ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVI/SUPLIMENT, ŞTIINŢE JURIDICE, 2020

Regimul sancţiunilor cibernetice în Uniunea Europeană
The cyber sanctions regime in the European Union

Adrian Corobană[1]

Rezumat: În data de 30 iulie 2020, Uniunea Europeană a anunţat decizia de a impune primele sancţiuni internaţionale împotriva atacurilor cibernetice. În aceeaşi zi, Departamentul de Stat al Statelor Unite ale Americii a emis un comunicat de presă prin care saluta aplicarea sancţiunilor cibernetice de către Uniunea Europeană. Scopul acestei lucrări este de a clarifica noţiunea de „*sancţiuni cibernetice*” şi să explice cum regimul aplicării sancţiunilor cibernetice de către Uniunea Europeană este în deplină concordanţă cu regulile dreptului internaţional public. Prin urmare, ipoteza de cercetare a acestui articol este următoarea: dreptul internaţional public se aplică şi în spaţiul cibernetic, iar sancţiunile cibernetice, în substanţa lor, nu diferă prea mult de sancţiunile internaţionale ţintite, astfel încât principala diferenţă dintre cele două tipuri de sancţiuni nu o reprezintă conţinutul acestor măsuri restrictive, ci acţiunile care au declanşat mecanismul de răspuns de către comunitatea internaţională.

Cuvinte-cheie: sancţiuni cibernetice; sancţiuni internaţionale ţintite; Uniunea Europeană; Regulamentul Consiliului nr. 2019/796.

Abstract: On 30 July 2020 the Council of the European Union announced the decision to impose the first ever sanctions against cyber-attacks. On the same day, the U.S. Department of State released a press statement welcoming the application of cyber sanctions by the European Union. The aim of this paper is to clarify the notion of cyber sanctions from the conceptual point of view and to explain how the EU's cyber sanctions regime complies with the rules of public international law. Therefore, the research hypothesis of this article is as follows: international law matters in cyberspace and the cyber sanctions in their substance do not differ much from targeted sanctions, so the main difference between them is not in the content of the restrictive measures, but in the actions that trigger the response of the international community.

Keywords: cyber sanctions; targeted sanctions; European Union; Council Regulation (EU) no. 2019/796.

Introducere

În ultimii ani, pe măsură ce noile tehnologii din domeniul comunicaţiilor au pătruns din ce în ce mai mult în viaţa oamenilor de rând, inevitabil statele

[1] Avocat în Baroul Bucureşti, doctorand la Academia de Studii Economice din Bucureşti, Şcoala Doctorală Drept, e-mail: corobana.adrian@gmail.com.

au început să se bazeze pe acestea în cele mai multe domenii vitale pe care le are de administrat, cunoscându-se o activitate tot mai mare a statelor în spaţiul cibernetic.

În mod evident, de la folosirea pe scară largă a noilor tehnologii de către state până la apariţia activităţilor ilicite în spaţiul cibernetic nu a fost decât un pas foarte mic, în prezent, în spaţiul cibernetic putându-se vorbi despre: spionaj cibernetic, atacuri cibernetice asupra infrastructurilor critice ale statelor şi, mai nou, despre sancţiuni cibernetice.

Deşi, la prima vedere, spaţiul cibernetic poate părea un spaţiu nou, în special în relaţiile internaţionale, acest lucru nu este nici pe departe aşa: dreptul internaţional public se aplică şi în cazul activităţilor din spaţiul cibernetic.

Cu toate acestea, ne raliem şi noi opiniei exprimate de autorul francez François Delerue în cartea *„Cyber operations and international law”*, conform căreia interpretarea şi aplicarea regulilor dreptului internaţional public la spaţiul cibernetic trebuie să cunoască o adaptare la specificul spaţiului cibernetic[2].

Problematica sancţiunilor internaţionale este deosebit de complexă şi deosebit de controversată în domeniul dreptului internaţional public.

Dificultatea identificării unor sancţiuni pentru încălcarea normelor de drept internaţional public a condus de multe ori în trecut la ideea doctrinară că dreptul internaţional public nu ar fi un drept veritabil în sensul de ordine juridică, ci o *„moralitate internaţională pozitivă”*[3].

În realitate, aşa cum remarca şi Lassa Oppenheim în articolul său intitulat *„The Science of International Law: Its Task and Method”*, negarea caracterului de ordine juridică a dreptului internaţional public provine din compararea acestuia cu dreptul naţional: *„De la Hobbes până la Blackstone şi Austin, este întotdeauna vorba despre acelaşi punct de plecare greşit – dreptul intern”*.[4]

Aceste dezbateri doctrinare au fost tranşate în doctrina de după cel de-al Doilea Război Mondial, odată cu apariţia cărţii lui Herbert Lionel Adolphus Hart intitulată „Conceptul de drept” (The concept of law), care a dezbătut ideea că existenţa sancţiunii în structura normei juridice nu este de chintesenţa unei ordini juridice.

Astfel, toate particularităţile dreptului internaţional public şi toate diferenţele sale faţă de dreptul intern nu pot conduce la concluzia greşită că în

[2] Fr. Delerue, *Cyber operations and international law*, Cambridge University Press, 2020, p. 2.

[3] J. Austin, *The Province of Jurisprudence Determined*, Cambridge University Press, New York, 2001, pp. 112, 160.

[4] L. Oppenheim, *The Science of International Law: Its Task and Method*, American Journal of International Law, Nr. 2, 1908, p. 330.

dreptul internaţional public nu ar exista sancţiuni. În dreptul internaţional public există forme de constrângere şi sancţiuni, unele dintre ele fiind prevăzute chiar de Carta Organizaţiei Naţiunilor Unite, în art. 41, art. 42 şi art. 51. În afara acestor sancţiuni prevăzute de Carta Organizaţiei Naţiunilor Unite, există şi sancţiuni specifice dreptului internaţional public, ce nu sunt prevăzute în documente internaţionale, cum ar fi: nerecunoaşterea statelor, nerecunoaşterea guvernelor, nulitatea unui tratat sau a unor clauze din cadrul unei convenţii internaţionale, excluderea din organizaţii internaţionale, sancţiuni economice, ş.a.[5]

În ultimii ani, în special în Uniunea Europeană, observăm apariţia unui nou tip de sancţiuni internaţionale: sancţiunile cibernetice sau, aşa cum sunt ele numite în limba engleză, cyber sanctions. Era şi firesc să apară, atâta timp cât dreptul urmează viaţa şi cu atât mai mult cu cât în dreptul internațional trebuie să fie create mecanisme prin care conduita unor subiecte de drept să fie adusă în matca legalităţii.

Începând cu anul 2015 se observă o preocupare intensă a Uniunii Europene cu privire la capacitatea sa de a descuraja atacurile cibernetice şi de a răspunde la acestea. Şi asta şi pentru că au existat evenimente care au adus în prim-plan, în rândul statelor importante din Uniunea Europeană, acest subiect. Şi mă refer aici, în special la un atac cibernetic împotriva parlamentului federal german (Deutscher Bundestag) din aprilie şi mai 2015. Acest atac cibernetic a fost îndreptat împotriva sistemului informatic al parlamentului federal german, căruia i-a afectat funcţionarea timp de mai multe zile. A fost furat un volum important de date şi au fost afectate conturile de e-mail ale mai multor parlamentari, inclusiv cele ale Angelei Merkel.

Articolul de faţă tratează regimul juridic al acestor sancţiuni cibernetice, analizând actele normative prin intermediul cărora sunt ele implementate, încercând să răspundă la întrebarea în ce tip de sancţiuni internaţionale pot fi încadrate sancţiunile cibernetice aplicate recent de Uniunea Europeană.

Putem vorbi într-adevăr de nişte tipuri noi de sancţiuni sau de fapt sunt doar acelaşi tip de sancţiuni internaţionale care existau şi până în prezent, dar care se aplică acum şi împotriva unor subiecte de drept care creează atacuri informatice?

1. Sediul materiei

La nivelul Uniunii Europene avem două acte normative deosebit de importante, care practic, constituie principalul sediu al materiei.

[5] A. Corobană, *Non-recognition of states as a specific sanction of public international law*, Juridical Tribune (Tribuna Juridica), 2019, vol. 9, issue 3, 589-598.

Este vorba despre:

1. Decizia Consiliului (PESC – Politica externă şi de securitate comună a UE) nr. 2019/797 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o ameninţare la adresa Uniunii sau a statelor sale membre şi

2. Regulamentul Consiliului nr. 2019/796 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o ameninţare la adresa Uniunii sau a statelor sale membre.

Ambele reglementări au fost adoptate în 17 mai 2019 şi au în proporţie de 90% acelaşi conţinut normativ, aducând mai multe clarificări cu privire la noţiunea de sancţiuni cibernetice: când se iau aceste sancţiuni cibernetice, cine este competent să le instituie, pentru ce tip de faptă ilicită şi care este conţinutul acestor sancţiuni.

În acest fel s-a creat un cadru normativ pentru măsurile restrictive specifice pentru a descuraja şi pentru a răspunde la atacurile cibernetice care au efecte semnificative şi care constituie o ameninţare externă la adresa Uniunii sau a statelor sale membre.

Aceste acte normative se înscriu în documentele ce au emanat de la Consiliul U.E. privind orientările şi bunele practici privind sancţiunile (măsurile restrictive), ca instrument al Politicii externe şi de securitate comună a U.E.

La nivelul Uniunii Europene, sancţiunile sau măsurile restrictive sunt privite ca *„un instrument politic la dispoziţia factorilor de decizie care încearcă a schimba, a limita sau a critica în termeni normativi comportamentul altui actor”*[6].

Cele două noţiuni *„sancţiuni”* şi *„măsuri restrictive”* sunt echivalente, fiind folosite cu acelaşi înţeles la nivelul documentelor Consiliului, U.E. adoptând *„o abordare orientată şi diferenţiată a măsurilor restrictive (sancţiuni)”* şi *„impunând măsuri restrictive, fie din proprie iniţiativă, fie pentru a pune în aplicare rezoluţiile Consiliului de Securitate al ONU”*.[7]

Aşadar, aceste sancţiuni trebuie să fie în deplină concordanţă cu obiectivele politicii externe şi de securitate comune, astfel cum sunt enunţate la articolul 21 alin. (2) din Tratatul privind Uniunea Europeană (TUE): *apărarea valorilor, a intereselor fundamentale, a securităţii, a independenţei şi integrităţii Uniunii Europene, consolidarea şi sprijinirea democraţiei, a statului de drept, a drepturilor omului şi a principiilor dreptului internaţional, menţinerea păcii, prevenirea conflictelor şi consolidării securităţii internaţionale, în conformitate cu scopurile şi principiile Cartei Organizaţiei Naţiunilor Unite, precum şi cu principiile Actului final de la Helsinki şi cu obiectivele Cartei de la Paris, inclusiv*

[6] P. Pawlak, Th. Biersteker, Guardian of the Galaxy. EU cyber sanctions and norms in cyberspace, Chaillot Paper nr. 155, European Union Institute for Security Studies (EUISS), 2019, p. 8.

[7] Council of the European Union, *Sanctions: how and when the EU adopts restrictive measures*, https://www.consilium.europa.eu/en/policies/sanctions/.

cele privind frontierele externe, promovarea dezvoltării durabile pe plan economic, social şi de mediu a ţărilor în curs de dezvoltare, cu scopul primordial de a eradica sărăcia, încurajarea integrării tuturor ţărilor în economia mondială, inclusiv prin eliminarea treptată a barierelor în calea comerţului internaţional, participarea la elaborarea unor măsuri internaţionale pentru conservarea şi îmbunătăţirea calităţii mediului şi gestionarea durabilă a resurselor naturale mondiale, în vederea asigurării unei dezvoltări durabile, acordarea de asistenţă populaţiilor, ţărilor şi regiunilor care se confruntă cu dezastre naturale sau provocate de om şi promovarea unui sistem internaţional bazat pe o cooperare multilaterală mai puternică şi pe o bună guvernare globală.[8]

De asemenea, la nivelul Uniunii Europene, identificăm două tipuri de sancţiuni: sancţiuni în sens larg şi sancţiuni în sens restrâns.

Dacă ne referim la sancţiuni, în sens larg, atunci acestea sunt denumite *„sancţiuni diplomatice"*, întrucât includ, printre altele, întreruperea relaţiilor diplomatice cu un stat sau retragerea reprezentanţilor diplomatici de la nivelul U.E. şi ai statelor sale membre, în deplină coordonare.

Dacă ne referim la sancţiuni în sens restrâns, atunci este necesar un temei juridic în tratatele Uniunii, întrucât acestea includ măsuri ca: 1. embargouri de armament; 2. restricţii privind admisia (interdicţii de călătorie – persoanele sancţionate, dacă nu sunt cetăţeni ai Uniunii Europene, nu pot intra pe teritoriul Uniunii, iar dacă sunt cetăţeni ai Uniunii Europene nu pot ieşi în afara statului membru ai cărui cetăţeni sunt); 3. îngheţarea activelor financiare (toate activele din Uniunea Europeană ale persoanelor vizate sunt îngheţate, iar persoanele fizice şi juridice din cadrul Uniunii Europene nu pot pune fonduri la dispoziţia persoanelor vizate) sau *4. sancţiuni economice privind sectoare specifice de activitate economică, inclusiv interdicţii privind importul sau exportul anumitor mărfuri, interdicţii privind investiţiile, interdicţii privind furnizarea anumitor servicii.*[9]

Pentru ca măsurile menţionate mai sus să poată fi implementate fie la nivelul Uniunii Europene, fie la nivel naţional, este necesar mai întâi de toate să fie adoptată de către Consiliu o decizie PESC, astfel cum se prevede în art. 29 din Tratatul privind Uniunea Europeană.

Aceste decizii privind Politica Externă şi de Securitate Comună care prevăd sancţiuni internaţionale împotriva persoanelor fizice şi juridice sunt supuse controlului judecătoresc la nivelul Uniunii Europene.

Sancţiunile ce privesc punctele 1 şi 2, adică cele privind embargourile de armament şi restricţiile privind admisia, sunt puse în aplicare în mod direct de statele membre, doar prin simpla adoptare a deciziei PESC, fără a mai fi

[8] Art. 21 alin. (2) din Tratatul privind Uniunea Europeană, publicat în Jurnalul Oficial al Uniunii Europene C326/29 din 26.10.2012.

[9] Council of the European Union, *Sanctions: how and when the EU adopts restrictive measures*, https://www.consilium.europa.eu/en/policies/sanctions/.

necesară adoptarea altor acte normative la nivelul Uniunii Europene. Statele membre sunt astfel obligate să acţioneze în conformitate cu deciziile PESC ale Consiliului. În acest sens, fiecare stat membru şi-a elaborat în cadrul sistemului de drept naţional un cadru legislativ de punere în aplicare a sancţiunilor internaţionale aplicate de către Uniunea Europeană.

În România, principalul act normativ care reglementează modul de punere în aplicare a sancţiunilor internaţionale îl reprezintă Ordonanţa de urgenţă nr. 202/2008 privind punerea în aplicare a sancţiunilor internaţionale[10] aprobată de Parlament prin Legea nr. 217/2009 şi intrată în vigoare la 08 decembrie 2008.

Pe lângă această ordonanţă de urgenţă există o serie de acte normative infralegale care reglementează procedural modul de punere în aplicare a sancţiunilor internaţionale la nivelul fiecărei instituţii ce i-au fost conferite atribuţii în acest domeniu:

– Regulamentul Băncii Naţionale a României nr. 28/2009 privind supravegherea modului de punere în aplicare a sancţiunilor internaţionale de blocare a fondurilor;[11]

– Hotărârea de Guvern nr. 603/2011 pentru aprobarea Normelor privind supravegherea de către Oficiul Naţional de Prevenire şi Combatere a Spălării Banilor a modului de punere în aplicare a sancţiunilor internaţionale;[12]

– Procedura privind modalitatea de ducere la îndeplinire a atribuţiilor Agenţiei Naţionale de Administrare Fiscală în domeniul sancţiunilor internaţionale, din 14.09.2020 aprobată prin Ordinul Preşedintelui Agenţiei Naţionale de Administrare Fiscală nr. 3486/2020;[13]

– Regulamentul Comisiei Naţionale a Valorilor Mobiliare nr. 9/2009 privind supravegherea punerii în aplicare a sancţiunilor internaţionale pe piaţa de capital;[14]

– Norma Comisiei de Supraveghere a Asigurărilor privind procedura de supraveghere, în domeniul asigurărilor, a aplicării sancţiunilor internaţionale din 30.07.2009;[15]

– Norma Comisiei de Supraveghere a Sistemului de Pensii Private nr. 11/2009 privind procedura de supraveghere a punerii în aplicare a sancţiunilor internaţionale în sistemul pensiilor private.[16]

Pentru celelalte sancţiuni privind punctele 3 şi 4 menţionate mai sus, se aplică articolul 215 din Tratatul privind funcţionarea Uniunii Europene: *în*

[10] Publicată în Monitorul Oficial, Partea I nr. 825 din 08 decembrie 2008.
[11] Publicat în Monitorul Oficial, Partea I nr. 891 din 18 decembrie 2009.
[12] Publicat în Monitorul Oficial, Partea I nr. 426 din 17 iunie 2011.
[13] Publicat în Monitorul Oficial, Partea I nr. 881 din 28 septembrie 2020.
[14] Publicat în Monitorul Oficial, Partea I nr. 916 din 28 decembrie 2009.
[15] Publicat în Monitorul Oficial, Partea I nr. 555 din 10 august 2009.
[16] Pubicat în Monitorul Oficial, Partea I nr. 328 din 18 mai 2009.

cazul în care o decizie, adoptată în conformitate cu titlul V capitolul 2 din Tratatul privind Uniunea Europeană, (n.a.: adică o decizie PESC –privind Politica Externă şi De Securitate Comună) *prevede întreruperea sau restrângerea, totală sau parţială, a relaţiilor economice şi financiare cu una sau mai multe ţări terţe, Consiliul, hotărând cu majoritate calificată la propunerea comună a Înaltului Reprezentant al Uniunii pentru afaceri externe şi politica de securitate şi a Comisiei, adoptă măsurile necesare* [17], Consiliul fiind obligat să informeze Parlamentul European cu privire la aceasta.

Astfel, în cazul acestor măsuri restrictive, ele sunt puse în aplicare printr-un Regulament adoptat de Consiliu, ce va avea forţă obligatorie, aplicându-se în mod direct în toate statele membre ale Uniunii Europene, în conformitate cu art. 288 din Tratatul privind funcţionarea Uniunii Europene.

Aşadar, cele două acte normative menţionate la începutul acestei secţiuni a articolului se înscriu în procedura de adoptare a actelor juridice prevăzută de Tratatul privind Uniunea Europeană şi Tratatul privind funcţionarea Uniunii Europene, descriind instrumentele prin care se înfăptuieşte o parte din Politica Externă şi de Securitate Comună.

2. