



## Administrative and legal regulation of the use of radio frequency resources for UAVs under martial law

Maryna Larchenko\*

PhD in Law, Associate Professor  
Chernihiv Polytechnic National University  
14035, 95 Shevchenka Str., Chernihiv, Ukraine;  
Mykola Gogol Nizhyn State University  
16602, 2 Graftska Str., Nizhyn, Ukraine  
<https://orcid.org/0000-0002-2643-980X>

**Abstract.** Given the growing significance of unmanned aerial vehicles in modern conflicts, the issue of legal regulation of their use under martial law is becoming increasingly relevant. The aim of this article was to identify the specific features of the administrative and legal approach to managing the radio frequency resource for unmanned aerial vehicles (UAVs) in the context of armed conflict and heightened threats of electronic warfare. To achieve this aim, methods of legal framework analysis, comparative legal approach, and systemic analysis of security challenges in frequency regulation were employed. The article provided a comprehensive study of the administrative and legal aspects of regulating the use of the radio frequency resource for UAVs under the legal regime of martial law in Ukraine. The author highlighted the strategic importance of unmanned platforms for ensuring national security and defence, and draws attention to the specific features of the legal status of UAVs in both military and civilian sectors. The study analysed the existing regulatory acts of Ukraine governing access to the radio frequency spectrum and identifies gaps that limit the effective deployment of drones in combat conditions. Particular attention was paid to the issue of protecting communication channels from enemy electronic warfare, the necessity of implementing cryptographic protection, and the creation of specialised military frequencies for UAVs. Based on an analysis of the practices of NATO, the European Union, and Israel, proposals were formulated to improve the Ukrainian model of administrative control over radio frequency use. The author emphasised the advisability of introducing licensing for civilian UAV operators in combat zones, strengthening coordination between military and civilian authorities in the field of frequency planning, and adapting international standards to the national legal framework. The article proposed a comprehensive approach to forming a frequency security strategy, taking into account the requirements of the digital transformation of the defence sector. The results of the study may be used for the further development of draft regulatory acts and in shaping national policy on UAV usage in the context of cyber and radio frequency threat environments

**Keywords:** unmanned aerial vehicles; electronic warfare; radio frequency resource; cryptographic protection; frequency regulation; national security

### Introduction

The Russian-Ukrainian war has become one of the most prominent examples of the combat use of drones, which has influenced the tactics of warfare and the security of the state. The Armed Forces of Ukraine actively use various types of unmanned aerial vehicles (UAVs) to perform combat missions, including 1) reconnaissance drones, which provide surveillance of enemy positions,

intelligence gathering and adjustment of artillery fire; 2) strike drones, which deliver high-precision strikes on enemy military targets, significantly increasing the effectiveness of operations; 3) kamikaze drones, which are cheap and effective means of destruction capable of inflicting significant losses on enemy forces; 4) logistics drones, which are used to deliver ammunition and

### Suggested Citation:

Larchenko, M. (2025). Administrative and legal regulation of the use of radio frequency resources for UAVs under martial law. *Philosophy, Economics and Law Review*, 5(1), 124-139. doi: 10.63341/2786-491X-2025-1-124.

\*Corresponding author



other resources to the front line. The issue of using the radio frequency resource for UAVs in wartime is extremely relevant. The absence of a clear strategy can lead to significant losses of equipment, intelligence information and combat effectiveness of the Armed Forces of Ukraine. Therefore, it is necessary to develop a comprehensive administrative and legal regulatory system that takes into account both domestic challenges and international experience.

Existing studies and publications showed that the use of radio frequencies for UAVs is currently relevant due to the high level of risks associated with electronic warfare (EW). Thus, according to S.M. Sholokhov *et al.* (2021), the proportion of electronic warfare forces and means used in wars and armed conflicts is constantly increasing due to the growing role of electronic means in enhancing the combat capabilities of troops. The prospects for the development of unmanned systems and the main challenges in the context of increasing the effectiveness of combat operations and the priority of preserving the lives of the military are discussed by O.O. Sapelnykov *et al.* (2024).

The problems of ensuring the security of radio communications and protection against electronic interference were considered in the works of Ukrainian and foreign authors, among which it is worth mentioning the work of V.P. Zaslavets *et al.* (2020), who emphasised the need to develop regulations to ensure stable communications during wartime. A number of authors, including L. Hlivinska *et al.* (2024) and V. Matniak (2024), pointed out critical issues related to the lack of clearly defined legal regulations for the allocation of frequency bands during martial law.

International practice in regulating the use of frequencies for UAVs, especially in martial law, demonstrates some success in ensuring reliable and secure communications. The experience of NATO countries and the United States, in particular, shows the use of encrypted communication channels for military drones and frequency allocation, which avoids the use of civilian frequencies that can be intercepted or jammed by the enemy (Pysarenko *et al.*, 2021). In the work of A. Onofriychuk (2024), the experience of NATO countries in the use of secure frequencies and data encryption in military missions was considered. According to the analysis, NATO countries are actively working to improve the frequency spectrum and develop new military frequencies for UAVs, which is a guarantee of safety and efficiency of their use. Special studies on reforming the administrative and legal regulation of UAV frequencies in Ukraine show that existing regulations need to be adapted to modern conditions. As noted by S.I. Bohdan *et al.* (2024), it is necessary to develop clear mechanisms for controlling the use of frequency bands, taking into account the specifics of martial law and the need to create specialised military frequencies for drones.

Particular attention should be paid to the practical aspects of integrating international experience into Ukrainian legislation, as well as the development of licensing procedures for UAV operators operating in combat zones, as emphasised by A.A. Sakovskiy (2022). Proposals in this regard include the creation of separate frequency bands for military UAVs, as well as the introduction of mandatory communication encryption for all unmanned systems operating in Ukraine under martial law.

Also, according to H.A. Zmiivskiy *et al.* (2024), the armed forces of the world's leading countries pay great attention to the development of mobile radio networks using airborne repeaters placed on telecommunications unmanned aerial platforms and the creation of wireless self-organised networks Flying Ad-hoc networks (FANET) Their use provides interconnection between remote units, increases network performance, communication reliability, quality of user service and enables operational redeployment. These networks can be restored and ensure rapid deployment of the communication system within the coverage area.

A review of the available literature confirmed the importance of developing and improving the administrative and legal regulation of the use of radio frequency resources for UAVs in Ukraine under martial law. It is necessary to take into account international experience and technological innovations in the field of electronic warfare, cryptography and frequency regulation to achieve the maximum effect of using drones in military operations.

The purpose of the article was to analyse the administrative and legal regulation of the use of radio frequency resources for UAVs under martial law. Attention was paid to both military and civilian aspects of the use of drones, in particular, legal support for their operation, countering electronic warfare and ensuring effective management of the frequency spectrum in the interests of national security. To achieve this goal, the following key tasks have been identified:

- 1) to study the administrative and legal aspects of regulating the radio frequency spectrum for UAVs in wartime;
- 2) to identify problems of the current legislation and prospects for its improvement;
- 3) to analyse international experience and the possibilities of its implementation in Ukraine.

## Materials and Methods

The study was carried out in several successive stages: collection and analysis of current Ukrainian regulations and international documents governing the use of the radio frequency spectrum; study of current international experience (NATO, EU, USA, Israel) in the field of frequency policy for UAVs; identification of the main problems related to regulatory support during the Russian-Ukrainian war; analysis of the potential

of current legislation to adapt to new wartime conditions; systematisation of the results obtained and identification of key trends and gaps in legal regulation; identification of areas for further research and current challenges for legal support of the use of radio frequency spectrum in times of war.

