MILITARY DIGITAL BUSINESS: CHALLENGES AND PROSPECTS OF DEVELOPMENT

Olena Rybytska
Lecturer at the Department of Law of National Security and Legal Work,
Military Law Institute of Yaroslav Mudryi National Law University, Ukraine
e-mail: rybytskaalyona@ukr.net, orcid.org/0000-0002-5382-3882

Eldar Fedorenko
Student, Military Law Institute of Yaroslav Mudryi National Law University, Ukraine
e-mail: eldarfedorenko@gmail.com, orcid.org/0009-0006-8610-2498

Summary

The relevance of the problem of conducting digital military records management is growing in the face of modern technological challenges, as military structures are increasingly switching to digital platforms for processing documents and information. However, this process faces several difficulties, such as insufficient integration of electronic systems, the lack of a unified regulatory framework, and technical problems related to data security. The purpose of the work is to study the complexities of digital records management in Ukrainian military units, as well as to develop proposals for solving the issue under study. To achieve this goal, methods of analyzing regulatory acts, comparative analysis of international experience, and expert surveys were used. The results of the study showed that the main difficulties are the low efficiency of existing software tools, the lack of a unified standard for processing electronic documents, as well as the imperfection of the regulatory framework that does not regulate specific requirements for military records management. It was also noted that military units violate procedures for complying with data security standards, which is a potential threat to information confidentiality. The practical value of the work lies in the fact that proposals for improving regulatory legal acts and introducing new technologies can help ensure more efficient and secure digital military record-keeping in Ukraine.

Key words: digital record keeping, military documentation, information security, electronic documents, legal framework, digitization, military units.

DOI https://doi.org/10.23856/6827

1. Introduction

Digitalisation of military records management in the context of modern warfare is an important aspect of ensuring the effectiveness of management processes in the Armed Forces of Ukraine. Russia's full-scale armed aggression has highlighted the fact that the speed of information exchange, access to up-to-date data and the effective use of digital technologies are critical for ensuring operational command and control of troops *(Constitution of Ukraine, 1996)*. However, the process of introducing digital technologies into the military records management of the security and defence forces faces a number of challenges, including technical, organisational and legal issues. These include an insufficient level of information protection, imperfect infrastructure to ensure the smooth operation of systems, and the lack of unified standards for digital records management *(On Defence of Ukraine, 1991)*.

The relevance of this issue is growing in the context of the special legal regime of martial law, as digital technologies can increase the efficiency of information processing, which is critical for combat operations and resource management *(On the Armed Forces of Ukraine, 1991)*. In this regard, there is a need to develop new approaches to the organisation of digital military records management that take into account the specifics of military service and current challenges, including cybersecurity threats and the need for rapid data exchange.

Violations of data protection requirements, errors in document processing or technical failures can lead to significant negative consequences, including human, material and territorial losses or erroneous decisions in the management of combat units *(On Military Duty and Military Service, 1992)*.

Given the relevance of the topic, it is necessary not only to improve existing digital record-keeping systems, but also to ensure proper training of personnel, introduce the latest security methods and technical solutions to overcome existing difficulties. Therefore, analysing the problems of digital military records management in wartime is important for improving the efficiency of management processes and strengthening the country's defence capability *(On Social and Legal Protection of Servicemen and Members of Their Families, 1991)*.

The purpose of this article is to study the main difficulties in maintaining digital military records in the context of modern warfare. The article is aimed at analysing the existing problems in the implementation of digital technologies in the organisation of military management and document management, as well as at studying their impact on the efficiency of the Armed Forces of Ukraine and other military formations. In addition, the goal is to identify technical, legal and organisational barriers that arise in the process of digitalisation, as well as to develop recommendations for improving digital processes in military records management, taking into account the specifics of the ongoing war.

The main objective is to assess the current state of digital systems in the Armed Forces, analyse security and efficiency issues in military data management, and identify ways to improve the digital record keeping system. The article also aims to emphasise the importance of ensuring that military professionals are properly educated and trained to work with new digital tools and software.

2. Literature review

Recent studies in the field of digital military records management emphasise the importance of introducing modern information technologies into the structure of the Armed Forces of Ukraine, in particular in the context of military management and data processing. Since the beginning of Russia's full-scale invasion, there has been a need to improve existing systems to ensure the efficiency and security of information exchange between units, which is confirmed by numerous publications analysing the use of digital technologies in war *(On Information, 1992)*.

In particular, a number of scientific papers on digital transformation in Ukraine address the problems of data protection, security of information systems and the importance of their modernisation in the context of armed conflict *(On State Secrets, 1994)*. The issue of creating a unified information space for military structures, which allows for the prompt processing and transmission of important information, is highlighted separately, which is key to ensuring effective command and control in combat operations *(On the Armed Forces of Ukraine, 1991)*.

Research on the legal aspects of digital military records management also deserves attention. Legislative initiatives adopted in Ukraine after 2014 have created a legal framework for the development of information infrastructure in the army and its adaptation to digital requirements. Relevant amendments to laws, such as the Law on Defence of Ukraine and the Law on Military Duty and Military Service, create a legal framework for the introduction of digital technologies in the defence sector *(On Defence of Ukraine, 1991; On Military Duty and Military Service, 1992).*

At the same time, despite the successes achieved, there are problematic issues that point to the need for further research in the area of standardisation of digital processes and integration of various information systems within a single network, which should ensure the coordinated and secure operation of military bodies *(On Access to Public Information, 2011)*. An important aspect is also the growing role of cybersecurity, which should be taken into account when developing new technologies for military records management, as possible cyber threats can negatively affect the stability and functionality of the entire information system.

3. Materials and methods

A variety of materials were used to study the difficulties in maintaining digital military records, including scientific publications, analytical reports and regulatory documents. The main focus was on the study of modern document management technologies in military formations of different countries. Articles from professional journals, conference materials, and reports covering the experience of implementing digital systems in the military were analysed. This allowed us to form a general idea of current problems and challenges.

4. Results and discussion

Digital military records management is one of the most important components of modern military command and control, especially in the context of armed conflict. In today's context, this aspect has become particularly important, as the effectiveness of military command depends not only on military strategy, but also on the ability to quickly and securely process, transmit and store information. However, the introduction of digital technologies in military records management in Ukraine faces a number of problems, both technical and legal (*Law of Ukraine 'On Defence of Ukraine', 1991*).

One of the main challenges is the need to adapt existing regulations to the new requirements of digitalisation. Legislation governing defence and military service remains largely traditional and does not always meet the needs of modern information technology. The Law of Ukraine 'On Defence of Ukraine' (1991) and the Law of Ukraine 'On the Armed Forces of Ukraine' (1991) regulate general issues of defence organisation and functioning of military structures, but do not always specify specific aspects of the use of digital systems in the record keeping process. As a result, in practical application, situations arise when the existing rules do not meet the requirements of efficiency and security of information exchange (*Law of Ukraine 'On the Armed Forces of Ukraine', 1991*).

In the context of the war with Russia, these problems are becoming even more urgent. Military units must be able to promptly transmit information about the tactical situation at the front, including not only data on the location of troops, but also on the state of equipment, ammunition, logistical needs and other important aspects. Accordingly, for the successful functioning of digital military records, it is necessary to ensure reliable protection of information from possible cyberattacks by the enemy, as well as to avoid technical failures in the operation of digital systems that could lead to the loss of important information (*Law of Ukraine 'On State Secrets', 1994*).

Legislation also plays an important role in ensuring the security of information in digital military records. Ukraine has legislation on state secrets and information security, including the Law of Ukraine 'On State Secrets' (1994) and the Law of Ukraine 'On Information' (1992), but these laws need to be adapted to meet the current challenges. Another important issue is the protection of confidential information transmitted between military units. In particular, during martial law, it is extremely important to ensure the security of information on plans and strategies, as the leakage of such data can have catastrophic consequences for the combat capability of the army (*Law of Ukraine 'On State Secrets', 1994*).

