



SECURITY SERVICE OF UKRAINE

ANNUAL REPORT 2025



CONTENTS

Foreword by the Acting Head of the Security Service of Ukraine	3
Chapter 1. General Information and Legal Framework	5
Chapter 2. Strategic Priorities and Institutional Transformation	7
Chapter 3. Operational Results	10
Chapter 4. Human Resources Management and Integrity Assurance	49
Chapter 5. Accountability, Transparency and Resource Support	50
Chapter 6. International Cooperation	53
Contact Information	63



FOREWORD BY THE ACTING HEAD OF THE SECURITY SERVICE OF UKRAINE

DEAR UKRAINIANS, COLLEAGUES AND FRIENDS,

Protecting the state and its citizens is the core mission of the Security Service of Ukraine. Now in the fifth year of Russia's full-scale invasion, Ukraine is not only holding the line but also delivering powerful and effective responses to the aggressor.

The SSU fights the enemy in all directions of this war. Every day we counter the activities of the Russian intelligence services, their agents and sabotage groups. Today, counterintelligence constitutes one of the key pillars of Ukraine's national defence. We act proactively, systematically disrupting and defeating the enemy's plans. During 2025, the Security Service of Ukraine initiated more than 1,000 criminal proceedings for high treason and over 1,670 proceedings related to collaboration activities. These figures clearly illustrate the scale of the threats facing Ukraine.

Russian sabotage and terrorist activities remain another critical challenge confronting the SSU. Terror has become an integral part of Russia's state policy. Our officers continuously prevent assassination attempts against Ukrainian military personnel and civilians while disrupting enemy efforts aimed at destabilising the internal situation in Ukraine.

We are equally engaged across the information, cyber and sanctions domains. Around the clock, we counter Russian information and psychological operations, repel cyberattacks against national information systems, prevent the aggressor from circumventing international sanctions, and document war crimes to ensure that every perpetrator is ultimately brought to justice.

At the same time, the SSU is, above all, a wartime security service operating in a nation at war. We conduct operations at tactical, operational and strategic levels. Owing to the actions of SSU personnel, 'bavovna' keeps striking deep inside the Russian rear. During 2025 alone, the Service successfully carried out more than 250 long-range strike operations, inflicting losses estimated at USD 9 billion. These sustained operations, conducted thousands of kilometres from the frontline, demonstrate that no location within Russia can any longer be considered secure.

Along the line of contact, our personnel operate continuously, twenty-four hours a day, eliminating enemy manpower in dozens of thousands on a large scale. Enemy military equipment remains another priority target. During the past year, fighters of the Special Operations Centre 'Alfa' and other SSU units destroyed 758 tanks, 2,414 artillery systems, 134 multiple-launch rocket systems, 455 air defence systems, together with hundreds of other items of military equipment. The enemy continues to suffer substantial losses, while its ability to generate additional resources to sustain its aggression is steadily diminishing.

I extend my sincere gratitude to every officer of the Security Service of Ukraine for their professionalism, resilience and unwavering dedication to defending our country. Over these years, the Service has acquired unparalleled operational, counterintelligence, combat and technological experience. Today, together with Ukrainian society and our international partners, we are transforming this experience into a new highly effective model of state security.

Our resistance continues for the sake of peace.

GLORY TO UKRAINE!

Major General
Yevgeniy Khmara
Acting Head of the SSU

A handwritten signature in blue ink, likely of Major General Yevgeniy Khmara, written over a white background.



GENERAL INFORMATION AND LEGAL FRAMEWORK

VISION:

We are an effective security service of a strong Ukraine trusted by Ukrainian society, and a reliable partner in defending democracy.

MISSION:

- ◆ We protect the Ukrainian people and the national interests of Ukraine;
- ◆ We uphold the constitutional order and ensure state security;
- ◆ We create conditions for our state's strategic advantage 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 intelligence services of partner nations;
- ◆ Corporate unity.

1.1. REGULATORY AND LEGAL FRAMEWORK

THE SECURITY SERVICE OF UKRAINE IS A STATE SPECIAL-PURPOSE BODY WITH LAW ENFORCEMENT FUNCTIONS, WHICH ENSURES THE STATE SECURITY OF UKRAINE (ART. 1 OF THE LAW OF UKRAINE 'ON THE SECURITY SERVICE OF UKRAINE').

THE LEGAL BASIS FOR THE SERVICE'S ACTIVITIES COMPRISES:

The Constitution of Ukraine;
The Criminal Code of Ukraine;
The Criminal Procedure Code of Ukraine;

Laws of Ukraine:

- ◆ 'On the National Security of Ukraine';
- ◆ 'On the Security Service of Ukraine';
- ◆ 'On the General Structure and Personnel Strength of the Security Service of Ukraine';
- ◆ 'On Counterintelligence Activity';
- ◆ 'On Investigative and Operational Activity';
- ◆ 'On the Fight Against Terrorism';
- ◆ 'On State Secrets';
- ◆ 'On the Basic Principles of Ensuring Cybersecurity of Ukraine';
- ◆ 'On Critical Infrastructure';
- ◆ other legislative acts defining the powers of the SSU.

Acts of the Security Service of Ukraine, etc.

For a more detailed overview of the regulatory framework, please visit the link: (<https://ssu.gov.ua/zakonodavstvo>)

1.2. STATUTORY MANDATE AND FUNCTIONS

STATUTORY MANDATE OF THE SSU IS PURSUANT TO ARTICLE 2 OF THE LAW OF UKRAINE 'ON THE SECURITY SERVICE OF UKRAINE':

- ◆ Protecting state sovereignty, the constitutional order, and territorial integrity;
- ◆ Safeguarding the scientific, technological, and defence potential of Ukraine;
- ◆ Shielding the legitimate interests of the state and the rights of citizens from hostile intelligence and subversive operations conducted by foreign intelligence agencies, as well as from threats posed by individual entities, groups, and organisations;
- ◆ Ensuring the protection of state secrets;
- ◆ Preventing, detecting, disrupting, and investigating crimes against peace and security of mankind, acts of terrorism, and other unlawful activities that pose a direct threat to the vital interests of Ukraine.

CHAPTER 2 STRATEGIC PRIORITIES AND INSTITUTIONAL TRANSFORMATION

The functions of the SSU are pursuant to Article 19 of the Law of Ukraine 'On the National Security of Ukraine':

- ◆ Countering hostile intelligence and subversive operations targeting Ukraine;
- ◆ Fighting against terrorism;
- ◆ Providing counterintelligence security for state sovereignty, constitutional order, territorial integrity, defence capabilities, scientific and technological potential, cybersecurity, state information security, and critical infrastructure assets;
- ◆ Protecting state secrets.

1.3. ORGANISATIONAL STRUCTURE

THE ORGANISATIONAL STRUCTURE OF THE SECURITY SERVICE OF UKRAINE IS DETERMINED BY THE LAW OF UKRAINE 'ON THE GENERAL STRUCTURE AND PERSONNEL STRENGTH OF THE SECURITY SERVICE OF UKRAINE' AND THE DECREE OF THE PRESIDENT OF UKRAINE NO. 1860/2005 DATED 27 DECEMBER 2005.

THE SSU CONSISTS OF:

- ◆ The Central Directorate of the Security Service of Ukraine;
- ◆ Regional bodies subordinated thereto;
- ◆ Military counterintelligence bodies;
- ◆ Educational, scientific, research, and other institutions, establishments, organisations, and enterprises of the Security Service of Ukraine.

TO ENSURE THE EFFECTIVE PERFORMANCE OF THE STATUTORY MANDATE ASSIGNED TO THE SECURITY SERVICE OF UKRAINE, THE FOLLOWING FUNCTIONAL DEPARTMENTS OPERATE WITHIN THE STRUCTURE OF THE SSU CENTRAL DIRECTORATE AND ITS SUBORDINATED BODIES:

- ◆ Counterintelligence;
- ◆ Protection of national statehood;
- ◆ Counterintelligence protection of state interests in the information security domain;
- ◆ Operational combat activities and special operations ('Alfa' Special Operations Centre);
- ◆ Pre-trial Investigation;
- ◆ Protection of state secrets;
- ◆ Operational and technical activities;
- ◆ Operational documentation;
- ◆ Special communications;
- ◆ Organisational, information and analytical, human resources, legal affairs, logistics, financial, and other support for the SSU's operational and service activities.

THE ANTI-TERRORIST CENTRE OPERATES AT THE SECURITY SERVICE OF UKRAINE.

2.1. STRATEGIC COURSE AND PRIORITIES OF THE SSU ACTIVITY

THE SECURITY SERVICE OF UKRAINE HAS ADOPTED A DEVELOPMENT STRATEGY FOR 2025-2030 AIMED AT INSTITUTIONAL DEVELOPMENT, MODERNISATION, AND TRANSFORMATION OF THE SERVICE INTO A SINGLE NATIONAL COUNTERINTELLIGENCE AGENCY CAPABLE OF PROMPTLY AND EFFECTIVELY COUNTERING EXTERNAL AND INTERNAL THREATS TO STATE SECURITY.

THIS DOCUMENT WAS DEVELOPED IN ALIGNMENT WITH KEY STRATEGIC AND POLICY PAPERS IN THE SPHERE OF NATIONAL AND STATE SECURITY, AS WELL AS THE REFORM ROADMAPS FOR THE SECURITY AND DEFENCE SECTOR. IT SPECIFICALLY INCORPORATES OBJECTIVES PURSUANT TO UKRAINE'S EUROPEAN AND EURO-ATLANTIC INTEGRATION COURSE.

FURTHERMORE, THE STRATEGY LEVERAGES EXPERIENCE GAINED IN COUNTERING RUSSIAN HYBRID AND ARMED AGGRESSION, ACCOUNTING FOR EVOLVING THREAT LANDSCAPES, ADVANCEMENTS IN MILITARY AND DIGITAL TECHNOLOGIES, AND CURRENT EU AND NATO STANDARDS.

PRIORITY AREAS OF THE SSU'S ACTIVITY:

- ◆ Executing counterintelligence operational activities;
- ◆ Conducting special and combat missions;
- ◆ Safeguarding national statehood;
- ◆ Combating terrorism and disrupting terrorist financing;
- ◆ Ensuring state information and cybersecurity;
- ◆ Providing counterintelligence protection of critical infrastructure, defence capabilities, scientific and technological potential;
- ◆ Protecting state secrets;
- ◆ Information and analytical activities;
- ◆ Conducting pre-trial investigations of crimes within the SSU jurisdiction.
- ◆ Implements digital transformation of processes and implements risk-oriented threat response methods;
- ◆ Improves personnel management, logistics, and resource management;
- ◆ Expands cooperation with international partners and other components of the security and defence sector.

The practical execution of the Strategy is carried out in accordance with its Implementation Plan. It defines the core objectives and key performance indicators for evaluating results, alongside specific measures executed by the SSU across key areas of its operational activities.

The overarching goal is to reinforce the capabilities of the Security Service of Ukraine during wartime and in the face of contemporary security threats. The effectiveness of this work is highlighted in the subsequent chapters of the Report.

Based on the defined priorities, the SSU:

- ◆ Strengthens its operational, combat, counterintelligence, and analytical capabilities;
- ◆ Advances modern technological solutions and military innovations;
- ◆ Develops unmanned, reconnaissance-strike, and information and analytical systems;
- ◆ Enhances capabilities in the fields of information and cybersecurity, as well as the counterintelligence protection of critical infrastructure;

2.2. INSTITUTIONAL TRANSFORMATION AND IMPLEMENTATION OF REFORMS

The actual process of reforming the Security Service of Ukraine began back in 2018 with the enactment of the Law of Ukraine 'On the National Security of Ukraine'. This document laid the foundation

for the SSU's transformation, anchoring its status as a special-purpose state body with law enforcement functions tasked with ensuring the state security of Ukraine. Furthermore, it envisages the development of new legislation governing the SSU.

The Security Service of Ukraine is engaged in systematic efforts to enhance the regulatory and legal framework of its operations and the mechanisms for ensuring state security. At the same time, the comprehensive update of legislation in the SSU's sphere of activity has not yet been fully completed, which necessitates the continuation of transformation processes within the framework of strategic and policy documents.

The transformation of the SSU is carried out in alignment with Ukraine's Euro-Atlantic and European integration course. The core principles and directions for reforming the Service are defined in the following strategic and policy documents:

- ◆ The Comprehensive Strategic Plan for the Reform of Law Enforcement Agencies as Part of the Security and Defence Sector of Ukraine for 2023–2027, along with the Government Action Plan for its implementation;
- ◆ The Rule of Law Roadmap;
- ◆ The Ukraine-NATO Interoperability Roadmap under the NATO Comprehensive Assistance Package for Ukraine;
- ◆ The Strategy for the Development of the Security Service of Ukraine for 2025–2030.

These documents establish the strategic directions of the SSU further renewal. Notably, they aim to reinforce the Service's capabilities in the sphere of state security, evolve key operational domains, advance democratic civilian oversight, drive digital transformation, and implement modernised human resources management strategies. The framework furthermore prescribes the institutionalisation of intelligence-led approaches and risk-oriented operational models within day-to-day practices.

Additionally, in 2025, the Verkhovna Rada of Ukraine enacted a series of regulatory and legal acts developed with the participation of the SSU. These statutes are designed to bolster the special

service's multi-directional capabilities under the current ruling martial law regime. Specifically, these include the following Laws of Ukraine:

'On Amendments to Article 8 of the Law of Ukraine 'On State Secrets' dated 12 February 2025, No. 4236-IX.

This Act stipulates, inter alia, the classification of information pertaining to the organisation, scope, requisite status, and protection blueprints of critical infrastructure objectives (CIOs) as state secrets. In particular, data regarding the establishment of comprehensive strategic resource reserves designed for crisis response and post-disaster mitigation at CIOs has been accorded classified status.

'On Amendments to Certain Laws of Ukraine Concerning Information Protection and Cyber Defence of State Information Resources and Critical Information Infrastructure Objects' dated 27 March 2025, No. 4336-IX

The nationwide cybersecurity system has been reinforced. The amendments clarify objectives regarding the fight against cyberterrorism, cybersabotage, and cyberespionage. The Cybersecurity Situation Centre of the Security Service of Ukraine has been designated as an integral component of the national response system for cyber incidents, cyberattacks, and cyber threats. The SSU has been authorized to develop and implement sectoral and/or targeted security profiles for information, electronic communication, and information-communication systems.

