CONSILIUL INTERINSTITUȚIONAL DE SUPERVIZARE

DECIZIA

nr. 16 din 22 noiembrie 2024

Privind punerea în aplicare a măsurilor restrictive internaționale ale Uniunii Europene împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii Europene sau a statelor sale membre

MODIFICAT
DCIS52 din 02.09.26, MO417-419/03.09.26 art.15; în vigoare 03.09.26

În conformitate cu prevederile art. 11 alin. (7) din Legea nr. 25/2016 privind aplicarea măsurilor restrictive internaționale (republicată în Monitorul Oficial al Republicii Moldova, 2024, nr. 28-31, art. 45), cu modificările ulterioare, pentru asigurarea punerii în aplicare a Ordinului ministrului afacerilor externe nr. 200-s-9 din 15 noiembrie 2024 cu privire la alinierea la măsurile restrictive internaționale ale Uniunii Europene împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii Europene sau a statelor sale membre, cu modificările ulterioare (Decizia (PESC) 2019/797 din 17 mai 2019, cu modificările ulterioare), Consiliul interinstituțional de supervizare

[Clauza de adoptare modificată prin DCIS52 din 02.09.26, MO417-419/03.09.26 art.15; în vigoare 03.09.26]

DECIDE:

1. Se dispune blocarea fondurilor și resurselor economice care aparțin, se află în proprietatea, sunt deținute sau controlate de persoanele fizice și juridice, entitățile și organismele incluse în anexă (în continuare – *subiecți ai restricțiilor*).

2. Se interzice punerea fondurilor și resurselor economice la dispoziția subiecților restricțiilor, precum și utilizarea fondurilor și resurselor economice în beneficiul acestora.

3. În vederea punerii în aplicare a măsurilor de blocare a fondurilor și a resurselor economice prevăzute la pct. 1 și 2:

3.1. entitățile raportoare prevăzute la art. 4 alin. (1) din Legea nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului (în continuare – *Legea nr. 308/2017*):

3.1.1. aplică măsuri de precauție privind clienții similar celor prevăzute de Legea nr. 308/2017 la identificarea subiecților restricțiilor în scopul blocării fondurilor și resurselor economice menționate la art. 28 alin. (1) din Legea nr. 25/2016 privind aplicarea măsurilor restrictive internaționale (în continuare – *Legea nr. 25/2016*). Totodată, pentru evitarea unor tentative de eludare a măsurilor restrictive internaționale, entitățile raportoare aplică măsuri de precauție sporită privind clienții și în cazul subiecților menționați la art. 6 alin (1) din Legea nr. 25/2016;

3.1.2. blochează fondurile și resursele economice care se află în proprietate, sunt deținute de subiecții restricțiilor sau se află sub controlul direct sau indirect al acestora și informează Serviciul Fiscal de Stat despre aceasta imediat, dar nu mai târziu de 24 de ore;

3.1.3. mențin măsurile de blocare până la recepționarea deciziei Serviciului Fiscal de Stat în conformitate cu art. 29 din Legea nr. 25/2016;

3.2. Instituția Publică Cadastrul Bunurilor Imobile, Agenția Servicii Publice, Depozitarul Central Unic al Valorilor Mobiliare, Comisia Națională a Pieței Financiare și alte persoane juridice învestite cu drept de înregistrare/dispunere a bunurilor și drepturilor, inclusiv asupra cotelor-părți

în capitalul social al persoanelor juridice, se vor abține de la executarea oricăror activități care ar facilita transferul și/sau convertirea acestora pentru subiecți ai restricțiilor. Informația cu privire la acțiunile întreprinse în vederea executării prevederilor prezentului subpunct este transmisă Serviciului Fiscal de Stat imediat, dar nu mai târziu de 24 de ore de la momentul identificării și aplicării măsurii corespunzătoare;

3.3. în conformitate cu prevederile art. 29 din Legea nr. 25/2016, Serviciul Fiscal de Stat:

3.3.1. emite decizii de blocare a fondurilor și resurselor economice ale subiecților restricțiilor identificate sau notificate conform subpct. 3.1 sau conform art. 23 și 28 din Legea nr. 25/2016;

3.3.2. informează autoritățile prevăzute la art. 29 alin. (3) din Legea nr. 25/2016 și Consiliul interinstituțional de supervizare despre măsurile întreprinse în conformitate cu prevederile subpct. 3.3;

3.3.3. analizează periodic, dar nu mai rar de o data pe an, măsura dispusă de blocare a fondurilor sau a resurselor economice și revocă din oficiu sau la cerere dacă constată că menținerea acesteia nu se mai justifică, informând neîntârziat despre acest fapt Consiliul interinstituțional de supervizare.

4. Supravegherea punerii în aplicare de către entitățile raportoare prevăzute la art. 4 alin. (1) din Legea nr. 308/2017 a măsurilor stabilite la pct. 1 și 2 se realizează de către organele cu funcții de supraveghere a entităților raportoare prevăzute la art. 15 alin. (1) din Legea nr. 308/2017 și, respectiv, de către Serviciul Prevenirea și Combaterea Spălării Banilor, pentru entitățile din aria sa de competență, conform legislației în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului.

5. În exercitarea atribuțiilor sale în domeniul măsurilor restrictive internaționale, Serviciul de Informații și Securitate:

5.1. informează Serviciul Fiscal de Stat, Serviciul Prevenirea și Combaterea Spălării Banilor și Banca Națională a Moldovei în cazul obținerii unor informații despre pregătirea și/sau aplicarea unor mecanisme de eludare a măsurilor prevăzute de prezenta decizie, care ar implica riscuri de derulare a unor tranzacții prevăzute la subpct. 3.1, 3.2 și 3.3;

5.2. elaborează și aprobă, în termen proxim și în funcție de informațiile de care dispune, lista persoanelor juridice în privința cărora există informații documentate că acestea se află sub controlul unui subiect al restricțiilor prevăzut în anexă sau sunt beneficiari efectivi ai acestuia și o comunică Serviciului Fiscal de Stat în vederea examinării oportunității adoptării deciziei de blocare a fondurilor sau a resurselor economice în conformitate cu prevederile art. 29 din Legea nr. 25/2016.

6. Excepțiile privind blocarea fondurilor și resurselor economice.

6.1. Serviciul Fiscal de Stat poate autoriza deblocarea anumitor fonduri sau resurse economice ori punerea la dispoziție a anumitor fonduri sau resurse economice, după ce a constatat că fondurile sau resursele economice în cauză:

6.1.1. sunt necesare pentru satisfacerea nevoilor de bază ale subiecților restricțiilor și ale membrilor de familie care se află la întreținerea respectivelor persoane fizice, inclusiv plăți necesare pentru achitarea unor cheltuieli pentru alimente, chirie sau rate ipotecare, medicamente și tratamente medicale, impozite, prime de asigurare și plata serviciilor de utilități publice;

6.1.2. sunt destinate exclusiv plății unor onorarii rezonabile și rambursării cheltuielilor suportate ca urmare a prestării unor servicii juridice;

6.1.3. sunt destinate exclusiv plății unor comisioane sau taxe aferente serviciilor de păstrare ori de gestionare curentă a unor fonduri sau resurse economice indisponibilizate;

6.1.4. sunt necesare pentru cheltuieli extraordinare, cu condiția ca Serviciul Fiscal de Stat să informeze Consiliul interinstituțional de supervizare despre motivele pe baza cărora consideră

că ar trebui acordată o autorizație specifică, cu cel puțin două săptămâni înainte de acordarea autorizației; sau

6.1.5. urmează să fie plătite în sau dintr-un cont al unei misiuni diplomatice sau consulare ori al unei organizații internaționale care beneficiază de imunități în conformitate cu dreptul internațional, în măsura în care astfel de plăți sunt destinate a fi utilizate în scopuri oficiale ale misiunii diplomatice sau consulare sau ale organizației internaționale;

