The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No.4 (2024)

DOI: 10.62524/msj.2024.2.4.12

The Security Service of Ukraine: key operations and challenges during the full-scale russian-Ukrainian war

Serhii Yevtukh
Postgraduate student of the Department of National Security
State University of Zhytomyr Polytechnic
10005, Chudnivska Street, 103, Zhytomyr, Ukraine
e-mail: phd256232_yesv@student.ztu.edu.ua
ORCID: 0009-0006-1799-5026

Abstract. The article examines the activities of the Security Service of Ukraine (SSU) in the context of the full-scale war of the russian federation against Ukraine. The main areas of work, methods and measures taken to counteract the existing challenges and threats to the national security of the state are considered. The author analyses the effectiveness of the SSU and identifies ways to improve its work.

Current research findings show the enormous impact of modern technologies on both battlefield operations and combat service support, emphasising their role in strengthening defence posture. The findings confirm that the integration of drones, robotic systems and artificial intelligence (AI) significantly enhances the potential to conduct reconnaissance missions and combat missions with increased accuracy and efficiency. Technological achievements, including improved software, advanced protection systems and strategic cooperation with specialised partner country structures, have been identified as crucial factors in strengthening the nation's cyber defence system.

These events emphasise the importance of coordinated international efforts to address new security challenges. The practical implications of this study go beyond academic discourse, serving as a call to action for society as a whole. The findings are intended to inspire both the state and private sectors to actively support national security initiatives and confront existing threats.

In addition, the study emphasises the importance of attracting investment in Ukraine's defence sector in order to strengthen the country's economic resilience and defence infrastructure. By using advanced technologies, the Security Service of Ukraine (SSU) and other security agencies can maximise their operational effectiveness in countering aggression.

Keywords: The Security Service of Ukraine, full-scale invasion, hybrid warfare, counterintelligence activities, special operation, agent network, counterterrorism, information security, cyber defence.

Introduction

Since Ukraine declared independence, the Russian Federation has consistently sought to maintain its influence over the country, employing a wide array of methods to shape Ukraine's political, economic, and social landscape. Russia's political leadership systematically leveraged Ukraine’s reliance on energy resources to exert economic pressure, undermining its sovereignty.

A key element of this strategy involved weakening Ukraine’s military capabilities. Moscow facilitated agreements such as the Budapest Memorandum, which led to Ukraine relinquishing its nuclear arsenal, transferring strategic bombers, and over 500 long-range air-launched cruise missiles. Ironically, many of these weapons are now used by Russia to conduct massive missile strikes against Ukraine.

Russia also established extensive agent networks across various sectors, creating a "fifth column" within Ukrainian politics, subverting institutions like the Ukrainian Orthodox Church under the Moscow Patriarchate, and destabilizing the nation's social fabric. Pro-Kremlin narratives were spread widely to influence public opinion and sow division.

These actions laid the groundwork for open aggression, beginning with the annexation of Crimea and the occupation of parts of Donetsk and Luhansk regions. This eventually escalated into the full-scale war between Russia and Ukraine that continues today.

Purpose of the Article to analyze the operations of Ukraine's key security structure during the ongoing full-scale war and to identify strategies for enhancing the effectiveness of the country's special services.

Literature review

The activities of the Security Service of Ukraine (SSU) have been explored in the works of O. Sigachenko, I. Kamenetskyi, O. Melnyk, D. Lyapina, V. Bondarenko, E. Magdy, P. Sheremet, S. Leshchenko, and O. Zhdanova. Additionally, the role of the SSU in countering Russian aggression has been analyzed in publications by Y. Sokolov, T. Kuzio, V. Zubenko, and M. Martyniuk.

Materials and Methods

Following Ukraine's declaration of independence, efforts to establish new law enforcement structures to replace the Soviet-era state security apparatus began. On September 20, 1991, the Verkhovna Rada adopted a resolution to create the National Security Service of Ukraine (NSSU), which assumed the functions and resources of the Ukrainian SSR's State Security Committee (SSC).

On March 25, 1992, the Security Service of Ukraine (SSU) was officially established through the law "On the Security Service of Ukraine." The SSU was tasked with safeguarding state sovereignty, the constitutional order, territorial integrity, and the nation's scientific, technical, and defense potential. Within its legal framework, the SSU protects state secrets, counters intelligence and subversive activities by foreign entities, and addresses threats from organizations, groups, or individuals targeting Ukraine's legitimate interests and citizens' rights.

