PONARS Eurasia
NEW APPROACHES TO RESEARCH AND SECURITY IN EURASIA

Ukraine's Current Counterintelligence Capabilities

PONARS Eurasia Policy Memo No. 833
March 2023

Eli C. Kaul[1]
Otterbein University

Ukraine suffered heavy casualties over the course of last summer. Tides turned in August when Ukrainian intelligence services and military forces began to increasingly destabilize Russian control in multiple areas, forcing Moscow "to devote more forces to counterinsurgency and internal security missions." Such achievements are remarkable considering that over three decades, the Ukrainian security apparatus has been plagued by corruption and infiltration, some of it directly linked to actions by agents from Russia. Personnel from the KGB were widely dispersed throughout the USSR, operating in overt and covert networks to combat opposition to the party from internal and external sources. Many networks disintegrated during the post-Soviet transition in the 1990s as personnel moved into lucrative positions in the private sector. However, evidence collected for research on the evolution of the SBU demonstrates that while the formal networks of Russia's security services diminished, informal networks persisted.

Even during times of immense affinity and cooperation between the two countries, operatives from Russia's Federal Security Service (FSB) cultivated networks of Ukrainian security personnel and state officials via multiple methods and embedded their own double agents into the SBU. While Kyiv has increasingly collaborated with Western intelligence services since the 2014 Euromaidan revolution, the Ukrainian authorities have needed to shuffle officers and agents to minimize exploitation and catch more infiltrators faster. Last July, the president was compelled to fire the chief of the Security Services of Ukraine (SBU) and the Prosecutor General for "improper performance of service duties." And only last month did it identify and remove a group of seven Russian agents. Still, Moscow's capacity is waning, a trend linked to Ukraine's counterintelligence improvements as well as the attrition and logistical difficulties the invasion created for Russia's intelligence agencies.

[1] Eli C. Kaul is Visiting Assistant Professor of Political Science at Otterbein University, Westerville, Ohio.

Voids On All Levels

Since Leonid Kuchma left office in 2005, the security apparatus of Ukraine has undergone a highly volatile period in which the personnel practices of its security apparatus fluctuated between patronage-based political loyalties and self-interested corruption, often intertwined. If one views the SBU as a single entity, measuring the loyalty and objectivity of its operations, the effectiveness of the organization in carrying out its core counterintelligence functions remained relatively stagnant throughout the Kuchma and Yanukovych presidencies. This intermittent period saw initial attempts to reform and correct the corruption and informal practices that tarnished the SBU and its colleagues through massive overhauls in personnel brought about by a distrustful Yushchenko administration.

This left a void in experienced personnel that the Yanukovych administration eventually filled with more experienced and frequently pro-Kremlin personnel. Many of these personnel had indirect ties to FSB operatives; some were even FSB conscripts serving as double agents. Post-Euromaidan personnel shifts saw many of these people follow Yanukovych into hiding, yet others remained. Leading up to the full-scale Russian invasion on February 24, 2022, the SBU frequently foiled attempts by foreign agents to steal military intelligence or commit subversive activities.

The SBU has collaborated with Western intelligence services since the Euromaidan era at a time when it was heavily infiltrated by Russian operatives who coordinated efforts to promote the interests of the incumbent president, Viktor Yanukovych, and of the Kremlin. Yet some personnel remained loyal to Ukrainian autonomy. The true level of influence Moscow had over Yanukovych may never be known, but evidence suggests that prior to his flight from power on February 22, 2014, Yanukovych had officials within the SBU destroy computer hard drives and remove classified data from secure networks containing the personal information of some 22,000 SBU employees. This bears repeating: 22,000 Ukrainian security personnel were apparently not upholding Ukrainian security as their top objective.

