CLOUD TECHNOLOGIES AND THE NEED FOR HYBRID CLOUD IMPLEMENTATION IN THE MILITARY ENVIRONMENT

Colonel Dan ȚIGĂNUȘ, PhD

Deputy Chief of Communications and Information Technology Directorate

10.55535/RMT.2023.2.2

Cloud computing has been widely adopted as the next-generation digitisation model for transforming the organisation into an entity that drives development and innovation. Nowadays, users of computing systems aim to get quick access to the virtual ecosystem and a new experience in cyberspace that seamlessly integrates with the existing services they use today. From the perspective of the military organisation/Military Enterprise, the cloud provides services for users and structures in a scalable, highly reliable and highly available manner, specifically with different security levels associated with the individual profile and functional roles in the organisation. From the end user's perspective, the cloud provides a simple model for accessing information technology/IT services without the need for the human factor to fully understand the transport/ transmission infrastructure and technology used.

This article explores how modern military-classified and unclassified cloud-native infrastructures can be secured and managed in a national, military-private, or mixed hybrid deployment cyber environment, along with various requirements and considerations for adapting cloud-native applications for military systems. In context, the article provides a simple but comprehensive introduction to the cloud native overview and the major technologies that developers use to build such reliable environments in cyberspace that could be the subject of a feasibility study to implement the concept of hybrid cloud in cyberspace with military use. The material is intended for IT experts, DevOps engineers, CIS (Communications and Information Technology) systems and infrastructure architects, cloud enthusiasts, cloud security experts, and any military professional involved in the development, migration, deployment, and management of current services and operations. of a cloud-native system.

Keywords: cloud computing; resilience; military organisation; information technology; cyberspace;

English version by **Iulia SINGER**.

Motto: *"...The Army cannot maximize its modernization strategy without the cloud, which is the backbone for artificial intelligence".*

HON Ryan D. McCarthy,
United States Secretary of the Army

INTRODUCTION

To take full advantage of the speed and agility of cloud services, many existing services and applications have been transformed into cloud-native applications, and new solutions are being developed to be cloud-first. Cloud applications are built right from the start to enable and incorporate subsequent changes at large scale, with minimal effort and in a short time, but also to ensure the availability and resiliency of systems in operation.

Infrastructure for cloud-native applications plays a critical role in efficiently meeting the needs of a military organisation and beyond, but this infrastructure must be designed or adaptable to the demands of information transfer over distances required by mobility and sometimes the expeditionary nature of military activities and operations.

By default, infrastructure for cloud-native applications plays a critical role in efficiently meeting the needs of a military organisation and beyond, but this infrastructure must be designed or adaptable to the demands of information transfer over distances required by mobility and sometimes the expeditionary nature of military activities and operations. If the transmission infrastructure (providing transmission services) is not designed to ensure maximum availability and implicitly provide resilience, based on redundancy, with distributed management that applies the correct practices and standards, even the best cloud-native applications will fail in military-use cyberspace.

Even though the use of the cloud offers an easy way to solve problems with the scalability, availability and reliability of IT services in the form of basic and specialised applications *(FAS – Functional Area Services)*[1], this technology is not a magic solution to all challenges in the field of communications, information technology and cyber

[1] *Functional area services/FAS* – specialised IT applications dedicated to specialised functions and services within a military organizational entity; e.g. LOGFAS – a package of specialised applications for the logistics field that provides access to data and information, some of which are georeferenced on digital maps, about the existence of material goods, mobility, transport, destination, supplier, beneficiary, operational status etc.

defense in the military environment. We cannot design applications in the cloud and expect them to run forever, nor can we demand that the applications required for static and deployable military systems be delivered in containers as remote provisioned services that can run in the cloud indefinitely and without interruptions. In order to take full advantage of what the cloud has to offer, it is necessary, first of all, to identify those cutting-edge services and applications which will be delivered primarily through cloud infrastructures. Therefore, in order to understand the importance and advantages offered by the native cloud as a process, it is necessary to review what the communication and IT infrastructure offers today, starting from the services developed during the evolution of the Internet and the takeover of commercial technologies in the military environment and for military use.

