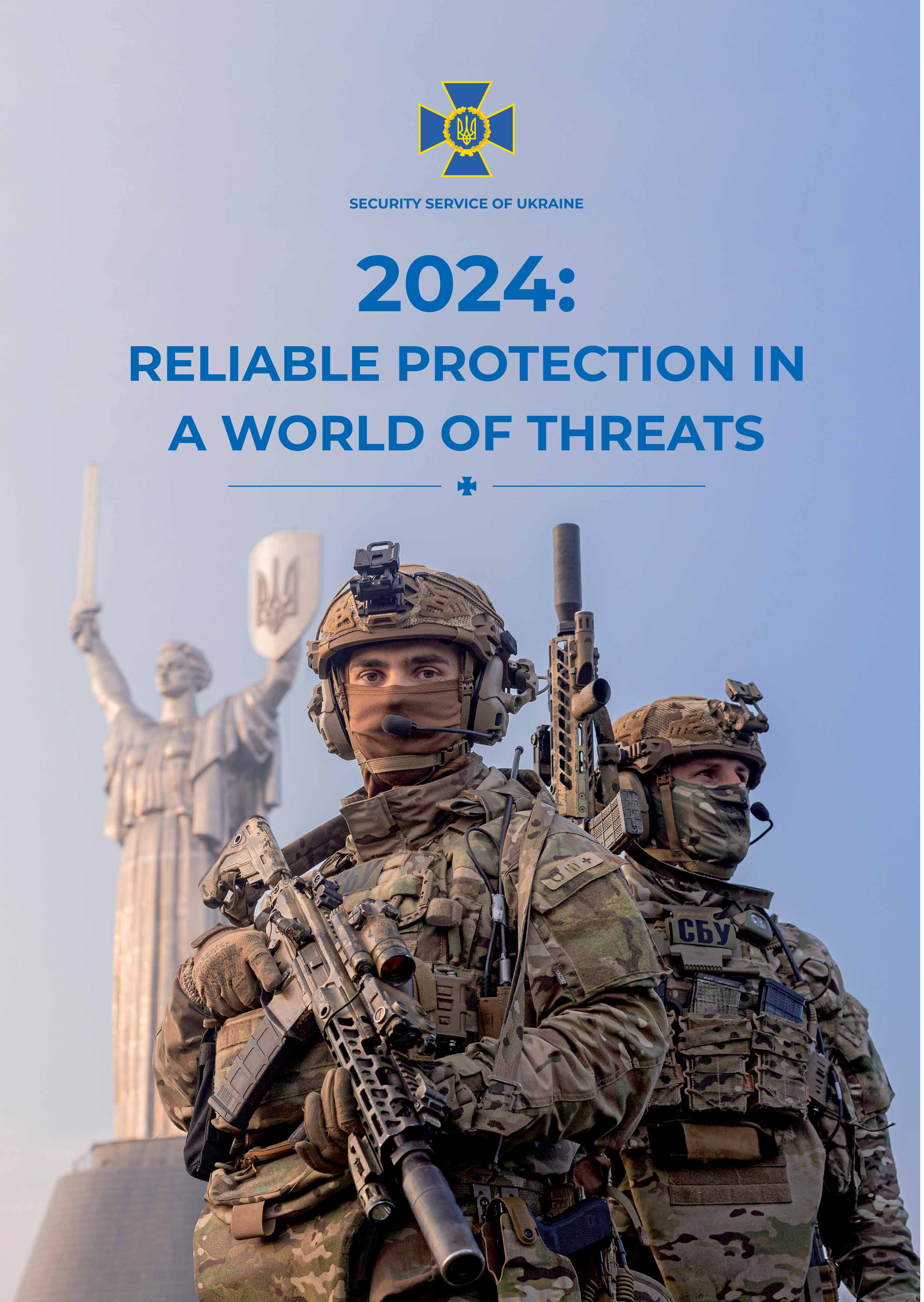
SECURITY SERVICE OF UKRAINE

2024:
RELIABLE PROTECTION IN A WORLD OF THREATS



CONTENTS

FOREWORD BY THE HEAD OF THE SSU

Dear Ukrainians, colleagues, friends and partners!

For more than three years, the SSU, together with other security and defence forces, has been mercilessly destroying the occupiers on the battlefield and weakening the military potential of the russian federation. At the same time, it performs the functions of a classic secret service, protecting the security of the state from an insidious and powerful enemy.

During this time, the Security Service has reorganised its work to respond as effectively as possible to any emerging challenges. We have become flexible, technologically advanced and mobile. It is because modern warfare has significantly changed the nature of threats, and our enemy regularly resorts to terrorist methods.

Today SSU is a secret service of a country that is fighting and defending its independence.

We are fulfilling our mission with dignity and have achieved real results in every area. We are implementing unique and ambitious plans that are changing the tide of the war.

For example, the unprecedented special operation called Spiderweb. SSU drones simultaneously demilitarised one-third of russian strategic aviation, striking 41 aircraft at key russian airbases.

We also struck the Crimean Bridge for the third time, mining its underwater pillars. This illegal structure was, is, and will always remain our legitimate target.

Every special operation carried out by the SSU proves that we will strike the enemy even in places where they consider themselves invulnerable.

Today SSU warriors, in particular the special forces of the Special Operations Centre “A”, are masterfully operating all types of drones. Throughout 2024, our fighters destroyed thousands of enemy military vehicles on the front lines and dozens of military facilities in the rear of the russian federation. We are doing everything to destroy the russian economy and disrupt the war logistics. The SSU military counterintelligence officers are successfully employing new modifications of Sea Baby maritime drones. Counterintelligence regularly exposes and detains traitors, collaborators, and russian agents operating within our society. Investigators are gathering high-quality evidence to ensure that every traitor and war criminal receives the punishment they deserve, no matter where they hide from justice.

Every aspect of the SSU work – combat missions, special operations, counterintelligence, cyber defence, coordination of Prisoner of War exchanges, and investigations – is our daily contribution to the country's defence. Secret service officers fight and work with utmost dedication, aware of their responsibility to the Ukrainian people and the state.

I am grateful to the Security Service staff for their professionalism and patriotism. We are currently gaining unique experience that no other secret service in the world has. Every day we are ready to carry out tasks that bring us closer to the end of the war and further reconstruction of our state.

Glory to Ukraine!

Head of the Security Service of Ukraine,
Lieutenant General
Vasyl MALIUK

MISSION, VISION, PRINCIPLES AND VALUES OF SECRET SERVICE

MISSION:

- protect the Ukrainian people and national interests of Ukraine;
- uphold the constitutional order, ensure state security;
- create conditions for Ukraine's strategic advantage in the world.

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

OUR 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 countries;
- corporate unity.

OUR PRINCIPLES:

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

DIRECT SPEECH: VASYL MALIUK REGARDING UNIQUE SPECIAL OPERATIONS OF THE SSU

Regarding the third attack on the Crimean Bridge

"God loves the Trinity, and the SSU always accomplishes what it intends to do and never repeats itself. We have previously targeted the Crimean Bridge twice, in 2022 and 2023. Thus, today we continued this tradition, this time underwater. There is no place for any illegal russian objects on the territory of our state. Therefore, the Crimean Bridge is a completely legitimate target, especially considering that the enemy used it as a logistical artery to supply its troops. Crimea is Ukraine, and any manifestations of occupation will meet strong response from us."

BBC Ukraine,
3 June 2025

Regarding the drone-assault operation carried out by the SSU in Kursk in August 2024

"We carried out a successful drone assault operation in Kursk: we captured 103 enemy servicemen, including those from Akhmat and, respectively, officers. It was a very difficult assault on a real underground fortress, where the enemy had entrenched themselves and were waiting for our arrival, ready to fight as fiercely as possible. In fact, that is what they did, but with the help of drones and assault troops, we managed to take them alive. A certain number, of course, died in battle, but the vast majority were captured alive, and in fact, we will exchange them for our heroes."

TV channel 'We Are Ukraine',
11 October 2024

Regarding the special operation Spiderweb that destroyed 41 russian strategic aircraft

"The destruction of enemy bombers is a task set before us by the President of Ukraine, Supreme Commander-in-Chief Volodymyr Zelenskyy. He personally supervised the special operation prepared by the Security Service. The enemy bombed our country almost every night using these aircraft, and today they have felt that retribution is inevitable. In total, 34% of strategic cruise missile carriers at the main russian airbases – Bielaia, Diahilievo, Olenia and Ivanovo – were destroyed. This was not just a devastating blow to enemy aviation, but a serious slap in the face to the power and terrorist nature of the russian federation."

TV Channel '1+1',
2 June 2025

Regarding the deterrence of russia in the Black Sea

"When talking about the maritime component, it is worth mentioning that 2024 was quite a difficult year. However, together with our colleagues from the Defence Intelligence of Ukraine, we achieved a lot at sea: we did not allow russian federation to re-establish its dominance there.

Today, our drones are not just drones operating in kamikaze mode, but multi-purpose platform carrying machine gun armament, FPV drones and other equipment, and are also used for remote mining."

Forum 'Ukraine. Year 2025',
23 February 2025

Regarding the detention of a traitor, recruited by the russian fsb

"The traitor had been under investigation by the SSU's internal security officers for a long time. We practically surrounded him on all sides, monitoring his every move 24/7 – his contacts, communications, correspondence. We literally 'lived' in his phone, and he was under constant audio and video surveillance. Neutralising such a traitor is, without exaggeration, a historic special operation, given the agent's level, his professional training and the scale of damage he could potentially cause to state security during the war. The case was under my personal supervision, and I reported on the development and implementation of the special operation to the Supreme Commander-in-Chief, President of Ukraine Volodymyr Zelenskyy, who was aware of all the details".

TV channel '1+1',
12 February 2025

Regarding the sea drone missions

"One of our missions – when SSU maritime drones hit a barge carrying military equipment in the Kerch Bay. The distance there was more than 700 km, and we were spotted already at a one-third of that distance. So our sea drones covered the rest of the distance under constant fire from enemy aircraft. But they couldn't get close enough to destroy us because our systems were working, including artificial intelligence."

