The Role of Joint Intelligence Preparation of the Operating Environment in Support of Future Military Operations

Radovan VASICEK
The University of Defence, Brno
THE CZECH REPUBLIC

radovan.vasicek@unob.cz

Petr HLAVIZNA, PhD.
The University of Defence, Brno
THE CZECH REPUBLIC

petr.hlavizna@unob.cz

ABSTRACT

Contemporary and emerging security threats as well as lessons learned from recent military operations have already proved that in order to achieve operational objectives in the traditional physical domains (land, air, maritime, space) it is crucial to ensure dominance in the non-physical domains, i.e. the cyberspace, electromagnetic environment (EME) and information environment. Therefore, besides the physical operating domains, the ability to achieve dominance in the non-physical domains will be decisive for achievement of both military and non-military objectives of the campaign.

The operational battle staff will be challenged to deconflict, coordinate, synchronize and integrate their operations in order to enable and deliver the synergic effect to confront multiple threats which may also include operations below the threshold of armed conflict from adversaries in every operating domain, including the non-physical ones.

The article examines the role and significance of Joint Intelligence Preparation of the Operating Environment (JIPOE) as one of the primary tools used to support joint operation planning, execution and assessment, thus contributing to synchronization and orchestration of multi-domain operations (MDO). In this respect, it is not possible to limit the analysis of the contemporary operating environment (OE), based on the Political, Military, Economic, Information, Infrastructure-Physical, Time (PMESII-PT) approach, only to the physical domains and their relationship to the non-physical ones. On the contrary, the authors are convinced that identification of a suitable method focused on effects of activities conducted either individually or jointly in the non-physical domains, their mutual convergence and relevance to the physical operating domains across all PMESII-PT areas will significantly contribute to the friendly forces' ability to identify and assess the adversary's centre of gravity (COG), critical vulnerabilities, intentions and courses of action (COAs), including respective indicators Thus, JIPOE products will provide the Joint Force Commander (JFC) with a holistic view of the OE which will be shared and developed in close cooperation with tactical level which should be able to overwhelm an adversary's forces by combining capabilities across different domains. This centralized control and decentralized execution approach will be instrumental for creation of synergy of effects between the operational and tactical levels.

1.0 INTRODUCTION

Future military operations will be characterized by the fusion of physical and non-physical dimensions, in which a multitude of different actors will operate. Any forces will need to adapt to an extremely complex OE and a vast number of operational variables, requiring the adaptive use a range of weapon systems to produce

both lethal and non-lethal effects. Therefore, besides the physical operating domains (i.e. land, air, maritime and space), the ability to achieve dominance in the non-physical domains (cyberspace, EME, information environment) will be decisive for achievement of both military and non-military objectives of the campaign [1, p. 280].

The OE is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander [2, p. 3]. Understanding factors and conditions of the OE is a critical prerequisite not only for all planning activities, particularly for operations design, but also for friendly force protection and many other related tasks [3, p. 41].

JIPOE represents a systematic methodology used to analyse information about the OE and the adversary. It can be applied to the full range of military operations. The commander and the staff develop a shared understanding and a holistic view of the OE in terms of the crisis background, the underlying causes and the specific dynamics. It allows the commander to visualize the extent of the problem and how they might shape and alter the OE to their advantage, which will inform their decision-making [2, p. 3–5].

JIPOE products significantly contribute to planning and execution of military operations at the joint (i.e. operational) level. Modern militaries, particularly those within the North Atlantic Treaty Organization (NATO), have for decades used the term joint when discussing operations coordinated across multiple domains (land, sea, and air). Nowadays, due to dramatic changes of the global security environment and growing ambitions of Russia and China, a multi-domain approach is required in order to challenge potential peer adversaries. Already, Allies and their partners are subject to persistent attacks across physical and non-physical domains under traditional thresholds of war [4, p. 2]. The term MDO differs from joint operations in that it is intended to focus on operations across multiple domains regardless of service affiliation, not necessarily on those conducted by multiple services [5, p. 49].