CIS support structures, at the request of the IT teams, had to physically purchase the servers and configure them locally, install custom operating systems for the servers, prepare the installation media for the applications, then deploy core and specialised applications for users, installed on these physical servers.

Subsequently, after a pertinent analysis of the cloud as a process and technology with military applicability, we must identify methods of efficiency and opportunities to use cloud capabilities jointly with other government and/or private organisations so that advantages are obtained maximums for the military establishment from the shared use of what is called, in specialist terms, the *hybrid cloud*.

THE ROAD TO THE CLOUD

Looking at the first IT service solutions in the early days of the Internet, including private data infrastructures, applications were hosted on *physical servers* that had to be purchased and prepared before they could be used. CIS support structures, at the request of the IT teams, had to physically purchase the servers and configure them locally, install custom operating systems for the servers, prepare the installation media for the applications, then deploy core and specialised applications for users, installed on these physical servers. There have been many problems and unfortunately, in the military environment, difficulties with this approach continue to be encountered: servers are underutilised because they are never fully utilised as a resource, it is difficult to run multiple applications simultaneously, and the costs of installation and maintenance are high under the conditions of a sufficiently rigid public procurement system so as to create major difficulties for ensuring maintenance throughout the life cycle of these systems and physical equipment.

Starting from these limitations, *virtualisation* was developed and embraced, including in the military environment, to allow more efficient use of physical servers. Virtualisation creates a logical layer over physical hardware that allows underlying resources such as processors, memory, and storage to be partitioned and shared. Virtualisation has solved many problems related to resource utilisation and multiple hosting of applications, but specialised CIS support structures still need to own the hardware equipment to implement the applications and also bear all the general costs of running the data center. This has given rise to the need to provide and run infrastructure as a service (IaaS[2]), where the servers are owned by third parties which are responsible for the underlying infrastructure on which the applications used by the beneficiary run. Thus began the era of cloud computing, which allowed commercial companies and public institutions to focus on the underlying applications and environments without worrying about the hardware that supported the operation of those applications, the staff resources to maintain it in operation or to configuration problems. IaaS was followed by platform-as-a-service (PaaS/Platform-as-a-Service), which focused on further reducing the effort of the beneficiaries by separating the use of the software in relation to the time of actual use. This meant that software application developers focused on writing application programs and defining infrastructure dependencies, while the service platform would be fully responsible for hosting, running, managing and accessing applications. PaaS paved the way for fully managed cloud services with the advent of software as a service (SaaS), popularly known as "*software on demand*", which provides beneficiaries with access to a specific application

ROMANIAN MILITARY THINKING

Virtualisation creates a logical layer over physical hardware that allows underlying resources such as processors, memory, and storage to be partitioned, shared, and shared. Virtualisation has solved many problems related to resource utilisation and multiple hosting of applications, but specialised CIS support structures still need to own the hardware equipment to implement the applications and also bear all the general costs of running the data center.

[2] In a typical IaaS model, a company, regardless of size, consumes services such as compute, storage, and database access from a cloud provider. The cloud provider provides these services by hosting hardware and software in its own physical facilities or in an integrated architectural constellation with well-defined governance, management and usage rules. The company no longer has to purchase and manage its own equipment or premises to host the equipment, and costs move to a pay-as-you-go model. When the company needs fewer resources, it pays less. As it grows, the company can secure access to additional computing resources and other technologies in minutes. In a traditional on-premise scenario, the company manages and maintains its own data center. The company/organisation must invest in servers, storage capacities, software, interfaces and other technologies; they also need to hire IT staff or contractors to acquire, manage and upgrade all equipment and licenses. The data center must be built to meet peak demands, even if sometimes the workload drops and these resources remain idle. Conversely, if the company is growing rapidly, the IT department may struggle to keep up. Text adapted from the source: https://www.oracle.com/ro/cloud/what-is-iaas/, retrieved on 9 December 2022.