Forum «Ukraine. Year 2025»,
23 February 2025

Regarding the use of UAVs on the front line and in the russian rear

"The President of Ukraine set a task before us, and we developed the appropriate methodology and tactics for using unmanned aerial systems. The SSU operates on the front line and 20 km, 20-40 km, 40-80 km, 80-120 km and 120+ km behind enemy lines. The 120+ km range is a so-called deep strike – long-range operations. We have trained professional operators for each range and distance and have the appropriate means of destruction. The work of combat UAVs is, in essence, 85% destruction of the enemy's manpower, combat equipment and armoured vehicles".

Forum «Ukraine. Year 2025»,
23 February 2025

Regarding the impact of long-range drones on military facilities in the russian rear

"The missile and drone attacks carried out by the enemy are acts of terrorism. We, in turn, choose only legitimate targets. Among the targets we have successfully hit are 48 military targets, including ammunition depots and airfields with military aircraft. Everyone remembers the depots in the town of Toropets, which exploded very loudly, causing four earthquakes.

160,000 tonnes of enemy ammunition were destroyed, including half of all stocks of 120 mm mines, which are essentially like hot pies for their soldiers. And there are many, many such special operations."

«24 Channel»,
23 February 2025

THE SSU'S CONTRIBUTION TO NATIONAL DEFENCE

From the very first days of the full-scale invasion, the SSU servicemen stood up to defend their country and have been fighting in the hottest spots on the front line ever since

In particular, combat missions on the battlefield are carried out by fighters from the SSU Special Operations Centre ‘A’, military counterintelligence, counterintelligence departments and other units. Their tasks include destroying enemy equipment and personnel, conducting assault operations, reconnaissance, fire correction and providing reliable fire support to their brothers-in-arms in the Defence Forces.

This allows intelligence services to effectively carry out the tasks assigned by the Supreme Commander-in-Chief on the front line, in the Black Sea and deep in the enemy rear.

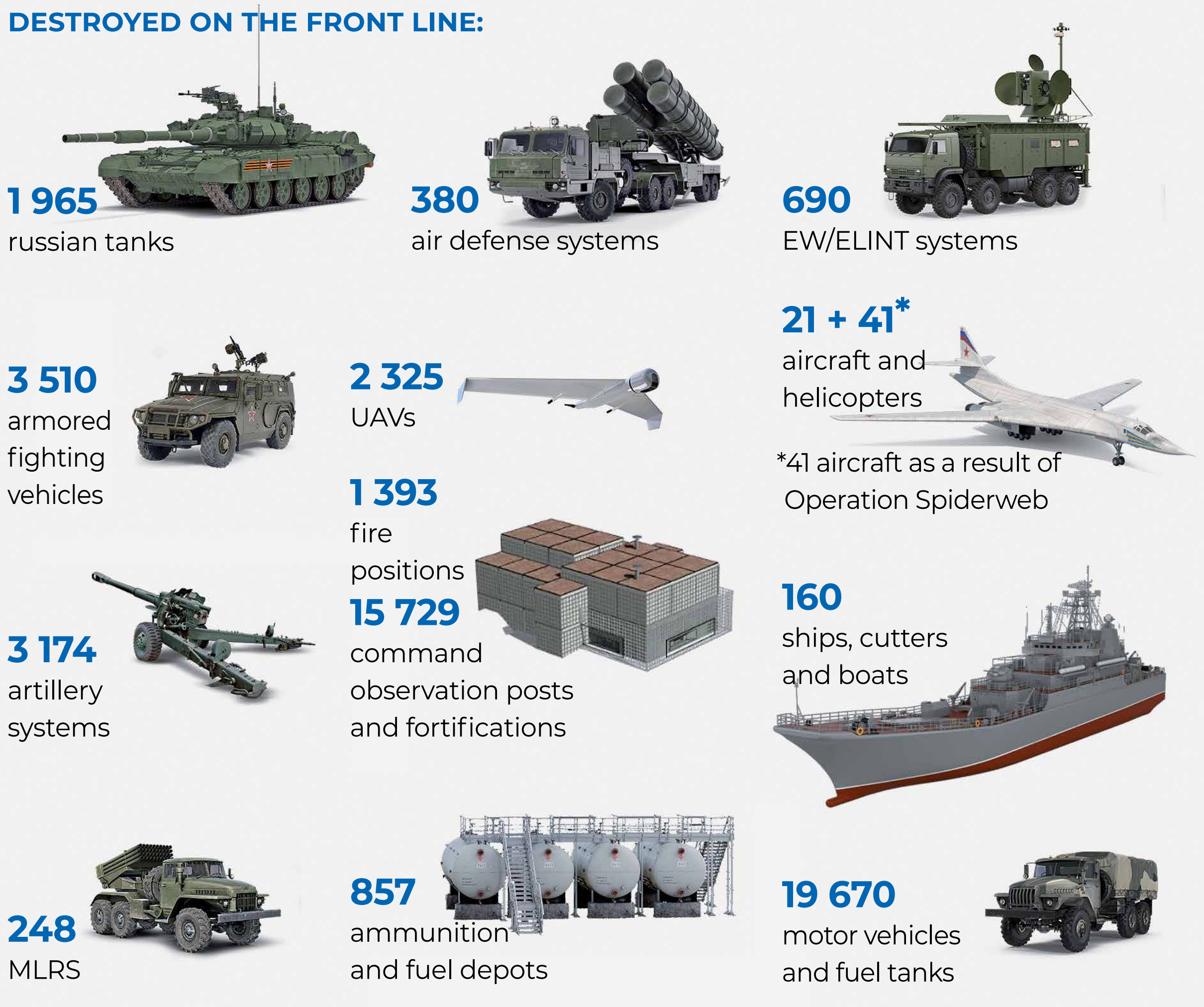
In 2024, SSU servicemen continued to intensify their efforts to defeat the enemy.

The integration of modern developments in the field of intelligence, automation and precision strikes allows them to respond even faster to changes on the front line and inflict significant losses on the enemy.

In fact, every sixth tank destroyed by the Defence Forces on the battlefield is the result of the Security Service work. And the Service special forces regularly head the rating of the most effective units in destroying enemy equipment using drones.

While performing combat missions on the front line, SSU soldiers pay particular attention to destroying strategic enemy targets – expensive air defence systems, electronic warfare systems and radar stations, such as Nebo-U, Nebo-M, Kasta and others.

FROM 24 FEBRUARY 2022 AND TO THE BEGINNING OF JUNE 2025, THE SSU UNITS DESTROYED ON THE FRONT LINE:



1 965 russian tanks

380 air defense systems

690 EW/ELINT systems

3 510 armored fighting vehicles

2 325 UAVs

21 + 41* aircraft and helicopters

*41 aircraft as a result of Operation Spiderweb

1 393 fire positions

15 729 command observation posts and fortifications

3 174 artillery systems

160 ships, cutters and boats

248 MLRS

857 ammunition and fuel depots

19 670 motor vehicles and fuel tanks

For example, the SSU cyber experts in cooperation with other units of the Armed Forces, used several FPV drones to destroy a $25 million “Zoo” counter-battery radar station. This complex is quite rare in the enemy's army. Its main purpose is reconnaissance and detection of ground artillery systems, in particular barrel artillery and MLRS.

The SSU has also set up effective anti-drone units that destroy enemy tactical-level UAVs such as Supercam, Orlan, Zala and Lancet on the front line. According to the SSU Chairman Vasyl Maliuk, Ukrainian FPV drones costing $700 are used to destroy these russian drones, which are worth $100,000 each. ‘There were days when we destroyed more than 20 reconnaissance drones in the Kursk region within a day. In other words, where the enemy is using ‘big know-how’, we simply find the solution to these issues,‘ said Vasyl Maliuk.

A separate area of work undertaken by the SSU Cyber Security Department is the detection and destruction of enemy operators who control reconnaissance drones. Since 2024, SSU cyber specialists have managed to strike more than 50 command and control centres for such UAVs.

In addition, the Security Service is actively transferring the war to enemy territory, carrying out targeted strikes on military facilities to disrupt logistics and weaken the military and economic potential of russia.

Thus, during the period of full-scale hostilities, the Security Service destroyed a total of 190 strategically important targets in the enemy's rear (as of mid-April 2025). These include military airfields, ammunition depots, weapons arsenals, military-industrial complex enterprises involved in the production of drones, missiles and guided aerial vehicles, as well as oil and gas and oil refining facilities, the proceeds from which are used to finance the war.

For example, drones struck the airfields of Khanska, Voronezh, Kursk, Savasleika, Borisohlebsk, Shaikovka, Marynivka, Lipetsk-2, Morozovsk and others, where russian fighter jets were stationed and ammunition was stored for missile and drone strikes on Ukrainian territory.

Such special operations are carried out by the SSU fighters using long-range drones capable of covering distances of over 1,500 km. These are so-called deep strikes, each of which is aimed at disrupting enemy supply chains (moving combat units to the front, supplying the army with fuel and lubricants, reducing stocks of weapons for missile and drone strikes on Ukrainian territory). Taken together, all this complicates the russian army's ability to manoeuvre effectively, conduct combat operations and coordinate units.

As a result of drone strikes by the Defence Forces on oil refining and production facilities, russian enterprises suffered billions losses, including lost profits.

Gaining unique combat experience every day, the Security Service of Ukraine is constantly improving and adapting to new conditions. It uses modern technologies to find the enemy's weak spots while minimising risks and saving the lives of Ukrainian defenders.

SSU – GENERATOR OF NEW MILITARY AND TECHNOLOGICAL SOLUTIONS

For the SSU, war began back in 2014, but at that time it was of a completely different nature – it was hybrid aggression with localized combat zones.

russia's invasion of Ukraine in 2022 posed a much greater threat, with a front stretching for thousands of kilometers. Therefore, the approaches to warfare and technical equipment used ten years ago cannot be compared to today's realities.

Although Ukrainian secret service began using unmanned technologies in the ATO zone in eastern Ukraine back in 2015 (mainly for reconnaissance purposes), it was during the full-scale war that the SSU became a generator of new military and technological solutions. It concerns not only the improvement of weapons and their adapting to modern warfare, but also to the development of strategies and planning of unique special operations changing the course of the war.

UNMANNED SURFACE VEHICLES

One of the areas of technological development is UAVs, which the SSU uses for combat missions not only on land but also at sea.

