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

No. 82 (2714), 19 NOVEMBER 2026 © PISM

BULLETIN

From attribution to costs: EU sanctions against Russia's hybrid activities

Elżbieta Kaca

On 16 November, the EU extended its sanctions against Russia, addressing the growing scale of threats directed at Member States that fall below the threshold of open armed conflict. Sanctions may increase the costs of conducting such operations and strengthen the deterrent effect. However, their effectiveness remains limited by problems such as attributing responsibility for actions and their limited impact on third-party actors.

Evolution. Russia employs a wide range of hybrid activities against EU countries, including cyber-attacks, disinformation, influence operations, interference in democratic processes, and sabotage, which also targets critical infrastructure. The intensification of such activities after 2014, and particularly following the full-scale aggression against Ukraine in 2022, prompted the EU to develop new response instruments, including sanctions packages. These primarily involve the freezing of assets and, in the case of individuals, a ban on entry into the EU.

The first such instrument was the sanctions regime concerning cyber-attacks, established in 2019. It allows restrictions to be imposed on individuals and entities responsible for cyber-attacks or attempted cyber-attacks targeting critical infrastructure, public institutions or electoral processes. A prerequisite for application is proof of the perpetrators' link to a specific operation. To date, 27 individuals and 7 entities linked to Russian cyberattacks have been subject to these sanctions (see table).

A turning point came in 2024 with the adoption of a separate sanctions regime targeting Russian destabilising activities. This covers activities including cyberattacks, sabotage, interference in democratic processes, foreign information manipulation and interference (FIMI), and the instrumentalisation of migration. In addition to asset freezes and EU travel bans, restrictions may also be imposed on transactions involving ships, aircraft, property, ports, digital infrastructure, or foreign cryptocurrency service providers used in destabilising activities. The EU may also ban the operation of media organisations involved in influence operations. To date, restrictions have been imposed on 111 individuals and 21 entities (see table). At the same time, the EU is imposing sanctions on individuals and organisations involved in Russian disinformation campaigns linked to the war against Ukraine.

The application of sanctions in practice. Between 2020 and 2026, the EU has gradually expanded the list of individuals and entities subject to the cyber-attacks sanctions regime. These included senior officers and leadership figures within Russian military intelligence involved in an attempted breach of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands, the NotPetya attack (a series of cyberattacks in 2017 causing significant economic losses globally), the cyberattack on the Bundestag, and attacks on Estonian state institutions. In subsequent years, the restrictions were also extended to members of hacker groups such as Callisto, Armageddon, Wizard Spider, Z-Pentest and NoName057(16), responsible for cyberattacks on the health, financial, defence and water supply sectors in the EU. Sanctions were also imposed on web hosting companies and malware developers supporting Russian cyber operations.

The sanctions imposed from 2024 onwards in response to Russian destabilising activities had a much broader scope. They have targeted participants in the 'Doppelgänger' disinformation campaign, individuals linked to acts of

vandalism and intimidation in Estonia, campaigns designed to stir up social tensions in France, and collaboration with the German far right to advance Russian political goals. Post-2024 measures also covered individuals responsible for funding specific political groups and candidates for the European Parliament, while restrictions were also imposed for a wide range of intelligence activities, including espionage against the German Federal Intelligence Service, the recruitment of saboteurs, including an arson attack on the Museum of the Occupation in Riga using Molotov cocktails, the jamming of GPS signals over the Baltic Sea, and the use of fishing vessels to conduct reconnaissance of critical infrastructure and military installations in the Baltic and North Seas. In 2026, sanctions were further extended to cover propagandists and information-operation participants, including television presenters, journalists, bloggers, influencers and artists disseminating pro-Russian narratives.

The significance of sanctions. The restrictions serve primarily as a way to politically attribute responsibility for hybrid activities. The joint identification of perpetrators by EU Member States strengthens threat assessments and sends an important political signal, while also raising public awareness of the scale of Russia's destabilising activities.

Sanctions may also increase the costs of Russian operations, particularly for entities that maintain economic ties with the EU. Asset freezes, restrictions on access to financial services and trade barriers limit their ability to operate. For example, the large Russian fishing companies Norebo JSC and Murman Sea Food have lost access to the important European market after becoming subject to sanctions, whilst Norebo JSC has also lost the right to fish in Norway's exclusive economic zone. Sanctions imposed by the G7+ countries, including the EU, on the major Russian hosting company Media Land LLC and its subsidiary ML.Cloud have restricted their access to Western clients and infrastructure. However, they have not been completely prevented from operating, as they have been able to use foreign intermediaries.

