Nazarenko, O. L., Hodlevskyi, S. O., Danko, V. V., & Fedorenko, V. O. (2025). Protecting Ukraine's critical infrastructure from drone threats: The role of security and defence forces. *Actual Issues of Modern Science. European Scientific e-Journal, 37*, 70–80. Ostrava.

DOI: 10.47451/mil2025-04-01

The paper is published in Crossref, ICI Copernicus, OJS, BASE, Zenodo, OpenAIRE, LORY, Academic Resource Index ResearchBib, J-Gate, ISI International Scientific Indexing, ADL, JournalsPedia, Scilit, EBSCO, Mendeley, and InternetArchive databases.

Oleh L. Nazarenko, Candidate of Military Sciences, Associate Professor, Department of Operational Training, National Academy of the National Guard of Ukraine. Kharkiv, Ukraine.
ORCID 0000-0001-7579-0658

Serhii O. Hodlevskyi, Candidate of Military Sciences, Department Head, Department of Operational Training, National Academy of the National Guard of Ukraine. Kharkiv, Ukraine.
ORCID 0000-0002-0437-7847

Vitalii V. Danko, Adjunct, National Academy of the National Guard of Ukraine. Kharkiv, Ukraine.
ORCID 0009-0006-1787-5980

Volodymyr O. Fedorenko, Cadet, 1st Platoon of the 273rd Training Group, Command and Staff Faculty, National Academy of the National Guard of Ukraine. Kharkiv, Ukraine.
ORCID 0009-0009-7084-9572

Protecting Ukraine's Critical Infrastructure from Drone Threats: The Role of Security and Defence Forces

Abstract: In the current conditions of the growth of technological threats, the problem of protecting critical infrastructure (CI) facilities from UAVs is gaining particular importance. The growing use of UAVs in various fields, namely, military conflicts, intelligence activities, terrorist attacks and sabotage, creates new challenges for the national security systems of Ukraine. In the context of the ongoing aggression against Ukraine, uncrewed aerial vehicles have become one of the key means of conducting combat operations, reconnaissance, and sabotage activities. The study examines the growing threat of uncrewed aerial vehicles (UAVs) to Ukraine's critical infrastructure (energy, transport, defence) amid ongoing hybrid warfare. UAVs are increasingly used for strikes, reconnaissance, and sabotage, demanding urgent improvements in detection, neutralisation, and legal frameworks. The research analyses technical solutions (electronic warfare, AI-driven systems), regulatory gaps, and interagency coordination challenges. Findings highlight the need for a multi-layered defence combining electronic countermeasures, air defence, and cyber capabilities, alongside updated laws to regulate UAV use. International cooperation and advanced technologies (swarm interceptors, sensor networks) are identified as critical for resilience. The study proposes legislative reforms, enhanced interagency synergy, and adoption of global best practices to fortify Ukraine's infrastructure against evolving drone threats.

Keywords: critical infrastructure protection, drone strikes, regulatory gaps, interagency coordination.

Abbreviations:

CI is critical infrastructure

UAV is an uncrewed aerial vehicles.

Introduction

In the current conditions of the growth of technological threats, the problem of protecting CI facilities from UAVs is gaining particular importance. The growing use of UAVs in various fields, namely, military conflicts, intelligence activities, terrorist attacks and sabotage, creates new challenges for the national security systems of Ukraine. In the context of the ongoing aggression against Ukraine, uncrewed aerial vehicles have become one of the key means of conducting combat operations, reconnaissance, and sabotage activities. They are designed to strike CI, which can lead to significant destruction and disruption of the functioning of strategic facilities, creating a substantial threat to the civilian population.

Today, measures are actively being implemented in Ukraine's security and defence sector to detect and neutralise UAVs. However, existing systems require further improvement by integrating the latest technologies (electronic warfare, laser destruction, cyber defence, etc.) and increasing the efficiency of interaction between Ukraine's security and defence forces. Another pressing issue is improving the modern regulatory framework, which regulates measures to protect CI from UAV attacks, namely, the Law of Ukraine "On Critical Infrastructure".