In October 2022, the first generation of surface drones were successfully employed in the Sevastopol Bay. Four russian military vessels were damaged, including the frigate Admiral Makarov. In fact, the SSU has launched a new maritime warfare strategy. Now many armies around the world are eager to adopt this experience.

Since then, with the help of unmanned surface vehicles, the Security Service has struck 11 russian military ships, as well as the Crimean Bridge in July 2023.

As a result of these actions, the Defense Forces managed to change the balance of power in the Black Sea in Ukraine's favor: russia lost its dominance and was forced to withdraw its most valuable military ships from Sevastopol Bay and hide them in Novorosiysk, while our state restored the ‘grain corridor’.

Currently the Security Service of Ukraine uses two types of marine drones – Sea Baby and Mamai – constantly improving them and adapting them to perform various combat tasks. Compared to the first prototypes, the current models of these drones have improved technical characteristics, greater combat power and maneuverability.

A distinctive feature of the modern Sea Baby is that it can be used not only as a kamikaze drone to strike enemy targets, but also as a multi-purpose platform for remote mining, naval combat, and other tasks.

For example in 2024, the SSU began installing Grad multiple launch rocket systems on Sea Babies, as well as large-caliber machine guns with ballistic programs for automatic targeting and target acquisition. And at the end of the year, it actually tested another way of using drones: several Sea Babies engaged in a naval battle with russian helicopters, aircraft, and Raptor patrol boats when they tried to destroy them.

russian radio communications intercepted by the SSU confirmed that there were casualties on board of the helicopters, which were significantly damaged and completely disabled.

UNMANNED TECHNOLOGIES ON THE BATTLEFIELD AND IN THE ENEMY'S REAR

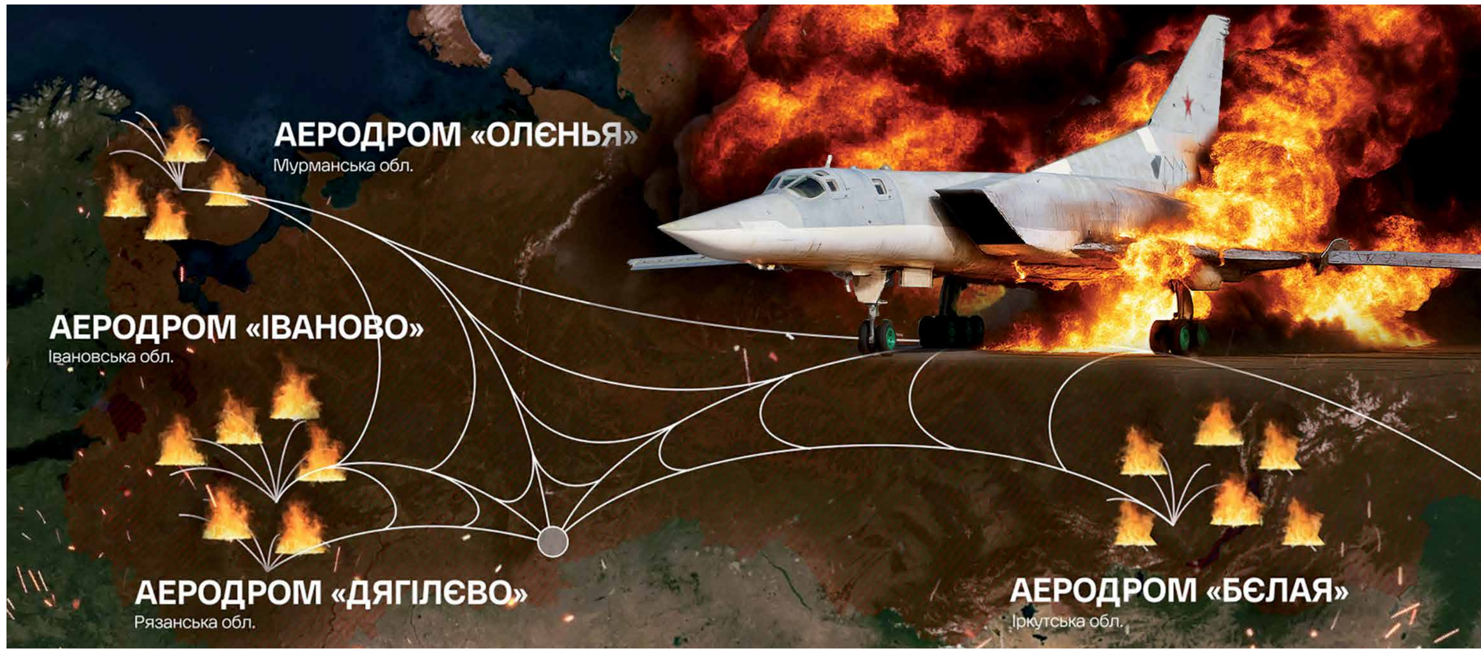
For the effective use of unmanned technologies on the front line and in the rear, the SSU has developed its own unique methods and tactics. These involve the use of various types of UAVs and ammunition for clearly defined distances and targets, as well as high-quality training for the relevant control teams.

In particular, on the front line, the distances for drone operations are ranged as follows: up to 20 km, from 20 to 40 km, from 40 to 80 km, and from 80 to 120 km. While to destroy military targets at distances of more than 120 km, SSU officers use long-range drones.

The SSU is also working on using artificial intelligence to program drones so that they can independently track and strike targets even in non-standard conditions, such as loss of communication with the pilot, difficult terrain, etc.

In developing unmanned technologies, the secret service is working not only to improve their technical characteristics, but also to improve the whole system. After all, when planning and implementing special operations, especially in the deep strike format, every element is important: high-quality reconnaissance and pre-reconnaissance, massive technical penetration and reconnaissance of the target, synchronization of control commands and drone launch timing, unhindered passage of own air defense systems, and neutralization of enemy air defense systems with false targets.

SPECIAL OPERATION “PAVUTYNA” (SPIDERWEB)



With the help of unmanned technologies, on June 1, 2025, the SSU conducted an unprecedented and unique special operation called Spiderweb to strike simultaneously four military airfields in the rear of the russian federation, where enemy strategic aviation is deployed.

As a result of the drone strikes, 41 aircraft were hit, including A-50, Tu-95, Tu-22 M3, and Tu-160.

The SSU task force that had been preparing the special operation “Spiderweb” for over a year and a half was headed by the Head of the Security service, Lieutenant General Vasyl Maliuk. Its course was personally supervised by the President of Ukraine, Supreme Commander-in-Chief Volodymyr Zelenskyy.

As a result, SSU drones targeted the main russian airfields – Belaia, Diagilevo, Olenia, and Ivanovo. Thanks to the plan, it became possible to strike simultaneously the largest number of enemy aircraft – 34% of strategic cruise missile carriers. The estimated cost of the destroyed aircraft is over $7 billion. "The most important thing you have proven with the brilliant operation “Spiderweb” is that war causes tangible damage and losses to the aggressor as well, and this is what restores justice and compels the aggressor to true peace. russia realizes its responsibility for its actions only when you and our other soldiers are taking action," emphasized Ukrainian President Volodymyr Zelenskyy.

For the implementation of this special operation, the Head of State awarded SSU officers, one of the servicemen was granted the title of Hero of Ukraine.

The special operation “Spiderweb” took place simultaneously in three time zones and was extremely complex from a logistical point of view.

At first, the SSU transported FPV drones to russia, followed by modular wooden houses. Once in russia, the drones were hidden under the roofs of the houses, which were placed on trucks. At the right moment, the roofs of the houses were remotely opened, and the drones took off to strike their targets — russian bombers. During the operation modern UAV control technology was used, combining autonomous artificial intelligence algorithms and manual operator intervention. In particular, because of signal loss, some of the UAVs switched to performing their mission using artificial intelligence along a pre-planned route. Upon approaching and making contact with a specific target, the combat unit was automatically activated. All participants involved in the "Spiderweb" have left russian territory and are currently in Ukraine.

"In accordance with the laws and customs of war, we have targeted entirely legitimate targets – military airfields and aircraft that regularly bomb our peaceful cities. Therefore, we are carrying out a real demilitarization of the russian federation, as we are destroying military targets. And our strikes will continue as long as the russian federation terrorizes Ukrainians with missiles and 'shaheds', emphasized SSU Chairman Vasyl Maliuk.

The next day, the General Staff of the Armed Forces of Ukraine confirmed that 41 russian military aircraft had been destroyed as a result of operation "Spiderweb". These included two A-50 long-range radar surveillance aircraft at the Ivanovo airfield. Each of these aircraft is worth over $300 million.

Ukraine's international partners highly praised "Spiderweb" and confirmed the SSU's estimate of over 40 aircraft. The North Atlantic Alliance leadership noted that this was Ukraine's "most successful operation" against russian strategic aviation and that it would have a critical impact on russia's capabilities.

THE THIRD ATTACK ON THE CRIMEAN BRIDGE

After two attacks on the Crimean Bridge – using explosives in October 2022 and naval drones in July 2023 - the SSU carried out a new unique special operation. And for the third time, it struck the Crimean Bridge – this time underwater. The operation took several months to prepare. Its planning and execution were coordinated by the Head of the SSU Vasyl Maliuk.

The SSU agents mined the piles of the illegally constructed bridge, and June 3, 2025, at 4:44 a.m., without any civilian casualties, the first explosive device was activated.

The underwater piles of the bridge were damaged at the bottom by 1,100 kg of explosives in TNT equivalent. The bridge is basically in bad condition and in fact isn't used by the enemy to deliver weapons to the front.

This special operation has once again confirmed the high level of training and effectiveness of the SSU in countering russian aggression. It also demonstrates that no facility used by the occupiers for war purposes will not be beyond the focus of attention of the Security and Defense Forces of Ukraine.

DRONE-ASSAULT OPERATIONS

Another successful military solution tested by the SSU in combat on certain sections of the front line is the use of drone-assault operations. These are carried out in close cooperation between the SSU and other units of the Defense Forces, allowing for high-precision strikes against enemy targets with minimal risk to Ukrainian defenders.