The study focused on the issues of delineating the frequency resource between military and civilian drones, protecting signals from enemy electronic warfare, analysing the restrictions imposed by NATO countries, and assessing the ability of national legislation to respond to cyber and radio frequency threats. The information was collected by analysing open state registers, official websites of government agencies of Ukraine and other countries, databases of regulatory acts, as well as specialised analytical reports published by research centres, defence companies and non-governmental organisations. It was also analysed the technical characteristics of anti-drone systems used in Ukraine and instructions for their use published on the manufacturers' official web resources. The study used an interdisciplinary approach that combined elements of law, information security, telecommunications and military affairs, which allowed us to assess the problem in its entirety. The choice of research methodology was based on the need for a comprehensive analysis of the legal regulation of the use of the radio frequency spectrum for UAVs under martial law. Given the complexity and multifaceted nature of this issue, the following methods were used:

1. Analysis of Ukrainian regulations and international standards, which is key to the study of administrative and legal regulation of the radio frequency resource for UAVs. This method made it possible to assess the current legal framework for the use of the frequency spectrum, identify its shortcomings and outline possible areas for improvement. The basis for the legal regulation of the use of radio frequency resources in Ukraine is a number of legal acts, which, in particular, helped in conducting the study. Among them are Order of the Ministry of Defence of Ukraine No. 661 (2016) and Law of Ukraine No. 1089-IX (2020). Also, the Resolution of the Cabinet of Ministers of Ukraine No. 1340 (2023), which was recently adopted, is of particular importance for the purpose of this study.

2. Comparative legal method (experience of NATO, the USA, the EU, Israel) used to analyse international experience in frequency spectrum regulation, as Ukraine can use proven practices of its Western partners in times of war.

3. The method of systematic analysis of problems and challenges in the regulation of the frequency spectrum for UAVs allowed for a comprehensive assessment of all aspects of administrative and legal regulation of the use of the radio frequency spectrum under martial law. The application of this method made it possible to obtain a holistic picture of the problem and develop comprehensive solutions to overcome it.

## Results and Discussion

In addition to military drones, civilian drones are actively used in warfare, performing important auxiliary functions. Volunteer and non-governmental organisations use them to take aerial photographs, search for victims, deliver humanitarian aid, etc. The role of UAVs in the current conflict is constantly growing, and their effective use is becoming a strategic advantage for Ukraine. However, with the development of technology, a number of problems arise, in particular in the field of radio frequency regulation, which is critical for UAV management, as the radio frequency spectrum is a limited resource used for communication and navigation. Military and civilian drones operate in different frequency bands, which creates additional challenges for their coordination and protection.

The importance of effective radio frequency resource management is explained by the following factors: the need to ensure uninterrupted communication between the operator and the UAV, as the drone must be in stable communication with the operator to perform combat and reconnaissance missions, and the use of encrypted communication channels is critical to preventing enemy interception of signals (Zyhrii *et al.*, 2023). Steady-state navigation and positioning means that UAVs use GNSS (Global Navigation Satellite System) for spatial orientation, but satellite navigation signals are jammed by EW on the front line. The use of alternative navigation methods, such as inertial systems or radar technologies, requires appropriate frequency coverage. Enemy forces are actively using jammers to suppress drone control signals. Ukraine needs to develop strategies for frequency distribution and create backup communication channels to ensure the sustainability of UAVs. The use of drones in wartime requires a clear delineation of the frequency spectrum between military and civilian users, and the uncontrolled use of civilian drones can pose risks to the operations of the Armed Forces, which requires appropriate regulation.

Electronic warfare has become an integral part of modern military conflicts, especially in the fight against UAVs. Russia is actively using electronic warfare to suppress Ukrainian drones, which poses serious challenges to the Ukrainian Armed Forces. The main threats posed by electronic warfare equipment are primarily related to jamming communications between the operator and the UAV. The enemy uses powerful jammers to block control signals, forcing the drone to either return to its starting point or crash. This is particularly dangerous for reconnaissance drones, which lose the ability to transmit intelligence. Another danger is the suppression of GNSS signals. Electronic warfare devices can distort or completely block the satellite signal, making it impossible for drones to navigate. The loss of navigation forces operators to look for alternative methods of orientation, which often makes it difficult to complete tasks. That is why, in the war of 2025,

GPS navigation near the front line is almost not used for UAVs (Balan *et al.*, 2025).

Another problem is the interception and hacking of control channels. The enemy can not only suppress the signal but also hack into the control channels of drones. This allows them to change the UAV's route or even use it against their own forces. Finally, physical destruction of UAVs through electronic warfare can occur, as in addition to electronic effects, cyberattacks are used to infect drone software or change their control algorithms. Some electronic warfare systems use directed microwave pulses to 'disable' UAV electronics. In view of these threats, administrative and legal regulation of the use of radio frequency resources should include: 1) identification of strategically important frequencies that must be protected from enemy attacks; 2) introduction of a system of backup frequencies and multi-level encryption of UAV control signals; 3) creation of a regulatory framework for state control over the allocation of frequencies for military purposes.

### **Regulatory and legal framework for the use of radio frequency spectrum for UAVs in Ukraine**

#### *1.1 Main regulatory acts governing the use of radio frequency resource*

Ensuring efficient use of the radio frequency resource under martial law is critical for military and civilian UAVs. In Ukraine, this area is regulated by a number of legislative and subordinate acts that define the procedure for the allocation, management and control of the radio frequency spectrum.

The Law of Ukraine No. 1089-IX (2020) is the main regulatory act governing the use of radio frequency spectrum. Its key provisions are: 1) creation of the basis for efficient and harmonised use of the radio frequency spectrum to ensure economic, social, information and cultural development, state security, defence capability, fulfilment of international obligations, as well as to ensure and protect the interests of the state and users of the radio frequency spectrum (Article 4); 2) distribution of powers of state bodies in the areas of electronic communications and radio frequency spectrum (Articles 5-7); 3) introduction of an electronic regulatory platform, which is an automated information and analytical system of the regulatory authority used to perform its powers under this Law and to provide administrative services in electronic form, electronic exchange of information, documents and interaction with providers of electronic communication networks and/or services, suppliers of radio equipment, users of radio frequency spectrum and numbering resources, and users of services (Article 8); 4) provides for state supervision (control) over compliance with the legislation on electronic communications and the radio frequency spectrum (Article 10); 5) establishes the procedure for licensing and issuing permits for the use of frequencies, the procedure for obtaining and

conditions for licensing the use of the radio frequency spectrum (Articles 48-51).

The Law of Ukraine No. 1089-IX (2020) defines the legal framework for the operation of electronic communication networks, including those used to control UAVs. Its key aspects are: 1) the legal regime of the radio frequency spectrum as a limited resource; 2) ensuring national security through the regulation of electronic communications; 3) the possibility of temporary restriction or redistribution of frequencies in a state of emergency or martial law; 4) setting standards for the protection of radio frequencies from external interference and cyberattacks. It is worth noting that the radio frequency resource is managed in accordance with international standards, and its use should be consistent with the needs of the defence sector, which is especially important in the context of war. However, it does not fully take into account the current challenges of electronic warfare and the need to quickly reallocate frequencies for military purposes, which necessitates its revision.

It is advisable to propose a number of changes that would allow for more flexible and efficient management of the radio frequency resource to meet the needs of the security and defence sector. First, it is necessary to enshrine in the law a separate special regime for the use of the radio frequency spectrum under martial law or in times of threat of armed aggression. Such a regime would provide for priority allocation of frequencies to military formations, automated temporary disconnection/restriction of commercial access to frequencies in designated combat zones, and a mechanism for emergency reallocation of spectrum without the need to go through a full administrative procedure.

Secondly, it is necessary to introduce a provision on the establishment of a Single Coordination Centre for Frequency Management in the Defence Sector, which would function on the basis of the General Staff of the Armed Forces of Ukraine in cooperation with the National Commission for the State Regulation of Electronic Communications, Radio Frequency Spectrum and Postal Services (NCEC). This centre would be empowered to coordinate strategic frequency planning, conduct frequency testing for new weapon systems, and implement operational reconfiguration of spectrum to meet the needs of electronic warfare and cyber threats.

Thirdly, it is advisable to provide for the creation of a register of crypto-secure UAV control channels, within which entities using drones in the interests of defence would be able to access licensed frequencies with an increased level of protection. At the same time, a mechanism for simplified licensing and registration of military drones should be defined, which would allow them to be quickly included in the general contingent of military equipment without delays from civilian spectrum management authorities.

Special attention should be paid to expanding the powers of the NCEC to block or restrict the operation

of drones in prohibited frequency bands, in particular through the creation of technological solutions in the field of electronic scanning and detection of third-party control signals of UAVs used by the enemy. The introduction of these changes will allow for a more rapid response to the dynamics of hostilities, reduce the risk of losing control of UAVs in conditions of active electronic interference, and increase the overall efficiency of drone use in the Armed Forces of Ukraine.