as a service for a fee. As cloud computing has gained in popularity, so has the idea of benefiting from cloud-native technologies that would use the cloud more efficiently, while harnessing the full potential of the cloud infrastructure and its various resources. This gave rise to the development of *cloud-native infrastructure* and the creation of cloud-native applications. Cloud-native infrastructure creates an abstraction of the cloud provider's infrastructure and provides the infrastructure with APIs[3] for the purpose of interconnecting this infrastructure with other, similar ones, belonging to the beneficiaries, such as systemic network components. This philosophy of managing infrastructure resources and software applications easily enables scalability and reduction of infrastructure complexity, indirectly improving availability, resiliency and lifecycle maintainability. Similarly, native cloud applications increase the connection between application and infrastructure by incorporating features such as health monitoring, telemetry and metrics, resiliency, network environment microservices, or self-healing.

Cloud-native infrastructure creates an abstraction of the cloud provider's infrastructure and provides the infrastructure with APIs for the purpose of interconnecting this infrastructure with other, similar, belonging to the beneficiaries, such as systemic network components. This philosophy of managing infrastructure resources and software applications easily enables scalability and reduction of infrastructure complexity, indirectly improving availability, resiliency and lifecycle maintainability.

THE ADOPTION OF CLOUD TECHNOLOGY IN THE MILITARY ENVIRONMENT

It is undeniable that cloud computing technology has changed the way in which the activities of an organisational entity, including the military, are carried out and, implicitly, the information exchange between it and those with which it cooperates at an inter-institutional, corporate or global level, in support of achieving operational efficiency in their own activities, be they of an economic, administrative-governmental or military nature. With the help of the cloud, organisations are now able to streamline their work, quickly implement IT services and digitise their processes.

Everything from human resources, financial reporting, supply chains, to simple mobile applications have benefited from cloud deployments. In addition to considerations of the appropriate deployment model, such as public, hybrid, or private cloud,

[3] The API is a powerful and versatile means of connecting diverse and disparate software applications. APIs allow a wide range of unrelated software products to integrate and interoperate with other software products and data. APIs also allow developers to add features and functionality to the software using a rich array of other developers' APIs. Source: https://www.techtarget.com/searchapparchitecture/tip/What-are-the-types-of-APIs-and-their-differences, retrieved on 6 December 2022.

organisations also face a decision regarding service models. The three common cloud-computing models each have unique characteristics and help solve specific needs in ways that suit your needs.

Organisations, including those in the public sector, routinely deploy different cloud solutions and use various service models. It becomes essential to remember that regardless of the service model we implement, the question arises whether we can also leverage for the military institution, in addition to its own private cloud, public cloud or hybrid cloud environments. In the event of a positive answer, there will be a need for strategic suppliers for the military institution that guarantee long-term public or hybrid cloud options and that provide continuity in their operation and maintenance over the life cycle for all cloud tools and technologies offered. Through cloud-delivered services, access to applications can be provided anywhere, anytime, and on any device, contributing to new operational and administrative efficiency benefits within the military organisation. When thinking about the right service model, military structures should start by asking themselves: *What is the solution to get the best overall return, with the resources available, for their activity, under conditions of economic efficiency and operational, peace, crisis or war?* It seems that the American partner has found the answer to this question, given the recently published intentions of the Pentagon to launch a competition in the profile market of about 9 billion USD through a contract signed on 7 December 2022 for the so-called multi-year *Joint Warfighting Cloud* project, competition in which Amazon, Google, Microsoft and Oracle will fight to obtain as much as possible of the rights to realise this strategic capability for defense until the year 2028 (Demarest).

The lines of demarcation between IaaS and PaaS have blurred recently as major cloud computing providers offer both in the same environment. IaaS can help organisations achieve cost efficiency with hardware and infrastructure, but PaaS can further reduce administrative overhead and expand usage to beneficiaries less accustomed to high-tech tools. Once a problem is defined that can be solved with a cloud computing solution, military structures can move on to develop the right type of cloud solution, which requires an understanding of Platform-as-a-Service, Infrastructure-as-a-Service and cloud-native applications, which we explore in this article.