Additionally, the SSU is responsible for preventing, investigating, and combating crimes against peace and human security, terrorism, and other unlawful activities that jeopardize Ukraine's vital national interests.

The establishment of the National Security Service of Ukraine (NSSU) immediately raised pressing concerns about personnel loyalty. Since the NSSU was built on the foundation of the Ukrainian SSR's State Security Committee (SSC), most staff were former officers of the Soviet special services. This legacy posed a significant challenge to ensuring the service acted in Ukraine's interests [1].

Notably, Mykola Golushko, the final head of the SSC of the Ukrainian SSR, was appointed as the NSSU's acting head. However, upon completing his tenure, Golushko returned to Russia, reportedly taking with him some of the SSC's funds. He later occupied high-ranking positions in Russian security institutions.

Ukraine's decision to reorganize the Soviet-era security structure rather than create an entirely new force allowed the Kremlin to maintain substantial influence. From the outset, the NSSU's ranks were infiltrated with agents and spies working under Moscow's direction, compromising its ability to act independently in defense of Ukraine's sovereignty.

The development and transformation of the Security Service of Ukraine (SSU) can be divided into two distinct stages: before and after Russia's full-scale aggression against Ukraine, which began on February 24, 2022.

During the pre-war period, the Security Service of Ukraine (SSU) transitioned from being part of the Soviet Union's extensive security apparatus to functioning as an independent body of a sovereign state. However, its operations remained closely tied to the political agenda of Ukraine's leadership, particularly the president, who holds authority over the appointment and dismissal of SSU officials.

This era was marked by internal struggles between loyal officers committed to safeguarding Ukraine's state interests and agents of Russia's Federal Security Service (FSS). Russian operatives aimed to infiltrate the SSU, securing leadership roles to access classified information and undermine Ukraine's sovereignty, keeping the country under Moscow's influence.

Each presidential administration faced scandals and investigations involving SSU officials, including allegations of corruption, espionage, and misuse of power. These controversies eroded public trust in the SSU and damaged its credibility internationally. A notorious case during this period was the 2000 murder of journalist Heorhiy Gongadze, which implicated high-ranking officials, including then-President Leonid Kuchma and SSU head Leonid Derkach.

Under Viktor Yanukovych's presidency (2010–2014), Ukraine pursued closer ties with Russia, including collaboration between security agencies. During this time, under SSU leaders Valery Khoroshkovsky and Oleksandr Yakymenko, the service deviated from its core mission. Instead of protecting Ukraine's sovereignty, the SSU engaged in activities that weakened state institutions, targeting pro-Ukrainian individuals and organizations. These operations were reportedly directed from Moscow.

The extent of Russian infiltration was starkly revealed during the 2014 annexation of Crimea. Of over 2,000 SSU personnel stationed on the peninsula, only 215 chose to return to Ukraine after the occupation, underscoring the depth of compromise within the service.

Despite being marred by scandals and challenges since its inception, the Security Service of Ukraine (SSU) has consistently delivered on its mandate to safeguard state security, sovereignty, constitutional order, territorial integrity, and defense capabilities. Over the years, the SSU has refined its operations, executing numerous successful missions to combat organized crime, corruption, and terrorist threats both domestically and abroad. These efforts were often conducted in close cooperation with international partners.

Following the onset of Russian aggression in 2014, the SSU shifted its focus to countering hybrid warfare, combating separatism, and protecting Ukraine's territorial integrity. SSU personnel played pivotal roles in special operations, particularly in eastern Ukraine, demonstrating their commitment to defending the nation during a period of heightened threats and instability.

The full-scale Russian invasion of Ukraine brought unprecedented challenges to national security, threatening Ukraine's very existence as an independent state. However, the effective coordination of the nation's power structures, coupled with the courage and heroism of Ukrainian soldiers, enabled Ukraine to mount a strong defense and thwart the enemy's initial invasion plans.

The Security Service of Ukraine (SSU) played a critical role in this effort. Beyond their regular duties, SSU personnel actively participated in combat operations and undertook specialized missions during some of the most demanding and high-stakes situations, contributing significantly to the defense and resilience of the nation.