The Government of Ukraine also plays an important role in regulating the allocation of spectrum. Relevant resolutions of the Cabinet of Ministers of Ukraine (CMU) regulate: 1) the allocation of radio frequency spectrum between public and private users; 2) the procedure for granting permits for the use of frequencies; 3) the definition of frequency bands for special use, including military purposes; 4) restrictions or adaptation of frequency use during martial law.

One of the key ones is the Resolution of the Cabinet of Ministers of Ukraine No. 1340 (2023), which contains a list of frequency bands and their purpose. In times of war, this plan must be adapted to ensure the effective operation of military UAVs and minimise threats from electronic warfare. In addition, the Cabinet of Ministers may decide to restrict the use of certain frequencies to prevent their use by the enemy, which is an important element of protecting the country's information space. These issues are regulated by Resolution of the Cabinet of Ministers of Ukraine No. 1459 (2022). As well as Resolution of the Cabinet of Ministers of Ukraine No. 1118 (2022).

The NCEC carries out state regulation in the specified area and is a key body in the field of radio frequency resource management. According to Law of Ukraine No. 1971-IX (2021), its powers include: 1) allocation of the frequency spectrum and issuance of licences for its use; 2) control over compliance with radio frequency legislation; 3) development of regulations and technical requirements for the use of frequencies; 4) ensuring harmonisation of the national frequency policy with international standards; 5) cooperation with the Ministry of Defence on the allocation of frequencies for military purposes.

Given the conditions of martial law, the NCEC plays a critically important role in the rapid reallocation of frequencies for the needs of military drones. It also oversees the blocking of frequencies that may be used by the adversary and enforces control over bands vulnerable to interception or jamming. In cooperation with the Ministry of Digital Transformation and the Ministry of Defence, the NCEC is developing mechanisms to protect critical frequencies from electronic warfare attacks.

The radio frequency resource in Ukraine is regulated by a set of laws and regulations. However, in times of war, new challenges arise that the current legislation does not always take into account, including: 1) the need for prompt reallocation of the frequency spectrum for

military purposes; 2) protection of military frequencies from enemy electronic attacks; 3) regulation of the use of frequencies for drones in the combat zone. Further improvements to the legislation should include more flexible mechanisms for adapting frequency regulation to wartime conditions, which will allow for more efficient use of UAVs in military operations and minimise the threat of jamming or interception by the enemy. In this context, it is advisable to introduce a simplified procedure for temporary military access to the radio frequency spectrum, which would provide for the issuance of permits for the use of frequencies on a 'fast track' basis through an electronic system without the need to go through a full licensing cycle. Such a mechanism could be based on pre-approved bands reserved for the Armed Forces and other law enforcement agencies, with the right to use them promptly upon request from an authorised unit.

In addition, it is proposed to develop and legislate an adaptive frequency map of the combat zone, which will be updated in real time and will allow direct UAV operators to avoid frequency conflicts and reduce the risk of interference. This map should be integrated into the digital management system of military operations. It is also advisable to introduce an experimental legal regime for innovative UAV control technologies (regulatory sandbox), within which the military and drone manufacturers will be able to test new ways of transmitting commands and signals within certain ranges with minimal administrative barriers. This will accelerate the introduction of modern solutions in the field of frequency management and increase the effectiveness of combat use of drones.

### *1.2 Frequency allocation for civil and military UAVs*

The radio frequency resource is a strategic resource of the state, especially in times of war. The use of the frequency spectrum for UAVs depends on their purpose - civilian or military. In Ukraine, frequencies are allocated in accordance with national legislation and international standards. However, war requires adaptation of the frequency policy to ensure the effective operation of military drones and protection against electronic warfare. According to the recommendations of the Centre for Operational Standards... (2019), it is important to ensure that communications are protected from interference caused by jamming systems. Frequency regulation in combat requires clear guidelines for the use of specialised frequencies for civilian and military UAVs, as well as the creation of new frequency bands that could provide reliable communication even in the face of active EW.

Civil UAVs in Ukraine use standard frequency bands permitted for wireless communication and control of electronic devices. These bands are permitted for use in accordance with the provisions of the International Telecommunication Union (ITU-R) (2020), in particular Articles 5.138, 5.150, 5.280 and Annex 1, which

establish global frequency allocations for short-range radio services, including UAVs.

Ukraine has adapted these standards through a number of regulatory acts, including the Technical Regulations for Radio Equipment (approved by Resolution of the Cabinet of Ministers of Ukraine No. 355 (2017) and the National Table of Radio Frequency Allocation of Ukraine, approved by Resolution of the Cabinet of Ministers of Ukraine No. 1340 (2023). These documents specify the permitted bands for wireless communication and determine that UAV equipment can use the relevant bands without licensing, subject to compliance with the technical characteristics and standards of electromagnetic compatibility. Main permitted frequency bands for civil UAVs:

- ▲ 2.4 GHz – widely used for Wi-Fi, Bluetooth, wireless controllers and drone communications;
- ▲ 5.8 GHz – used for video broadcasting and short-range communication with UAVs;
- ▲ 433 MHz – used for radio control of model aircraft;
- ▲ 868-915 MHz – used for telemetry and long-term communication between UAVs and ground stations.

Civil UAVs are subject to certain restrictions. In particular, the power of transmitters is limited by law (for example, for 2.4 GHz, usually no more than 100 mW). In case of interference or frequency band congestion, the state may impose temporary restrictions on the use of civilian frequencies. Some frequencies may be blocked in a war zone to prevent unauthorised use. Also, due to the widespread use of civilian frequencies by adversaries, including reconnaissance and commercial drones, these bands are often targeted by electronic warfare equipment, making them difficult to use in combat. Military drones use closed or specially reserved frequency bands to ensure communication security and counter electronic attacks. Taking into account the Resolution of the Cabinet of Ministers of Ukraine No. 1340 (2023), the main military frequency bands (may vary depending on operational needs) are as follows:

- ▲ L-band (1-2 GHz) – used for drone control and secure satellite communications;
- ▲ S-band (2-4 GHz) – used for communication between UAVs and command centres;
- ▲ C-band (4-8 GHz) – used for military aviation and satellite communications;
- ▲ X-band (8-12 GHz) – provides high-speed secure communication between military UAVs;
- ▲ Ku-band (12-18 GHz) – used to transmit data from drones over long distances via satellite channels;
- ▲ VHF/UHF (30 MHz-3 GHz) – used for military communications and special missions.

The peculiarities of military use of frequencies are that cryptographic protection of communications is widely used. Thus, military UAVs use encrypted channels to prevent signal interception. To counter

electronic warfare, some drones can automatically change frequencies or use adaptive technologies (frequency hopping) to avoid jamming. Reserving frequencies for uninterrupted communication is critical during combat operations, as it is necessary to maintain UAV control even in the face of electronic attacks. In 2025, more and more UAVs will be used for short distances on fibre optics, which are not afraid of electronic warfare, but this technology also has its drawbacks, namely, limited range due to the length of the cable (the coil is placed inside the UAV), difficulty in deploying in the field, and vulnerability of the fibre optic line to physical damage. The prolonged use of fibre-optic UAVs in a certain area of the territory leads to the creation of a "spider web" that prevents further flights of both enemy and friendly UAVs. Therefore, frequency spectrum regulation remains relevant.

War creates new challenges for frequency spectrum management, as civilian and military frequencies may overlap. In such circumstances, the state must effectively manage the frequency resource to ensure reliable communication for its own forces and prevent the enemy from using the frequencies. That is why there is a group of so-called licensed frequencies. These are frequencies that have been officially allocated by government agencies and require special permission to use. Military UAVs, government agencies, and some telecoms operators use licensed frequencies, which are protected from outside interference. In times of war, licensed frequencies may be reallocated for defence purposes and military UAVs may receive priority access to certain bands (Resolution of the Cabinet of Ministers of Ukraine No. 1459, 2022). The state can also restrict or block the use of licensed frequencies by civilians, especially in combat zones (Resolution of the Cabinet of Ministers of Ukraine No. 1118, 2022).