'On Amendments to Certain Laws of Ukraine Concerning the Improvement of Particular Aspects of the Activities of the Security Service of Ukraine and Enhancing Its Efficiency in Connection with Its Participation in Repelling and Detering Armed Aggression Against Ukraine' dated 16 July 2025, No. 4542-IX

The personnel strength of the SSU Special Operations Centre 'A' ('Alfa') has been increased to 10,000 service members. The SSU's legal authority to deploy and use weapons, combat hardware, as well as all types of unmanned systems, has been specified in detail.

'On Amendments to Certain Laws of Ukraine Concerning the Improvement of the Procedure for Submitting Draft Regulatory Acts on Matters Within the Competence of the Security Service of Ukraine for Consideration by the President of Ukraine and the Cabinet of Ministers of Ukraine' dated 9 October 2025, No. 4633-IX

The powers of the SSU regarding the development and submission of draft regulatory acts on matters within its competence (e.g., in the areas of state secrets protection, counterterrorism, etc.) for consideration by the President of Ukraine and the Cabinet of Ministers of Ukraine have been clarified.

Furthermore, the National Academy of Legal Sciences of Ukraine conducted a 'Review of the Legislation of Ukraine Defining the Powers of the Security Service of Ukraine'. This work is mandated by the requirements of the Rule of Law Roadmap. Its objective is to focus the SSU's activities specifically on ensuring the national security of Ukraine.

During this process, the Ukrainian side analysed the legislation governing the activities of intelligence and security services in NATO and EU member states, and researched international experience to guide the further development of the Service.

Throughout the year, the Security Service developed and implemented a series of regulatory and organisational solutions aimed at enhancing its capabilities under martial law. Specifically:

◆ IN THE FIELD OF PERSONNEL POLICY AND STAFF MANAGEMENT:

- ◆ The Procedure for Conducting the Assessment of Military Servicemen of the Security Service of Ukraine and the Guidelines on its Organisation;
- ◆ The Regulation on Professional Training in the SSU;
- ◆ The Regulation on the Continuous Professional Development of Military Servicemen of the Security Service of Ukraine;

◆ WITHIN THE FRAMEWORK OF IMPROVING THE INTERNAL CONTROL AND ANTI-CORRUPTION SYSTEM:

- ◆ The Anti-Corruption Program of the SSU for 2025–2027;

◆ IN THE DIRECTION OF DIGITAL CAPABILITIES DEVELOPMENT AND INFORMATION PROTECTION MECHANISMS ENHANCEMENT:

- ◆ The Digital Transformation Strategy of the Security Service of Ukraine;
- ◆ The Procedure for Processing and Protecting Personal Data within the Security Service of Ukraine;

◆ IN THE FIELD OF FIGHT AGAINST TERRORISM:

- ◆ The Procedure for Compiling and Maintaining the List of Terrorist Organisations and Groups.

THE SSU HAS ALSO:

- ◆ Drafted a new edition of the Concept for Fighting Against Terrorism in Ukraine (approved by the Decree of the President of Ukraine dated 11 June 2026, No. 492/2026);
- ◆ Initiated the modernisation of the professional training system for representatives of state authorities, local self-government bodies, and the civil sector on issues of fighting against terrorism, as well as their involvement in counter-terrorism exercises, specifically hosted by the National Academy of the Security Service of Ukraine.

Further comprehensive updates to the legislation governing the activities of the SSU are directly linked to the adoption of the Law of Ukraine 'On Law Enforcement Agencies' and the Law of Ukraine 'On Criminal Intelligence'. These documents are intended to define the system of law enforcement agencies, the criteria for their delineation, and the clear separation of criminal intelligence from criminal proceedings, intelligence, and counterintelligence activities.

Following the establishment of this foundational legislative framework, alongside the renewing of legislation in the fields of counterintelligence activities and state secrets protection, the SSU will promptly submit proposals to refine the Law of Ukraine 'On the Security Service of Ukraine'.

CHAPTER 3

OPERATIONAL RESULTS



COUNTERINTELLIGENCE ACTIVITIES AND COUNTERING INTERNAL THREATS TO STATE SECURITY

COUNTERINTELLIGENCE ACTIVITIES ARE A FOUNDATIONAL COMPONENT OF STATE SECURITY, PARTICULARLY UNDER THE CONDITIONS OF THE RUSSIAN FEDERATION'S FULL-SCALE AGGRESSION. COUNTERINTELLIGENCE ENABLES NOT ONLY TO RESPOND TO THREATS BUT ALSO PREVENTIVELY TO IDENTIFY AND NEUTRALISE THEM AT THE PREPARATION STAGE. ITS EFFICIENCY DIRECTLY IMPACTS THE RESILIENCE OF STATE INSTITUTIONS, THE PROTECTION OF INFRASTRUCTURE AND CRITICAL INFORMATION, AND THE PRESERVATION OF NATIONAL SOVEREIGNTY.

The contemporary security environment is characterized by the constant transformation of the adversary's forms and methods of intelligence-subversive activities. The enemy actively adapts its approaches: altering communication channels, utilising cutting-edge technologies, disguising intelligence assets as citizens of third states, and employing complex, multi-tiered recruitment and influence schemes.

Concurrently, SSU counterintelligence operates proactively, functioning in a mode of continuous mobilisation of forces and assets, and maintaining a high level of readiness for new challenges. It systematically updates its operational tools, implements modern countermeasures, and takes pre-emptive action, striving to remain one step ahead.

A significant portion of counterintelligence activities remains non-public due to the necessity to safeguard operational methods and sources of information; however, the results are of critical importance to state security.

Today, SSU counterintelligence counters a broad spectrum of threats ranging from classic manifestations of intelligence-subversive activities (detecting spies, traitors, collaborators, and accomplices of the aggressor state) to complex hybrid threats that combine information operations, cyber operations, and human intelligence activities.

In 2025, the nature of threats to Ukraine's state security remained unchanged and was primarily characterised by the active operations of the Russian intelligence services. Their efforts were aimed at undermining the constitutional order, weakening defence and economic potential, causing internal destabilisation, and degrading the state's resilience to aggression.

The scale of these threats is evidenced by the results of the SSU's operations in detecting and documenting criminal activities that threaten state security. The number of initiated criminal proceedings indicates the high intensity of the adversary's activities, while simultaneously demonstrating the systematic efforts of the Ukrainian security service to counter such manifestations.

Specifically, during 2025, based on materials provided by SSU units, pre-trial investigations were initiated regarding the commission of crimes stipulated by:

Article 111 (High Treason) of the CC of Ukraine – **1 091 criminal proceedings**;

Article 111-1 (Collaborative Activity) of the CC of Ukraine – **1 671 criminal proceedings**;

Article 111-2 (Assisting the Aggressor State) of the CC of Ukraine – **350 criminal proceedings**;

Article 114 (Espionage) of the CC of Ukraine – **9 criminal proceedings**.



► **The SSU Counterintelligence apprehended fsb agents** who supplied the ruscists with Ukrainian SIM cards for kamikaze drones. Those microchips improved the connectivity and navigation of russian unmanned aerial vehicles during attacks on our state. SSU investigators served the detainees with notices of suspicion under Article 111 of the CC of Ukraine (High Treason).

► **The SSU exposed and documented a belarusian kgb agent** who was gathering intelligence on the defence of Ukraine's northern borderlands. The perpetrator recorded the locations of checkpoints, fortifications, and the movement routes of the Defence Forces, transmitting this data to the foreign intelligence service. The 24-year-old resident of the Volyn region was sentenced to 15 years of imprisonment for high treason (Article 111 of the CC of Ukraine) committed under martial law.

Human intelligence penetration remains one of the adversary's key tools for executing subversive activities. Acting systematically, in an organised and coordinated manner, the adversary utilises both individual agents and extensive spy networks. The efficiency of the SSU's countermeasures against such threats

is evidenced by the operational results in exposing the adversary's intelligence apparatus and ensuring its timely elimination. Specifically, over the past year, the Service's personnel exposed 36 russian spy networks, which comprised 152 individuals.

► **In the Zakarpattia region, counterintelligence eliminated a spy network of the Hungarian Military Counterintelligence, consisting of Ukrainian citizens.** In exchange for financial remuneration, the traitors gathered and transmitted data regarding the region's military defences, local socio-political sentiments, and the potential reaction of the population in the event of a Hungarian troop deployment to the area. Due to their involvement in intelligence activities on the territory of Ukraine, two Hungarian diplomats were declared personae non gratae and recalled early from Ukraine.

► **The SSU exposed a spy network of russian military intelligence in Zaporizhzhia, which was coordinated by a priest of the UOC (MP).** According to the case files, the cleric searched for pro-russian residents during his sermons. Subsequently, he began recruiting potential candidates into the aggressor country's intelligence apparatus.

It was established that the parish rector recruited a 41-year-old mobilised individual who transmitted data on AF units to the enemy. Furthermore, a russian passport, ammunition for a Kalashnikov assault rifle, and bladed weapons were found in the cleric's possession.

The domestic defence-industrial complex, military-related information, and infrastructure facilities critically vital to the defence of Ukraine remain targeted by foreign intelligence services. The adversary aims to acquire data regarding the deployment and capabilities of the Defence Forces of Ukraine, the execution of defence contracts, and cutting-edge developments in the field of weaponry.

The SSU systematically counters attempts by foreign intelligence services to penetrate the defence sector, exposes intelligence networks, disrupts leakage channels of sensitive information, and ensures the counterintelligence protection of defence-industrial complex enterprises.

► **In Mykolaiv, the SSU exposed a pair of russian intelligence assets attempting to acquire data regarding a defence enterprise.** The female asset was recruited by russian intelligence services, and she involved her cohabitant, a factory employee, in the information gathering process, who subsequently transmitted data on defence-industrial complex facilities and the execution of state defence orders. The suspects were apprehended at the initial stage. Evidence of communication with their 'handler' - Serhii Lebediev (known under the pseudonym 'Lokhmatyi'), who operates for the fsb and russian military intelligence in Donetsk - was seized.

► **The SSU Counterintelligence apprehended an FSB agent - a citizen of a Middle East country** who was gathering intelligence for the enemy regarding the energy infrastructure of the Zhytomyr and Khmelnytskyi regions, specifically in the vicinity of the Khmelnytskyi Nuclear Power Plant. The perpetrator photographed energy facilities and Defence Forces checkpoints

to facilitate targeting missile and drone strikes. The suspect was served with a notice of suspicion under the articles concerning the preparation of sabotage and unauthorized dissemination of information regarding the deployment of military formations. The individual faces life imprisonment.

Assassination attempts against Ukraine's top military and political leadership, as well as public figures and activists, remain a distinct vector of the enemy's subversive activities. These actions aim to destabilise the socio-political situation, demoralise the population, and undermine the capabilities of the security and defence sector.

The SSU systematically conducts activities aimed at the timely detection and elimination of relevant threats, demonstrating the effectiveness of preventive counterintelligence measures and the ability to act pre-emptively to disrupt the execution of hostile intentions. Specifically, the SSU has repeatedly thwarted assassination attempts targeting top military and political leadership, public figures, and community activists.

► **In May, officers of the Security Service detained a 45-year-old native of the Odesa region** residing in the capital. She had been remotely recruited by russian intelligence services while seeking 'easy money' on the internet. As volunteer Serhii Sternenko was leaving his building, the russian agent fired several shots, hitting him in the leg with one of the bullets. The assailant was instantly detained on the spot by officers of the Security Service of Ukraine..

The SSU's counterintelligence work is a constant confrontation with a wide spectrum of threats – ranging from conventional to complex hybrid manifestations. Its outcomes are measured not only by detained agents and disrupted enemy special operations, but also by the saved lives of individuals whom russia attempted to target. This defines counterintelligence as one of the key tools for ensuring state resilience and protecting national interests.



COUNTERING TERRORISM AND SABOTAGE, PROTECTING CRITICAL INFRASTRUCTURE

THE YEAR 2025 IS CHARACTERISED BY AN INCREASE IN THE INTENSITY OF SABOTAGE AND TERRORIST ACTIVITY. AS EARLY AS 2023, PUTIN APPROVED THE SO-CALLED 'SABOTAGE NOISE' PLAN. ITS CORE OBJECTIVE IS TO SCALE UP AND INCREASE THE NUMBER OF SABOTAGE ACTS, TERRORIST ATTACKS, AND ARSON INCIDENTS ACROSS UKRAINE. THROUGH THESE MEANS, THE OCCUPIERS ARE ATTEMPTING TO 'DESTABILISE' THE SITUATION IN OUR COUNTRY.

In 2025, the number of sabotage and terrorist incidents increased by nearly a third compared to the previous year, totalling 870 cases. However, the Security Service of Ukraine acts pre-emptively, systematically exposing russian agents planning terrorist attacks and sabotage at early stages, eliminating suspicious activity, and employing advanced counterintelligence tools. Thanks to the coordinated and targeted efforts of its operational units, the security service successfully thwarted 262 sabotage and terrorist plots during their preparation stage in 2025, 164 of which involved the planned use of improvised explosive devices (IED).

► **The SSU Counterintelligence and investigators prevented a large-scale terrorist attack on one of Kyiv's central crowded streets.** A female russian agent was preparing to detonate explosives near the building of SSU structural unit. Upon apprehension, a bag was seized from the suspect containing an IED with an explosive yield equivalent to 7 kg of TNT. A charge of this magnitude is sufficient to inflict severe structural damage on a building and cause mass fatalities among individuals near the blast epicentre.

► **The SSU Counterintelligence prevented another terrorist attack orchestrated by russian intelligence services in the city of Kyiv.** A female suspect who attempted to detonate explosives in a

cafe in the very centre of Ukraine's capital was apprehended. To commit the crime, she planned to leave two improvised explosive devices (IEDs) inside the coffee shop, with a total yield of nearly 1.5 kg in TNT equivalent. According to the case files, russian intelligence officers planned to remotely detonate both IEDs during the evening rush hour to maximise casualties.

Socio-economically vulnerable segments of the population (individuals in debt, persons suffering from drug or gambling addictions, etc.) most frequently become potential perpetrators of terrorist attacks and sabotage. A distinct demographic group of population that Russia actively attempts to recruit is minors. They are easier to manipulate, as they do not always fully realize the consequences of their actions. Teenagers often perceive tasks from the enemy as games or quests, and the occupiers also offer them financial remuneration. Frequently, they are used blindly. The SSU has documented instances where the tactic of detonating the perpetrators of terrorist attacks themselves was employed.

► **On 11 March 2025, in the centre of Ivano-Frankivsk,** the russian intelligence service detonated two assets who were carrying improvised explosive device (IED) near to the railway station. As the investigation established, the enemy's accomplices turned out to be two local



minors, aged 15 and 17, recruited by Russia through Telegram channels looking for 'easy money' and entangled in criminal activity. As a result of the incident, the 17-year-old perpetrator died on the spot, while his 15-year-old accomplice was hospitalised with severe injuries.

Recruitment primarily occurs remotely, utilising online platforms commonly used by Ukrainians: Telegram, TikTok, Instagram, other messengers, social networks, online games, etc. In this context, the priority of the SSU's activities is the timely detection and elimination of such threats. The Service constantly improves the response of operational teams and implements new standards of coordination on the ground, which significantly reduce the response time to potential threats, execute a complex of preventive measures at the regional level, develop a system of public engagement, and deepen cooperation with local self-government bodies.

A vital direction of SSU activities during the war remains the protection of critical infrastructure objects (CIOs) and state strategic resources, as their functioning is crucial to the resilience of the economy and the continuity of life support systems for the population. The primary targets of the enemy's sabotage activities are energy facilities, transport hubs, communication systems, defence-industrial complex

enterprises, as well as military logistics sites, including warehouses, supply bases, and other elements of critical infrastructure. Specifically, hostile intelligence services systematically attempt to inflict damage to railway infrastructure, destruction of which disrupts the supply chains of humanitarian and military cargo, negatively impacting the functioning of the state as a whole.

► **The SSU and the National Police apprehended 13 arsonists who were executing tasks for the FSB. As a result of comprehensive operations conducted in Kyiv, as well as in the Kyiv, Odesa, Zaporizhzhia, and Vinnytsia regions, perpetrators were detained. At the behest of the enemy, they set fire to Ukrzaliznytsia (Ukrainian Railways) facilities and vehicles belonging to the Defence Forces, while certain suspects were preparing terrorist attacks. Evidence of crimes was discovered in possession of the suspects in all revealed facts.**

Ensuring the security of CIOs encompasses not only their physical protection and cybersecurity but also a counterintelligence component, which plays a decisive role in identifying and eliminating threats. In this context, SSU activities are directed, in particular, toward the timely exposure and elimination of networks of informants and spotters who transmit data on CIOs to the enemy.

Concurrently, an expansion of financing instruments for subversive activities has been observed. Alongside traditional means, the enemy is increasingly utilising virtual assets. The Russian intelligence services deploy crypto wallets, cryptocurrency exchange platforms, as well as networks of shell individuals, through whom 'shadow' funds are moved rapidly and anonymously between states.

IN TOTAL, DURING 2025, REGARDING THE COMMISSION OF THE RESPECTIVE CRIMES, THE SSU INITIATED:

141 criminal proceedings under Article 113 (Sabotage) of the CC of Ukraine;

166 criminal proceedings under Article 258 (Terrorist Act) of the CC of Ukraine;

79 criminal proceedings regarding the commission of other terror-related offenses (Articles 258-1 – 258-6 of the CC of Ukraine).

The SSU is also working to detect and eliminate threats related to international terrorist organisations (ITOs), illegal armed formations (IAFs), and religious extremist organisations (REOs). Specifically, to minimise the number of terrorist threats, the SSU banned 90 individuals involved in ITO activities from entering the territory of Ukraine. As a result of cooperation with partner intelligence services, 4 members of the ITO 'Islamic State - Khorasan Province' (ISKP), who were preparing terrorist attacks in European Union countries, were brought to criminal justice. Furthermore, the SSU established, identified, and ceased the illicit activities of 6 citizens of the Republic of Tajikistan involved in the activities of the 'ISKP' ITO.

The Security Service is the primary body within the nationwide system for countering terrorism. The Anti-Terrorist Centre at the SSU is responsible for compiling and maintaining the List of Terrorist Organizations. In 2025, 28 terrorist organizations and groups were added to this List. The relevant information is published on the official website of the SSU and the Unified State Web Portal of Open Data.

The SSU constantly improves response mechanisms to terrorist and sabotage threats. Specifically, it strengthens the coordination of counter-terrorism entities and the integration



of analytical and operational tools, also take preventive measures at the regional level, and develop interaction with state authorities and international partners. This is accompanied by enhancing of information exchange and reducing of response time, thus ensuring the timely detection and elimination of threats at early stages.

The SSU constantly improves response mechanisms to terrorist and sabotage threats. Specifically, it strengthens the coordination of counter-terrorism entities and the integration of analytical and operational tools, also take preventive measures at the regional level, and develop interaction with state authorities and international partners. This is accompanied by enhancing of information exchange and reducing of response time, thus ensuring the timely detection and elimination of threats at early stages.

The regulatory and strategic framework for countering terrorism remains an important area of this effort. Accordingly, in 2025, the SSU drafted a new edition of the Concept for Countering Terrorism in Ukraine. Furthermore, a draft Law of Ukraine 'On Combating the Dissemination of Terrorist and Other Illicit Content on the Internet' was developed. It is specifically aimed at countering the spread of destructive content online and preventing the use of the digital environment for the recruitment of citizens.

Thus, the SSU's activities in the field of countering terrorism and sabotage are systemic and comprehensive, targeted at preventing threats, ensuring the resilient functioning of critical infrastructure, and protecting national security under the conditions of ongoing armed aggression.



MILITARY COUNTERINTELLIGENCE AND ENSURING DEFENCE CAPABILITIES



MILITARY COUNTERINTELLIGENCE IS A KEY ELEMENT OF THE SECURITY OF UKRAINE'S DEFENCE SECTOR AND PLAYS A DECISIVE ROLE IN COUNTERING THREATS WITHIN THE MILITARY ENVIRONMENT. THE SSU UNITS, SPECIFICALLY THE MILITARY COUNTERINTELLIGENCE DEPARTMENT, EXECUTE A COMPREHENSIVE SET OF MEASURES AIMED AT PROTECTING THE AFU AND OTHER COMPONENTS OF THE SECURITY AND DEFENCE SECTOR FROM THE ADVERSARY'S INTELLIGENCE-SUBVERSIVE ACTIVITIES.

Under contemporary conditions, military counterintelligence is an indispensable component of the combat support system. It operates both in rear regions and directly within combat areas. Officers of the unit identify and eliminate enemy intelligence

assets within the military environment, prevent the leakage of sensitive military information, provide counter-sabotage protection, and counter internal threats. Furthermore, they are directly deployed to execute combat missions..



In 2025, one of the most critical threats in this domain remained the activities of spy networks, which Russian intelligence services systematically create for covert penetration into military formations, as well as collection of critical information and interference with the functioning of the defence sector. The elimination of these networks is of paramount importance for the timely detection and disruption of enemy subversive activities within Ukraine's defence sector. Notably, over the past year, military counterintelligence officers revealed 4 spy networks. Their operations were aimed at gathering intelligence on the deployment of Ukrainian forces, ammunition and supply depots, operational plans, and other sensitive data that pose a direct threat to the state's defence capability.

► **The SSU Counterintelligence has thwarted another terrorist attack planned by the Russians in Zaporizhzhia.** As a result of pre-emptive actions, a Russian agent preparing to detonate an improvised explosive device (IED) in the city centre was apprehended. The investigation established that the suspect was ordered to plant the explosives near a crowded public area and

'report back' to his Russian handler. The occupiers planned to detonate the IED remotely during rush hour to maximise civilian casualties at the location.

In total, Military Counterintelligence Department uncovered 62 agents throughout 2025. Among them was an aviation brigade flight instructor, a Major of the Armed Forces of Ukraine, who reported data to the main directorate of the general staff of the armed forces of Russia regarding tactical aviation, the operational deployment of combat aircraft (F-16, Mirage 2000, Su-24), and air defence systems, as well as intelligence used by the enemy to plan new missile and drone strikes against Armed Forces of Ukraine Air Force facilities.

Twelve agents of the Russian intelligence services were convicted of high treason, with 8 of them sentenced to 15 years of imprisonment. Those sentenced include individuals involved in transferring classified documents and operational plans of the Ukrainian Defence Forces to the enemy, as well as gathering intelligence on the deployment of Ukrainian military units and defence sector facilities.

Safeguarding the state's military-economic potential and preventing

abuses in defence procurement remain among the top priorities of the SSU Military Counterintelligence. This line of effort involves detecting and disrupting illicit schemes related to the embezzlement of budget funds, the illegal exploitation of defence sector resources, and other offenses that undermine the state's defence capabilities.

► **The SSU Military Counterintelligence, in cooperation with the National Police, exposed the Chief of Staff of a battalion within a Territorial Defence Forces unit of the Armed Forces of Ukraine in the Lviv region,** who had illegally authorised additional combat payment. From August to December 2023, the officer unjustifiably paid 'combat' financial bonuses in large amounts to subordinates who were not performing duties on the front lines.

► **The SSU detained the Chief Psychiatrist of the Armed Forces, who 'resolved' issues regarding the fitness of military personnel for military service.** According to the case materials, this official acquired significant unjustified assets during the full-scale invasion. The individual was served a notice of suspicion under Article 368-5 and Article 366-2 of the Criminal Code of Ukraine. A preventive measure in the form of detention has been enforced against the perpetrator.

In total, the SSU Department of Military Counterintelligence prevented financial losses to the state exceeding UAH 34 billion in 2025, demonstrating the unit's systematic and effective performance. Concurrently, in close coordination with military unit commanders, systematic efforts are underway to reinforce the counter-sabotage protection of military facilities. This approach mitigates threats within the military environment and enhances the overall resilience of the defence sector.

Specifically, additional security measures are being implemented to ensure the timely detection of enemy sabotage and reconnaissance plots, prevent unauthorised access to military infrastructure, and eliminate internal



threats. Particular emphasis is placed on vetting individuals with access to sensitive information and military sites. The SSU Military Counterintelligence units also actively counter the illicit trafficking of weapons, ammunition, and other ordnance. Throughout 2025 alone, 285 cases of illegal trafficking of military ordnance were interdicted.

► **In March, the SSU Military Counterintelligence exposed a perpetrator in the Kharkiv region – a squad head of an unmanned combat aerial vehicle unit.** He was attempting to establish an illicit network for selling drone components (including optical sights and initiation boards) and military ordnance smuggled out of frontline areas.

The strategic priority for military counterintelligence remains to operate pre-emptively-identifying threats, preventing their execution, and ensuring the uninterrupted functioning of the defence sector.

The fulfilment of these objectives directly impacts the effectiveness of the state's defence operations and aligns with national priorities in the area of national security and defence. These priorities are aimed at strengthening the country's defence capabilities, state resilience, and the effective functioning of Ukraine's security and defence forces.



PROTECTION OF NATIONAL STATEHOOD

THE PROTECTION OF NATIONAL STATEHOOD IS A FUNDAMENTAL CONDITION FOR PRESERVING THE SOVEREIGNTY, TERRITORIAL INTEGRITY, AND STABLE FUNCTIONING OF THE STATE. NATIONAL STATEHOOD SERVES AS ONE OF THE KEY ELEMENTS OF THE COUNTRY'S RESILIENCE AGAINST EXTERNAL AND INTERNAL THREATS.

Amid the full-scale invasion, the enemy combines military, informational, political, and other instruments of influence to undermine the state's internal resilience - weakening state institutions, fracturing society, and declining the constitutional order.

Encroachments on national statehood are increasingly executed through covert instruments of influence. The enemy establishes agent networks, conducts psychological operations (PSYOPs), and leverages controlled organisations, individuals, and the information space. These activities are coordinated and aimed at penetrating deep into internal state processes, fostering destructive sentiments, and weakening state institutions.

Concurrently, the SSU ensures systematic counteraction to these threats. To achieve this, the Service personnel combine operational, counterintelligence, preventive, and law enforcement measures. The outcomes of these activities include exposing and terminating illegal actions that encroach upon the foundations of statehood, as well as holding the perpetrators accountable.

SPECIFICALLY, IN 2025, BASED ON MATERIALS PROVIDED BY THE SSU UNITS, PRE-TRIAL INVESTIGATIONS WERE INITIATED IN CRIMINAL PROCEEDINGS CONCERNING THE FOLLOWING OFFENSES:

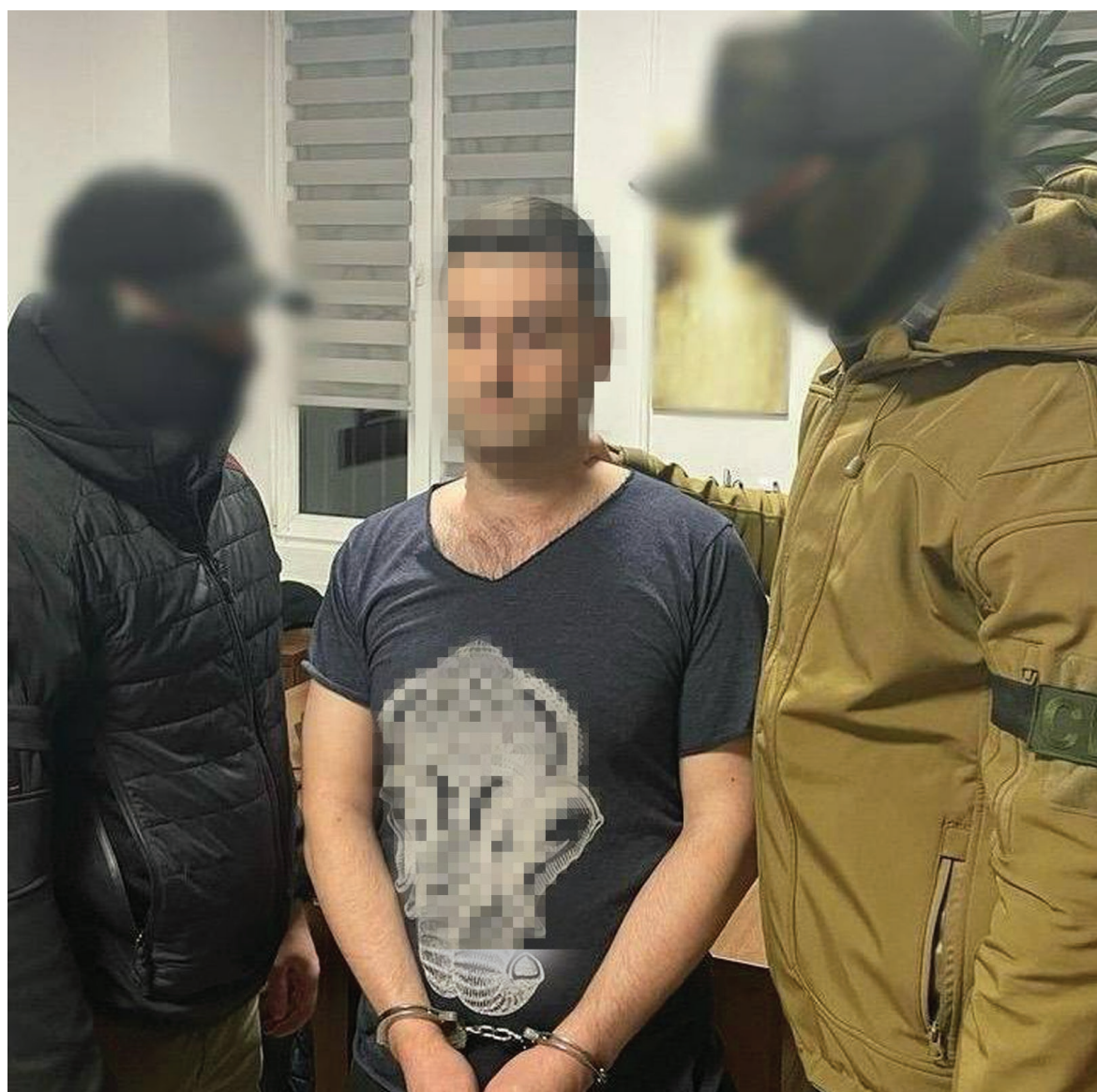
82 criminal proceedings under Art. 109 (Actions aimed at forceful change or overthrow of the constitutional order or take-over of government) of the Criminal Code of Ukraine;

219 criminal proceedings under Art. 110 (Encroachment on the territorial integrity and inviolability of Ukraine) of the Criminal Code of Ukraine.