The Center for Special Operations "A" (CSO "A"), an elite unit within the Security Service of Ukraine (SSU), was established to tackle high-risk missions, including counterterrorism operations, the capture of dangerous criminals, hostage rescues, and the protection of witnesses in legal proceedings. From the very outset of Russia's full-scale invasion in 2022, CSO "A" fighters, commonly known as "Alpha", played a crucial role in defending Kyiv. They mined key logistical routes, destroyed bridges to hinder enemy movement, and successfully neutralized Russian soldiers and equipment.

In March 2022, CSO "A" conducted a daring sabotage operation behind enemy lines to eliminate a Russian control point. The unit's combat efforts were instrumental in liberating not only the Kyiv region but also parts of Sumy, Chernihiv, Kharkiv, Kherson, and Zaporizhzhia regions. CSO "A" forces, working alongside other defense units, also played a key role in the liberation of Zmiinyi Island (Snake Island).

As of August 24, 2024, according to SSU head Vasyl Malyuk, the unit's operations have contributed to the destruction of 1,152 Russian tanks, over 1,890 armored fighting vehicles, 440 electronic warfare devices, and 167 air defense systems. This tally continues to grow as CSO "A" soldiers carry out critical missions on the front lines and behind enemy lines [2].

A particularly successful unit within CSO "A" is the "White Wolf" group, which specializes in the use of unmanned aerial vehicles (UAVs) for both reconnaissance and attack missions. This highly motivated and well-trained unit has proven instrumental in the destruction of Russian military equipment and personnel.

The "White Wolf" fighters have carried out a range of successful operations, including targeting enemy logistics routes, fortifications, and ammunition depots. These strategic strikes have dealt significant blows to the Russian forces, crippling their supply lines and weakening their overall combat capability. Thanks to the unit's professionalism and expertise, they have become a vital asset in Ukraine's defense efforts.

An essential aspect of Ukraine's success in weakening Russia's military and economic potential has been the significant contributions of the Security Service of Ukraine (SSU) in both air and naval operations. Despite the Russian Navy's overwhelming presence in the Black and Azov Seas, Ukraine, with the active participation of the SSU, has achieved a historic shift in naval confrontations.

Through strategic actions, Ukraine forced Russia to relocate nearly all of its warships stationed in Crimea to the port of Novorossiysk, where they were confined to coastal bays, greatly diminishing the effectiveness of Russia's naval forces. This dramatic turn of events was made possible by the creation and deployment of innovative surface marine drones, such as the "Magura V5" and the "Sea Baby." The "Magura V5," developed by a private company for Ukraine's Main Directorate of Intelligence (MDI), and the "Sea Baby," a fully independent SSU innovation, have proven highly effective in neutralizing Russia's naval capabilities, marking a major achievement for Ukraine in its defense efforts.

The "Magura V5" drone has proven to be a game-changer in Ukraine's naval operations, demonstrating exceptional versatility and effectiveness. While capable of performing a range of tasks such as surveillance, reconnaissance, patrolling, search and rescue, mine countermeasures, and naval protection, it has gained particular notoriety for its strike capabilities.

Recognized as one of the most effective tools during the Russian-Ukrainian war, the "Magura V5" has had a profound impact on the Russian fleet. By July 2024, these drones were responsible for inflicting significant fire damage on 14 Russian warships, 8 of which were completely destroyed. This remarkable success has made the "Magura V5" one of the most impactful weapons in Ukraine's arsenal, contributing to the destruction of a substantial portion of Russia's naval forces during the full-scale invasion [3].

The "Sea Baby" is a highly versatile unmanned surface vehicle that has proven invaluable in Ukraine's defense efforts. Not only does it serve as a powerful attack drone, carrying a warhead of up to 850 kg, but it also functions as a multi-purpose platform capable of deploying various types of weapons. The drone can be used for sea mining and, thanks to its jet equipment and salvo fire system, can even carry out land-based strikes, destroying enemy targets on shore.

The "Sea Baby" has inflicted significant damage to several enemy vessels, but its most high-profile mission occurred on July 17, 2023. In a joint operation between the Security Service of Ukraine and the Ukrainian Navy, a "Sea Baby" drone was used to target the Crimean Bridge, a

critical supply route for Russian forces. The operation resulted in severe damage to the bridge's support structure and two spans, disrupting Russia's ability to reinforce its troops in the occupied Crimea. This mission highlighted the strategic impact of the "Sea Baby" and its role in weakening Russia's logistical capabilities.