ROMANIAN MILITARY THINKING

Organisations, including those in the public sector, routinely deploy different cloud solutions and use various service models. It becomes essential to remember that regardless of the service model we implement, the question arises whether we can also leverage for the military institution, in addition to its own private cloud, public cloud or hybrid cloud environments. In the event of a positive answer, there will be a need for strategic suppliers for the military institution that guarantee long-term public or hybrid cloud options and that provide continuity in their operation and maintenance over the life cycle for all cloud tools and technologies offered.

With *Infrastructure as a Service (IaaS)*, military organisations can leverage the resources made available by a cloud provider to make cost savings in processing and storage capabilities, as well as gain the ability to scale or rapidly shrink its own deployable capabilities, scalable according to operational design and missions assigned to CIS support structures. With IaaS, beneficiaries can instantly access increased processing and traffic capabilities without making expensive hardware investments. Adopting IaaS in the military environment mainly solves two sets of problems.

With Infrastructure as a Service (IaaS), military organisations can leverage the resources made available by a cloud provider to make cost savings in processing and storage capabilities, as well as gain the ability to scale or rapidly shrink its own deployable capabilities, scalable according to operational design and missions assigned to CIS support structures.

The first of these is related to capital expenditure and investment budgeting. Considering the urgent needs, most of the time, for the rapid provision of the extended infrastructure in the mission execution environment and the design of scalable and modular CIS services, adapted to the dynamics of the military environment, it is necessary to have an operational budget at your disposal, as benefiting, for example, multinational security and defense organisations for ongoing missions, as well as certain specialised entities for rapid intervention at the national level, as well as spending on services (O&M/O&M) to enable access to capabilities, based on predefined contractual arrangements, depending on the nature of urgency and the needs of the beneficiaries participating in the mission, without the need to refer to the budget cycle for investments.

The second set of benefits that IaaS can bring to the military system is the management of its own infrastructure. Keeping, continuously upgrading, troubleshooting and maintaining the IT infrastructure is a resource-intensive activity that can be outsourced to an external cloud computing provider, with the maintenance, of course, of those services that particularly concern cyber security and information resource management critical to the military organisation. To determine the strategy for defining the level of implementation of the outsourcing of these infrastructure services based on the IaaS model, agencies and military decision-makers will determine what is the critical threshold to achieve maximum benefits under conditions of maximum operational effectiveness and economic efficiency. From a technical perspective, with IaaS, military CIS structures can expect benefits on the following levels of effort aimed at the capabilities of collecting, processing, analysing and disseminating information, storing data and providing shared access to information/data, depending on the user profile,

as well as ensuring data redundancy/backup and disaster recovery, as follows:

- scalable solutions for processing and extended data storage capabilities;
- IT infrastructure cost control based on time and capacity used;
- optimisation of network resources through automation;
- reducing costs with the purchase and maintenance over the life cycle of hardware equipment;
- reducing the pressure on the highly qualified personnel resource, which requires a long time of training and specialisation and whose retention in the military organisation is increasingly difficult;
- quick access to services for operation in conditions of maximum mobility of the organisational entities benefiting from these services in the static, but especially deployable environment.

But IaaS is not the only cloud service model, it should be part of a larger cloud strategy that includes PaaS, which offers additional benefits in a complete cloud solution. By implementing PaaS in cyberspace with military use, it gives the external service provider more responsibility to manage and optimise the cloud environment, which can lead to reduced IT administration expenses and increased performance of providing these services. Simultaneously with the adoption and application of the *"Zero Trust"*[4] security model in military infrastructures and systems, PaaS can be an essential evolution for the military organisation through its potential to leverage outsourced application management layers, including SaaS provisioning and the data that constitute information resources, analytical applications, and applications for mobile and deployable systems. In particular, PaaS can benefit military structures by:

- greater efficiency in the use of personnel resources in the field of IT program development;
- enhanced CIS security through cloud process automation, protection and updates for infrastructure management without human intervention;

Simultaneously with the adoption and application of the "Zero Trust" security model in military infrastructures and systems, PaaS can be an essential evolution for the military organisation through its potential to leverage outsourced application management layers, including SaaS provisioning and the data that constitute information resources, analytical applications, and applications for mobile and deployable systems.