In peacetime, unlicensed frequencies can be used without special permission, such as 2.4 GHz and 5.8 GHz, which are used for commercial drones. In times of war, the military may use civilian frequencies for covert operations to make it more difficult for the enemy to detect drones. The enemy may use the same frequencies, which creates a risk of control override or jamming of signals. Therefore, to protect critical frequencies, jamming systems can be used to block the operation of vulnerable frequencies in certain areas.

Thus, frequency spectrum allocation for UAVs in wartime is a complex and dynamic process. The main challenges are jamming of civilian frequencies by electronic warfare, which complicates the use of drones, the need to adapt the frequency plan for military operations, and the protection of critical military frequencies from interception and attacks. Therefore, further improvements to the legislation should take into account flexible mechanisms for reallocating frequencies in emergency situations, the use of dynamic frequency spectrum management to avoid jamming, and the introduction

of secure communication and cryptographic protection technologies for military UAVs. Implementation of these measures will make it possible to use unmanned systems more effectively in combat situations and increase Ukraine's resilience to electronic threats.

### *1.3. Legal restrictions and liability for violation of frequency regulation*

Regulation of the radio frequency spectrum is an important component of national security, especially in times of war. States impose strict restrictions on the use of frequencies and introduce liability for their violation to avoid chaos in communications and prevent potential threats. For example, in the United States, the use of radio frequencies is regulated by the Federal Communications Commission (FCC) under Title 47 of the Code of Federal Regulations (CFR) (1997), and in the European Union – on the basis of Directive of the European Parliament and of the Council No. 2018/1972 (2018), which provides for a permissive procedure for access to spectrum and criminal liability for violation of the terms of use. In the context of martial law, control over the use of frequencies is significantly enhanced, which requires clear legislative regulation and an effective enforcement mechanism. Unauthorised use of the radio frequency spectrum can pose a threat to military operations, lead to information leakage or facilitate enemy activities. Therefore, the legislation provides for administrative and criminal liability for violation of the rules for the use of radio frequencies.

For example, under the Code of Ukraine on Administrative Offences (1984), Article 145 provides for fines for operating radio electronic equipment without a permit, while Article 188-7 establishes penalties for violating the procedure for using radio frequency resources, specifically for failure to comply with the lawful requirements of the National Commission for the State Regulation of Communications and Informatization. The amount of such fines depends on the severity of the violation and may reach tens of thousands of hryvnias. During wartime, actions that may undermine the state's defence capabilities pose a particular threat – including the unauthorised use of frequencies that interfere with military communications, the malicious jamming of military or critical infrastructure signals, and the transmission of information about military frequencies to the enemy.

According to the Criminal Code of Ukraine (2001), Article 361 provides for liability for unauthorised interference with electronic computer systems (may include radio frequency attacks); Article 361-1 for the creation of software or hardware to interfere with communication networks; and Article 114-2 for the unauthorised dissemination of information on the movement of military formations. Such actions are punishable by imprisonment for a term of several years to life imprisonment (depending on the consequences of the offence).

In times of war, a state may restrict or prohibit the use of certain frequencies by civilians to prevent them

from being used by the enemy or to avoid interfering with military communications. The main legal restrictions may include: temporary disconnection or blocking of certain frequency bands in combat areas, a ban on the use of civilian drones without permission from military administrations, and the transition to centralised state management of the frequency spectrum. These restrictions are set by the General Staff, the National Commission in cooperation with the Ministry of Defence and other security agencies. Examples of prohibitions during the war in Ukraine include restrictions on the use of drones in combat zones without the approval of the military; blocking dangerous frequency bands that could be used to target enemy missiles or drones; and criminalising the illegal use of drones in wartime, especially in frontline regions. Such measures, according to S. Truxal & B. Scott (2024), as well as F. Borsari & G.B., Jr. Davis (2023), are being introduced not only in Ukraine, but also in NATO, the United States and EU countries, which also restrict the use of civilian radio frequency spectrum during wartime or emergency situations.

The state control over the use of radio frequencies is carried out to prevent unlawful interference, interference and threats to the security of communications. The main controlling bodies are the NCEC, which regulates frequency allocation, issues licences and imposes sanctions, the Ukrainian State Centre of Radio Frequencies (USCRF), which monitors the frequency spectrum, records violations and coordinates with other services (Ukrainian State Centre of Radio Frequencies, n.d.), the Security Service of Ukraine (SSU), which investigates cases of unauthorised use of frequencies, especially in the context of espionage or sabotage, and the Ministry of Defence of Ukraine, which ensures military control over frequencies required for defence purposes.

They use automated monitoring of the radio frequency spectrum to detect unauthorised activity. They may also use specialised equipment to identify radio signal sources and implement technologies to jam and neutralise unauthorised signals. Countermeasures may include detecting and blocking enemy drones using civilian frequencies, as well as tightening control over licensing and registration of unmanned aerial vehicles. In some cases, operational measures are taken to identify individuals using illegal frequencies.

Thus, the regulation of the radio frequency resource is an important element of Ukraine's cybersecurity and defence in time of war. The main aspects that require attention are: increased liability for unauthorised use of frequencies, especially in times of war; stricter restrictions on civilian frequencies to avoid threats to military operations; and strengthening state control over the frequency spectrum, in particular through modern systems for monitoring and blocking unwanted signals. Further improvement of administrative legislation in this area should help to increase the effectiveness of

military communications and minimise the risks of enemy electronic interference.

### Challenges of regulating the frequency resource for UAVs in wartime

#### 2.1. Electronic warfare threats and their impact on UAVs

Electronic warfare plays a crucial role in modern conflicts, including the Russian-Ukrainian war, where drones have become key reconnaissance, artillery and strike assets. The enemy's electronic warfare capabilities can significantly reduce the effectiveness of UAVs or disable them completely. The main electronic warfare threats to UAVs include jamming of communication and navigation signals (GPS/GNSS), radio frequency interception and spoofing of control commands, and the use of enemy drones controlled via open frequencies. In particular, the suppression of navigation signals and communication channels renders the drone uncontrollable or forces it into emergency mode. The enemy uses powerful transmitters that generate interference in the GPS/GNSS band, which causes the drone to lose its orientation in space because it has no coordinates for flight, cannot adjust the route or complete the task, and therefore automatically returns to the take-off area or crashes due to loss of communication. Examples of hostile systems are: Zhitel, a Russian satellite jamming system; Pole-21, a GPS/GNSS jamming system with a radius of up to 50 km; Tirada-2S, a strategic-level satellite jamming system (3GIMBALS, 2023).

If an adversary jams the frequencies used by the operator to control the drone, this may result in a loss of communication between the operator and the UAV. Consequently, the drone may automatically switch to return-to-home (RTH) mode or initiate a forced landing. A complete loss of control renders the UAV vulnerable to hijacking or destruction. To achieve this, stationary and mobile electronic warfare (EW) systems are employed to jam the command frequencies of drones (2.4 GHz, 5.8 GHz).

In addition to jamming, the enemy may intercept UAV control signals, which allows access to drone commands, enables route manipulation, or interception of the video feed, with the aim of capturing the drone

and using it for their own purposes. Such actions are called spoofing. This is an attack in which the enemy replaces the GPS signal with false coordinates, causing the drone to fly in the wrong direction or, for example, land in enemy-controlled territory. The drone can also lose its orientation, which leads to a crash. Such attacks are carried out using special transmitters that mimic satellite signals.

If a drone transmits unencrypted data, the adversary may also intercept the video feed and target coordinates, or even hack the control system to force the UAV to alter its course. The intercepted information can be used for counterattacks (for example, to determine the position of Ukrainian forces). The aggressor state actively employs counter-drone systems, including the Krasukha-4 and Leer-3 complexes, which are capable of simulating communication signals and distorting UAV data (3GIMBALS, 2023). The enemy also makes extensive use of loitering munitions (kamikaze drones) that are operated via open or poorly protected communication channels. This poses new challenges for Ukrainian defence. According to a joint Ukrainian-Romanian study by M. Samus (2024), the main types of enemy loitering munitions include the Shahed-136 (Geran-2) – Iranian-manufactured loitering munitions that strike targets using GPS coordinates; the Lancet – a Russian kamikaze drone guided by an operator in real time; and the Kub-UAV – a small strike drone that operates on open frequencies.

