New Sanctioning Regime against External Cyber-Attacks

Thomas Wahl

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Thomas Wahl
Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

ISSN: 1862-6947
https://eucrim.eu

The Council has established a framework that allows the EU to impose restrictive sanctions against external cyber-attacks threatening the Union or its Member States. The framework consists of:

- Council Regulation (EU) 2019, 796 (which is based on Art. 215 TFEU);
- Council Decision (CFSP) 2019, 797 (which is based on Art. 29 TEU).

The acts were published in the Official Journal L 129 I, 17.5.2019, 1. They entered into force on 18 May 2019.

The framework comes in response to recent malicious cyberattacks that originated or were carried out outside the EU and affected the EU Member States' critical infrastructure, competitiveness, and/or state functions. It is a measure within the EU's Common Foreign and Security Policy (CFSP) and part of the "cyber diplomacy toolbox."

The framework applies to cyber-attacks with a "significant effect," including attempted cyber-attacks with a potentially significant effect. Cyber-attacks that constitute an external threat to the Union or its Member States include those which:

- Originate, or are carried out, from outside the Union;
- Use infrastructure outside the Union;
- Are carried out by any natural or legal person, entity, or body established or operating outside the Union;
- Are carried out with the support, at the direction of, or under the control of any natural or legal person, entity, or body operating outside the Union.

The Regulation allows the Council to list natural or legal persons, entities or bodies who/which are responsible for such cyber-attacks, who/which provide financial, technical or material support, or who/which are associated with the responsible or supporting persons. Targeted sanctions against these listed persons include:

- Entry ban into or transit ban through the EU;
- Freezing of all funds and economic resources;
- Prohibition of EU citizens and entities from making funds available to those persons listed.

According to the recitals of the Decision, the new sanctioning regime may also be applied in case of cyber-attacks with a significant effect against third countries or international organisations if this is necessary to achieve CFSP objectives.

It is also clarified, that the targeted restrictive measures must be differentiated from the attribution of responsibility for cyber-attacks to a third State. The application of targeted restrictive measures does not amount to such attribution, which is a sovereign political decision taken on a case-by-case basis. Every Member State is free to make its own determination with respect to the attribution of cyber-attacks to a third State.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).


Co-funded by
the European Union