6.2. Serviciul Fiscal de Stat poate autoriza deblocarea anumitor fonduri sau resurse economice și în situația în care sunt îndeplinite următoarele condiții:

6.2.1. fondurile sau resursele economice fac obiectul unei hotărâri arbitrale pronunțate înainte de data la care au fost aplicate măsurile restrictive față de subiecți ai restricțiilor prevăzuți în anexă sau al unei hotărâri judecătorești ori decizii administrative executorii pe teritoriul Republicii Moldova anterior sau ulterior datei respective;

6.2.2. fondurile sau resursele economice vor fi utilizate exclusiv pentru a satisface cererile garantate printr-o hotărâre sau decizie menționată la subpct. 6.2.1 ori a căror valabilitate este recunoscută printr-o astfel de hotărâre sau decizie, în limitele stabilite de normele legale ce reglementează drepturile persoanelor care formulează astfel de cereri;

6.2.3. hotărârea sau decizia nu este în beneficiul unui subiect al restricțiilor prevăzut în anexă; și

6.2.4. recunoașterea hotărârii sau a deciziei nu contravine ordinii publice;

6.3. pentru obținerea excepțiilor menționate la subpct. 6.1 și 6.2, orice subiect al restricțiilor poate adresa, în scris, o cerere către Serviciul Fiscal de Stat, însoțită detoate documentele relevante care demonstrează întrunirea condițiilor specificate la subpct. 6.1. sau 6.2;

6.4. Serviciul Fiscal de Stat decide asupra acordării excepției solicitate după obținerea avizului Ministerului Afacerilor Externe. Avizul Ministerului Afacerilor Externe este transmis în termen de 5 zile lucrătoare de la primirea solicitării din partea Serviciului Fiscal de Stat;

6.5. răspunsul la cererea adresată potrivit subpct. 6.3 se comunică solicitantului de către Serviciul Fiscal de Stat în scris, în termen de 15 zile lucrătoare de la primirea acesteia. În cazul în care se solicită o excepție pentru satisfacerea unor nevoi esențiale sau pentru motive umanitare, răspunsul se comunică în termen de 10 zile lucrătoare de la primirea cererii;

6.6. în cazul în care Serviciul Fiscal de Stat autorizează deblocarea anumitor fonduri sau resurse economice, autorizația este strict limitată la scopul pentru care a fost acordată și exclusiv la subiecți ai restricțiilor vizați în mod direct de aceasta;

6.7. restricțiile menționate la pct. 1 nu împiedică subiecții restricțiilor incluși în lista din anexă să efectueze plăți datorate în temeiul unui contract încheiat de subiectul restricțiilor în cauză înainte de data la care măsurile restrictive internaționale au fost aplicate față de subiectul respectiv al restricțiilor, cu condiția ca Serviciul Fiscal de Stat să fi stabilit că beneficiarul plății respective nu este, în mod direct sau indirect, un subiect al restricțiilor și cu respectarea prevederilor art. 31 din Legea nr. 25/2016;

6.8. restricțiile menționate la pct. 1 nu împiedică creditarea conturilor blocate de către societățile de investiții, băncile și alți prestatori de servicii de plată care primesc fonduri transferate de terți în contul subiectului restricției, cu condiția ca toate aceste sume care sunt transferate în conturile respective să fie, de asemenea, blocate. Instituțiile respective informează, fără întârziere, Serviciul Fiscal de Stat cu privire la orice tranzacție de acest tip;

6.9. restricțiile menționate la pct. 2 nu se aplică sumelor transferate în conturile blocate care reprezintă:

6.9.1. dobânzi sau alte sume generate de aceste conturi;

6.9.2. plăți datorate pe baza unor contracte, acorduri care au fost încheiate sau a unor obligații care au survenit anterior datei la care au fost aplicate măsurile restrictive internaționale față de subiectul respectiv al restricțiilor; sau

6.9.3. plăți datorate în temeiul unor hotărâri judecătorești, decizii administrative sau

hotărâri arbitrale care sunt executorii pe teritoriul Republicii Moldova;

6.10. prevederile subpct. 6.9 se aplică cu condiția ca orice astfel de dobânzi, venituri și plăți să rămână blocate pe conturile respective;

6.11. restricțiile menționate la pct. 1 și 2 nu se aplică punerii la dispoziție de fonduri sau resurse economice necesare pentru a asigura furnizarea la timp a asistenței umanitare sau pentru a sprijini alte activități care răspund unor nevoi umane de bază în cazul în care asistența și activitățile menționate sunt desfășurate de:

6.11.1. Organizația Națiunilor Unite, inclusiv prin programele, fondurile și alte entități și organisme ale acesteia, precum și agențiile sale specializate și organizațiile conexe;

6.11.2. organizații internaționale;

6.11.3. organizații umanitare cu statut de observator în cadrul Adunării Generale a Organizației Națiunilor Unite și membri ai respectivelor organizații umanitare;

6.11.4. organizații neguvernamentale finanțate bilateral sau multilateral care participă la planurile de răspuns umanitar ale Organizației Națiunilor Unite, la planurile de răspuns pentru refugiați, la alte apeluri sau clustere umanitare ale Organizației Națiunilor Unite coordonate de Oficiul Organizației Națiunilor Unite pentru Coordonarea Afacerilor Umanitare;

6.11.5. organizații și agenții cărora Uniunea Europeană le-a acordat certificatul de parteneriat umanitar sau care sunt certificate sau recunoscute de către un stat membru al Uniunii Europene sau de către Republica Moldova în conformitate cu procedurile naționale;

6.11.6. agenții specializate ale statelor membre ale Uniunii Europene sau ale Republicii Moldova; sau

6.11.7. angajații, beneficiarii de granturi, filialele sau partenerii de implementare ai entităților menționate la subpct. 6.11.1-6.11.6 atunci când și în măsura în care aceștia acționează în calitățile respective;

6.12. fără a aduce atingere subpct 6.11 și prin derogare de la pct. 1 și 2, Serviciul Fiscal de Stat poate autoriza deblocarea anumitor fonduri sau resurse economice înghețate ori punerea la dispoziție a anumitor fonduri sau resurse economice, în condițiile pe care le consideră adecvate, după ce au stabilit că punerea la dispoziție a respectivelor fonduri sau resurse economice este necesară pentru a asigura furnizarea la timp a asistenței umanitare sau pentru a sprijini alte activități care răspund unor nevoi umane de bază;

6.13. nu se dă curs niciunei cereri în legătură cu orice contract sau tranzacție a cărei executare a fost afectată, în mod direct sau indirect, în totalitate sau în parte, de măsurile impuse în temeiul prezentei decizii, inclusiv cererilor de acordare de despăgubiri sau oricărei alte cereri de acest tip, cum ar fi cererile de compensare sau cele de chemare în garanție, în special cererilor de prelungire sau de plată a unei obligațiuni, a unei garanții sau a unei indemnizații, în special a unei garanții financiare sau a unei indemnizații financiare, indiferent de formă, în cazul în care sunt formulate de:

6.13.1. subiecți ai restricțiilor prevăzuți în anexă;

6.13.2. orice persoană fizică sau juridică, entitate sau organism care acționează prin intermediul sau în numele unui subiect al restricțiilor;

6.14. Serviciul Fiscal de Stat informează neîntârziat Consiliul interinstituțional de supervizare despre acordarea excepțiilor prevăzute la pct. 6.

7. Se aplică interdicții de intrare, tranzitare, ședere și aflare pe teritoriul Republicii Moldova față de persoanele fizice, conform anexei.