If unmanned aerial vehicles (UAVs) are controlled via unencrypted communication channels, this creates risks of interception and course deviation due to jamming or command distortion. There is also the possibility of using enemy drones against themselves (through reverse engineering). Ukrainian specialists are developing anti-drone systems capable of intercepting and blocking control signals of hostile UAVs, allowing for more effective countermeasures against such threats. One example is the Ukrainian system KVS ANTIDRON G-6 (Fig. 1), which, according to the manufacturer QUADRO.UA (n.d.), effectively suppresses drone control and navigation channels, causing them to lose connection with the operator and land.



**Figure 1.** Portable anti-drone system KVS ANTIDRON G-6

Source: QUADRO.UA (n.d.)

The Ukrainian system Bukovel-AD (Fig. 2) is capable of detecting UAVs at a distance of up to 100 km

and jamming their control and navigation signals at a range of up to 20 km.



**Figure 2.** Electronic warfare system Bukovel-AD

Source: Spetstechnoexport (n.d.)

These systems demonstrate a high level of effectiveness and adaptability in the context of modern warfare, providing reliable protection against threats associated with the use of enemy UAVs. Electronic warfare tools are actively deployed on the battlefield, and to mitigate their impact, it is essential to employ encrypted communication channels for military drones, develop domestic technologies for intercepting hostile signals, and enhance counter-drone systems that operate across unsecured frequencies. Therefore, further research should focus on developing UAV platforms resistant to EW, as well as improving the legal framework for protecting the radio frequency spectrum in Ukraine.

### *2.2. Restrictions on the use of civilian frequencies for UAVs during wartime*

Civilian drones are actively used in combat zones for reconnaissance, fire correction, and cargo delivery. However, the open frequencies used by civilian UAVs are easily jammed by EW systems. The enemy may also detect the operator's location, putting them at risk. Uncontrolled use of drones can additionally interfere with military operations. In light of these threats, restrictions or even complete bans on the use of civilian drones may be enforced in military zones. In the United States and other NATO countries, according to S. Truxal & B. Scott (2024), strict regulations govern civilian UAV flights near military facilities. In Israel, as noted by P. Schwennesen (2024), civilian drones are prohibited in combat areas unless coordinated with the military. Therefore, the deployment of civilian UAVs in military zones must be strictly regulated to avoid security threats.

The use of unsecured civilian frequencies during wartime can be dangerous, as the adversary may jam the signals of civilian drones. EW systems can easily block the 2.4 GHz and 5.8 GHz frequencies used by commercial UAVs. If a drone does not use signal encryption, the adversary may intercept control and redirect

it elsewhere. In addition, the enemy may capture civilian drones and use them for reconnaissance. Hackers aligned with the adversary may remotely access drone video feeds by exploiting software vulnerabilities. These risks demonstrate the necessity of restricting open frequencies during wartime and strengthening flight security requirements.

Since February 2022, several significant legislative initiatives concerning the use of the radio frequency spectrum for UAVs have been introduced in Ukraine. During 2022-2023, flight bans for civilian UAVs without special permits were imposed in certain regions. Under decisions made by military administrations, the operation of drones must be coordinated with military authorities. Discussions are also underway regarding the transfer of military UAVs to secure frequency bands. A proposal has been made to establish a separate registry for civilian drone operators operating in military zones. As part of efforts to strengthen frequency control, government authorities have been granted expanded powers to monitor and regulate spectrum usage, while the NCEC coordinates frequency regulation measures for drones during wartime. It has also been proposed to implement encryption standards for military and critically important civilian drones, and to introduce licensing requirements for drone operations under martial law.

Civilian drones may be used in military zones, but their use must be regulated by state authorities. Open frequencies pose security risks, as they may be exploited by the enemy to intercept or jam signals. It is necessary to implement legislative mechanisms to restrict the use of civilian frequencies during wartime and to ensure their proper allocation is controlled. Further research should focus on developing regulatory acts to protect the frequency resource, establishing a system for the identification and monitoring of civilian UAVs, and enhancing protection against electronic warfare threats through the implementation of encrypted

communication channels. Thus, the effective regulation of radio frequency spectrum usage is a critically important element in ensuring the security and effectiveness of military operations involving UAVs.

### *2.3. Challenges of secure communication for military unmanned aerial vehicles*

In the context of modern combat operations, ensuring reliable and secure communication is critically important for the effective use of UAVs. The lack of adequate communication protection poses significant risks, including signal jamming, control interception, and the compromise of intelligence data. For this reason, states actively employing UAVs in military operations are implementing advanced cryptographic protection technologies, secure data transmission standards, and specialised military communication frequencies. One of the main challenges for military UAVs is the need to effectively protect communication channels from enemy electronic warfare systems.

The following technological solutions are used for this purpose, such as real-time data encryption. Control commands and telemetry data are transmitted via secure communication channels. Robust cryptographic algorithms are employed, including AES-256 (symmetric encryption), RSA-4096, and ECC (asymmetric encryption). Encryption ensures the confidentiality of the data, even if it is intercepted by the enemy (Navrotskyi, 2014).

Another technological solution is frequency hopping spread spectrum (FHSS). The use of dynamic frequency hopping technology makes it possible to minimise the risk of signal jamming. The UAV and the ground control station switch operating frequencies thousands of times per second according to a pre-agreed algorithm. Satellite communication can also be used as a backup communication channel. The use of encrypted satellite communication (SATCOM) ensures stable control over UAVs even in the event of radio frequency jamming. The Armed Forces of Ukraine actively use Starlink terminals as a means of communication. In the future, it is necessary to develop domestic military satellite communication systems to minimise dependence on foreign operators.

The reliable protection of communication channels for military unmanned aerial vehicles must comply with international security standards and take into account emerging threats. The main requirements for cryptographic protection include the use of certified cryptographic algorithms that meet the requirements of international standards (Committee on National Security..., 2016, which regulates encryption policy in the United States, and the National Institute of Standards..., 2020). For instance, NIST recommendations define requirements for key lifecycle management, cryptographic algorithms, and their administration in high-security systems. Meanwhile, CNSSP-15 policy regulates the use of open standards for information exchange between U.S. national security systems, including

encryption, authentication, and data integrity protection. AES-256 encryption algorithms are used to protect control commands, while RSA-4096 or ECC are used for authentication. The integrity of transmitted data is ensured using the SHA-3 algorithm. In view of future threats, the implementation of post-quantum cryptographic solutions must be considered (Rohde & Schwarz, 2024).

To protect against Man-in-the-Middle attacks, all control commands must have a cryptographic signature that makes their forgery impossible. Each UAV must contain a unique encrypted identifier that confirms the authenticity of received commands. The regular rotation of cryptographic keys increases the system's resilience. Quantum-resistant key exchange protocols are used to mitigate future threats posed by quantum computing. In the event of unauthorised interference or loss of communication, the UAV must automatically destroy critical data and either switch to autonomous mode or return to a controlled area.

The use of publicly accessible civilian frequencies for military UAVs poses a threat of signal jamming and interception. In this regard, a priority direction for the development of radio frequency policy in Ukraine should be the establishment of specialised military frequencies for unmanned aerial vehicles. The advantages of introducing military frequencies in Ukraine include increased resilience to EW systems through the use of protected bands; integration of UAVs with existing military communication systems (such as tactical radios and satellite systems); and the elimination of conflicts between civilian and military UAV usage. Potential frequency bands for military UAVs include: 1) L-band (1-2 GHz) – used for satellite communication and military aviation systems; 2) S-band (2-4 GHz) – potentially adaptable for medium-range military drones; 3) X-band (8-12 GHz) – promising for long-range tactical UAVs.

It is also necessary to study international experience in regulating military frequencies for UAVs. In the United States, military drones operate on specialised frequency bands that are protected against unauthorised access. More broadly, NATO countries adhere to unified standards for secure communication in UAV military operations. For implementation in Ukraine, it is essential to develop new regulatory acts to allocate military frequencies. Further modernisation of EW systems is also required to effectively counter hostile UAVs, along with the development of new, more efficient types of UAVs, the creation of a unified register of Ukrainian military drones, and their integration with NATO-protected communication systems.