Ukraine has made history as the first country in the world to create a fleet of naval drones, marking a significant milestone in modern warfare. The Ukrainian military is continuously enhancing the capabilities of its existing surface drones while also developing new technological solutions to strengthen its naval defense. One notable initiative is the *FURY* project, which aims to deploy underwater drones, further expanding Ukraine's robotic fleet.

This pioneering effort underscores Ukraine's commitment to innovation and technological advancement in the face of Russian aggression. The development and deployment of these drones have significantly bolstered Ukraine's naval and coastal defense capabilities, positioning the country at the forefront of unmanned maritime warfare.

On December 5, 1994, Ukraine signed the Budapest Memorandum, agreeing to relinquish the third-largest nuclear arsenal in the world in exchange for security assurances from the United States, Russia, and Great Britain. Throughout the 1990s and 2000s, Ukraine entered into several international disarmament agreements, leading to the dismantling of significant military assets. This included scrapping 19 Tu-160 bombers capable of carrying nuclear warheads, 60 Tu-22 missile-carrying aircraft, and 21 Tu-95MS heavy bombers.

Additionally, an agreement with Russia saw the transfer of Tu-160 and Tu-95MS bombers, along with 575 long-range air-launched cruise missiles (X-55), and related maintenance equipment. These same bombers, which Ukraine had relinquished, are now being used by Russia to launch missile strikes on Ukrainian territory since the full-scale invasion began on February 24, 2022. This painful legacy of disarmament has become a critical element in the current conflict, with Ukraine facing the consequences of giving up its nuclear deterrent.

As a result of disarmament policies in the 1990s and early 2000s, Ukraine found itself with a severely limited arsenal of long-range weapons at the time of Russia's full-scale invasion. The country had only a small number of outdated Soviet-era systems and a few modern weapons still under development or testing. In light of this, Ukraine urgently needed a cost-effective solution to strike military targets in occupied territories and key strategic sites within Russia.

The answer came in the form of unmanned aerial vehicles (UAVs), which proved to be a game-changer. UAVs are far more affordable to develop and produce than traditional missile systems, and their effectiveness was quickly demonstrated in successful attacks on Russian military infrastructure. These drones have been used to destroy enemy warehouses, airfields, logistics centers, military factories, and oil refineries, inflicting significant damage to Russia’s military and economic capabilities. This shift to UAVs has allowed Ukraine to continue striking high-value targets while minimizing costs and maintaining a strategic advantage.

From the outset of Russia's full-scale invasion, the production of unmanned aerial vehicles (UAVs) became a top priority for Ukraine’s military-industrial complex (MIC), which is composed of both state-owned and private enterprises. This sector has seen rapid growth, fueled by substantial government orders and significant investments from international partners.

In 2022, Ukraine had fewer than ten drone manufacturers, but by 2024, that number surged to nearly 90. With the right financial support, the country’s production capacity has expanded significantly. Ukraine now stands as one of the global leaders in UAV manufacturing.

At the end of 2023, Ukrainian President Volodymyr Zelenskyi unveiled an ambitious goal to produce 1 million drones by 2024. This target was surpassed within 10 months, and the new goal for the following year is set at 4 million drones. The bulk of this production will focus on first-person view (FPV) drones, as well as reconnaissance drones, medium-range attack UAVs, and long-range models capable of flying over 1,000 kilometers. This exponential growth in UAV

production highlights Ukraine's commitment to strengthening its military capabilities through innovative and cost-effective technologies.

To carry out its critical missions, the Security Service of Ukraine (SSU) utilizes a broad range of unmanned aerial vehicles (UAVs), with long-range drones playing a particularly pivotal role in special operations. These operations are conducted in close coordination with other Ukrainian military units, including the Special Operations Forces, the Main Directorate of Intelligence, and the Armed Forces of Ukraine.

Among the most notable UAVs in use are the UJ-26 "Beaver," the "Morok" with a range of up to 800 km, and the "Lyuty," which boasts a range of up to 1,500 km. Thanks to these advanced drones, Ukrainian forces have successfully targeted and destroyed key enemy infrastructure, including 36 oil tanks, terminals, and refineries, as well as dozens of warehouses storing weapons such as missiles, guided bombs, and artillery shells.

