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

NO. 6 (2507), 24 JANUARY 2025 © PISM

BULLETIN

China Increasingly Implicated in Russian Destabilisation Efforts Against the EU

Marcin Przychodniak

Chinese actors are suspected of involvement in Russian destabilisation operations in the EU, including damage to critical infrastructure in the Baltic. Alignment in the objectives of Sino-Russian strategic cooperation makes approval by the Chinese authorities of hybrid actions likely. Such operations aimed to increase the sense of insecurity in the societies of EU states and induce governments to push for peace talks with Russia. China's involvement in such activity should prompt the EU to impose sanctions on Chinese companies involved in destabilisation activities and deepen cooperation between the Member States and their partners in protecting critical infrastructure.

Russian destabilisation operations in EU countries include cyberattacks, information manipulation, and interference (known as FIMI) and sabotage of critical infrastructure. They cause serious financial damage and increase the sense of insecurity in the EU about Russia's full-scale aggression against Ukraine. So far, China has supported Russia primarily politically and diplomatically (e.g., with regard to Russian demands to change the European security architecture) and by helping Russia's war economy. In parallel, China's cooperation with Russia and Belarus in the security sphere has progressed. In July 2016, anti-terrorism units from China and Russia held an exercise in Smolensk, and in July 2017, in the Baltic Sea, navies from both countries trained. In July 2024, Chinese vessels paid a courtesy visit to Saint Petersburg, and held manoeuvres with Russian units in the Gulf of Finland. In the same month, Chinese army units practised with the Belarusian army near Brest. In recent months, the likely involvement of Chinese actors in Russian destabilisation operations in Europe has increased and in Russian military support.

Forms of Chinese Involvement. The first dimension, and the one most visible at the moment, is the suspected deliberate actions of Chinese-linked vessels in damaging critical infrastructure, mainly in the Baltic Sea. In October 2024, the container ship *PolarBear* damaged the Balticonnector pipeline, a source of gas for Finland, and an adjacent fibre-optic cable between Sweden and Estonia. Last November, the ship *Yipeng-3* breached fibre-optic cables between Finland and Germany and Sweden and Lithuania. The status of the vessels were not identical but had similarities, with *PolarBear* being bought by Russian entities from a Chinese ship owner and *Yipeng-3* being owned by a Chinese company based in a military zone in Ningbo, according to Swedish media reports. The Chinese authorities denied that the actions of either *PolarBear* or *Yipeng-3* were deliberate, but have limited cooperation with Swedish and Finnish law enforcement authorities. This has made it difficult to reliably investigate the incidents and raised suspicion about the intentional actions of the vessels. An indication that the Chinese ships were in the Baltic to assist Russia stems from accusations by Taiwan's Ministry of Digital Affairs of similar actions by China against critical installations. In January this year, a Cameroonian-flagged vessel owned by a Chinese entity was implicated in such an incident. The *modus operandi* in the Baltic is reminiscent of an idea by Chinese engineers—published in Google's patent database as having been submitted in 2020 by Lishui University—to use a system of hooks and knives on chains dragged by an anchor along the bottom to cut cables.

The second dimension of Chinese involvement concerns information activities aimed at influencing political decisions in EU countries, including through Chinese companies

operating in the Union. An example of this was the use of misinformation on Tik Tok during the campaign for the presidential elections in Romania last year. According to the Romanian special services, the results were allegedly manipulated, allegedly in favour of Russia's interests (in December, the Romanian Supreme Court annulled the elections). The role of Tik Tok, which is linked to the Chinese authorities, in the success of the Russian operation was based on the platform's popularity, as well as the inadequate response to suspicious activity. Despite indications from the central election office in Romania, the platform did not quickly remove suspicious content, such as posts from fake accounts, and labelled some of them as entertainment, which increased their views and popularity. Last November, Google also pointed to the practice of Chinese marketing and PR companies setting up fake news sites operating in the national languages of dozens of countries, including Austria, Poland, South Korea, and Germany, which replicated Chinese party media reports and messaging.