Thus, the development of secure communication channels for military UAVs is a strategic objective for Ukraine. The implementation of modern cryptographic mechanisms, the use of dynamic frequency management, and the allocation of specialised military bands will significantly increase the resilience of UAVs to enemy EW systems. At the same time, further development

of national communication security standards and the reduction of dependence on foreign technologies in this field are necessary.

### **International experience in UAV spectrum regulation and its potential adaptation in Ukraine**

#### *3.1. Radio frequency regulation of UAVs in NATO and EU countries*

Ensuring the effective use of the radio frequency resource for UAVs is an important task for NATO and European Union countries. The operation of both military and civilian drones requires a clear allocation of the frequency spectrum, particularly taking into account security needs, protection against EW, and the integration of UAVs into the overall air traffic management system.

The United States, the United Kingdom, and Germany apply different approaches to UAV frequency regulation; however, the general principles are similar – they involve the allocation of specialised bands, the integration of UAVs into the military aviation network, and protection against electronic attacks. In the United States, spectrum regulation is carried out by the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA). Military UAVs operate within specialised frequency bands in the L- and Ku-bands, which provide stable and secure communication. According to M.A. Jasim *et al.* (2022), the U.S. Army actively uses satellite communication to control drones, which reduces the risk of enemy interference.

In the United Kingdom, responsibility for frequency allocation lies with Ofcom (the Office of Communications) and the UK Ministry of Defence. Military UAVs operate within designated frequency bands that are compatible with NATO communication systems. Considerable attention is given to frequency hopping technologies and encrypted communication to reduce the risk of signal jamming by the adversary (GOV.UK, 2023).

In Germany, regulation is carried out by the Federal Network Agency (Bundesnetzagentur). Military UAVs operate on protected frequencies that do not overlap with civilian usage. Additionally, the country is actively implementing the concept of integrating military drones into the overall air traffic management system, which requires the harmonisation of the frequency spectrum in line with EU and NATO standards (Bundesnetzagentur, 2024). The European Union Aviation Safety Agency (EASA) is the key body responsible for developing recommendations for the integration of UAVs into European airspace. One of the agency's main areas of activity is the unification of frequency regulation for both civilian and military drones.

Within the European Union, the use of frequencies for UAVs is regulated in accordance with Directive of the European Parliament and of the Council No. 2018/1972 (2018), which sets out the general rules for radio spectrum allocation. The main focus is on: 1) the

harmonisation of frequencies for drones in the 2.4 GHz and 5.8 GHz bands for civilian use; 2) the introduction of a unified standard for communication between UAVs and control stations; and 3) the implementation of safe frequency usage principles under the SESAR (Single European Sky ATM Research) programme (European Commission, n.d.). It is important to note that at the European Union level, in line with Decision of the European Parliament and of the Council No. 676/2002/EC (2002), the creation of a dedicated frequency band for military UAVs is being considered – one that would be protected from unauthorised use and jamming.

NATO and EU experience in UAV frequency regulation highlights the importance of clear coordination between military and civilian authorities to ensure the safe and efficient use of drones across various sectors. Ukraine should take these approaches into account to improve its own frequency management system and enhance the country's defence capabilities.

#### *3.2. Frequency regulation and UAV communication security in combat conditions (the case of Israel)*

Israel's experience in the use of UAVs is among the most advanced in the world. Faced with constant military threats and a high probability of enemy EW activity, the Israel Defense Forces (IDF) have developed a comprehensive communication protection system for their military drones. The core elements of this system include strict spectrum control, the use of cryptographic protection, and the deployment of advanced communication technologies.

One of the key challenges in combat operations involving UAVs is the threat of electronic jamming. To counter this, the Israeli military applies an integrated approach to frequency protection. This includes the use of narrow-beam antennas and directional signals, which significantly reduce the likelihood of detection and jamming of communication channels. Another method involves dynamic frequency switching (FHSS), as previously mentioned. A distributed UAV control architecture also helps to minimise the risk of vulnerabilities associated with centralised communication channels.

Moreover, Israel's military drones are equipped with autonomous control systems, enabling them to continue carrying out missions even if communication with the operator is lost. This significantly enhances their resilience to enemy EW measures. One of the key innovations in the field of military communications being implemented by Israel is the use of decentralised networks (Mesh Network) for unmanned aerial vehicles. According to G. Kedar (2024), this technology enables the creation of a robust communication system even under conditions of intense electronic warfare.

The main advantages of Mesh Network for UAVs lie in the absence of a single point of failure. Drones can transmit information through multiple nodes, making the network highly resilient to attacks. UAVs can

dynamically change data transmission routes, bypassing areas where the enemy is conducting jamming. The drones are capable of relaying signals through one another, creating an extended communication network without the need for centralised towers or satellites. According to the analysis by L. Oleksiuk (n.d.), in combat operations, Israeli forces actively employ Mesh Network to facilitate interaction between reconnaissance UAVs, strike drones, and ground command posts. This system enables rapid acquisition of information about battlefield changes and swift adaptation of combat tactics.

Israel's experience in frequency regulation and communication protection for military UAVs demonstrates the importance of a comprehensive approach to security. The combination of protected frequencies, cryptography, frequency hopping spread spectrum (FHSS), and decentralised Mesh Networks significantly enhances the effectiveness of unmanned operations even under challenging combat conditions. Ukraine would benefit from taking these developments into account to improve its own system for the military use of UAVs.

### *3.3. Recommendations for improving the administrative and legal regulation of UAV frequencies in Ukraine?*

Taking into account the current challenges related to the use of unmanned aerial vehicles (UAVs) under martial law, it is particularly important to develop an effective system for regulating the radio frequency spectrum. Insufficient legal clarity and the absence of clear control mechanisms pose risks both to the military use of UAVs and to the safety of civil aviation and state communication systems.

One of the most important areas for improving regulation is the strengthening of state control over the use of the radio frequency spectrum. This would reduce the risks of unauthorised frequency usage and enhance the effectiveness of EW measures. To achieve this, it is necessary to implement automated spectrum monitoring systems capable of detecting and locating unauthorised transmissions in real time. Furthermore, it is important to strengthen the powers of the NCEC regarding frequency allocation oversight and coordination with military authorities, as well as to expand legal liability for the unauthorised use of military or strategically significant frequencies during wartime. One of the key current issues is that military UAVs often operate on frequencies that may also be used by civilian operators or even by the adversary, which poses a threat to the effective deployment of unmanned systems in combat environments. The recommended measures can be summarised as follows:

1) the allocation of dedicated frequency bands exclusively for military UAVs, which will enhance the protection of communication channels from unauthorised interference;

2) the implementation of Dynamic Spectrum Access (DSA) technologies, enabling adaptive frequency changes based on threat levels;

3) the use of encrypted and frequency hopping communication channels, which complicate signal interception and jamming.

The introduction of dedicated military frequencies would significantly reduce the likelihood of successful EW deployment by the adversary and ensure stable communication between operators and UAVs even under challenging combat conditions. In the current context, civilian drones are actively used for reconnaissance, fire adjustment, search operations, and humanitarian tasks. However, the lack of proper regulation of their use during wartime may lead to information leaks, accidental interference with military systems, or even the enemy's exploitation of such drones.

It is therefore advisable to introduce a special licensing system for civilian UAV operators working in combat zones. The main requirements for this process may include: 1) preliminary checks on operators regarding their qualifications and compliance with information security measures; 2) defining clear zones where the use of civilian drones is permitted to avoid conflicts with military operations; 3) creating a unified register of authorised UAV operators, which would prevent chaotic use of the frequency spectrum. Introducing licensing would not only improve the safety of drone operations in combat areas but also contribute to more effective coordination between military and civilian entities.

Thus, in the context of modern warfare, the administrative and legal regulation of the frequency spectrum for UAVs must become one of the key priorities of state policy. Strengthening control over frequency usage, establishing dedicated military bands, and introducing licensing for civilian operators will enhance the effectiveness of unmanned operations, ensure reliable protection of communication channels, and minimise threats from the enemy. The development of a comprehensive frequency regulation strategy in Ukraine should be based on the best international practices, particularly the experiences of NATO, the EU, and Israel, which have successfully implemented similar mechanisms under combat conditions.