In the build-up to the Euromaidan and the subsequent protracted conflict (war) with Russian-backed separatists in Donbas, there were immense questions regarding the efficacy of governance structures and political reforms in Ukraine. In the subsequent eight years, there has been a measurable but not too remarkable improvement along the corruption front with the successes of the Western-imposed National Anticorruption Bureau of Ukraine (NABU), making life harder for corrupt officials and foreign infiltrators alike. By shrinking the capacity of officials to engage in informal financial transactions and increasing the level of transparency in the security apparatus (the SBU Twitter and telegram accounts, for example), the Ukrainian state has diminished the capacity of the aforementioned Russian agents and their networks of conspirators to operate at pre-Euromaidan levels in Ukraine.

Pre-Invasion and Post-Invasion Counterintelligence

Despite frequent SBU reforms aimed at minimizing the capacity of foreign agents to operate in Ukraine, the core function of the SBU's counterintelligence mission, current events have demonstrated that such operations continue. For example, on January 20, 2023, the SBU detained a Russian agent for ongoing collaboration with Russian intelligence services, alleging he systematically transferred information about the positioning of critical infrastructure and Ukrainian defense forces near the city of Izmail near Odesa. The SBU also detained seven "Russian agents" for transmitting coordinates of critical infrastructure facilities near Dnipro on the same day.

Interestingly, the mechanisms of infiltration and subterfuge on behalf of the FSB appear drastically reduced as the SBU's improved performance in thwarting cyber-attacks (and mitigating cyberspace vulnerabilities), monitoring channels for subversive activity, and increased level of public trust and transparency have made conditions for conducting FSB operations much more difficult. Add in the rapidly dwindling resources available to the Russian state to fund and support impactful intelligence operations in Ukraine, and it becomes no great surprise to see rapidly increasing number of FSB operations foiled in Ukraine since the outbreak of the war.

When I visited Ukraine in July and August 2021, there was a notable air of change within the few academic colleagues and SBU personnel I reconnected with. One might call it anger, frustration, or even anxiety, brought about by the assassination of Belarusian activist Vitaliy Shyshov under the tacit protection of the Ukrainian state. The event was eerily reminiscent of a series of similar circumstances in the past, including the murder of journalist Gregory Gongadze. In an informal discussion with a colleague, the lack of SBU capacity to effectively protect Shyshov directly demonstrated the organization's inability to carry out one of its core tasks in protecting individuals against the "intelligence and subversive activities" of foreign special services. I was assured that things were going to start to change rapidly, and I naively considered this a statement of frustration that would not amount to a great deal of tangible alterations in the SBU's operations. I was wrong.

The SBU's enhancements in cybersecurity and cyber counterintelligence operations have been an ongoing evolution since the Zelensky administration took power. The subsequent reforms have sought to bring the SBU closer to a "Western" counterintelligence organization and have only recently started to consistently demonstrate the efficacy of such reforms. The combination of enhanced cyber intelligence and counterintelligence capabilities with Western support and guidance has demonstrated tangible outcomes for the counterintelligence mission in the SBU. A crucial element of the improved success of the SBU in conducting its counterintelligence mission has been the support and trust of the Ukrainian people. This has been brought on through the increased effectiveness of statewide anticorruption reforms (notably the impact of NABU). Public relations reforms

internal to the SBU have also enhanced its level of public trust and, thus, the willingness of the public to inform and collaborate with SBU counterintelligence missions.

In tracing SBU activities through its Telegram and Twitter posts, its transparency has improved drastically since 2019. The disclosure of information pertaining to national security via social media (Twitter in this case) represents a thorough shift in the ability of the security apparatus to inform (or misinform) the public. The SBU began openly conveying operational capabilities (without posting detailed methods) about their counterintelligence and counter-corruption missions back in 2019. This includes providing detailed assessments of the arrests of their own personnel for abuse of office, and describing the use of a Telegram bot to live-report enemy positions and activities. This level of communication with the public, including the openness to describe agency shortcomings, is a dramatic shift in the behavior of the post-Soviet security apparatus.

The SBU's general Twitter activity is in **Table 1**. As can be seen in the table, from January 1 to August 10 of 2022, the activity level on the SBU Twitter account increased dramatically, with a record number of tweets (884) and average retweets (229.3) that were largely inflated by increased public awareness because of the invasion. The number of tweets and their content indicates the level of transparency and the retweets depict the level of dissemination of that information. The data demonstrate that the information from the SBU's tweets has been more widely distributed since the invasion than before, while the transparency itself began in mid-to-late 2021.