An example of such drone-assault operation was the capture by the SSU Special Forces of an enemy stronghold near the village of Sverdlikove in Kursk in August 2024. It was a professionally constructed and prepared fortification with underground tunnels stretching over 1 km. FPV drones were used to capture it, attacking the bunker for 24 hours, along with ground-based robotic systems and, in the final stage, involving assault groups from the SSU Special Operations Centre 'A.'

Thanks to a well-thought-out strategy and coordinated actions during the battle, the special operation was successful and resulted in minimal losses.

As a result SSU Special Forces captured over a hundred russian prisoners of war, including officers and militants from the Akhmat unit. They were subsequently added to the exchange fund, which made it possible to intensify exchanges and return Ukrainian defenders from russian captivity.

Thus, development and innovation not only increase the efficiency of the SSU units, but also enable them to adapt quickly and respond promptly to modern challenges and threats, reduce risks to personnel, and gain a strategic advantage on the battlefield.

COUNTERINTELLIGENCE

Counterintelligence activity is the foundation of national security. The SSU regularly detects and successfully thwarts attempts by russian intelligence services to destabilize the situation within our country.

In order to stay one step ahead of the enemy, Ukrainian secret service is constantly improving methods and techniques, drawing on experience and taking into account developments in technology and methods used by the enemy to carry out their subversive activities.

The SSU Counterintelligence Department operates 24/7, although its work remains invisible to the public in most cases.

In 2024, the key challenges and threats to Ukraine's national security remained the active actions of russian intelligence services aimed primarily at overthrowing the constitutional order or state power, reducing defense and economic potential, internal destabilization, inclining society to surrender to the russian federation, and undermining all components of our state's stability in repelling the aggressor.

The key tasks of the SSU Counterintelligence in wartime are to counteract intelligence and sabotage activities and attempts by foreign intelligence services, in particular exposing enemy agents, spies, traitors, and collaborators.

Combating internal enemies is an important front for the Ukrainian secret services. To this end the SSU uses the full range of counterintelligence capabilities

EXPOSURE OF INTELLIGENCE GATHERING NETWORKS

One of the key preconditions for effective counterintelligence is proactive work.

During 2024, the SSU Counterintelligence Department exposed 47 enemy intelligence networks, which included 267 individuals. Their tasks were:

- conducting HUMINT and SIGINT;
- carrying out acts of sabotage and terrorism;
- information and propaganda activities.

The enemy was most active in establishing its agent networks in Kyiv, Odesa, Dnipropetrovsk, Zaporizhzhia, Donetsk, Kharkiv, Chernihiv, Mykolaiv, Sumy, and Kherson regions, providing funding and support for future large-scale special operations.

The russian secret services have traditionally tried to involve politicians and high-ranking officials in these networks, using their access to “sensitive” and classified information.

However, despite the fact that throughout the full-scale war the enemy has been making constant attempts to build up its intelligence capabilities, the SSU is quickly adapting to new challenges, identifying and countering completely different approaches of the russian intelligence services.

In May 2024, Counterintelligence and investigators from the Security Service of Ukraine disrupted plans of the russian federal security service (fsb) to assassinate the President of Ukraine, the Head of the Defence Intelligence of Ukraine of the Ministry of Defense, and other senior military and political leaders of the state. The plans were to be carried out by an intelligence network that included two colonels of the State Guard Service who passed classified information to the enemy and were involved in a special operation by the fsb to eliminate Ukrainian officials with the help of missiles and FPV drones.

In July 2024, the SSU Counterintelligence neutralized a large-scale fsb intelligence network that was preparing missile and drone strikes by the russian federation on six regions of Ukraine.

At the same time nine russian agents were detained in Dnipro, Zaporizhzhia, and Sumy, as well as in Donetsk, Odesa, and Kirovohrad regions, who were handled by one fsb officer.

The agents performed different functions in their region: identified the locations of air defense and key power substations to adjust russian shelling, reconnoitered the concentration of personnel, military equipment, and the location of fortifications and firing positions of the Ukrainian army artillery, tracked the movement of the Ukrainian army trains towards the eastern front, and recorded the consequences of russian attacks on energy facilities.

In December 2024, the military counter intelligence of SSU neutralized a large-scale russian agent network. The criminals spied on the Defense Forces in five regions of Ukraine and collected information on the Operational Command "East" of the Armed Forces of Ukraine, combat aviation (F-16 aircraft) and aviation infrastructure, the deployment of the Joint Forces Operation, and structures involved in the production of electronic warfare to counter UAVs.

In addition, the SSU CI exposed a russian agent group that was spying on the Armed Forces of Ukraine in Zaporizhzhia. The russian agents were two residents of the regional center, including an employee of a strategic defense factory. The criminals were preparing coordinates for russian air strikes on air defense systems, locations of the Defense Forces and defense industry complex enterprises, and a woman also reported on missile attacks on the enterprise where she worked.

Also as a result of special multi-stage operation in Kharkiv, the SSU detained design engineers who helped to connect Zaporizhzhia NPP to Rosatom for reward in cryptocurrency. At the request of the russian corporation, they developed research and design documentation for the modernization of russian nuclear power plants, including Kursk, Rostov, Novovoronezh, and Balakovo. Subsequently, the defendants of the case were to help the occupiers fully integrate the Zaporizhzhia NPP into the russian energy system.

EXPOSING TRAITORS AND SPIES

Counteracting the internal enemy, including exposing traitors and spies, is another important front for the Ukrainian secret service. To this end, the SSU uses the full range of counterintelligence capabilities. It has already done a lot of work to purge enemy agents from all spheres of life – from government, military structures, the church environment, strategic sectors of the economy, etc.

Thus, in 2024, the units of the SSU launched a pre-trial investigation:

- 1122 criminal proceedings under Article 111 of the Criminal Code (high treason),
- 31 criminal proceedings under Article 114 of the Criminal Code (espionage).

For example, based on SSU materials, a Ukrainian citizen who voluntarily took the position of "deputy head of the government of the LPR was found guilty of treason and collaboration and sentenced (in absentia) to 15 years in prison with confiscation of all property and 10 years with disqualification to hold positions in state and local government.

Work to clear the country of internal enemy is under way. The SSU pays special attention to countering threats related to enemy infiltration and recruitment in the units of the Security and Defense Forces of Ukraine. And in most cases, it is a matter of preventing such risks.

For example, the SSU detained former police officers for treason who were collecting information on the location of the Defense Forces and UAV manufacturing facilities in Kyiv. One of them also conducted online training for enemy Special Forces units "Akhmat" and "Wagner" and searched for the remains of russian military personnel in Kyiv region.

The internal cleansing of the Service from any russian influence is extremely important. This is one of the main priorities of the SSU Head Vasyl Maliuk. Therefore, he personally coordinated special operations to expose and detain top traitors in the ranks of the special service – the former head of the SSU Main Directorate in Crimea, Oleh Kulinich (2022) and the former head of the ATC Headquarters, Dmytro Koziura (2025).

It was established that the latter, in particular, was recruited by the FSB back in 2018. For some time, the suspect was put on ice by russian handlers for security reasons and did not perform active espionage activities. However, at the end of December 2024, the fsb resumed contacts with him.

At that time SSU internal security officers were already keeping the traitor under operational control. To prevent him from harming Ukraine's national security, he was restricted from accessing really important data. Instead, the SSU used the traitor in a counterintelligence game: it fed the enemy a large amount of disinformation through him.

"This special operation demonstrates that the SSU is able to respond quickly to threats and effectively counteract the enemy. Since the beginning of the full-scale invasion, we have performed a serious cleansing process, which is still ongoing. We are doing everything to protect our country from internal and external enemies," said SSU Head Vasyl Maliuk.

In particular, in recent years, the Security Service of Ukraine has radically changed its approach to personnel policy: it has strengthened its multi-level internal control and security system, focusing on preventive risk identification at the stage of candidate selection.

The measures taken make it virtually impossible for enemy agents to infiltrate the ranks of the Ukrainian secret service. The use of all possible tools to strengthen institutional capacity allows the SSU to effectively implement combat, counterintelligence and special task.

PROTECTION OF CRITICAL INFRASTRUCTURE

One of the priorities of the SSU security policy during the war is the protection of critical infrastructure objects (CIO) and state strategic resources. Today it is energy networks, transportation routes, utility systems, military-industrial complex enterprises, supply chains, and other key industries that determine the state's ability to function, maintain economic stability, and ensure the livelihoods of the population.

The protection of these facilities involves not only physical security, cybersecurity, but also intellectual protection at all levels. In this context, counterintelligence protection plays a critical role.

On the part of the SSU, it implies timely detection and elimination of networks of informants and spotters who, for various reasons (personal or financial), transferred information about critical infrastructure objects to the enemy. In most cases, the secret service managed to prevent catastrophic consequences that would have affected the functioning of the CIO.

For example, the SSU exposed an employee of Ukrzaliznytsia who spotted russian strikes against military and critical infrastructure in Dnipropetrovsk region. The main targets of the enemy were railroad junctions used to transport heavy weapons and ammunition to the front line. The occupiers were also interested in places of concentration of personnel and military equipment of Ukrainian troops involved in combat missions. According to the investigation, the 39-year-old railroad worker got in the focus of the enemy attention because of his comments in pro-kremlin Telegram channels, where he approved russian war against Ukraine. The offender was sentenced to life imprisonment.

COUNTERING RECRUITMENT

In 2024, the SSU organized an effective counteraction to another threatening trend - the enemy's remote recruitment of Ukrainian citizens, including socially vulnerable categories such as youth and juveniles. For the initial recruitment, russian special services use sites for earning “easy money”, social media and messengers, followed by tactics of gradual involvement in illegal activities through blackmail, threats, etc.

The russian intelligence services use the individuals recruited in this way to engage in sabotage and terrorist activities. In particular, they are involved in arson attacks on the property of military personnel of the Security and Defense Forces of Ukraine and infrastructure facilities, as well as in installing self-made explosives, thus infringing on the life of policemen and servicemen.

The SSU immediately established a clear link between such crimes and the russian intelligence services: the recruitment of citizens for sabotage work in Ukraine is conducted by a separate unit of the fsb.

As of April 2025, the SSU, together with the National Police, had already uncovered more than 600 criminals who had set fire to military vehicles, Ukrainian Railways facilities, or blew up explosives near the shopping malls. In fact, there is not a single case where the perpetrators of these crimes have not been identified. Moreover, the courts have already begun to pronounce guilty sentences in such cases.

To prevent the recruitment of teenagers, the SSU, together with the National Police, launched a large information campaign “Burn the fsb”. Active educational work is underway throughout Ukraine. It includes videos, social networks, video adverts, outdoor advertising etc.

Also in December 2024, the SSU created a special chatbot - t.me/spaly_fsb_bot - to report recruitment attempts. This can also be done by calling the SSU hotline at 0 800 501 482.

Over the six months of its operation, the chatbot has already received almost seven thousand messages. The security service carefully analyzes and processes all the information received.

Also in May 2025, the SSU, together with the Juvenile Police, launched a series of meetings directly at schools and colleges to explain explicitly to teenagers what to do when they are recruited. After all, the enemy is now using a new tactic: they are remotely blow up IEDs together with the perpetrator who plants them. In fact, russian intelligence services eliminate a recruited agent unwittingly to remove a witness to the crime and not to pay him the reward.

PROTECTION OF STATE SECRETS

In the context of russia's armed aggression, the importance of protecting state secrets is a prerequisite for maintaining Ukraine's defense capability and stability. That is why one of the main tasks of the SSU is to prevent, localize and block channels of possible leakage of classified information.

In particular, the SSU performs appropriate vetting on the reliability of persons claiming the access to state secrets. The main goal is to discover persons who have circumstances that can be exploited by the intelligence services of the aggressor country to conduct intelligence and sabotage activities. In 2024, more than 2,500 citizens were denied access to state secrets.

In order to eliminate the causes and conditions leading to law violations in state secrets protection area, the SSU conducted more than 1,700 preventive events in 2024.

Around 900 officials were brought to administrative responsibility, which eliminated the preconditions for leaking classified information.

The SSU is actively working to improve legislation to enhance the protection of classified and sensitive information. With the support of the Verkhovna Rada of Ukraine, a number of amendments were made to the legal acts regulating the protection of state secrets, taking into account current security threats. During the martial law in Ukraine, the protection of state secrets and classification of information on critical infrastructure objects (CIO), which are priority targets for the enemy, are significantly strengthened.

COUNTERING TERRORIST AND SABOTAGE ACTIVITIES

Since the beginning of russia's full-scale invasion of Ukraine, the war has continued not only directly on the front line, but also in the relatively rear regions of our country. It concerns rocket attacks, ‘shahed’ attacks, and intensified terrorist and sabotage activities of the enemy.

The SSU pays considerable attention to deter this threat, as the methods of work of russian intelligence services can cause significant harm to the lives and health of citizens.

Today, the SSU timely detects evidence of terrorist attacks and sabotage, usually before they happen, localizes suspicious activity at the first sign of it, and responds quickly to new enemy tactics.

It is systematic work, which the SSU regularly reinforces:

- improves the response of operational teams;
- introduces new standards for local coordination, which significantly reduces the time required to respond to potential threats;
- implements a set of measures to prevent threats at the regional level;
- develops a system of public interaction;
- actively cooperates with local governments.

Targeted work has yielded real results. During 2024 the SSU uncovered and prevented dozens of cases of terrorist attacks, identified and detained hundreds of people involved in sabotage activities, and neutralized a large number of caches with weapons, explosives and munitions.

So, the main targets of terrorist attacks and sabotage are vehicles, railway infrastructure, administrative buildings (TCRs, National Police departments), energy infrastructure, communication networks and post offices, etc. A significant number of such crimes are committed with the involvement of intelligence gathering networks rather than individual perpetrators.

Thus, as a result of a multi-stage special operation, the SSU Counterintelligence prevented four terrorist attacks in Kyiv that were to take place on May 9. The SSU CI detained russian agents red-handed, who were installing packed explosive devices (disguised in tea packages) in construction hypermarkets of a well-known network and near a cafe (the explosive devices were planned to be placed in a car parked nearby). The russian ‘gru’* wanted to destabilize the situation in Ukraine and send a signal on the symbolic Victory Day about the alleged presence of the russian underground in Kyiv, which is waiting for the coming of the "russian world."

The SSU and the National Police have prevented a bloody terrorist attack in Kyiv, which was also planned by a russian group. A 20-year-old resident of Zaporizhzhia and her 26-year-old partner were to prepare an improvised explosive device and blow it up in a crowded place in the capital. Before committing the terrorist attack, both offenders had to perform the trial task - to set several military vehicles of the Armed Forces of Ukraine in Zaporizhzhia region on fire. However, the SSU Counterintelligence officers detained both traitors red-handed when they were trying to set an infantry fighting vehicle on fire.

In addition, the SSU neutralized an operational and combat group of russian ‘gru’ that committed terrorist attacks in frontline Kharkiv, spied on the Defense Forces units and prepared new terrorist attacks. The enemy group consisted of four local residents: a Kharkiv software engineer, a former military man, and two unemployed people. The group's activities were coordinated by a ‘dpr’* special forces militant fighter engaged on the eastern front in cooperation with russian main intelligence directorate. The defendants received a mission – to track and derail the train that was transporting Ukrainian military equipment to the front line.

In December 2024, counterintelligence prevented a terrorist act in Kyiv region, in particular in a building where one of the Defense Forces units was deployed. The SSU detained a juvenile perpetrator of the terrorist attack, who was to disguise himself in a Ukrainian military uniform and deliver an improvised explosive device to the building. Also two russian intelligence services agents were detained who were manufacturing explosives and placing them in a cache. The enemy tracked the route of the perpetrator online and planned to blow up the explosives immediately after he entered the premises.

Thus, in 2024, the SSU initiated 196 criminal proceedings for committing crimes related to terrorist activities and terrorist financing, 146 for committing sabotage.

These investigations are not only a proof of the SSU effectiveness, but also an indicator of changes in approaches to security within the country. Successfully documented and brought to court cases, effective sentences, and dismantled enemy intelligence networks are all evidence of the quality of our analytics, prompt response, and legal support.

The SSU also takes comprehensive measures to counteract the illegal activities of international terrorist organizations (ITOs), illegal armed groups (IAGs), religious extremist organizations and groups (REOs).

In particular, within the framework of international cooperation between the SSU and the Federal Criminal Police Office of Germany, a set of procedural actions was implemented in two international investigative cases "BURAN" and "VITTER". As a result of the measures taken in the EU, 13 members of the ISIS and ISIL were detained.

Further development of the counter-sabotage and counter-terrorist system in Ukraine should be evolved, in particular, in the areas of strengthening coordination of counter-terrorist entities and expanding international cooperation in countering terrorism and its financing.

Work with the public also remains an important factor, including the development of a security culture, surveillance skills, suspiciousness without panic, and a clear understanding of the algorithm of actions in case of detecting suspicious objects and suspicious behavior of individuals and close associates.

PROTECTION OF NATIONAL STATEHOOD

In the context of war, the main threat to Ukraine's national statehood is the armed aggression of the russian federation and subversive activities of enemy intelligence services. Encroachment on the constitutional order, attempts to overthrow state power, incitement of religious conflicts and hostilities, destructive propaganda and spread of separatist sentiments are all urgent challenges to our state in general and to the SSU in particular.

Such threats do not always take the form of open aggression, but are often covert or secretive (intelligence networks, information and psychological operations, infiltration into government structures, propaganda campaigns, etc.)

The SSU has considerable experience in countering various forms of subversive activities, which can range from the dissemination of disinformation to open cooperation with the enemy (transfer of intelligence or collaboration with occupation administrations).

Throughout 2024 the SSU units exposed and stopped subversive activities to the detriment of our state, which resulted in the launch of a pre-trial investigation in criminal proceedings on the facts of committing the following crimes:

- overthrow of the constitutional order or seizure of state power – 72;
- encroachment on the territorial integrity and inviolability of Ukraine – 285;
- collaboration activities – 2,173;
- Aiding and abetting the aggressor state – 430.

One example of countering the enemy: the SSU neutralised a 28-member operational and combat unit of the russian military intelligence. Its task was to seize power in Odesa. The SSU detained the organisers and accomplices, seized a large arsenal of firearms and explosives, money and methodological manuals of sabotage and reconnaissance activities. Twelve people were served with a notice of suspicion. Two of them have already received fair court sentences.

An important component of protecting national statehood is countering kremlin propaganda in the national information space. In this context, the SSU exposes and blocks the spread of hostile narratives, fake news, and the use of so-called bot farms - automated networks of fake accounts aimed at disrupting society and weakening trust in state institutions.

Thus, a Ukrainian citizen was sentenced to five years' imprisonment for committing crimes under Part 2, Part 3 of Article 109 and Part 2, Part 3 of Article 436-2 of the Criminal Code. The man created and administered Telegram and YouTube channels, where he disseminated anti-semitic publications accusing Jews of starting the war, calls to fight against "fascist regime" and to armed overthrow of the power in Ukraine.

The SSU also takes comprehensive measures to bring to justice representatives of the aggressor country for encroachment on the foundations of the state system in Ukraine. Thus, 14 deputies of the russian state duma were found guilty (in absentia) and sentenced to 15 years of imprisonment with confiscation of all property for encroachment on the territorial integrity and inviolability of Ukraine.

Among other things, the SSU actively works on neutralising pro-russian movements within our country, which, according to the kremlin's plan, were supposed to become the "fifth column" that would help the occupiers.

Exploiting political parties, as well as church influence, is one of the tactics of hybrid warfare aimed at undermining internal stability and splitting Ukrainian society. Political parties, churches and social movements often become a dangerous tool in the hands of the enemy, as they are also used to promote pro-russian narratives and disinformation.

Throughout 2024, in order to protect Ukraine's national statehood, activities of five political parties such as the Social and Patriotic Assembly of Slavs (SPAS), Nash Krai, "Slava", "Slavic Party", "Garant"), as well as three NGOs (All-Ukrainian Union of Public Associations "Association of Compatriots' Organisations "russian Commonwealth, the Army of the Faithful Black Sea Cossacks named after Hetman B. Khmelnytskyi, and All-Ukrainian Movement Against Fascism ‘Patriots for Life’) have been banned by court order.