Given the need to respond quickly to changing conditions on the frontline, the automation of military records management processes is particularly relevant. Military structures must be able to quickly process documents and other materials received in the course of military operations. However, many existing software products for the automation of military records management are not able to work in real time due to the lack of necessary computing power or technical problems that arise when they are used in the field (*Law of Ukraine 'On Access to Public Information', 2011).*

Insufficient training of personnel to work with new information systems is also a serious obstacle to the introduction of digital technologies. Military professionals must be prepared not only for physical but also for digital threats. However, in reality, the level of education and training of military personnel in this area does not always meet the requirements of the times. In order for the military to be able to effectively use digital tools in the process of record keeping, it is necessary to conduct regular training and improve the skills of the military in the field of information technology (*Law of Ukraine 'On Social and Legal Protection of Servicemen and Members of Their Families', 1991*).

Legal aspects of digital record keeping are also an important issue. Legislation governing access to public information, such as the Law of Ukraine 'On Access to Public Information' (2011), may not always be applicable in times of war, when information of national importance may be withheld from the public. During an armed conflict, it is important to maintain a balance between openness of information and its protection from potential threats. This requires constant adaptation of legislative norms to the changing situation on the frontline (*Law of Ukraine 'On Access to Public Information', 2011*).

Another important issue in the context of digital military records management is the preservation and archiving of information related to the country's security and defence. In the face of constant cyberattacks by the enemy aimed at destroying or altering important data, the issue of reliable information storage is becoming critical. The system of archiving and preserving digital data should be as secure as possible, which requires the introduction of the latest encryption and backup technologies *(Law of Ukraine on Defence of Ukraine, 1991; Law of Ukraine on State Secrets, 1994)*. Digital archives should store not only operational data on the combat capability of units, but also the history of decisions made and operations performed, which can be important for internal analysis, as well as for future research and strategy planning *(Constitution of Ukraine, 1996)*.

An integral part of digital military records is the military resource management system. In a warfighting environment, it is important to have constant information on the availability of material resources such as ammunition, medical supplies, vehicles, equipment and other important elements to support the army. Digital systems should ensure the operational tracking and management of these resources, allowing for timely replenishment and avoidance of stock-outs *(Law of Ukraine on Military Duty and Military Service, 1992)*. However, in times of war, access to such systems may often be limited or impeded by physical and technical damage to the infrastructure. Therefore, in the event of a failure of the main channels of digital records management, backup mechanisms should be developed to support management functions, reducing dependence on digital platforms and ensuring continuity of management processes *(Law of Ukraine on Social and Legal Protection of Servicemen, 1991)*.

Another important challenge is the issue of legal protection of digital data in military records. In Ukraine, as in other countries, there are a number of laws and regulations governing the processing and storage of information of strategic or defence importance *(Law of Ukraine on Information, 1992; Law of Ukraine on Access to Public Information, 2011)*. However, in the practice of using digital technologies on the frontline, situations often arise when the existing legal norms do not cover all aspects of modern threats and opportunities for manipulating digital data. Issues related to the reliable protection of data concerning tactical operations, strategic plans or personal information of military personnel require additional legal regulation that must meet the requirements of modern information technologies *(Law of Ukraine on State Secrets, 1994)*.

In particular, it is necessary to actively work on improving the system of legal control over access to sensitive information and ensuring transparency of its use without violating the principles of national security *(Law of Ukraine on Defence of Ukraine, 1991)*.

5. Conclusions

In the process of analysing the difficulties in maintaining digital military records in the context of the war with Russia, several important aspects have been identified that need to be improved to ensure effective management and defence capability of the country. First of all, it is necessary to ensure proper protection of digital data, in particular in the face of constant cyberattacks that can lead to the leakage or destruction of important information. To this end, a comprehensive cybersecurity system should be implemented that combines the latest methods of data encryption and backup storage. In addition, it is important to ensure the archiving and preservation of data on a long-term basis, in particular, information on strategies and tactics used in warfare.

Another important challenge is the effective management of military resources through digital systems. To address this issue, it is necessary to develop and implement modern programmes to monitor the availability of equipment, ammunition, medical supplies and other important material resources. The system should ensure real-time monitoring and accurate forecasting of the required resources, which will help to avoid shortages and a decrease in combat readiness. At the same time, the system must be resistant to technical damage and be ready to operate in limited conditions, especially in field situations.

