2026

SITUATION IN RUSSIA

Pax Consulting

28-06-2026

Index

1. A YEAR AGO

On June 1st, 2025, Ukraine attacked Russia hundreds of kilometres inside Russian soil. Ukraine called it Operation Spiderweb.

Operation Spiderweb was a bold and catastrophic coordinated drone swarm attack, executed by the Security Service of Ukraine (SBU) **against Russia's strategic aviation.** Under the direction of Vasyl Maliuk, the operation required eighteen months of meticulous preparation and represented **a milestone in the history of unmanned vehicle warfare.**

The sabotage tactics used were described by NATO experts as a reinvention of the "Trojan Horse method," as they managed to strike targets thousands of kilometres deep into Russia, completely bypassing anti-aircraft and ground defences. The sabotage was executed as follows:

- **Infiltration and camouflage:** Instead of launching the drones from Ukraine, the devices were hidden inside cargo containers, cabins, or specially designed wooden crates. The preparation phase took place directly on Russian territory, even in cities like Chelyabinsk, just a short distance from Russian intelligence agencies (FSB).
- **Blind transport:** The drones were loaded onto trucks and transported for over 5,000 kilometres by Russian truck drivers who were completely unaware of the nature of the cargo they were carrying. The vehicles were strategically positioned in multiple locations near Russian administrative divisions such as Murmansk, Irkutsk, and Amur, and in cities like Ivanovo and Ryazan.
- **Simultaneous remote attack:** At the exact moment designated for the offensive, the roofs of the containers were opened via remote control, releasing swarms of drones *en masse*.

The drones simultaneously attacked four strategic airbases: Belaya, Olenya, Dyagilevo, and Ivanovo (a fifth base, Ukrainka, could not be reached).

The results of Operation Spiderweb were devastating to Russian strike capabilities:

- Damage to 41 military aircraft, with an estimated cost of over $7 billion.
- The incapacitation of 34% of the Russian cruise missile bomber fleet, affecting heavy and supersonic strategic bombers such as the Tu-95MS "Bear," Tu-22M3 "Backfire," and Tu-160 "Blackjack."

- The destruction of crucial A-50 "Mainstay" early warning aircraft, as well as transport and refuelling aircraft like the An-12 "Cub" and Il-78 "Midas".

Beyond the enormous material losses, the tactic demonstrated that **Ukraine does not need to match Russia in the number of combat aircraft;** it is enough to sow distrust within Russian supply chains to crumble the integrity of their systems from the inside. The success of this operation generated a **strong sense of vulnerability in the Kremlin,** and the director of the SBU has warned that they are already preparing "new surprises" that will be equally painful.

2. THE SAINT PETERSBURG INTERNATIONAL ECONOMIC FORUM (SPIEF).

On June 3, 2026, another impactful attack was carried out by Ukraine against Russia.

The attacks surrounding what is often referred to as the Russian equivalent of the G7 or Davos—the **St. Petersburg International Economic Forum (SPIEF)**—were a highly symbolic and coordinated drone offensive carried out by Ukraine to disrupt Vladimir Putin's showcase event.

The SPIEF is an annual three-day event that historically served as Russia's premier gathering to attract Western

investors, but since the invasion of Ukraine, it has transitioned into a major propaganda tool for the Kremlin. This year, the forum expected around **20,000 guests from 130 countries** and featured a planned address by Vladimir Putin to project an image of regional power and economic stability. However, on the night between Tuesday and Wednesday, just as the forum was being inaugurated, **Ukraine launched a massive attack** deliberately designed to "spoil the party".

Ukraine launched a **swarm of over 350 drones targeting the cities of Moscow and St. Petersburg.** A primary target was a major oil terminal located in the Gulf of Finland in St. Petersburg, which is one of Russia's largest storage and export facilities. The psychological and physical proximity of the attack was notable: **the targeted oil terminal is situated a mere 17 kilometres away from the Expoforum convention centre** where the SPIEF was being held.

Images distributed on social media showed thick columns of black smoke rising over the golden domes of St. Petersburg. While the local Russian governor, Alexander Beglov, claimed there were no fatalities, he acknowledged that several pieces of infrastructure were damaged in the resulting fires.

The Security Service of Ukraine (SBU) orchestrated these attacks to **puncture the "anti-aircraft bubble" and shatter the illusion of security** that the Kremlin attempts to sell to the Russian public. **The SBU pointed out the hypocrisy of the forum's official motto, *"Pragmatic dialogue: the path to a stable future",*** contrasting it with Russia's ongoing aggression and recent missile strikes on Ukrainian cities that left dozens of civilians dead.

By striking St. Petersburg on the exact day Putin inaugurated his flagship forum, Ukraine sent a clear message that Russia's deep rear is no longer safe. Ukrainian forces defended the operation by stating that their campaign aims to block the production and sale of oil and gas, warning that **as long as Russia chooses war over peace, the facilities and petrodollars that finance its aggression will continue to burn.**

Key details on how this attack was executed and the magnitude of the operation against St. Petersburg:

- **Very long-distance attack:** The attack demonstrated that geographical distance is no longer an obstacle for Kyiv's forces. The oil terminal at the Greater Port of St. Petersburg, located in the Gulf of Finland, is situated 1,100 kilometers from the Ukrainian border.
- **Coordinated swarm and multiple targets:** The operation was not limited to a single point but was executed using

a massive "drone swarm." Ukrainian President Volodymyr Zelensky confirmed that, in addition to the oil terminal, they managed to **strike the Kronstadt military base (located west of St. Petersburg) and the Michurinsky Progress enterprise (a factory in the Tambov region dedicated to the production of precision weaponry components).**

- **Direct and visible impact:** The attack managed to penetrate Russian defences, causing several explosions. Russian social media was filled with images showing thick columns of black smoke rising above the city's historic golden domes. Faced with the evidence, **the Russian Governor of St. Petersburg, Alexander Beglov, had to publicly acknowledge that "various" infrastructures were damaged,** although he stated that there were no fatalities.
- **Prior knowledge of the terrain:** This attack was not by chance. Ukrainian forces already had the measure of this strategic target, as in January 2024 they had managed to reach this exact terminal with another drone, causing a fire when it was shot down over it.

In summary, the attack was perpetrated by launching a **swarm of long-range drones that flew over a thousand kilometres to execute simultaneous precision strikes** against energy infrastructure and military bases deep within the Russian rear.

3. INTELLIGENCE EFFORT

Previous operations require an enormous quantity of information in order to produce **high quality and actionable intelligence.**

Gathering information on the anti-air defence system, technical capabilities to track containers and drones, knowledge of the installations, sources on the ground to report before and after the actions were required to carry out the operations. It means money, resources, time and determination.

It's also worth noting that it is the SBU, the Ukranian domestic intelligence service, the one in charge of carrying out these operations. It mimics the FSB —also the Russian domestic intelligence service— who is in charge of the Russian near abroad (former USSR territories). It's like a joke but the SBU also considers Russia as its own near abroad.

A document unveiled by the outlet VSQUARE (see annex), shows reflections of the Directorate of Coordination, Analysis, and Control of Activity of the First Service(counterintelligence) of the FSB. The document reveals information gathered between January and May 2024.

It highlights a significant **surge in foreign intelligence activities directed against Russian individuals with access to state secrets** across two periods. Here are the specific numbers mentioned:

Overall Foreign Intelligence Actions

- **2017–2021:** Russian security agencies detected **1,953** intelligence actions carried out by foreign special services.
- **2022–Present (2024):** The number of detected actions grew to **2,874.**

Ukrainian Intelligence Activity

- From 2022 to the present (2024), Ukrainian intelligence services carried out **1,960** of the detected actions, which accounts for more than **50% of the total.**
- This figure represents a **7.5-fold increase** in the activity of Ukrainian special services compared to the 2017–2021 period.

Due to Western sanctions reducing foreign travel and tightened security around state secrets, **intelligence services shifted heavily toward internet-based recruitment contacts** (online recruitment and targeting):

- Between 2022 and 2024, **3,457 cases** of internet recruitment attempts were detected, reflecting a **5.5-fold increase.**
- The proportion of these online recruitment attempts out of the total volume of detected intelligence actions skyrocketed from **6% in 2017 to 90% at present.**
- When looking solely at Ukrainian special services, their use of online recruitment methods jumped from **20% in 2017 to 98% at present.**

Additionally, between January and May 2024, foreign adversaries collected data on over **13,500 Russian citizens** via open-source intelligence (OSINT) and technical communication channels. Out of these, **1,860** had access to state secrets and **603** were military personnel from the Russian Ministry of Defence.

Don't forget **this is the FSB talking of the adversaries' activities against their interests.** It means that the mentioned data are detected actions, and it means that the universe of actions is larger.

Numbers mean that Ukraine has exponentially increased its targeting and recruitment efforts. This is important because the SBU at the beginning of the Russian invasion was heavily penetrated by Russia. This increase reflects the cleansing that has taken place and its positive results.

Given that the first period covers exactly 5 years (2017-2021) and the second period covers approximately 2.5 years (from early 2022 to May 2024, the date the report was written), the recalculation yields the following picture:

Period 1 (2017 — 2021): 5 years in duration

- **Total:** 1,953 actions / 5 years = ~391 actions per year.
- **Ukraine:** 261 actions / 5 years = ~52 actions per year.
- **The West:** 1,692 actions / 5 years = ~338 actions per year.

Period 2 (2022 — mid-2024): ~2.5 years in duration

- **Total:** 2,874 actions / 2.5 years = ~1,150 actions per year.
- **Ukraine:** 1,960 actions / 2.5 years = ~784 actions per year.
- **The West:** 914 actions / 2.5 years = ~366 actions per year (even if we were to round up to 3 full years, it would be about 304 actions annually).

3.1 Conclusions

Ukraine has deployed an incredible effort to keep Russia at bay. The effort is bearing fruit.

The West is keeping the activity level although the number of targets present in the West has been heavily reduced after the **large number of expulsions** that took place between March and May 2022. They have reduced in half the presence of Russian intelligence services agents in the West. And the West has imposed sanctions (travel ban).

Many government officials (diplomats and members of the Presidential Administration) used to spend holidays in Spain or Italy and many own properties in the West. They have changed those trips to Turkey and other destinations which are still available in line with Kremlin rules.

Despite those limitations the West has been able to keep its level of activity trying to approach and recruit Russian assets.

As the document notes, Western sanctions drastically reduced Russian citizens' foreign travel, eliminating the United States' preferred tactic of intercepting and physically coercing them at borders and airports. To maintain its level of activity—those roughly 366 actions per year—the West had to carry out **a forced and successful transition toward digital espionage, now relying on Open-Source Intelligence (OSINT) and leaked databases.**

4. CONSEQUENCES IN RUSSIA

The perception of **insecurity in Russia has grown significantly** as Ukraine successfully brings the consequences of the war directly into Russian territory. Audacious long-range drone attacks, such as the strikes targeting the St. Petersburg International Economic Forum (SPIEF) and the massive Operation Spiderweb, were deliberately orchestrated to puncture the Kremlin's "anti-aircraft bubble". By striking deep within Russia's borders—sometimes over 1,000 kilometres away —Ukrainian forces have shattered the illusion of safety and the "quiet life" that the Russian government attempts to project to its public. These operations have generated **a profound sense of vulnerability across the country,** demonstrating that the logistics, fuel terminals, and military bases supporting the aggression are no longer safe.

This rising tide of insecurity has deeply affected **Vladimir Putin, triggering severe paranoia and a drastic change in his personal behaviour.** A major turning point was the assassination of Ayatollah Ali Khamenei in Tehran, which was **facilitated by Israeli intelligence hacking into local traffic cameras and using artificial intelligence to track his movements.**

Terrified that foreign intelligence could similarly hijack Russia's own vast surveillance apparatus to target him, **Putin took extraordinary precautions. Russian security services were forced to shut down parts of the special surveillance system protecting the president and his closest aides,** only turning it back on after engineers worked to hermetically **seal it off from the internet** to prevent third-party hacking.

Driven by an escalating fear of a drone assassination or even a coup d'état, **Putin has retreated into extreme isolation.** He is reportedly spending far more time inside **underground bunkers** than in his official Kremlin office. Furthermore, he has imposed **draconian restrictions on his immediate entourage to prevent any digital footprint that could reveal his exact location.** Close collaborators, including bodyguards, cooks, and photographers, are strictly prohibited from using public transport, and they are **forbidden from carrying mobile phones or any internet-connected devices** while in his presence.

5. ANEXO. FSB DOCUMENT (VSQUARE).

Совершенно секретно

(п. 1.34 Перечня - приказ № 0180 -2022 г.)

ОБЗОР

практики выявления разведывательных акций в отношении секретоносителей по закрепленным за головными подразделениями ФСБ России сферам деятельности, в том числе вербовочных выходов по сети Интернет

Во исполнение решения Директора ФСБ России от 15.01.2024

№ 16/2/753 1 Службой ФСБ России совместно с головными подразделениями ФСБ России проведен анализ практики выявления разведывательных акций по закрепленным сферам деятельности, в том числе вербовочных выходов по сети Интернет.

Результаты свидетельствуют, что после начала СВО фиксируется многократный рост количества разведывательных акций иностранных спецслужб в отношении секретоносителей.

В период е 2022 года по настоящее время органами безопасности выявлено 2874 разведывательных акuий иностранных спеuслужб, тогда как е 2017 по 2021 гг. только 1953 разведывательные акции противника.

Установлено, что в указанный период наибольшее количество разведывательных акций в отношении секретоносителей осуществлено спецслужбами Украины - 1960, что составляет более 50 % от общего их числа и свидетельствует об увеличении активности украинских спецслужб в 7,5 раз в сравнении с 2017-2021 гг.

Объектами разведывательных устремлений спецслужб Украины являлись военнослужащие ВС России, работники ОПК и ядерно-оружейного комплекса, объектов оперативного обеспечении по линии «М», сотрудники ОГВУ, КФС и дипломатического корпуса, сферы транспорта, представители научной и образовательной и отрасли «связь».

На канале выезда за границу разведывательные акuии осуществлялись спецслужбами США и их союзников по НАТО к лицам:

- находящимся в длительных либо краткосрочных

загранкомандировках;

- трудоустроенным в российских организациях, попавших под санкции, и осведомленных в «чувствительной» информации.

Сбор данных в отношении представляющих интерес граждан РФ ведется противником с использованием агентурного аппарата, мониторинга открытых источников, электронных отраслевых и корпоративных ресурсов.

Спецслужбы США, используя информацию систем бронирования билетов, гостиниц и регистрации на международных мероприятиях, отслеживают прибытие представляющих разведывательный интерес российских граждан и заблаговременно создают условия по их вербовочному изучению. Приоритет отдается лицам, неоднократно выезжающим в служебные командировки.

Для установления личных контактов американские спецслужбы

используют пункты пограничного и миграционного контроля в аэропортах с привлечением местного персонала.

При прохождении пограничного контроля объекты вербовочной разработки подвергаются «жесткому» допросу о профессиональной сфере деятельности, включая принудительный сбор биоматериала, изъятие документов, средств связи и вычислительной техники, а также истребование парольно-логиновых комбинаций к устройствам и почтовым учетным записям.

Вербуемым предлагаются конкретные формы поощрения за конфиденциальное сотрудничество, например, содействие в получении американской визы, либо оказывается давление с угрозой аннулирования виз. После всестороннего анализа личностного и поведенческого профилей объектов заинтересованности принимается решение о целесообразности дальнейшей разработки, в том числе вербовки.

В условиях вызванного санкционной политикой стран Запада сокращения зарубежных поездок секретоносителей в страны

НАТО, а также ужесточения режимных мер в области защиты государственной тайны, отмечается возрастание более чем в 5,5 раз числа вербовочных выходов на секретоносителей по сети Интернет, которых с 2022 по 2024 гг. выявлено 3457 фактов. Их доля в общем объеме выявленных разведывательных акций

возросла с 2017 года до настоящего времени с 6 % до 90 %, применительно к украинским спецслужбам – с 20 % до 98 %.

В 2024 году противник скорректировал тактику поисково-вербовочной деятельности. Так, в 5 раз увеличилось количество персонифицированных зондирующих и вербовочных выходов на объекты разведывательного интереса в Интернет-мессенджерах, а массовые телефонные звонки и спам-рассылки с предложениями сотрудничества или предоставления информации российским секретоносителям,~ сотрудникам объектов связи, транспорта и промышленности, военнослужащим, состоящим в виртуальных тематических группах на платформах «Вконтакте», «Одноклассники» приобрели агрессивный характер и осуществляются с позиций подконтрольных спецслужбам Украины т.н. «мошеннических колл-центров».

Последний прием, по нашим оценкам, направлен для отвлечения сил

и средств контрразведывательных подразделений, маскировки устремлений к истинным объектам разработки.

Для поиска и изучения объектов вербовочного интереса иноспецелужбы активно применяют современные методики разведки по открытым источникам данных (OSINT) и Интернет-сервисы «пробива», содержащие персональные и контактные данных граждан России (адреса работы, реквизиты средств связи, номера автотранспорта и т.п), осуществляют мониторинг переписки участников деструктивных и иных представляющих оперативный интерес виртуальных групп в социальных сетях и Интернет-мессенджерах.

По имеющимся в 1 Службе ФСБ России материалам, в январе-мае 2024 года противник осуществлял сбор в ОТКС данных.

в отношении более 13500 граждан России, из которых 1860 являются секретоносителями, 603 – военнослужащими МО РФ.

В ходе установления контактов представители спецслужб Украины:

- демонстрируют осведомлённость о биографических данных и родственных связях объекта интереса, предлагают денежное вознаграждение за предоставление информации, оказывают психологическое давление путем запугивания возможными сообщениями в российские правоохранительные органы о якобы имевших место ранее фактах передачи украинской стороне секретных

материалов, публикацией сведений компрометирующего характера, угрозами жизни и здоровью;

- применяют методы социальной инженерии для получения скрытого удаленного доступа к аккаунтам мессенджеров российских граждан, находящихся в вербовочном изучении, прежде всего бывших **и** действующих секретоносителей объектов ОПК и военнослужащих МОРФ;

- используют мошеннические схемы для инициирования перевода гражданами России денежных средств на счета, используемые для подпержки воинских формирований Украины с последующим побуждением их к осушествлению разведывательных или диверсионных акций под угрозой передачи сведений о факте «финансирования ВСУ» спецслужбам РФ.

Отмечаем, что подавляющее большинство разведывательных акций вскрыто ОБВ (68 процентов от общего числа) в результате инициативных обращений в органы безопасности военнослужащих о выходах на них иностранных спецслужб, что свидетельствует о выстроенной эффективной системной профилактической работе на объектах МОРФ. При этом с начала СВО указанная тенденция прослеживается наиболее явно.

Вместе с тем анализ добываемых 1 Службой ФСБ России сведений об объектах устремления противника свидетельствует о том, что доля военнослужащих *в* их объеме не превышает 30 процентов. Полагаем, что данное обстоятельство является следствием имеюшихся недостатков.

в организации профилактической работы на объектах оперативного обеспечения ТОБ, ослабления межлинейного взаимодействия и координирующей роли контрразведывательных подразделений. Неоднократно в результате разработки аккаунта противника выявлялись

массовые вербовочные и зондирующие выходы на сотрудников предприятий

ОПК, в отношении которых ТОБ несколько месяцев информацией не располагал.

Кроме этого изучение отчетных материалов показывает, что получаемая самостоятельно на местах информация о сетевых реквизитах

секретоносителей и иных сотрудников режимных объектов, а также объединяющих их групп в ряде случаев пассивно накапливается и не задействуется в поисковых мероприятиях для выявления признаков поисково-вербовочной деятельности иноспецслужб. Попытки перехвата

устремлений противника и технического проникновения на его средства

коммуникаций носят фрагментарный характер.

В отдельных случаях сведения об обращениях с признаками вербовочных и зондирующих выходов поступают из ТОБ в 1 Службу ФСБ

России со значительными временными задержками, что не позволяет своевременно выявлять объекты заинтересованности иноспецслужб, купировать их вербовочные выходы, создавать условия для проведения встречной разработки и проведения контрразведывательных…

для проведения встречной разработки и проведения контрразведывательных мероприятий.

С учетом изложенного необходимо:

1. Активизировать профилактическую работу на объектах контрразведывательной защиты, обеспечить актуальный учет виртуальных групп и сообществ режимных организаций, усилить агентурный контроль за действиями их участников и администраторов, а также межлинейное взаимодействие на данном направлении оперативно-служебной деятельности. Информацию о проведенных мероприятиях и их результатах включать в отчётные материалы по КП «Пассаж».

2. Информировать 1 Службу ФСБ России о наличии оперативных позиций в интернет-сервисах OSINT и «пробива» для последующего совместного выявления и разработки аккаунтов представителей иноспецслужб.

3. Организовать накопление сведений об участниках проукраинских и иных деструктивных Интернет-сообществ и использовать их при проведении автоматизированного сравнительного анализа с реквизитами средств связи

секретоносителей (в том числе военнослужащих) и результатами контрразведывательного поиска на технических каналах связи. Добытые материалы также направлять в 1 Службу ФСБ России для учета в ведущихся подсобных информационных

:массивах.

Одновременно сообщаем, что обобщенные сведения об участниках деструктивных «Telegram»-каналов необходимо получить из ЦБД.

УКАКД 1 Службы