► *The SSU detained 5 Russian accomplices who attempted to establish an 'insurgent movement' and revive 'soviet power' in Ukraine. The organisation's activities were aimed at destabilising the socio-political situation and undermining Ukraine's defence capabilities, specifically by disrupting the Defence Forces of Ukraine.*

Countering propaganda and coordinated information campaigns carried out by enemy in national information space is a crucial work direction for relevant SSU departments. SSU units expose the activities of individuals and networks involved in spreading disinformation, hostile narratives, manipulative content and neutralise information campaigns aimed at destabilising society, discrediting state institutions, and undermining international image of Ukraine.

► *The SSU has exposed an organised group of 12 people that carried out media attacks against Ukraine and operated under the guidance of Viktor Medvedchuk. The group operated within the framework of the 'Drugaiia Ukraina' (eng: 'Other Ukraine') association based in Moscow utilising it as a platform for disseminating anti-Ukrainian content. The SSU detained key suspect in the case – a well-known journalist, M., who worked for two intelligence services of the*



aggressor state at the same time, the fsb and russian foreign intelligence service. The network members were involved in justifying russian aggression, discrediting Ukraine on the international stage, and destabilising domestic situation in partner countries. The journalist M. himself organised public events in the EU countries calling to halt support for Ukraine.

The enemy systematically exploits political, public, and religious organisations to covertly influence internal processes in Ukraine. Such organisations are used to promote pro-russian narratives, foster loyalty to the aggressor state, support the occupation administrations, and create prerequisites for destabilising our country.

To counter these threats, the Security Service of Ukraine takes systematic measures to stop the activities of such organisations. Thus, following the SSU initiative, one pro-russian political party and seven pro-russian public organisations have been banned.

Following the SSU materials, a court has also banned the activities of four cossack public organisations, which were forcibly dissolved (liquidated), as well as the religious organisation 'Spiritual Administration of the Muslims of Crimea', which collaborated with the occupation authorities and was used as a tool to exercise influence in the temporarily occupied territory.

In 2025, nine pro-russian political parties were added to the list of non-resident

political parties and public organisations of Ukraine that pose a threat to its national security. Furthermore, the procedure for terminating the activities of the pro-russian political party 'GARANT' was completed, resulting in its removal from the list and blocking party's destructive online platforms, which had been used to publish anti-Ukrainian material. The total number of subscribers accounted approximately to 400,000.

► **The SSU has thwarted the illicit activities of the head of the 'Garant' political party, a citizen referred to as T., who illegally sought to raise funds to finance party's destructive activities. The suspect demanded USD 160,000 from a citizen of Ukraine for including him in the top ranks of the 'Garant' political party's list as a candidate for the Verkhovna Rada of Ukraine.**

The SSU ensures systematic countermeasures against external and internal destabilising factors, in particular in cooperation with the Ministry of Foreign Affairs initiates and implements political and diplomatic countermeasures. Such efforts aim to restrain the influence of foreign actors who spread destructive narratives, support the aggressor state, and engage in other subversive activities against Ukraine.

Meanwhile, a number of measures have been taken to prevent foreign nationals whose activities pose a threat to national security, from entering Ukraine. In total, 1,633 foreign nationals were banned from entering the country.

To prevent the exploitation of the religious community as a tool for influencing domestic affairs, individual restrictive measures have been imposed on certain religious figures on the basis of information provided by the SSU.

In particular, the Ukrainian citizenship of Metropolitan Onufrii (O. Berezovskyi) of the Ukrainian Orthodox Church (MP) has been revoked following the confirmation that he voluntarily acquired russian citizenship.



Another important area of the SSU's work is combating the illegal trafficking of weapon, ammunition, and other weaponry, blocking the channels through which they enter the illicit market, including the areas where hostilities are taking place, and dismantling networks involved in their illegal online distribution. Throughout 2025, following the SSU investigations, law enforcement agencies registered 1,242 criminal proceedings involving illegal weapons trafficking, 128 of which were brought by the SSU's investigators. 813 individuals were served with notices of suspicion, and 331 were convicted.

These threats are systematic and comprehensive in their nature and directly affect the state's stability and the operation of its institutions. Given these circumstances, the effective work of the SSU is a key factor in countering such threats that requires constant adjustment of working tools and methods. The ability to act pre-emptively, to detect and eliminate threats promptly determines the effectiveness of the protection of state sovereignty and the constitutional order.



INFORMATION AND CYBERSECURITY OF THE STATE

CYBERSPACE HAS BECOME ANOTHER IMPORTANT AREA OF INFLUENCE ON UKRAINE'S NATIONAL SECURITY. THE ENEMY CARRIES OUT MASSIVE CYBERATTACKS IN SYNERGY WITH MILITARY ACTIONS. THEIR AIM IS TO DISRUPT FUNCTIONING OF STATE BODIES, CRITICAL INFRASTRUCTURE FACILITIES, AND CRITICAL PUBLIC SERVICES. SUCH ACTIONS ARE SYSTEMIC IN NATURE AND ARE A PART OF THE HYBRID WAR.

Targeted attacks against state information resources and critical infrastructure, in particular energy sector, transport, financial system, and government bodies, remain the main cyber threats.

Such attacks are characterised by growing complexity and the use of modern technologies, including the latest malware and elements of artificial intelligence.

The Security Service of Ukraine systematically counters these cyber threats and ensures the protection of the national cyberspace, combining operational, technical, and preventive measures. To strengthen cooperation with entities involved in the national response system to cyber incidents, cyberattacks, and cyber threats, there exists a Situation Centre for Cybersecurity at the SSU, as well as regional cybersecurity centres ensuring cybersecurity for its regional branches.

Regional cybersecurity centres now operate in every region of Ukraine as a part of a decentralised cyber defence system. They are tasked with quick identification of vulnerabilities affecting critical infrastructure facilities, prevention and mitigation of cyberattacks, and direct cooperation with local authorities and enterprises to strengthen cyber resilience.

In total, throughout 2025 SSU cybersecurity experts promptly detected, prevented, and eliminated more than 3,000 critical cyber incidents and targeted cyberattacks on the information systems of state bodies and critical sectors for the country's economy and security.

At the beginning of 2025, the SSU's cyber experts successfully localised and eliminated the consequences of one of the largest enemy cyberattacks, which was carried out against the information and communication systems of the state-owned enterprise 'National Information Systems'. The attack disrupted stable functioning of the state registers.

The SSU's cyber experts quickly restored critical government services, mitigated the risks of data leaks, and helped to restore the integrity of the registers as quickly as possible.

Cyberespionage and attempts to get unauthorised access to classified information pose a particular threat, creating risks of 'sensitive' information leaks and undermining the state's defence capabilities.

Synchronically the enemy conducts coordinated information and psychological operations aimed at destabilising social and political situation, undermining trust in state authorities, and discrediting military and political leadership.



► **In Kyiv region, officers of the SSU's Cyber Department have exposed a covert PR agency and detained two professional PR specialists** who carried out information sabotage against Ukraine by the order of the Russian intelligence services. The suspects operated primarily within the EU's 'media market'. They created more than 200 websites that mirrored official Kremlin propaganda 'media mouthpieces' and registered them under fake accounts to avoid blocking.

In addition, the SSU's cyber experts take necessary measures to prevent the spread of harmful content. In particular, nearly a dozen hostile centres have been exposed and shut down, including eight bot farms that were used to discredit state authorities and justify Russia's armed aggression against Ukraine.

At the same time, the SSU personnel regularly block channels spreading destructive information and bring individuals involved to criminal liability.

► **The SSU has exposed the illegal activities of a citizen referred to as N, a former TV presenter associated with Medvedchuk and Muraiev's TV channels**, who spread Russian propaganda. The man created his own YouTube channel, where he disseminated Kremlin propaganda and justified war crimes, including strikes on civilian infrastructure. To this end, he regularly invited pro-Russian 'political experts' onto his programmes, though a significant number of them are currently hiding in Russia. The suspect was served with a notice of suspicion under Article 436-2 of the Criminal Code of Ukraine, with an indictment submitted to the court at the end of 2025.

The SSU's cyber experts also actively cooperate with Ukrainian and foreign intelligence services and law enforcement agencies to identify and shut down international hacker groups.

► **Jointly with the National Police and Czech law enforcement agencies, the SSU has exposed hackers** who were stealing from bank accounts and crypto wallets owned by EU and US citizens. The perpetrators stole personal data using custom-developed malware. All members of the hacker group have now been served with notices of suspicion under Article 361-1 of the Criminal Code of Ukraine.

A key focus for the SSU's cyber units remains the protection of digital transformation sector of Ukraine, which, being the actively implementing digital solutions, is vulnerable to corruption risks and abuse of power. The SSU takes effective countermeasures to detect and prevent offences related to the misuse of public funds and abuses in the process of the state's digital modernisation.

► **Following the information provided by the Cyber Department, two former Deputy Ministers of Social Policy** who caused a loss of UAH 47 million to the State Budget of Ukraine have been notified of suspicions under Article 367

of the Criminal Code of Ukraine. Three senior officials from the Ministry of Justice of Ukraine who caused losses to the state budget amounting to approximately UAH 10 million through procurement in the field of digital modernisation have also been served with a notice of suspicion under Article 191 of the Criminal Code of Ukraine.

Beyond countering direct cyber threats and information influence, the SSU specialists are committed to strengthening the state's cyber resilience, enhancing the security of information resources, and developing the capabilities of the national cyber defence system.

This approach includes improving the protection of critical information infrastructure, enhancing mechanisms for responding to cyber threats, developing interdepartmental and international cooperation, and expanding organisational and technological capabilities.

Thus, in 2025, the SSU organised and conducted practical workshops on enhancing cyber resilience for representatives of central government bodies and national critical infrastructure. The workshops were held with the support of international partners ESET and Microsoft. In total, representatives from more than 130 different agencies, enterprises and institutions participated in the events.

► **In October 2025, the Security Service of Ukraine conducted command and staff exercise (CSE) on countering cyberterrorism.** In particular, SSU cyber experts, together with colleagues from other sectors, practiced joint responses to a coordinated enemy cyberattack against our country's critical infrastructure. It was the first large-scale event of that kind in Ukraine, where response protocols for cyberterrorism and terrorist threats were practised. The event combined a hands-on phase of simulation of real-life cases of terrorist acts and cyberattacks with the development of solutions for their effective elimination.

Based on the experience gained, cyber experts also conducted a series of sessions for media representatives to improve cyber literacy and online safety as a part of the seminar organised by the OSCE Support Programme for Ukraine.

In addition, in 2025 the SSU's Cyber Units exposed a number of spy networks that were sharing coordinates for missile strikes via messengers and shut down groups that were setting fire to infrastructure facilities following online Russian guidance, as well as thwarted the preparation of terrorist attacks coordinated remotely.

Special attention should be paid to the exposure and elimination of the hostile residency that guided Russian strikes in the Kyiv and Kharkiv regions. The enemy network was organised and led by an engineer at the Kyiv Metro public utility company, who recruited a number of agents living in Kyiv and Kharkiv, including a deserter (who had previously worked for Ukrzaliznytsia (Ukrainian Railway)) and an international truck driver.

The intelligence network was utilised by the Russian intelligence services to systematically obtain information regarding the deployment of military facilities, command and control centres, and other critical infrastructure facilities in Ukraine.

► **In July 2025, cyber specialists took pre-emptive action and prevented a large-scale sabotage act in the Odesa region.** Two FSB agents who were preparing to blow up a facility storing explosive mineral fertilisers at a transit depot in one of the seaports, were detained.

The SSU plays a crucial role in protecting the state's cyber resilience. The enemy combines military operations, cyberattacks, and information influence, whereas technological development, particularly artificial intelligence, make these threats more sophisticated and covert. Consequently, the SSU constantly updates its approaches and promptly responds to new challenges.



STATE SECRETS PROTECTION

THE PROTECTION OF STATE SECRETS IN THE CONTEXT OF RUSSIAN FULL-SCALE ARMED AGGRESSION IS OF THE UTMOST IMPORTANCE FOR ENSURING NATIONAL SECURITY, THE STATE'S DEFENCE CAPABILITY, AND THE RESILIENCE OF ITS INSTITUTIONS. THE PROTECTION OF RESTRICTED INFORMATION IS A PREREQUISITE FOR THE EFFECTIVE FUNCTIONING OF THE SECURITY AND DEFENCE SECTOR, CRITICAL INFRASTRUCTURE, AS WELL AS INTERNATIONAL COOPERATION.

The SSU ensures the protection of classified information in the defence, economy, science and technology, foreign relations, national security and law enforcement spheres, the disclosure of which could harm national security of Ukraine.

The SSU's efforts are focused on establishing a modern flexible system for safeguarding state secrets, adapted to the conditions of martial law and current threats. This involves improving the regulatory framework, the procedures for granting clearance and access to state secrets, and the mechanisms for classifying information, as well as aligning the national information security system with NATO and EU standards.

