

Cyber attacks: EU ready to respond with a range of measures, including sanctions

The Council agreed to develop a framework for a **joint EU diplomatic response** to malicious cyber activities, the **cyber diplomacy toolbox**.

The EU recognises that cyberspace offers significant opportunities, but also poses continuously evolving challenges for EU external action. The EU is concerned by the increased ability and willingness of state and non-state actors to pursue their objectives through malicious cyber activities. Such activities may constitute **wrongful acts under international law** and could give rise to a joint EU response. The EU reiterates that states should not knowingly allow their territory to be used for internationally wrongful acts using Information and Communication Technologies (ICT).

The framework for a joint EU diplomatic response is part of the **EU's approach to cyber diplomacy**, which contributes to conflict prevention, the mitigation of cybersecurity threats and greater stability in international relations. The framework is expected to encourage cooperation, facilitate mitigation of immediate and long-term threats, and influence the behaviour of potential aggressors in the long term.

The EU diplomatic response to malicious cyber activities will make full use of **measures within the Common Foreign and Security Policy**, including, if necessary, restrictive measures. A joint EU response to malicious cyber activities would be **proportionate** to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity.

The EU reaffirms its **commitment to the settlement of international disputes in cyberspace by peaceful means**. In this context, all of the EU's diplomatic efforts should as a priority aim to promote security and stability in cyberspace through increased international cooperation, and at reducing the risk of misperception, escalation and conflict that may stem from ICT incidents.

[Read the full text of the Council conclusions](#)
[Council conclusions on cyber diplomacy of 11 February 2015](#)