►B

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

(JO L 129I, 17.5.2019, p. 1)

Astfel cum a fost modificat prin:

		Jurnalul Oficial		
		NR.	Pagina	Data
►M1	Regulamentul de punere în aplicare (UE) 2020/1125 al Consiliului din 30 iulie 2020	L 246	4	30.7.2020
►M2	Regulamentul de punere în aplicare (UE) 2020/1536 al Consiliului din 22 octombrie 2020	L 351 I	1	22.10.2020
►M3	Regulamentul de punere în aplicare (UE) 2020/1744 al Consiliului din 20 noiembrie 2020	L 393	1	23.11.2020
►M4	Regulamentul de punere în aplicare (UE) 2022/595 al Comisiei din 11 aprilie 2022	L 114	60	12.4.2022
►M5	Regulamentul (UE) 2023/2694 al Consiliului din 27 noiembrie 2023	L 2694	1	28.11.2023
►M6	Regulamentul de punere în aplicare (UE) 2024/1390 al Consiliului din 17 mai 2024	L 1390	1	17.5.2024

rectificat prin:

►C1 Rectificare, JO L 230, 17.7.2020, p. 37 (2019/796)

▼B

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

Articolul 1

(1) Prezentul regulament se aplică atacurilor cibernetice care au efecte semnificative, inclusiv tentativelor de atacuri cibernetice care au un efect potențial semnificativ, care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.

(2) Printre atacurile cibernetice care constituie o amenințare externă se numără cele care:

(a) provin sau sunt efectuate din exteriorul Uniunii;

(b) utilizează infrastructură din exteriorul Uniunii;

(c) sunt efectuate de orice persoană fizică sau juridică, entitate sau organism stabilit în exteriorul Uniunii sau care își desfășoară activitatea în exteriorul acesteia; sau

(d) sunt efectuate cu sprijinul, sub conducerea sau sub controlul oricărei persoane fizice sau juridice, al oricărei entități sau al oricărui organism care își desfășoară activitatea în exteriorul Uniunii.

(3) În acest scop, atacurile cibernetice constituie acțiuni care implică oricare dintre următoarele:

(a) accesarea de sisteme de informații;

(b) interferența cu sisteme de informații;

(c) interferența cu date; sau

(d) interceptarea de date,

în cazul în care aceste acțiuni nu sunt autorizate în mod corespunzător de către proprietar sau de către alt titular de drepturi asupra sistemului sau datelor ori asupra unor părți ale acestora sau nu sunt permise în temeiul dreptului Uniunii sau al legislației statului membru în cauză.

(4) Printre atacurile cibernetice care constituie o amenințare pentru statele membre se numără cele care afectează sistemele informatice legate, printre altele, de:

(a) infrastructura critică, inclusiv cablurile submarine și obiectele lansate în spațiul cosmic, care sunt esențiale pentru menținerea funcțiilor vitale ale societății sau pentru sănătatea, siguranța, securitatea și bunăstarea economică sau socială a oamenilor;

(b) serviciile necesare pentru menținerea unor activități sociale și/sau economice esențiale, în special în sectoare precum energia (electricitate, petrol și gaze); transporturile (aerian, feroviar, pe apă și rutier); bancar; infrastructurile pieței financiare; sănătatea (furnizori de asistență medicală, spitale și clinici private); furnizarea și distribuirea de apă potabilă; infrastructura digitală; precum și în orice alt sector care este esențial pentru statul membru în cauză;

▼B

(c) funcţii critice ale statului, în special în domeniile apărării, al guvernanţei și al funcţionării instituţiilor, inclusiv în ceea ce privește alegerile publice sau procesul de votare, al funcţionării infrastructurii economice și civile, al securităţii interne și al relaţiilor externe, inclusiv prin misiuni diplomatice;

(d) stocarea sau prelucrarea de informaţii clasificate; sau

(e) echipe guvernamentale de răspuns la situaţii de urgenţă.

(5) Atacurile cibernetice care constituie o ameninţare pentru Uniune le includ pe cele efectuate împotriva instituţiilor, organelor, oficiilor și agenţiilor acesteia, a delegaţiilor sale în ţări terţe sau la organizaţii internaţionale, a operaţiilor și misiunilor din cadrul politicii de securitate și apărare comune (PSAC) și a reprezentanţilor speciali ai acesteia.

(6) Măsurile restrictive prevăzute de prezentul regulament pot fi de asemenea aplicate ca răspuns la atacuri cibernetice cu efecte semnificative asupra unor state terţe sau organizaţii internaţionale, în cazul în care se consideră că acest lucru este necesar pentru realizarea obiectivelor din cadrul politicii externe și de securitate comună (PESC) din dispoziţiile relevante prevăzute la articolul 21 din Tratatul privind Uniunea Europeană.

