Cyber-attacks: three individuals added to EU sanctions list for malicious cyber activities against Estonia

Archived: 2026-04-05 12:49:43 UTC

- Council of the EU
- Press release
- 27 January 2025 17:04

The Council today adopted additional restrictive measures against three Russian individuals responsible for a series of cyberattacks carried out against the Republic of Estonia in 2020. **The individuals listed are officers of the General Staff of the Armed Forces of the Russian Federation (GRU) Unit 29155.**

The cyber-attacks granted attackers unauthorized access to non-public information and sensitive data stored within several government ministries. These included the Ministries of Economic Affairs and Communications, and Social Affairs, **leading to the theft of thousands of confidential documents**. These documents included business secrets, health records, and other critical information compromising the security of the affected institutions. Although the Ministry of Foreign Affairs was also targeted, no sensitive or non-public data was accessed. Unit 29155 is also responsible for conducting cyber-attacks against other EU member states and partners, notably Ukraine.

The covert unit, known for its involvement in foreign assassinations and destabilisation activities such as bombings and cyber-attacks across Europe, and some of its military personnel active in Ukraine, Western Europe and Africa, was also sanctioned last year under the new sanction regime in view of Russia’s destabilising activities.

With today’s listings, the EU horizontal cyber sanctions regime now applies to **17 individuals and 4 entities**. It includes an **asset freeze** and a **travel ban**, and the prohibition for EU persons and entities to make funds available to those listed.

This decision confirms the willingness of the EU and its member states to provide a strong and sustained response to persistent malicious cyber activities targeting the EU, its member states and partners.

The EU and its member states will continue to cooperate with our international partners to promote an open, free, stable and secure cyberspace.

The relevant legal acts have been published in the Official Journal of the European Union.

Background

In June 2017, the EU established a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (the "Cyber Diplomacy Toolbox"). The framework allows the EU and its member states to use all CFSP measures,

including restrictive measures if necessary, to prevent, discourage, deter and respond to malicious cyber activities targeting the integrity and security of the EU and its member states.

The EU framework for restrictive measures against cyber-attacks threatening the EU and its member states was set up in May 2019.

On May 21st, 2024, the Council approved conclusions on the future of cybersecurity aiming to provide guidance and setting the principles towards building a more cyber secure and more resilient EU.On June 24, 2024, the European Union added six individuals to its sanctions list due to their involvement in malicious cyber activities, specifically cyberattacks targeting EU member states and Ukraine. These individuals were linked to harmful actions that threatened the security and stability of the region. The sanctions include asset freezes and travel bans.

In parallel, on October 8th, 2024, the Council established a new framework for restrictive measures in response to Russia's destabilising actions abroad. This framework allows the EU to target individuals and entities engaged in actions and policies, including cyber-attacks, by the government of the Russian Federation, which undermine the fundamental values of the EU and its member states, their security, independence and integrity, as well as those of international organisations and third countries.

In its most recent conclusions of 19 December 2024, the European Council strongly condemned Russia's hybrid campaign, including sabotage, disruption of critical infrastructure, cyber-attacks, information manipulation and interference, and attempts to undermine democracy, including in the electoral process, against the European Union and its member states.

- Council Decision (CFSP) 2025/171 of 27 January 2025 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (including the details of the individuals sanctioned today)
- Council Implementing Regulation (EU) 2025/173 of 27 January 2025 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (including the details of the individuals sanctioned today)
- European Council Conclusions (19 December 2024)
- Cybersecurity: Council approves conclusions for a more cyber secure and resilient Union (press release, 21 May 2024)
- Cybersecurity: How the EU tackles Cyber Threads (background information)
- Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (consolidated text dated 24 June 2024)

Visit the meeting page

Last review: 7 April 2025