In 2024, two foreign pro-russian political parties (the Hungarian ‘Our Fatherland’ and the Serbian ‘Serbian Rights’) and the russian Charitable Foundation Gulfstream, operating in the temporarily occupied territories of certain regions of Ukraine, were included in the list of political parties and NGOs that pose a threat to national security.

In addition, the SSU blocked the destruction activities of a number of activists of pseudo-nationalist movements. In particular, the heads of the russian Community of Poltava Region and the Poltava regional branch of the all-Ukrainian NGO russian Council of Ukraine (ruska Rada Ukrainy) were found guilty of committing a crime under Part 2 Article 111, Parts 2, 3 Article 436-2 of the Criminal Code and sentenced to 15 years' imprisonment with confiscation of property.

The SSU officers also tracked down and detained a suspect in the criminal proceedings – one of the leaders of the “people’s power” movement, a follower of separatist A. Balakhnin and the head of the regional branch of “Stremousov's Journalists.” He had been hiding from the pre-trial investigation authorities and the court. He was found guilty under Part 2 Article 436-2 of the Criminal Code and sentenced to three years' imprisonment. The protection of national sovereignty remains a priority for the Security Service of Ukraine. An important element in further strengthening this direction is the implementation of a proactive approach to responding to new challenges and threats, the use of modern technologies for monitoring, analyzing, and countering manipulation and information influence, and enhancing cooperation with international partners.

CYBER SECURITY

In today's world, global digitalisation processes make everyday life easier for citizens, but at the same time can pose serious risks to the national security of the state. Ukraine has also faced such challenges, especially in 2022, when cyberattacks, cyber incidents, information and psychological operations, disinformation, propaganda and other means of influence became an integral part of the war waged by russia.

After all, enemy military operations are often accompanied by massive cyberattacks aimed at destabilising the state from the inside. Therefore, in 2024, the SSU cyber specialists' main efforts were aimed at countering technical penetration of russian intelligence services into computer networks of state authorities, automated information processing systems and communication channels of military units, cyber defence of critical infrastructure and state information systems.

Last year, the SSU cyber specialists neutralised almost 3,000 cyber attacks and cyber incidents, which targeted, among others, the defence sector, central executive authorities, transport and logistics companies, energy and life support facilities, electronic communication networks, etc.

Investigating such cyberattacks and bringing the perpetrators to justice is an important part of the SSU Cyber Security Department's work.

Thus, according to the CSD, in 2024, two hackers from a well-known group “Armagedon”, which carried out more than 5,000 cyberattacks against Ukraine received prison sentences in absentia. The largest number of attacks targeted the electronic systems of the Ministry of Foreign Affairs and the Ministry of Economic Development of Ukraine. Their goal was to gain access to the electronic document management system and servers of government agencies of our country.

In 2024, the SSU also dismantled 10 large-scale bot farms that were used to anonymously disseminate specially prepared materials on the Internet aimed at discrediting the Ukrainian government, justifying russia's armed aggression against Ukraine, spreading pro-russian narratives, etc.

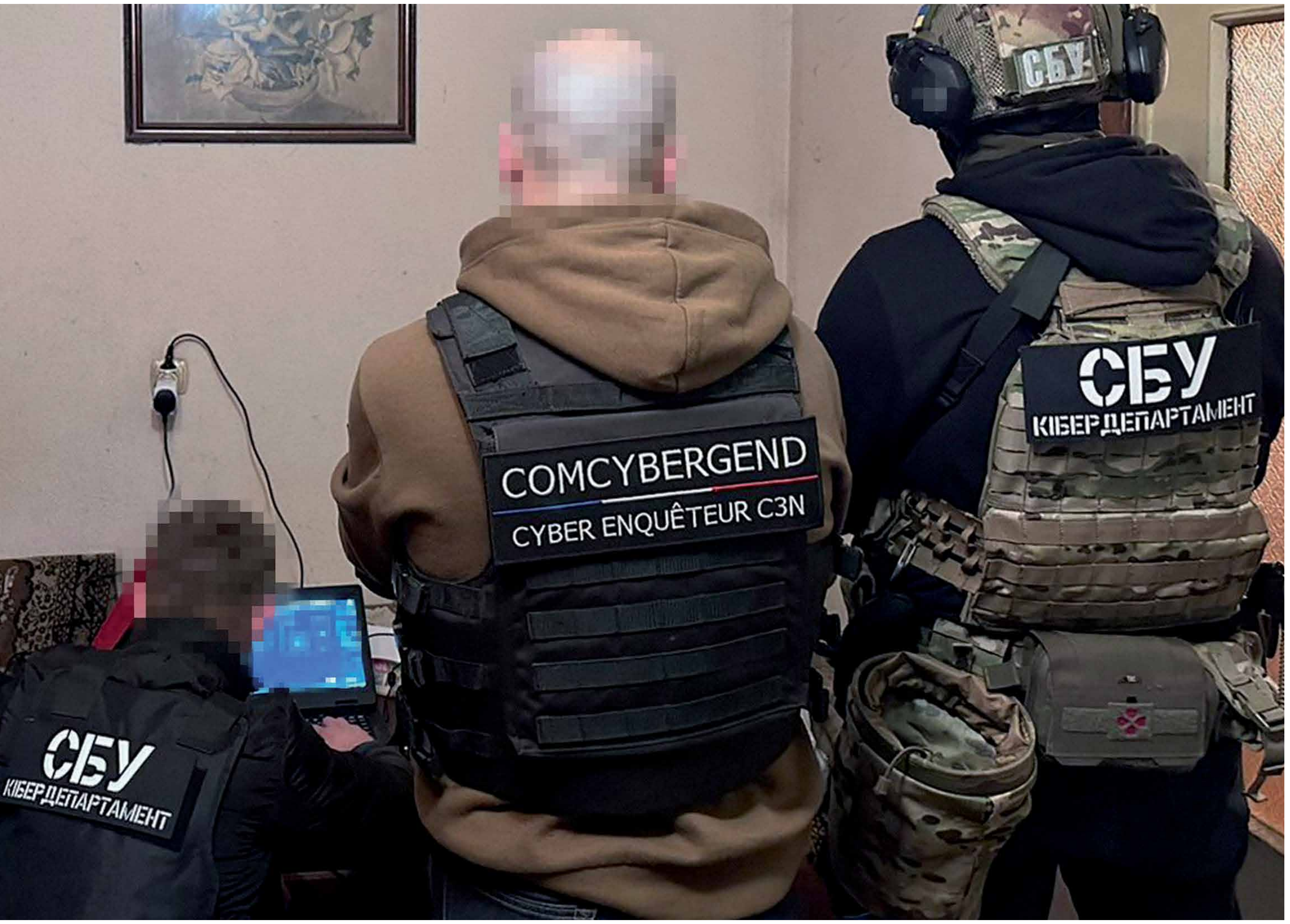
To obtain intelligence and inflict maximum damage to the Ukrainian information infrastructure, the enemy engages a significant number of forces and means (highly specialised and highly professional IT specialists from the personnel of the russian general staff, the russian federal security service and affiliated hacker groups), and uses the entire available cyber arsenal.

Accordingly, one of the SSU's important tasks is to counteract technical intelligence conducted by the enemy to obtain information on strategic plans, military deployments, supply chains and production facilities that manufacture weapons, as well as to establish control over the electronic networks of the Ukrainian Defence Forces and personal mobile devices of their representatives.

To prevent similar infiltrations the SSU cyber specialists work directly with the Defence Forces units on the frontline. They also take an active part in detecting and destroying enemy electronic warfare systems and UAV control points.

The SSU cyber specialists actively and effectively cooperate with specialists of intelligence services and law enforcement agencies of partner countries to counteract and stop the activities of international hacker criminal groups.

An example of such cooperation is the international special cyber operation "EndGame” conducted by the SSU together with partner intelligence services.



In total, more than 30 members of transnational hacker groups were exposed, including the russian "BlackBasta", "Revil" and "Conti", which extorted tens of millions of US dollars from representatives of foreign corporations. The development and distribution of malicious software has been stopped, over 90 servers have been seized, and more than 1,000 domains used by hackers have been blocked.

A significant achievement on the cyber front is a joint special operation by the SSU Cyber Unit and law enforcement agencies from 13 countries to target a group of cyber criminals "LockBit". Thanks to coordinated actions supported by Eurojust and Europol, the criminals were dealt a serious blow, as the searches resulted in access to and destruction of a significant part of group's infrastructure. Information from servers was deleted and cryptocurrency accounts were blocked.

At the same time, SSU cyber specialists are constantly monitoring and neutralising any attempts of information influence by russian agents. In particular, the SSU exposed an intelligence group that, as a part of a pro-kremlin political project "Different Ukraine" under the supervision of Viktor Medvedchuk, accused of high treason, was engaged in information sabotage against Ukraine. The agents distributed video content discrediting the Defence Forces and calling on Ukrainians to lay down their arms and surrender to the occupiers. They sent the completed media products for approval to a russian curator, Denis Zharkikh, a former presenter on Medvedchuk's channels and currently the director of his organisation, Drugaya Ukraina, in moscow. Thus, the SSU cyber units make a significant contribution to ensuring the information and cyber security of our country.

SANCTIONS POLICY

Ukraine's sanctions policy, developed and implemented in response to russia's aggression, is an important tool in the fight against the enemy. Its main goal is not only to reduce military potential, but also to isolate the aggressor state from strategically important sectors of the economy, blocking its influence on the socio-political, cultural, information and other key sectors of our country.

In this case, sanctions perform a preventive function - they deprive the aggressor of a resource used in the war against Ukraine.

The Law of Ukraine "On Sanctions" defines more than 30 types of sanctions covering various areas, including blocking assets, restricting trade operations, stopping the transit of resources through the territory of Ukraine, preventing the withdrawal of capital from Ukraine, cancelling or suspending licences and other permits, prohibiting participation in privatisation, leasing state property by residents of a foreign country, using the radio frequency spectrum and distributing media in Ukraine, etc.

In particular, economic restrictions aimed at blocking access to international financial markets, technology, energy resources and dual-use goods.

At the same time, such type of sanctions as the recovery of assets of individuals or legal entities into the state's revenue is exceptional and can be applied only to individuals and legal entities that have posed a significant threat to the national security, sovereignty or territorial integrity of Ukraine (including through armed aggression or terrorist activities) or have significantly contributed (including by financing) to the commission of such actions by other persons, including residents.