8. Ministerul Afacerilor Interne va asigura aplicarea restricțiilor menționate la pct. 7.

9. Excepțiile privind aplicarea restricțiilor de călătorie:

9.1. restricțiile menționate la pct. 7 nu se aplică persoanelor fizice cetățeni ai Republicii Moldova;

9.2. prevederile pct. 7 nu aduc atingere cazurilor în care Republicii Moldova îi revine o obligație de drept internațional, și anume:

9.2.1. în calitate de țară-gazdă a unei organizații internaționale interguvernamentale;

9.2.2. în calitate de țară-gazdă a unei conferințe internaționale convocate de Organizația Națiunilor Unite sau desfășurate sub auspiciile acesteia;

9.2.3. în temeiul unui acord multilateral care conferă privilegii și imunități;

9.3. excepțiile de la restricțiile impuse în temeiul pct. 7 pot fi acordate atunci când deplasarea subiectului restricțiilor se justifică din motive umanitare urgente sau se efectuează în scopul participării la reuniuni interguvernamentale și la reuniuni promovate sau găzduite de Uniune, sau la reuniuni găzduite de un stat membru care asigură președinția OSCE, în cazul în care se poartă un dialog politic care vizează direct promovarea obiectivelor de politică ale măsurilor restrictive, inclusiv securitatea și stabilitatea în spațiul cibernetic.

9.4. de asemenea, pot fi acordate derogări de la măsurile impuse în temeiul pct. 7 și în cazul în care intrarea sau tranzitul este necesar pentru îndeplinirea unor proceduri judiciare.

10. Pentru obținerea excepțiilor menționate la subpct. 9.2, 9.3 și 9.4, orice subiect al restricțiilor de călătorie poate adresa, în scris, o cerere către Ministerul Afacerilor Interne, însoțită de toate documentele relevante ce confirmă scopul și circumstanțele deplasării subiectului restricțiilor.

11. Ministerul Afacerilor Interne decide asupra acordării excepției solicitate după obținerea avizelor Ministerului Afacerilor Externe și ale Serviciului de Informații și Securitate. Avizele menționate se transmit în termen de 5 zile lucrătoare de la primirea solicitării din partea Ministerului Afacerilor Interne.

12. Răspunsul la cererea adresată potrivit pct. 10 se comunică solicitantului de către Ministerul Afacerilor Interne în scris, în termen de 15 zile lucrătoare de la primirea acesteia. În cazul în care se solicită o excepție pentru satisfacerea unor nevoi esențiale sau pentru motive umanitare, răspunsul se comunică în termen de 10 zile lucrătoare de la primirea cererii.

13. În cazul în care Ministerul Afacerilor Interne autorizează intrarea, tranzitarea, șederea sau aflarea pe teritoriul Republicii Moldova a unor subiecți ai restricțiilor, autorizația este strict limitată la scopul pentru care a fost acordată și exclusiv la subiecți ai restricțiilor vizați în mod direct de aceasta.

14. Ministerul Afacerilor Interne informează neîntârziat Consiliul interinstituțional de supervizare despre acordarea excepțiilor menționate la pct. 9.

15. Serviciul de Informații și Securitate va elabora, în termen proxim și în funcție de informația de care dispune, lista persoanelor fizice și juridice în privința cărora există probe și informații documentate că sunt asociate subiecților restricțiilor prevăzuți în anexă și va întreprinde acțiunile subsecvente stabilite de art. 6 din Legea nr. 25/2016.

16. Pentru identificarea, prevenirea și evitarea activităților sau a tranzacțiilor care urmăresc eludarea măsurilor restrictive internaționale prevăzute la pct. 1 și 2, instituțiile și autoritățile publice cu competențe în domeniul vizat întreprind măsurile necesare în conformitate cu art. 6 din Legea nr. 25/2016.

17. Autoritățile și instituțiile publice, precum și persoanele fizice și juridice informează Consiliul interinstituțional de supervizare cu privire la situațiile considerate ca fiind o încălcare a măsurilor restrictive internaționale aplicate prin prezenta decizie.

18. Ca urmare a recepționării informațiilor menționate la pct. 17, Consiliul interinstituțional de supervizare va sesiza organele de drept cu privire la cazurile de încălcare a

măsurilor restrictive prevăzute de prezenta decizie.

19. Autoritățile și instituțiile publice pot sesiza direct organele de drept cu privire la cazurile de încălcare a măsurilor restrictive prevăzute de prezenta decizie. În aceste cazuri, copia sesizării se transmite Consiliului interinstituțional de supervizare.

20. Autoritățile și instituțiile publice abilitate prin prezenta decizie informează Consiliul interinstituțional de supervizare semestrial, precum și la solicitare, despre acțiunile întreprinse pentru punerea în aplicare a măsurilor restrictive prevăzute în prezenta decizie, precum și, neîntârziat, despre dificultățile de aplicare identificate.

21. Consiliul interinstituțional de supervizare, prin intermediul Ministerului Afacerilor Externe, informează instituțiile relevante ale Uniunii Europene despre acțiunile întreprinse pe plan intern și despre dificultățile de aplicare a măsurilor restrictive.

22. Ținerea evidenței măsurilor restrictive prevăzute în prezenta decizie se face cu respectarea prevederilor legale privind protecția și prelucrarea datelor cu caracter personal. În cazul în care această posibilitate nu este prevăzută de prevederile legale speciale ce reglementează atribuțiile lor de serviciu, persoanele responsabile din cadrul Consiliului interinstituțional de supervizare și al altor autorități/instituții publice competente pot prelucra, dacă este cazul, datele relevante referitoare la infracțiuni comise de subiecți ai restricțiilor prevăzuți în anexă, la condamnări penale ale acestora sau la măsuri de securitate privind aceştia numai în măsura în care o astfel de prelucrare este necesară pentru desfăşurarea procedurilor de aplicare a măsurilor restrictive internaționale și de întocmire și completare a listei naționale cu persoanele subiecți ai restricțiilor.
În asemenea situații, Consiliul interinstituțional de supervizare și autoritățile/instituțiile publice competente exercită atribuțiile prevăzute de Legea nr. 25/2016 în calitate de operatori de date cu caracter personal, iar persoanele responsabile din cadrul acestora – în calitate de persoane împuternicite de către operator, astfel cum sunt reglementate acestea de legislația privind protecția datelor cu caracter personal.

23. Asigurarea publicității informațiilor în privința subiecților restricțiilor prevăzuți în anexă, cu respectarea condițiilor stabilite de Legea nr. 25/2016, nu reprezintă o încălcare a reglementărilor legale privind protecția datelor cu caracter personal și nu poate angaja răspunderea persoanelor responsabile.

24. Mecanismul de implementare a măsurilor restrictive internaționale prevăzut de prezenta decizie se aplică pe durata valabilității Deciziei (PESC) 2019/797 a Consiliului Uniunii Europene din 17 mai 2019, cu modificările ulterioare.

25. Prezenta decizie intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova și se publică inclusiv pe site-ul web oficial al Guvernului, precum şi pe site-urile web ale autorităților şi instituțiilor publice responsabile de punerea în aplicare a acesteia.

26. Consiliul interinstituțional de supervizare poate modifica prezenta decizie prin adoptarea deciziilor de modificare pe baza ordinelor de aliniere la măsurile restrictive ale Uniunii Europene, emise de către ministrul afacerilor externe, în conformitate cu prevederile art. 11 alin. (8) din Legea nr. 25/2016.