The restrictions can be particularly severe for EU citizens involved in Russian information operations. They make it difficult for them to find gainful employment, which is why some have challenged the sanctions decisions, citing issues including breaches of their freedom of expression. Examples include the businessman and former military officer Xavier Moreau (whose appeal was dismissed on procedural grounds) and the German bloggers Thomas Röper and Alina Lipp (whose cases are still pending). Röper argued that the sanctions had led to the loss of payment channels, business partnerships and part of his income from book sales and donations. The case law of the General Court to date has not called into question the legality of imposing sanctions on participants in information operations, focusing instead on the quality of evidence and the proportionality of the measures. Such restrictions have been deemed compatible with freedom of expression, as they do not prohibit media activities outright, but instead restrict their funding.

Key limitations. The primary challenges lie in the relatively low cost of conducting influence operations, cyber-attacks, and disinformation campaigns, alongside their decentralised nature. Dismantling a single network or channel of operation often triggers the rapid emergence of new structures. Russia also relies on foreign intermediaries who have no assets or significant economic interests in the EU, making them largely immune to the impact of restrictions.

An additional challenge is the development of new technologies. Artificial intelligence, crypto-assets, and new communication platforms facilitate both the financing of influence operations and the dissemination of disinformation. The effectiveness of these restrictions is also undermined by uneven monitoring and enforcement of sanctions regulations by Member States, as well as by the ease with which restrictions can be circumvented online, including through alternative domains, VPNs and IPTV platforms.

Identifying perpetrators and gathering sufficient evidence also remain significant challenges. Attributing responsibility for cyber-attacks, influence operations, or acts of sabotage often takes years and requires establishing a link between a specific operation and the individuals or entities responsible for it. This process is hampered by the limited intelligence-sharing of classified information between Member States and insufficient resources devoted to monitoring the financial aspects of hybrid activities, including cryptocurrency flows. Consequently, sanctions are usually imposed after a considerable delay, reducing their deterrent effect.

Conclusions. The EU's sanctions policy has evolved from responding to individual cyber-attacks to addressing the broader spectrum of Russian hybrid activities. Although sanctions are not capable of halting destabilising operations on their own, they play an important role in attributing responsibility, raising awareness of threats, and increasing some of the costs borne by Russia.

In future, curbing the sources of funding for influence operations by imposing sanctions on entire financial networks—including the cryptocurrency sector—may become increasingly important. The effectiveness of sanctions could also be enhanced by applying them more broadly to the supporting technological infrastructure behind hybrid operations—targeting hosting companies, domain operators, advertising networks, and digital service providers. It will also be important to identify perpetrators more swiftly, freeze the assets of key intermediaries in third countries, combine sanctions with criminal proceedings, and cooperate more closely with the US, the UK and the other G7 countries. Viewed in this light, sanctions become part of an effective strategy to counter hybrid threats.

Analysis prepared in collaboration with Weronika Moroz.

Table. Individuals and entities subject to EU sanctions for Russian cyberattacks and destabilising activities between 2020 and 2026

Sanctions regime for Russian destabilising activities			
Date	**Individuals**	**Entities**	**Characteristics of the package**
16 December 2024	1. Artem Sergeyevich Kuryev 2. Nikolai Alexandrovich Tupikin 3. Sofya Avramovna Zakharova 4. Andrei Vladimirovich Averjanov 5. Tinatin Givievna Kandelaki 6. Vladimir Vladimirovich Sergienko 7. Denis Alexandrovich Smolaninov 8. Volodymyr Lipchenko 9. Yuri Sizov 10. Visa Nokhaevich Mizayev 11. Olga Alekseyevna Belavtseva 12. Timofey Vyacheslavovich Bordachev 13. Harouna Douamba 14. Antolii Prizenko 15. Alesya Miloradovich 16. Oleg Sergeyevich Eremenko	1. GRU Unit No. 29155 FKU "Military Unit 29155" (Moscow) 2. Pan-African Group for Trade and Investment GPCI (Lomé) 3. African Initiative (Moscow)	Units and officers of the Russian special services and armed forces; individuals and entities involved in influence operations and disinformation in the EU and Africa
20 May 2025	17. Alik Yuryevich Khuchbarov (nationality: Russian, Estonian) 18. Ilia Sergeyevich Bocharov 19. Yelena Kolbasnikova 20. Hüseyin Dogru 21. Yulia Sergeyevna Prokhova 22. Rostislav Tiesluk 23. Alina Lipp (nationality: German) 24. Viktor Vladimirovich Medvedchuk 25. Artem Pavlovich Marchewski 26. Natalia Sudlenkova 27. Iurie Neculti 28. Ivan Neculti 29. Andrei Kharkovsky 30. Antolij Yurevich Abramov 31. Ruslan Vasilyevich Nesterenko 32. Viktor Aleksandrovich	4. AFA Media (Istanbul) 5. Voice of Europe (Prague) 6. Norebo JSC (Murmansk) 7. Murman Sea Food (Murmansk) 8. Main Radio Frequency Centre (Moscow) 9. Stark Industries Solutions Ltd. (London)	Propagandists, bloggers, media companies, fishing companies used for reconnaissance activities, entities conducting influence operations in Europe and Africa, and individuals associated with the Voice of Europe channel and disinformation campaigns