AN IMPORTANT ELEMENT OF THE SECURITY SYSTEM IS THE BACKGROUND CHECK ON INDIVIDUALS APPLYING FOR STATE SECRETS CLEARANCE. IN 2025, SSU PERSONNEL:

- ◆ denied access to state secrets to over **1 700** citizens;
- ◆ brought **800** officials to account based on the results of information security checks;
- ◆ revoked or suspended access to state secrets for nearly **500** individuals.

The SSU's systematic work also aims to prevent and localise threats of classified information leaks. The adversary makes constant and targeted attempts to gain access to information constituting state secrets. To achieve this, it employs a wide range of tools - from agent infiltration and cyberattacks to information operations, compromise, and the recruitment of information holders.

Following the established facts of violations in the field of state secrets protection in 2025, the SSU initiated 13 criminal proceedings on the grounds of offences under Article 328 of the Criminal Code of Ukraine (Disclosure of State Secrets).

The SSU is also strengthening the institutional capacities of the state secrets protection system, taking into account current challenges and threats. Relevant measures are being implemented in cooperation with the Verkhovna Rada of Ukraine and the Cabinet of Ministers of Ukraine.

In 2025 the SSU started the work on the draft law in order to update licensing mechanisms for activities involving state secrets, and to improve the procedures for granting and revoking clearance and access to state secrets, etc. The draft law also envisages the establishment of appropriate legal conditions for parliamentary oversight of the activities of security and defence sector bodies through the creation of a specialised committee within the Verkhovna Rada.

Overall, the SSU ensures the effective functioning of a system for the protection of state secrets, which is constantly adapting to changes in the security environment and the development of modern technologies. The implementation of these measures contributes to strengthening the state's defence capabilities, protecting its strategic interests, and maintaining resilience in the face of constant pressure from the adversary.



COMBAT AND SPECIAL OPERATIONS

THE SECURITY SERVICE OF UKRAINE IS AN INTEGRAL AND EFFECTIVE PART OF THE DEFENCE FORCES. FROM THE VERY FIRST DAYS OF THE FULL-SCALE INVASION, SSU PERSONNEL DIRECTLY PARTICIPATED IN COMBAT OPERATIONS IN THE HOTTEST FRONTLINE ZONES. COMBAT MISSIONS ARE CARRIED OUT BY FIGHTERS FROM THE 'ALFA' SPECIAL OPERATIONS CENTRE, THE DEPARTMENTS OF MILITARY COUNTERINTELLIGENCE, COUNTERINTELLIGENCE, CYBERSECURITY, AND OTHER UNITS.



In 2025, the SSU fighters were active across the entire frontline and deep in the Russian rear, carrying out asymmetric strikes against the enemy. The SSU also conducted a series of unique special operations that changed the course of the war.

► *The SSU's historic special operation 'Spider Web'. As a result, the Ukrainian security service destroyed 41 enemy strategic aircraft. These included Tu-95s, Tu-22M3s, Tu-160s, as well as unique A-50 reconnaissance aircraft, which were used by the enemy to attack Ukrainian*



cities. Losses to the enemy inflicted by that special operation amounted to over USD 7 billion.

► **In June 2025, SSU carried out a third strike on the Crimean Bridge.** This time, SSU managed to blow up the bridge's underwater pillars. The bridge suffered serious damage and currently cannot be used for military purposes.

► **In December, the SSU carried out another unique special operation and staged a maritime 'bavovna' (explosive strike) in the port of Novorossiysk.** For the first time in history, underwater drones 'Sub Sea Baby' blew up a russian submarine. As a result of the explosion, the submarine suffered critical damage and got out of order. The submarine carried four launchers for 'Kalibr' cruise missiles, used by the enemy to strike targets in the territory of Ukraine.

In terms of combat operations carried out by the SSU directly on the frontline

in 2025, SSU personnel destroyed 758 enemy tanks, 1,425 armoured vehicles, 2,414 artillery systems, 134 multiple launch rocket systems, 411 electronic warfare, radio-electronic reconnaissance and radar systems, 455 air defence systems, 686 ammunition and fuel and oil depots, etc.

The SSU's 'Alfa' Special Operations Centre regularly ranked among the top three in the list of the best special operations units in terms of eliminating enemy personnel and russian equipment using UAVs.

Another important area of work for the fighters of the SSU 'Alfa' Special Operations Centre is the destruction of enemy strike drones (Shaheds, Herans, Herbers, Lancets, Molnias, etc.). In 2025, they destroyed 1,276 russian aerial targets using interceptor drones. One of 'Alfa's' most effective crews, consisting of only three members, has already shot down nearly **150 of such drones.**

The Security Service of Ukraine also regularly carries out combat and special operations in close cooperation with other representatives of the Ukrainian Defence Forces. Working side by side with servicemen from the Armed Forces of Ukraine, the Special Operations Forces, intelligence agencies, and other components of the Defence Forces, SSU fighters systematically inflict heavy losses on the enemy and destroy its equipment.

► **The SSU and the Special Operations Forces of the Armed Forces of Ukraine carried out a joint special operation resulting in the destruction of two russian SU-34 fighter-bombers at the Marinovka airfield and the damage to two more aircrafts with the aid of long-range drones.** The enemy actively deploys such fighter-bombers on the front line for bombardments, including the dropping of guided bombs.

Fighters of the Security Service of Ukraine continue to destroy the enemy across all key areas and systematically weaken the russian military capabilities, until the enemy agrees to peace talks.

ACTIVITIES OF THE MILITARY MEDICAL DIRECTORATE



In 2025 the SSU Military Medical Directorate continued to carry out its key tasks providing medical support to SSU personnel, medical treatment and evacuation of the wounded and injured, tactical medicine training for military personnel, as well as supplying of individual and collective medical protection equipment, etc.

The Directorate actively provides specialised medical care to wounded military personnel of the SSU and other defence forces. For instance, SSU medical staff carries out medical and psychological rehabilitation. These measures aim to restore personnel combat readiness and mitigate the effects of psychotraumatic factors.

To improve the effectiveness of treatment for the wounded, the Military Medical Directorate employs advanced techniques. First and foremost, it relates to the treatment of mine and explosive injuries. The surgical care provided for complex combat injuries, particularly injuries to the eyes, has also been improved, and the range of specialised trauma interventions has been expanded. In addition, the SSU

medical staff have applied a broader range of psychotherapeutic techniques to minimise the effects of psychotraumatic factors.

In 2025 the SSU Military Medical Directorate significantly strengthened its medical rehabilitation program based on the principles of a phased approach, continuity, and evidence-based practice. A comprehensive rehabilitation process has been established now within the SSU system for servicemen who suffered from injuries and underwent multiple surgical interventions. It starts from the moment of injury, includes the necessary surgical procedures, and covers the entire recovery period, from the acute phase of treatment to the return to active duty and subsequent reintegration into society.

The effective organisation of medical care by the SSU military medical units helps to minimise casualties and ensure a high-quality recovery of personnel. As a result, over 96 percent of those wounded return to their duties. It helps to maintain the SSU's personnel at the adequate level of combat readiness in combat conditions.

IMPLEMENTATION OF SANCTIONS POLICY

UKRAINE'S SANCTIONS POLICY IS A PART OF A SYSTEMATIC RESPONSE TO THE RUSSIAN ARMED AGGRESSION. SANCTIONS REDUCE THE ENEMY'S RESOURCES USED TO WAGE THE WAR AGAINST UKRAINE, AND WEAKEN THE AGGRESSOR STATE'S MILITARY AND ECONOMIC CAPACITY.



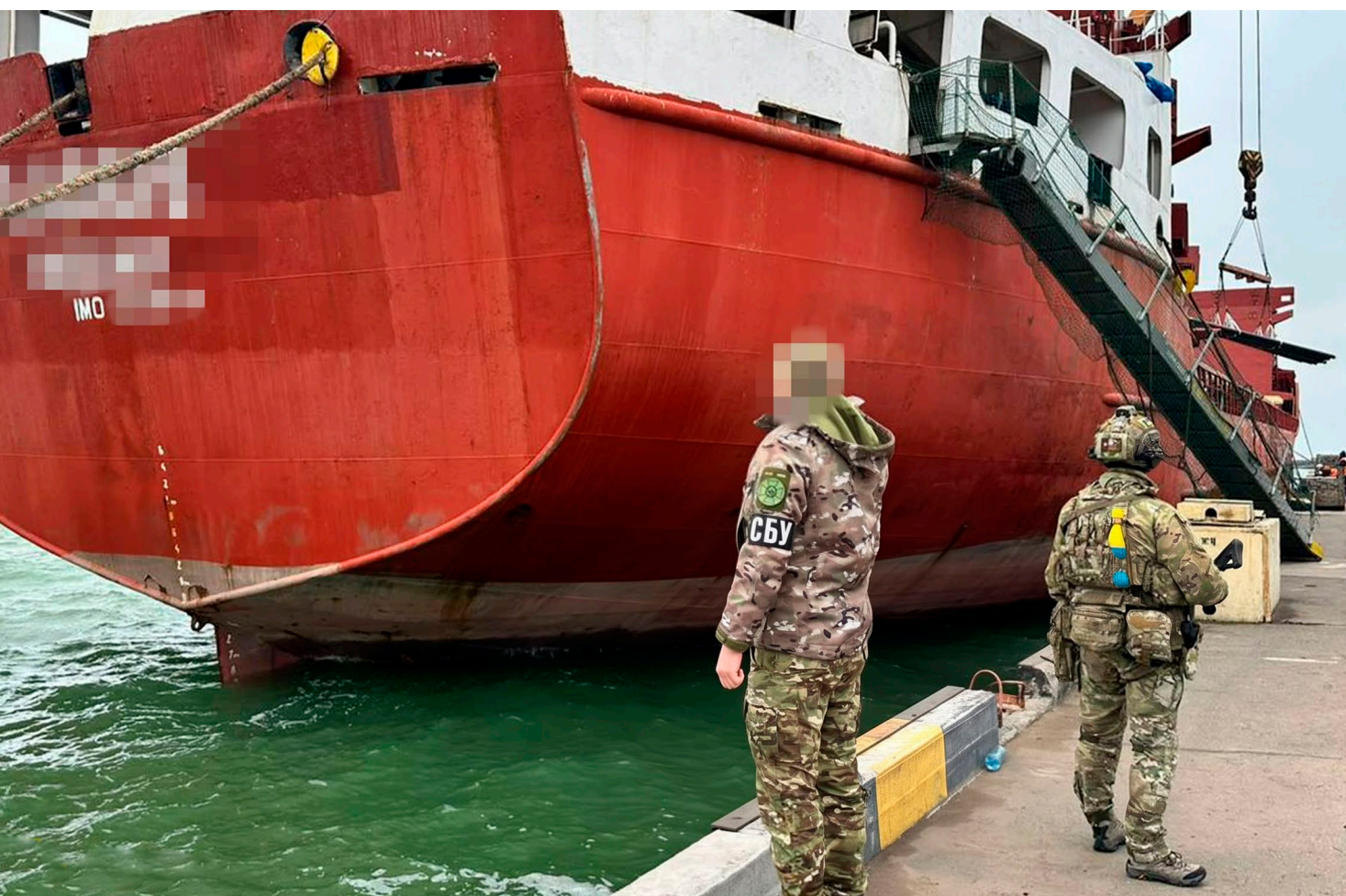
The SSU is one of the key initiators of imposing special economic and other restrictive measures (sanctions). It ensures their implementation based on the evidence collected. Following the initiative of the SSU sanctions were imposed on **2 479 entities** by decisions of the National Security and Defence Council of Ukraine during 2025. These include enterprises, individuals and organisations that support the aggression or directly assist the aggressor state.

In total, since the beginning of the full-scale invasion, the SSU has initiated the

imposition of sanctions against **17 881 entities**. These restrictions are aimed at:

- ◆ countering the mechanisms of financing the enemy's intelligence and subversive activities and its information operations;;
- ◆ undermining the aggressor's financial and economic resources (blocking channels for replenishing the budget, restricting access to resources necessary for the production of weapons, military equipment, the operation of the defence industry, etc.).

An important component of restrictive measures is countering the activities of



the so-called russian 'shadow fleet'. Since imposing the sanctions, many russian vessels and shipping companies have been attempting to circumvent them. For example, they operate under false flags, forge documents, and use other schemes to conceal their activities.

It requires a further tightening of sanctions pressure and the improvement of mechanisms for their implementation. In particular, in 2025, relevant legislative amendments were adopted, enabling sanctions to be imposed directly on maritime vessels and their captains personally.

Following the SSU materials, last year **239** russian 'shadow fleet' captains and **712** vessels were subject to sanctions.

The individuals and companies subject to sanctions assisted russia in waging war against Ukraine. They financed or supplied russian troops, sold oil and petroleum products in circumvention of international

restrictions, acted in the interests of the occupying administrations, supplied resources to russian military units, and supported the defence industry and energy sector of the aggressor state.

The illegal export of agricultural products from the temporarily occupied territories of Ukraine is one of the forms of such unlawful activity.

The SSU has documented the activities of officials from the occupying authorities who, through 'food companies' under their control, stole grain in the Zaporizhzhia, Kherson, Donetsk, Luhansk, and Kharkiv regions. It has been established that **587 905 tonnes** of Ukrainian grain products, worth **over UAH 9 billion**, were illegally exported by sea.

In order to put an end to the illegal maritime export of grain from the temporarily occupied territories and its transit through maritime straits, 56 marine vessels and 28 russian citizens (captains)

involved in the operation of the so-called russian 'shadow grain fleet' were added to the sanctions lists in 2025.

FURTHERMORE, SSU HAS DOCUMENTED ILLEGAL ACTIVITIES AND NOTIFIED RUSSIAN SENIOR OFFICIALS OF SUSPICIONS, IN PARTICULAR::

- ◆ Patrushev D. M., Deputy Prime Minister of russia;
- ◆ Lut O. M., Minister of Agriculture of russia;
- ◆ Razin A. V., Deputy Minister of Agriculture of russia;
- ◆ Lieonov V. I., Head of the Department at the Ministry of Agriculture of russia.

They are suspected of large-scale acquisition of agricultural assets and food supplies in the occupied territories.

Another aspect of the sanctions policy involves restrictions against those who threaten Ukraine's information security. It refers to individuals and organisations, in particular media representatives and entities, who systematically disseminate disinformation, manipulation, and other content directed against Ukraine. Such actions are aimed at undermining trust in state institutions and the security and defence sector, discrediting Ukraine and instigating anti-Ukrainian sentiment within society.

The aim of sanctions in this area is to limit the spread of destructive content and channels of informational influence, and to minimise harmful consequences for national security. Over the past year, following SSU initiative, special restrictive measures (sanctions) have been imposed on 24 legal entities and 159 individuals involved in such activities.