[4] Innovative approach to the concept of IT protection introduced almost a decade ago by John Kindervag, an analyst at Forester Research at the time, which makes susceptibility the *centerpiece* of a cyber security strategy called *Zero Trust*, i.e. nothing can be trusted, always the identity and authenticity of a network query must be verified – article ul *The Zero trust security model, benefits and implementation possibilities*, Datanet System Integration, https://datanets.ro , retrieved on 9 December 2022.

- increased performance in providing services, given the limited access in time and volume, depending on the type and tempo of military activities;
- increased resilience based on increased fault tolerance and availability of cloud services.

In context, there could be the question or even the prejudice among technical experts and resource analysts that we would no longer need IT management or expertise, cloud architects or database administrators in the private military environment, given the access government or hybrid public cloud resources. The answer is as simple as it is true: there will always be a need for *tech-savvy resource* in the military, as the role of these experts will now focus on the qualitative adaptation of the use of applications to the needs of military users, on ensuring adequate technical support for management informational, the implementation of the architectural security model appropriate to the type of activity based on operational design and access and sharing architecture oriented to the profile and roles held in the organisation. It is equally true that some of the infrastructure and service administration activities, especially those services common to the entire organisational entity will become more efficient by eliminating redundancy between administrators and by reducing operation and maintenance costs, also considering the resources used for architectural design, system implementation and configuration management with own resources of expertise and operation. Focusing the work of CIS experts in the army on the development of proprietary applications, based on software resources provided in the cloud as PaaS and/or SaaS, including the use of cloud-native applications, will lead to the rapid obtaining for the benefit of users of support appropriate to their own needs, starting from to operational requirements which, most of the time, are difficult to interpret without an adequate *knowledge management* process leading to the identification of CIS resource requirements and their effective allocation in support of those who use them, in particular user communities in the operational and warfighter environment. Rapid exploration of service support requirements in deployable and mobile environments, identification of information flows and data and information access needs, based on matrixes with information exchange requirements, process management in permanent or temporary military activities and actions,

There will always be a need for tech-savvy resource in the military, as the role of these experts will now focus on the qualitative adaptation of the use of applications to the needs of military users, on ensuring adequate technical support for management informational, the implementation of the architectural security model appropriate to the type of activity based on operational design and access and sharing architecture oriented to the profile and roles held in the organisation.

creation virtual environment of centralised and computerised data management *(data lake)* with the role of allowing the timely identification of relevant information for the user with a personalised profile, there are as many challenges that face us before adopting a certain architecture for access to available resources in a private, hybrid or public cloud.

CLOUD CHALLENGES AND RESISTANCE TO CHANGE

Commercial cloud providers have become a dominant solution for *enterprise applications*[5] as market demands and operational needs in the public and government space have grown. This approach offers advantages such as higher availability and scalability, along with the flexibility to design applications in a way that indicates the use of cloud services from the outset.

However, when cloud solutions were first introduced, many challenges were considered by potential beneficiaries, including security, cost effective management, compliance or performance. It is appreciated in the literature (Singh, Kehoe, 2022) that those initial challenges are now a thing of the past for most cloud consumers, as advances have been made both in the technologies applied by cloud providers and in the way that consumer organisations implement cloud solutions, taking into account their own particularities and needs. Obviously, although they have come a long way, this does not mean that cloud technologies are perfect. What matters for a possible design of the application of the hybrid model of implementing the cloud in the military environment is that it has reached a sufficient maturity in the profile market, that it becomes not only opportune, but also mandatory to analyse whether or not there is a need for outsourcing some cloud services for the information system in cyberspace with military use. By the nature of the evolution in the digital transformation process

Commercial cloud providers have become a dominant solution for enterprise applications as market demands and operational needs in the public and government space have grown. This approach offers advantages such as higher availability and scalability, along with the flexibility to design applications in a way that indicates the use of cloud services from the outset.