Recent decades have seen the rapid development of UAVs, which have been used for civilian and military purposes (*Nashivochnikov, 2024*). In the context of modern military conflicts and hybrid threats, the use of UAVs has become one of the most effective means of conducting combat operations, reconnaissance, sabotage, and terrorist attacks.

Continuing to resist military aggression, Ukraine faces a significant threat to the CI facilities (*Gerasymenko, 2024*). Hostile UAVs are actively used to strike at energy, transport, communications, and defence industry facilities, which have serious consequences.

Despite Ukraine's efforts to counter UAVs, key challenges remain, namely (*Nashivochnikov, 2024*): limited effectiveness of traditional air defence against small, agile drones; lack of a unified national strategy for UAV threats, requiring better coordination among security agencies; need for advanced detection/neutralisation tech (electronic warfare means, lasers, cyber defences, automated systems); insufficient laws regulating UAV use and countermeasures; gaps in interagency coordination in protecting CI from drone threats.

Thus, the problem of increasing the effectiveness of protecting CI from threats posed using UAVs is multifaceted and requires a comprehensive solution. It includes technical and organisational legal aspects and requires coordinated interaction of all components of Ukraine's security and defence sectors. Analysing the growing threat of strike UAVs to troops and CI (*Lenkov et al., 2023*), propose increasing the effectiveness of active defence using fragmentation engineering munitions, in particular MON–50, MON–90, MON–100, MON–200, to destroy low-flying targets.

The study (*Krivtsun et al., 2024*) covers technical solutions for countering drones, including electronic means of neutralisation, laser technologies, and mechanisms for physical destruction of drones.

Havrys et al. (*2024*) describes protecting Ukraine's CI facilities during a military conflict, emphasising the complexity of modern threats and the need for an integrated approach. The authors examine the features of information analysis of security systems of strategic facilities during martial law and justify the need to integrate advanced threat monitoring methods.

Thus, the study of measures to counter the threats posed by UAVs to the CI of Ukraine is relevant, allowing: to assess the real threats posed by uncrewed aerial vehicles to the CI of Ukraine; to determine effective methods and means of protecting the CI from UAV attacks, including technical, organisational and legal mechanisms; to develop recommendations for improving the security system of the CI, considering international experience and the specifics of military threats in Ukraine. Given these factors, the study's topic has theoretical and practical significance for ensuring national security and the effective functioning of critical state facilities.

Results

UAVs have become an important element of modern military and terrorist strategies, posing serious threats to CI such as power plants, transportation hubs, military facilities, government buildings, etc. Threats from UAVs can be divided into three main categories: reconnaissance operations, strike impact, and sabotage-terrorist attacks.

Uncrewed aerial vehicles are actively used for reconnaissance due to their ability to penetrate controlled areas while remaining invisible to traditional detection systems. The main threats to reconnaissance UAVs include aerial reconnaissance during which UAVs can photograph strategical facilities in high resolution; radio reconnaissance, carried out by UAVs equipped with devices for intercepting radio signals and collecting information about the operation of communication systems; cyber threats, during which UAVs can be used to hack wireless networks and obtain confidential information.

Modern UAVs can carry various weapons: missiles, explosive devices, unguided munitions and even chemicals. They are used for pinpoint strikes on CI, which can have catastrophic consequences. The main threats from strike-type UAVs include attacks on energy facilities to damage power plants, substations, oil refineries, which can cause massive power outages; destruction of transport infrastructure, attacks on railway junctions, bridges and airports are carried out, which can paralyse logistics; pinpoint strikes on military facilities carried out Kamikaze drones can be used to eliminate important targets.