2.0 AIM AND METHOD

This article examines whether the current concept of JIPOE is adequate and capable to support not only contemporary joint military operations, but also future engagements in the multi-domain arena. The aim is to identify the problems and deficiencies associated with the current conduct of JIPOE, and to propose solutions on how this process can be improved to effectively support future military operations. Based on their experience gained during their deployments to NATO multinational intelligence staffs and deployment to various intelligence positions at all command and control (C2) levels, the authors argue that typical description of the OE relying almost exclusively on the PMESII-PT model, focusing predominantly on the physical domains and their relationship to the non-physical ones, provides only limited understanding of the OE, as it fails to analyze synergies and interdependencies between the domains.

This applies especially to planning and execution of operations in the non-physical domains, such as electromagnetic operations (EMO), information operations (INFOOPS) or cyberspace operations, where the thorough insight must be obtained in order to identify windows of opportunity in the multi-domain OE, execute faster decision cycles and create synergic effect exploiting collective capabilities available across all the domains.

In order to identify the gaps and opportunities related to the JIPOE process, the authors propose two key questions:

- What are the challenges of the current JIPOE concept and its contribution to military operations at the national and multinational level?
- How can the JIPOE process be improved in order to support future military operations?

Several analytical methods were used involving comparative analysis of doctrinal documents related to the

intelligence support to military operations and process analysis aimed at review of the JIPOE processes. During the research the authors extensively applied their practical experience with the JIPOE process to state the hypothesis, identify critical areas and formulate suggestions for improvement.

3.0 THE CURRENT STATUS

The complexity and variability of contemporary military operations requires situational awareness about the current developments in the joint operations area and the OE, which must be shared across all C2 levels with special emphasis on the operational and tactical levels. Hence, although the OE is primarily dealt with at the operational level, its minimum knowledge is also essential at the tactical level. For example, a land component commander's information requirements focus on the land domain naturally, but at the same time he or she should be aware of the status, capabilities and dispositions of the air force (both friendly and adversary) to a certain extent, as air activities will most likely affect land operations as well.

In the context of joint operations, most military forces have been focused primarily on the physical domains of the OE, i.e. land, maritime and air. Thus, operational planning is still component-centered, creating the risk of insufficient expertise in all domains [6, p. VIII]. In practice it means that operations and planning staffs prefer to seek solutions in traditional domains, and struggle with recently declared domains such as space and cyberspace. Similarly, although the growing importance of the EME and information environment has been acknowledged by military forces, the non-physical domains are much more difficult to conceptualize and bound within a constructive definition which means that they have often been deconflicted rather than truly integrated. That often leads us to situations where operations in these non-physical domains are ill-defined and opening critical vulnerabilities to adversaries [7, p. 9].

In general, planners have insufficient expertise in or access to information about relevant domains, not to mention about the capabilities and limitations of operations in all domains. They also need information about what forces are available as well as information on what other activities are taking place in the OE [6, p. 12], because not only military aspects of the OE can affect military operations (for instance, civilian aspects, pandemic situation etc.). One of the key stakeholders significantly contributing to the development of the situational awareness and information support of the commanders and their staffs, is the intelligence personnel. Its members are also responsible for timely assessments and valid predictive estimates without which commanders and staffs would not be able to plan and execute any military operation. Predictive intelligence is the main focus of the JIPOE process, which identifies adversary and other relevant actors' COGs and determines their capabilities to operate within the OE [8, p. I-2].

The NATO principles and processes of JIPOE are described in the intelligence publication AIntP-17 Ed. A, ver. 1, which was promulgated in 2019. This document was based on the best practices of NATO HQs' intelligence staffs and intelligence communities of NATO member states, yet its content does not set a dogma which must be followed unconditionally. Despite its undisputed benefits, such as providing a common baseline for intelligence support to operations planning and execution, both NATO multinational intelligence staffs as well as national military forces have to face several challenges.

First of them is the JIPOE implementation process itself. NATO member states usually need several years to implement new concepts into their national doctrinal systems and put them into practice. Since the AIntP-17 was published in 2019, it is still too early to expect that JIPOE has been fully implemented and integrated into the national standing operating procedures of the intelligence staffs.