[5] Being a comprehensive solution at the scale of the organisation, including the military type, this implementation has the role of solving a problem or streamlining a critical process for the modernisation and development of the organisation or to increase the performance of the information exchange system inside or outside the organisation. Gartner, a well-known research and consulting company, defines *enterprise* applications as being designed to *"integrate software solutions into a single system with which to carry out all the operations of a company to facilitate cooperation and coordination of activity throughout the organization. Enterprise applications also have the role of connecting the organization with suppliers, business partners and customers"*, https://www.roweb.ro/ro/blog/ce-sunt-aplicatiile-enterprise, retrieved on 7 January 2023.

As the transition to the cloud era is realised, the architecture of applications that come from various generations of infrastructure solutions, from data centers based on physical servers to virtual machines, to containers, respectively to no server technologies gets complicated. Migrating applications requires a significant effort to understand advanced technology elements and how to use them to their maximum capacity based on operational and technical performance.

at the national, inter-institutional, European or North-Atlantic Alliance level and with expansion and interdependencies on a global scale, the virtual space with military use is already exposed to the phenomenon of integration and federalisation in the virtual environment. If we continue to turn our backs on hybrid cloud solutions (own private cloud, supplemented with access to outsourced infrastructure and services), there is a risk of delaying the implementation and operationalisation of military-use cyberspace with high costs and additional effort that is difficult to justify.

Certainly, the decisions regarding the adoption of hybrid cloud solutions must take into account the particularities of the military system, in terms of security and cyber defense in general, respectively the requirements for the preparation of platforms and access interfaces in particular, the profile of users with specific rights for the use of information resources depending on the role and functions performed by applying the *"Zero Trust"* model, but, we consider, the most difficult component in the implementation of such a construct – the contractual and cooperative relationship for an indefinite period with the strategic supplier/suppliers cloud services and applications, potentially usable in the military organisation.

A number of challenges in adopting a solution suitable for the military cloud environment remain under consideration, such as:

❖ *too many choices*: there are a lot of cloud providers with a wide range of services and this entails the need to have expert architects and engineers to build teams capable of operating the services and using them according to technical requirements and operational in the military organisation. But the training time, functional area specialisation and retention of these engineers are difficult, unfortunately, as the current reality shows;

❖ *rapid development of cloud services and technologies*: a large number of new cloud services are launched by cloud provider giants such as Amazon, Microsoft or Google. This leads to a greater need to train military engineers capable of taking on these new services and a greater need for knowledge to maintain these services as applications upgrade through new releases;

❖ *successive generations of technology solutions*: as the transition to the cloud era is realised, the architecture of applications that come from various generations of infrastructure solutions, from data

centers based on physical servers to virtual machines, to containers, respectively to no server technologies gets complicated. Migrating applications requires a significant effort to understand advanced technology elements and how to use them to their maximum capacity based on operational and technical performance;

❖ *ever-increasing systemic complexity:* These rapidly growing technologies, combined with the accelerated migration of workloads to the cloud, have given rise to life-cycle operations and maintenance (O&M) complexity by, among other things, increasing the stack of tracked, such as storage systems, security models, governance models and/or management platforms;

❖ *the evolution of the operational domains and, implicitly, of the informational ones in the multinational and inter-institutional military environment*: the functional services in continuous development in the operational domains (land, air, naval, cyber and space) where the armed forces operate, generated at the inter-institutional level by the National Security System, as well as the scale of military activities carried out by multinational operational entities on the territory of the country (corps, division, brigade, battle groups, etc.) or outside it in the theaters of operations creates difficulties from the perspective of using the principles of federalisation in the mission execution environment or military operation; combined with the specific application areas of each user in command points and headquarters and the multitude of proprietary software solution providers, it is necessary to apply a well-defined set of standards in the field of the military cloud and, hence, interoperable interface solutions between different applied systems and solutions;