One of the most significant achievements was the attack on the "Olenya" long-range aviation airfield, located 1,750 km from Ukraine’s border. These UAV operations are also part of a broader strategy to weaken Russia’s military-industrial complex by targeting enemy factories and enterprises critical to the war effort. Through the effective use of UAVs, the SSU continues to strike critical enemy assets, significantly disrupting Russian operations.

Unmanned aerial vehicle (UAV) strikes have proven highly effective in damaging Russia’s military capabilities and delivering both practical and psychological impacts. These strikes not only inflict significant damage but also bring the war directly to the aggressor’s territory, shifting the battlefield dynamics. However, despite their successes, drones alone are insufficient to achieve the ultimate strategic goal of crippling Russia’s military and economic infrastructure to the point where it would be forced to cease hostilities.

One of the main limitations of UAVs is their relatively low speed, which makes them vulnerable to enemy air defense systems. Additionally, the payloads carried by most drones, while impactful, are not powerful enough to completely destroy critical targets like factories or military airfields. Instead, they are more effective at inflicting targeted damage to strategic enemy sites.

To achieve more decisive results, Ukraine urgently needs permission from all its international partners to carry out long-range missile strikes on Russian territory. NATO-produced long-range missiles, delivered in a timely manner and in sufficient numbers will significantly increase Ukraine's ability to strike and dismantle Russia's military infrastructure. Additionally, continuing to develop Ukraine’s own missile program is vital to achieving long-term strategic objectives and enhancing the country’s deterrence capabilities against further Russian aggression.

One of the most significant sabotage operations conducted by the Security Service of Ukraine (SSU) was the bombing of the Crimean Bridge on October 8, 2022. The attack, which involved the detonation of a truck carrying 21 tons of explosives, destroyed two spans of the road surface and severely damaged the railway section of the bridge. This operation dealt a severe blow to Russian logistical capabilities, particularly in the south, and had a profound impact on the situation along the front lines.

The destruction of the Crimean Bridge, one of the most heavily guarded structures in the world, was not only a major military success but also a huge psychological and media victory. The attack created a considerable reputational blow to the Kremlin, demonstrating the vulnerability of Russian assets in occupied territories.

The operation was meticulously planned, with SSU specialists overcoming significant obstacles, including countering enemy radio-electronic warfare and ensuring the safe delivery of the explosives. The success of this mission highlighted the exceptional professionalism and ingenuity of Ukraine’s special services, marking the event as one of the most remarkable and impactful military operations in the ongoing conflict.

In addition to its combat operations, the Security Service of Ukraine (SSU) plays a crucial role in counterintelligence and anti-terrorism efforts. The service is actively involved in identifying and neutralizing collaborators, spies, state traitors, saboteurs, and Russian agents who engage in anti-Ukrainian activities and pose a serious threat to the country's national security.

The fight against internal threats is just as vital as the battle against external aggressors. The Russian Federation employs a range of hybrid warfare tactics, including spreading its propaganda both within Ukraine and internationally, in an attempt to destabilize the country. The SSU's responsibilities extend to countering these efforts, preventing political and social unrest, and ensuring the nation's cybersecurity. This multifaceted approach is integral to safeguarding Ukraine's sovereignty and maintaining national unity during the ongoing conflict.

Among the many successful operations carried out by the Security Service of Ukraine (SSU), one of the most significant was the arrest of Viktor Medvedchuk, a Ukrainian politician and oligarch with strong pro-Russian ties. Medvedchuk, known for his close relationship with Russian President Vladimir Putin, actively promoted ideas that undermined national unity and fueled separatist sentiments in eastern Ukraine. His influence was particularly evident through the media outlets he controlled, which spread pro-Russian narratives.

The arrest of Medvedchuk marked a crucial victory in the SSU's efforts to combat pro-Russian elements within Ukraine. It sent a strong message that such forces would not be tolerated and that the Ukrainian state would take decisive action to protect its sovereignty and preserve national unity.

