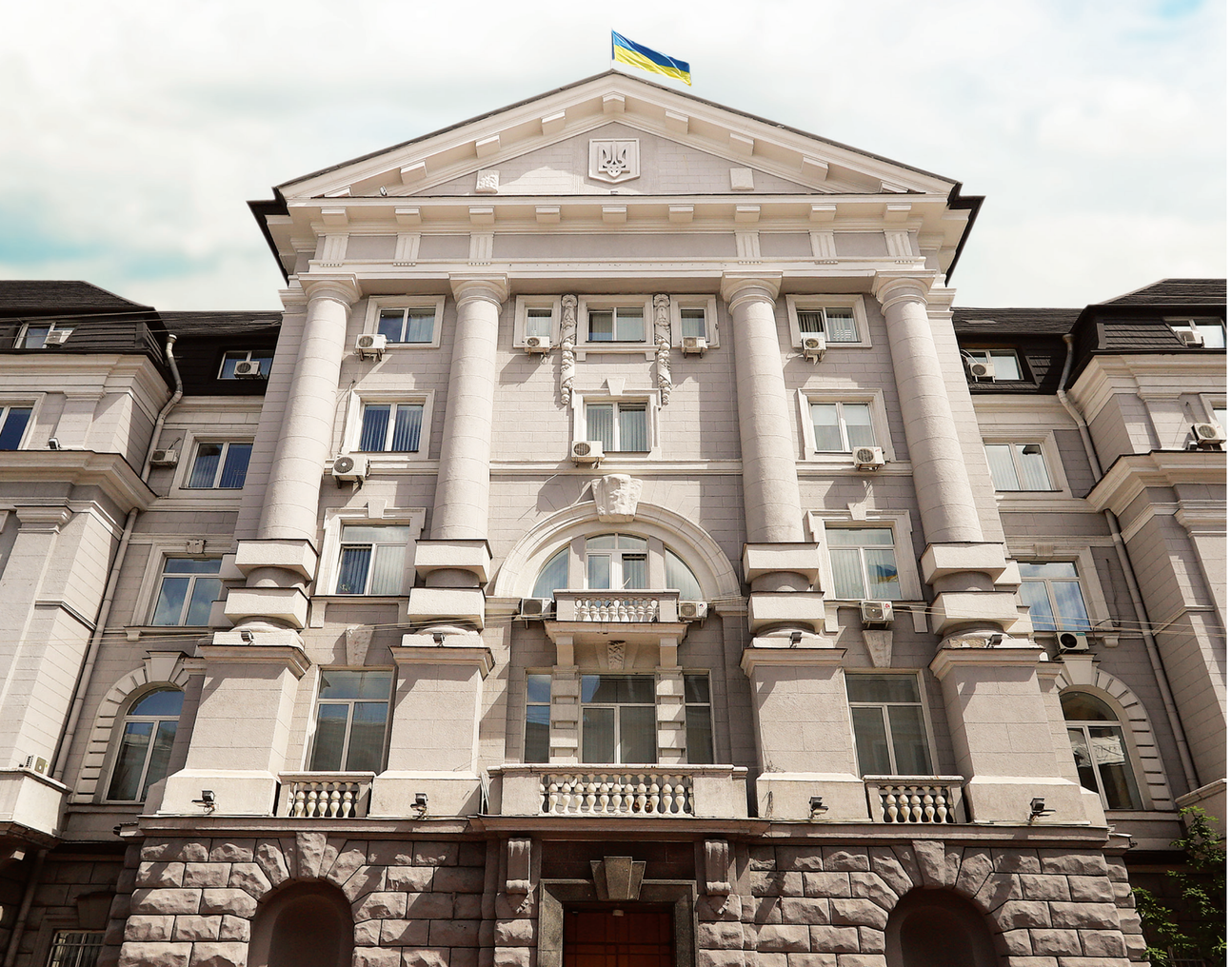
SECURITY SERVICE OF UKRAINE

DEVELOPMENT STRATEGY OF THE SECURITY SERVICE OF UKRAINE FOR 2025 – 2030



CONTENTS

PREAMBLE

The SSU Development Strategy is worked out in accordance with the National Security Strategy of Ukraine, approved by the Decree of the President of Ukraine No. 392 dated 14.09.2020, the State Security Strategy, approved by the Decree of the President of Ukraine No. 56 dated 16.02.2022, other strategic programme documents, and takes into account the provisions of the Comprehensive Strategic Plan for Reforming Law Enforcement Agencies as Part of the Security and Defence Sector of Ukraine for 2023-2027, approved by the Decree of the President of Ukraine No. 273 dated 11.05.2023, and the Implementation Plan, approved by the Order of the Cabinet of Ministers of Ukraine No. 792-r dated 23.08.2024.