Another problem is that the current JIPOE concept, describing the OE via PMESII-PT model (see Fig. 1), has not been prepared to fully reflect the dynamic developments in the realm multi-domain integration. NATO JIPOE description of the OE is conducted within the context of the land, maritime, air and space, physical domains; the cyberspace domain; and the information environment. Interestingly, the current version of AIntP-17 does not take account of the EME; it only acknowledges the electromagnetic spectrum

(EMS) as one of the aspects which should be taken into consideration, for example, when assessing electromagnetic effects or influence on specific military assets, such as spaced-based sensors. Nevertheless, the absence of the EME in the AIntP-17 does not mean that NATO denies its existence at all. On the contrary, in 2007 NATO promulgated a concept which shaped the principles of the EMO [9, p. 62]. In this document the EME was declared as an environment within the battlespace, and subsequently the EME was implemented into NATO doctrinal documents related to electronic warfare (EW), such as the AJP-3.6 (Allied Joint Doctrine for EW).

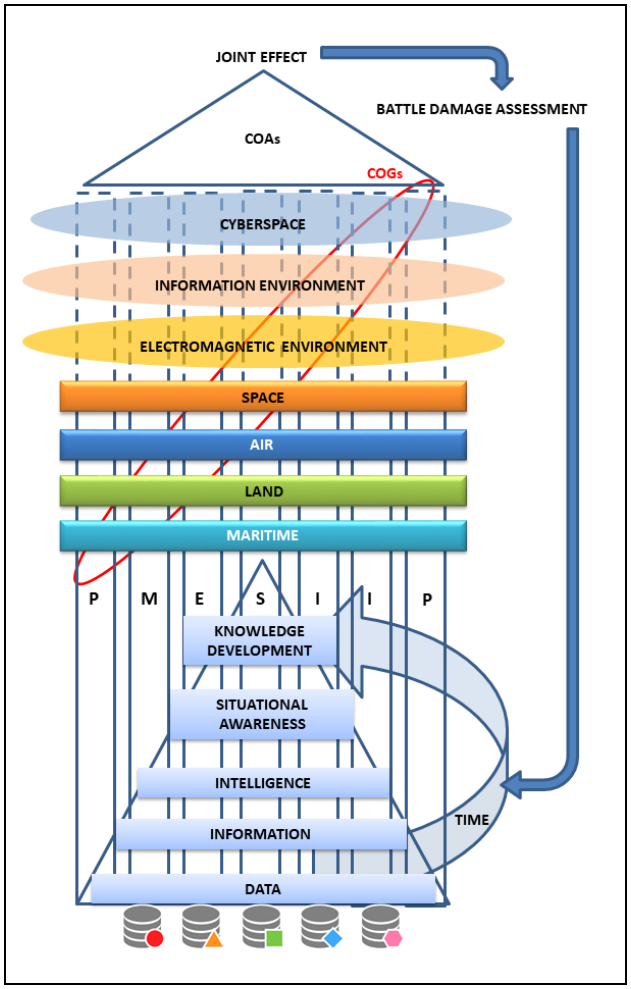

Figure 1: Visualisation of the current JIPOE process in support of joint operations.

The incompleteness and inconsistency of the current JIPOE categorical approach may result in critical failure to fully recognize interdependencies across the domains and the PMESII-PT categories, as the assessments are rather stove-piped than fused. As a result, the COGs may not be identified correctly, because in this manner the JIPOE analysts are not able to provide the full insight into the complex relationships between factors shaping the OE, actors and their capabilities. Consequently, the process of COA development is also negatively affected, thus derailing effective operational planning. All these omissions leave future military operations at a higher risk of failure.

The validity and overall quality of JIPOE intelligence assessments and estimates always largely depend on professional experience and knowledge of JIPOE analysts, however, due to the complexity of the OE, it is not possible for them to possess all the expertise required. In operational reality, they usually seek assistance from relevant subject matter experts (SME's) covering numerous aspects of the OE, including the EME. The

use of SME's represents a practical solution providing more comprehensive description and analysis. For example, knowledgeable EW SME's will most likely develop their EME assessments well beyond the extent of the AIntP-17, as they have clear understanding of importance of the EME to joint operations. The challenges are then how this expertise will be integrated into the overall assessment, or whether operational commanders actually understand the EME and are capable of orchestrating EW activities and actions across the levels of warfare and land, maritime, air, space, and cyber space forces for integrated and unified action in joint operations at operationally relevant speed and scale.