❖ *data management and artificial intelligence models:* the forms of organisation, storage, access and dissemination of data, the technological tools available for architectural developments in IT, the intelligent rapid analysis solutions for identifying and providing data, respectively transforming them into information for the user, intelligent machines that process through knowledge, the emergence of the DevOps culture as an architectural model that allows an application that once took a long time to develop can now be launched in a few minutes are just as many challenges before those who have the responsibility to identify and apply the more appropriate solutions for cloud deployment in the military environment.

The forms of organisation, storage, access and dissemination of data, the technological tools available for architectural developments in IT, the intelligent rapid analysis solutions for identifying and providing data, respectively transforming them into information for the user, intelligent machines that process through knowledge, the emergence of the DevOps culture as an architectural model that allows an application that once took a long time to develop can now be launched in a few minutes are just as many challenges before those who have the responsibility to identify and apply the more appropriate solutions for cloud deployment in the military environment.

Therefore, despite the multiple advantages that the cloud introduces as an architectural model for the management and use of information technology services in the military system, there are a number of complexities that determine the extent, speed of adoption and identification of potential hybrid model providers, government institutions and commercial operators, but none of these complexities and possible limitations represent insurmountable obstacles and, moreover, do not diminish the need for pertinent analysis for the adoption of hybrid cloud solutions in the military environment.

The technical solutions for adopting cloud computing and related technologies native to this service delivery model are constantly evolving, but their adoption and use to the benefit of military organisational entities is only a matter of understanding, will and our decision to adapt to digital transformation processes and to step over the not so much technological, but especially cultural-organisational barriers today.

CONCLUSIONS

In this article, I have tried to present, with the help of bibliographic references and based on current efforts in the field of developing national military capabilities focused on cloud computing, how cloud-native technologies can influence the adoption of feasible, timely and effective solutions for military systems of communications and information technology.

Starting from an understanding of the technological journey through which the cloud has become popular and how it has rapidly evolved in the public and commercial space, from physical hardware equipment passing through virtualisation to the self-managed serverless working environment using applications native software in the cloud, I want to bring to the attention of those involved in the design and implementation of military capabilities in cyberspace intended to support joint-type operations in multiple operational domains (multi/all-domain operations: land, sea, air, space and cyberspace) the need to apply good practices, technical standards and CIS security models to implement and expand the use of the latest technologies for the military environment.

I also understand the challenges that the evolving adoption of the cloud in the multi-level classified network environment implies and, above all, the difficulties generated by resistance to the changes introduced by the use of cloud-native technologies and applications in the cyberspace controlled by the institutions of the national system of security. The technical solutions for adopting cloud computing and related technologies native to this service delivery model are constantly evolving, but their adoption and use to the benefit of military

organisational entities is only a matter of understanding, will and our decision to adapt to digital transformation processes and to step over the not so much technological, but especially cultural-organisational barriers today.

BIBLIOGRAPHICAL REFERENCES:

1. Demarest, C., https://www.c4isrnet.com/author/colin-demarest, retrieved on 8 December 2022.
2. Singh, N., Kehoe, M. (2022). *Cloud Native Infrastructure with Azure, Building and Managing Cloud Native Applications*. Editura O'reilly Media.
3. https://azure.microsoft.com/pt-br/blog/azure-application-architecture-guide, retrieved on 22 February 2023.
4. https://docs.microsoft.com/en-us/azure/architecture
5. https://datanets.ro, retrieved on 17 February 2023.
6. https://www.oracle.com/ro/cloud/what-is-iaas/, retrieved on 21 January 2023.
7. https://www.techtarget.com/searchapparchitecture/tip/What-are-the-types-of-APIs-and-their-differences, retrieved on 17 February 2023.