The list includes I. Mosiichuk, a Member of the Ukrainian Parliament, who conducts information campaigns in the interests of the aggressor state (disseminating anti-Ukrainian content), as well as A. Dmytruk, a Member of the Ukrainian Parliament, due to his anti-Ukrainian activities in the information sphere in favour of the aggressor state.

Sanctions imposed by Ukraine are not only a domestic defence mechanism but



also an important signal to the international community. Indeed, following their implementation, the Ukrainian Ministry of Foreign Affairs informs its partners and encourages the introduction of similar international restrictive measures.

Throughout 2025 Ukraine synchronised 44 sanction packages with the international community, targeting 1,372 entities. These sanctions were imposed by the United States, the United Kingdom, Canada, Australia, the Swiss Confederation, Japan, and New Zealand. Materials have also been prepared for further building the evidence base and initiating the imposition of sanctions against 1,163 entities.

The synchronisation of sanctions with international partners creates a multi-tiered pressure that gradually weakens the russian economic and financial capabilities. It directly affects the aggressor state's ability to continue its war against Ukraine.



SEARCH FOR AND RELEASE OF PRISONERS OF WAR

SEARCHING FOR AND RELEASING UKRAINIAN CITIZENS FROM CAPTIVITY REMAINS ONE OF THE STATE'S KEY HUMANITARIAN AND SECURITY PRIORITIES. THE JOINT CENTRE FOR COORDINATION OF SEARCH AND RELEASE OF PERSONS UNLAWFULLY DEPRIVED OF LIBERTY AS A RESULT OF AGGRESSION AGAINST UKRAINE, WHICH WAS CREATED AT THE SSU TOGETHER WITH OTHER AUTHORISED BODIES OF OUR STATE, CARRIES OUT SYSTEMATIC EFFORTS TO LOCATE AND REPATRIATE THOSE HELD CAPTIVE.

Special attention is paid to collecting and verifying information regarding detained persons, to coordinating actions with relevant security and defence agencies, and fostering cooperation with international partners in order to facilitate the exchange and repatriation of Ukrainian citizens.

Implementing such measures is an extremely complex, multi-stage process that requires constant coordination among state bodies, security agencies, and international intermediaries. Further difficulties arise from the aggressor state's systematic violation of the norms of international humanitarian law, concealing information regarding detainees, manipulation of exchange processes, and use of prisoners as a tool for political and psychological pressure.

In cooperation with the security and defence forces and other authorised state bodies, 26 operations were carried out to release Ukrainian defence personnel held captive and unlawful detainees. As a result of these operations, 3,385 citizens were released from captivity in the aggressor state.

Also, as part of the implementation of release measures, 238 civilians were transferred to the government-controlled territory. These individuals had been serving sentences in the temporarily occupied territory of Ukraine, russia, and the Republic of Belarus, or were being held in temporary accommodation facilities.

To support the work of the Coordination Council on the Protection and Safety of Children under the President of Ukraine, the Joint Centre at the Security Service of Ukraine collects and systematises data



on illegally transferred minor citizens of Ukraine who are being held in the temporarily occupied territory of Ukraine, the territory of russia, and the Republic of Belarus.

Through the joint efforts of the Joint Centre at the SSU, the security and defence forces, and relevant state authorities, 663 minor citizens were returned to Ukraine-controlled territory over the past year. As a part of the development of the President of Ukraine's initiative 'Bring Kids Back UA,' the SSU's coordinating and advisory body established the 'Kids at Home UA' project, aimed at supporting returned children who were at risk and/or subjected to forced displacement or deportation in the temporarily occupied territories of Ukraine or russia, as well as the children of Ukraine's defenders.

The return of every person is the result of complex and persistent work. At the same time, it is evident that the state is fighting for its citizens and does not leave them alone in the face of the challenges of war.



PRE-TRIAL INVESTIGATION

THE SSU INVESTIGATIVE DEPARTMENT CONDUCTS INVESTIGATIONS INTO CRIMINAL OFFENCES THAT FALL WITHIN ITS JURISDICTION AS DEFINED BY LAW. FIRST AND FOREMOST, THESE ARE CRIMES AGAINST THE FOUNDATIONS OF NATIONAL SECURITY, TERRORIST AND WAR CRIMES, VIOLATIONS OF STATE SECRETS, THE INTANGIBILITY OF THE STATE BORDER, AS WELL AS CERTAIN CRIMES IN THE FIELD OF INTERNATIONAL SECURITY

The SSU investigative units work under conditions of ongoing hostilities, the temporary occupation of certain territories, and restricted access to crime scenes that makes it difficult to build a case and bring the perpetrators to justice.

In these circumstances, SSU investigators are constantly adapting, implementing modern information technologies and strengthening their analytical capabilities. These approaches help to improve the effectiveness of investigations.

Thus, during 2025, SSU investigators conducted pre-trial investigations in **141 569 criminal proceedings**, of which – **114 475** were criminal proceedings on the grounds of the offence under Article 438 (War crimes). Overall, investigations were conducted regarding **6 165 individuals**. Charges were brought against **4 548 individuals**. A total of **3 894** cases involving **4 473 individuals**, were referred to court with indictments, including **40 indictments** against **201 individuals**, who acted as a part of organised groups. Following the court proceedings, **1919 individuals** were convicted.

The reimbursement of losses incurred and the seizure of assets are key indicators of the effective work of the investigating units. In concluded criminal proceedings, the total amount of established losses exceeds **UAH 335,5 million**. In addition, the property of suspects and assets obtained illegally were frozen, amounting to **over UAH 809 million**. Legal claims totalling **over UAH 96,7 million** were initiated, whilst suspects voluntarily reimbursed **over UAH 9,8 million**.

In 2025, the SSU investigators paid particular attention to investigating the enemy's subversive activities. During the year, they **documented the unlawful activities of 152 Ukrainian citizens** operating as a part of **36 agent networks** crun by the russian intelligence services.

Last year there was an increase in incidents obstructing the lawful activities of the Armed Forces of Ukraine and other military formations. Pursuant to Article **114-1** Kof the CC of

Ukraine, **540 criminal cases** were brought to court, compared with **214** in 2024.

At the same time, SSU investigators significantly improved their effectiveness in investigating sabotage and terrorist offences. Thus, in 2025, 112 criminal cases were brought to court under Article 113 (Sabotage) of the Criminal Code of Ukraine (compared with 25 in 2024). Pursuant to Article 258 (Terrorist Act), 85 criminal cases were brought to court (compared with 11 in 2024).

In general, the majority of the concluded criminal proceedings are related to offences against the foundations of national security, in particular:

- ◆ high treason – **739**;
- ◆ collaboration – **1 251**;
- ◆ assisting the aggressor state – **165**;
- ◆ acts of sabotage and terrorist offences – **326**;
- ◆ crimes of aggression and war crimes - **77**
- ◆ and other crimes against peace and the security of humankind.

SSU investigators ensure systematic collection, recording, and procedural evidence documentation of crimes related to waging an aggressive war against Ukraine, as well as intended attacks against the civilians and critical infrastructure.

In particular, the involvement of representatives of the russian military leadership in organising the torture of the civilian population in the temporarily occupied territories of Ukraine has been documented, which is a gross violation of international humanitarian law.

The documentation of war crimes is systematic in nature and covers a significant number of incidents, viewed as components of a consistent russian policy of aggression. The materials collected form the evidence base which is used both in national criminal proceedings and within the framework of international justice. It is necessary to bring the senior military and political leadership of the aggressor state to accountability.



COOPERATION AND COORDINATION WITH OTHER LAW ENFORCEMENT AGENCIES

THE SECURITY SERVICE OF UKRAINE ENSURES CONSTANT COORDINATION AND COOPERATION WITH BODIES IN THE SECURITY AND DEFENCE SECTOR, STATE AND LAW ENFORCEMENT AGENCIES, PROSECUTORIAL AUTHORITIES, INTERNATIONAL PARTNERS.

SUCH COOPERATION IS ONE OF THE KEY FACTORS IN COUNTERING THREATS TO NATIONAL SECURITY UNDER MARTIAL LAW. IT HELPS TO BRING TOGETHER OPERATIONAL, ANALYTICAL, INVESTIGATIVE, MILITARY, AND TECHNICAL CAPABILITIES OF THE STATE TO RESPOND PROMPTLY AND EFFECTIVELY TO CURRENT CHALLENGES.

SYSTEMIC INTERAGENCY COOPERATION ENABLES TO GIVE A COMPREHENSIVE RESPONSE TO THREATS, TO CONDUCT JOINT ACTIONS MORE EFFECTIVELY, UNITE RESOURCES, AND TO STRENGTHEN THE STATE'S CAPACITY TO COUNTER RUSSIAN AGGRESSION. IT IS A KEY COMPONENT OF THE STATE'S RESILIENCE, THE PROTECTION OF NATIONAL INTERESTS, AND STRENGTHENING NATIONAL SECURITY OF UKRAINE.

One of the key areas of interagency cooperation remains countering sabotage, eliminating enemy agent networks, and preventing the illicit trafficking of weapons and ammunition.

► *Last January, SSU and the National Police caught fsb saboteurs red-handed after having blown up a railway track in front of 'Ukrzaliznytsia' (Ukrainian Railway) train using an improvised explosive device.*

► *Following comprehensive actions by the SSU, the State Bureau of Investigation, and the National Police, nine individuals, engaged in the trafficking of weapons and munitions illegally exported from frontline areas and the combat zone were detained.*

In the context of documenting and investigating war crimes committed by Russia, the SSU ensures close coordination,

foremost with the Prosecutor General's Office, the Main Intelligence Directorate of the Ministry of Defence of Ukraine, and the National Police of Ukraine.

► *The SSU and the Prosecutor General's Office collected substantial evidence regarding the illegal seizure and exploitation of Ukrainian industrial enterprises in coal mining, metallurgy, and coke-chemical industries in the temporarily occupied territories of the Donetsk and Luhansk regions. Notification of suspicion has been served in absentia to Ukrainian fugitive businessman Serhii Kurchenko, senior Russian officials, and other individuals involved in looting national assets and resources in the temporarily occupied territories.*

The Temporary Expert Working Group (TEWG) on documenting war crimes committed by Russia on the territories of



Ukraine, led by the SSU, continues its work. The group consists of SSU investigators, representatives of the Prosecutor General's Office, the Foreign Intelligence Service, the Defence Intelligence Directorate of the Ministry of Defence, and the Intelligence Directorate of the State Border Guard Service. TERC's main objective is to enhance the effectiveness of cooperation between the SSU's pre-trial investigation units and intelligence agencies of Ukraine in the course of investigating war crimes, and to establish and develop new mechanisms for obtaining additional sources of evidence.

► **Within the framework of joint efforts of the SSU, the Defence Intelligence Directorate of the Ministry of Defence, and the National Police, war crimes** *е perpetrated by two more officials of the russian federal penitentiary service, involved in torturing Ukrainian prisoners of war, have been documented. According to the investigation materials, the suspects systematically subjected the prisoners to physical violence, torture, and inhuman treatment.*

Working together with the National Anti-Corruption Bureau of Ukraine, Economic Security Bureau, State Bureau of Investigation, the Ministry of the Internal Affairs, the Prosecutor General's Office, and other state bodies, the SSU systematically detects and eliminates threats to national security in the budgetary, financial, economic, defence and other sectors that could harm the country.

► **Security Service of Ukraine, National Anti-Corruption Bureau of Ukraine and Specialised Anti-Corruption Prosecutor's Office have revealed a criminal group in Kyiv led by a Member of the Ukrainian Parliament.** *According to the investigation, members of this group offered a business representative USD 250,000 to arrange the imposition of sanctions by the National Security and Defence Council of Ukraine on a rival company.*

► **In Poltava region, the SSU and the State Bureau of Investigation have exposed a large-scale scheme to circumvent tax payments to the Ukrainian budget.**



According to case materials the suspects embezzled nearly UAH 2.5 billion between 2020 and 2023. Based on the evidence provided by the agencies, the former director of a state-owned factory was served with a notice of suspicion.

► **Together with French and Monegasque law enforcement agencies, SSU and Prosecutor General's Office have detained the son of the former president of 'Motor Sich' JSC,** *who, together with his father, is suspected of embezzling assets from that industrial giant, a critically important enterprise for Ukraine's defence. To launder the stolen assets, the perpetrators sold them to foreign companies and used the profits to purchase luxury real estate within the EU.*

► **In July 2025, the SSU, in cooperation with the Prosecutor General's Office, the State Bureau of Investigation, National Police and the Economic Security Bureau, carried out a special operation targeting illegal schemes at customs in several regions of Ukraine.** *During these comprehensive operations, evidence of illegal assistance in evasion of mobilization,*

the organisation of illegal migration routes, smuggling, and abuses during the customs checks of goods and vehicles was uncovered.

Another area of interdepartmental cooperation is the systemic elimination of illegal channels for smuggling people across the state border and the exposure of schemes to evade mobilisation.

► **Together with the Prosecutor General's Office, the SSU exposed a deputy of the Volyn Regional Council for organising schemes to smuggle draft evaders across Ukraine's state border.** *Military-liable men were sent abroad by the Volyn Regional State Administration under the guise of 'volunteers' to deliver humanitarian aid.*

► **SSU and National Police have uncovered individuals selling fake 'Reserve+' and 'Diia' apps to draft evaders,** *as well as forged documents, to ensure 'smooth' checks by the Territorial Recruitment Centres. The suspects sold their 'mobile apps' via specially designed Telegram bots. To make forged documents, the fraudsters set up an undercover printing office on the premises of a private car service centre.*



CHAPTER 4. HUMAN RESOURCES MANAGEMENT AND INTEGRITY ASSURANCE

4.1. PERSONNEL POLICY

PERSONNEL, THEIR EXPERTISE AND MOTIVATION LAY THE FOUNDATION FOR THE EFFECTIVE WORK OF THE SECURITY SERVICE OF UKRAINE. GIVEN THE WAR, THE CHANGING NATURE OF THREATS AND TRANSFORMATION OF THE SECURITY ENVIRONMENT, SSU IS DEVELOPING AN UP-TO-DATE PERSONNEL POLICY, AIMED AT RAISING PROFESSIONAL STANDARDS, ENHANCING ADAPTABILITY, DEVELOPING COMPETENCIES AND STRENGTHENING THE PERSONNEL'S MOTIVATION.