Due to UAVs' availability and relative cheapness, even small terrorist or sabotage groups can use them to perform illegal actions. Risks of using UAVs by enemy sabotage and reconnaissance groups are as follows (*Yerylkin et al., 2022*):

- using UAVs equipped with explosive devices to attack civilian objects, mass events, government institutions, industrial enterprises, etc.;
- using UAVs to spray biological or chemical weapons;
- using UAVs for sabotage operations (undermining of CI).

Reconnaissance UAVs allow the enemy to obtain precise coordinates of objects. Strike UAVs can destroy strategic objects, causing severe damage. Terrorists can use UAVs to attack civilians.

Protecting CI from UAVs requires a comprehensive approach that includes technical means of detecting and neutralising UAVs, organisational and strategic measures, and electronic counter-UAV systems.

Technical means of combating UAVs are divided into detection systems (*Table 1*) (radars, sensors) and neutralisation means (*Table 2*) (anti-drone guns, laser systems, signal interception).

Unmanned aerial vehicle detection systems include radar systems, which detect drones using radio waves; acoustic sensors, which detect the sound of a drone's engine running; optical and thermal imaging cameras, which identify drones visually; and radio frequency detectors, which analyse drone control signals.

The UAV neutralisation system includes anti-drone guns that create radio interference for drones, causing them to lose contact with the operator; laser installations that physically destroy drones at a long distance (*Shaptala et al., 2023*); interceptor drones equipped with nets to capture enemy UAVs; and cybernetic interception, which is the hacking of drone control channels.

The main security measures for combating UAVs include delimitation of airspace, which is carried out by establishing zones prohibited for UAV flights; increased patrolling, namely, involving the military, police, and private security companies; personnel training, namely, training employees of critical facilities to recognise and respond to threats; cooperation with international partners, exchange of experience and implementation of the latest technologies (*Table 3*).

In addition to physical combat methods, electronic means allow jamming control signals or even intercepting the control of enemy drones (*Table 4*).

The main types of electronic warfare with UAVs include (*Shumygai et al., 2020*) radio-electronic jamming to block communication between the drone and the operator; GPS spoofing, which creates false GPS coordinates for the drone, forcing it to change course; and cybernetic interception, which allows one to take control of an enemy drone.

Adequate protection against UAVs requires a combination of technical, organisational, and electronic measures. The most effective approach combines radar, radio frequency jamming, laser weapons, and territory patrolling. Organisational measures help reduce the risk of attacks but are ineffective without modern technologies. Electronic warfare is a key area, as it allows blocking or capturing drones without physically destroying them (*Tsapura, 2023*).

Protection of CI facilities from UAVs is one of the key tasks of Ukraine's security and defence sector, especially in military conflict and hybrid threats. Legislative regulation of this issue remains relevant, as the use of UAVs for reconnaissance, sabotage, and attacks on strategic facilities is becoming increasingly widespread (*Morkvin et al., 2022*).

Legal regulation in this area should ensure a clear definition of entities responsible for protecting the CI from UAVs, coordination of actions of various structures of Ukraine's security and defence sector, definition of legal mechanisms for neutralizing flights of unauthorized UAVs, and establishment of liability for airspace violation.

Ukraine's regulatory and legal framework regarding the protection of CI from UAVs is based on several main legislative acts (*Table 5*). The shortcomings of the current legislation include an insufficiently developed single mechanism of interdepartmental coordination for combating UAVs, insufficiently defined legal grounds for destroying drones in peacetime, an insufficiently developed mechanism for financing UAV countermeasure systems at the CI, and limited access of law enforcement agencies to technologies for neutralizing UAVs.

Studying the experience of leading countries in legal regulation of the protection of CI from UAVs allows identifying effective legal models for combating drones. In the USA (FAA Part 107, National Defense Authorization Act)—all UAVs weighing more than 250 g are subject to mandatory registration, law enforcement agencies have the right to shoot them down; EU (Regulation 2019/947, 2021/664)—regulates the use of UAVs in general airspace, defines

"drone-free zones: over critical infrastructure; Israel—a strict system of control over UAV flights, active use of electronic warfare (EW) systems to neutralise them; Great Britain (Air Navigation Order 2016)—provides for hefty fines and criminal liability for violating the rules for using UAVs (*Yerylkin et al., 2022*).