THE STRATEGY:

- defines the main directions of the SSU transformation into a single national counterintelligence agency capable of timely and effectively countering external and internal threats to state security;
- envisages the implementation of modern approaches to personnel management and professional training, risk-based methods of responding to threats, and the introduction of the latest technological solutions in operational and combat activities, including the development of weapons and the application of military innovations, the improvement of the information analytical component, resource support, digital transformation, and the expansion of international cooperation;
- takes into account more than 30 years of experience of the SSU, including 10-year countering russian hybrid and armed aggression against Ukraine, revolutionary changes in military and information technologies, the transformation of Ukrainian legislation, the provisions of international security treaties, changes in the global security environment and measures taken by Ukraine in the framework of European integration.

Certain provisions of the Strategy may be reviewed and adapted depending on changes in the security environment.

VISION, MISSION, VALUES AND PRINCIPLES

VISION:
we are an effective special service of a strong Ukraine, trusted by Ukrainian society, a reliable partner in defending democracy.

MISSION

- we protect the Ukrainian people and national interests of Ukraine;
- defend the constitutional order, ensure state security;
- create conditions for the strategic advantage of our country in the world.

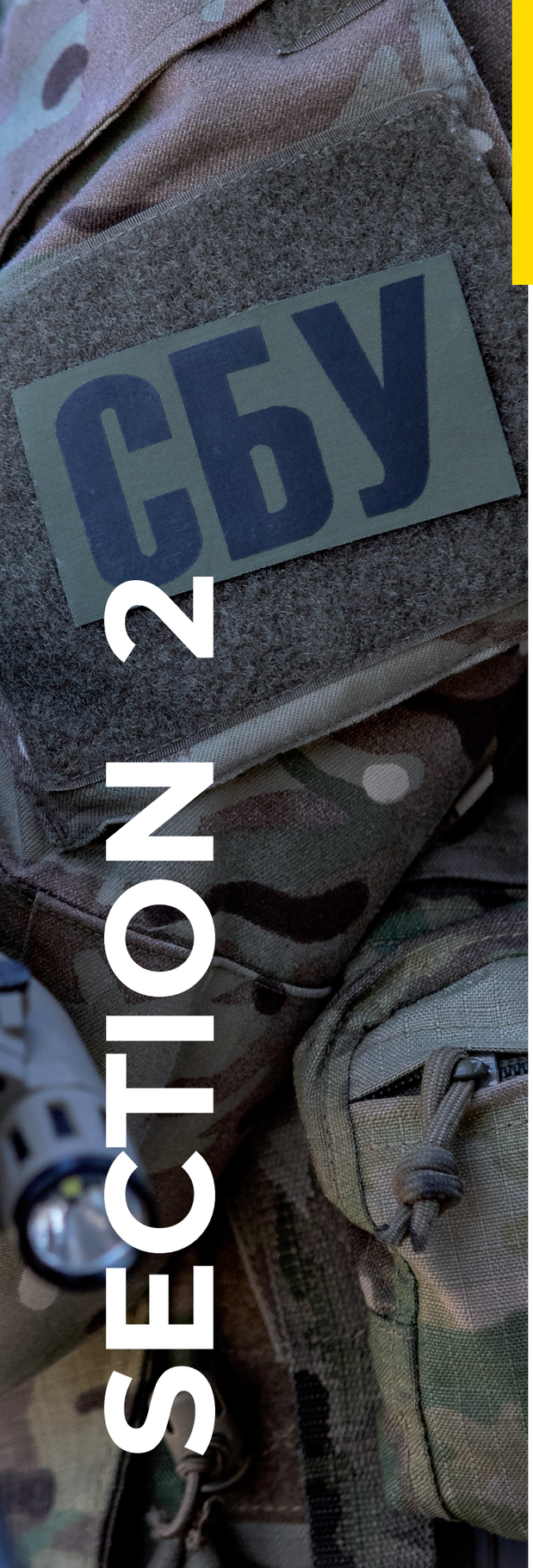
VALUES

- trust of the Ukrainian people;
- respect for human and civil rights and freedoms;
- patriotism, professionalism and continuous improvement;
- unique experience gained during the war;
- effective cooperation with the special services of partner countries;
- corporate unity.

PRINCIPLES

- rule of law and legality;
- responsibility and accountability;
- political neutrality;
- efficiency, innovation, flexibility and adaptability;
- readiness for challenges;
- integrity and commitment to serving the Ukrainian people.

THE STRATEGY IMPLEMENTATION IS BASED ON PEOPLE, PROCESSES, INNOVATION AND PARTNERSHIP.



SECTION 2

PRIORITY AREAS OF ACTIVITY

IN DETERMINING THE PRIORITIES OF OUR MISSION, WE MUST ANSWER THE FOLLOWING QUESTIONS:

- What are the current and potential threats to Ukraine's security?
- Which of these threats should the SSU counteract?
- Which threats currently pose the greatest danger?
- What forces, means, resources, technologies, organisational and legal measures are needed to respond to threats?

The greatest threat to Ukraine's sovereignty, constitutional order and territorial integrity remains the aggressive war waged by the russian federation with the support of its allies.