One of the most revealing cases of treason investigated by the Security Service of Ukraine (SSU) involved Oleg Kulinych, a graduate of the Federal Security Service (FSS) Academy, who was appointed head of the SSU in Crimea in 2020. According to materials from the State Bureau of Investigation, Kulinych was found to have actively collaborated with the FSS, following instructions from his Russian handlers to infiltrate Ukrainian state and law enforcement agencies. His activities included espionage, sabotage, and inciting Ukrainian citizens to commit acts of treason.

Kulinych had prior knowledge of the Russian Federation's plans to launch an attack from the temporarily occupied territory of Crimea, but he deliberately concealed this critical information from Ukrainian leadership. He also prevented the transmission of relevant intelligence to the central SSU and, in the early hours of the invasion, blocked all attempts to inform both the SSU leadership and the Ukrainian public about the real situation on the ground. Instead of taking measures to defend Ukraine's sovereignty, he instructed personnel to abandon their posts, undermining the nation's security at a crucial moment. This case highlights the depths of infiltration and betrayal within Ukraine's own security apparatus and underscores the SSU's ongoing efforts to root out traitors who threaten the country's survival [4].

Ilya Kyva, a former Ukrainian politician and ex-deputy of the Verkhovna Rada, became a prominent figure for his pro-Russian views and support for the invasion of Ukraine. He was known for publicly siding with the Russian Federation, making inflammatory statements, and spreading Russian propaganda. His actions were seen as undermining Ukraine's sovereignty and national security, leading to charges of treason and other serious crimes.

On November 13, 2023, the Lychakiv District Court in Lviv found Kyva guilty of treason, among other charges, and sentenced him to 14 years in prison with the confiscation of his property. Following the verdict, Kyva was declared an international wanted fugitive. On December 6, 2023, during an operation carried out by the Security Service of Ukraine, Kyva was reportedly eliminated in the village of Suponevo, located in the Moscow region. This operation is part of the broader efforts by the SSU to identify, eliminate, and hold accountable those who collaborate with the Russian Federation and promote anti-Ukrainian activities, including propagandists and war

criminals. Kyva's elimination further underscores the SSU's commitment to addressing traitors and external collaborators who pose a threat to Ukraine's national security.

The searches carried out by the Security Service of Ukraine (SSU) in churches and monasteries of the Ukrainian Orthodox Church of the Moscow Patriarchate (UOC MP) have been a subject of significant public discussion and controversy, especially given the sensitive nature of religious matters in Ukraine. These actions were part of a larger counter-intelligence operation aimed at addressing potential security threats, particularly the infiltration of pro-Russian elements within the church.

As the war with Russia escalated, the SSU conducted a series of searches that led to the discovery of a range of compromising materials. These included pro-Kremlin propaganda, political leaflets from banned Russian-backed political parties, and symbols associated with Russia. More alarmingly, some church leaders were found to possess documents indicating Russian citizenship, which raised suspicions of espionage and collaboration with the enemy. These findings were seen as evidence of efforts to undermine Ukrainian sovereignty through religious institutions.

In response, the SSU opened criminal investigations against several high-ranking UOC MP officials suspected of espionage, collaboration, and other activities that posed a threat to Ukraine's national security. Some were also accused of aiding the Russian military by providing intelligence or adjusting enemy fire.

These actions were part of the SSU's broader strategy to neutralize internal threats that could be used by the Russian Federation as part of its hybrid warfare tactics. The investigations and operations within religious institutions highlight the challenge of maintaining national security while balancing respect for religious freedoms, especially during a time of war when external threats are at their peak.

Another important direction in the context of waging an information war with the enemy is ensuring the cybersecurity of the state. Cybersecurity is the protection of the vital interests of any citizen, society and the state during the use of cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace [5]. To fulfill this task, a separate department was created in the Security Service of Ukraine, whose specialists work around the clock to counter the intelligence of foreign states in cyberspace, deal with the fight against cyberterrorism and cyberespionage, carry out counter-intelligence and operational-investigative measures, and counter attempts to destabilize the situation in the country through various information "leaks" [6]. Since the beginning of the Russian Federation's full-scale invasion of Ukraine, the SSU has identified and neutralized almost 10,000 cyberattacks and cyber incidents.