4.0 CHALLENGES OF FUTURE WARFARE

Due to dramatic changes of the global security environment and growing ambitions of Russia and China, a multi-domain approach is required in order to challenge not only potential near-peer adversaries, but also hostile non-state actors operating in the so-called 'grey zone'. MDO are not just an evolution of joint operations [10, p. 54]. They require mission commanders to simultaneously conduct parallel actions in multiple domains of the battlespace according to dynamic situations. The U.S. Army defines the MDO as "operations conducted across multiple domains and contested spaces to overcome an adversary's (or enemy's) strengths by presenting them with several operational and/or tactical dilemmas through the combined application of calibrated force posture; employment of multi-domain formations; and convergence of capabilities across domains, environments, and functions in time and spaces to achieve operational and tactical objectives" [6, p. 3].

Since future wars will feature a variety of threats (symmetric, asymmetric, hybrid), it is imperative to seamlessly integrate military but also non-military instruments in the pursuit of influence. Most competitive efforts are likely to be conducted through and across multiple domains, both offensively and defensively. Accordingly, the development of cross-domain command capabilities is of paramount importance [4, p. 12].

The aim in multi-domain integration is not to use as many domains as possible when planning for effects; rather it is to create, find and exploit unprotected vulnerabilities by extending the range of activities and capabilities that can be brought to bear across the domains. Doing this presents too many combinations for the adversary to guard against. For example, a naval surface combatant expects to defend itself from hostile aircraft or cruise missiles fired from the coast but will be less familiar with the threat from long-range land-based fires in combination with disruption to satellite navigation systems [11, p. 19]. Another example of an MDO can involve an opponent attacking or manipulating the use of radio frequencies within the EME, through EW or a cyberspace operation. In this manner, he could deny access to vital satellites that we rely on for intelligence, surveillance, and reconnaissance; communications; early warning; and navigation. The consequences would severely affect a JFC's planning, decision, and execution cycle and could render operations in the air, on land, and at sea ineffective [12, p. 20].

An effective multi-domain C2 structure will be required to recognise windows of opportunity, through real-time situational awareness in all domains, and execute faster decision cycles [10, p. 54]. As every functional component would be doing multi-domain planning and assessment, each operations center or command staff would have an increased demand for data and information on friendly forces and adversary forces across all the domains. The level of specificity may not need to be too detailed for every domain, yet each component may have priority information requirements in more domains than in the past [6, p. 86]. Planning, executing, or assessing multi-domain options will require more time and will involve more complexity than single domain alternatives or their combinations. Thus, demand for timely and accurate assessments of the OE will increase dramatically, underscoring the importance of intelligence and JIPOE in particular.

5.0 THE WAY AHEAD

In the future, the Allied forces will have to rapidly understand the battlespace, direct forces faster than the enemy, and deliver synchronized combat effects across all domains [13, p. 2–3]. This will require the

commander and the staff to have a comprehensive insight into the OE interdependencies, which will be facilitated by JIPOE. The key role of JIPOE in support of the decision-making process will further increase. It is assessed that the current way, in which JIPOE is conducted, provides a solid foundation but it needs to be improved to better accomplish requirements and effectively support of future operations. In order to make JIPOE more relevant and adequate for future military operations, it will be necessary to consider all of the physical and non-physical domains, including the EME, as a combination of tools for achievement of future operational objectives. In other words, it will be very difficult to update and adjust JIPOE processes, if JIPOE primary customers (plans, operations) do not change their pertaining overall perception of the OE. All these aspects will also have to be reflected and described in new or updated doctrinal documents.

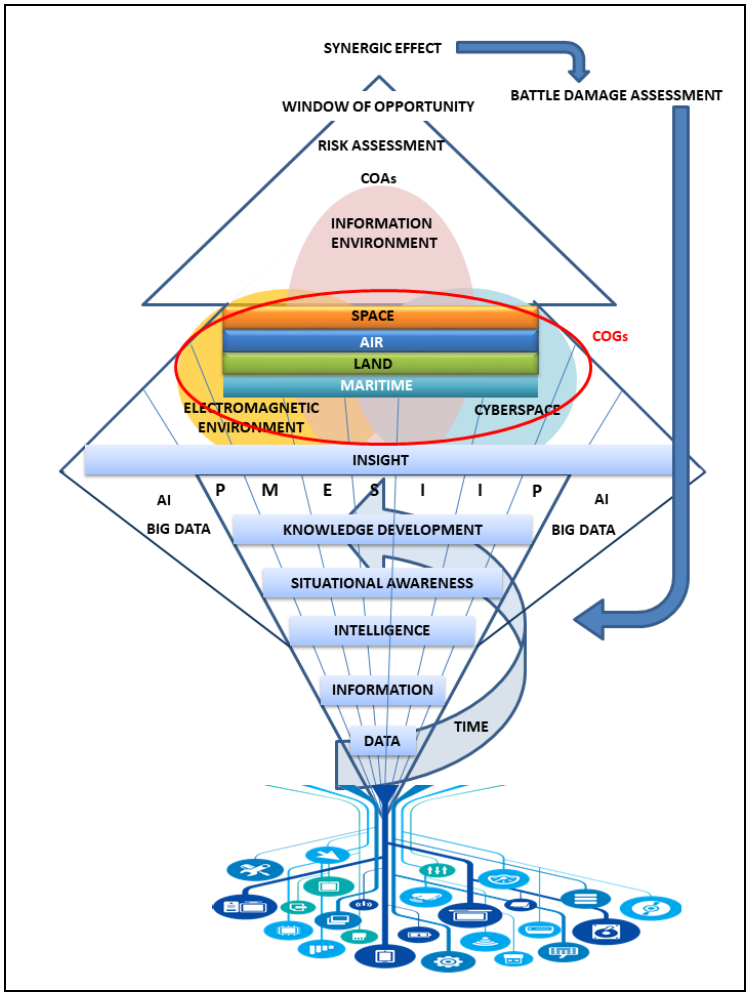

Figure 2: The proposed scheme of the JIPOE process in support of MDO.

The application of complex systems through JIPOE can be improved by changing from a categorical description to the interdependency-focused approach, because categories provide descriptions, but interdependencies provides insights [14]. One of the methods, which will have to be introduced and included into JIPOE procedures, is comprehensive risk assessment measuring the impact of threats on multiple assets of the OE (see Figure 2). In this way, it will be possible to prioritize the threats, understand interdependencies across the OE or identify COG's more precisely. This intelligence will need to be available in a way that is contextualised to the user. It will also have to be integrated across the C2 to be able to realise windows of opportunity at all levels, thus exploiting the specific conditions and circumstances in the OE.

Therefore, access to readily available relevant data, information, intelligence assessments and estimates provided by JIPOE, will be critical. In this respect, the use of technologies such as Artificial Intelligence (AI), big data processing and Machine Learning (ML) is crucial. New technologies can be used to collect and process ever-increasing amounts of data, which can then be collated, contextualized and analyzed by cross-disciplinary teams of well-informed and highly educated human operators [4, p. 7]. This is particularly valid in case of JIPOE which is a continuous process, and due to permanently changing variables (e.g. opponent's combat effectiveness) its products must be updated during the whole duration of the military operation.

Despite indisputable benefits of modern technologies, personnel will remain the most critical asset ensuring the cognitive superiority needed for success in future military operations. As of now, education of military professionals in most NATO countries, including members of intelligence staffs, is still focused on tactical level competencies, whereas operational level knowledge is usually gained during their further military career. Such an approach then creates a widening capability gap, because appropriately qualified military personnel is not always readily available. In order to outcompete opponents in future military conflicts, NATO countries should also update their military education programmes and prepare their personnel how to employ joint capabilities across a multi-domain environment. Hence, in addition to the implementation of cutting-edge technologies as well as conceptual and procedural changes, innovative steps must be taken in relation to the development of expertise and knowledge not only of dedicated JIPOE analysts, but also of all potential customers who are expected to request and use JIPOE products in support of future military operations.