(7) În sensul prezentului regulament, se aplică următoarele definiţii:

(a) „sisteme de informaţii” înseamnă un dispozitiv sau un grup de dispozitive interconectate sau omoloage, dintre care unul sau mai multe asigură, prin intermediul unui program, prelucrarea automată a datelor digitale, precum și a datelor digitale stocate, prelucrate, extrase sau transmise de dispozitivul sau grupul de dispozitive respectiv în vederea exploatării, a utilizării, a protecţiei și a întreţinerii lor;

(b) „interferenţă cu un sistem informatic” înseamnă obstrucţionarea funcţionării sau întreruperea funcţionării unui sistem de informaţii prin introducerea de date digitale, prin transmiterea, afectarea, ștergerea, deteriorarea, modificarea sau suprimarea unor astfel de date ori prin transformarea acestora în date inaccesibile;

(c) „interferenţă cu date” înseamnă ștergerea, afectarea, deteriorarea, modificarea sau suprimarea de date digitale într-un sistem informatic sau transformarea acestora în date inaccesibile; se încadrează aici și furtul de date, de fonduri, de resurse economice sau de proprietate intelectuală;

(d) „interceptare de date” înseamnă interceptarea, prin mijloace tehnice, a transmiterilor de date digitale care nu sunt publice, de la un sistem informatic la altul sau în cadrul aceluiași sistem informatic, inclusiv a emisiilor electromagnetice provenite de la un sistem informatic care transmite astfel de date digitale.

(8) În sensul prezentului regulament, se aplică următoarele definiţii suplimentare:

(a) „cerere” înseamnă orice cerere, contencioasă sau necontencioasă, introdusă anterior sau ulterior datei intrării în vigoare a prezentului regulament în temeiul unui contract sau al unei tranzacţii sau în legătură cu un contract sau cu o tranzacţie și include în special:

(i) o cerere de executare a unei obligaţii care rezultă în temeiul unui contract sau al unei tranzacţii ori în legătură cu un contract sau cu o tranzacţie;

(ii) o cerere de prelungire sau de plată a unei obligaţiuni, a unei garanţii financiare ori a unei indemnizaţii, indiferent de forma acesteia;

(iii) o cerere de acordare de despăgubiri în temeiul unui contract sau al unei tranzacţii;

(iv) o cerere reconvenţională;

▼B

(v) o cerere de recunoaștere sau de executare, inclusiv prin procedura de *exequatur*, a unei hotărâri judecătorești, a unei hotărâri arbitrale sau a unei hotărâri echivalente, indiferent de locul unde a fost pronunțată;

(b) „contract sau tranzacție” înseamnă orice tranzacţie, indiferent de formă și de legislația aplicabilă, care include unul sau mai multe contracte ori obligaţii similare stabilite între aceleași părți sau între părți diferite; în acest scop, termenul „contract” include orice obligaţiune, garanţie sau indemnizaţie, în special orice garanţie financiară sau indemnizaţie financiară, și orice credit, indiferent dacă este sau nu independent din punct de vedere juridic, precum și orice clauză conexă care rezultă din tranzacția respectivă sau care are legătură cu aceasta;

(c) „autorități competente” înseamnă autoritățile competente ale statelor membre, astfel cum sunt identificate pe site-urile web care figurează în anexa II;

(d) „resurse economice” înseamnă activele de orice fel, corporale sau necorporale, mobiliare sau imobiliare, care nu sunt fonduri, dar pot fi utilizate pentru obţinerea de fonduri, bunuri sau servicii;

(e) „înghețarea resurselor economice” înseamnă împiedicarea utilizării resurselor economice pentru obținerea în orice mod de fonduri, bunuri sau servicii, inclusiv, dar nu exclusiv, prin vânzarea, închirierea sau ipotecarea acestora;

(f) „înghețarea fondurilor” înseamnă împiedicarea oricărui tip de circulație, transfer, modificare, utilizare, accesare sau tranzacționare de fonduri care ar avea drept rezultat orice modificare a volumului, a cuantumului, a locației, a proprietății, a posesiei, a naturii sau a destinației acestora, sau orice altă modificare care ar permite utilizarea fondurilor, inclusiv administrarea portofoliilor;

(g) „fonduri” înseamnă activele financiare și beneficiile de orice natură, inclusiv, dar fără a se limita la:

(i) numerar, cecuri, creanțe în numerar, cambii, ordine de plată și alte instrumente de plată;

(ii) depozite la instituții financiare sau la alte entități, solduri de conturi, creanțe și titluri de creanță;

(iii) titluri de valoare și instrumente de datorie, inclusiv titluri și acțiuni, certificate reprezentând titluri de valoare, obligațiuni, bilete la ordin, warante, obligațiuni negarantate și contracte derivate, tranzacționate în mod public și privat;

(iv) dobânzi, dividende sau alte venituri din active sau plusvalori percepute pe active sau generate de acestea;

(v) credite, drepturi compensatorii, garanții, garanții de bună execuție sau alte angajamente financiare;

(vi) acreditive, conosamente și contracte de vânzare; și

(vii) documente care atestă deținerea de cote-părți dintr-un fond sau din resurse financiare;

▼B

(h) „teritoriul Uniunii” înseamnă teritoriile statelor membre cărora li se aplică tratatul, în condiţiile prevăzute de acesta, inclusiv spaţiul lor aerian.

Articolul 2

Factorii care determină dacă un atac cibernetic are efecte semnificative, astfel cum se menţionează la articolul 1 alineatul (1), includ oricare dintre următoarele:

(a) domeniul de aplicare, amploarea, impactul sau gravitatea perturbării cauzate, inclusiv în ceea ce privește activităţile economice și societale, serviciile esenţiale, funcţiile critice ale statului, ordinea publică sau siguranţa publică;

(b) numărul persoanelor fizice sau juridice, a entităţilor sau a organismelor afectate;

(c) numărul statelor membre afectate;

(d) valoarea prejudiciilor economice cauzate de exemplu de furtul de mari dimensiuni de fonduri, de resurse economice sau de proprietate intelectuală;

(e) beneficiile economice obţinute de către autor, pentru sine sau pentru alţii;

(f) volumul sau natura datelor furate sau amploarea încălcării securităţii datelor, sau

(g) natura datelor sensibile din punct de vedere comercial accesate.

Articolul 3

(1) Se îngheaţă toate fondurile și resursele economice care aparţin, se află în proprietatea, sunt deţinute sau sunt controlate de oricare dintre persoanele fizice sau juridice, entităţile sau organismele care figurează în anexa I.

(2) Se interzice punerea la dispoziţie de fonduri sau resurse economice, direct sau indirect, în beneficiul persoanelor fizice sau juridice, entităţilor sau organismelor incluse în lista din anexa I.

(3) Anexa I include, astfel cum s-a identificat de Consiliu în conformitate cu articolul 5 alineatul (1) din Decizia (PESC) 2019/797:

(a) persoanele fizice sau juridice, entităţile sau organismele care sunt responsabile de atacuri cibernetice sau tentative de atacuri cibernetice;

(b) persoanele fizice sau juridice, entităţi sau organisme care furnizează sprijin financiar, tehnic sau material pentru atacuri cibernetice sau tentative de atacuri cibernetice sau care sunt implicate în alt mod în acestea, inclusiv prin planificarea sau pregătirea lor, participarea la ele, conducerea lor, oferirea de asistenţă pentru ele sau încurajarea lor ori facilitarea lor fie prin acţiune, fie prin omisiune;

(c) persoanele fizice sau juridice, entităţile sau organismele asociate cu persoanele fizice sau juridice, cu entităţile sau cu organismele menţionate la literele (a) și (b) din prezentul alineat.

▼B

Articolul 4

(1) Prin derogare de la articolul 3, autorităţile competente ale statelor membre pot autoriza deblocarea anumitor fonduri sau resurse economice îngheţate sau punerea la dispoziţie a anumitor fonduri sau resurse economice, în condiţiile pe care le consideră adecvate, după ce au stabilit că fondurile sau resursele economice în cauză:

(a) ►C1 sunt necesare pentru satisfacerea necesităţilor de bază ale persoanelor fizice sau juridice, ale entităţilor sau organismelor care figurează în anexa I ◄ și ale membrilor de familie care se află în întreţinerea respectivelor persoane fizice, inclusiv plăţile necesare pentru achitarea unor cheltuieli legate de alimente, chirie sau rate ipotecare, medicamente și tratamente medicale, impozite și taxe, prime de asigurare și servicii de utilităţi publice;

(b) sunt destinate exclusiv plăţii unor onorarii rezonabile sau rambursării cheltuielilor legate de prestarea unor servicii juridice;

(c) sunt destinate exclusiv plăţii comisioanelor sau a cheltuielilor corespunzătoare păstrării sau administrării curente a fondurilor sau a resurselor economice îngheţate;

(d) sunt necesare pentru cheltuieli extraordinare, cu condiţia ca autoritatea competentă relevantă să fi notificat autorităţilor competente ale celorlalte state membre și Comisiei, cu cel puţin două săptămâni înainte de acordarea autorizaţiei respective, motivele pentru care consideră că ar trebui acordată o autorizaţie în cazul în speţă; sau

(e) urmează să fie plătite în sau dintr-un cont al unei misiuni diplomatice sau consulare ori al unei organizaţii internaţionale care beneficiază de imunităţi în conformitate cu dreptul internaţional, în măsura în care astfel de plăţi sunt destinate a fi utilizate în scopuri oficiale ale misiunii diplomatice sau consulare ori ale organizaţiei internaţionale respective.

(2) Statul membru în cauză informează în termen de două săptămâni celelalte state membre și Comisia atunci când acordă o autorizaţie în temeiul alineatului (1).

▼M5

Articolul 4a

(1) Articolul 3 alineatele (1) și (2) nu se aplică punerii la dispoziţie a fondurilor sau resurselor economice necesare pentru a asigura furnizarea cu promptitudine a asistenţei umanitare sau a sprijini alte activităţi care răspund unor nevoi umane de bază, atunci când asistenţa și celelalte activităţi sunt desfășurate de:

(a) Organizaţia Naţiunilor Unite (ONU), inclusiv programele, fondurile și alte entităţi și organisme ale acesteia, precum și agenţiile sale specializate și organizaţiile conexe;

(b) organizaţii internaţionale;

(c) organizaţii umanitare cu statut de observator în cadrul Adunării Generale a ONU și membri ai respectivelor organizaţii umanitare;

(d) organizaţiile neguvernamentale finanţate bilateral sau multilateral care participă la planurile de răspuns umanitar ale ONU, la planurile de răspuns pentru refugiaţi, la alte apeluri sau clustere umanitare ale ONU coordonate de Oficiul ONU pentru Coordonarea Afacerilor Umanitare;

▼M5

(e) organizaţii și agenţii cărora Uniunea le-a acordat certificatul de parteneriat umanitar sau care sunt certificate sau recunoscute de un stat membru în conformitate cu procedurile naţionale;

(f) agenţii specializate ale statelor membre; sau

(g) angajaţii, beneficiarii de granturi, filialele sau partenerii de implementare ai entităţilor menţionate la literele (a)-(f) atunci când și în măsura în care aceștia acţionează în calităţile respective.