We do everything possible to liberate the temporarily occupied Ukrainian territories from the enemy, effectively destroy its capabilities, neutralise its spies and their agents, bring traitors, collaborators and war criminals to justice, counter sabotage, terrorism, information and cyber attacks, protect the defence-industrial complex, critical infrastructure and supply chains, protect state secrets, and increase the trust of Ukrainian society.

We integrate innovations into operational and combat activities, improve resource support, establish interaction and coordination with other components of the security and defence sector and with security institutions of partner countries during joint operations.

To effectively protect Ukraine's national interests in times of war and during the reconstruction period, we need modern technological solutions and tools, weapons and armaments, trained personnel, and sufficient resources.

In wartime and during the reconstruction period our activities will focus on the fulfilling tasks in the following areas.

COMBAT OPERATIONS

For the SSU, the war began back in 2014, when the conflict had a different character - it was a hybrid aggression with localised combat zones. russia's full-scale invasion in 2022 became a much greater threat, stretching the front lines across for thousands of kilometres. Therefore, the approaches to warfare and technical equipment used ten years ago cannot be compared with current realities.

During the war with russia, the SSU has become a generator of new military ideas, technologies and competencies.

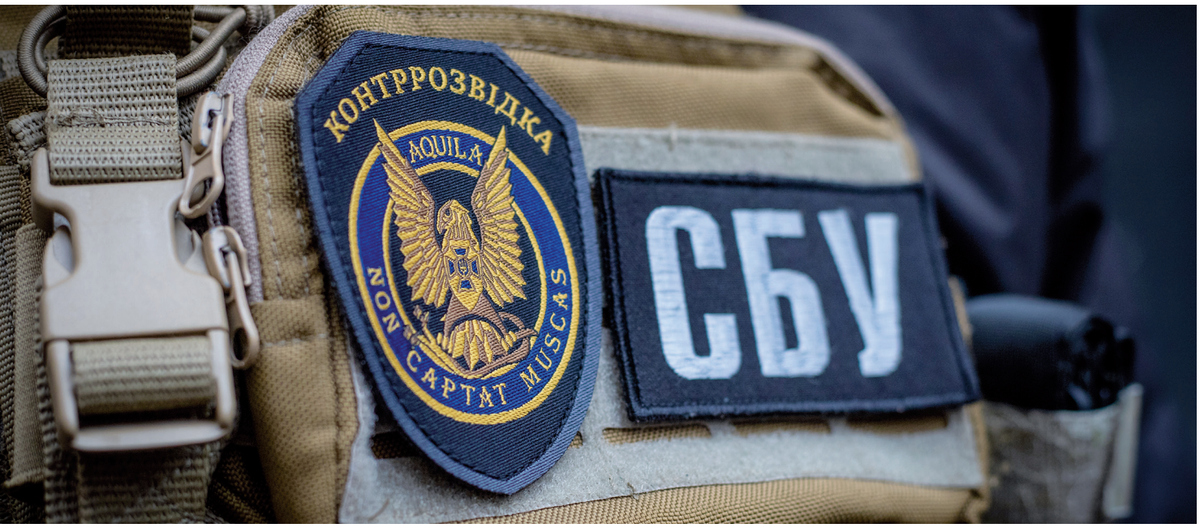
We actively use high-precision weapons, modern intelligence systems, automated control systems, and various types of strike UAVs. This gives us the advantage of staying one step ahead of the enemy and striking where they do not expect it including military-industrial facilities and enemy army supply centres in their deep rear.

To this end, we are constantly working to improve operational and combat support, including the integration of artificial intelligence into military technologies that can reshape the battlefield dynamics.

PRIORITIES

- *development of ground based robotic systems, reconnaissance and strike UAVs in combination with artificial intelligence, electronic intelligence and warfare systems as a powerful tool to counter the enemy on all domains - at sea, in the air and on land;*
- *development of the latest means of controlling and protecting forces and assets;;*
- *increasing the mobility and protection of units through the use of armoured land vehicle, aircraft, sea and river vessels;*
- *cooperation with the defence industrial complex to develop and produce modern weapons, armaments and equipment;*
- *use of SIGINT, OSINT, IMINT, and artificial intelligence technologies to detect and eliminate enemy targets under any conditions;*
- *improving maintenance, medical and logistics support for operational and combat activities regardless of their operational location.*

COUNTERINTELLIGENCE



Since Ukraine gained its independence, our adversaries have been conducting mostly covert reconnaissance and subversive operations (actions).

In today's geopolitical realities and with the technological advance, a part of the targeted actions of foreign states against Ukraine remain covert.

To counter adversaries more effectively, we need to obtain reliable information in advance about their plans, intentions, methods, tactics, involved persons, and vulnerabilities. We also must to focus on conducting human intelligence (HUMINT), open source intelligence (OSINT), scientific and technical intelligence (MASINT), electronic intelligence (SIGINT) and image-based intelligence (IMINT), automate data processing and analysis using the latest tools and technologies that will help understand better the scale and nature of threats.

We must go beyond the existing approach to identifying and predicting the actions of our adversaries and build a modern, effective system of proactive influence on their activities against Ukraine.

