Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Oleksandr Levchenko

The Russian connection – sabotage against Europe's defence industry

The Russian intelligence-linked organisation Global Citizens Against War 1984 may, according to journalistic investigations, be connected to a series of acts of sabotage targeting defence industry facilities in Europe.

These include a fire at a WB Electronics facility in the Polish city of Skarżysko-Kamienna and an attempted arson attack on a plant operated by the Ukrainian company Skyeton in Slovakia.

The fire at the WB Electronics facility caused preliminary estimated damage of approximately PLN 15 million (€3.7 million).

The plant is an important part of Poland's production of FlyEye unmanned systems and Warmate loitering munitions, which are used by the armed forces of both Poland and Ukraine.

Poland's Internal Security Agency is treating the incident as a possible act of sabotage inspired by a foreign intelligence service.

Several days earlier, Slovak security services foiled an attempt to set fire to a facility operated by the Ukrainian company Skyeton.

As part of the operation, one Ukrainian national and two Latvian nationals were detained.

Responsibility for both incidents was claimed by the previously unknown organisation Global Citizens Against War 1984, which presents itself as an international anti-war movement and claims that companies whose products are supplied to conflict zones are legitimate targets.

Digital indicators of a Russian connection

An investigation by the Slovak outlet Aktuality.sk and The Insider, cited by the Polish publication Niezalezna.pl, identified several digital and other indicators that may point to the Russian origin of, or coordination behind, the organisation's activities.

In particular, elements of a Russian-language interface remained visible on the group's Instagram accounts.

An analysis of the website's source code also revealed the use of the YS Text font, developed and used by the Russian technology company Yandex.

According to the journalists, certain characteristics of the website and its technical structure indicate the use of automated content-generation and artificial intelligence tools.

> Global Citizens Against War 1984 may not be a genuine civic movement, but rather a digital cover structure

The biographies of two individuals presented on the website as members of the organisation's team also raise questions.

One is allegedly a Pole named Robert Lewanowski, while the other is identified as a Serb, Stefan Ilić.

Journalists have found no convincing independent evidence confirming that these individuals exist.

The biographical information also contains inconsistencies. For example, the website states that Lewanowski served for two years in the Polish army between 2007 and 2009, although compulsory military service in Poland was considerably shorter at that time.

According to the investigation, the organisation's website was created using the Wix platform and artificial intelligence tools.

Taken together, these indicators suggest that Global Citizens Against War 1984 may not be a genuine civic movement, but rather a digital cover structure.

Pacifist rhetoric

The nature of the group's public communication is particularly significant. It uses pacifist rhetoric while simultaneously justifying attacks on defence-industry facilities.

This combination can create the appearance of an independent civil-society initiative while concealing the possible foreign origins of the operations.

If a connection to Russian intelligence services is confirmed, this would fit a model already associated with Russian hybrid operations: the use of ostensibly independent structures to conceal activities conducted by state or state-linked actors.

> An information platform could perform several functions simultaneously

In this case, an information platform could perform several functions simultaneously: claiming responsibility for acts of sabotage, promoting an alternative narrative about their origins, and reducing the risk of direct attribution to Russia.

Equally important is the use of artificial intelligence to create digital infrastructure and fabricated identities.

This significantly reduces the cost and time required to establish a plausible cover structure.

Similar tools can be used not only to create websites but also to generate biographies, photographs, texts and other elements needed to simulate the activities of a genuine organisation.

Recruitment of foreign operatives

Another important element of this model is the recruitment of foreign operatives. Rather than directly involving Russian intelligence personnel, sabotage assignments can be given to individuals who are easier to recruit and use as operational proxies.

This creates an additional layer of separation between the organisers of an operation and those directly carrying it out.

> Telegram and anonymous parts of the internet may be used to recruit potential operatives

According to European investigations into Russian sabotage activities, Telegram and anonymous parts of the internet may be used to recruit potential operatives.

Recruiters pay particular attention to people experiencing financial difficulties or other vulnerabilities.

If such operatives are arrested, Russia can deny any involvement while simultaneously promoting the narrative that the attacks were the independent actions of radical groups.

Putting pressure on Europe's defence industry

The geography and nature of these incidents suggest that they should not be regarded as isolated criminal episodes, but potentially as elements of a broader campaign aimed at putting pressure on Europe's defence industry.

The targets include companies involved in producing unmanned systems and munitions that are directly relevant to military support for Ukraine.

In this context, the potential objectives extend beyond physically damaging production facilities.

Russia's strategy may be aimed at creating a systemic sense of insecurity around European defence investment - Leipzig airport

They may also include disrupting supply chains, delaying deliveries, increasing security costs and creating additional risks for companies expanding defence production in Europe.

Particularly significant are public threats directed at Germany and at Covenant's planned missile plant near Leipzig.

If such threats are followed by further acts of sabotage, this could indicate an attempt to exert preventive psychological pressure on European defence companies and investors.

For European states, this means that protecting defence production can no longer be limited to physical security at industrial facilities.

It requires a combination of counter-intelligence measures, cyber protection, scrutiny of digital infrastructure, monitoring of recruitment channels, and rapid coordination among the intelligence and security services of NATO member states and their partners.

The main risk lies not only in physical damage to individual facilities. Russia's strategy may be aimed at creating a systemic sense of insecurity around European defence investment.

If such tactics become more widespread, the consequences could include not only temporary reductions in production but also deterring private capital from participating in projects necessary for the long-term strengthening of Europe's defence capabilities and military support for Ukraine.

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).