(2) Fără a aduce atingere alineatului (1) și prin derogare de la articolul 3 alineatele (1) și (2), autorităţile competente ale statelor membre pot autoriza deblocarea anumitor fonduri sau resurse economice îngheţate ori punerea la dispoziţie a anumitor fonduri sau resurse economice, în condiţiile pe care le consideră adecvate, după ce au stabilit că furnizarea respectivelor fonduri sau resurse economice este necesară pentru a asigura acordarea cu promptitudine a asistenţei umanitare sau a sprijini alte activităţi care răspund unor nevoi umane de bază.

(3) În absenţa unei decizii negative, a unei cereri de informaţii sau a unei notificări privind necesitatea unei perioade de timp suplimentare din partea autorităţii competente relevante în termen de cinci zile lucrătoare de la data primirii unei cereri de autorizare în temeiul alineatului (2), se consideră că respectiva autorizaţie a fost acordată.

(4) Statul membru în cauză informează celelalte state membre și Comisia cu privire la orice autorizaţie acordată în temeiul alineatelor (2) și (3) în termen de patru săptămâni de la o astfel de autorizare.

▼B

Articolul 5

(1) Prin derogare de la articolul 3 alineatul (1), autorităţile competente ale statelor membre pot autoriza deblocarea anumitor fonduri sau resurse economice îngheţate dacă sunt îndeplinite următoarele condiţii:

(a) fondurile sau resursele economice fac obiectul unei hotărâri arbitrale pronunţate anterior datei la care persoana fizică sau juridică, entitatea sau organismul menţionat la articolul 3 a fost inclus pe lista din anexa I, al unei hotărâri judecătorești ori al unei decizii administrative pronunţate în Uniune sau al unei hotărâri judecătorești executorii în statul membru în cauză, anterior sau ulterior datei respective;

(b) fondurile sau resursele economice vor fi utilizate exclusiv pentru a satisface cererile garantate printr-o astfel de hotărâre sau decizie ori a căror valabilitate este recunoscută printr-o astfel de hotărâre sau decizie, în limitele stabilite de actele cu putere de lege și de normele administrative aplicabile ce reglementează drepturile persoanelor care formulează astfel de cereri;

(c) hotărârea sau decizia nu este în beneficiul unei persoane fizice sau juridice, al unei entităţi sau al unui organism care figurează în anexa I; și

(d) recunoașterea hotărârii sau deciziei nu contravine ordinii publice din statul membru respectiv.

▼B

(2) Statul membru în cauză informează în termen de două săptămâni celelalte state membre și Comisia atunci când acordă o autorizaţie în temeiul alineatului (1).

Articolul 6

(1) Prin derogare de la articolul 3 alineatul (1), în cazul în care o persoană fizică sau juridică, o entitate sau un organism inclus pe lista din anexa I trebuie să efectueze o plată în baza unui contract sau a unui acord încheiat de persoana fizică sau juridică, entitatea sau organismul în cauză sau în baza unei obligaţii care a apărut în sarcina persoanei fizice sau juridice, a entităţii sau a organismului în cauză anterior datei la care persoana fizică sau juridică, entitatea sau organismul respectiv a fost inclus pe lista din anexa I, autorităţile competente ale statelor membre pot autoriza, în condiţiile pe care le consideră adecvate, deblocarea anumitor fonduri sau resurse economice îngheţate, cu condiţia ca autoritatea competentă în cauză să fi stabilit că:

(a) fondurile sau resursele economice vor fi utilizate pentru efectuarea unei plăţi de către o persoană fizică sau juridică, entitate sau organism care figurează în anexa I; și

(b) plata nu încalcă dispoziţiile articolului 3 alineatul (2).

(2) Statul membru în cauză informează în termen de două săptămâni celelalte state membre și Comisia atunci când acordă o autorizaţie în temeiul alineatului (1).

Articolul 7

(1) Articolul 3 alineatul (2) nu împiedică creditarea conturilor îngheţate de către instituţiile financiare sau de credit care primesc fonduri transferate de terţi în contul persoanei fizice sau juridice, al entităţii sau al organismului inclus pe listă, cu condiţia ca toate aceste sume care sunt transferate în conturile respective să fie, de asemenea, îngheţate. Instituţia financiară sau de credit informează, fără întârziere, autoritatea competentă relevantă cu privire la orice tranzacţii de acest tip.

(2) Articolul 3 alineatul (2) nu se aplică sumelor vărsate în conturile îngheţate care reprezintă:

(a) dobânzi sau alte venituri generate de conturile respective;

(b) plăţi cuvenite în baza unor contracte, acorduri sau obligaţii care au fost încheiate sau au survenit anterior date la care persoana fizică sau juridică, entitatea sau organismul menţionat la articolul 3 alineatul (1) a fost inclus pe lista din anexa I; sau

(c) plăţi cuvenite în temeiul unor hotărâri judecătorești, decizii administrative sau hotărâri arbitrale pronunţate într-un stat membru sau care sunt executorii în statul membru respectiv,

cu condiţia ca orice astfel de dobânzi, alte venituri și plăţi să rămână sub incidenţa măsurilor prevăzute la articolul 3 alineatul (1).

Articolul 8

(1) Fără a aduce atingere normelor aplicabile în materie de raportare, confidenţialitate și secret profesional, persoanele fizice și juridice, entităţile și organismele:

▼B

(a) furnizează de îndată autorității competente a statului membru în care își au reședința sau sunt stabilite toate informațiile care pot facilita respectarea prezentului regulament, în special cu privire la conturile și sumele înghețate în temeiul articolului 3 alineatul (1), și transmit aceste informații Comisiei, direct sau prin intermediul statului membru în cauză; și

(b) cooperează cu autoritatea competentă în privința oricărei verificări a informațiilor menționate la litera (a).

