Consiliul
Uniunii Europene

Bruxelles, 7 iulie 2026
(OR. en)

8645/26

LIMITE

CORLX 390
CFSP/PESC 586
RELEX 561
CYBER 194
JAI 507
FIN 594

ACTE LEGISLATIVE ȘI ALTE INSTRUMENTE

Subiect:	REGULAMENT DE PUNERE ÎN APLICARE AL CONSILIULUI 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

REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2026/… AL CONSILIULUI

din …

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,

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

întrucât:

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

(2) Ca parte a acțiunii susținute, adaptate și coordonate a Uniunii împotriva actorilor care generează amenințări cibernetice persistente, opt persoane fizice și patru entități ar trebui să fie adăugate pe lista persoanelor fizice și juridice, a entităților și a organismelor cărora li se aplică măsuri restrictive prevăzută în anexa I la Regulamentul (UE) 2019/796. Persoanele și entitățile 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.

(3) 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 …, …

Pentru Consiliu
Președintele

ANEXĂ

Anexa I la Regulamentul (UE) 2019/796 se modifică după cum urmează:

1. În secțiunea „A. Persoane fizice” se adaugă următoarele rubrici:

	Nume	Informații de identificare	Motive	Data includerii pe listă
„20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ Alias: «Bentley», «Bergen», «Alex Konor», «Benny», «Ben», «Stern» Data nașterii: 23.6.1988 Adresa: Serebristy Bulvar 34 (Serebristyy Bul’var); krp 1; flt 528; 197341; St Petersburg, Russian Federation Cetățenia: rusă Sexul: masculin Entități asociate: TrickBot, Wizard Spider, Conti	Vitaly Kovalev este o figură importantă în programele malware «Trickbot» și «Conti». Este cunoscut și sub pseudonimele online «Bentley», «Bergen», «Alex Konor», «Benny», «Ben» și «Stern». Conti și Trickbot au fost create și dezvoltate inițial de Wizard Spider. Wizard Spider a desfășurat campanii de tip ransomware într-o varietate de sectoare, inclusiv servicii esențiale cum ar fi sănătatea și serviciile bancare, a infectat calculatoare din întreaga lume, iar programele sale malware au fost dezvoltate într-un ansamblu de programe malware foarte modular. Campaniile desfășurate de Wizard Spider, prin utilizarea de programe malware cum ar fi Conti și TrickBot, sunt responsabile pentru daune economice substanțiale în Uniunea Europeană. Prin urmare, Vitaly Kovalev este răspunzător pentru atacuri cibernetice cu un efect semnificativ, care constituie o amenințare externă la adresa Uniunii și a statelor sale membre, și este implicat în astfel de atacuri.	+

+ JO: a se introduce data publicării prezentului regulament.

	Nume	Informații de identificare	Motive	Data includerii pe listă
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Data nașterii: 30.1.1983 Locul nașterii: URSS Cetățenia: rusă Numărul pașaportului: 762988138 Sexul: masculin Entități asociate: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Alexander Volosovik este proprietarul Media Land LLC. Încă din 2016, furnizorul de servicii de găzduire «bulletproof» Media Land LLC facilitează o gamă largă de atacuri malware atât împotriva Uniunii, cât și la nivel mondial, oferind servicii de găzduire care ascund identitățile utilizatorilor și rezistă la acțiunile de dezactivare de către autoritățile de aplicare a legii. Media Land LLC a facilitat operațiuni de tip ransomware de mare amploare, servicii de comandă și control și operațiuni de phishing, care au vizat infrastructura critică și serviciile esențiale din statele membre ale Uniunii, ducând la pierderi financiare semnificative. Operațiunile facilitate de Media Land LLC includ, printre altele, LockBit, EvilCorp și BlackBasta. Prin urmare, Media Land LLC este implicată în atacuri cibernetice cu efecte semnificative, care constituie o amenințare externă la adresa Uniunii și a statelor sale membre. În calitate de proprietar al Media Land LLC, Alexander Volosovik este răspunzător pentru aceste atacuri cibernetice și este implicat în acestea. De asemenea, este asociat cu Media Land LLC.	+

+ JO: a se introduce data publicării prezentului regulament.

