EU imposes the first ever sanctions against cyber-attacks

The Council today decided to impose **restrictive measures** against **six individuals** and **three entities** responsible for or involved in various **cyber-attacks**. These include the attempted cyber-attack against the **OPCW** (Organisation for the Prohibition of Chemical Weapons) and those publicly known as **‘WannaCry’**, **‘NotPetya’**, and **‘Operation Cloud Hopper’**.

The sanctions imposed include a **travel ban** and an **asset freeze**. In addition, EU persons and entities are forbidden from making funds available to those listed.

Sanctions are one of the options available in the EU’s cyber diplomacy toolbox to prevent, deter and respond to malicious cyber activities directed against the EU or its member states, and today is the **first time the EU has used** this tool. The legal framework for targeted restrictive measures against cyber-attacks was adopted in May 2019 and recently renewed.

Background

In recent years, the EU has scaled up its resilience and its ability to prevent, discourage, deter and respond to cyber threats and malicious cyber activities in order to safeguard European security and interests.

In June 2017, the EU stepped up its response by establishing 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.

Targeted restrictive measures have a deterrent and dissuasive effect and should be distinguished from attribution of responsibility to a third state.

The EU remains committed to a global, open, stable, peaceful and secure cyberspace and therefore reiterates the need to strengthen international cooperation in order to promote the **rules-based order** in this area.