Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Oleksandr Levchenko

Russia expands its sabotage operations in Europe targeting defence industrial infrastructure



A sabotage network has been uncovered in Romania whose members, according to local intelligence services, were acting on behalf of Russian intelligence agencies and preparing attacks on defence industry facilities in European Union countries.

The Romanian Intelligence Service (SRI) identified a group involved in an attempted arson attack on the Carfil arms manufacturing plant in Brașov.

The investigation established that three citizens of post-Soviet states, legally residing in EU countries, were involved in preparing the sabotage operation. The SRI emphasised that the activities of the uncovered network were not limited to Romania.

Russian handlers had identified a number of potential targets across the region, including state-owned and private defence industry enterprises, as well as other facilities of military and industrial significance.

The Wall Street Journal reported that Russian President Vladimir Putin had personally ordered an intensification of sabotage operations against NATO member states.

According to the publication, an unsuccessful drone attack attempt near Leipzig Airport was among the first operations conducted as part of this campaign.

A series of other incidents subsequently occurred across Europe. In August, arson attacks targeted drone manufacturing facilities in Estonia and Poland.

Slovak authorities reported foiling a similar attempt. Poland, Lithuania and Bulgaria also reported sabotage incidents targeting the ground infrastructure of the Starlink satellite system.

Defence industrial infrastructure

The exposure of a Russian sabotage network in Romania demonstrates that Europe's defence industrial infrastructure is becoming one of the priority targets of Russia's hybrid operations.

The objective is not merely to cause direct damage to production facilities, but also to obstruct the expansion of European arms manufacturing and the provision of military assistance to Ukraine. For Romania, this incident represents a direct national security challenge.

The intensification of sabotage activities can be viewed as one of Russia's attempts to extend its confrontation with the West beyond the immediate theatre of military operations in Ukraine.

Moscow uses covert operations to create additional security and political challenges for European governments while avoiding direct military confrontation with NATO member states.

> The potential economic consequences of these operations are another important factor

Such activities allow Russia to test the effectiveness of counterintelligence agencies, identify vulnerabilities in critical infrastructure and assess European countries' readiness to respond collectively to hybrid threats.

The potential economic consequences of these operations are another important factor.

The need to strengthen security at industrial facilities, modernise protection systems and restore damaged infrastructure increases costs for manufacturers and national budgets.

The threat of further attacks may also undermine the defence sector's investment appeal at a time when European countries are seeking to expand their domestic production capacities.

Attacks on Starlink infrastructure

Following incidents involving Starlink ground stations in Poland and Bulgaria, Russian intelligence services reportedly attempted to organise a sabotage operation against a similar facility in Lithuania.

Unidentified individuals planned to set fire to an industrial facility housing satellite antennas and Starlink ground station equipment.

The plot was foiled thanks to an advance warning from Lithuanian intelligence services.

Lithuanian Prime Minister Mindaugas Sinkevičius linked the attempted sabotage to possible Russian involvement, describing it as a potential element of the Kremlin's hybrid warfare against European democratic states.

According to the Lithuanian prime minister, the facility supports the operation of nine Starlink antennas used by Ukraine in its defence against Russian armed aggression.

In mid-October, the German magazine Der Spiegel reported that members of the Turkish criminal organisation Daltons were allegedly involved in setting fire to a Starlink ground station in Poland, acting on instructions from Russian intelligence services.

Following the fire, Polish Deputy Prime Minister and Minister of Digital Affairs Krzysztof Gawkowski stated that several indications suggested the incident was consistent with Russia's evolving doctrine of hybrid attacks.

Several days earlier, Bulgarian authorities had reported a fire at a Starlink ground station near Sofia.

> The recurrence of incidents in different countries shows that protecting individual facilities cannot be effective without regional coordination

The head of Bulgaria's State Agency for National Security, Plamen Tonchev, expressed his conviction that the incident had been an act of sabotage.

Attempts to attack Starlink ground infrastructure in Lithuania, Poland and Bulgaria indicate an expansion of the range of facilities that may become targets of Russian hybrid operations.

Whereas the primary focus was previously on cyberattacks, disinformation and interference in the domestic political processes of European states, physical sabotage targeting critical infrastructure is now increasingly being added to this arsenal.

The functional purpose of the targeted facilities is particularly significant. Starlink ground stations support satellite communications, which play an important role in Ukraine's communications infrastructure.

According to Lithuanian officials, the nine antennas that became potential targets of the saboteurs are used to maintain communications essential to Ukraine's efforts to counter Russian aggression.

Consequently, attacks on these facilities may be directed not only against the infrastructure of European countries but also, indirectly, against the technological capabilities underpinning Ukraine's defence.

Preventing the sabotage attempt in Lithuania thanks to advance warning from intelligence services demonstrates the practical importance of timely intelligence sharing and preventive counterintelligence efforts.

At the same time, the recurrence of incidents in different countries shows that protecting individual facilities cannot be effective without regional coordination.

Statements by senior officials in Lithuania, Poland and Bulgaria also indicate awareness of the potential links between individual incidents and a broader campaign of Russian hybrid activities.

Tinder as a tool for intelligence gathering

Russian intelligence services are also using social engineering techniques to obtain confidential information about European defence industry companies.

Norwegian company Nammo, a manufacturer of artillery ammunition, has become the target of intelligence-gathering attempts through dating applications, including Tinder.

Users operating profiles under unusual or exotic names have attempted to establish contact with employees at the company's facility in Raufoss to obtain information about artillery shell production.

Nammo's management has confirmed attempts to gather information and conduct phishing attacks through social media and has announced that security measures are being strengthened.

This approach illustrates the expansion of intelligence-gathering methods, with personal contacts and digital platforms used for everyday communication increasingly replacing traditional methods of infiltration.

Nammo is one of Europe's major manufacturers of large-calibre artillery ammunition.



The number of successful cyberattacks against Norwegian organisations had tripled over the preceding six months

In response to the growing demand for ammunition following the start of Russia's aggression against Ukraine, Norway allocated more than one billion kroner in government support to the company to substantially expand its production capacity.

Over the past 18 to 24 months, the Raufoss facility has recruited approximately 1,000 new employees. Consequently, the plant is important not only to Norway's defence sector but also to broader European efforts to increase ammunition production.

Amid Russia's war against Ukraine, the continuity of its operations is directly linked to European countries' ability to expand their own stockpiles and maintain arms supplies to Kyiv.

Threats to Norway's defence sector are not limited to attempts to obtain information through social media.

The Norwegian National Security Authority (NSM) reported that the number of successful cyberattacks against Norwegian organisations had tripled over the preceding six months.

The agency also warned of a high level of national security threats. Previously, the Norwegian Police Security Service (PST) had linked a series of sabotage incidents in Europe to the activities of Russian intelligence services.

Attempts to obtain confidential information about Nammo should be viewed as part of broader efforts to assess the capabilities and vulnerabilities of Europe's defence industrial complex.

Information about production processes, technologies, output volumes, logistics and the organisation of the company's operations could be of practical value to intelligence agencies.

Exploiting could enable them to assess the company's production potential, identify critical infrastructure components and prepare more targeted operations aimed at

disrupting its activities.

Sabotage attacks against defence industry facilities and Starlink ground infrastructure, together with attempts to conduct intelligence operations against a Norwegian defence manufacturer, illustrate different dimensions of the same problem: Russia seeks to influence the security of European states not only through military and political means but also through covert operations targeting critical infrastructure and the defence industry.

Oleksandr Levchenko, a former Ukrainian diplomat, is a professor at the State University (Kyiv) and a member of the Academy of Geopolitics and Geostrategy (Kyiv).