To increase the effectiveness of the protection of the CI from UAVs, it is necessary to determine the legal grounds for the destruction of UAVs by law enforcement agencies; introduce a single state register of UAVs to which all civilian and commercial UAVs should be entered; develop a system of "drone-free zones" over military, energy, and transport facilities; strengthen criminal liability for the use of UAVs for illegal purposes; implement a state program for the development of anti-drone systems, finance the creation of technologies to neutralise them. Amendments to the legislation will allow for a more effective response to threats and increase CI facilities' security level.

Protecting CI facilities from threats posed by UAVs requires a comprehensive approach and coordinated interaction between all components of Ukraine's security and defence sector (*Plahotniuk, 2023*). The subjects of the National Critical Infrastructure Protection System are Armed Forces of Ukraine (AFU), Security Service of Ukraine (SBU). National Guard of Ukraine (NGU), National Police of Ukraine (NPU), State Emergency Service (SES), State Border Service of Ukraine (SBSU), local government bodies, private sector and CI operators, international partners, allies and others.

Adequate protection of CI depends on a well-established communication mechanism, joint threat analysis, information exchange, and coordinated response to threats from hostile unmanned aerial vehicles.

The Armed Forces of Ukraine are the main force protecting strategic facilities, military bases, and government institutions from air threats. The main functions of the Armed Forces of Ukraine in the fight against UAVs are their detection and identification. For this purpose, modern air defence and radar surveillance systems are used. Electronic warfare means are used to suppress the communication of enemy UAVs.

Air defence systems, such as surface-to-air missile systems and automated drone destruction systems, are used to physically neutralise UAVS. Mobile teams use small arms and specialized systems (e.g., anti-drone rifles) to neutralise UAVS.

To protect military facilities, special networks and barriers are being established to physically block enemy UAVs. In addition to the above, the latest technologies, such as laser weapons and kinetic weapons, are being considered.

Strategies and exercises are being developed to improve the quality of training, namely conducting joint exercises with NATO allies to improve tactics for combating UAVs while protecting the CI, and developing and implementing new anti-drone technologies and tactical solutions.

The joint work of the SBU, NGU, NPU, and SES is a key element in ensuring critical infrastructure security (*Table 6*). This table lists the main public security sector agencies involved in protecting CI from threats posed by unmanned aerial vehicles and their main functions in countering UAVs. It can be used to analyse the effectiveness of interagency cooperation and further improve the CI protection system.

Key measures to improve cooperation: To respond quickly to UAV threats, an operational headquarters (single coordination center) must be created; intelligence must be exchanged to ensure effective situation analysis and coordination between state bodies; and regular training and joint exercises with practicing drone attack scenarios must be conducted to increase the level of readiness.

The areas of international cooperation are aimed at: obtaining information about the latest threats and methods of countering UAVs; transferring technologies for the supply of modern electronic warfare systems, anti-drone complexes and drone detection means; joint training—participation in international military training on tactics for combating UAVs; financial support—attracting grants and assistance from Western partners to strengthen the protection of critical infrastructure.

The growing threat from UAVs requires continuous improvement of the critical infrastructure protection system. The future development of this system is based on implementing innovative technologies, strengthening the regulatory framework, international cooperation, and increasing the level of coordination between government agencies.

One key development area is the introduction of modern technologies in UAV detection and neutralisation (*Yarosh, 2021*). Promising solutions include modern technologies for protecting CI from UAVs (*Table 7*).

To ensure adequate protection of the CI, significant financial investments are required. The main areas of investment include development and production of domestic UAV countermeasure systems (*Azarenko et al, 2024*); purchase of advanced foreign drone protection technologies; equipping law enforcement agencies with modern electronic warfare and air defence equipment; creation of specialised training centres for operators to combat unmanned threats.