PRIORITIES:

- *countering intelligence, subversive and other activities of special services of foreign states and other entities to the detriment of Ukraine;*
- *counterintelligence support of the defence, economic, information, scientific and technical potential, critical infrastructure, supply chains, components of the security and defence sector, foreign diplomatic missions of Ukraine, security of their staff and families in the host country;*
- *assisting in enforcing international sanctions, international non-proliferation regimes, and state control over international transfers of military and dual-use goods;*
- *separating counterintelligence, operational and investigative activities (criminal intelligence), criminal procedure, and regulating procedures for conducting counterintelligence activities;*
- *developing a system to ensure the counterintelligence regime in Ukraine;*
- *introducing a flexible structure capable of responding promptly to threats to Ukraine's national security;*
- *ensuring the SSU's own safety.*

PROTECTION OF NATIONAL STATEHOOD

Protecting state sovereignty, territorial integrity and constitutional order is one of the Service's top priorities.

Anti-Ukrainian policies, economic expansion, territorial encroachment, and incitement of religious, ideological, ethnic, and other hostilities remain the main source of threats to national statehood.

Unfriendly foreign states widely use all opportunities - from foreign policy platforms to spreading fake information on social media.

We must detect signs of preparations for hostile actions, their main purpose and focus, the structures, individuals, the resources involved, the forms and methods of their conduct, and adequately counter them in advance.

PRIORITIES:

- *neutralizing destructive influence on the socio-political, cultural, scientific, educational and informational spheres;*
- *improving the system of detecting and counteracting destructive information influence, including preventing its organisation, coordination and financing;*
- *participating in nation-wide events to improve media literacy of the population.*

FIGHTING TERRORISM

From the very first days of its establishment, the Security Service of Ukraine has given priority to the fight against terrorism.

We counteract manifestations of terrorism and its financing and coordinate the activities at the state level. The Anti-Terrorist Centre at the SSU functions for this very purpose.

Today the terrorist threat has evolved: alongside the activities of organised terrorist groups, the threat of lone terrorists acting autonomously, but often under ideological or informational influence, has increased. These individuals are radicalised via Internet and can quickly mobilise to commit violent acts. The lack of a clear affiliation to terrorist organisations makes it difficult to identify them, detect and neutralise terrorist plotting, as well as investigate such acts.

International terrorist organisations widely use the Internet and social networks to spread their ideologies, radicalise and recruit people, and coordinate terrorist attacks.

In fulfilling our international obligations in the field of counter-terrorism, we join efforts with foreign partners to neutralise terrorist organisations (groups), identify signs of preparation of terrorist acts, persons being recruited or encouraged to commit them, to neutralise supply chains of explosives and other weapons, international channels of transfer of perpetrators, financing, and training terrorists.

In wartime and after the end of hostilities, illicit trafficking of weapons, armaments, ammunition and explosives is expected to increase and be used by terrorist organisations (groups, terrorists) and other components of the criminal environment.

PRIORITIES:

- *enchancing the effectiveness of SSU interaction with other counter-terrorism entities and international partners;*
- *harmonizing national anti-terrorism legislation with international standarts;*
- *implementing effective mechanisms for monitoring, processing and exchanging information on detected signs of preparation of a terrorist act (activity), related persons, forms, methods and means of terrorist activity, and sources of its financing;*
- *providing professional training for representatives of the civil sector, state authorities and local self-government bodies on counter-terrorism, and involving relevant representatives in anti-terrorism exercises.*

ENSURING INFORMATION SECURITY AND CYBERSECURITY

The world is changing rapidly due to acceleration of digital transformation, the intensive development of information and communication technologies and the expected growing role of intelligent computer systems.

It is cyberspace and its tools that provide the enemy with ample opportunities to carry out various destructive activities without personal risk - from collecting the necessary information through in-depth monitoring of the information segment, unauthorised technical intrusions, to cyberattacks on critical infrastructure, military and public administration, the spread of destructive propaganda and disinformation.

Our adversaries make extensive use of information and cyberspace, modern technologies, including those designed to interfere with the automated management of life support and decision-making processes. This poses new risks and threats to the state and people.

Within the limits of our authority, together with other subjects relevant to information security and cybersecurity, we must create conditions to prevent destructive impact on the information and cyberspace of the state, develop deterrence capabilities, ensure resilience and interaction.

