Client Alert | International Trade

New EU sanctions to target malicious external cyber-attacks

May 2019

Authors: James Killick, Genevra Forwood, Jacquelyn MacLennan, Sara Nordin, Fabienne Vermeeren, Charlotte Van Haute

On 17 May 2019, the EU put in place a new legal framework for sanctions targeting malicious cyber activities from outside the EU that threaten the Union or its Member States.[1] The aim is to enhance the EU's cyber resilience and address cyber-attacks that undermine the *"EU's integrity, security and economic competitiveness, including increasing acts of cyber-enabled theft of intellectual property"*.[2]

This is the first time that EU sanctions have targeted those responsible for actual or attempted cyber-attacks. Similar to the recent EU sanctions targeting chemical weapons,[3] these sanctions are country neutral, and do not mention any specific third country. It is reported that these sanctions were advocated by the UK and the Netherlands after an investigation uncovered cyber-attacks reportedly originating from the GRU, the Russia military intelligence service, targeting the Organisation for the Prohibition of Chemical Weapons in The Hague.

These new sanctions target actual and attempted cyber-attacks having a (potentially) "significant effect", in light of the scope and scale of disruption, the number of persons affected, the number Member States concerned, the extent of economic loss or economic gain to the perpetrator, the extent of any data breaches and the loss of commercially sensitive data.[4] In addition, such cyber-attacks must represent an "external threat" to the Union and its Members, meaning they must have originated outside the EU, used infrastructure outside the Union, or the persons instrumental to the cyber-attack's operations are established abroad.[5] Importantly, these sanctions also cover malicious cyber activities towards third States and international organizations.[6]

The new EU sanctions would impose an "asset freeze" on (i) natural or legal persons, entities or bodies who are responsible for cyber-attacks or attempted cyber-attacks; (ii) natural persons or legal persons, entities or bodies that provide financial, technical or material support for or are otherwise involved in cyber-attacks or attempted cyber-attacks; (iii) natural or legal persons, entities or bodies associated with the natural or legal persons, entities or bodies described above.[7] So far, no-one has yet been listed, and the Council would require unanimity to designate individuals and entities.

---

1 See Council Decision 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, and Council Regulation 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

2 For the Declaration by the High Representative on behalf of the EU on respect for the rules-based order in cyberspace, 12 April 2019, see here.

3 See Client Alerts: *EU lays ground for sanctions against use and proliferation of chemical weapons*, available here, and *EU sanction Syrian and Russian parties involved in the use and proliferation of chemical weapons,* available here.

4 See Article 2 of Council Regulation 2019/796 and Article 3 of Council Decision 2019/797.

5 See Article 1 of Council Regulation 2019/796 and Council Decision 2019/797.

6 Ibid.

7 See Article 3 of Council Regulation 2019/796.

As a result of the asset freeze, all funds and economic resources belonging to, or controlled by, the listed persons and that fall under EU jurisdiction (e.g., held by EU banks) will be frozen. Furthermore, no funds or economic resources may be made available – directly or indirectly – to or for the benefit of the listed persons by parties falling under EU jurisdiction.

The asset freeze sanctions apply to the EU territory (including its airspace), to nationals of EU Member States (including those located outside the EU), and on board vessels and aircraft under Member State jurisdiction. Sanctions also apply to companies incorporated or registered under the law of an EU Member State and to other non-EU companies in respect of business done in whole or in part in the EU. This means that non-EU companies may also be affected by the measures once specific parties are listed, depending on the particular circumstances in which business activities are performed in the EU.

In addition, EU Member States will impose a travel ban on the persons listed under these sanctions.[8] In order to maximise the impact of these EU sanctions, the EU will also encourage third States to adopt similar restrictive measures.[9]

White & Case LLP
Wetstraat 62 rue de la Loi
1040 Brussels
Belgium

T +32 2 239 26 20

8 See Article 4 Council Decision 2019/797.

9 See Article 9 Council Decision 2019/797.