Prim-ministru,
Președinte al Consiliului
interinstituțional de supervizare **Dorin RECEAN**

CANCELARIA DE STAT A REPUBLICII MOLDOVA
DIRECȚIA MANAGEMENTUL DOCUMENTELOR
3

ANEXĂ

[Anexă modificată prin DCIS52 din 02.09.26, MO417-419/03.09.26 art.15; în vigoare 03.09.26]

LISTA
subiecților în privința cărora au fost aplicate măsurile restrictive internaționale
conform Deciziei (PESC) 2019/797 a Consiliului Uniunii Europene din 17 mai 2019

A. PERSOANE FIZICE

Nr. crt.	Numele, prenumele	Informațiile de identificare	Motivele aplicării măsurilor restrictive de către Uniunea Europeană	Data includerii pe listă de către Uniunea Europeană și data aplicării restricțiilor de către Republica Moldova
1.	GAO Qiang	Data nașterii: 4 octombrie 1983 Locul nașterii: provincia Shandong, China Adresa: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Cetățenia: chineză Sexul: masculin	Gao Qiang are legături cu actorul generic „APT10” („Advanced Persistent Threat 10”) (*alias „*Red Apollo”, „CVNX”, „Stone Panda”, „MenuPass” și „Potassium”) și a fost implicat în „Operation Cloud Hopper„, o serie de atacuri cibernetice având efecte importante, a căror origine se situează în afara Uniunii și care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre, precum și în atacuri cibernetice având efecte importante asupra unor state terțe. „Operation Cloud Hopper” a vizat sistemele de informații ale unor întreprinderi multinaționale de pe șase continente, inclusiv ale unor întreprinderi situate în Uniune, și a dobândit acces neautorizat la date sensibile din punct de vedere comercial, ceea ce a provocat pierderi economice importante. Gao Qiang este asociat cu infrastructura de comandă și control a APT10. În plus, Huaying Haitai, o societate utilizată de APT10 și desemnată pentru că a oferit sprijin și a facilitat «Operation	UE – 30.07.2020 RM – 13.06.2023

			Cloud Hopper», l-a avut drept angajat pe Gao Qiang. Gao Qiang este asociat și cu Zhang Shilong, care are legături cu APT10 și care a fost, de asemenea, angajat al Huaying Haitai	
2.	ZHANG Shilong	Data nașterii: 10 septembrie 1981 Locul nașterii: China Adresa: Hedong, Yuyang Road No 121, Tianjin, China Cetățenia: chineză Sexul: masculin	Zhang Shilong are legături cu actorul generic „APT10” («Advanced Persistent Threat 10») (*alias „*Red Apollo”, «CVNX», „Stone Panda”, „MenuPass” și „Potassium”) și a fost implicat în „Operation Cloud Hopper”, o serie de atacuri cibernetice având efecte importante, a căror origine se situează în afara Uniunii și care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre, precum și în atacuri cibernetice având efecte importante asupra unor state terțe. „Operation Cloud Hopper” a vizat sistemele de informații ale unor întreprinderi multinaționale de pe șase continente, inclusiv ale unor întreprinderi situate în Uniune, și a dobândit acces neautorizat la date sensibile din punct de vedere comercial, ceea ce a provocat pierderi economice importante. Zhang Shilong este asociat cu APT10, inclusiv prin programele malware pe care le-a dezvoltat și testat în legătură cu atacurile cibernetice desfășurate de APT10. În plus, Huaying Haitai, o societate utilizată de APT10 și desemnată pentru că a oferit sprijin și a facilitat «Operation Cloud Hopper», l-a avut drept angajat pe Zhang Shilong. Zhang Shilong este asociat cu Gao Qiang, care are legături cu APT10 și care a fost, de asemenea, angajat al Huaying Haita.	UE – 30.07.2020 RM – 13.06.2023
3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Data nașterii: 27.05.1972 Locul nașterii: Regiunea Perm, RSFS Rusă (în prezent Federația Rusă) Numărul pașaportului: 120017582 Eliberat de: Ministerul de Externe al Federației Ruse	Alexey Minin a luat parte la o tentativă de atac cibernetic cu efecte potențial semnificative asupra Organizației pentru Interzicerea Armelor Chimice (OIAC) în Țările de Jos și la atacuri cibernetice cu efecte semnificative asupra unor state terțe. În calitatea sa de ofițer de sprijin specializat în informații din surse umane al Direcției principale a Statului-Major al forțelor armate ruse (GU/GRU), Alexey Minin a făcut parte dintr-o echipă formată din patru ofițeri din serviciul militar de informații rus, care a încercat să obțină accesul neautorizat la rețeaua Wi-Fi	UE – 30.07.2020 RM – 13.06.2023

		Valabil de la 17.4.2017 la 17.4.2022 Loc: Moscova, Federația Rusă Cetățenie: rusă Sexul: masculin	a OIAC de la Haga, Țările de Jos, în aprilie 2018. Tentativa de atac cibernetic viza accesul neautorizat la rețeaua Wi-Fi a OIAC, care, în caz de reușită, ar fi compromis securitatea rețelei și activitatea de investigare în curs a OIAC. Serviciul de securitate, de informații și de apărare din Țările de Jos (Militaire Inlichtingen- en Veiligheidsdienst) a întrerupt tentativa de atac cibernetic, preîntâmpinând astfel un prejudiciu grav pentru OIAC. Un mare juriu din districtul Pennsylvania de Vest (Statele Unite ale Americii) l-a pus sub acuzare pe Alexey Minin, ca ofițer al GRU, pentru piraterie informatică, fraudă cu ajutorul mijloacelor de comunicare, furt de identitate calificat și spălarea banilor. GRU rămâne activă în desfășurarea de atacuri cibernetice împotriva Uniunii sau a statelor sale membre. În calitatea sa de membru al GRU, Alexey Minin este implicat așadar în atacuri cibernetice cu un efect semnificativ, inclusiv tentative de atacuri cibernetice care au un efect potențial semnificativ, care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.	
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Data nașterii: 31.7.1977 Locul nașterii: Regiunea Murmansk, RSFS Rusă (în prezent Federația Rusă) Numărul pașaportului: 100135556 Eliberat de: Ministrul de Externe al Federației Ruse Valabil de la 17.4.2017 la 17.4.2022 Loc: Moscova, Federația Rusă Cetățenia: rusă Sexul: masculin	Alexey Morenets a luat parte la o tentativă de atac cibernetic cu efecte potențial semnificative asupra Organizației pentru Interzicerea Armelor Chimice (OIAC) în Țările de Jos și la atacuri cibernetice cu efecte semnificative asupra unor state terțe. În calitatea sa de operator informatic pentru Direcția principală a Statului-Major al forțelor armate ruse (GU/GRU), Aleksei Morenets a făcut parte dintr-o echipă formată din patru ofițeri din serviciul militar de informații rus, care a încercat să obțină accesul neautorizat la rețeaua Wi-Fi a OIAC de la Haga, Țările de Jos, în aprilie 2018. Tentativa de atac cibernetic viza accesul neautorizat la rețeaua Wi-Fi a OIAC, care, în caz de reușită, ar fi compromis securitatea rețelei și activitatea de investigare în curs a OIAC. Serviciul de securitate, de informații și de apărare din Țările de Jos (Militaire Inlichtingen- en Veiligheidsdienst) a întrerupt tentativa de atac cibernetic, preîntâmpinând astfel un prejudiciu grav pentru OIAC. Un mare juriu din districtul	UE – 30.07.2020 RM – 13.06.2023