Protecting CI from UAVs requires close cooperation between the military, law enforcement, and other government agencies. The main steps in this direction are creating a unified airspace monitoring system that would combine data from radars, electronic warfare, and observation posts; developing joint protocols for actions in case of detection of a threat from UAVs; conducting joint exercises and training to practice tactics to combat drones; and exchanging intelligence data.

Given the dynamics of UAV technology development, future research and implementation in their neutralisation will focus on the following further development areas:

- improvement autonomous drone interceptors capable of destroying enemy UAVs in the air;
- improvement of the laser drone destruction system, which allows for effective counteraction to UAV swarms;
- integration of electromagnetic pulse systems for deactivating drones;
- expansion of cyber defence capabilities to counter attacks on UAV control systems;
- implementation of intelligent threat analysis systems based on artificial intelligence (*Kazmiruk et al, 2024*).

Discussion

The article's analysis showed that UAVs are becoming one of the key threats to the Ukrainian security forces (*Krivtsun et al., 2024*). They are used both for reconnaissance purposes and for strike action, terrorist acts, and sabotage. Of particular danger are advanced drones with artificial intelligence systems, the ability to operate autonomously, and circumvention algorithms to counteract detection means.

Analysis of the regulatory framework for protecting CI from UAVs showed that Ukraine's current legislation contains separate provisions on this topic. However, it requires updating and detailing regarding countering UAVs (*Slobodska et al., 2023*). There is a need to create a single integrated system of legal regulation to coordinate the actions of state bodies responsible for protecting strategic objects.

The most effective methods of combating UAVs are multi-level protection, namely, electronic warfare (*Tsapura, 2023*), short-range air defence, laser and electromagnetic means, and the development of swarm systems of drone interceptors. Successful protection of critical facilities depends on implementing automated management systems and artificial intelligence for early detection of threats and rapid response (*Kazmiruk et al., 2024*).

An important factor in countering threats from UAVs is effective interaction between the SBU, the Armed Forces of Ukraine, the National Security Service, the State Emergency Service and other security sector structures. Establishing cooperation with international partners, integrating advanced world experience, and adapting modern technologies are key to increasing the country's defence capabilities.

The recommendations were developed on developing the legislative framework, namely, the need to adopt the Law of Ukraine on Combating Unmanned Aerial Vehicles and update existing regulatory legal acts according to international standards; regulation of the use of both civil and military UAVs; definition of restricted airspace zones and legal mechanisms for the forced neutralisation of drones in the event of a threat.

It is necessary to introduce modern technologies, namely, the creation of a multi-level system for detecting and combating UAVs, which will include combined methods of electronic warfare, air defence, laser installations, anti-drone nets, and cyber defence; and the integration of artificial intelligence and automated threat analysis systems to increase the speed of decision-making in the event of an attack.

To increase the effectiveness of the protection of the CI, it is necessary to strengthen international cooperation constantly: exchange of experience with NATO countries in combating UAVs, joint exercises in countering unmanned threats; involvement of international technical assistance and cooperation with companies developing counter-UAV systems.

Protection of the CI requires increased coordination between state structures. This includes a clear definition of the areas of responsibility of various law enforcement agencies in the event of UAV threats and the development of interdepartmental centres for analysis and coordination of measures to counter drone attacks.

Further research directions in this area may include studying promising technologies for combating UAVs, developing effective methods for combining electronic warfare, air defence, laser, and electromagnetic weapons, and implementing distributed airspace monitoring systems based on a network of sensors and analytical centres.

Conclusion

Protection of CI from threats associated with using UAVs is one of the priority tasks of Ukraine's security and defence sector. Modern UAVs are capable of performing reconnaissance operations, carrying out strikes on strategic objects, and also being used in terrorist and sabotage acts. Therefore, the issues of their detection, neutralization, and prevention of attacks are critically important for national security.

