2025/173

27.1.2025

REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2025/173 AL CONSILIULUI

din 27 ianuarie 2025

privind punerea în aplicare a Regulamentului (UE) 2019/796 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2019/796 al Consiliului din 17 mai 2019 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre ([1]), în special articolul 13 alineatul (1),

având în vedere propunerea Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate,

întrucât:

(1) La 17 mai 2019, Consiliul a adoptat Regulamentul (UE) 2019/796.

(2) Măsurile restrictive specifice împotriva atacurilor cibernetice având efecte importante care reprezintă o amenințare externă la adresa Uniunii sau a statelor sale membre sunt una dintre măsurile incluse în cadrul Uniunii privind un răspuns diplomatic comun la activitățile cibernetice răuvoitoare, mai exact Setul de instrumente pentru diplomația cibernetică, precum și un instrument vital pentru a preveni, a împiedica și a descuraja atacurile cibernetice și a răspunde la acestea.

(3) Activitățile cibernetice răuvoitoare împotriva infrastructurii critice sau a serviciilor esențiale, inclusiv prin utilizarea atacurilor de tip ransomware și a celor care vizează ștergerea datelor (wiper), atacarea lanțurilor de aprovizionare și spionajul cibernetic, inclusiv activitățile de furt de proprietate intelectuală, sunt în creștere ca număr, frecvență și complexitate. Având în vedere efectele lor perturbatoare și distructive, activitățile respective reprezintă o amenințare sistemică la adresa securității, a economiei și a democrației Uniunii și a societății în general.

(4) În 2020, au fost desfășurate atacuri cibernetice cu efecte semnificative împotriva Estoniei. Au fost comise atacuri cibernetice care au avut drept țintă sisteme informatice ale mai multor instituții, cu scopul de a utiliza datele pentru a amenința securitatea Estoniei. Atacurile cibernetice respective au vizat stocarea informațiilor clasificate.

(5) Ca parte a acțiunii susținute, adaptate și coordonate a Uniunii împotriva entităților care reprezintă amenințări cibernetice persistente, trei persoane fizice ar trebui să fie incluse pe lista persoanelor fizice și juridice, a entităților și a organismelor cărora li se aplică măsurile restrictive prevăzută în anexa I la Regulamentul (UE) 2019/796. Persoanele respective sunt răspunzătoare pentru atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre sau sunt implicate în astfel de atacuri.

(6) Prin urmare, anexa I la Regulamentul (UE) 2019/796 ar trebui să fie modificată în consecință,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Anexa I la Regulamentul (UE) 2019/796 se modifică în conformitate cu anexa la prezentul regulament.

Articolul 2

Prezentul regulament intră în vigoare la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 27 ianuarie 2025.

Pentru Consiliu

Președinta

K. KALLAS

([1]) JO L 129 I, 17.5.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

ANEXĂ

În anexa I la Regulamentul (UE) 2019/796 se adaugă următoarele rubrici la secțiunea „A. Persoane fizice”:

	Nume	Informații de identificare	Motive	Data includerii pe listă
„15.	Nikolay Alexandrovich KORCHAGIN	Николай Александрович Корчагин Data nașterii: 16.9.1997 Cetățenia: rusă Sexul: masculin Entitate asociată: Direcția principală a Statului-Major al Forțelor Armate ale Federației Ruse	Nikolay Korchagin este implicat în atacuri cibernetice cu efecte semnificative și este răspunzător pentru acestea prin desfășurarea de activități de informații împotriva Estoniei și prin obținerea ilegală de acces la un sistem informatic. Nikolay Korchagin este ofițer al unității militare 29155 din cadrul Direcției principale a Statului-Major al Forțelor Armate ale Federației Ruse (GRU). În funcția respectivă, el este implicat în atacuri cibernetice împotriva sistemelor informatice și este răspunzător pentru acestea, atacurile având ca scop colectarea din sistemele de date ale mai multor instituții, date care, în mod independent sau în combinație, oferă o imagine de ansamblu a politicii de securitate cibernetică a Estoniei, a capacităților cibernetice ale statului, a datelor sensibile cu caracter personal și a altor date sensibile, cu scopul de a utiliza datele pentru a amenința securitatea Estoniei. Prin urmare, atacurile vizează stocarea informațiilor clasificate. Atacurile au vizat aliați și parteneri ai Estoniei. Prin urmare, Nikolay Korchagin este implicat în atacuri cibernetice cu efecte semnificative care constituie o amenințare externă la adresa unui stat membru și este răspunzător pentru acestea.	27.1.2025
16.	Vitaly SHEVCHENKO	Виталий Шевченко Data nașterii: 1.9.1997 Cetățenia: rusă Sexul: masculin Entitate asociată: Direcția principală a Statului-Major al Forțelor Armate ale Federației Ruse	Vitaly Shevchenko este implicat în atacuri cibernetice cu efecte semnificative și este răspunzător pentru acestea prin desfășurarea de activități de informații împotriva Estoniei și prin obținerea ilegală de acces la un sistem informatic. Vitaly Shevchenko este ofițer al unității militare 29155 din cadrul Direcției principale a Statului-Major al Forțelor Armate ale Federației Ruse (GRU). În funcția respectivă, el este implicat în atacuri cibernetice împotriva sistemelor informatice și este răspunzător pentru acestea, atacurile având ca scop colectarea de date din sistemele de date ale mai multor instituții, care, individual sau împreună, oferă o imagine de ansamblu a politicii de securitate cibernetică a Estoniei, a capacităților cibernetice ale statului, a datelor sensibile cu caracter personal și a altor date sensibile, cu scopul de a utiliza datele pentru a amenința securitatea Estoniei. Prin urmare, atacurile vizează stocarea informațiilor clasificate. Atacurile au vizat aliați și parteneri ai Estoniei. Prin urmare, Vitaly Shevchenko este implicat în atacuri cibernetice cu efecte semnificative care constituie o amenințare externă la adresa unui stat membru și este răspunzător pentru acestea.	27.1.2025

	Nume	Informații de identificare	Motive	Data includerii pe listă
17.	Yuriy Fedorovich DENISOV	Юрий Федорович Денисов Data nașterii: 17.6.1980 Cetățenia: rusă Sexul: masculin Entitate asociată: Direcția principală a Statului-Major al Forțelor Armate ale Federației Ruse	Yuriy Denisov este implicat în atacuri cibernetice cu efecte semnificative și este răspunzător pentru acestea prin desfășurarea de activități de informații împotriva Estoniei și prin obținerea ilegală de acces la un sistem informatic. Yuriy Denisov este ofițer al unității militare 29155 din cadrul Direcției principale a Statului-Major al Forțelor Armate ale Federației Ruse (GRU). În funcția respectivă, el este implicat în atacuri cibernetice împotriva sistemelor informatice și este răspunzător pentru acestea, atacurile având ca scop colectarea de date din sistemele de date ale mai multor instituții, date care, în mod independent sau în combinație, oferă o imagine de ansamblu a politicii de securitate cibernetică a Estoniei, a capacităților cibernetice ale statului, a datelor sensibile cu caracter personal și a altor date sensibile, cu scopul de a utiliza datele pentru a amenința securitatea Estoniei și care, astfel, vizează stocarea informațiilor clasificate. Atacurile au vizat aliați și parteneri ai Estoniei. Prin urmare, Yuriy Denisov este implicat în atacuri cibernetice cu efecte semnificative care constituie o amenințare externă la adresa unui stat membru și este răspunzător pentru acestea.	27.1.2025”