			Pennsylvania de Vest (Statele Unite ale Americii) l-a pus sub acuzare pe Alexey Morenets ca membru al unității militare 26165, pentru piraterie informatică, fraudă cu ajutorul mijloacelor de comunicare, furt de identitate calificat și spălarea banilor. GRU rămâne activă în desfășurarea de atacuri cibernetice împotriva Uniunii sau a statelor sale membre. În calitatea sa de membru al GRU, Aleksei Morenets este așadar implicat în atacuri cibernetice cu un efect semnificativ, inclusiv tentative de atacuri cibernetice care au un efect potențial semnificativ, care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.	
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Data nașterii: 26.7.1981 Locul nașterii: Kursk, RSFS Rusă (în prezent, Federația Rusă) Numărul pașaportului: 100135555 Eliberat de: Ministerul de Externe al Federației Ruse Valabil de la 17.4.2017 la 17.4.2022 Loc: Moscova, Federația Rusă Cetățenie: rusă Sexul: masculin	Evgenii Serebriakov a luat parte la o tentativă de atac cibernetic cu efecte potențial semnificative asupra Organizației pentru Interzicerea Armelor Chimice (OIAC) în Țările de Jos și la atacuri cibernetice cu efecte semnificative asupra unor state terțe. În calitatea sa de operator informatic pentru Direcția principală a StatuluiMajor al forțelor armate ruse (GU/GRU), Evgenii Serebriakov a făcut parte dintr-o echipă formată din patru ofițeri din serviciul militar de informații rus, care a încercat să obțină accesul neautorizat la rețeaua Wi-Fi a OIAC de la Haga, Țările de Jos, în aprilie 2018. Tentativa de atac cibernetic viza accesul neautorizat la rețeaua Wi-Fi a OIAC, care, în caz de reușită, ar fi compromis securitatea rețelei și activitatea de investigare în curs a OIAC. Serviciul de securitate, de informații și de apărare din Țările de Jos (Militaire Inlichtingen- en Veiligheidsdienst) a întrerupt tentativa de atac cibernetic, preîntâmpinând astfel un prejudiciu grav pentru OIAC. Din primăvara anului 2022, Evgenii Serebriakov conduce «Sandworm» (alias «Sandworm Team», «BlackEnergy Group», «Voodoo Bear», «Quedagh», «Olympic Destroyer» și «Telebots»), un actor și un grup de piraterie informatică afiliat unității 74455 a Direcției principale de informații ruse. Sandworm a desfășurat atacuri cibernetice asupra Ucrainei, inclusiv asupra agențiilor guvernamentale ucrainene, în urma războiului de agresiune al Rusiei împotriva	UE – 30.07.2020 RM – 13.06.2023

			Ucrainei. GRU rămâne activă în desfășurarea de atacuri cibernetice împotriva Uniunii sau a statelor sale membre. În calitatea sa de membru al GRU, Evgenii Serebriakov este așadar implicat în atacuri cibernetice cu un efect semnificativ, inclusiv tentative de atacuri cibernetice care au un efect potențial semnificativ, care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.	
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Data nașterii: 24.8.1972 Locul nașterii: Ulianovsk, RSFS Rusă (în prezent, Federația Rusă) Numărul pașaportului: 120018866 Eliberat de: Ministerul de Externe al Federației Ruse Valabil de la 17.4.2017 la 17.4.2022 Loc: Moscova, Federația Rusă Cetățenie: rusă Sexul: masculin	Oleg Sotnikov a luat parte la o tentativă de atac cibernetic cu efecte potențial semnificative asupra Organizației pentru Interzicerea Armelor Chimice (OIAC) în Țările de Jos și la atacuri cibernetice cu efecte semnificative asupra unor state terțe. În calitatea sa de ofițer de sprijin specializat în informații din surse umane al Direcției principale a Statului-Major al forțelor armate ruse (GU/GRU), Oleg Sotnikov a făcut parte dintr-o echipă formată din patru ofițeri din serviciul militar de informații rus, care a încercat să obțină accesul neautorizat la rețeaua WiFi a OIAC de la Haga, Țările de Jos, în aprilie 2018. Tentativa de atac cibernetic viza accesul neautorizat la rețeaua Wi-Fi a OIAC, care, în caz de reușită, ar fi compromis securitatea rețelei și activitatea de investigare în curs a OIAC. Serviciul de securitate, de informații și de apărare din Țările de Jos (Militaire Inlichtingen- en Veiligheidsdienst) a întrerupt tentativa de atac cibernetic, preîntâmpinând astfel un prejudiciu grav pentru OIAC. Un mare juriu din districtul Pennsylvania de Vest (Statele Unite ale Americii) l-a pus sub acuzare pe Oleg Sotnikov ca ofițer al GRU, pentru piraterie informatică, fraudă cu ajutorul mijloacelor de comunicare, furt de identitate calificat și spălarea banilor. GRU rămâne activă în desfășurarea de atacuri cibernetice împotriva Uniunii sau a statelor sale membre. În calitatea sa de membru al GRU, Oleg Sotnikov este așadar implicat în atacuri cibernetice cu un efect semnificativ, inclusiv tentative de atacuri cibernetice care au un efect potențial semnificativ, care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.	UE – 30.07.2020 RM – 13.06.2023

7.	Dmitri Sergheevici BADIN	Дмитрий Сергеевич БАДИН Data nașterii: 15.11.1990 Locul nașterii: Kursk, RSFS Rusă (în prezent, Federația Rusă) Cetățenie: rusă Sexul: masculin	Dmitry Badin a luat parte la un atac cibernetic cu efecte semnificative asupra parlamentului federal german (Deutscher Bundestag) și la atacuri cibernetice cu efecte semnificative asupra unor state terțe. În calitatea sa de ofițer în serviciul militar de informații al celui de al 85-lea Centru principal de servicii speciale (GTsSS) din cadrul Direcției principale a Statului-Major al forțelor armate al Federației Ruse (GU/GRU), Dmitry Badin a făcut parte dintr-o echipă de ofițeri ai serviciului militar de informații rus care a organizat un atac cibernetic împotriva parlamentului federal german în aprilie și mai 2015. Respectivul atac cibernetic a fost îndreptat împotriva sistemului informatic al parlamentului, căruia i-a afectat funcționarea timp de mai multe zile. A fost furat un volum important de date și au fost afectate conturile de e-mail ale mai multor parlamentari, precum și cel al fostei cancelare Angela Merkel. Un mare juriu din districtul Pennsylvania de Vest (Statele Unite ale Americii) l-a pus sub acuzare pe Dmitry Badin ca membru al unității militare 26165, pentru piraterie informatică, fraudă cu ajutorul mijloacelor de comunicare, furt de identitate calificat și spălarea banilor. GRU rămâne activă în desfășurarea de atacuri cibernetice împotriva Uniunii sau a statelor sale membre. În calitatea sa de membru al GRU, Dmitry Badin este așadar implicat în atacuri cibernetice cu un efect semnificativ, inclusiv tentative de atacuri cibernetice care au un efect potențial semnificativ, care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.	UE – 22.10.2020 RM – 13.06.2023

8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Data nașterii: 21.2.1961 Cetățenie: rusă Sexul: masculin	Igor Kostyukov este actualul șef al Direcției principale a Statului-Major al forțelor armate al Federației Ruse (GU/GRU), unde a ocupat anterior funcția de prim-șef adjunct. Una dintre unitățile aflate sub comanda sa este cel de al 85-lea Centru principal de servicii speciale (GTsSS) (alias «unitatea militară 26165», «APT28», «Fancy Bear», «Sofacy Group», «Pawn Storm» și «Strontium»). În această calitate, Igor Kostyukov este responsabil de atacurile cibernetice desfășurate de GTsSS, inclusiv de atacuri cu efecte semnificative care reprezintă o amenințare externă la adresa Uniunii sau a statelor sale membre. În special, ofițerii serviciului militar de informații al GTsSS au luat parte la atacul cibernetic împotriva parlamentului federal german (Deutscher Bundestag) în aprilie și mai 2015, precum și la tentativa de atac cibernetic din aprilie 2018 care a avut drept scop piratarea rețelei Wi-Fi a Organizației pentru Interzicerea Armelor Chimice (OIAC) din Țările de Jos. Atacul cibernetic împotriva parlamentului federal german a fost îndreptat împotriva sistemului informatic al acestuia, căruia ia afectat funcționarea timp de mai multe zile. A fost furat un volum important de date și au fost afectate conturile de e-mail ale mai multor parlamentari, precum și cel al fostei cancelare Angela Merkel. GRU rămâne activă în desfășurarea de atacuri cibernetice împotriva Uniunii sau a statelor sale membre. În calitatea sa de membru al GRU, Igor Kostyukov este așadar implicat în atacuri cibernetice cu un efect semnificativ, inclusiv tentative de atacuri cibernetice care au un efect potențial semnificativ, care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.	UE – 22.10.2020 RM – 13.06.2023
9.	Ruslan Aleksandrovich PERETYATKO	Руслан Александрович ПЕРЕТЯТЬКО Data nașterii: 03.08.1985 Cetățenia: rusă Sexul: masculin	Ruslan Peretyatko a participat la atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre. Ruslan Peretyatko face parte din „grupul Callisto” format din ofițeri de informații militari ruși care desfășoară operațiuni	UE – 24.06.2024 RM – 26.11.2024