The study showed that despite Ukraine's already some experience in countering UAVs, many issues need to be urgently addressed.

First, the current regulatory framework does not yet fully meet modern challenges. The legislation should be supplemented with provisions that regulate the use of drones, establish restrictions on their operation in CI areas, and determine mechanisms for their forced neutralisation. Studying international experience in the legal regulation of UAVs and adapting it to Ukrainian realities is also important.

Secondly, adequate protection of UAVs is possible only if an integrated approach is used, which includes technical means of detection, electronic countermeasures, short-range air defence, and cyber defence. The development of automated control systems and artificial intelligence will increase the speed and accuracy of response to threats from UAVs.

Thirdly, an important aspect is coordination between state structures responsible for protecting critical infrastructure. Interagency coordination is a key factor in ensuring an effective response to drone threats. In addition, international cooperation, the exchange of experience with NATO countries, and the introduction of the latest technologies will also contribute to increasing the level of protection of critical infrastructure.

The prospects for developing the CI protection system as a comprehensive approach include improving legislation, expanding technical capabilities in combating UAVs, and increasing the level of training of personnel responsible for the security of strategic facilities. Further research should focus on developing new methods of combating unmanned threats, integrating artificial intelligence into security systems, and creating effective mechanisms for interagency cooperation.

Conflict of interest

The authors declare that there is no conflict of interest.

References:

Azarenko, O., Goncharenko, Y., Divizinyuk, M., Kamyshentsev, G., & Farrakhov, O. (2024). Some aspects of the classification of unmanned aerial vehicles in the interests of protecting critical infrastructure. *InterConf*, *193*, 624–637. (In Ukr.). https://doi.org/10.51582/interconf.19-20.03.2024.060

Gerasymenko, O. (2024). Threats to critical infrastructure facilities of Ukraine under martial law. *Scientific Bulletin of Uzhhorod National University. Series: Law*, *83*(3), 257–263. (In Ukr.). https://doi.org/10.24144/2307-3322.2024.84.3.39

Havrys, A., Fillipova, V., & Tur, N. Y. (2024). Informative analysis systems protection objects critical infrastructure during the period actions military state. *Bulletin of the Lviv State University of Life Safety*, *30*, 173–187. (In Ukr.). https://doi.org/10.32447/20784643.30.2024.17

Kazmiruk, S., Leonov, B., & Omelyan, O. (2024). Ensuring cybersecurity of critical infrastructure facilities based on the use of artificial intelligence in military conditions. *Legal Scientific Electronic Journal*, *6*, 201–205. (In Ukr.). https://doi.org/10.32782/2524-0374/2024-6/49

Krivtsun, V., & Golushko, S. (2024). Analysis ways and means countermeasures unmanned flying devices and directions their improvement. *Journal of Scientific Papers Social Development and Security*, 210–222. (In Ukr.). https://doi.org/10.33445/sds.2024.14.4.17

Lenkov, S., Kryvtsun, V., Miroshnichenko, O., Golushko, S., & Koltsov, R. (2023) Analysis of the state of development of the issue of protection of critical infrastructure facilities using engineering ammunition. *Underwater Technologies Industrial and Civil Engineering*, 81–91. (In Ukr.). https://doi.org/10.32347/uwt.2023.13.1803

Morkvin, D., & Pershina, K. (2022). Novelties of legislation and modern trends in regulatory and legal support for the protection of critical infrastructure facilities by units of the National Guard of Ukraine. *Legal Scientific Electronic Journal*, *10*, 444–447. (In Ukr.). https://doi.org/10.32782/2524-0374/2022-10/109

Nashivochnikov, O. (2024). Experience of using unmanned aircraft in the Russian-Ukrainian armed conflict (2014-2018). *Collection of Scientific Papers of the Center for Military Strategic Research of the National Defense University of Ukraine*, 2(81), 124–129. (In Ukr.). https://doi.org/10.33099/2304-2745/2024-2-81/124-129