## **Conclusions**

The use of UAVs for military and civilian purposes requires clearly defined regulation of the radio frequency spectrum. In the context of the Russian-Ukrainian war, the effective management of frequency resources directly affects the success of combat operations and the state's information security. Based on the conducted research, a number of issues were identified that complicate the efficient use of the frequency spectrum in Ukraine: insufficient legal clarity regarding the allocation of frequencies between civilian and military UAVs; EW threats, particularly GPS/GNSS jamming and radio frequency interception; the absence of dedicated military frequencies for UAVs; the lack of mechanisms to

control the use of civilian drones in combat zones; and a low level of coordination among state authorities responsible for frequency regulation.

The current legislation requires substantial improvement in light of new challenges in the field of security and defence. The experience of NATO, EU countries, and Israel demonstrates effective approaches to regulating the frequency spectrum for UAVs. Based on this experience, it is advisable for Ukraine to allocate frequencies into separate military bands for drones, ensuring their protection through encryption and frequency hopping technologies. It is also important to introduce automated frequency spectrum monitoring systems, which would allow for prompt detection of violations and unauthorised frequency usage, and to strengthen control over the use of civilian UAVs in combat zones by implementing mandatory drone operator licensing and defining regulated usage zones. The improvement of administrative and legal regulation of the

frequency resource will contribute to enhancing the efficiency of UAV use in military operations, ensuring their protection from EW systems, and strengthening Ukraine's overall defence capability in wartime conditions.

A promising direction for further research may be the development of an adaptive model for frequency resource management and the advancement of Mesh Network technology for military drones, which would enable the creation of autonomous and secure communication channels independent of centralised transmitters.

### Acknowledgements

None.

### Funding

None.

### Conflict of Interest

None.

### References

- [1] 3GIMBALS. (2023). *Russian electronic warfare systems: Analytic insight report*. Retrieved from [https://sprotyvg7.com.ua/wp-content/uploads/2023/11/COGINT\\_Analytic\\_Insight\\_Report\\_Russian\\_EW\\_Systems\\_231119\\_114942.pdf](https://sprotyvg7.com.ua/wp-content/uploads/2023/11/COGINT_Analytic_Insight_Report_Russian_EW_Systems_231119_114942.pdf).
- [2] Balan, S., Balan, L., Vorotynskyy, V., Rybak, I., & Tarasiuk, V. (2025). State information policy in the context of hybrid threats: Legal and political aspects. *Social and Legal Studies*, 8(1), 165-178. doi: 10.32518/sals1.2025.165.
- [3] Bohdan, S.I., Porynos, Ye.O., Shendryk, V.I., & Dmytriienko, O.A. (2024). Testing of unmanned aerial vehicles of the copter type (FPV) in conditions of active action of enemy electronic warfare means. In *XXIV Scientific and technical conference of the state research institute for testing and certification of military equipment* (pp. 326-328).
- [4] Borsari, F., & Davis, G.B., Jr. (2023). *An urgent matter of drones*. Retrieved from <https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/>.
- [5] Bundesnetzagentur. (2024). *Administrative regulations on the assignment of frequencies for satellite communications (VV SatFu)*. Retrieved from [https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen\\_Institutionen/Frequenzen/SpezielleAnwendungen/Satellitenfunk/VVSatFu\\_EN.pdf?\\_\\_blob=publicationFile&v=3](https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/SpezielleAnwendungen/Satellitenfunk/VVSatFu_EN.pdf?__blob=publicationFile&v=3).
- [6] Center for Operational Standards and Methods of Preparation of the Armed Forces of Ukraine jointly with the Main Directorate of Preparation of the Armed Forces of Ukraine. (2019). *Methodological recommendations "Fighting against unmanned aerial vehicles" (based on the experience of conducting the Joint Operational Operation (formerly the ATO))*. Retrieved from <https://surl.lu/uirmel>.
- [7] Code of Federal Regulations. (1997, January). Retrieved from <https://www.govinfo.gov/help/cfr>.
- [8] Code of Ukraine on Administrative Offenses No. 8073-1-X. (1984, April). Retrieved from <https://zakon.rada.gov.ua/laws/show/80731-10#Text>.
- [9] Committee on National Security Systems. (2016). *Use of public standards for secure sharing of information among national security systems*. Retrieved from <https://imlive.s3.amazonaws.com/Federal%20Government/ID151830346965529215587195222610265670631/CNSSP15.pdf>.
- [10] Criminal Code of Ukraine. (2001, January). Retrieved from <https://zakon.rada.gov.ua/laws/show/2341-14#Text>.
- [11] Decision of the European Parliament and of the Council No. 676/2002/EC "On a Regulatory Framework for Radio Spectrum Policy in the European Community (Radio Spectrum Decision)". (March 2002). Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002D0676>.
- [12] Directive of the European Parliament and Council of the European Union No. 2018/1972 "On Establishing the European Electronic Communications Code". (2018, December). Retrieved from [https://zakon.rada.gov.ua/laws/show/984\\_013-18#Text](https://zakon.rada.gov.ua/laws/show/984_013-18#Text).
- [13] European Commission. (n.d.). Retrieved from [https://transport.ec.europa.eu/transport-modes/air/single-european-sky/sesar-project\\_en](https://transport.ec.europa.eu/transport-modes/air/single-european-sky/sesar-project_en).

- [14] GOV.UK (2023). *Policy paper: Spectrum statement*. Retrieved from <https://www.gov.uk/government/publications/spectrum-statement/spectrum-statement>.
- [15] Hlivinska, L., Nikolaienko, K., & Vychavka, V. (2024). [Current problems of legal support for national security and defense](#). In *III International scientific and practical conference "The security and defense sector of Ukraine in the protection of national interests: Current problems and tasks in the conditions of martial law"* (pp. 866-868). Khmelnytskyi: NADPSU.
- [16] International Telecommunication Union. (2020). *Radio regulations 2020*. Geneva: ITU.
- [17] Jasim, M.A., Shakhathreh, H., Siasi, N., Sawalmeh, A.H., Aldalbahi, A., & Al-Fuqaha, A. (2022). A survey on spectrum management for unmanned aerial vehicles (UAVs). *IEEE Access*, 10, 11443-11499. doi: [10.1109/ACCESS.2021.3138048](https://doi.org/10.1109/ACCESS.2021.3138048).
- [18] Kedar, G. (2024). *Nomadic networks: Wireless connectivity for defense and public safety field operations*. Retrieved from <https://www.ceragon.com/blog/nomadic-networks-wireless-connectivity-for-defense-and-public-safety-field-operations>
- [19] Law of Ukraine No. 1089-IX "On Electronic Communications". (2020, April). Retrieved from <https://zakon.rada.gov.ua/laws/show/1089-20#Text>.
- [20] Law of Ukraine No. 1971-IX "On the National Commission for State Regulation in the Spheres of Electronic Communications, Radio Frequency Spectrum and Provision of Postal Services". (2021, April). Retrieved from <https://zakon.rada.gov.ua/laws/show/1971-20#Text>.
- [21] Matniak, V. (2024). [Legal support for national security of Ukraine: Current problems and ways to solve them](#). In *III International scientific and practical conference "The security and defense sector of Ukraine in the protection of national interests: Current problems and tasks in the conditions of martial law"* (pp. 956-957). Khmelnytskyi: NADPSU.
- [22] National Institute of Standards and Technology. (2020). Retrieved from <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-57pt1r5.pdf>.
- [23] Navrotskyi, D. (2014). [Cryptographic system for protecting UAV radio channels from unauthorized interference](#). *Ukrainian Scientific Journal of Information Security*, 20(3), 248-252.
- [24] Oleksiuk, L. (n.d.). *Cybersecurity management best practices*. Retrieved from [https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report\\_on\\_Cybersecurity\\_04.pdf](https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_04.pdf).
- [25] Onofriychuk, A. (2024). NATO and EU experience in building national resilience in the security sector. *Journal of Scientific Papers Social development & Security*, 14(1), 138-149. doi: [10.33445/sds.2024.14.1.12](https://doi.org/10.33445/sds.2024.14.1.12).
- [26] Order of the Ministry of Defense of Ukraine No. 661 "On Approval of the Rules for Flights by Unmanned Aircraft Complexes of the State Aviation of Ukraine". (2016, December). Retrieved from <https://zakon.rada.gov.ua/laws/show/z0031-17#Text>.
- [27] Pysarenko, T., Kvasha, T., Havrys, T., Paladchenko, O.F., Molchanova, I.V., Shabranska, N.I., Osadcha, A.B., & Kochetkova, O.P. (2021). In T.V. Pysarenko (Ed.), *Analysis of global technological trends in the military sphere*. Kyiv: UkrINTEI.
- [28] QUADRO.UA. (n.d.). Retrieved from <https://store.quadro.ua/ru/antidron-portativniy-kvs-antidron-g-6>.
- [29] Resolution of the Cabinet of Ministers of Ukraine No. 1118 "On Approval of the Procedure for Using the Radio Frequency Spectrum During a Special Period and in Conditions of Emergency or Martial Law". (2022, October). Retrieved from <https://zakon.rada.gov.ua/laws/show/1118-2022-%D0%BF#Text>.
- [30] Resolution of the Cabinet of Ministers of Ukraine No. 1340 "On Approval of the Plan for the Allocation and Use of the Radio Frequency Spectrum in Ukraine". (2023, December). Retrieved from <https://zakon.rada.gov.ua/laws/show/1340-2023-%D0%BF#Text>.
- [31] Resolution of the Cabinet of Ministers of Ukraine No. 1459 "On Approval of the Procedure for Introducing Temporary Restrictions on the Use of Radio Equipment, Radiating Devices, Radio Electronic Means And Special-Purpose Radiating Devices in the Event of a State of Emergency or Martial Law Throughout the Territory of Ukraine or in its Individual Regions". (2022). Retrieved from <https://zakon.rada.gov.ua/laws/show/1459-2022-%D0%BF#n8>.
- [32] Resolution of the Cabinet of Ministers of Ukraine No. 355 "On Approval of the Technical Regulations for Radio Equipment". (2017, May). Retrieved from <https://zakon.rada.gov.ua/laws/show/355-2017-%D0%BF#Text>.
- [33] Rohde & Schwarz (2024). *What are frequency-agile short-time signals?*. Retrieved from <https://surl.li/shbtgt>.
- [34] Sakovskyi, A.A. (Ed.). (2022). *Features of the use of unmanned aerial vehicles by police agencies and units: Methodological recommendations*. Kyiv: NAVS.
- [35] Samus, M. (2024). *Lessons learned from the war in Ukraine. The impact of drones*. Retrieved from <https://newstrategycenter.ro/wp-content/uploads/2024/02/Lessons-Learned-from-the-War-in-Ukraine-The-impact-of-Drones-2.pdf>.