On February 15, 2022, at 8:21 p.m., a massive Distributed Denial of Service (DDoS) attack targeted Ukrainian websites, with officials attributing it to Russia. Around 15 banks, as well as government websites with the *.gov.ua* domain, were disrupted for nearly five hours. Key targets included the websites of *PrivatBank*, *Oschadbank*, the Ministry of Defense, the Armed Forces, and the Ministry for Reintegration of the Temporarily Occupied Territories. Ukrainian Minister of Digital Transformation, Mykhailo Fedorov, described it as the largest cyberattack in Ukraine's history, with losses running into millions of dollars.

Just eight days later, on February 23, a second cyberattack hit key Ukrainian government and banking websites, including the Verkhovna Rada, Cabinet of Ministers, Ministry of Foreign Affairs, and the Security Service of Ukraine (SSU). The attacks were part of Russia's broader strategy to destabilize Ukraine in the lead-up to its invasion the following day [7].

A cyberattack on Kyivstar, Ukraine's largest telecommunications operator, caused significant disruptions to the country's infrastructure and economy. The large-scale failure left 24 million Kyivstar subscribers without mobile communication and internet access. Additionally, equipment

reliant on the operator's services, including bank terminals, were affected, further complicating the situation and highlighting the vulnerabilities in Ukraine's digital infrastructure amid the ongoing conflict.

Cyberattacks, often carried out at the direction or with the direct involvement of foreign intelligence agencies, have become a constant and growing threat to Ukraine. These attacks occur almost daily, underscoring the urgent need for the country to strengthen and enhance its cyber defense systems. In response, the Security Service of Ukraine (SSU) established the Cybersecurity Situation Center on January 26, 2018. The center is equipped with a system for detecting and responding to cyber incidents, as well as a computer forensics laboratory, aimed at preventing cyberattacks, tracing their origins, and analyzing them to improve countermeasures.

Ukraine's collaboration with NATO has been instrumental in bolstering its cyber defense capabilities. In 2014, the NATO Trust Fund was launched to assist Ukraine in building its national cybersecurity infrastructure. This initiative provided Ukraine with critical equipment and software for securing the SSU's information systems. Furthermore, on May 16, 2023, Ukraine officially joined the NATO Center for Cooperation in the Field of Cyber Defense (CCDCOE). This center facilitates collective efforts to combat cyberattacks, protect the information systems of member countries, and share best practices. It also plays a key role in training cybersecurity experts, significantly strengthening Ukraine's ability to safeguard its national security in cyberspace.

Conclusion

Despite the unprecedented challenges posed by Russia's full-scale aggression, the Security Service of Ukraine (SSU) has successfully carried out its duties, playing a critical role in preserving the sovereignty and independence of the country. Throughout its history, the SSU has had to confront numerous employees who operated in the interests of the Russian Federation, but with the onset of Russia's armed aggression, a concerted effort has been made to purge the SSU of foreign intelligence operatives. This process has proven especially difficult, as it requires not only the planning and execution of operations against external threats but also the identification and neutralization of spies and traitors within Ukraine itself.

The SSU's units have displayed immense courage and resilience, effectively dismantling enemy forces across both the frontlines and deep behind enemy lines. Their high level of professionalism, morale, and resourcefulness, coupled with the use of cutting-edge technology and creative strategies, have led to numerous successful operations that have inflicted significant damage on Russia's military and economic capabilities, ultimately influencing the course of the war. Notable progress has been made in counter-intelligence and anti-terrorist activities, particularly in the detection and neutralization of collaborators and espionage networks within Ukraine, as well as in securing the nation's cybersecurity.

However, there remain concerns about the SSU's response to a large number of individuals and organizations that have been openly hostile to Ukraine since its independence. There is also the troubling issue of traitors within Ukraine's security forces, who have passed sensitive information to Russian intelligence and facilitated the annexation of Crimea and the invasion of Ukraine. Despite many successes, some special operations have failed due to information leaks, suggesting that enemy agents are still present within the SSU, and these failures have sometimes led to the capture or death of valuable service personnel. Additionally, the failure to prevent massive cyberattacks has caused significant damage to the country.

To enhance the effectiveness of the SSU, it is essential to modernize its methods, moving away from outdated practices and adopting advanced technologies and best practices from the world's leading special services. Strengthening cooperation with international partners is also crucial, including intelligence sharing, joint operations, and training exercises. Aligning with EU and NATO standards will improve the interoperability of Ukraine's security sector and support the

country's continued integration into these international organizations, further bolstering its defense capabilities.