Realizing the need for urgent and effective response to existing and potential threats to Ukraine's national interests and national security, the SSU has become one of the key initiators of the application of special economic and other restrictive measures (sanctions).

To this end, the secret service is constantly collecting evidence and preparing sanctions proposals.

In total, since the beginning of the full-scale war, the NSDC* has imposed sanctions on more than 14,300 entities at the SSU's initiative, including businesses, individuals and organisations that support russian aggression or directly assist the aggressor country.

For example, in order to prevent and suppress illegal actions to the detriment of Ukraine by foreign entities, the SACCU's* decision in 2024 recovered assets worth billions of hryvnias for the state. This significantly reduced russia's influence on critical sectors of Ukraine's economy.

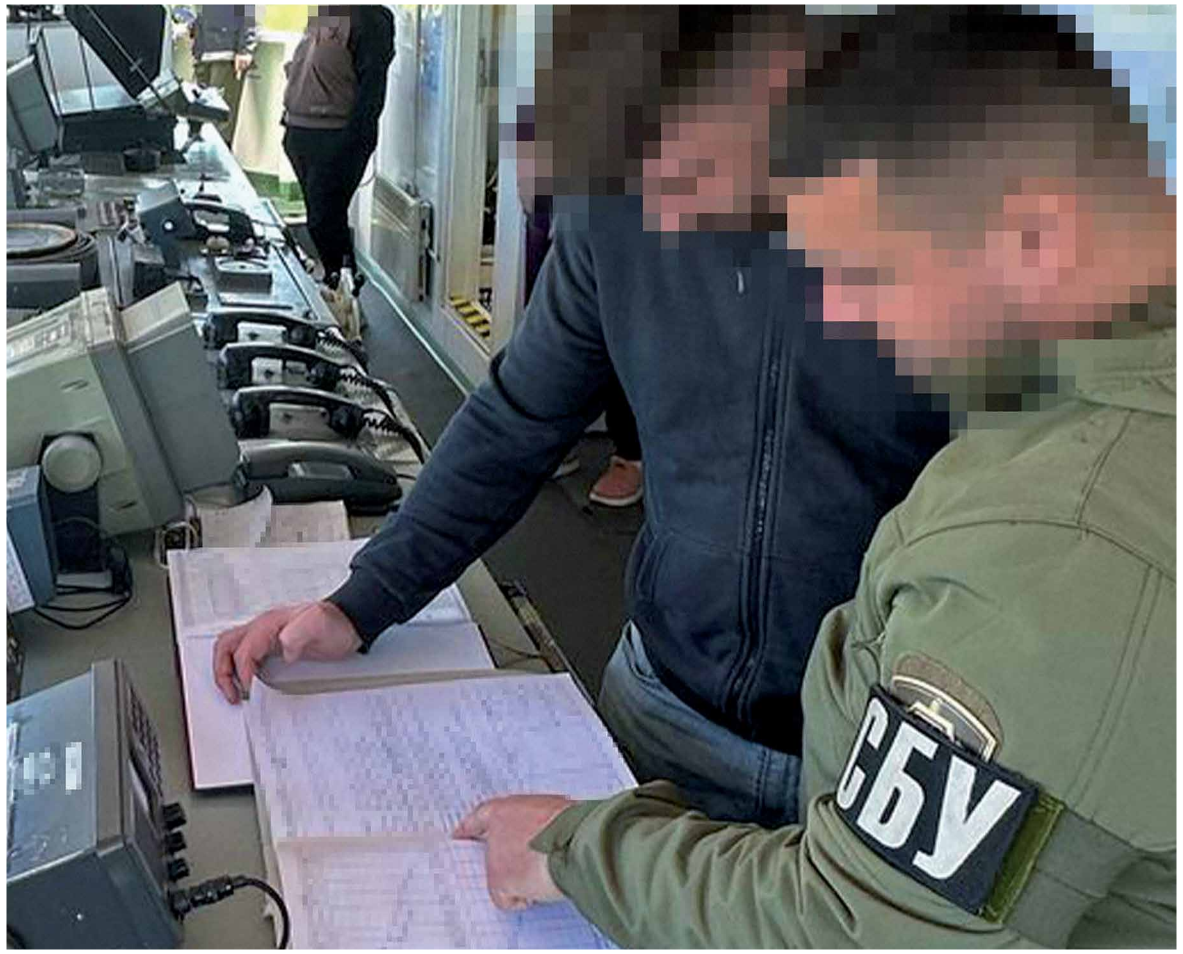
In particular, the assets of the mining companies - Mykolaiv Alumina Plant LLC and Hlukhiv Quartzite Quarry LLC - owned by sanctioned russian billionaire Oleg Deripaska alone contributed more than UAH 10 billion to the state budget.

In 2024, the SACC* also seized the assets of russian billionaire Alisher Usmanov, owner of the metallurgical holding "USM Holdings", with a total value of almost UAH 900 million, and transferred it to the state budget.

Economic sanctions have been imposed on the corporate rights of russian oligarch Vladimir Lukyanenko with regard to a number of strategic enterprises, including JSC Nasosenergomash (90.6% of shares), Sumy Machine Building Scientific and Production Association, which manufactures equipment for the oil, gas, nuclear, and chemical industries (83.9% of shares), SMNVO-Engineering, which manufactures hydraulic and pneumatic equipment (100% of shares), and the pharmaceutical company Kusum Farm (50% of the authorized capital). The total value of assets recovered to the state budget amounted to over UAH 4 billion.

These are just a few examples of how sanctions have blocked the preconditions for economic control and likely channels of financing by russian oligarchs for the russian federation's intelligence and subversive activities and the war against Ukraine: replenishment of the budget, arms production, support for propaganda, etc.

An important component of these restrictive measures is the fight against russia's so-called "shadow fleet". After the sanctions had been imposed, many russian vessels and shipping companies began to look for various ways to avoid restrictions. These included, among other things, changing flags and forging documents. According to the SSU, sanctions were imposed on 116 captains of this "shadow fleet".



The SSU also initiated the seizure of the property of russian oligarch Alexander Verkhovsky. In 2014 as a member of russian council of federation of federal assembly, he voted for the deployment of the russian armed forces on the territory of Ukraine and the annexation of Crimea, and in early 2023 he declared his support to a full-scale russian invasion of Ukraine.

The sanctions applied by Ukraine are not only an internal defence mechanism, but also an important signal to the international community. The Ministry of Foreign Affairs actively informs our international partners - the European Union, the United States and other countries - on the introduction of new sanctions and calls on them to introduce similar restrictive measures.

This process helps to build an international coalition against the aggressor, which is a key element in ensuring stability, sovereignty and independence of Ukraine in conditions of war.

Thanks to this work, Ukraine and partner countries have included in the sanctions lists enterprises of the russian military-industrial complex, representatives of the occupation authorities in the temporarily occupied territory of Ukraine, russian federal media companies and media resources in the occupied Crimea involved in anti-Ukrainian activities.

In 2024 restrictive measures against 736 entities (181 individuals and 555 legal entities) were synchronised with the countries of the international sanctions coalition (the EU, the US, Canada, Japan, the UK, and the Swiss Confederation).

Thus, the application of economic sanctions against the russian federation is not only a response to aggression, but also a strategic safeguard to stop russia's economic, political and military expansion in Ukraine. After all, russia has repeatedly demonstrated its ability to use economic ties as an instrument of influence and, in some cases, as a weapon.

SEARCH FOR AND LIBERATION OF PRISONERS

The SSU plays a significant role in the process of exchange of prisoners of war. Since 2014, this function has been performed by the Joint Centre for Coordination of Search and Liberation of Prisoners of War and Persons Illegally Deprived of Liberty as a Result of Aggression against Ukraine, which is part of the Security Service.

Between 2014 and russia's full-scale invasion, the Joint Centre helped to set free around 3 500 people who had been illegally detained. The exchanges took place on the contact line and on the territory controlled by the enemy.

Currently, the Joint Centre at the SSU keeps records of those who are in captivity, conducts search and directly organizes exchanges in cooperation with other state agencies within the Coordination Staff for Treatment of PoWs.

Our goal is to bring everyone back: military personnel, civilians and illegally deported children. This is a very important point in the Peace Formula proposed by President of Ukraine Volodymyr Zelenskyy. After all, the life of every Ukrainian is of the utmost value!

Starting from 24 February 2022 and as of March 2025, over 4 000 citizens have been returned from russian captivity thanks to the joint efforts of the Coordination Staff.

In 2024 alone, 19 exchanges were carried out to free prisoners and illegally detained persons, bringing back 1 304 defenders of Ukraine. As a result of repatriation measures, 3 390 bodies of deceased defenders have been returned.

The release and return to Ukraine of civilians illegally convicted in russia was especially significant, including the return of:

- Nariman Dzhelyal, Ukrainian Crimean Tatar politician, Deputy Chairman of the Mejlis of the Crimean Tatar People, currently Ambassador of Ukraine to Turkey;
- Valera Matyushenko, who assisted Ukrainian military personnel and had been held captive from 2017;
- Ivan Levytsky, priest of the Ukrainian Greek Catholic Church, abbot of the Church of Nativity of the Mother of God, and others.

In addition, the experience gained by the Joint Centre in conducting negotiations to carry out so-called field exchanges made it possible to bring the 2nd battalion and the repair battalion of the 110th AFU Brigade out of encirclement in the areas of Donetsk Filtration Station and Avdiivka's eastern outskirts without surrendering, as proposed by the russian side.

Moreover, at the end of October 2024, the Joint Centre, in cooperation with the AFU, organized and carried out the liberation of 30 Ukrainian defenders from captivity in Kursk region through a well-established channel. This swap took place between the positions of the AFU and the enemy forces.

A separate important area is the return of Ukrainian children back who were illegally deported and forcibly displaced to russia. Such activity is carried out by the Joint Centre in close cooperation with the Ukrainian Parliament Commissioner for Human Rights within the framework of the Bring Kids Back UA program under the President of Ukraine, as well as Save Ukraine charitable organization.

As of March 2025, 1 243 minors – children who had been in the temporarily occupied territories and in russia – have been returned to Ukraine. Bringing back one child is a complex process and often takes months.

