PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NO. 112 (2420), 29 JULY 2024 © PISM

BULLETIN

NATO Members On Guard Against Russian Sabotage

Filip Bryjka

Since the beginning of this year, Russia has stepped up offensive hybrid activities against NATO countries. Russian intelligence services are increasingly recruiting proxies to carry out subversion and sabotage attacks. These are directed against civilian and military infrastructure, politicians, journalists, and representatives of the arms industry. Their aim is to intimidate Western societies and decision-makers, thereby weakening their willingness to continue providing military assistance to Ukraine.

At the beginning of July, the alert level at some U.S. military bases in Europe was raised to "CHARLIE", marking an incident or intelligence indicating that attacks on facilities and personnel are likely. The strengthening of security measures this time is linked to increased Russian subversive and sabotage activity. In April, two individuals—German nationals of Russian origin—were detained in Germany and charged with acting on behalf of Russian intelligence by preparing attacks on military facilities, arms factories, industrial facilities, and transport infrastructure used to supply Ukraine. These acts were to take the form of arson and the detonation of explosives, and one of the planned targets was U.S. armed forces installations in Bavaria where Ukrainian soldiers are trained.

Methods of Russian Subversion. The hybrid operations conducted by Russia against NATO states are increasingly aggressive in nature. They are not limited to non-kinetic actions (e.g., disinformation campaigns, graffiti, cyberattacks) but also take the form of sabotage (including arson), acts of violence, vandalism, or provocations at the border using instrumentalised migration.

So far, with Russian encouragement, saboteurs have attacked mainly "soft" civilian targets (e.g., industrial halls, shops, warehouses), including in Lithuania, Latvia, Estonia, the UK, and Poland. In France, a series of arson attacks paralysed the operation of high-speed rail lines on the opening day of the Olympic Games, causing traffic difficulties and undermining the French authorities' ability to ensure security. Information from the Internal Security Agency (ABW) suggests that the Russian military intelligence service GRU is the instigator of subversion in Poland. At the end of July, the Security Service of Ukraine (SBU) detained another group of saboteurs being prepared for operations in Poland and the Baltic States by the Russian Federal Security Service (FSB). Although the attacks so far have not led to the disruption of the functioning of the state or created a major crisis, some of them were carried out in places where various types of plastics and chemicals are stored, which carries the risk of environmental contamination and civilian casualties. One such incident was prevented by the ABW in February this year in Wrocław. Through such subversive actions, Russian intelligence is attempting to create an atmosphere of fear and signal a willingness to impose costs and generate risks on countries supporting Ukraine in order to lower support among Western societies for its policies.

Military infrastructure facilities and those belonging to the arms industry are also important targets for Russian subversion. Attacks on these are intended to limit the pace and scale of Western support for Ukraine. So far, Russia has not succeeded in carrying out a successful sabotage action targeting military infrastructure (along the lines of the blowing up of arms depots in Czechia by GRU officers in 2014), but there have been incidents at arms factories in Latvia, Germany, the UK, and Poland that may have been the result of deliberate sabotage. Military facilities are already subject to intensive reconnaissance by Russian agents. In May 2022, individuals preparing an attack on the Lielvārde military airport were detained in Latvia. In Poland, on the

other hand, in mid-2023, ABW dismantled a spy network of more than a dozen people who were preparing sabotage attacks on railway lines, seaports, and military bases.

To minimise costs and risks, Russian intelligence recruits untrained agents for subversive activities. This allows Russia to deny links to incidents and avoid responsibility. Recruitments are carried out, among others, on social media (e.g., Telegram) and payment is made in the form of cryptocurrencies, making it difficult to detect the principals. The recruitment base consists of migrants from Eastern Europe and Russian-speaking citizens of countries where the sabotage operations are carried out. They are often individuals with criminal histories or financial problems. Their main motivation for cooperating with foreign intelligence is material gain. The *modus operandi* adopted by the Russians is also due to the expulsion of more than 600 diplomats (including intelligence officers) from Europe.

Russian intelligence services also order acts of violence and assassinations to intimidate and influence the professional activities of specific individuals. The planned assassination of Armin Papperger, the director of the German company Rheinmetall, which produces 155mm artillery ammunition supplied to Ukraine, was prevented thanks to U.S. intelligence. Earlier, perpetrators paid by Russian services in Lithuania beat up Russian opposition figure Leonid Volkov and also destroyed the car of Estonian Interior Minister Lauri Laanemets. The foiled attacks on representatives of the arms sector indicate that Russia's intention is to intimidate Western governments and their societies with terrorist methods in order to reduce the scale of aid to Ukraine.

Cyberattacks and Electronic Warfare. Since the beginning of the full-scale invasion of Ukraine, Russian APT hacking groups have been conducting intensive cyberoperations against NATO countries. Among other things, they are targeting state administration networks and military ICT systems. The targets of cyberattacks include rail, maritime, and aviation infrastructure. Between 2022 and 2024, their victims have included Czech, Latvian, Lithuanian, Polish, Romanian, and Estonian railway companies. On 15 July this year, hackers from the group NoName057(16) carried out a series of DDoS (denial of service) attacks targeting the Polish defence industry and aviation infrastructure, in response to Poland's initiative to potentially shoot down Russian missiles on Ukrainian territory by NATO countries. Russian hackers are primarily attempting to undermine the logistical capabilities of the Alliance countries to supply Ukraine with armaments and military equipment.

Russia is increasingly using elements of electronic warfare (EW) against NATO countries. Since the end of 2023, GPS signals on the territory of the Baltic states have been periodically jammed from Kaliningrad Oblast, Saint Petersburg, and Moscow. This has led to the disruption of thousands of civilian and military flights. Between January and April this year, they were experienced by 28% of Royal UK Air Force transport and surveillance flights over Eastern Europe and 16% over North West Europe. Russia conducts similar operations in the Middle East (from bases inside Syria) and the Atlantic Ocean (from naval vessels) jamming GPS signals in the strategic GIUK area between the west coast of Scotland and Ireland and the southwest coast of Iceland. Russia's involvement in creating a threat to the air traffic control of Luxembourg, Sweden, France, and the Netherlands is also indicated in the findings of the International Telecommunications Union. In addition to jamming navigation, interference has consisted of interrupting television programmes and broadcasting propaganda material about the war in Ukraine. Russia is thus generating additional costs on the part of countries that are trying to obstruct its strategic goals.

Conclusions and Outlook. Russia will be stepping up its hybrid actions primarily against the states that have the most influence in supporting Ukraine. By using increasingly offensive methods—which carry the risk of casualties—Russia is testing how far it can go. Failure to respond decisively may encourage Russia to further escalate its aggression. Although NATO stresses that hybrid actions may lead to the triggering of Article 5 (a reference to collective defence), strengthening deterrence requires political preparedness to take proactive action in response to Russian subversion. Therefore, the Alliance should prepare options for a flexible response to Russian acts of sabotage that impose more severe costs on the attacker.

Poland, which serves as a logistical hub through which about 80% of Western aid to Ukraine passes, is particularly vulnerable to Russian subversive attacks. In order to strengthen Alliance countries' resilience to such threats, they can request the advisory and consultative support of NATO Counter-Hybrid Support Teams (CHSTs). However, the responsibility for countering and responding to such threats is primarily a national competence. While it is possible to obtain support from allies in response to a hybrid attack, the misuse of such mechanisms (Article 4, or Article 5 consultations) may undermine their political relevance. Strengthening national resilience, including increasing the budgets of the counter-intelligence and intelligence services, should therefore be a high priority.