- [36] Sapelnykov, O.O., Kaluhin, D.S., Kotliar, M.O., Maksymov, M.O., Ovcharenko, Ye.I., & Tymoshenko, P.V. (2024). Prospects for the development of unmanned systems and their impact on the course of hostilities during the large-scale invasion of the Russian Federation into Ukraine. *Science and Technology of the Air Force of the Armed Forces of Ukraine*, 3(56), 7-15. doi: [10.30748/nitps.2024.56.10](https://doi.org/10.30748/nitps.2024.56.10).
- [37] Schwennesen, P. (2024). *Drones and asymmetric warfare in Ukraine and Israel. Attack drones are transforming modern battlefield operations, with today's conflicts serving as laboratories for rapid innovation*. Retrieved from <https://www.gisreportsonline.com/r/drones-ukraine-israel/>.
- [38] Sholokhov, S.M., Samborskyi, I.I., Vakulenko, O.V., & Nikolaienko, B.A. (2021). *Interference protection of radio electronic devices*. Kyiv: Igor Sikorsky Kyiv Polytechnic Institute.
- [39] Spetstechnoexport. (n.d.). Retrieved from <https://spetstechnoexport.com/uk/product/bukovel-ad>.
- [40] Truxal, S., & Scott, B. (2024). The regulation of unmanned aircraft systems in the European Union. In *Civil regulation of autonomous unmanned aircraft systems in Europe* (pp. 31-63). Cheltenham: Edward Elgar Publishing. doi: [10.4337/9781035312344.00008](https://doi.org/10.4337/9781035312344.00008).
- [41] Ukrainian State Centre of Radio Frequencies. (n.d.). Retrieved from <https://www.ucrf.gov.ua/>.
- [42] Zaslavets, V.P., Dolyna, M.P., & Chechui, O.V. (2020). Features of calculating the interference immunity of radio communication lines in conditions of radio suppression (radioelectronic conflict). *Weapons Systems and Military Equipment*, 1(61), 7-12. doi: [10.30748/soivt.2020.61.01](https://doi.org/10.30748/soivt.2020.61.01).
- [43] Zmiivskiy, H.A., Puhach, V.V., Morokhovskiy, M.L., & Horbunov, V.I. (2024). Analysis of the experience of using communication repeaters based on unmanned aerial platforms when performing tactical tasks by units of the Armed Forces of Ukraine, other military formations and law enforcement agencies. *Legal Scientific Electronic Journal*, 11, 550-554. doi: [10.32782/2524-0374/2024-11/129](https://doi.org/10.32782/2524-0374/2024-11/129).
- [44] Zyhrii, O., Trufanova, Yu., Parashchuk, L., Sampara, N., & Tsvigun, I. (2023). Law and technology: The impact of innovations on the legal system and its regulation. *Social and Legal Studios*, 6(4), 267-275. doi: [10.32518/sals4.2023.267](https://doi.org/10.32518/sals4.2023.267).

## Адміністративно-правове регулювання використання радіочастотного ресурсу для БПЛА в умовах воєнного стану

Марина Ларченко

Кандидат юридичних наук, доцент  
Національний університет «Чернігівська політехніка»  
14035, вул. Шевченка, 95, м. Чернігів, Україна;  
Ніжинський державний університет імені Миколи Гоголя  
16602, вул. Графська, 2, м. Ніжин, Україна  
<https://orcid.org/0000-0002-2643-980X>

**Анотація.** З огляду на зростаюче значення безпілотних літальних апаратів у сучасних конфліктах, питання правового регулювання їх використання в умовах воєнного стану набуває особливої актуальності. Метою статті було визначення особливостей адміністративно-правового підходу до управління радіочастотним ресурсом для безпілотних літальних апаратів (БПЛА) в умовах збройного конфлікту та посиленої загрози радіоелектронного впливу. Для досягнення поставленої мети використано методи аналізу нормативно-правової бази, порівняльно-правовий підхід і системний аналіз безпекових викликів у сфері частотного регулювання. У статті здійснено комплексне дослідження адміністративно-правових аспектів регулювання використання радіочастотного ресурсу для БПЛА в умовах дії правового режиму воєнного стану в Україні. Автор підкреслив стратегічне значення безпілотних платформ для забезпечення національної безпеки та оборони, а також звернув увагу на особливості правового статусу БПЛА у військовому та цивільному сегментах. У роботі проаналізовано існуючі нормативно-правові акти України, які регулюють доступ до радіочастотного спектра, виявлено прогалини, що обмежують ефективність застосування дронів у бойових умовах. Окрему увагу приділено проблематиці захисту каналів зв'язку від радіоелектронного впливу противника, необхідності впровадження криптографічного захисту та створення спеціалізованих військових частот для БПЛА. На основі аналізу практик країн НАТО, Європейського Союзу та Ізраїлю сформульовано пропозиції щодо удосконалення української моделі адміністративного контролю за використанням радіочастот. Автор наголосив на доцільності запровадження ліцензування операторів цивільних БПЛА для роботи у зонах бойових дій, посиленні координації між військовими та цивільними органами управління у сфері частотного планування, а також адаптації міжнародних стандартів до національного правового поля. У статті запропоновано комплексний підхід до формування стратегії частотної безпеки з урахуванням вимог цифрової трансформації оборонного сектору. Результати дослідження можуть бути використані для подальшої розробки проектів нормативно-правових актів, а також у процесі формування національної політики у сфері використання БПЛА в умовах загроз кібер- та радіочастотного втручання

**Ключові слова:** безпілотні літальні апарати; радіоелектронна боротьба; радіочастотний ресурс; криптографічний захист; частотне регулювання; національна безпека