(2) Orice informații suplimentare primite direct de Comisie se comunică statelor membre.

(3) Orice informații furnizate sau primite în conformitate cu prezentul articol se utilizează exclusiv în scopul pentru care au fost furnizate sau primite.

Articolul 9

Este interzisă participarea în cunoștință de cauză și deliberată la activități care au drept scop sau efect eludarea măsurilor menționate la articolul 3.

Articolul 10

(1) Înghețarea fondurilor și a resurselor economice sau refuzul de a pune la dispoziție aceste fonduri sau resurse economice, cu bună-credință, pe motiv că o astfel de acțiune este conformă cu dispozițiile prezentului regulament, nu angajează în niciun fel răspunderea persoanei fizice sau juridice, a entității sau a organismului care o efectuează ori a personalului de conducere sau a angajaților acestora, cu excepția cazului în care se dovedește că fondurile și resursele economice în cauză au fost înghețate sau reținute din neglijență.

(2) Acțiunile întreprinse de persoane fizice sau juridice, de entități sau de organisme nu angajează în niciun fel răspunderea acestora în cazul în care nu au știut și nu au avut niciun motiv întemeiat să suspecteze că acțiunile lor ar încălca măsurile prevăzute în prezentul regulament.

Articolul 11

(1) Nu se dă curs niciunei cereri legate de orice contract sau tranzacție a cărei executare a fost afectată, în mod direct sau indirect, în totalitate sau parțial, de măsurile impuse în temeiul prezentului regulament, inclusiv cererilor de despăgubire sau oricărei alte cereri de acest tip, cum ar fi cererile de compensare sau cele de chemare în garanție, mai ales 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:

(a) persoanele fizice sau juridice, entitățile sau organismele desemnate, care figurează în anexa I;

(b) orice persoană fizică sau juridică, entitate sau organism care acționează prin intermediul sau în numele uneia dintre persoanele fizice sau juridice, entitățile sau organismele menționate la litera (a).

(2) În cadrul oricărei proceduri de executare a unei cereri, sarcina de a dovedi că satisfacerea cererii nu este interzisă în temeiul alineatului (1) incumbă persoanei fizice sau juridice, entității sau organismului care solicită executarea respectivei cereri.

(3) Prezentul articol nu aduce atingere dreptului persoanelor fizice sau juridice, al entităților sau al organismelor menționate la alineatul (1) la controlul jurisdicțional al legalității neexecutării obligațiilor contractuale în conformitate cu prezentul regulament.

▼B

Articolul 12

(1) Comisia și statele membre se informează reciproc cu privire la măsurile luate în temeiul prezentului regulament și fac schimb de orice alte informaţii relevante de care dispun în legătură cu prezentul regulament, în special de informaţii cu privire la:

(a) fondurile îngheţate în temeiul articolului 3 și la autorizaţiile acordate în temeiul articolelor 4, 5 și 6;

(b) aspectele referitoare la încălcări și de executare și la hotărârile pronunţate de instanţele naţionale.

(2) Statele membre se informează reciproc și informează Comisia imediat cu privire la orice alte informaţii relevante de care dispun care ar putea afecta punerea în aplicare efectivă a prezentului regulament.

Articolul 13

(1) În cazul în care decide să aplice măsurile menţionate la articolul 3 unei persoane fizice sau juridice, unei entităţi sau unui organism, Consiliul modifică anexa I în consecinţă.

(2) Consiliul comunică decizia menţionată la alineatul (1), inclusiv motivele includerii pe listă, persoanei fizice sau juridice, entităţii sau organismului vizat(e), fie direct, dacă adresa este cunoscută, fie prin publicarea unui anunţ, oferind persoanei fizice sau juridice, entităţii sau organismului în cauză posibilitatea de a formula observaţii.

(3) În cazul în care se transmit observaţii sau se prezintă dovezi substanţiale noi, Consiliul își reexaminează decizia menţionată la alineatul (1) și informează în consecinţă persoana fizică sau juridică, entitatea sau organismul vizat(ă).

(4) Lista din anexa I se revizuiește periodic și cel puţin la fiecare 12 luni.

(5) Comisia este împuternicită să modifice anexa II pe baza informaţiilor furnizate de statele membre.

Articolul 14

(1) Anexa I cuprinde motivele includerii pe listă a persoanelor fizice sau juridice, a entităţilor sau a organismelor vizate.

(2) Anexa I conţine, dacă sunt disponibile, informaţiile care sunt necesare pentru identificarea persoanelor fizice sau juridice, a entităţilor sau a organismelor în cauză. În ceea ce privește persoanele fizice, astfel de informaţii pot include numele și pseudonimele, data și locul nașterii, cetăţenia, numărul de pașaport și de carte de identitate, sexul, adresa (dacă este cunoscută) și funcţia sau profesia. În ceea ce privește persoanele juridice, entităţile sau organismele, astfel de informaţii pot cuprinde denumirea, locul și data înregistrării, numărul de înregistrare și sediul.

Articolul 15

(1) Statele membre stabilesc normele privind sancţiunile aplicabile în cazul încălcării dispoziţiilor prezentului regulament și iau toate măsurile necesare pentru a asigura punerea în aplicare a acestora. Sancţiunile prevăzute sunt eficace, proporţionale și descurajante.