Table 1. Tweets and Retweets by the Security Services of Ukraine (SBU)

	2019	**2020**	**2021**	**2022**
Tweets	747	780	745	884
Retweets (average)	48.4	46.8	55.4	229.3

Since the invasion, the SBU has incorporated a designated spokesman to share information with the public and caution about security threats. This increased presence on social media has coincided with an increase in collaboration between the SBU and the public to aid in the resistance to the Russian invasion. On February 28, just four days after the invasion started, the SBU cyber-ops launched a chatbot feature that enables citizens to post information about the movements of Russian forces within the territories of Ukraine. This feature has improved the SBU's ability to assist Military Intelligence in locating Russian troops, but it has also proven useful in receiving tips about collaborators and infiltrators.

The effectiveness of the SBU's counterintelligence capabilities in rooting out and apprehending (when possible) collaborators and infiltrators has been impressive. However, the presidential removals in 2022 of SBU chief Ivan Bakanov and Prosecutor

General Iryna Venedyktova for failing to adequately tackle infiltrations indicate that Russian subversions still flourish in Ukraine. Upon closer reflection, however, this act may signify real progression in the ability of the Ukrainian state to hold its security apparatus personnel accountable and even, as I will argue, demonstrates a positive sign for improving the performance of SBU personnel amidst a period of high demand for their best performance.

Meanwhile, the FSB has been relegated to contacts with the remnants of its preexisting networks within Ukraine. Many of these are likely being closely observed by counterintelligence personnel but allowed to continue operating because of the value intercepted communications with their Russian minders have for the Ukrainian Defense. One particular aspect that likely has diminished FSB capabilities within Ukraine is the increased necessity to focus efforts on the anti-war movement within Russia itself. The recent death of Darya Dugina demonstrates the increased destabilizing capabilities of the anti-war movement in Russia.[2] Because a core mission of all organizations inheriting the role of the KGB is focused on internal surveillance, it is possible we will see an even greater reduction of the FSB in the Ukrainian theater.

Conclusion

The Russian FSB has seen diminishing returns on its intelligence collection and operations not just in the Ukrainian region but elsewhere around the globe because of the war. The Ukrainian SBU has generated successes in identifying and apprehending infiltrators of the Ukrainian political and security apparatus. The war has not prevented the SBU from carrying out its other functions as well. The SBU continues to investigate illicit activities such as lower-level corruption, trafficking in drugs and counterfeit goods, and even war profiteering.

Yes, the Ukrainian president has withdrawn his support from many high-ranking security apparatus officials. At face value, this appears to indicate a major problem within the SBU and its colleagues in the security apparatus; however, these personnel changes convey an improved evolution of the Ukrainian security apparatus that demands higher standards from its personnel. The continued collaboration with the West on intelligence and defense matters further indicates a positive trend in the evolution of the SBU's counterintelligence capabilities moving forward. What is crucial is that the momentum gained by these successes is not lost as things begin to normalize and, hopefully, quiet down. The war has displaced many people, and as Ukrainians begin to return home from abroad, there is a high likelihood that Russian operatives may be among them. For the positive trajectory of the SBU to be maintained, it is vital that the repatriation process does not inhibit the rights

[2] Dugina's assassination (as well as attacks on the Crimea bridge and suspicious fires throughout Russia) could be seen as signs of a weakened Russian intelligence apparatus. It is possible the apparatus has been focusing on threats closer to Putin and the elite. Such events, however, could also depict potential Kremlin false flag operations.

of Ukrainians while simultaneously ensuring that foreign operatives are restricted from entry—or at least monitored closely should they return.

PONARS EURASIA NEW APPROACHES TO RESEARCH AND SECURITY IN EURASIA

Elliott School of International Affairs
THE GEORGE WASHINGTON UNIVERSITY