	Nume	Informații de identificare	Motive	Data includerii pe listă
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО Alias: «Dena» Data nașterii: 9.10.1989 Locul nașterii: URSS Cetățenia: rusă Sexul: masculin Adresa: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Denis Degtyarenko, alias Dena, este un hacker rus al CARR (Cyber Army of Russia Reborn - Armata cibernetică a Rusiei renăscute). CARR a fost răspunzătoare pentru atacuri cibernetice împotriva serviciilor necesare pentru menținerea activităților economice esențiale și a funcțiilor de stat critice în statele membre, precum și împotriva infrastructurii din Ucraina și din alte țări terțe. CARR este legată de Centrul principal pentru tehnologii speciale (GTsST) din cadrul Direcției principale a Statului-Major al Forțelor Armate ale Federației Ruse (GRU). GTsST rămâne activ în desfășurarea de atacuri cibernetice împotriva Uniunii sau a statelor sale membre. CARR vizează, printre altele, agenții guvernamentale, instituții financiare, canale mass-media și infrastructura critică din statele membre și din Statele Unite. CARR a desfășurat atacuri distribuite de blocare a accesului (*distributed denial-of-service* – DDoS) în Ucraina și împotriva unor guverne și întreprinderi situate în țări care au sprijinit Ucraina. Prin urmare, Denis Degtyarenko, unul dintre principalii hackeri ai CARR, este implicat în atacuri cibernetice cu un efect semnificativ, inclusiv în tentative de atacuri cibernetice cu un efect potențial semnificativ, care constituie o amenințare externă la adresa statelor membre, precum și împotriva unor state terțe. De asemenea, în calitate de membru al CARR, Denis Degtyarenko este asociat cu GTsST.	+

+ JO: a se introduce data publicării prezentului regulament.

	Nume	Informații de identificare	Motive	Data includerii pe listă
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА Alias: «YUliYA» Data nașterii: 6.4.1984 Locul nașterii: URSS Cetățenia: rusă Sexul: feminin Adresa: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Yuliya Pankratova este un hacker rus care a lucrat pentru CARR (Cyber Army of Russia Reborn - Armata cibernetică a Rusiei renăscute) și a fondat Z-Pentest și continuă să lucreze pentru aceasta. CARR a fost răspunzătoare pentru atacuri cibernetice împotriva serviciilor necesare pentru menținerea activităților economice esențiale și a funcțiilor de stat critice în statele membre, precum și împotriva infrastructurii din Ucraina și din alte țări terțe. CARR este legată de Centrul principal pentru tehnologii speciale (GTsST) din cadrul Direcției principale a Statului-Major al Forțelor Armate ale Federației Ruse (GRU). GTsST rămâne activ în desfășurarea de atacuri cibernetice împotriva Uniunii sau a statelor sale membre. CARR vizează, printre altele, agenții guvernamentale, instituții financiare, canale mass-media și infrastructura critică din statele membre ale UE și din Statele Unite. CARR a desfășurat atacuri distribuite de blocare a accesului (*distributed denial-of-service* – DDoS) în Ucraina și împotriva unor guverne și întreprinderi situate în țări care au sprijinit Ucraina.	+

+ JO: a se introduce data publicării prezentului regulament.

	Nume	Informații de identificare	Motive	Data includerii pe listă
			Z-Pentest este răspunzătoare pentru atacuri cibernetice cu un efect semnificativ, printre altele, împotriva serviciilor necesare pentru menținerea activităților esențiale în statele membre. Prin urmare, Yuliya Pankratova, unul dintre principalii hackeri ai CARR și ai Z-Pentest, este implicată în atacuri cibernetice cu un efect semnificativ, inclusiv în tentative de atacuri cibernetice cu un efect potențial semnificativ, care constituie o amenințare externă la adresa statelor membre, precum și împotriva unor state terțe. De asemenea, Yuliya Pankratova este asociată cu Z-Pentest.	

	Nume	Informații de identificare	Motive	Data includerii pe listă
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН Alias: «Daugn0» Cetățenia: presupus rusă Sexul: masculin	Maksim Voronin, alias Daugn0, este implicat în dezvoltarea, distribuirea și vânzarea programului malware de furt de informații LummaC2 (alias Lumma Infostealer, Lumma Stealer). LummaC2 este o platformă Malware-as-a-Service (MaaS) utilizată pentru furtul de date sensibile, credențiale pentru browsere, portofele cripto sau informații despre sistem, cu scopul de a instala programe malware suplimentare pe dispozitivele infectate, pentru furtul de criptomonede și pentru campanii de spionaj. Atacurile cibernetice care implică malware LummaC2 sunt utilizate, de asemenea, de actori motivați financiar care generează amenințări cibernetice, cum ar fi Storm-113, Storm-1607, Storm-1674, Octo Tempest și alții. Programul malware LummaC2 a fost utilizat pentru atacuri cibernetice împotriva unor funcții și servicii critice ale statului, necesare pentru menținerea activităților sociale și economice esențiale ale statelor membre. În 2024 și 2025, LummaC2 a fost unul dintre cele mai utilizate instrumente pentru furtul de informații la nivel mondial. Prin urmare, Maksim Voronin, în calitate de dezvoltator, distribuitor și comerciant al LummaC2, este implicat în atacuri cibernetice cu un efect semnificativ, care constituie o amenințare externă la adresa statelor membre, și facilitează aceste atacuri.	+

+ JO: a se introduce data publicării prezentului regulament.

	Nume	Informații de identificare	Motive	Data includerii pe listă
25.	Maksim Aleksandrovich GORDIENKO Alias Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО Alias: «Lummaseller» Cetățenia: presupus rusă Sexul: masculin	Maksim Gordienko, alias Lummaseller, este implicat în dezvoltarea și distribuirea programului malware de furt de informații LummaC2 (alias Lumma Infostealer, Lumma Stealer). LummaC2 este o platformă Malware-as-a-Service (MaaS) utilizată pentru furtul de date sensibile, credențiale pentru browsere, portofele cripto sau informații despre sistem, cu scopul de a instala programe malware suplimentare pe dispozitivele infectate, pentru furtul de criptomonede și pentru campanii de spionaj. Atacurile cibernetice care implică malware LummaC2 sunt utilizate, de asemenea, de actori motivați financiar care generează amenințări cibernetice, cum ar fi Storm-113, Storm-1607, Storm-1674, Octo Tempest și alții. Programul malware LummaC2 a fost utilizat pentru atacuri cibernetice împotriva unor funcții și servicii critice ale statului, necesare pentru menținerea activităților sociale și economice esențiale ale statelor membre. În 2024 și 2025, LummaC2 a fost unul dintre cele mai utilizate instrumente pentru furtul de informații la nivel mondial. Prin urmare, Maksim Gordienko, în calitate de dezvoltator, distribuitor și comerciant al LummaC2, este implicat în atacuri cibernetice cu un efect semnificativ, care constituie o amenințare externă la adresa statelor membre, și facilitează aceste atacuri.	[+]

[+] JO: a se introduce data publicării prezentului regulament.

	Nume	Informații de identificare	Motive	Data includerii pe listă
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Data nașterii: 25.1.1980 Locul nașterii: URSS Cetățenia: rusă Sexul: masculin Persoane fizice asociate: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Entități asociate: Unitatea GRU 29155, «Impuls» LLC	Evgeniy Bashev este membru al Agenției ruse de informații militare GRU, unitatea 29155. În cadrul acestei unități, sprijină și facilitează atacuri cibernetice cu un efect semnificativ împotriva statelor membre, printre altele prin controlarea serverului «Aegon», utilizat pentru operațiuni de piraterie informatică. În special, furnizează sprijin tehnic și material pentru atacurile cibernetice ale unității GRU 29155 prin intermediul societății sale «Impuls LLC», care a facilitat acoperirea operațională, infrastructura și plățile și a gestionat activele tehnice, inclusiv serverele, utilizate pentru atacurile cibernetice. De asemenea, Evgeniy Bashev a coordonat cooperarea dintre structurile GRU și rețelele externe de hackeri. Atacurile cibernetice pe care le-a facilitat au vizat sisteme și servicii cu funcții de stat critice, necesare pentru menținerea activităților sociale și/sau economice esențiale în statele membre, în special în sectorul transporturilor. Prin intermediul campaniei WhisperGate, unitatea GRU 29155 a vizat, de asemenea, infrastructura critică a Ucrainei.	+

+ JO: a se introduce data publicării prezentului regulament.

	Nume	Informații de identificare	Motive	Data includerii pe listă
			Prin urmare, Evgeniy Bashev furnizează sprijin tehnic și material pentru (sau este implicat în alt mod în) atacuri cibernetice cu un efect semnificativ, inclusiv tentative de atacuri cibernetice cu un efect potențial semnificativ, care constituie o amenințare externă pentru statele membre, precum și atacuri cibernetice cu un efect semnificativ împotriva unei țări terțe. În calitate de proprietar și director general, este asociat cu societatea «Impuls» LLC. În calitate de membru al Unității GRU 29155, este asociat și cu respectiva entitate.	

	Nume	Informații de identificare	Motive	Data includerii pe listă
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Locul nașterii: Federația Rusă Cetățenia: rusă Sexul: masculin Persoane fizice asociate: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Entități asociate: Unitatea GRU 29155	Roman Puntus este membru al Agenției ruse de informații militare GRU, unitatea 29155. În cadrul acestei unități, deține un rol de lider în organizarea și coordonarea atacurilor cibernetice cu un efect semnificativ împotriva statelor membre. De asemenea, sprijină dezvoltarea capacității cibernetice interne a unității, inclusiv recrutarea și supravegherea personalului, cum ar fi hackerii și programatorii. Prin înființarea societății-paravan «Aegeon-Impulse», a facilitat aspectele logistice și financiare ale operațiunilor cibernetice. Sub coordonarea sa, unitatea a desfășurat atacuri cibernetice care au vizat sisteme și servicii cu funcții de stat critice, necesare pentru menținerea activităților sociale sau economice esențiale în statele membre, în special în sectorul transporturilor. Prin intermediul campaniei WhisperGate, unitatea GRU 29155 a vizat, de asemenea, infrastructura critică a Ucrainei.	[+]”.

[+] JO: a se introduce data publicării prezentului regulament.

	Nume	Informații de identificare	Motive	Data includerii pe listă
			Prin urmare, Roman Puntus este răspunzător pentru (sau este implicat în alt mod în) atacuri cibernetice cu un efect semnificativ, inclusiv tentative de atacuri cibernetice cu un efect potențial semnificativ, care constituie o amenințare externă pentru statele membre, precum și atacuri cibernetice cu un efect semnificativ împotriva unei țări terțe. În calitate de membru al Unității GRU 29155, este asociat și cu respectiva entitate.	

2. În secțiunea „B. Persoane juridice, entități și organisme” se adaugă următoarele rubrici:

	Nume	Informații de identificare	Motive	Data includerii pe listă
„8.	Media Land LLC (Media Land S.R.L.)	Adresa: Tsvetnochnaya st., 16 Litera P, Room 27, Moskovskaya Zastava Municipal District St Petersburg, 196006, Russian Federation Tipul de entitate: societate cu răspundere limitată Locul înregistrării: Sankt Petersburg Data înregistrării: 19.10.2015 Numărul de înregistrare: 1152536009900 Locul principal de desfășurare a activității: Sankt Petersburg, Federația Rusă Entitate asociată: ML.Cloud	Încă din 2016, furnizorul de servicii de găzduire «bulletproof» Media Land LLC facilitează o gamă largă de atacuri malware atât împotriva statelor membre, cât și la nivel mondial, oferind servicii de găzduire care ascund identitățile utilizatorilor și rezistă la acțiunile de dezactivare de către autoritățile de aplicare a legii, ceea ce generează pierderi financiare semnificative. Media Land LLC a facilitat operațiuni de tip ransomware de mare amploare, servicii de comandă și control și operațiuni de phishing, care au vizat infrastructura critică și serviciile esențiale din statele membre. Operațiunile facilitate de Media Land LLC includ, printre altele, LockBit, EvilCorp și BlackBasta. Prin urmare, Media Land LLC este implicată în atacuri cibernetice cu efecte semnificative, care constituie o amenințare externă la adresa statelor membre.	[+]

[+] JO: a se introduce data publicării prezentului regulament.