▼B

(2) După intrarea în vigoare a prezentului regulament, statele membre notifică fără întârziere Comisiei normele menţionate la alineatul (1), precum și toate modificările ulterioare aduse acestora.

Articolul 16

(1) Comisia prelucrează datele cu caracter personal în scopul de a-și exercita atribuţiile conferite în temeiul prezentului regulament. Aceste atribuţii includ:

(a) adăugarea conţinutului anexei I la lista consolidată, în format electronic, a persoanelor, a grupurilor și a entităţilor care fac obiectul sancţiunilor financiare ale Uniunii și în harta interactivă a sancţiunilor, ambele fiind disponibile public;

(b) prelucrarea informaţiilor privind impactul măsurilor prevăzute în prezentul regulament, precum valoarea fondurilor îngheţate, și a informaţiilor privind autorizaţiile acordate de autorităţile competente.

(2) În scopul aplicării prezentului regulament, serviciul din cadrul Comisiei prevăzut în anexa II este desemnat ca „operator” al Comisiei în sensul articolului 3 alineatul (8) din Regulamentul (UE) 2018/1725, pentru a asigura faptul că persoanele fizice în cauză își pot exercita drepturile ce le revin în temeiul regulamentului menţionat.

Articolul 17

(1) Statele membre desemnează autorităţile competente menţionate în prezentul regulament și le indică pe site-urile web care figurează în anexa II. Comisiei i se notifică de către statele membre orice modificare a adreselor site-urilor lor web care figurează în anexa II.

(2) După intrarea în vigoare a prezentului regulament, statele membre notifică fără întârziere Comisiei autorităţile lor competente, inclusiv datele de contact ale acestor autorităţi competente, precum și orice modificare ulterioară adusă în privinţa acestora.

(3) În cazul în care prezentul regulament prevede o obligaţie de a notifica, a informa sau a comunica în alt mod cu Comisia, adresa și celelalte date de contact care trebuie utilizate în vederea efectuării acestei comunicări sunt cele indicate în anexa II.

Articolul 18

Prezentul regulament se aplică:

(a) pe teritoriul Uniunii, inclusiv în spaţiul său aerian;

(b) la bordul oricărei aeronave sau nave aflate sub jurisdicţia unui stat membru;

(c) oricărei persoane fizice aflate pe teritoriul sau în exteriorul teritoriului Uniunii, care este resortisant al unui stat membru;

(d) oricărei persoane juridice, entităţi sau organism aflat pe teritoriul sau în exteriorul teritoriului Uniunii care este înregistrat sau constituit în temeiul legislaţiei unui stat membru;

(e) oricărei persoane juridice, entităţi sau organism în legătură cu orice activitate desfășurată în întregime sau în parte pe teritoriul Uniunii.

▼B

Articolul 19

Prezentul regulament intră în vigoare în ziua următoare datei publicării în *Jurnalul Oficial al Uniunii Europene*.

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

▼B

ANEXA I

Lista persoanelor fizice și juridice, a entităților și a organismelor menționate la articolul 3

▼M1

A. Persoane fizice

	Nume	Informații de identificare	Motive	Data includerii pe listă
▼M3				
1.	GAO Qiang	Data nașterii: 4 octombrie 1983 Locul nașterii: Shandong Province, China Adresă: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Cetățenie: chineză Sexul: masculin	Gao Qiang este 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, 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. Actorul cunoscut în mod public sub numele de „APT10” („Advanced Persistent Threat 10”) (alias „Red. Apollo”, „CVNX”, „Stone Panda”, „MenuPass” și „Potassium”) a efectuat „Operation Cloud Hopper”. Se poate stabili o legătură între Gao Qiang și APT10, inclusiv prin asocierea acestuia cu infrastructura de comandă și control a APT10. În plus, Huaying Haitai, entitate desemnată pentru că a oferit sprijin și a facilitat „Operation Cloud Hopper”, l-a avut drept angajat pe Gao Qiang. Acesta are legături cu Zhang Shilong, desemnat la rândul său în legătură cu „Operation Cloud Hopper”. Prin urmare, Gao Qiang este asociat atât cu Huaying Haitai, cât și cu Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Data nașterii: 10 septembrie 1981 Locul nașterii: China Adresă: Hedong, Yuyang Road No 121, Tianjin, China Cetățenie: chineză Sexul: masculin	Zhang Shilong este 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, 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.	30.7.2020

▼M3

	Nume	Informaţii de identificare	Motive	Data includerii pe listă
			Actorul cunoscut în mod public sub numele de „APT10” („Advanced Persistent Threat 10”) (alias „Red. Apollo”, „CVNX”, „Stone Panda”, „MenuPass” și „Potassium”) a efectuat „Operation Cloud Hopper”. Se poate stabili o legătură între Zhang Shilong și APT10, inclusiv prin programele malware pe care acesta le-a dezvoltat și testat în legătură cu atacurile cibernetice desfășurate de APT10. În plus, Huaying Haitai, entitate desemnată pentru că a oferit sprijin și a facilitat „Operation Cloud Hopper”, l-a avut drept angajat pe Zhang Shilong. Acesta are legături cu Gao Qiang, desemnat la rândul său în legătură cu „Operation Cloud Hopper”. Prin urmare, Zhang Shilong este asociat atât cu Huaying Haitai, cât și cu Gao Qiang.	

▼M6

3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Data naşterii: 27.5.1972 Locul naşterii: Regiunea Perm, RSFS Rusă (în prezent Federaţia Rusă) Numărul paşaportului: 120017582 Eliberat de: Ministrul de Externe al Federaţiei Ruse valabil de la 17.4.2017 la 17.4.2022 Loc: Moscova, Federaţia Rusă Cetăţenia: rusă Sexul: masculin	Alexey Minin a luat parte la o tentativă de atac cibernetic care ar fi putut avea efecte importante asupra Organizaţiei pentru Interzicerea Armelor Chimice (OIAC) în Ţările de Jos și la atacuri cibernetice cu efecte semnificative asupra unor state terţe. În calitatea sa de ofiţer de sprijin specializat în informaţii din surse umane al Direcţiei principale a Statului-Major al forţelor armate ruse (GU/GRU), Alexey Minin a făcut parte dintr-o echipă formată din patru ofiţeri din serviciul militar de informaţii rus, care a încercat să obţină acces neautorizat la reţeaua Wi-Fi a OIAC de la Haga, Ţările de Jos, în aprilie 2018. Tentativa de atac cibernetic viza accesul neautorizat la reţeaua WiFi a OIAC, care, în caz de reuşită, ar fi compromis securitatea reţelei și activitatea de investigare în curs a OIAC. Serviciul de securitate, de informaţii și de apărare din Ţările 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 ofiţer al Direcţiei principale de informaţii a Rusiei (GRU), pentru piraterie informatică, fraudă cu ajutorul mijloacelor de comunicare, furt de identitate calificat și spălarea banilor.	30.7.2020”

▼M6

	Nume	Informații de identificare	Motive	Data includerii pe listă
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 care ar fi putut avea efecte importante 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 acces 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 WiFi 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 Morenets ca membru al unității militare 26165, pentru piraterie informatică, fraudă cu ajutorul mijloacelor de comunicare, furt de identitate calificat și spălarea banilor.	30.7.2020
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: Ministrul de Externe al Federației Ruse valabil de la 17.4.2017 la 17.4.2022 Loc: Moscova, Federația Rusă Cetățenia: rusă Sexul: masculin	Evgenii Serebriakov a luat parte la o tentativă de atac cibernetic care ar fi putut avea efecte importante 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), Evgenii Serebriakov a făcut parte dintr-o echipă formată din patru ofițeri din serviciul militar de informații rus, care a încercat să obțină acces 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 WiFi 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 Ucrainei.	30.7.2020

▼M6

	Nume	Informaţii de identificare	Motive	Data includerii pe listă
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Data naşterii: 24.8.1972 Locul naşterii: Ulianovsk, RSFS Rusă (în prezent, Federaţia Rusă) Numărul paşaportului: 120018866 Eliberat de: Ministrul de Externe al Federaţiei Ruse valabil de la 17.4.2017 la 17.4.2022 Loc: Moscova, Federaţia Rusă Cetăţenia: rusă Sexul: masculin	Oleg Sotnikov a luat parte la o tentativă de atac cibernetic care ar fi putut avea efecte importante asupra Organizaţiei pentru Interzicerea Armelor Chimice (OIAC) în Ţările de Jos și la atacuri cibernetice cu efecte semnificative asupra unor state terţe. În calitatea sa de ofiţer de sprijin specializat în informaţii din surse umane al Direcţiei principale a Statului-Major al forţelor armate ruse (GU/GRU), Oleg Sotnikov a făcut parte dintr-o echipă formată din patru ofiţeri din serviciul militar de informaţii rus, care a încercat să obţină acces neautorizat la reţeaua Wi-Fi a OIAC de la Haga, Ţările de Jos, în aprilie 2018. Tentativa de atac cibernetic viza accesul neautorizat la reţeaua WiFi a OIAC, care, în caz de reuşită, ar fi compromis securitatea reţelei și activitatea de investigare în curs a OIAC. Serviciul de securitate, de informaţii și de apărare din Ţările 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 l-a pus sub acuzare pe Oleg Sotnikov ca ofiţer al Direcţiei principale de informaţii a Rusiei (GRU), pentru piraterie informatică, fraudă cu ajutorul mijloacelor de comunicare, furt de identitate calificat și spălarea banilor.	30.7.2020
7.	Dmitri Sergheevici BADIN	Дмитрий Сергеевич БАДИН Data naşterii: 15.11.1990 Locul naşterii: Kursk, RSFS Rusă (în prezent, Federaţia Rusă) Cetăţenia: rusă Sexul: masculin	Dmitri Badin a luat parte la un atac cibernetic cu efecte importante împotriva parlamentului federal german (Deutscher Bundestag) și la atacuri cibernetice cu efecte semnificative asupra unor state terţe. În calitatea sa de ofiţer în serviciul militar de informaţii al celui de al 85-lea Centru principal de servicii speciale (GTsSS) din cadrul Direcţiei principale a Statului-Major al forţelor armate al Federaţiei Ruse (GU/GRU), Dmitri Badin a făcut parte dintr-o echipă de ofiţeri ai serviciului militar de informaţii 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 funcţionarea 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 unităţii militare 26165, pentru piraterie informatică, fraudă cu ajutorul mijloacelor de comunicare, furt de identitate calificat și spălarea banilor.	22.10.2020

▼M6

	Nume	Informaţii de identificare	Motive	Data includerii pe listă
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Data naşterii: 21.2.1961 Cetăţenia: rusă Sexul: masculin	Igor Kostyukov este actualul şef al Direcţiei principale a Statului-Major al forţelor armate al Federaţiei Ruse (GU/GRU), unde a ocupat anterior funcţia de prim-şef adjunct. Una dintre unităţile 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 importante care reprezintă o ameninţare externă la adresa Uniunii sau a statelor sale membre. În special, ofiţerii serviciului militar de informaţii al GTsSS au luat parte la atacul cibernetic împotriva parlamentului federal german (Deutscher Bundestag) din aprilie și mai 2015, precum și la tentativa de atac cibernetic din aprilie 2018 care a avut drept scop piratarea reţelei Wi-fi a Organizaţiei pentru Interzicerea Armelor Chimice (OIAC) din Ţările de Jos. Atacul cibernetic împotriva parlamentului federal german a fost îndreptat împotriva sistemului informatic al acestuia, căruia i-a afectat funcţionarea 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.	22.10.2020

▼M1

B. Persoane juridice, entități și organisme

	Nume	Informații de identificare	Motive	Data includerii pe listă
1.	Tianjin Huaying Haitai Science and Technology Development Co Ltd (Huaying Haitai)	Alias Haitai Technology Development Co. Ltd Localizare: Tianjin, China	Huaying Haitai a oferit sprijin 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, 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. Actorul cunoscut în mod public sub numele de «APT10» («Advanced Persistent Threat 10») (alias «Red. Apollo», «CVNX», «Stone Panda», «MenuPass» și «Potassium») a efectuat «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 asociat cu Gao Qiang și cu Zhang Shilong.	30.7.2020
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 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.	30.7.2020

▼M1

	Nume	Informații de identificare	Motive	Data includerii pe listă
			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.	

▼M6

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 tehnologii speciale (GTsST) al Direcției principale a Statului-Major al forțelor armate ruse (GU/GRU)]	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 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.	30.7.2020

▼M6

	Nume	Informații de identificare	Motive	Data includerii pe listă
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 de servicii speciale (GTsSS) din cadrul Direcției principale a Statului-Major al forțelor armate al Federației Ruse (GU/GRU)]	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 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 fostei cancelare 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).	22.10.2020

▼B

ANEXA II

Site-urile web care conţin informaţii privind autorităţile competente și adresa pentru notificările adresate Comisiei

▼M4

BELGIA

https://diplomatie.belgium.be/en/policy/policy_areas/peace_and_security/sanctions

BULGARIA

https://www.mfa.bg/en/EU-sanctions

CEHIA

www.financnianalytickyurad.cz/mezinarodni-sankce.html

DANEMARCA

http://um.dk/da/Udenrigspolitik/folkeretten/sanktioner/

GERMANIA

https://www.bmwi.de/Redaktion/DE/Artikel/Aussenwirtschaft/embargos-aussenwirtschaftsrecht.html

ESTONIA

https://vm.ee/et/rahvusvahelised-sanktsioonid

IRLANDA

https://www.dfa.ie/our-role-policies/ireland-in-the-eu/eu-restrictive-measures/

GRECIA

http://www.mfa.gr/en/foreign-policy/global-issues/international-sanctions.html

SPANIA

https://www.exteriores.gob.es/es/PoliticaExterior/Paginas/SancionesInternacionales.aspx

FRANȚA

http://www.diplomatie.gouv.fr/fr/autorites-sanctions/

CROAȚIA

https://mvep.gov.hr/vanjska-politika/medjunarodne-mjere-ogranicavanja/22955

ITALIA

https://www.esteri.it/it/politica-estera-e-cooperazione-allo-sviluppo/politica_europea/misure_deroghe/

CIPRU

https://mfa.gov.cy/themes/

LETONIA

http://www.mfa.gov.lv/en/security/4539

LITUANIA

http://www.urm.lt/sanctions

LUXEMBURG

https://maee.gouvernement.lu/fr/directions-du-ministere/affaires-europeennes/organisations-economiques-int/mesures-restrictives.html

UNGARIA

https://kormany.hu/kulgazdasagi-es-kulugyminiszterium/ensz-eu-szankcios-tajekoztato

▼**M4**

MALTA

https://foreignandeu.gov.mt/en/Government/SMB/Pages/SMB-Home.aspx

ȚĂRILE DE JOS

https://www.rijksoverheid.nl/onderwerpen/internationale-sancties

AUSTRIA

https://www.bmeia.gv.at/themen/aussenpolitik/europa/eu-sanktionen-nationale-behoerden/

POLONIA

https://www.gov.pl/web/dyplomacja/sankcje-miedzynarodowe

https://www.gov.pl/web/diplomacy/international-sanctions

PORTUGALIA

https://www.portaldiplomatico.mne.gov.pt/politica-externa/medidas-restritivas

ROMÂNIA

http://www.mae.ro/node/1548

SLOVENIA

http://www.mzz.gov.si/si/omejevalni_ukrepi

SLOVACIA

https://www.mzv.sk/europske_zalezitosti/europske_politiky-sankcie_eu

FINLANDA

https://um.fi/pakotteet

SUEDIA

https://www.regeringen.se/sanktioner

Adresa pentru notificările către Comisia Europeană:

Comisia Europeană

Direcţia Generală Stabilitate Financiară, Servicii Financiare și Uniunea Pieţelor de Capital (DG FISMA)

Rue de Spa 2

B-1049 Bruxelles/Brussel, Belgium

E-mail: relex-sanctions@ec.europa.eu