References

1. Verkhovna Rada of Ukraine. (1992). *About the Security Service of Ukraine: Law of Ukraine dated March 25, 1992*. https://zakon.rada.gov.ua/laws/show/2229-12#Text
2. Mazur, E. (2024, August 24). "We will fight for a long time." What supports the belief in victory: We asked the leaders of the Defense Forces. *Liga.net*. https://www.liga.net/ua/politics/articles/voiuvaty-budemo-dovho-shcho-pidtrymuie-viru-u-peremohu-my-spytaly-u-kerivnykiv-syl-oborony
3. Wikipedia contributors. (n.d.). *Magura (unmanned aerial vehicle)*. *Wikipedia, The Free Encyclopedia*. Retrieved January 30, 2025, from https://uk.wikipedia.org/wiki/Magura_(безпілотний_надводний_апарат)
4. State Bureau of Investigation. (2023, July 3). Oleg Kulinich, the former head of the main department of the SSU in the Republic of Crimea, will appear in court. https://dbr.gov.ua/news/kolishnij-nachalnik-golovnogo-upravlinnya-SSU-v-ar-krim-oleg-kulinich-postane-pered-sudom
5. Verkhovna Rada of Ukraine. (2024). *On the main principles of ensuring cybersecurity of Ukraine: Law of Ukraine dated June 28, 2024*. https://zakon.rada.gov.ua/laws/show/2163-19#Text
6. Security Service of Ukraine. (n.d.). *Cyber Security Situation Center*. https://ssu.gov.ua/sytuatsiinyi-tsentr-zabezpechennia-kiberbezpeky
7. Wikipedia contributors. (n.d.). *Russian-Ukrainian cyber war*. *Wikipedia, The Free Encyclopedia*. Retrieved January 30, 2025, from https://uk.wikipedia.org/wiki/Російсько-українська_кібервійна

Служба безпеки України: ключові операції та виклики під час повномасштабної російсько-української війни

Сергій Євтух
аспірант кафедри національної безпеки
Державний університет «Житомирська політехніка»
10005, вулиця Чуднівська, 103, Житомир, Україна
e-mail: phd256232_yesv@student.ztu.edu.ua
ORCID: 0009-0006-1799-5026

Анотація. У статті досліджується діяльність Служби безпеки України (СБУ) в умовах повномасштабної війни Російської Федерації проти України. Розглянуто основні напрями роботи, методи та заходи, що здійснюються для протидії існуючим викликам і загрозам національній безпеці держави. Проведено аналіз ефективності роботи СБУ та пошук шляхів удосконалення роботи служби.

Поточні результати досліджень показують величезний вплив сучасних технологій як на операції на полі бою, так і на підтримку тилу, підкреслюючи їх роль у зміцненні обороноздатності. Отримані дані підтверджують, що інтеграція дронів, роботизованих систем і штучного інтелекту (ШІ) значно розширює потенціал для проведення розвідувальних місій і виконання бойових завдань з підвищеною точністю та ефективністю. Технологічні досягнення, включаючи покращене програмне забезпечення, вдосконалені

системи захисту та стратегічну співпрацю зі спеціалізованими структурами країн-партнерів, були визначені як вирішальні фактори для зміцнення системи кіберзахисту нації.

Ці події підкреслюють важливість скоординованих міжнародних зусиль для вирішення нових викликів безпеці. Практичні наслідки цього дослідження виходять за межі наукового дискурсу, слугуючи закликом до дії для суспільства в цілому. Результати мають на меті надихнути як державний, так і приватний сектори активно підтримувати ініціативи з національної безпеки та протистояти існуючим загрозам.

Крім того, дослідження підкреслює важливість залучення інвестицій в оборонний сектор України з метою зміцнення економічної стійкості та оборонної інфраструктури країни. Використовуючи передові технології, Служба безпеки України (СБУ) та інші силові структури здатні максимізувати свою оперативну ефективність у протидії агресії.

Ключові слова: Служба безпеки України, повномасштабне вторгнення, гібридна війна, контррозвідувальна діяльність, спецоперація, агентурна мережа, боротьба з тероризмом, інформаційна безпека, кіберзахист.