PRIORITIES:

- *countering destructive influences (special information, information and psychological special operations) in the information space;*
- *improving the system of countering and responding to cyber incidents, cyber attacks, and cyber threats, including updating national legislation in the field of combating cybercrime;*
- *strengthening the capabilities of counterintelligence support in the field of electronic communications, IT sectors and their affiliated environment, conducting cyber intelligence, investigating cyber incidents and cyber attacks, acts of cyber espionage, cyber terrorism, and cyber sabotage;*
- *coordinating the activities of cybersecurity entities to counter cyber espionage, cyber terrorism, cyber sabotage and other cyber threats in the field of state security;*
- *improving the procedures for the use of electronic (digital) evidence in criminal proceedings, partial disclosure of data on information movement and the use of urgent storage of information aimed at the full implementation of the Convention on Cybercrime;*
- *developing and implementating modern cybersecurity tools and IT technologies in counterintelligence support of cybersecurity and information security of the state;*
- *introducing a system for verifying the readiness of critical infrastructure facilities to withstand possible cyber attacks and cyber incidents;*
- *expanding cooperation with foreign partners on investigations of cyber incidents, cyber attacks, cyber espionage and cyber terrorism, and holding offenders accountable.*

PROTECTING CRITICAL INFRASTRUCTURE AND SUPPLY CHAINS

The proper protection of critical infrastructure and supply chains is essential for the development and functioning of any state in the modern world. Disruption of critical infrastructure can threaten the stability of economic sectors and national security.

Counterintelligence support for the resilience of critical infrastructure, in particular energy, industry, transport systems, and other critical infrastructure facilities is a component of such protection.

Hostile and unfriendly countries are actively seeking information about critical infrastructure facilities, their protection and life support. They are interested in technologies and equipment, elements of assistance provided to Ukraine by partner countries, supply chains of such assistance and other critical goods, works and services.

Alongside the targeted destruction of critical infrastructure, attempts of industrial espionage, blocking foreign investment, sanction evasion, and reducing the competitiveness of Ukrainian products remain.

Together with other entities in the national critical infrastructure protection system, we must build a sustainable and effective system for detecting and countering threats to critical infrastructure and supply chains.

PRIORITIES:

- *enhancing the security and resilience of the national critical infrastructure;*
- *assisting in establishing response platforms for incidents affecting the critical infrastructure facilities, and improving existing interagency response systems;*
- *reducing terrorism and sabotage risks regarding critical infrastructure and supply chains by developing cooperation between the subjects of the national critical infrastructure protection system;*
- *counter-intelligence protection of innovations in the construction, operation and restoration of critical infrastructure.*

PROTECTION OF STATE SECRETS

Ukraine, like every other state, protects information leakage, which could harm national interests.

The importance of this activity has increased with the outbreak of hybrid and full-scale warfare.

Foreign intelligence services are actively conducting Humint Osint, legal and technical intelligence to obtain information, in particular, on the state's defence capability, the functioning of the defence industrial complex, energy and transport sectors, defence research and developments and their implementation, life support needs, foreign relations, including international technical cooperation.

We constantly monitor the intelligence activities of foreign intelligence services and their agents, and restrain the preconditions for leaking classified and sensitive information.

Protection of state secrets and classified information, as well as fulfilment of international obligations to protect such information, remain key areas of our activities.

PRIORITIES:

- *improving the system of counterintelligence support for the protection of state secrets and proprietary information processed in information and communication systems, taking into account NATO and EU security standards;*
- *improving the licensing procedure for activities related to state secrets, the procedure for granting and terminating access to state secrets to citizens, and the procedure for classifying information;*
- *adapting the system of restricted information protection to current threats to state security;*
- *introducing mechanisms for protecting information leakage and dissemination that could harm national interests.*

ANALYTICS

Timely and balanced decision-making by the leadership of the state and the Security Service of Ukraine depends on providing them with accurate, up-to-date analytical and information products.

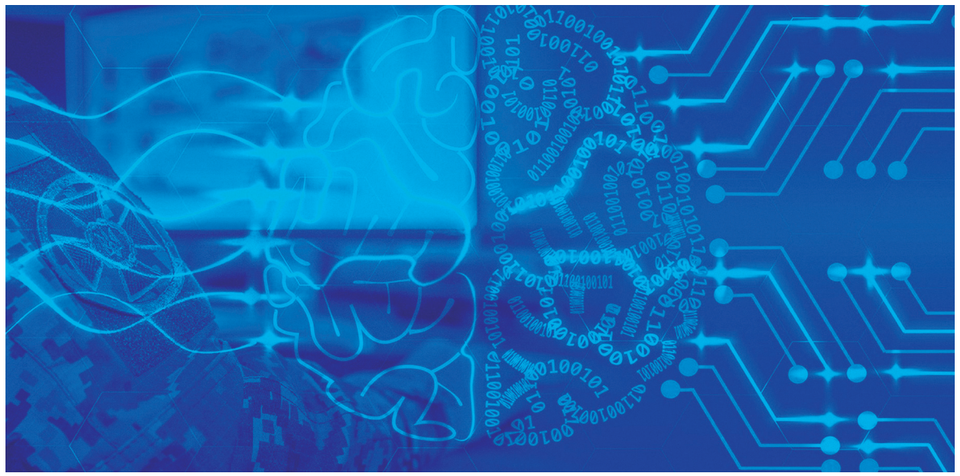
We constantly monitor the state of the security environment, investigate threats and risks to national security, and forecast possible developments.

To process and analyse information, we use modern tools and technologies that help us process large amounts of data faster and better, understand the scale and nature of threats, and ensure prompt response to them.

We actively implement the latest analytical intelligence methods and tools, including open source intelligence (OSINT), artificial intelligence and machine learning capabilities.

