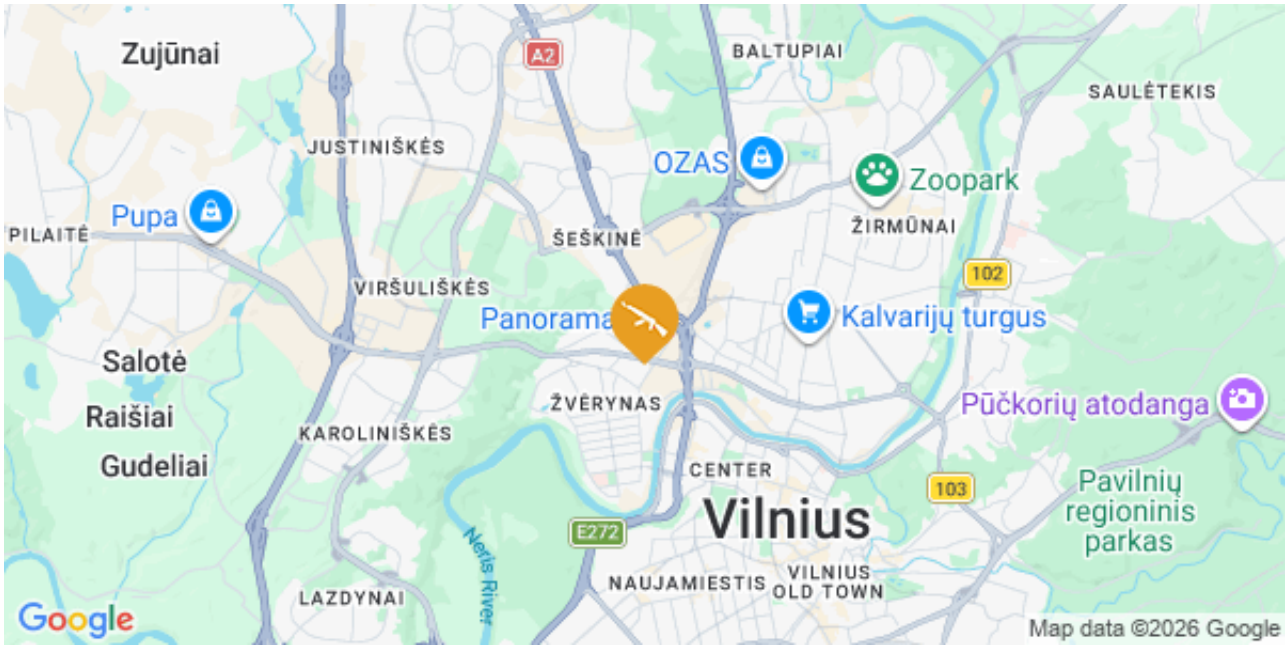
Militancy/Terrorism



29
APR
12:31 UTC

Lithuania Alert: 13 suspects charged over Russian-linked attempted assassinations in Vilnius on April 27; elevated risk of Russian covert operations to persist

Current Situation

- On April 27, authorities charged 13 individuals for planning the assassinations of two individuals in Vilnius, linking the plot to Russia's military intelligence service GRU following an investigation launched in early 2025.
- One of the victims is a pro-Ukraine Lithuanian national involved in fundraising activities for Ukraine, while the other is a Russian dissident and activist for the rights of Bashkirs, a minority in Russia, who has been given asylum in Lithuania.
- The suspects, who are from Belarus, Georgia, Greece, Latvia, Moldova, and Russia, allegedly conducted surveillance of the targets' homes and workplaces and exchanged guidance on acquiring weapons.
- Nine suspects have been arrested in Lithuania and abroad, while the remaining four have been identified and are being tracked by authorities. The investigation began when one of the targets discovered a tracking device placed on his vehicle in early 2025.
- Moreover, Lithuanian authorities noted that the same network may be linked to a separate arson incident involving military supplies intended for Ukraine in Bulgaria, as well as suspected intelligence-gathering activity targeting Greek military establishments. Ukrainian officials also indicated the group had plans to target Ukrainian journalists and an intelligence officer. Though exact details on these plots remain unconfirmed.

Source: Reuters

Assessments & Forecast

1. The above reiterates the elevated risk of Russian covert operations in Lithuania, including targeted attacks against individuals and entities that are anti-Kremlin or pro-Ukraine, as well as espionage and sabotage activity. This is supported by the precedent of similar plots and attacks in recent years, notably the March 2024 attack on Leonid Volkov, former chief of staff to the late Russian opposition leader Alexei Navalny, in Vilnius, which Lithuanian authorities attributed to Russian special services. Polish nationals were also detained for carrying out the assault, and a Belarusian national was suspected of coordinating it. Additional incidents include two attempted arson attacks in Lithuania in September 2024 targeting a defense manufacturer supplying military equipment to Ukraine, as well as a May 2024 arson attack targeting a Swedish company's retail outlet in Vilnius, which authorities have linked to the GRU.
2. The reported surveillance of targets' homes and workplaces, the use of a tracking device, and discussions around acquiring weapons indicate that the plot had progressed beyond initial planning into an advanced preparatory phase. Also, the profile of the targets fits into the target pattern of Russian covert activities, with the focus on a pro-Ukraine Lithuanian national and a Russian dissident granted asylum, indicating an intent to intimidate local support networks for Ukraine, suppress anti-Kremlin activism abroad, and signal operational reach into host countries perceived as aligned against Moscow.
3. Furthermore, the network's suspected involvement in arson targeting military supplies intended for Ukraine in Bulgaria, as well as intelligence-gathering against military structures in Greece, underscores the persistent threat posed by Russian-linked sabotage activity targeting Ukraine-related supply chains, defence infrastructure, logistics networks, and commercially accessible sites supporting Ukraine. Notably, as of February 2026, European authorities have reported over 150 suspected incidents of Russian covert activity since the start of the full-scale invasion in February 2022, highlighting the scale and continuity of this threat.
4. The network's composition, including the 13 suspects from multiple countries recently charged, illustrates Moscow's reliance on organized, multi-actor cells to carry out operations in Europe. Such structures allow tasks to be distributed across individuals, making operations more difficult to attribute and fully dismantle. This is further evidenced by September 2025 reports indicating that approximately 89 percent of Russian-linked sabotage and attack activities in Europe involve multiple perpetrators rather than lone actors.
5. The backgrounds of the suspects further reinforce this pattern. With many originating from Eastern European countries, including Belarus, Georgia, Latvia, Moldova, and Russia, the case suggests a continued reliance on operatives from the wider post-Soviet space, wherein Russia still wields considerable influence. Such individuals likely offer advantages, including regional mobility, Russian-language fluency, and access to diaspora or criminal networks, while also attracting less immediate scrutiny than official Russian personnel. This approach has been observed in other cases, including a reported April 2024 arson attack at a hardware store in Warsaw allegedly carried out by a Belarusian national. The use of such operatives provides Moscow with a degree of plausible deniability.
6. **FORECAST:** Amid the protracted Russia–Ukraine war, sustained European support for Kyiv, and expanding deterrence measures, such as increased NATO forward deployments, military aid packages, sanctions regimes, and efforts to reduce dependence on Russian energy, the risk of Moscow-backed covert operations is likely to further increase Europewide, including in Lithuania. These operations will likely include assassination attempts, sabotage, and espionage, with Moscow seeking to intimidate pro-Ukraine countries, undermine public support for continued assistance to Kyiv, and signal its ability to operate across Europe.
7. **FORECAST:** Russian-linked sabotage is likely to prioritize defense companies and their personnel, as well as transport and logistics infrastructure supporting Ukrainian military and commercial supply chains. This is evidenced by Moscow's April 16 warning to the UAV companies in Europe supporting the Ukrainian military as 'potential targets." Energy assets, including offshore and

undersea infrastructure, will also remain high-risk targets due to their strategic impact on supply disruption and European efforts to reduce reliance on Russian energy. Beyond strategic sectors, Moscow is likely to continue targeting commercially accessible, non-critical entities, such as retail outlets and shopping centers, to generate media attention and public disruption.

Recommendations

1. Travel to and within Lithuania can continue as normal; however, individuals are advised to maintain heightened vigilance near military facilities, logistics centers, and sites associated with Ukraine support, particularly if security activity is observed.
2. Organizations and individuals linked to Ukraine aid, transport, or defense supply chains are advised to remain alert to suspicious activity, including surveillance or unauthorized access attempts, and to report concerns to authorities promptly.
3. Limit public disclosure of sensitive operational details, such as shipment schedules, infrastructure locations, or personnel movements, particularly on open-source or social media platforms.
4. Organizations should implement continuous online threat monitoring, including tracking open-source platforms, social media, and messaging apps for indicators of hostile reconnaissance, recruitment efforts, or emerging threats.
5. For further questions and risk assessments, please contact intel@max-security.com