HUMAN CAPITAL

The key to building up the Security Service of Ukraine team is selecting patriotic, motivated and honest professionals.

Precisely such people are currently forming the SSU team, where everyone must work efficiently and cohesively.

Therefore, a high level of professionalism and moral resilience are important competencies for the staff of Ukraine's security service, given the scope and complexity of the tasks assigned to its units.

OUR HEROES

SSU personnel is directly involved in defending the state and destroying the enemy. Servicemen of the Special Operations Centre "A", Military Counterintelligence, Counterintelligence, Cybersecurity Departments and other units carry out combat missions on the front line.

Since the beginning of the full-scale invasion, 19 SSU officers have been awarded the highest honour - the Hero of Ukraine title - for their exceptional courage and heroism in defending Ukraine's state sovereignty and territorial integrity, as well as for their selfless service to the Ukrainian people. Unfortunately, six of these defenders were awarded the title posthumously.

The Service's leadership and brothers-in-arms of the fallen Heroes continue to care for their families, providing the necessary assistance with everyday issues, legal, social needs and rehabilitation. The Security Service is making every effort to ensure the families of the fallen Heroes feel care, support and gratitude to them.

During 2024, 424 officers of the Security Service and citizens who contributed to the fulfilment of important missions received state awards of Ukraine.

Among the SSU staff, there are full cavaliers of the Orders of Courage, Orders of Bohdan Khmelnytsky and Princess Olha. The Military Counterintelligence Department has been awarded the honorary distinction For Courage and Bravery.

"We are fighting on our land, for victory, for our families, for our independence", *- said a sniper from the SSU Special Operations Centre 'A' nicknamed 'Coconut' about his motivation.*

"If a person is trained, one will be confident. And confidence will enable a person to win on the battlefield. Don't waste time", *- said Dmytro Bashkintsev (nicknamed 'Dimon'), Hero of Ukraine and the head of the SSU Special Operations Centre 'A' sector, on the importance of training.*

> **"The 'Lord of the Horizon' rifle can fire a bullet faster and more accurately than its foreign counterparts. It broadens horizons"**, *- said Viacheslav Kovalskyi, a sniper of the SSU Military Counterintelligence Department, who set a world record on the front line in 2023 by hitting a russian soldier from a distance of 3,800 meters.*

RECRUITMENT TO SSU SPECIAL OPERATIONS CENTRE 'A'

In April 2024, the SSU Special Operations Centre 'A' launched a large-scale recruitment campaign, opening up opportunities for candidates eager to join the team. For the first time, even those with no previous military experience but with the most important qualities – determination, responsibility and a commitment to serving Ukraine – were given the chance to become a part of this legendary special forces unit.

Recruitment is carried out for several key specialties: military, medicine, engineering, information technology, communications and telecoms, analytics, logistics, humanitarian support and other areas needed for effective operation of a modern special forces unit.

An important part of the campaign was that each candidate independently chose their desired area of service based on their knowledge, skills, and potential.

During the recruitment process, the Recruitment Center of the SSU Special Operations Center 'A' assists in forming auxiliary units within the Armed Forces of Ukraine, supporting the large-scale transformation of the defense sector in line with NATO standards.

By April 2025 the SSU special forces unit had filled critical vacancies and moved on to selecting staff for specific, narrow fields. These are technological areas that include work with unmanned systems, electronic warfare and reconnaissance, cyber defense, operations in the information environment, and the analytical sector.

Today, the SSU Special Operations Center 'A' continues to form a team of those who are ready to act where the future of the country is decided.

PERSONNEL TRAINING

The Security Service takes a balanced and thorough approach to training its future personnel. SSU educational institutions constantly update and improve their training programs, taking into account the unique practical experience gained by the SSU in real combat and the best practices of leading security services worldwide.

A flexible education system allows employees to access the knowledge and skills they need depending on demand. This improves the level of training and ensures high efficiency of personnel, allowing them to quickly adapt to complex and changing security situation.

In 2024, the National Academy of the Security Service of Ukraine set up an educational and research training center for operational and combat training. The center trains specialists in the fields of firearms, tactical and special training, physical and tactical medicine training as well as Class I UAV piloting.

In the Academy there is a Training Situation Centre on critical infrastructure cybersecurity, where future SSU cyber staff are trained. The scenarios for their training are developed by the SSU operational units jointly with teams of Ukraine's leading critical infrastructure facilities.

The teaching staff at SSU educational institutions are constantly working to improve their professional knowledge and skills, mastering modern techniques and practices, as well as the latest educational, information and communication technologies. These efforts allow them to effectively adapt to present-day requirements and ensure a high level of training for future specialists.

Ukraine has also launched a cross-agency educational platform Cooperation for Victory for representatives of the security and defense sector.

It allowed to implement certification programs on counterterrorism, negotiation, critical infrastructure protection, OSINT methods and tools, and operational psychology.

INTEGRITY

Given the war challenges, the Security Service of Ukraine has significantly updated its approaches to human resources management and developed the Concept for the SSU Human Resources Policy for the period up to 2028.

We have introduced a transparent and flexible recruitment system, updated integrity requirements for personnel and candidates, and created a system of step-by-step career growth and continuous professional development. Professional and psychological support has been improved, and an inclusive approach has been introduced to engage people who participated in combat and were wounded.

An important part of the changes was the new Procedure for the Attestation of SSU Military Personnel, developed in 2024. This procedure sets a standardized, impartial and transparent model for evaluating personnel. The attestation determines the suitability of military personnel for their positions, assesses their career prospects, and increases integrity while reducing corruption risks.

The Security Service has updated the Rules of Professional Ethics and Integrity for SSU Military Personnel, which govern the military personnel's conduct while performing their duties. SSU officers regularly attend the course on strengthening integrity developed by Allied experts as part of NATO Building Integrity Program.

The SSU is committed to combatting corruption. The Service's Anti-Corruption Program is instrumental in this regard. Mechanisms for transparency and integrity have been improved, reducing corruption risks and increasing public trust in the SSU.

These measures aim to enhance ethical standards, transparency and professionalism in the SSU.

The Security Service regularly informs the public about its activities on its official website (ssu.gov.ua), verified pages of the SSU and its regional offices on social media, as well as through the mass media.

SSU TRANSFORMATION

In wartime conditions, the Security Service of Ukraine continues its transformation into a modern and effective security service in order to reliably protect state security.

Its task is to stay one step ahead of potential enemies. To do this, it must adapt to new challenges and threats, introduce modern technology, improve strategies for collecting and analyzing information, and cooperate closely with law enforcement and intelligence agencies, including at the international level.

To increase its effectiveness, the Security Service continues to improve by focusing on key areas of its activity, technological development, and international cooperation. A clear division of functions between the SSU and other law enforcement and intelligence services prevents duplication of efforts, raising the efficiency and effectiveness of each agency.

In the current environment, the key areas of the SSU's activity remain:

- counterintelligence, countering espionage, subversive and sabotage activities of foreign intelligence services;
- combating terrorism;
- ensuring information and cyber security;
- counterintelligence protection of critical infrastructure and supply chains;
- state secrets protection.

The challenges and threats that the Security Service faced during the war clearly demonstrated the need for a flexible structure. It is the ability to adapt quickly the Service's structure depending on the security situation that will enable the most optimal and rational use of available capabilities.

In the process of transformation the SSU is improving its methods and means of operation, and proposing necessary legislative changes, moving forward on the path of reform. This includes not only modernizing operational and technical capabilities, but also systematic work on legislative initiatives.

Currently, the main directions of the SSU's transformation in the short and medium terms are defined by several doctrines, strategies and concepts directly relating to the Security Service. These are:

- NATO-Ukraine Interoperability Roadmap;
- Overarching Strategy for the Reform of Law Enforcement Agencies as Part of Ukraine's Security and Defense Sector for 2023-2027 and the Government Plan for its Implementation;
- other laws and by-laws.

The Overarching Strategy provides for improving the system of democratic civilian control over the SSU's activities; comprehensive digital transformation; improving the crime prevention system based on a proactive approach to threat response; modernization of approaches to human resource management; strengthening adherence to moral principles and professional ethical standards; development of an analytical

approach and a risk-oriented model of operation, etc.

The Security Service is enhancing national counterintelligence capabilities to thwart the enemy's attempts to carry out terrorist, espionage, subversive, and sabotage as well as other unlawful activities against Ukraine, its partners and allies.

The Service's counterterrorist capabilities are strengthened through improved coordination between counterterrorist actors, and international cooperation in the field of combating terrorism and its financing is expanded. Special emphasis is placed on information security – the state secrets protection system is being improved, and NATO standards for restricted information protection are being implemented.

The SSU is actively introducing cutting-edge technology, modern tools and IT-solutions to develop the information and analytical component for high-quality threat analysis and decision-making.

As one of the key components of Ukraine's security and defense sector, the Security Service is actively involved in implementing state policies of Euro-Atlantic and European integration and is working to strengthen its core areas of activity, particularly under wartime conditions.

In cooperation with NATO, the SSU continues to pursue interoperability with the Alliance. Requirements covering the SSU's transformation, strengthening its counterintelligence capabilities, combating terrorism etc. were elaborated and approved at the Washington Summit.

As part of European integration, the Security Service is engaged in the official screening of Ukrainian legislation for compliance with EU law. In preparation for EU membership negotiations, the SSU team participated in the development of the Roadmap on the Rule of Law, which will be an important step on the European integration path.

The main document integrating the provisions of these initiatives and defining a comprehensive vision for the SSU's modernization is the 2025–2030 Development Strategy. The Strategy outlines key priorities for institutional development and transformation of the Service into a single national counterintelligence agency capable of promptly and effectively countering external and internal threats to state security.

Achieving the key goals and objectives set out in the Strategy requires introduction of modern approaches to personnel management and professional training, risk-oriented methods of threat response, and latest technological solutions in operational and combat activities. This includes the development of weapons and implementation of military innovations, improving the information analysis component and resource provision, digital transformation and expansion of international cooperation.

People, processes, innovation, and partnership are the foundation for implementing the Strategy.

E-VERSION PUBLIC REPORT OF THE SECURITY SERVICE OF UKRAINE FOR 2024
IN ENGLISH:

SECURITY SERVICE OF UKRAINE