IMPROVING HUMAN RESOURCES POLICY IS ONE OF THE PRIORITIES OF THE SSU'S DEVELOPMENT STRATEGY FOR 2025–2030. AMONG ITS KEY OBJECTIVES ARE:

- ◆ introduction of modern approaches to human resources management;
- ◆ modernisation of the professional training system and the development of personnel potential;
- ◆ improvement of social and psychological support for personnel;
- ◆ formation of a personnel reserve and development of a corporate culture.

The document envisages updating the recruitment system and establishing a clear career growth model. Promotion should be based on professional competencies and practical work outcomes.

The SSU's human resources management system is based on the principles of consistency, flexibility and a human-centred approach. The SSU has renovated its approaches to human resources and personnel management. In 2025, the Organisational Principles for Staffing and Personnel Management at the SSU were approved. They outline how the system for staffing, military service, personnel management and professional development of its personnel should evolve.

The SSU has also approved a new Procedure for the Performance Assessment of Servicemen and Methodological Guidelines on its Organisation and Implementation. These documents aim to introduce modern approaches to assessing professional performance, professional training, moral and professional qualities, professional ethics, and integrity of personnel.

The SSU adheres to the principles of gender equality, non-discrimination, and

equal opportunities for the professional development of its personnel. The career growth of its personnel is based on professional competencies, performance, and personal qualities, regardless of gender. Currently, women make up more than a quarter of the SSU's personnel, with more than 300 holding leadership positions, including those with the military rank of colonel, and two female leaders holding the rank of major-general. The SSU also adheres to the Methodological Guidelines on Preventing and Combating Gender Discrimination and Sexual Harassment in Law Enforcement Agencies and the Public Prosecutor's Office.

The SSU is modernizing the system of professional training and continuous professional development for the personnel. Educational programmes, postgraduate training mechanisms, academic disciplines, practical training and work placements are being renewed. The experience of countering modern threats and NATO member states' standards are taken into account. Special attention is paid to developing analytical skills, digital literacy and preparing personnel to operate in a highly volatile security environment.

The system for staffing and professional recruitment is being consistently improved. Modern approaches to recruitment are being introduced, procedures for searching, selecting and vetting candidates are being optimised, and the system of professional and psychological screening is being modernised. The SSU strengthens the staffing of operational and combat units and builds up a reserve of military-trained personnel. This allows the SSU to maintain an adequate staffing level in line with current security challenges and wartime needs.

The SSU has improved the system of psychological support for staff and introduced mechanisms to prevent occupational stress and burnout. Measures for psychological adaptation are carried out on an ongoing basis. Special attention is paid to supporting the families of deceased officers, ensuring their social support and state guarantees.

Meanwhile, veteran policy and the social reintegration of military personnel are being developed. New mechanisms for professional and social reintegration of veterans are being introduced, along with additional support programmes for SSU personnel and their families. Additionally, the SSU continuously monitors professional achievements and performance outcomes of its personnel. High levels of professionalism, initiative, perseverance and outstanding performance in carrying

out their duties have led to 654 the SSU officers receiving state honours.

Since the beginning of the full-scale invasion, 30 SSU officers have been awarded with the title of Hero of Ukraine by the President of Ukraine, and granted the Order of the 'Golden Star' in recognition of their personal courage and heroism in defending Ukraine's state sovereignty and territorial integrity, and their selfless service to the Ukrainian people. Unfortunately, 12 SSU employees were awarded with this title posthumously.

Overall, the personnel policy of the SSU seeks to establish an up-to-date, professional and stable human resource management system capable of ensuring the effective fulfilment of national security tasks in the context of a long-term war, hybrid threats and ongoing changes in the security environment..

4.2. IMPLEMENTATION OF THE ANTI-CORRUPTION PROGRAMME BY THE SSU

The SSU's anti-corruption policy is implemented in accordance with Ukrainian laws 'On the Prevention of Corruption' and 'On the Security Service of Ukraine', taking into account approaches and standards of NATO Building Integrity Programme. At the same time the corrupt prevention system combines external control mechanisms with internal means of promoting integrity.

Every three years, the Security Service of Ukraine adopts an Anti-Corruption Programme. In 2025, the SSU conducted a comprehensive assessment of corruption risks and adopted the Anti-Corruption Programme for 2025–2027. This document outlines legal, organisational, educational and preventive measures to counter and prevent corruption. The programme provides for mechanisms to assess and mitigate corruption risks in the SSU's activities.

In accordance with the Anti-Corruption Programme, the SSU has approved the Action Plan for Training and Dissemination of Information on Anti-Corruption Programmes within the Security Service of Ukraine for 2025–2027 as well as the Register of Corruption Risks of the Security Service of Ukraine.

THE SSU'S NEW ANTI-CORRUPTION PROGRAMME FOR 2025–2027 ENVISAGES TO ELIMINATE (OR MINIMISE) 15 CORRUPTION RISKS WITHIN THE SSU SYSTEM. THE MOST VULNERABLE AREAS TO CORRUPTION INCLUDE:

- ◆ human resources management;
- ◆ operational, investigative and counterintelligence activities;
- ◆ pre-trial investigations;
- ◆ management of material resources;
- ◆ procurement;
- ◆ expert activities;
- ◆ authorisation procedures relating to state secrets.

SSU constantly monitors the implementation of the Anti-Corruption Programme. Semi-annual reports for 2025 were submitted by the designated SSU unit responsible for the prevention and detection of corruption and published on the NACP Integrity Portal.

SSU constantly monitors the implementation of the Anti-Corruption Programme. Semi-annual reports for 2025 were submitted by the designated SSU unit responsible for the prevention and detection

of corruption and published on the NACP Integrity Portal.

The implementation of practical internal control mechanisms and the digitalisation of anti-corruption processes is ongoing. In particular, in 2025, the development of the 'Declaration Verification' software and hardware system was completed and launched. It is designed to carry out logical and arithmetic checks on the completeness and accuracy of declarations submitted by the SSU personnel. Control mechanisms were also improved in the areas of procurement, vetting of counterparties, management of military assets, and carrying out of forensic examinations.

Substantial attention was paid to the prevention of corruption offences and increasing integrity of personnel. Throughout 2025, more than 6,000 the

4.3 INTEGRITY

Ensuring integrity is a fundamental principle and an essential prerequisite for the effective operation of the SSU enhancing public trust and increasing resilience to internal and external threats.

Competency models, professional training systems and integrity mechanisms are implemented in accordance with the Concept of Personnel Policy in the Security Service of Ukraine for the period up to 2028 and the Rules of Professional Ethics and Integrity for Servicemen of the SSU. Integrity mechanisms are embedded into all levels of human resources management and form an integral part of the system for making personnel decisions.

There are Rules of Professional Ethics and Integrity for Military Personnel operating in the SSU. They set out unified standards of professional conduct for personnel, strengthen corporate culture, uphold integrity and help to increase public trust in the Service. Compliance with these Rules is taken into account when promoting servicemen.

These rules enshrine the principles of patriotism, rule of law, professionalism, integrity, independence, personal responsibility, political neutrality and gender equality. Special attention is paid to

SSU officers underwent training on anti-corruption legislation, conflicts of interest, codes of ethical conduct and international standards in the field of corruption prevention. Consultations and briefings were held on the submission of declarations, the resolution of conflicts of interest and the protection of whistleblowers.

The SSU also maintains internal and external channels for communicating corruption offences, including the Unified Whistleblower Reporting Portal, the SSU's official communication channels, and the option to contact specially authorised bodies in the field of preventing corruption (the Public Prosecutor's Office, the National Police, the National Anti-Corruption Bureau, the National Agency for Corruption Prevention) or the State Bureau of Investigation

the protection of human rights, elimination of conflicts of interest, adherence to ethical standards of communication, and the maintenance of a healthy moral and psychological climate within personnel.

Issues of integrity, accountability, transparency and other standards of professional ethics have been incorporated into the courses 'Countering Systemic Threats to State Governance' and 'Ensuring Integrity in Ukraine's Security Sector' at the National Academy of the SSU, and into the courses 'Organisational and Legal Foundations of the SSU's Activities', 'Professional Responsibility of a Lawyer' and 'The European Convention for the Protection of Human Rights and Fundamental Freedoms and Legal Practice' at the SSU Institute of Yaroslav Mudryi National Law University.

Further development of the integrity assurance system, improvement of comprehensive personnel assessment mechanisms and the introduction of modern standards of professional ethics will be implemented in accordance with the SSU Development Strategy for 2025–2030 and the Concept of Personnel Policy in the Security Service of Ukraine for the period up to 2028..

CHAPTER 5. ACCOUNTABILITY, TRANSPARENCY AND RESOURCE SUPPORT

5.1. PUBLIC COMMUNICATION, TRANSPARENCY AND INTERACTION

DEMOCRATIC CIVIL CONTROL AND OPEN TRANSPARENT COMMUNICATION BETWEEN THE SSU AND SOCIETY STRENGTHENS TRUST IN STATE INSTITUTIONS AND SUPPORTS THE SYSTEM OF DEMOCRATIC CIVIL CONTROL. AT THE SAME TIME THESE PROCESSES ARE CARRIED OUT CONSIDERING THE PARTICULARITIES OF THE SECURITY SERVICE ACTIVITIES, THE NEED TO PROTECT INFORMATION WITH RESTRICTED ACCESS AND THE MARTIAL LAW PERIOD.

According to the Law of Ukraine 'On the Security Service of Ukraine', the SSU regularly reports to the President of Ukraine, the National Security and Defence Council of Ukraine and other designated officials on its key activities, whilst the Head of the SSU submits annual written reports on the work of the SSU to the President of Ukraine and the Verkhovna Rada of Ukraine.

Ongoing parliamentary oversight over the SSU's activities is exercised by the Verkhovna Rada of Ukraine, which may hold parliamentary hearings and interview officials from the security and defence sector on matters of public interest.

To keep the public informed about the SSU's activities as a part of the security and defence sector of Ukraine, the SSU releases



public reports containing information on its main activities, performance and the development of the Service's institutional capacity.

COMMUNICATION AND SHARING INFORMATION ON THE SSU'S ACTIVITIES

The SSU's public communications system has been adapted to the circumstances of martial law and current hybrid threats. The SSU shares information with the public via its official website, verified social media pages and channels, press, and other communication channels. The SSU's digital resources regularly publish and update information on the Service's mission and priorities, results of its work in various areas, budget spending, public procurement, enrolment procedures for departmental educational institutions, service requirements and contact details.

During the year, the SSU publishes approximately **1 000 press releases** on its official website. Taking into account

the updates published by its regional offices at the local level, that total number exceeds **4 000**.

The audience for the SSU's digital resources is among the largest of Ukraine's security and defence agencies, with individual news items reaching up to **80 million** impressions within a 24-hour period.

The SSU maintains effective engagement with the media, bloggers, and opinion leaders. The Service regularly holds meetings with media representatives, provides comments and clarifications, supports the preparation of journalistic materials, including those produced by foreign journalists and international media outlets.

ENGAGEMENT WITH THE PUBLIC AND FEEDBACK

The Security Service continuously processes reports and information received from the public. The data are used for assessing and mitigating potential threats to national security, while ensuring citizens' rights to submit requests and get access to information.

THROUGHOUT 2025 THE SSU RECEIVED:
24 113 citizens' appeals;
3 009 attorney requests;
1414 appeals and requests from Members of the Parliament of Ukraine and appeals from Committees of the Verkhovna Rada of Ukraine;
2 159 reports of possible criminal offences;
988 attorney motions;
1119 requests pursuant to the Law of Ukraine 'On Government Cleansing';
2 455 documents received by the SSU Central Directorate via the Unified Judicial Information and Telecommunication System and its Electronic Office and Electronic Court subsystems.

The SSU official website includes the section dedicated to 'Access to Public Information' that outlines the categories of public information available, the procedure for submitting requests, and contact details. In 2025 the SSU processed and responded to 1,469 requests for public information. During 2025 the SSU helplines received 36,771 calls, showing a 23% increase compared with 2024. Following initial processing, relevant reports were forwarded to the appropriate SSU departments in accordance with their operational responsibilities. The reports covered issues including separatist activities, collaboration, attempts by the russian intelligence services to recruit Ukrainian citizens, espionage, enemy fire spotting, military offences, threats to information security, and other matters falling within the SSU's remit.

REPORTS RECEIVED (BY TOPIC):

443 Separatist activities	273 collaboration with russia	179 corruption schemes, incl. mobilisation evasion schemes	141 recruitment attempts
117 espionage/adjustment of enemy fire	79 military-related offences	78 threats to information security	58 offers to cooperate with the SSU
44 threats to carry out terrorist acts	43 complaints concerning SSU officers	39 movement/ deployment of enemy military equipment	32 illicit storage/trafficking of weapons and ammunition
28 PoWs and missing persons	21 reports on russian military personnel and members of illegal armed formations	14 illegal border crossings	12 activities of religious organisations
11 sale of humanitarian aid	10 smuggling	290 other topics	

Over the past year, the SSU received 73,659 emails via its dedicated IP-address, callcenter@ssu.gov.ua. While,

6,983 of these messages were forwarded to relevant SSU units for operational follow-up..

SPECIALISED COMMUNICATION CHANNELS

Specialised digital channels and chatbots facilitate rapid interaction with citizens, enabling them to report war crimes, collaboration, russian intelligence recruitment attempts, enemy positions, and other national security threats. In particular, the @stop_russian_war_bot chatbot is

used specifically to gather information on russian war crimes, alongside other specialised communication channels via messaging apps, email, and a hotline.

13,398 reports were received via the Burn the FSB-man chatbot in 2025.

REPORTS RECEIVED (BY TOPIC):

4 985 offers to carry out arson	496 russia's recruitment attempts	365 separatism-related
269 offers to plant explosives	40 threats to carry out a terrorist act	3 328 other reports of interest to the SSU

INFORMATIONAL RESILIENCE AND COOPERATION WITH CIVIL SOCIETY

The Security Service tailors its communications to specific target audiences through daily briefings, interviews, documentaries, and themed information campaigns. Key initiatives include countering the recruitment of Ukrainian youth by the russian intelligence services, promoting service in the 'Alfa' Special Operations Centre, raising public awareness on security issues, and actively countering disinformation. In collaboration with the National Police and the Ministry of Education and Science of Ukraine, the SSU engages the media, bloggers, educators, and the general public in its nationwide information campaigns. Together with the Centre for Countering Disinformation, the SSU systematically identifies and exposes information manipulation, disinformation, and other hostile information campaigns aimed at destabilising the socio-political situation and undermining Ukraine's defence capabilities.