			cibernetice împotriva statelor membre ale UE și împotriva unor state terțe. Grupul Callisto (cunoscut și sub denumirea de „Seaborgium”, „Star Blizzard”, „ColdRiver”, „TA446”) a lansat campanii multianuale de phishing utilizate pentru a fura date din conturi și elementele personale de acces la acestea. În plus, grupul Callisto este responsabil de campanii care vizează persoane și funcții critice ale statului, inclusiv în domeniul apărării și al relațiilor externe. Prin urmare, Ruslan Peretyatko este implicat în atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre	
10.	Andrey Stanislavovich KORINETS	Андрей Станиславович КОРИНЕЦ Data nașterii: 18.05.1987 Locul nașterii: orașul Syktyvkar, Rusia Cetățenia: rusă Sexul: masculin	Andrey Stanislavovich Korinets a participat la atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre. Andrey Stanislavovich Korinets este ofițer al „Centrului 18” al Serviciului Federal de Securitate (FSB) al Federației Ruse. Andrey Stanislavovich Korinets face parte din „grupul Callisto” format din ofițeri de informații militari ruși care desfășoară operațiuni cibernetice împotriva statelor membre ale UE și împotriva unor state terțe. Grupul Callisto (cunoscut și sub denumirea de „Seaborgium”, „Star Blizzard”, „ColdRiver”, „TA446”) a lansat campanii multianuale de phishing utilizate pentru a fura date din conturi și elementele personale de acces la acestea. În plus, grupul Callisto este responsabil de campanii care vizează persoane și funcții critice ale statului, inclusiv în domeniul apărării și al relațiilor externe. Prin urmare, Andrey Stanislavovich Korinets este implicat în atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre	UE – 24.06.2024 RM – 26.11.2024

11.	Oleksandr SKLIANKO	Александр СКЛЯНКО (ortografie rusă) Олександр СКЛЯНКО (ortografie ucraineană) Data nașterii: 05.08.1973 Pașaport: EC 867868, eliberat la 27.11.1998 (Ucraina) Sexul: masculin	Oleksandr Sklianko a participat la atacuri cibernetice cu un efect semnificativ împotriva statelor membre ale UE, precum și la atacuri cibernetice cu un efect semnificativ împotriva unor state terțe. Oleksandr Sklianko face parte din grupul de hackeri Armageddon, sprijinit de Serviciul Federal de Securitate (FSB) al Federației Ruse, care a desfășurat diverse atacuri cibernetice cu un efect semnificativ asupra Guvernului Ucrainei și asupra statelor membre ale UE și a funcționarilor lor guvernamentali, inclusiv prin utilizarea e-mailurilor de phishing și prin campanii de malware. Prin urmare, Oleksandr Sklianko este implicat în atacuri cibernetice cu un efect semnificativ împotriva unor state terțe, precum și în atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre	UE – 24.06.2024 RM – 26.11.2024
12.	Mykola CHERNYKH	Николай ЧЕРНЫХ (ortografie rusă) Микола ЧЕРНИХ (ortografie ucraineană) Data nașterii: 12.10.1978 Pașaport: CE 922162, eliberat la 20.1.1999 (Ucraina) Sexul: masculin	Mykola Chernykh a participat la atacuri cibernetice cu un efect semnificativ împotriva statelor membre ale UE, precum și la atacuri cibernetice cu un efect semnificativ împotriva unor state terțe. Mykola Chernykh face parte din grupul de hackeri Armageddon sprijinit de Serviciul Federal de Securitate (FSB) al Federației Ruse, care a desfășurat diverse atacuri cibernetice cu un efect semnificativ asupra Guvernului Ucrainei și asupra statelor membre ale UE și a funcționarilor lor guvernamentali, inclusiv prin utilizarea de e-mailurilor de phishing și prin campanii de malware. În calitate de fost angajat al Serviciului de Securitate al Ucrainei, este acuzat în Ucraina de trădare și intervenție neautorizată în funcționarea mașinilor electronice de calcul și a sistemelor automatizate Prin urmare, Mykola Chernykh este implicat în atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre	UE – 24.06.2024 RM – 26.11.2024

13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Data nașterii: 20.4.1989 Locul nașterii: Serpuhov, Federația Rusă Cetățenia: rusă Adresa: Serpuhov Sexul: masculin	Mikhail Mikhailovich Tsarev a participat la atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa statelor membre ale UE. Mikhail Mikhailovich Tsarev, cunoscut și sub pseudonimele online „Mango”, „Alexander Grachev”, „Super Misha”, „Ivanov Mixail”, „Misha Krutysha” și „Nikita Andreevich Tsarev”, este un actor-cheie în răspândirea programelor malware „Conti” și „Trickbot” și este implicat în grupul ostil „Wizard Spider” din Rusia. Wizard Spider continuă să evolueze și să își intensifice operațiunile. Programele malware Conti și Trickbot au fost create și dezvoltate de Wizard Spider. Wizard Spider a desfășurat campanii de tip ransomware în diverse sectoare, inclusiv servicii esențiale cum ar fi sănătatea și serviciile bancare. Grupul a infectat computere în 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, TrickBot „Ryuk” sau Black Basta, sunt responsabile pentru daune economice substanțiale în Uniunea Europeană. Prin urmare, Mikhail Mikhailovich Tsarev este implicat în atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre	UE – 24.06.2024 RM – 26.11.2024
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Data nașterii: 19.5.1982 Locul nașterii: Abakan, Federația Rusă Cetățenia: rusă Sexul: masculin	Maksim Galochkin a participat la atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa statelor membre ale UE. Maksim Galochkin este cunoscut și sub pseudonimele online „Benalen”, „Bentley”, „Volhvb”, „volhvb”, „manuel”, „Max17” și „Crypt”. Galochkin este un actor-cheie în răspândirea programelor malware «Conti» și «Trickbot» și este implicat în grupul ostil «Wizard Spider» din Rusia. El a condus un grup de testeri, având responsabilități legate de dezvoltarea, controlul și aplicarea testelor pentru programul malware TrickBot, creat și implementat de Wizard Spider. Wizard Spider continuă să	UE – 24.06.2024 RM – 26.11.2024”;

			evolueze și să își intensifice operațiunile. Wizard Spider a desfășurat campanii de tip ransomware în diverse sectoare, inclusiv servicii esențiale cum ar fi sănătatea și serviciile bancare. Grupul a infectat computere în 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, TrickBot „Ryuk” sau Black Basta, sunt responsabile pentru daune economice substanțiale în Uniunea Europeană. Prin urmare, Maksim Galochkin este implicat în atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre	
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	UE –27.01.2025 RM – 07.03.2025

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	UE –27.01.2025 RM – 07.03.2025
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	UE –27.01.2025 RM – 07.03.2025

			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	
18.	CHEN Cheng	陈诚 (ortografia chineză) Alias: Jesse Chen lengmo l3n6m0 Data nașterii: 20.10.1984 Locul nașterii: Yancheng, Jiangsu, China Cetățenia: chineză Sexul: masculin	Chen Cheng este un om de afaceri chinez, cofondator și unul dintre directorii generali (director general administrativ) ai Anxun Information Technology Co. Ltd. De asemenea, este reprezentant legal al sucursalei din Sichuan a respectivei societăți. Anxun Information Technology Co. Ltd., cunoscută și sub denumirea i-Soon, este o societate cu sediul în Republica Populară Chineză (RPC) care oferă servicii de tip «hacking-for-hire». Anxun Information Technology Co. Ltd. a vizat infrastructura critică și funcțiile critice ale statului din statele membre și a accesat și vândut informații clasificate. În plus, Anxun Information Technology Co. Ltd. a atacat guverne din diferite state terțe, ceea ce reprezintă o amenințare la adresa obiectivelor Uniunii în materie de politică externă și de securitate comună (PESC), astfel cum se prevede la articolul 21 alineatul (2) literele (a)-(c) din Tratatul privind Uniunea Europeană. Anxun Information Technology Co. Ltd. obține un beneficiu economic important din serviciile furnizate. Prin urmare, Anxun Information Technology Co. Ltd. este responsabilă de atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa statelor membre ale Uniunii, precum și de atacuri la adresa statelor terțe. În calitatea respectivă, Chen Cheng este responsabil de atacuri cibernetice cu efecte semnificative care reprezintă o amenințare externă la adresa statelor membre, precum și de atacuri cibernetice cu efecte semnificative împotriva unor state terțe și este implicat în astfel de atacuri	UE – 16.03.2026 RM – 23.04.2026