	Lukovenko 33. Oleg Antolevich Voloshin 34. Justine Blaise Tagouh (nationality: Russian, Estonian) 35. Mikhail Mikhailovich Prudnikov 36. Sylvian Afoua (nationality: French, Togolese) 37. Thomas Röper (nationality: German)		
26 June 2025	38. Nathalie Yamb (nationality: Swiss, Cameroonian)		A social media influencer. Since 2019, she has openly supported Russia, echoed its narratives and attacked France and the West to undermine their influence in Africa. She also has close ties to AFRIC, an organisation linked to Russian private military companies
15 July 2025	39. Andrei Yuryevich Romanchenko 40. Vladimir Naidenov 41. Dimitri Buimistru 42. Ceaceslav Valico 43. Simeon Boykov 44. Vitaly Kulikov 45. Yuri Illarionovich Lastochkin 46. Yevgeny Shevchenko 47. Alexei Nikolayevich Shavrov	10. Federal State Enterprise 'Russian Radio and Television Network' (RTRS) (Moscow) 11. Separate Radio-Electronic Warfare Centre of the Baltic Fleet (Kaliningrad Oblast) 12. BRICS Journalists' Association 13. Centre for Geopolitical Expertise (Moscow) 14. Foundation to Battle Injustice 15. Tiger Web	Individuals and entities responsible for disinformation, information manipulation and the jamming of GNSS navigation signals in Europe
15 December 2025	48. John Mark Dougan (nationality: American, Russian) 49. Andrei Andreyevich Sushencov 50. Dmitry Vyacheslavovich Suslov 51. Fyodor Alexandrovich Lukyanov 52. Ivan Nikolayevich Timofeyev 53. Andrei Georgievich Bystritsky 54. Vladislav Yevgenyevich Borovkov 55. Denis Igorevich Denisienko 56. Dmitri Yuryevich Goloshubov	16. 142nd Independent Radio-Electronic Warfare Battalion (Kumachevo) 17. International Movement of Russophiles	Persons and entities responsible for hybrid activities, including disinformation campaigns, pro-Russian propaganda and cyber-attacks targeting EU Member States, NATO and Ukraine

	57. Jacques Baud (nationality: Swiss) 58. Xavier Moreau (nationality: French) 59. Diana Vitalievna Panchenko		
29 January 2026	60. Dmitry Viktorovich Guberniev 61. Ekaterina Sergeyevna Andreyeva 62. Mariya Eduardovna Sittel 63. Pavel Alexandrovich Zarubin 64. Roman Vasilyevich Chumakov 65. Sergei Vladimirovich Polunin		Propagandists, including Russian television presenters and artists.
16 March 2026	66. Sergei Alexandrovich Klyuchenkov 67. Ernest Gedrvich Mackevicius (nationality: Lithuanian, Russian) 68. Graham Williams Phillips (nationality: British) 69. Adrie Coquet (nationality: French, Russian)		Propagandists.
21 April 2026		18. Euromore (Brussels) 19. Foundation for the Support and Protection of the Rights of Compatriots Living Abroad (Pravfond) (Moscow)	Entities responsible for destabilisation, including a media platform disseminating Kremlin propaganda.
15 June 2026	70. Mariya Vladimirovna Dudko 71. Alexandra Jost 72. Roman Yuryevich Antonovsky 73. Pavel Alekseevich Astakhov 74. Olga Adolfovna Kiriy 75. Igor Valentinovich Malcev 76. Mariya Yuryevna Volkonskaya 77. Anatoly Alexandrovich Kuzichev 78. Georgy Alexandrovich Shevkunov 79. Kirill Fedorov (Latvian national)	20. Presidential Foundation for Cultural Initiatives/PFKI (Moscow)	Propagandists.
13 July 2026	80. Ivan Sergeyevich Kasyanenko		Deputy Commander of the Special Operations Service (SSD), he co-organised the activities of a unit linked to Afghanistan, including the payment of bounties to encourage attacks on US and

			international coalition personnel operating in Afghanistan. He also co-ordinated operations relating to the poisoning of Sergei Skripal and his daughter and managed the Wagner Group's networks in Africa, as well as joint military-technical projects with Iran.
24 September 2026	81. Xenia Fedorova		A Russian public figure associated with the media and a former member of the management team at Russia Today (RT) in France. In her role as chairperson and director of news at RT France, she was involved in implementing and promoting the station's editorial line, including pro-Russian narratives.
16 November 2026	82. Andrei Naumovich Perla 83. Alexei Vitalyevich Ulyanov 84. Viktor Nikolayevich Ostreshko 85. Anastasia Olegovna Kazakova 86. Vladimir Igorevich Golovashen 87. Aleksandr Pavlovich Kochetov 88. Sergei Vyacheslavovich Tatti 89. Yelena Grigoryeva 90. Olga Alexandrovna Polosina 91. Viktoria Igorevna Gordieva 92. Andrei Petrovich Manzolevsky 93. Mikhail Alexandrovich Barayev 94. Alexei Vladimirovich Medvedev 95. Yan Gennadievich Nalimov 96. Yevgeniya Viracheva 97. Gulnara Vilsurovna Androsova 98. Igor Vladimirovich Bogatyrev 99. Vladimir Viktorovich Kremlev 100. Sergei Nikolayevich Korsun 101. Armen Genrikhovich Asryan 102. Ilya Vladimirovich Lipkind	21. Social Design Agency LLC, SDA (Social Design Agency LLC), also known as Agentstvo Sotsialnogo Proektirovania (ASP)	SDA is a Moscow-based company specialising in public relations and political technology, which carries out large-scale projects involving the manipulation and interference in information, funded, directed and supervised by the Russian presidential administration. SDA staff, journalists, bloggers

	103. Vladimir Alexandrovich Troshin 104. Alexei Andreyevich Klimovsky 105. Alina Maratovna Gabdullina 106. Chay Bowes (nationality: Irish) 107. Alexei Stepanov 108. Vitaly Borisovich Yeliseyev 109. Yuri Ivanovich Podolaka 110. Daniil Viktorovich Bezsonov 111. Pyotr Valentinovich Marchenko		
EU sanctions regime for cyberattacks			
Date	**Individuals**	**Entities**	**Characteristics of the package**
30 July 2020	1. Alexey Valeryevich Minin 2. Aleksei Sergeyevich Morenets 3. Evgenii Mikhaylovich Serebriakov 4. Oleg Mikhaylovich Sotnikov	1. The Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)	Russian cyberattacks targeted international organisations, energy infrastructure, and businesses and public institutions. These included attempts to hack into the OPCW's network, the NotPetya attack, which caused massive economic losses, and operations disrupting the functioning of the Ukrainian power grid
22 October 2020	7. Dmitry Sergeyevich Badin 8. Igor Olegovich Kostyukov	2. Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU GRU)	Russian cyber-attacks targeted the IT systems of state institutions, including the German parliament, leading to the theft of confidential data and the hijacking of politicians' email accounts, including that of Chancellor Angela Merkel
24 June 2024	9. Ruslan Aleksandrovich Peretyatko 10. Andrey Stanislavovich Korinets 11. Oleksandr Sklianko 12. Mykola Chernykh 13. Mikhail Mikhailovich Tsarev 14. Maksim Sergeevich Galochkin		Russian cyberattacks targeted critical infrastructure, government IT systems and institutions responsible for defence, security and foreign relations in EU Member States and Ukraine. They included phishing, ransomware and malware designed to steal sensitive data and disrupt services, including in the health and banking sectors

27 January 2025	15. Nikolay Alexandrovich Korchagin 16. Vitaly Shevchenko 17. Yuriy Fedorovich Denisov		Russian cyberattacks targeted government institutions in EU countries, including Estonian ministries, and led to the theft of confidential documents, health data and other sensitive information
13 July 2026	20. Vitaly Nikolayevich Kovale 21. Alexander Alexandrovich Volosovik 22. Denis Olegovich Degtyarenko 23. Yuliya Vladimirovna Pankratova 24. Maksim Evgenevich Voronin 25. Maksim Aleksandrovich Gordienko 26. Evgeniy Viktorovich Baashev 27. Roman Alexandrovich Puntus	3. Media Land LLC (St. Petersburg) 4. ML. Cloud (Riga) 5. Implus LLC (Russian Federation) 6. Z-Pentest (Russian Federation)	Russian cyber-attacks primarily targeted critical infrastructure (particularly the energy and water supply sectors) as well as government institutions, financial institutions and the media in EU Member States, Ukraine and other countries supporting Ukraine. The attacks included ransomware, phishing, DDoS and data theft
16 November 2026		7. NoName057(16)	NoName057(16) is a pro-Russian hacking group which has carried out attacks on services essential to the maintenance of basic social and economic activities and critical state functions in Member States, including government portals, military intelligence services, political parties and candidates during electoral processes, the energy and industrial sectors, transport infrastructure, water supply systems, banks, financial institutions and online payment services, and national postal services

Source: PISM analysis based on European Commission regulations, 2026.