

Il presente testo è un semplice strumento di documentazione e non produce alcun effetto giuridico. Le istituzioni dell'Unione non assumono alcuna responsabilità per i suoi contenuti. Le versioni facenti fede degli atti pertinenti, compresi i loro preamboli, sono quelle pubblicate nella Gazzetta ufficiale dell'Unione europea e disponibili in EUR-Lex. Tali testi ufficiali sono direttamente accessibili attraverso i link inseriti nel presente documento

► **B**                    ► **C1** **REGOLAMENTO DI ESECUZIONE (UE) 2020/1536 DEL CONSIGLIO**  
del 22 ottobre 2020

che attua il regolamento (UE) 2019/796 concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri ◀

(GU L 351I del 22.10.2020, pag. 1)

Rettificato da:

► **C1**    Rettifica, GU L 406 del 3.12.2020, pag. 67 (2020/1536)

▼B

▼C1

**REGOLAMENTO DI ESECUZIONE (UE) 2020/1536 DEL  
CONSIGLIO**

**del 22 ottobre 2020**

**che attua il regolamento (UE) 2019/796 concernente misure  
restrittive contro gli attacchi informatici che minacciano l'Unione  
o i suoi Stati membri**

▼B

*Articolo 1*

L'allegato I del regolamento (UE) 2019/796 è modificato conformemente all'allegato del presente regolamento.

*Articolo 2*

Il presente regolamento entra in vigore il giorno della pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

## ALLEGATO

Le seguenti voci sono aggiunte all'elenco delle persone fisiche e giuridiche, delle entità e degli organismi riportato nell'allegato I del regolamento (UE) 2019/796:

## A. Persone fisiche

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
«7.	Dmitry Sergeevich BADIN	<p>Дмитрий Сергеевич БАДИН</p> <p>Data di nascita: 15 novembre 1990</p> <p>Luogo di nascita: Kursk, RSFS russa (ora Federazione russa)</p> <p>Cittadinanza: russa</p> <p>Sesso: maschile</p>	<p>Dmitry Badin ha partecipato a un attacco informatico con effetti significativi ai danni del parlamento federale tedesco (Deutscher Bundestag).</p> <p>In qualità di agente dell'intelligence militare dell'85° Centro principale per i servizi speciali (GTsSS), direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), Dmitry Badin faceva parte di una squadra di agenti dell'intelligence militare russa che ha condotto un attacco informatico ai danni del parlamento federale tedesco (Deutscher Bundestag) tra aprile e maggio 2015. Tale attacco ha colpito il sistema informatico del parlamento, compromettendone il funzionamento per diversi giorni. È stato sottratto un ingente volume di dati e sono stati violati gli account di posta elettronica di diversi parlamentari, nonché quello della Cancelliera Angela Merkel.</p>	22.10.2020
8.	Igor Olegovich KOSTYUKOV	<p>Игорь Олегович КОСТЮКОВ</p> <p>Data di nascita: 21 febbraio 1961</p> <p>Cittadinanza: russa</p> <p>Sesso: maschile</p>	<p>Igor Kostyukov è l'attuale capo della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), presso cui ha precedentemente svolto le funzioni di primo vice capo. Tra le unità sotto il suo comando vi è l'85° Centro principale per i servizi speciali (GTsSS), noto anche come unità militare 26165 (alias: APT28, Fancy Bear, Sofacy Group, Pawn Storm, Strontium).</p> <p>In tale veste, Igor Kostyukov è responsabile degli attacchi informatici condotti dall'85° Centro principale per i servizi speciali (GTsSS), tra cui quelli con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.</p> <p>In particolare, agenti dell'intelligence militare dell'85° Centro principale per i servizi speciali (GTsSS) hanno partecipato all'attacco informatico ai danni del parlamento federale tedesco (Deutscher Bundestag) tra aprile e maggio 2015, nonché al tentativo di attacco informatico finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi nell'aprile 2018.</p> <p>L'attacco informatico ai danni del parlamento federale tedesco ha colpito il sistema informatico del parlamento, compromettendone il funzionamento per diversi giorni. È stato sottratto un ingente volume di dati e sono stati violati gli account di posta elettronica di diversi parlamentari, nonché quello della Cancelliera Angela Merkel.</p>	22.10.2020»

▼B

## B. Persone giuridiche, entità e organismi

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
«4.	85° Centro principale per i servizi speciali (GTsSS), direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU)	Indirizzo: Komsomol'skiy Prospekt, 20, Mosca, 119146, Federazione russa	<p>L'85° Centro principale per i servizi speciali (GTsSS), direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), noto anche come unità militare 26165 (alias: APT28, Fancy Bear, Sofacy Group, Pawn Storm, Strontium), è responsabile di attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.</p> <p>In particolare, agenti dell'intelligence militare dell'85° Centro principale per i servizi speciali (GTsSS) hanno partecipato all'attacco informatico ai danni del parlamento federale tedesco (Deutscher Bundestag) tra aprile e maggio 2015, nonché al tentativo di attacco informatico finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi nell'aprile 2018.</p> <p>L'attacco informatico ai danni del parlamento federale tedesco ha colpito il sistema informatico del parlamento, compromettendone il funzionamento per diversi giorni. È stato sottratto un ingente volume di dati e sono stati violati gli account di posta elettronica di diversi parlamentari, nonché quello della Cancelliera Angela Merkel.</p>	22.10.2020»