19.	WU Haibo	吴海波 (ortografia chineză) Alias: shutdown shutd0wn Locul nașterii: China Cetățenia: chineză Sexul: masculin	Wu Haibo este un om de afaceri chinez, cofondator și unul dintre directorii generali (director general administrativ) ai Anxun Information Technology Co. Ltd. De asemenea, este reprezentant legal, președinte și director general al sucursalei din Shanghai («societatea mamă») a Anxun Information Technology Co. Ltd. De asemenea, acționează și în calitate de reprezentant legal al sucursalei din Sichuan al respectivei societăți. Anxun Information Technology Co. Ltd., cunoscută și sub denumirea i-Soon, este o societate cu sediul în Republica Populară Chineză (RPC) care oferă servicii de tip «hacking-for-hire». Anxun Information Technology Co. Ltd. a vizat infrastructura critică și funcțiile critice ale statului din statele membre și a accesat și vândut informații clasificate. În plus, Anxun Information Technology Co. Ltd. a atacat guverne din diferite state terțe, ceea ce reprezintă o amenințare la adresa obiectivelor Uniunii în materie de politică externă și de securitate comună (PESC), astfel cum se prevede la articolul 21 alineatul (2) literele (a)-(c) din Tratatul privind Uniunea Europeană. Anxun Information Technology Co. Ltd. obține un beneficiu economic important din serviciile furnizate. Prin urmare, Anxun Information Technology Co. Ltd. este responsabilă de atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa statelor membre, precum și de atacuri la adresa statelor terțe. Wu Haibo a fost implicat în conducerea și încurajarea tentativelor de atacuri cibernetice cu efecte semnificative asupra statelor membre. În calitatea respectivă, el este responsabil de atacuri cibernetice cu efecte semnificative care reprezintă o amenințare externă la adresa statelor membre, precum și de atacuri cibernetice cu efecte semnificative împotriva unor state terțe și este implicat în astfel de atacuri	UE – 16.03.2026 RM – 23.04.2026
20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ alias: «Bentley», «Bergen», «Alex Konor», «Benny», «Ben», «Stern»	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.	UE – 13.07.2026 RM - 28.08.2026

		Data nașterii: 23.06.1988 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	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	
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Data nașterii: 30.01.1983 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	UE – 13.07.2026 RM - 28.08.2026
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО alias: «Dena» Data nașterii: 09.10.1989 Locul nașterii: URSS Cetățenia: rusă	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	UE – 13.07.2026 RM - 28.08.2026

		Sexul: masculin Adresa: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	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	
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА alias: «YUliYA» Data nașterii: 06.04.1984 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.	UE – 13.07.2026 RM - 28.08.2026

			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	
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	UE – 13.07.2026 RM - 28.08.2026
25.	Maksim Aleksandrovich 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	UE – 13.07.2026 RM - 28.08.2026

	alias Maxim Alexandrovich GORDIENKO		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	
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Data nașterii: 25.01.1980 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. 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	UE – 13.07.2026 RM - 28.08.2026

			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	
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. 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	UE – 13.07.2026 RM -28.08.2026.”

B. PERSOANE JURIDICE, ENTITĂȚI SAU ORGANISME

Nr.crt.	Denumirea	Informațiile de identificare	Motivele aplicării măsurilor restrictive de către Uniunea Europeană	Data includerii pe listă de către Uniunea Europeană și data aplicării restricțiilor de către Republica Moldova
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Compania de dezvoltare științifică și tehnologică Huaying Haitai SRL din Tianjin) (Huaying Haitai)	*alias*: Haitai Technology Development Co. Ltd Localitate: Tianjin, China	Huaying Haitai a sprijinit financiar, tehnic sau material și a facilitat „Operation Cloud Hopper”, o serie de atacuri cibernetice având efecte importante, a căror origine se situează în afara Uniunii și care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre, precum și atacuri cibernetice având efecte importante asupra unor state terțe. „Operation Cloud Hopper” a vizat sistemele de informații ale unor întreprinderi multinaționale de pe șase continente, inclusiv ale unor întreprinderi situate în Uniune, și a dobândit acces neautorizat la date sensibile din punct de vedere comercial, ceea ce a provocat pierderi economice importante. Actorul cunoscut în mod public sub numele de „APT10” („Advanced Persistent Threat 10”) (*alias „*Red Apollo”, „CVNX”, „Stone Panda”, „MenuPass” și «Potassium») a desfășurat «Operation Cloud Hopper». Poate fi stabilită o legătură între Huaying Haitai și APT10. În plus, Gao Qiang și Zhang Shilong, ambii desemnați în legătură cu „Operation Cloud Hopper”, au fost angajați ai Huaying Haitai. Prin urmare, Huaying Haitai este, de asemenea, asociată cu Gao Qiang și Zhang Shilong	UE – 30.07.2020 RM – 13.06.2023
2.	Chosun Expo	*alias* Chosen Expo; Korea Export Joint Venture Locație RPDC	Chosun Expo a oferit sprijin financiar, tehnic sau material și a facilitat o serie de atacuri cibernetice având efecte importante, a căror origine se situează în afara Uniunii și care au constituit	UE – 30.07.2020 RM – 13.06.2023

			o amenințare externă la adresa Uniunii sau a statelor sale membre, și în atacuri cibernetice având efecte importante asupra unor state terțe, inclusiv atacurile cibernetice cunoscute sub numele de „WannaCry” și atacurile cibernetice împotriva Autorității de supraveghere financiară din Polonia și împotriva Sony Pictures Entertainment, precum și furtul cibernetic de la Bangladesh Bank și tentativa de furt cibernetic de la Vietnam Tien Phong Bank. „WannaCry” a perturbat sistemele de informații din întreaga lume prin vizarea sistemelor de informații cu programe de tip ransomware și prin blocarea accesului la date. A afectat sistemele de informații ale întreprinderilor din Uniune, inclusiv sistemele de informații referitoare la serviciile necesare pentru menținerea serviciilor esențiale și a activităților economice din statele membre. Atacul „WannaCry” a fost comis de actorul cunoscut în mod public sub numele de «APT38 („Advanced Persistent Threat 38”) sau „Lazarus Group”. Se poate stabili o legătură între Chosun Expo și APT38/Lazarus Group, inclusiv prin intermediul conturilor utilizate pentru atacurile cibernetice	
3.	Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) [Centrul principal pentru	Adresă: 22 Kirova Street, Moscow, Russian Federation (str. Kirova nr. 22, Moscova, Federația Rusă)	Centrul principal pentru tehnologii speciale (GTsST) al Direcției principale a Statului-Major al forțelor armate ruse (GU/GRU), cunoscut și prin codul său poștal de teren 74455, este implicat într-o serie de atacuri cibernetice având efecte importante, a căror origine se situează în afara Uniunii și care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre, și în atacuri cibernetice având efecte importante asupra unor state terțe, inclusiv atacurile cibernetice cunoscute în mod public sub numele „NotPetya” sau „EternalPetya” din iunie 2017 și atacurile cibernetice îndreptate împotriva unui sistem electroenergetic ucrainean din iarna anilor 2015 și 2016. „NotPetya” sau „EternalPetya” a blocat accesul la date în mai multe întreprinderi din Uniune, din Europa în ansamblu și din	UE – 30.07.2020 RM – 13.06.2023