Overall, the SSU continues to develop a modern system of public communication, transparency, and accountability that is adapted to the conditions of martial law and the specific nature of its activities. This contributes to strengthening public trust, enhancing engagement with the public, and reinforcing the principles of democratic civilian oversight within Ukraine's security and defence sector. The effectiveness of these efforts and the high level of public confidence in the SSU are reflected in sociological surveys. According to a nationwide public opinion poll presented in September 2025 by the European Union Advisory Mission in Ukraine and the 'Rating' sociological group, the SSU ranked second in public trust among security institutions with a 78% trust level. At the same time, the research of the Kyiv International Institute of Sociology confirms that public trust in the SSU nearly doubled compared with 2021.

5.2 THE SSU BUDGET

ADEQUATE FUNDING OF THE SSU'S ACTIVITIES IS ESSENTIAL FOR MAINTAINING THE STATE'S DEFENCE CAPABILITY AND ENABLING THE SERVICE TO CARRY OUT ITS TASKS IN THE FIELD OF NATIONAL SECURITY. BUDGETARY RESOURCES ARE ALLOCATED TO SUPPORT OPERATIONAL ACTIVITIES, CAPABILITY DEVELOPMENT, LOGISTIC SUPPORT, SOCIAL PROTECTION FOR PERSONNEL, AND MEASURES TO COUNTER CURRENT NATIONAL SECURITY THREATS.

The expenditure of the Security Service of Ukraine for 2025, taking into account the amendments made, was approved at UAH 72 billion 936 million 111,5 thousand, out of which UAH 44 billion 165 million 889,0 thousand was allocated to the general fund. Consumption expenditure

under the general fund amounted to UAH 41 billion 827 million 111,3 thousand, development expenditure – UAH 2 billion 338 million 777,7 thousand.

The SSU cash expenditure under the general fund amounted to UAH 44 billion 120 million 97,7 thousand in 2025.

EXPENDITURE CATEGORIES BY PROGRAM CLASSIFICATION	PLANNED EXPENDITURE (UAH)	CASH EXPENDITURE (UAH)
Consumption expenditure, including:	41,827,111,300	41,805,205,000
Personnel compensation	32,667,284,400	32,667,283,900
Utility services and energy carriers	465,371,500	458,999,200
Development expenditure	2,338,777,700	2,314,892,600

The largest share of funding was allocated to the budget programme 'Ensuring Measures in the Field of State Security and the Activities of the Security Service of Ukraine', for which general fund cash expenditure amounted to UAH 43 billion 926 million 14,8 thousand.

Separate funding was provided for measures to coordinate activities to prevent terrorist acts and combat terrorism on the territory of Ukraine, with

cash expenditure from the general fund under this budget programme amounting to UAH 29 million 999,9 thousand.

Under the budget programme 'Construction (Purchase) of Housing for SSU Military Personnel', cash expenditure from the general fund amounted to UAH 164 million 82,9 thousand. The number of SSU service personnel on the housing waiting list fell by 10,7% – in 2025 – from 6 053 to 5 495.

BUDGET PROGRAMME	PLANNED EXPENDITURE (UAH)	CASH EXPENDITURE (UAH)
Ensuring measures in the Field of State Security and the Activities of the SSU	43,960,605,263	43,926,014,755
Coordination of Activities to Prevent Terrorist Acts and Combat Terrorism on the Territory of Ukraine	30,000,000	29,999,997
Construction (Purchase) of Housing for SSU Military Personnel	175,283,737	164,082,916

5.3 AUDIT

THE SSU'S INTERNAL AUDIT EVALUATES THE EFFECTIVENESS OF INTERNAL CONTROLS, RISK MANAGEMENT, AND THE USE OF BUDGETARY FUNDS, STATE PROPERTY, AND OTHER ASSETS.

It also verifies legal compliance across all SSU operations - particularly within counterintelligence and operational-investigative activities. Ultimately, the internal audit strengthens management efficiency, optimises internal controls, mitigates operational risks, and ensures rigorous accountability.

The SSU internal audits are built on independence, objectivity, and a systematic, risk-based approach - fully aligning with European public internal financial control standards, good governance, and accountability. Based on audit findings, actionable recommendations are developed to rectify deficiencies, optimise internal procedures, and enhance overall operational effectiveness.

In 2025, the SSU's internal audit unit conducted 18 audits across various agency bodies and units. Concurrently, the Service introduced IT auditing practices to assess the reliability, efficiency, and overall effectiveness of its information systems and technologies.

Based on the audit findings, recommendations were made to improve the internal control and management system, enhance the efficient use of budgetary resources and assets, minimise the risk of irregularities, and rectify the identified shortcomings.

Furthermore, pursuant to Article 26 of the Budget Code of Ukraine, the SSU took measures to ensure the effective functioning of its internal audit system and the SSU Audit Committee.

5.4 PUBLIC PROCUREMENT AND LOGISTICAL SUPPORT

In 2025 the SSU's procurement and logistical support activities were focused on ensuring the timely and uninterrupted provision of the resources required for the Service's units to carry out their duties. Public procurement was conducted in accordance with the applicable legislation, while taking into account the legal regime of martial law. At the same time, procurement procedures reflected the SSU's specific role as a specialised state body responsible for national security. Attention was therefore paid to striking an appropriate balance between ensuring the openness and transparency of procurement procedures and safeguarding information with restricted access.

Procurement within the SSU was carried out in accordance with the principles of fair competition, the efficient use of budgetary

funds, openness, transparency, and equal treatment of all participants. Suppliers were selected through objective and impartial procedures, with due regard for measures to prevent corruption and other abuses. At the same time, procurement processes were organised in a manner that safeguarded information relating to state security, as well as other information with restricted access.

The development of the SSU's material resources and technical capabilities was carried out in response to current security challenges, the Service's operational needs, and the objectives set out in the SSU Development Strategy for 2025–2030. Information on public procurement, where disclosure is required by law, is published in the 'Prozorro' electronic public procurement system and on official websites within the scope prescribed by law.



CHAPTER 6 INTERNATIONAL COOPERATION

IN 2025, THE SSU'S INTERNATIONAL COOPERATION FOCUSED ON THE PROFESSIONAL TRAINING OF PERSONNEL, DEVELOPMENT OF INNOVATIVE AND TECHNOLOGICAL CAPABILITIES, COOPERATION IN THE FIELD OF INTERNATIONAL CRIMINAL JUSTICE, DOCUMENTATION OF WAR CRIMES, COUNTERING CONTEMPORARY GLOBAL THREATS, STRENGTHENING THE PROTECTION OF CRITICAL INFRASTRUCTURE, AND OTHER PRIORITY AREAS..

6.1 COOPERATION WITH THE EUROPEAN UNION

THROUGHOUT 2025 SSU PERSONNEL PARTICIPATED IN TRAINING PROGRAMMES CONDUCTED UNDER THE AUSPICES OF THE EU MILITARY ASSISTANCE MISSION TO UKRAINE (EUMAM) AND COMPLETED 35 SPECIALISED PRACTICAL TRAINING COURSES.

The training programmes covered combat medic training, including training for field surgeons, combat engineering and EOD training, de-mining instructor training, command and staff, and K9 handling courses.

In December 2025 the Security Service, in cooperation with the European Commission under the TAIEX programme, co-organised a workshop on cross-sectoral cooperation in responding to cyber threats, development of public-private partnerships in cybersecurity, and information-sharing on cyber incidents. The workshop provided a platform for the practical exchange of expertise between representatives of Ukrainian public authorities and experts from EU Member States, strengthening the cooperation in responding to contemporary cyber threats.

In 2025 the SSU continued its systematic cooperation with the EU Advisory Mission on Civilian Security Sector Reform Ukraine (EUAM Ukraine). SSU personnel



participated in 33 training courses and workshops covering the investigation of international crimes, counterterrorism, cybersecurity, risk management, intelligence analysis, OSINT methods and tools, virtual asset tracing, and internal control and external oversight.

6.2 COOPERATION WITH NATO AND ACTIVITIES WITHIN THE JATEC

In 2025 joint research with the participation of the SSU was conducted within the framework of the NATO-Ukraine Joint Analysis, Training and Education Centre (JATEC), focusing on countering modern air-to-ground weapons and unmanned systems, including glide bombs and fibre-optic-controlled FPV drones. The Security Service of Ukraine also participated in the NATO REPMUS/Dynamic Messenger exercises, marking an important milestone in strengthening operational interoperability with the Alliance.

The Security Service of Ukraine and the Armed Forces of Ukraine, together

with NATO partners, participated in testing artificial intelligence and machine learning models designed to enhance situational awareness, analyse data on enemy activities, and to predict potential threats.

The protection of critical infrastructure remained a key focus of Ukraine-NATO cooperation. At the SSU's initiative, an international workshop was held in 2025, bringing together Ukrainian and Allied experts. The workshop resulted in the development of a set of 50 practical recommendations to enhance the resilience of critical infrastructure.

6.3 INTERNATIONAL CRIMINAL JUSTICE AND COOPERATION WITH INTERNATIONAL ORGANISATIONS

IN 2025 THE SSU COOPERATED EXTENSIVELY WITH INTERNATIONAL ORGANISATIONS AND INSTITUTIONS IN DOCUMENTING WAR CRIMES COMMITTED BY RUSSIA AND BRINGING THE PERPETRATORS TO JUSTICE. THE VERIFIED MATERIALS COLLECTED BY THE SERVICE CONTRIBUTED TO THE REPORTS OF INTERNATIONAL ORGANISATIONS, INCLUDING THE UNITED NATIONS, AND TO THE ESTABLISHMENT OF THE EVIDENCE BASE DOCUMENTING VIOLATIONS OF INTERNATIONAL HUMANITARIAN LAW AND INTERNATIONAL CONVENTIONS.

Investigators of the SSU Main Investigation Directorate continued to collect evidence in criminal proceedings on crimes against Ukraine's national security, peace, human security, and the international legal order, stemming from Russia's military aggression. These findings are used to build cases against senior military and political leaders of the aggressor state. As a part of international cooperation, SSU investigators collaborate closely with the International Criminal Court (ICC), the Joint Investigation Team (JIT), the International Centre for the Prosecution of the Crime of Aggression against Ukraine, and the Organisation for the Prohibition of Chemical Weapons.

In 2025 the Security Service of Ukraine processed thematic requests from the ICC to document and gather evidence of international crimes committed by Russia. Key focus areas included massive missile strikes on civilian and energy infrastructure, the unlawful deportation of Ukrainian children, and international humanitarian law violations against Ukrainian prisoners of war. The compiled evidentiary materials were subsequently forwarded to the ICC Office of the Prosecutor via the Prosecutor General's Office of Ukraine.

As a part of the JIT, the SSU, in collaboration with the law enforcement agencies of the Republic of Lithuania, documented war crimes committed by Russian servicemen against captured citizens of Ukraine and Lithuania.

As a result, a Russian serviceman, G., who was captured in the Zaporizhzhia region, was notified of his status as a suspect in the

commission of war crimes and extradited to Lithuania. There, he was remanded in custody on suspicion of committing war crimes against civilians and prisoners of war, torture, and violations of the laws and customs of war.

In addition, based on evidence provided by the SSU, a Russian citizen, Yan Petrovsky, was detained in Finland and sentenced to life imprisonment for committing war crimes in Ukraine.

The SSU also participates in the work of the International Centre for the Prosecution of the Crime of Aggression against Ukraine (ICPA), which serves as a platform for building the evidence base for the future Special Tribunal for the Crime of Aggression against Ukraine. As a part of this work, evidence is being systematised, while command-and-staff documentation, open-source information, and materials from criminal proceedings are analysed to prepare indictments against members of Russia's senior military and political leadership.

One of the tasks carried out by SSU investigators within the ICPA is the preparation of model indictments against specific members of Russia's senior military and political leadership who may bear responsibility for the crime of aggression. To support this work, investigators analyse open-source information alongside evidence collected during criminal proceedings. They also organise, classify and upload evidentiary materials to Eurojust's Core International Crimes Evidence Database (CICED) and exchange information with other ICPA participants.

As a part of the ICPA's work, SSU

investigators, in cooperation with military experts from the Interagency Working Group under the Prosecutor General's Office, have conducted a large-scale investigation and gathered a substantial body of evidence. This evidence documents the spatial and temporal development of military operations on the territory of Ukraine from 24 February 2022 to the present, as well as the strategies and tactics employed by the aggressor state.

Cooperation with the Organisation for the Prohibition of Chemical Weapons (OPCW) has become a distinct area of the SSU's international engagement. In 2025 the OPCW Technical Secretariat published the results of its analysis of evidence submitted by Ukraine, confirming Russia's systematic use of chemical weapons against the Ukrainian Defence Forces. These findings constitute a proof of a serious violation of the Chemical Weapons Convention of 13 January 1993.

Based on this evidence, the Council of the European Union has imposed additional sanctions on the relevant individuals and legal entities of the aggressor state. It has also called on the OPCW to initiate the attribution process to determine whether there exist sufficient grounds to establish Russia's international legal responsibility for the use of CS tear gas during hostilities on the territory of Ukraine.

On 24 July 2025, based on the evidence collected by SSU investigators, 41 participating States of the Organisation for Security and Cooperation in Europe activated the Moscow mechanism to examine Russia's treatment of Ukrainian prisoners of war. The expert mission presented its findings to the OSCE Permanent Council in a report entitled 'Report on Possible Violations and Abuses of International Humanitarian and Human Rights Law, War Crimes and Crimes Against Humanity, Related to the Treatment of Ukrainian POWs by the Russian Federation'. The report also contains recommendations on appropriate mechanisms for ensuring accountability for those responsible for such crimes.



Together with international experts, SSU investigators implement modern approaches to working with victims of war-related violence, including the application of trauma-informed methodologies aligned with international human rights standards. These approaches enhance the effectiveness of documenting war crimes while ensuring a people-centred approach and protecting the safety of victims.

Alongside these efforts, the Service's strategic priority remains proactive efforts to anticipate and prevent emerging global threats. A distinct area of international cooperation is the SSU's participation in projects aimed at countering radiological, chemical and nuclear threats. The Security Service contributes to international initiatives focused on risk assessment, development of early warning and detection mechanisms, and training of specialists in the area of non-proliferation of hazardous materials.

CONTACTS

HOTLINE:

1516

EMAIL INBOX FOR CITIZENS' APPEALS

callcenter@ssu.gov.ua

POSTAL ADDRESS:

33 Volodymyrska Street
Kyiv 01601
Ukraine

FOR FURTHER CONTACT
DETAILS, VISIT THE SSU
WEBSITE

SSU ONLINE:

FACEBOOK
YOUTUBE
TWITTER
INSTAGRAM
TELEGRAM



SECURITY SERVICE OF UKRAINE