Plahotniuk, R. (2023). Conceptual principles for improving interaction between authorized bodies in the field of critical infrastructure protection. *Problems of Modern Transformations. Series: Law, Public Management and Administration*, *7*. (In Ukr.). https://doi.org/10.54929/2786-5746-2023-7-01-17

Shaptala, S., Romanenko, E., & Khraschevskiy, R. (2023). Using lasers to counter unmanned aerial vehicles. *Science and Technology Today. Series: Technology*, *11*(25), 617–629. (In Ukr.). https://doi.org/10.52058/2786-6025-2023-11(25)-617-629

Shumygai, O., & Ermolenko, O. (2020). Current state of multifunctional means and complexes of electronic warfare. *Collection of scientific works of the State Research Institute of Testing and Certification of Armaments and Military Equipment*, *3*(5), 119–125. (In Ukr.). https://doi.org/10.37701/dndivsovt.5.2020.14

Slobodska, I., & Yukhymovych, M. (2023). Legal regulation using unmanned aircraft devices in civil aviation Ukraine. *Legal Bulletin*, *1*, 112–126. https://doi.org/10.18372/2307-9061.65.17036

Tsapura, M. (2023). Analysis of electronic warfare systems against unmanned aerial vehicles: qualification work for the degree of Master in the specialty "125 – Cybersecurity" Ternopil: TNTU. (In Ukr.) http://elartu.tntu.edu.ua/handle/lib/43363

Yarosh, S., & Guriev, D. (2021). Justification of the possibility of using modern, advanced and promising weapons to combat unmanned aerial vehicles in the anti-aircraft missile forces group. *Science and Technology of the Air Forces of the Armed Forces of Ukraine*, *3*(44), 88–100. https://doi.org/10.30748/nitps.2021.44.10

Yerylkin, A. G., Guriev, D. O., Karlov, D. V., Korobetsky, O. V., & Shevchenko, Y. A. (2022). Review and analysis of world experience in combating strike unmanned aircraft. *Science and Technology of the Air Forces of the Armed Forces of Ukraine*, *4*(49), 15–22. (In Ukr.). https://doi.org/10.30748/nitps.2022.49.02

Appendix

Table 1. Main UAV detection systems

System name	Working principle	Range (km)	Advantages
AN/TPQ-53	radar detection	20	large radius of action
DroneShield DroneSentry	combined approach (radar + acoustics)	10	high accuracy
Dedrone RF-100	radio frequency analysis	5	affordable price

Table 2. Means of UAVs neutralisation

Weapon type	Principle of operation	Range (km)	Advantages
DroneGun Tactical	Radio electronic jamming	1	Compactness, mobility
Thor C-UAS	Electromagnetic pulse	5	Mass destruction
High Energy Laser	Laser radiation	10	Instant destruction of UAVs

Table 3. Organisational measures to combat UAVs

Action (mesure)	The essence of the event	Expected effect
Flight zone control	Introducing restrictions on the use of drones close to the strategic facilities	Reducing the likelihood of unauthorized flights
Protection of critical facilities	Organization of physical security using modern technologies	Rapid response to threats
Staff training	Conducting training on UAV identification and neutralization	Increasing readiness

Table 4. Electronic systems for combating UAVs

System name	Principle of operation	Efficiency (%)	Range (km)
SkySafe	Radio frequency jamming	85	3
DroneDefender	GPS spoofing	90	1
MESMER	Cyber Interception	95	5

Table 5. Legal regulation of combating UAVs in the field of protecting CI

Document	Main provisions	Importance for the protection of CI
Constitution of Ukraine	Defines the sovereignty and security of the state as a priority	Guarantees the state's right to protect critical infrastructure facilities
On National Security, Law of Ukraine	Determines the structure of the security and defence sector, coordination between agencies	Establishes those responsible for protecting CI from air threats
Air Code of Ukraine	Regulates the use of airspace, determines the order of UAV flights	Sets restrictions for flights over critical infrastructure
On Combating Terrorism, Law of Ukraine	Allows special units to eliminate threats, including from UAVs	Used to neutralise drones in the event of a terrorist attack

