Council Implementing Regulation (EU) 2020/1536 of 22 October 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

[X1COUNCIL IMPLEMENTING REGULATION (EU) 2020/1536

of 22 October 2020

implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States]

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States[(1)], and in particular Article 13(1) thereof,

Having regard to the proposal from the High Representative of the Union for Foreign Affairs and Security Policy,

Whereas:

(1) On 17 May 2019 the Council adopted Regulation (EU) 2019/796.

(2) Targeted restrictive measures against cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States are among the measures included in the Union's framework for a joint diplomatic response to malicious cyber activities (the cyber diplomacy toolbox) and are a vital instrument to deter and respond to such activities.

(3) In order to prevent, discourage, deter and respond to continuing and increasing malicious behaviour in cyberspace, two natural persons and one body should be included in the list of natural and legal persons, entities and bodies subject to restrictive measures set out in Annex I to Regulation (EU) 2019/796. Those persons and that body are responsible for or were involved in cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States, in particular the cyber-attack against the German federal parliament (Deutscher Bundestag) which took place in April and May 2015.

(4) Annex I to Regulation (EU) 2019/796 should therefore be amended accordingly,

HAS ADOPTED THIS REGULATION:

Editorial Information

X1 Substituted by Corrigendum to Council Implementing Regulation (EU) 2020/1536 of 22 October 2020 of implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks

Changes to legislation: *There are currently no known outstanding effects for the Council Implementing Regulation (EU) 2020/1536. (See end of Document for details)*

threatening the Union or its Member States (Official Journal of the European Union L 351 I of 22 October 2020).

Article 1

Annex I to Regulation (EU) 2019/796 is amended in accordance with the Annex to this Regulation.

Article 2

This Regulation shall enter into force on the date of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

***Changes to legislation:** There are currently no known outstanding effects for the Council Implementing Regulation (EU) 2020/1536. (See end of Document for details)*

ANNEX

The following entries are added to the list of natural and legal persons, entities and bodies set out in Annex I to Regulation (EU) 2019/796:

A. Natural persons

	Name	**Identifying information**	**Reasons**	**Date of listing**
‘7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Date of birth: 15 November 1990 Place of birth: Kursk, Russian SFSR (now Russian Federation) Nationality: Russian Gender: male	Dmitry Badin took part in a cyber-attack with a significant effect against the German federal parliament (Deutscher Bundestag). As a military intelligence officer of the 85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Dmitry Badin was part of a team of Russian military intelligence officers which conducted a cyber-attack against the German federal parliament (Deutscher Bundestag) in April and May 2015. This	22.10.2020

			cyber-attack targeted the parliament's information system and affected its operation for several days. A significant amount of data was stolen and the email accounts of several MPs as well as of Chancellor Angela Merkel were affected.	
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Date of birth: 21 February 1961 Nationality: Russian Gender: male	Igor Kostyukov is the current Head of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), where he previously served as First Deputy Head. One of the units under his command is the 85th Main Centre for Special Services (GTsSS), also known as "military unit 26165" (industry nicknames: "APT28", "Fancy Bear", "Sofacy Group", "Pawn Storm" and "Strontium").	22.10.2020'

			In this capacity, Igor Kostyukov is responsible for cyber-attacks carried out by the GTsSS, including those with a significant effect constituting an external threat to the Union or its Member States. In particular, military intelligence officers of the GTsSS took part in the cyber-attack against the German federal parliament (Deutscher Bundestag) which took place in April and May 2015 and the attempted cyber-attack aimed at hacking into the Wi-Fi network of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands in April 2018. The cyber-attack against the German federal parliament targeted the