2025/173

27.1.2025

REGOLAMENTO DI ESECUZIONE (UE) 2025/173 DEL CONSIGLIO

del 27 gennaio 2025

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

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2019/796 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri [1], in particolare l'articolo 13, paragrafo 1,

vista la proposta dell'alta rappresentante dell'Unione per gli affari esteri e la politica di sicurezza,

considerando quanto segue:

(1) Il 17 maggio 2019 il Consiglio ha adottato il regolamento (UE) 2019/796.

(2) Le misure restrittive mirate contro gli attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri sono una delle misure previste nel quadro dell'Unione relativo a una risposta diplomatica comune alle attività informatiche dolose, ossia il pacchetto di strumenti della diplomazia informatica, e sono uno strumento fondamentale per prevenire, scoraggiare e contrastare tali attività.

(3) Le attività informatiche dolose contro le infrastrutture critiche o i servizi essenziali, anche attraverso l'uso di ransomware e wiper, il targeting delle catene di approvvigionamento e il ciberspionaggio, comprese le attività di furto di proprietà intellettuale, sono in aumento in termini di numero, frequenza e sofisticatezza. Con i loro effetti dirompenti e distruttivi, queste attività rappresentano una minaccia sistemica per la sicurezza, l'economia e la democrazia dell'Unione e la società in generale.

(4) Nel 2020 sono stati perpetrati attacchi informatici con effetti significativi contro l'Estonia. Sono stati condotti attacchi informatici contro i sistemi computerizzati di diverse istituzioni, allo scopo di utilizzare i dati per minacciare la sicurezza dell'Estonia. Tali attacchi informatici hanno interessato la conservazione di informazioni classificate.

(5) Nel quadro dell'azione dell'Unione duratura, mirata e coordinata contro gli autori di minacce informatiche persistenti, tre persone fisiche dovrebbero essere inserite nell'elenco delle persone fisiche e giuridiche, delle entità e degli organismi oggetto di misure restrittive di cui all'allegato I del regolamento (UE) 2019/796. Tali persone sono responsabili di attacchi informatici o vi sono coinvolte con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.

(6) È pertanto opportuno modificare di conseguenza l'allegato I del regolamento (UE) 2019/796,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

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.

Fatto a Bruxelles, il 27 gennaio 2025

Per il Consiglio

La presidente

K. KALLAS

[1] GU L 129 I del 17.5.2019, pag. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

ALLEGATO

Nell'allegato I del regolamento (UE) 2019/796, le voci seguenti sono aggiunte alla sezione «A. Persone fisiche»:

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
«15.	Nikolay Alexandrovich KORCHAGIN	Николай Александрович Корчагин Data di nascita: 16.9.1997 Cittadinanza: russa Sesso: maschile Entità associata: direzione principale dello Stato maggiore delle forze armate della Federazione russa	Nikolay Korchagin è coinvolto in attacchi informatici con effetti significativi e ne è responsabile in quanto ha svolto attività di intelligence dirette contro l'Estonia ottenendo accesso illegalmente a un sistema informatico. Nikolay Korchagin è un ufficiale dell'unità militare 29155 della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GRU). In tale ruolo è coinvolto in attacchi informatici contro sistemi computerizzati, intesi a raccogliere, dai sistemi di dati di diverse istituzioni, informazioni che in modo indipendente o combinato forniscono una panoramica della politica di sicurezza informatica dell'Estonia, delle capacità informatiche dello Stato, dei dati personali sensibili e di altri dati sensibili, al fine di utilizzare i dati per minacciare la sicurezza dell'Estonia. Gli attacchi interessano pertanto la conservazione di informazioni classificate, ed è responsabile di tali attacchi. Gli attacchi hanno riguardato alleati e partner dell'Estonia. Nikolay Korchagin è pertanto coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per uno Stato membro, e ne è responsabile.	27.1.2025
16.	Vitaly SHEVCHENKO	Виталий Шевченко Data di nascita: 1.9.1997 Cittadinanza: russa Sesso: maschile Entità associata: direzione principale dello Stato maggiore delle forze armate della Federazione russa	Vitaly Shevchenko è coinvolto in attacchi informatici con effetti significativi e ne è responsabile in quanto ha svolto attività di intelligence dirette contro l'Estonia ottenendo accesso illegalmente a un sistema informatico. Vitaly Shevchenko è un ufficiale dell'unità militare 29155 della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GRU). In tale ruolo è coinvolto in attacchi informatici contro sistemi computerizzati, intesi a raccogliere, dai sistemi di dati di diverse istituzioni, informazioni che in modo indipendente o combinato forniscono una panoramica della politica di sicurezza informatica dell'Estonia, delle capacità informatiche dello Stato, dei dati personali sensibili e di altri dati sensibili, al fine di utilizzare i dati per minacciare la sicurezza dell'Estonia. Gli attacchi interessano pertanto la conservazione di informazioni classificate, ed è responsabile di tali attacchi. Gli attacchi hanno riguardato alleati e partner dell'Estonia. Vitaly Shevchenko è pertanto coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per uno Stato membro, e ne è responsabile.	27.1.2025

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
17.	Yuriy Fedorovich DENISOV	Юрий Федорович Денисов Data di nascita: 17.6.1980 Cittadinanza: russa Sesso: maschile Entità associata: direzione principale dello Stato maggiore delle forze armate della Federazione russa	Yuriy Denisov è coinvolto in attacchi informatici con effetti significativi e ne è responsabile in quanto ha svolto attività di intelligence dirette contro l'Estonia ottenendo accesso illegalmente a un sistema informatico. Yuriy Denisov è un ufficiale dell'unità militare 29155 della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GRU). In tale ruolo è coinvolto in attacchi informatici contro sistemi computerizzati, intesi a raccogliere, dai sistemi di dati di diverse istituzioni, informazioni che in modo indipendente o combinato forniscono una panoramica della politica di sicurezza informatica dell'Estonia, delle capacità informatiche dello Stato, dei dati personali sensibili e di altri dati sensibili, al fine di utilizzare i dati per minacciare la sicurezza dell'Estonia. Gli attacchi interessano pertanto la conservazione di informazioni classificate, ed è responsabile di tali attacchi. Gli attacchi hanno riguardato alleati e partner dell'Estonia. Yuriy Denisov è pertanto coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per uno Stato membro, e ne è responsabile.	27.1.2025».