On Critical Infrastructure, Law of Ukraine	Identifies critical infrastructure facilities and measures to protect them	Provides for the implementation of counter-UAV technologies
On Approval of the Regulations on the Use of the Airspace of Ukraine, Resolution of the Cabinet of Ministers No. 954 from December 6, 2017	Defines a list of no-fly zones	Prohibits UAV flights over CI

Table 6. Functions of government structures in the field of countering UAVs

Authority	Functions in countering UAVs
Main Intelligence Directorate of the Ministry of Defence of Ukraine (GUR MO)	Identifying sources of enemy UAV launches, collecting and analysing intelligence on unmanned threats. Coordinating actions with international partners to obtain the latest UAV defence technologies.
Armed Forces of Ukraine (AFU)	Using electronic warfare (EW) to neutralise enemy UAVs, deploying air defence (AD) systems to protect strategic targets. Conducting special operations to destroy enemy drone operators.
Security Service of Ukraine (SBU)	Counterintelligence activities, counterterrorism, detection and elimination of sabotage groups using UAVs. Threat analysis and development of response measures.
National Guard of Ukraine (NGU)	Protection of strategic critical infrastructure facilities, protection of industrial and energy enterprises. Implementation of special measures to identify and neutralise threats associated with UAVs.
State Border Service of Ukraine (SBSU)	Detection of illegal UAV airspace crossings, protection of border facilities, surveillance and threat analysis. Use of specialised electronic warfare systems to combat drones at borders.
National Police of Ukraine (NPU)	Public order protection, response to incidents involving the use of drones in urban environments, combating the illegal use of UAVs. Conducting operational measures to detect illegal drones.
State Emergency Service (SES)	Elimination of the consequences of UAV attacks on critical infrastructure, conducting evacuation measures, training personnel of critical facilities. Demining and disposal of dangerous facilities after drone attacks.
State Enterprise "Ukroboronprom"	Development and implementation of the latest UAV detection and neutralisation systems. Production of electronic warfare (EW) and air defence systems.

Table 7. Modern technologies for protecting CI from UAVs

Technology	Principle of operation	Expected effect
Electronic warfare (EW)	Suppression of communication channels between the UAV and the operator, blocking of navigation signals (GPS, GLONASS).	Loss of control of drones, their forced landing or departure in an unspecified direction.
UAV detection systems	Optical, acoustic and radar sensors for real-time drone tracking.	Early detection of threats, increased response time, increased defence effectiveness.
Short-range air defence	The use of portable air defence systems, C-RAM-type systems, and anti-aircraft artillery to destroy enemy drones.	Physical destruction of attacking UAVs, reducing damage to critical infrastructure.

Automated security management systems	Using artificial intelligence to analyse threats, make decisions, and coordinate security forces.	Increasing the efficiency of CI security management, rapid response to UAV attacks.
Cybersecurity	Implementation of technologies to protect against cyberattacks on infrastructure related to UAV control.	Minimising the risks of hacking control and navigation systems, protecting critical digital networks.
Anti-drone nets and mechanical devices	Using special nets and UAV interceptors to capture enemy drones physically.	Safe neutralisation of drones without the use of weapons, minimising collateral damage.
Laser weapon	The use of high-energy lasers for pinpoint destruction of UAVs at close and medium distances.	Destruction of drones without ammunition, high accuracy of destruction.
Drone swarm systems	Using groups of interceptor drones to counter enemy UAVs in automatic mode.	Collective fight against massive drone attacks, creating an effective defence barrier.
Electromagnetic weapons (microwave guns)	Generating a powerful pulse of electromagnetic radiation to disable drone electronics.	Mass disabling of UAVs in the affected area without physical destruction of objects.