	tehnologii speciale (GTsST) al Direcției principale a Statului-Major al forțelor armate ruse (GU/GRU)]		întreaga lume, prin vizarea computerelor prin programe de tip ransomware și prin blocarea accesului la date, ceea ce a dus, printre altele, la pierderi economice importante. Atacul cibernetic asupra unui sistem electroenergetic ucrainean a condus la întreruperea unor porțiuni ale acestuia în timpul iernii. Actorul cunoscut în mod public sub numele de „Sandworm” (*alias*„Sandworm Team”, „BlackEnergy Group”, „Voodoo Bear”, „Quedagh”, „Olympic Destroyer” și „Telebots”), aflat, de asemenea, în spatele atacului asupra sistemului electroenergetic ucrainean, a comis atacul „NotPetya” sau „EternalPetya”. Sandworm a desfășurat atacuri cibernetice împotriva Ucrainei, inclusiv asupra agențiilor guvernamentale ucrainene și asupra infrastructurii critice ucrainene, în urma războiului de agresiune al Rusiei împotriva Ucrainei. Printre respectivele atacuri cibernetice se numără campanii de spear-phishing, atacuri de tip malware și ransomware. Centrul principal pentru tehnologii speciale al Direcției principale a Statului-Major al forțelor armate ruse din Federația Rusă are un rol activ în activitățile cibernetice desfășurate de Sandworm și poate fi stabilită o legătură între centru și acesta	
4.	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) [Cel de al 85-lea Centru principal	Adresă: Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation (Komsomol'ski Prospekt, 20, Moscova, 119146, Federația Rusă)	Cel de-al 85-lea Centru principal de servicii speciale (GTsSS) din cadrul Direcției principale a Statului-Major al forțelor armate al Federației Ruse (GU/GRU) (*alias* „unitatea militară 26165”, „APT28”, „Fancy Bear”, „Sofacy Group”, „Pawn Storm” și „Strontium”) este implicat în atacuri cibernetice cu efecte semnificative care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre și în atacuri cibernetice cu efecte semnificative împotriva unor state terțe. În special, ofițerii serviciului militar de informații al GTsSS au luat parte la atacul cibernetic împotriva parlamentului federal german (Deutscher Bundestag) în aprilie și mai 2015, precum și la tentativa de atac cibernetic din aprilie 2018 care a avut	UE – 22.10.2020 RM – 13.06.2023

	de servicii speciale (GTsSS) din cadrul Direcției principale a Statului-Major al forțelor armate al Federației Ruse (GU/GRU)]		drept scop piratarea rețelei Wi Fi a Organizației pentru Interzicerea Armelor Chimice (OIAC) din Țările de Jos. Atacul cibernetic împotriva parlamentului federal german a fost îndreptat împotriva sistemului informatic al acestuia, căruia i-a afectat funcționarea timp de mai multe zile. A fost furat un volum important de date și au fost afectate conturile de e-mail ale mai multor parlamentari, precum și cel al fostului cancelar Angela Merkel. În urma războiului de agresiune al Rusiei împotriva Ucrainei, au fost comise atacuri cibernetice împotriva Ucrainei de către GTsSS (atacuri de tip spear-phishing și atacuri malware)	
5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (ortografia chineză) Alias:Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Adresa: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, China Locul înregistrării: Beijing, China Data înregistrării: 2.9.2010 Codul unificat de credit social: 91110108562135265P	Integrity Technology Group este o întreprindere din domeniul securității cibernetice, cu sediul în Republica Populară Chineză (RPC), care a facilitat atacuri cibernetice legate de Advanced Persistent Threat – (APT) Flax Typhoon. Respectiva APT a utilizat produsele și tehnologia Integrity Technology Group pentru a-și desfășura activitățile de exploatare a rețelelor informatice. De atunci, produsele Integrity Technology Group au fost utilizate pentru a compromite și a accesa dispozitive din internetul obiectelor în statele membre, cât și în țări din întreaga Europă și la nivel global. Între 2022 și 2023, Flax Typhoon a accesat cel puțin 65 600 de dispozitive din internetul obiectelor în șase state membre prin utilizarea produselor Integrity Technology Group. Prin urmare, produsele comerciale și infrastructura Integrity Technology Group au fost utilizate în mod curent în atacurile cibernetice împotriva statelor membre, precum și a statelor terțe. În consecință, prin afectarea sistemelor informatice legate de infrastructura digitală, Integrity Technology Group oferă sprijin tehnic și material pentru atacurile cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa statelor membre și a statelor terțe	UE – 16.03.2026 RM – 23.04.2026
6.	Emennet Pasargad	Alias: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Locul înregistrării: Teheran, Iran	Emennet Pasargad este un actor cibernetic iranian (societate) care a vizat numeroase entități, în special în statele membre, precum și în Statele Unite (SUA). Emennet Pasargad, care acționează sub denumirea «Anzu Team»,	UE – 16.03.2026 RM –23.04.2026

		Număr de înregistrare: 554267 Locul principal de desfășurare a activității: Teheran, Iran	a vizat infrastructura digitală din Suedia și a compromis un serviciu SMS suedez, afectând un număr mare de persoane. În plus, acționând sub denumirea «Holy Souls», entitatea a compromis baza de date a abonaților revistei satirice franceze Charlie Hebdo și a oferit-o spre vânzare pe dark web. Emennet Pasargard a compromis panourile publicitare în timpul Jocurilor Olimpice de la Paris și a afișat campanii de dezinformare. Emennet Pasargad a încercat, de asemenea, să intervină în alegerile prezidențiale din SUA în 2020, amenințând democrația și statul de drept, obținând informații confidențiale despre alegătorii americani și obținând acces neautorizat la rețeaua informatică a unei societăți mass-media din SUA. Prin urmare, Emennet Pasargad este responsabil de atacuri cibernetice cu efecte semnificative care reprezintă o amenințare externă la adresa statelor membre, precum și de atacuri cibernetice cu efecte semnificative împotriva unui stat terț	
7.	Anxun Information Technology Co. Ltd.	安洵信息技术有限公司 (ortografia chineză) Alias: i-Soon Adresa: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai Codul unificat de credit social: 91510105332025597A (sucursala din Sichuan) Codul unificat de credit social: 91310116561906136G (sucursala din Shanghai) Site web: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Numere de telefon: +862161119992,+8605645893417, +8613761671735, +864000665915 E-mail: shutdown@163.com,	Anxun Information Technology Co. Ltd. este o societate cu sediul în Republica Populară Chineză care oferă servicii de tip «hacking-for-hire». Aceasta a vizat infrastructura critică și funcțiile critice ale statului din statele membre și a accesat și vândut informații clasificate. În plus, Anxun Information Technology Co. Ltd. a atacat guverne din diferite state terțe, ceea ce reprezintă o amenințare la adresa obiectivelor Uniunii în materie de politică externă și de securitate comună (PESC), astfel cum se prevede la articolul 21 alineatul (2) literele (a)-(c) din Tratatul privind Uniunea Europeană. Anxun Information Technology Co. Ltd. obține un beneficiu economic important din serviciile furnizate. Prin urmare, Anxun Information Technology Co. Ltd. este responsabilă de atacuri cibernetice cu efecte semnificative care reprezintă o amenințare externă la adresa statelor membre, precum și de atacuri cibernetice cu efecte semnificative împotriva unor state terțe	UE - 16.03.2026 RM - 23.04.2026

		isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net		
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	UE – 13.07.2026 RM - 28.08.2026
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	UE – 13.07.2026 RM - 28.08.2026

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 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	«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. 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	UE – 13.07.2026 RM - 28.08.2026
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 Reborn* (Armata cibernetică a Rusiei renăscute)/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	UE – 13.07.2026 RM - 28.08.2026”.