The third dimension of Chinese participation in operations affecting EU security is possible direct military support to the Russian Federation, besides the supply of dual-use goods conducted to date. This very likely involves the production of Chinese military drones in Xinjiang for Russian forces. The information was unofficially confirmed in media by EU diplomats. Alongside support of Russian troops with satellite imaging provided by Chinese companies, the drone production is further confirmation of China's direct involvement in Russian aggression against Ukraine

EU Response. The EU's response to the Chinese actions has so far been mainly limited to expressions of disapproval, both by the European Commission (EC) and some Member States. Sweden's action on the Baltic incident was legally limited, as the Chinese vessel was in international waters at the time of the damage, and so it ended without resolution. More decisive was the EC's strike against Tik Tok. Under the Digital Services Act, on 5 December 2024 the Commission demanded information from the platform's operator regarding its activities in the context of the Romanian elections, and on 17 December the EC opened proceedings into the risk of interference by the platform in an electoral process. The response to reports of military drone production in Xinjiang was mainly limited to a diplomatic note to China from the EC and 15 Member States, demanding clarification on the matter (which remains unanswered). The Chinese support for Russia's war economy (including through the supply of parts for drones and chips) was also the reason for the imposition of further restrictions under the 15th sanctions package of December 2024, listing one person and six Chinese companies.

Conclusions and Outlook. While the involvement of Chinese actors in Russian destabilisation operations in the EU is limited and mainly at Russia's initiative, it has intensified recently. This may be due to Russia's greater use of Chinese actors, who had been less likely to be perceived as a threat from the perspective of some European states and therefore able to act more effectively than Russian actors.

China's involvement, however, seems to confirm its declarations about intending to shape the security situation in Europe. Chinese rhetoric about the need to cooperate with the EU in the face of the threats posed by the United States under Donald Trump's presidency is calculated to reinforce the demands made in the EU by, for example, Hungary, Slovakia, and Germany, which are favourable to China. These include the resumption of the ratification process of the EU-China investment agreement and/or the easing of EU trade policy towards China. It is aware that in the optics of the EU institutions and the majority of the Member States, Chinese support for Russia in the war with Ukraine is an element blocking the improvement of EU-China relations. At the same time, the Chinese are aware of the difficulties associated with the implementation of Trump's call for an immediate end to the fighting in Ukraine, including the uncertain prospect of the start of Ukrainian-Russian talks. Increasing insecurity in European public opinion, including through support for Russian destabilisation operations, is aimed at intensifying public pressure on governments to support the start of peace talks. A possible ceasefire in the Russian-Ukrainian war would bring China closer to improving relations with the EU, especially in an economic context, which would be important given the expected strong tensions in China-U.S. relations. It would also allow Russia to further engage Western attention and maintain U.S. activity in Europe to the benefit of Chinese interests in the Asia-Pacific region.

The EU is faced with the task of taking into greater account Chinese complicity when countering Russian operations. Currently, Chinese activity in this context is treated as different, less threatening and incidental, unlike the Russian activity. The EU and Member State responses should include Chinese actors when relevant in sanctions imposed in relation to Russian aggression against Ukraine. Visa restrictions on Chinese nationals suspected of possible involvement in destabilisation operations in the EU would be one solution. It is advisable to monitor and cooperate within the Union with regard to the activities of Chinese entities, for example, in the context of restrictions on access to critical infrastructure (including key EU "strategic" companies). Intelligence-sharing and operational cooperation is important, such as in the Baltic Sea, including the monitoring Chinese vessels and actions by the NATO *Baltic Sentry* mission.

Editors: Jarosław Ćwiek-Karpowicz, Rafał Tarnogórski,
Jędrzej Czerep, Wojciech Lorenz, Justyna Szczudlik, Daniel Szeligowski, Jolanta Szymańska, Marcin Terlikowski, Damian Wnukowski, Szymon Zaręba, Tomasz Żornaczuk