We should invest more in the development of information analytics.

In order to counter effectively threats in a fast-moving and multidimensional security environment, we should implement modern IT technologies and solutions. This will ensure a comprehensive strengthening of the SSU's capabilities to perform a full range of tasks.



PRIORITIES:

- *development of the technological component of information and analytical work, digitalisation of service processes, improvement of information and communication systems and other IT services, automation of procedures for obtaining (collecting), processing, analysing and displaying information;*
- *constant cooperation between the SSU analytical and operational components to enhance the ability to timely detect and respond to threats;*
- *introducing innovative methods of analytical intelligence and OSINT activities using artificial intelligence and machine learning tools;*
- *improving approaches and tools for monitoring and situational analysis of the operational situation, as well as interaction within the framework of situation centres of state authorities;*
- *continuous improvement of analysts professional competencies and their interaction with the expert community.*

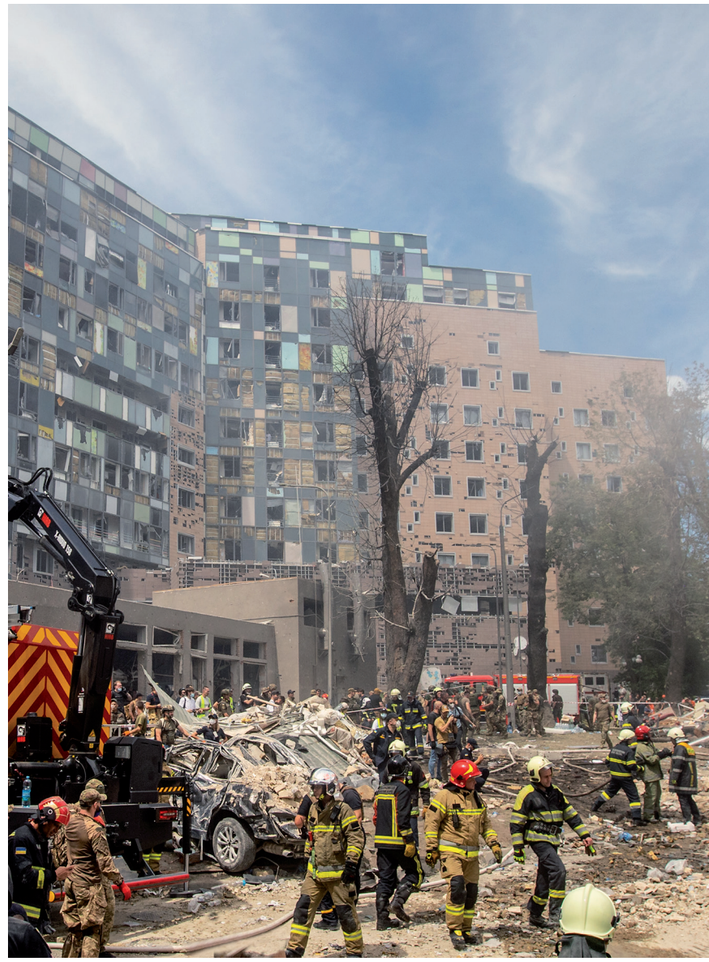
INVESTIGATION

Since the beginning of the russian hybrid war, we have faced new crimes that cause significant damage to state security.

The russian occupation forces and special services systematically commit a large number of crimes aimed at annihilating us as a nation and encroaching on the national security of Ukraine. The territories and settlements liberated from the temporary occupation of the invaders reveal to the world evidence of their cruel and inhuman crimes, including crimes of genocide, crimes against humanity, and war crimes.

Our activities are aimed at pre-trial investigation of crimes against the foundations of national and state security, crimes against peace, human security and international law and order, crimes in the field of state secrets, and terrorism.

Each fact of criminal activity is documented in detail in the interest of administration not only Ukrainian but also international justice. Both direct perpetrators of the crime and the military and political leadership of the aggressor state must be held accountable before the International Criminal Court.



PRIORITIES:

- *implementing information and communication systems in the pre-trial investigation process, the latest technologies and modern tools for collecting and preserving primary evidence from the scene;*
- *improving methods of collecting, processing, structuring and forensic analysis of evidence;*
- *improving the process of recording and using digital evidence in criminal proceedings;*
- *enhancing technical and forensic capacities to ensure effective pre-trial investigation;*
- *improving the legal framework for international cooperation in criminal justice between Ukraine and partner countries;*
- *ensuring mobile and autonomous activities of pre-trial investigation units in the combat zone, including creating conditions for proper and secure documentation of crimes committed in the temporarily occupied territories.*