6.0 REFERENCES

[1] Vašíček, Radovan. (2021). "Cyber and Electromagnetic Activities and Their Importance For Military Operations". In *15th Annual Doctoral Conference proceedings on the topic New Approaches to State Security Assurance* , 280-289. Brno: University of Defence. https://aktivity.unob.cz /dk/Documents/2021/15th%20Annual%20Doctoral%20Conference% 20proceedings.pdf.

[2] AJP-5 Allied Joint Doctrine for the Planning of Operations: Edition A Version 2, UK Change 1. 2019. Shrivenham: Ministry of Defence. https://assets.publishing.service.gov.uk/government/uploads /system/uploads/attachment_data/file/971390/20210310-AJP_5_with_UK_elem_final_web.pdf

[3] PARKINSON, Jeremy. Is Fluidity the Key to Effective Multi-Domain Operations? In: Joint Air & Space Power Conference [online]. Kalkar: Joint Air Power Competence Centre, 2019, p. 39–45. https://www.japcc.org/is-fluidity-the-key-to-effective-multi-domain-operations/

[4] The NATO Warfighting Capstone Concept: Key Insights from the Global Expert Symposium Summer 2020. 2020. The Hague: The Hague Centre for Strategic Studies. https://mk0hcssnlsb22xc4fhr7.kinstacdn.com/wp-content/uploads/attachments/ NATO_Symposium_Final_Version_For_Publication.pdf

[5] Heren, Henry. 2020. "Multi-Domain Operations: Inconceivable!" *The Journal of JAPCC*, no. 29: 48–53. https://www.japcc.org/multi-domain-operations-inconceivable/.

[6] Priebe, Miranda, and Douglas C. Ligor. 2020. *Multiple Dilemmas: Challenges And Options For All-Domain Command And Control*. Santa Monica: RAND Corporation. https://www.rand.org/pubs/research_reports/RRA381-1.html.

[7] Townsend, Stephen. 2019. "Defining the 'Domain' in Multi-Domain." In *Joint Air & Space Power Conference: Shaping NATO for Multi-Domain Operations of the Future*, 7–12. Kalkar: Joint Air Power Competence Centre. https://www.japcc.org/defining-the-domain-in-multi-domain/.

[8] Joint Publication 2-01.3: Joint Intelligence Preparation of the Operational Environment [online]. Washington: Joint Staff, 2014 [cit. 2021-8-23]. Available at: https://fas.org/irp/doddir/dod/jp2-01-3.pdf

[9] Nieto, Ignacio. 2020. "The Electromagnetic Environment and the Global Commons." *The Journal of JAPCC*, no. 29: 61–65. https://www.japcc.org/portfolio/journal-29/.

[10] Canovas, Juan. 2019. "Multi-Domain Operations and Challenges to Air Power." In *Joint Air & Space Power Conference: Shaping NATO for Multi-Domain Operations of the Future*, 47–54. Kalkar: Joint Air Power Competence Centre. https://www.japcc.org/multi-domain-operations-and-challenges-to-air-power/.

[11] *Joint Concept Note 1/20 Multi-Domain Integration*. (2020). 1st ed. Bristol: Ministry of Defence. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950789/20201112-JCN_1_20_MDI.PDF.

[12] Reilly, Jeffrey. 2019. "Multi-Domain Operations." In *Joint Air & Space Power Conference: Shaping NATO for Multi-Domain Operations of the Future*, 15–24. Kalkar: Joint Air Power Competence Centre. https://www.japcc.org/multi-domain-operations/.

[13] Hoehn, John R. 2021. "Joint All-Domain Command and Control." Congressional Research Service. 1 July 2021. https://crsreports.congress.gov/product/pdf/IF/IF11493.

[14] Pike, Thomas. "Analysis and Artificial Intelligence in Integrated Campaigning." 17 Jan 2020. https://nsiteam.com/analysis-and-artificial-intelligence-in-integrated-campaigning/.