	Nume	Informații de identificare	Motive	Data includerii pe listă
9.	ML.Cloud	Adresa: Brivibas iela 52, Riga, LV-1011, Latvija; Russian Federation, Kazan, Peterburgskaya st. 52 Locul înregistrării: Riga Persoană fizică asociată: Alexander Volosovik Alte entități asociate: Media Land LLC	ML.Cloud este societatea-soră a Media Land LLC, furnizându-i acesteia infrastructura tehnică. Încă din 2016, furnizorul de servicii de găzduire «bulletproof» Media Land LLC facilitează o gamă largă de atacuri malware atât împotriva statelor membre, cât și la nivel mondial, oferind servicii de găzduire care ascund identitățile utilizatorilor și rezistă la acțiunile de dezactivare de către autoritățile de aplicare a legii, ceea ce generează pierderi financiare semnificative. Media Land LLC a facilitat operațiuni de tip ransomware de mare amploare, servicii de comandă și control și operațiuni de phishing, care au vizat infrastructura critică și serviciile esențiale din statele membre. Operațiunile facilitate de Media Land LLC includ, printre altele, LockBit, EvilCorp și BlackBasta. Prin urmare, Media Land LLC este implicată în atacuri cibernetice care constituie o amenințare externă cu efecte semnificative asupra statelor membre. Prin urmare, ML Cloud furnizează sprijin tehnic pentru atacuri cibernetice cu un efect semnificativ, care constituie o amenințare externă la adresa statelor membre.	+

+ JO: a se introduce data publicării prezentului regulament.

	Nume	Informații de identificare	Motive	Data includerii pe listă
10.	«Impuls» LLC	Общество с ограниченной ответственностью «Импульс» Adresa: 344015, Russian Federation, Rostov Region, Rostov-on-Don, ul. Eremenko, d. 56, k. 6, apt. 88 Tipul de entitate: societate cu răspundere limitată Locul înregistrării: Interdistrict Inspectorate of the Federal Tax Service No. 26 for the Rostov Region, 344019, Rostov-on-Don, ul. Myasnikova, d. 52/32, Russian Federation Data înregistrării: 27.9.2010	«Impuls» LLC este o societate rusă deținută de Evgeniy Viktorovich Bashev, membru al Agenției ruse de informații militare GRU, unitatea 29155. Societatea furnizează sprijin tehnic și material pentru atacurile cibernetice și tentativele de atacuri cibernetice desfășurate de unitatea GRU 29155. În special, «Impuls» LLC servește drept intermediar operațional care facilitează desfășurarea de activități legate de piraterie informatică prin intermediul unei societăți fără legături formale cu statul rus. Aceasta a facilitat acoperirea operațională, infrastructura și plățile pentru atacurile cibernetice și a fost conectată la active tehnice, inclusiv la serverele utilizate în sprijinul activităților de piraterie informatică. În special, «Impuls» LLC a făcut posibilă cooperarea dintre structurile GRU și rețelele externe de hackeri. Operațiunile cibernetice facilitate de «Impuls» LLC vizează funcții și servicii de stat critice, necesare pentru menținerea activităților sociale și economice esențiale în statele membre, în special în sectorul transporturilor. Prin intermediul campaniei WhisperGate, unitatea GRU 29155 a vizat, de asemenea, infrastructura critică a Ucrainei.	+

+ JO: a se introduce data publicării prezentului regulament.

	Nume	Informații de identificare	Motive	Data includerii pe listă
		Numărul de înregistrare: INN (ИНН): 6168033776; OGRN (ОГРН): 1106194004850 Locul principal de desfășurare a activității: Federația Rusă Persoane fizice asociate: Evgeniy Bashev Entități asociate: Unitatea GRU 29155	Prin urmare, «Impuls» LLC furnizează sprijin tehnic și material pentru (sau este implicată în alt mod în) atacuri cibernetice cu un efect semnificativ, care constituie o amenințare externă pentru statele membre, precum și atacuri cibernetice cu un efect semnificativ împotriva unei țări terțe.	

	Nume	Informații de identificare	Motive	Data includerii pe listă
11.	Z-Pentest	Alias: «Z-Pentest Alliance», «Z-Alliance» Locul principal de desfășurare a activității: Federația Rusă Persoane fizice asociate: Yuliya Pankratova Entități asociate: Cyber Army of Russia (Armata cibernetică a Rusiei)/CARR Contul X.com: ZPentest (Cont suspendat) Contul Telegram: Zpentestalliance	Z-Pentest este un grup de hacktiviști pro-Rusia, alcătuit din membri ai CARR (Cyber Army of Russia Reborn - Armata cibernetică a Rusiei renăscute) și NoName057, care vizează la nivel mondial infrastructura critică, în special sectorul energiei și al apei. Se remarcă atacul grupului asupra unei unități daneze de alimentare cu apă în decembrie 2024. Prin urmare, Z-Pentest este răspunzătoare pentru atacuri cibernetice cu un efect semnificativ, care constituie o amenințare externă la adresa statelor membre.	[+]”.

[+] JO: a se introduce data publicării prezentului regulament.