As for the legal aspect, it is important to improve the legal framework governing the processing and storage of digital data in military records. In this context, it is necessary to develop clearer rules for access to sensitive information to protect data from unauthorised use and abuse. Given the rapid development of technology and its impact on the military sphere, the legal framework should be constantly updated to ensure the highest level of protection and security. In particular, this applies to information related to national security, intelligence and personal information of military personnel.

Given the importance of adaptive command and control in wartime, it is recommended to develop flexible digital systems that can quickly respond to changes in the situation at the front. Such systems should allow for real-time adjustments to battle plans, strategies and tactics depending on operational data. This will significantly improve the effectiveness of command

and coordination of forces in real time. However, this will require the creation of algorithms and programs that can automatically take into account changing conditions without the need for constant human intervention.

Given all of these challenges, it is also important to pay attention to the need to develop technologies to work in conditions of limited communications. Digital systems must be able to operate autonomously, which will ensure continuity of operation even if the main communication channels are destroyed or damaged. Thus, for effective digital military records management in the context of war with Russia, it is necessary to ensure not only technological, but also legal, organisational and methodological readiness for the challenges faced by the army in a hybrid war.

So, to summarise all of the above, it should be emphasised once again that in order to solve the main problems of digital military records management in Ukraine, it is necessary to take a comprehensive approach to the integration of the latest information technologies, increase cybersecurity, optimise resource management and improve legal support in this area.

References

1. Konstytutsiia Ukrainy. [Constitution of Ukraine]: Zakon Ukrainy vid 28.06.1996 r. № 254k/96-VR. Vidomosti Verkhovnoi Rady 1996, № 30, st. 141 [in Ukrainian].
2. Pro oboronu Ukrainy [On the Defense of Ukraine]: Zakon Ukrainy vid 06.12.1991 r. № 1932-XII. Vidomosti Verkhovnoi Rady Ukrainy (VVR), 1992, № 9, st.106 [in Ukrainian].
3. Pro Zbroini Syly Ukrainy [On the Armed Forces of Ukraine]: Zakon Ukrainy vid 06.12.1991 r. N 1934-XII. Vidomosti Verkhovnoi Rady Ukrainy (VVR), 1992, № 9, st.108 [in Ukrainian].
4. Pro viiskovyi oboviazok i viiskovu sluzhbu [On Military Duty and Military Service]: Zakon Ukrainy vid 25.03.92 r. № 2232-XII. Vidomosti Verkhovnoi Rady Ukrainy (VVR), 1992, № 27, st. 385 [in Ukrainian].
5. Pro sotsialnyi i pravovyi zakhyst viiskovosluzhbovtsiv ta chleniv yikh simei [On Social and Legal Protection of Military Personnel and Their Families]: Zakon Ukrainy vid 20.12.1991 r. № 2011-XII. Vidomosti Verkhovnoi Rady, 1992 r. № 15, st. 190 [in Ukrainian].
6. Pro informatsiiu [On Information]: Zakon Ukrainy vid 02.10.1992 r. N 2657-XII: [Elektronnyi resurs]. Rezhym dostupu: https://zakon.rada.gov.ua/laws/show/2657-12 [in Ukrainian].
7. Pro derzhavnu taiemnytsiu [On State Secrets]: Zakon Ukrainy vid 21.01.1994 r. N 3855-XII. [Elektronnyi resurs]. Rezhym dostupu: https://zakon.rada.gov.ua/laws/show/3855-12 [in Ukrainian].
8. Pro zvernennia hromadian [On Citizens' Appeals]: Zakon Ukrainy vid 02.10.1996 r. [Elektronnyi resurs]. Rezhym dostupu: https://zakon.rada.gov.ua/laws/show [in Ukrainian].
9. Pro dostup do publichnoi informatsii [On Access to Public Information]: Zakon Ukrainy vid 13.01.2011r.№ 2939-VI/ [Elektronnyi resurs]. Rezhym dostupu: https://zakon.rada.gov.ua/laws/show/2939-17 [in Ukrainian].