SECTION 3
OUR GOALS AND OBJECTIVES

INSTITUTIONAL RESILIENCE

- delineation of powers with other components of Ukraine's security and defence sector;
- strengthening the role of the SSU as the sole national counterintelligence agency within the security and defence sector;
- further development of the SSU combat component as a part of the security and defence forces capable of employing all types of weapons, armaments, military and special equipment;
- enhancing coordination of counter-terrorism entities;
- improving the system for countering and responding to cyber threats, delineating tasks and powers among the subjects of the national cybersecurity system, investigating cyber incidents and cyber attacks, implementing modern cybersecurity tools and IT technologies, and creating tools for the SSU's cyber capabilities;
- strengthening the counterintelligence component in protecting national critical infrastructure and supply chains, as well as improving coordination and interaction among authorised entities;
- improving forms and methods of analytical risks and threats forecasting to national and state security, and planning countermeasures;
- creating an effective system of legal regulation for ensuring state security, considering geopolitical changes;
- implementing a flexible and adaptive structure of the SSU and risk-oriented approaches;
- achieving a balanced combination of democratic civilian oversight and accountability, internal control, and adherence to integrity principles;
- implementing a strategic management system;
- determining capabilities and needs in accordance with the SSU's functions and tasks in peacetime and for a special period.

OPERATIONAL PROCESSES

- developing an internal communications system and effective interaction among employees and departments at horizontal levels including;
- unifying and standardizing the main service activities;
- improving operational combat processes and tools used by of the SSU units;
- modernizing forms, methods and means used to perform the tasks, functions and exercise powers of the Service;
- updating the mechanisms and tools for monitoring the security environment, identifying threats and assessing national security risks, and responding to them;
- implementing advanced algorithms for logistics and other types of support.

HUMAN RESOURCES

- implementing transparent human resources management in line with gender equality principles, whereby recruitment and promotions are based on their professional competencies and integrity;
- modernising departmental education according to current needs of the SSU;
- ensuring personnel adaptation to changes in the security environment through continuous training and professional competencies development, including English as a tool for international communication;
- creating a reserve of military-trained human resources, ensuring their training, accumulation and maintenance;
- developing a system for monitoring personnel efficiency, creating conditions for motivation and career planning;
- developing corporate culture, professional ethics and integrity;
- increasing the level of social and legal protection, financial support for personnel, medical care for employees and family members, as well as veterans;
- reintegration into civilian life of servicemen who are to be discharged from military service.

INFRASTRUCTURE AND TECHNOLOGY

- developing and implementing new management and protection tools supporting innovations in the field of armaments and equipment;
- digital transformation and modernisation of technological infrastructure, introducing modern IT technologies and solutions in the processes of collecting, processing and analysing information in priority areas of activity;
- building a single secure information space using advanced security technologies;
- improving the system of technical protection of information, implementing new e-communication and special communication tools;
- ensuring fail-safe operation and use of information and communication systems, registers, data bases, reference resources and other IT services.

COORDINATION, INTERACTION AND PARTNERSHIP

- improving interaction mechanisms between the SSU and other security and defence sector components, other state bodies, local self-government bodies, enterprises, institutions and organisations;
- cooperation with citizens and their associations based on trust in the interests of jointly ensuring national security and national interests;
- training personnel of Ukraine`s security and defence sector in national security issues;
- preparing the population for actions in conditions of terrorist threats;
- expanding cooperation with the special services and law enforcement agencies of other countries and the security structures of international organisations.

SECTION 4-5

EXPECTED RESULTS

AS A RESULT OF IMPLEMENTATION OF THE STRATEGY, THE SECURITY SERVICE OF UKRAINE WILL BECOME:

a modern and effective national special service focused on performing tasks in the following areas: counterintelligence; special and combat missions; protection of national statehood; counterterrorism and countering its financing; counterintelligence support for information security and cyber security of the state; counterintelligence support for critical infrastructure and supply chains, as well as defence, and scientific and technical potential; protection of state secrets; information and analytical work; investigation of crimes within its competence;

the sole national counterintelligence agency that directs the activities of other entities ensuring state security;

an effective combat component of the security and defence forces with the functions, powers, modern tools and resources to timely detect and effectively respond to challenges and threats to state security;

an organization that applies risk-oriented approaches in its activities, forms an organisational staff structure taking into account the security situation and resources;

a body that uses modern strategic, external and internal communication systems, has an effective internal control system and implements anti-corruption programme;

a politically neutral and independent special service;

a trusted and authoritative institution within Ukrainian society;

an entity under transparent civilian democratic oversight;

a reliable international partner that effectively exchanges information and coordinates joint actions through established mechanisms of interaction between Ukraine and partner countries;

a service employing a modernized human resource management system.

Employees of the Security Service of Ukraine are professionals who are guided by the principles of integrity and professional ethics in their daily activities and are committed to protecting human and citizen rights and freedoms.

MECHANISM OF IMPLEMENTATION AND FINANCING OF THE STRATEGY

THE STRATEGY IS IMPLEMENTED THROUGH:

development and adoption of necessary legislative changes in the field of national security, state security, counterintelligence, counterterrorism, protection of state secrets, operational investigative activities (criminal intelligence), information security and cybersecurity of the state, electronic communications, information and protection of personal data, democratic civilian oversight, social and legal protection;

preparation and implementation of projects necessary to achieve the goals. Projects may be reviewed annually for updating.

The evaluation of the Strategy implementation includes ongoing monitoring and annual assessment of the success of the planned projects based on the defined indicators.

The main source of funding for the implementation of the Strategy is the State Budget of Ukraine, which allocates the expenditures for the proper functioning and sustainable development of the SSU. Additional sources of funding may also include international technical assistance and other sources not prohibited by law.

APPENDIX 1

LEGAL FRAMEWORK FOR SSU TRANSFORMATION

CONSTITUTION OF UKRAINE

CODES

- Criminal Code of Ukraine
- Criminal Procedure Code of Ukraine
- Code of Ukraine on Administrative Offences
- Code of Administrative Procedure of Ukraine

LAWS OF UKRAINE

- «On the Security Service of Ukraine»
- «On Counterintelligence Activities»
- «On Operational and Investigative Activities»
- «On the National Security of Ukraine»
- «On the Fight Against Terrorism»
- «On Critical Infrastructure»
- «On Intelligence»
- «On Ensuring the Rights and Freedoms of Citizens and the Legal Regime in the Temporarily Occupied Territory of Ukraine»
- «On Basic Principles of Ensuring Cybersecurity of Ukraine»
- «On State Secrets»
- «On Information»
- «On Access to Public Information»
- «On Citizens' Appeals»
- «On Protection of Personal Data»
- «On Protection of Information in Information and Communication Systems»
- «On Principles of Domestic and Foreign Policy»
- «On Prevention of Corruption»
- «On Sanctions»
- «On Electronic Communications»
- «On Forensic Examination»
- «On Ensuring the Safety of Persons Participating in Criminal Proceedings»
- «On the General Structure and Number of the Security Service of Ukraine»
- «On Social and Legal Protection of Servicemen and Members of Their Families»
- «On State Protection of Judicial and Law Enforcement Officers»
- «On the Organisational and Legal Framework for Combating Organised Crime»
- «On Military Duty and Military Service»
- «On Civil Service»
- «On the State Programme of Civil Aviation Security»

NATIONAL STRATEGIES/CONCEPTS

- Concept for Combating Terrorism in Ukraine (Decree of the President of Ukraine No. 53 of 05 March 2019)
- National Security Strategy of Ukraine (Decree of the President of Ukraine No. 392 of 14 September 2020)
- Strategy for Combating Organised Crime (Order of the Cabinet of Ministers of Ukraine of 16 September 2020 No. 1126-r)
- Cybersecurity Strategy of Ukraine (Decree of the President of Ukraine of 26 August 2021 No. 447)
- Strategic Defence Bulletin of Ukraine (Decree of the President of Ukraine of 17 September 2021 No. 473/2021)
- Concept for Ensuring the National Resilience System (Decree of the President of Ukraine of 27 September 2021 No. 479)
- Information Security Strategy (Decree of the President of Ukraine of 28 December 2021 № 685)
- Strategy for Ensuring State Security (Decree of the President of Ukraine No. 56 of 16 February 2022)
- Communication Strategy for Ukraine's European Integration for the period up to 2026 (Resolution of the Cabinet of Ministers of Ukraine of 09 December 2022 No. 1155-r)
- Communication Strategy for Preventing and Combating Corruption for the period up to 2025 (Resolution of the Cabinet of Ministers of Ukraine of 22 December 2023 No. 1203-r)
- Maritime Security Strategy of Ukraine (Decree of the President of Ukraine of 17 July 2024 No. 468)
- Strategy for the Formation of a System for Returning from Military Service to Civilian Life for the period up to 2033 (Resolution of the Cabinet of Ministers of Ukraine of 31 December 2024 No. 1350-r)

AGREEMENTS ON SECURITY COOPERATION AND LONG-TERM SUPPORT BETWEEN UKRAINE, FOREIGN STATES AND INTERNATIONAL ORGANISATIONS

EU–UKRAINE POLICY DOCUMENTS

- Roadmap for the Rule of Law and Security sector
- Comprehensive Strategic Plan for the Reform of Law Enforcement Agencies as a Part of the Security and Defence Sector of Ukraine for 2023-2027 (Decree of the President of Ukraine of 11 May 2023 No. 273)
- Action Plan for the Implementation of the Comprehensive Strategic Plan for the Reform of Law Enforcement Agencies as a Part of the Security and Defence Sector of Ukraine for 2023-2027 (Order of the Cabinet of Ministers of Ukraine of 23 August 2024 No. 792-r)

NATO – UKRAINE POLICY DOCUMENTS

- Charter on a Distinctive Partnership between Ukraine and the North Atlantic Treaty Organisation (of 09 July 1997, Madrid))
- UKRAINE ADAPTED ANNUAL NATIONAL PROGRAMME ASSESSMENT FOR 2024.
- NATO Strategic Concept 2022 (adopted by Heads of State and Government at the NATO Summit in Madrid on 29 June 2022)
- NATO-Ukraine Interoperability Roadmap
- NATO Interoperability Requirements

E-VERSION OF THE STRATEGY:

SECURITY SERVICE OF UKRAINE