Congressional Research Service, *Defense Primer: Army Multi-Domain Operations (MDO)*, January 2, 2024, https://crsreports.congress.gov/product/pdf/IF/IF11409.
[19] UK MOD, Joint Concept Note 1/20 Multi-Domain Integration, November 2020, https://assets.publishing.service.gov.uk/media/6579c11a254aaa000d050c6e/20201112-ARCHIVE_JCN_1_20_MDI_Official.pdf; the publication was further archived by the UK Ministry of Defence with the adoption of the NATO concept for MDO.
[20] World Economic Forum, *These are the top 10 emerging technologies of 2023: Here's how they can impact the world*, June 26, 2023, https://www.weforum.org/agenda/2023/06/emerging-technologies-innovation-2023/.
[21] Daniel Kahneman, *Thinking, Fast and Slow*, Ed. Farrar, Straus and Giroux, New York, 2021.
[22] According to NATO's Data Exploitation Framework Strategic Plan, being "data-centric" means fully leveraging the value of NATO-generated, national, and publicly available data to achieve information superiority and data-driven decision-making at all levels across the Alliance (NATO, *Summary of NATO's Data Exploitation Framework Strategic Plan*, October 13, 2022, https://www.nato.int/cps/en/natohq/official_texts_209999.htm).
[23] NATO, *Summary of NATO's Data Exploitation Framework Strategic Plan*, October 13, 2022, https://www.nato.int/cps/en/natohq/official_texts_209999.htm.
[24] Allied Command Transformation, *Empowering NATO's Multi-Domain Operations Through Digital Transformation*, October 16, 2023, https://www.act.nato.int/article/empowering-nato-mdo-through-digital-transformation/.
[25] Allied Command Transformation, Multi-Domain Operations: Enabling NATO to Out-pace and Out-think its Adversaries, *July 29, 2022, https://www.act.nato.int/article/multi-domain-operations-enabling-nato-to-out-pace-and-out-think-its-adversaries/*.
[26] John W. Tammen, *NATO's Warfighting Capstone Concept: anticipating the changing character of war*, NATO Review, July 09, 2021, https://www.nato.int/docu/review/articles/2021/07/09/natos-warfighting-capstone-concept-anticipating-the-changing-character-of-war/index.html.
[27] Allied Command Transformation, *The Alliance's Warfare Development Agenda: Achieving a 20-year Transformation*, March 29, 2022, https://www.act.nato.int/article/the-alliances-warfare-development-agenda-achieving-a-20-year-transformation/.
[28] Alexandru Kis, Vasilică Arhip, Oliver Tarcala, *Skills and Traits of the HUMINT Operator*, in the volume of the 14th International Scientific Conference *Defense Resources Management in the 21st Century*, DRESMARA, Braşov, 07-08 November 2019.
[29] Margaret Rouse, *Digital Literacy (Digital Fluency)*, July 10, 2023, https://www.techopedia.com/definition/digital-literacy-digital-fluency.
[30] NATO Science and Technology Organization, *Science & Technology Trends 2023-2043*, Brussels, 2023.
[31] NATO Innovation Podcast, *Multi-Domain Operations: The NATO Perspective*, December 22, 2022, https://podcasters.spotify.com/pod/show/natoinnovation/episodes/Multi-Domain-Operations-The-NATO-Perspective-e1sju3q.
[32] Allied Command Transformation, *Multi-Domain Operations: Enabling NATO to Out-pace and Out-think its Adversaries*, July 29, 2022,

https://www.act.nato.int/article/multi-domain-operations-enabling-nato-to-out-pace-and-out-think-its-adversaries/.
[33] US Army, *FM 3.0 Operations*, October 2022, pp. 1-16 – 1-17, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf.