PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NO. 183 (2100), 25 NOVEMBER 2022 © PISM

BULLETIN

Preparing for Russian Hybrid Activities Against NATOand EU Countries

Anna Maria Dyner

In pursuit of its goals in Ukraine, Russia will intensify hybrid activities, including information warfare, cyberattacks, or acts of sabotage against the critical infrastructure of NATO and EU countries. These actions are intended to increase fear in the European public about an uncontrolled escalation of the conflict and further deterioration of the economic situation. In this way, Russia seeks to weaken Allied unity, which is necessary to continue the support for Ukraine, implement new strategies of the Alliance and the EU, and react quickly to emerging threats. The importance of building state and societal resilience at the level of individual states and both NATO and the EU is growing.

Russia has been developing its concept of hybrid operations against Western states for years. It involves the use of the entire spectrum of political, economic, and social instruments to, among others, manipulate the public's mood in states Russia considers to be adversaries. The most important areas of the Russian activity include information warfare, cyberattacks, and instrumentalisation of migration.

The Information War. In the case of Russian disinformation activities against EU and NATO members, social media play a special role. The Russian messaging is promoted on social media through individual accounts and groups, some of which have been existing for years, including fake ones that often have spread anti-system slogans. Moreover, specialised companies that employ people to disseminate a specific type of disinformation on the web—so-called troll factories—also have increase their activity. The Russian activities in this area focus on the most socially and politically sensitive issues among a population, and the message is shaped in a way that is intended to influence public sentiment. Currently, these key topics are rising inflation and energy security. In the first case, inflation, the amount of military assistance given by EU and NATO countries to Ukraine is emphasised, as is the increase in defence spending of some members of the Alliance, indicating (falsely) that this is a major factor responsible for the rising prices. In the latter area, energy, the Russian influencers note (again incorrectly) that for years Russia was a guarantor of low energy prices and that since EU countries have withdrawn from the existing cooperation, they are responsible for the increase in prices. Russia is also trying to use the issue of refugees from Ukraine to blame the governments of the countries that have welcomed them of focusing on helping Ukrainians at the expense of their own citizens, including their health and education security.

Russia's goal in these endeavours is to reduce the sense of security of the inhabitants of Western countries regarding, for example, fuel and energy supplies and undermine their trust in the national authorities, the EU, and NATO, as well as to increase social polarisation, for example, in matters related to health protection.

Threats to Critical Infrastructure. Although the war in Ukraine is sapping Russia's resources, it still has considerable potential to carry out sabotage activities and cyberattacks against functioning critical infrastructure (power plants, transmission networks, railways) in NATO and EU countries. It also finances hacking groups in third countries, such as the self-named UNC1151/Ghostwriter or Digital Shadows/Conti. A report by The European Union Agency for Cybersecurity (ENISA) shows that since the outbreak of the current phase of the war in Ukraine, the threat to governments, businesses, and key sectors such as energy, transport, banking, and digital infrastructure has increased. In turn, a Microsoft report states that in February-May 2022, Russia carried out cyberattacks in 42 countries (not including Ukraine), the main targets of which were government agencies (49%) and institutions managing critical infrastructure (19%). The countries most often attacked were Poland (8% of cases) and the Baltic states (a combined 14%).

Despite the intensified actions of Alliance countries to increase the physical protection of critical infrastructure, Russia still has the potential to conduct sabotage activities, as indicated by the explosions on the Nord Stream 1 and 2 pipelines. For this purpose, as in cyberspace, it can use third-country citizens.

Instrumentalisation of Migration. The interests of the EU and NATO are also threatened by Russian activities in Africa, the Middle East, and Latin America, where propaganda about the West's responsibility for local economic problems is spread. For this purpose, apart from social media, Russia uses local traditional media it has developed, including RT television and the Sputnik portal. These activities have intensified since last year and are one of the elements of the instrumentalisation of migration and an attempt to trigger additional migration flows towards Europe. This conclusion is indicated by, among others, Polish Border Guard statistics showing that people trying to cross the Belarusian-Polish border illegally frequently have Russian visas. The Russian authorities also allowed the landing of planes from Turkey, Syria, and Belarus in Kaliningrad Oblast, which indicated the possibility of an attempt to destabilise the border with Poland and Lithuania.

Threat of Intensification of Russian Activities. Despite the war in Ukraine, Russia will try to achieve its political goals towards the EU and NATO at a relatively low cost, mainly through hybrid activities. Particularly vulnerable will be the countries that support Ukraine the most and which are crucial for decision-making within both organisations, as well as those in which presidential or parliamentary elections will be held in the coming months (in 2023, this includes Czechia, Estonia, Finland, and Poland). Russia will focus on conducting and intensifying an information war aimed at decisions related to arming Ukraine. It also will try to undermine NATO cohesion, which is essential for the implementation of the Alliance's new strategy of strengthening collective defence mechanisms.

It is possible Russia will intensify cyberattacks and acts of sabotage and terrorism targeting critical and ICT infrastructure, which will be aimed at paralysing key services in the attacked country. Such activities seek to increase the sense of the threat of war, as well as probing the defence capabilities of EU and NATO countries.

Russia will continue to instrumentalise migration and fuel anti-immigrant and anti-refugee sentiments. The purpose of these activities will be to put pressure on European countries, test the EU's and NATO's external border protection systems, and provoke serious political disputes between the organisations' member states on migration policy.

Conclusions and Recommendations. NATO and EU countries must consider there will be an intensification of hybrid activities aimed at weakening their support for Ukraine. Both organisations should launch extensive information campaigns for the societies of their member states to build resistance to disinformation and shape social competences in verifying information sources. As part of such activities, it will be worth pointing out the mechanisms of the most popular solutions used in the Russian information war, such as creating a chain of seemingly reliable information that may lead to unfavourable social events, such as panic associated with a fabricated threat.

One particularly dangerous hybrid scenario will be Russia triggering another wave of migration to Europe. Hence, the need for the EU, in cooperation with other countries, to take aid measures for countries particularly affected by the food crisis (also within the framework of the UN, which will make it difficult for Russia to take advantage of this organisation). It also will be necessary to increase intelligence and counterintelligence cooperation between EU and NATO countries in order to identify threats related to irregular migration and to extend cooperation between the border services of EU countries to increase the protection of the external border.

It also will be important to develop social and institutional competences in the field of responding to cyberthreats, especially those related to the functioning of critical infrastructure. It is worth considering the introduction and testing of critical infrastructure management models that do not rely on the internet in the event of a serious failure caused by a cyberattack, an act of sabotage, or some other threat to ensure the possibility to maintain access to key services.

In addition, Poland may consider introducing legislative changes to facilitate the fight against hybrid threats. In cases of cyber and physical attacks, Russia's activity is made easier because EU and NATO countries only conduct reactive actions in defence. One element to compensate for this may therefore be to increase the competence of institutions responsible for state security, which in certain situations indicating a very high risk of a hybrid attack, could use preventive measures.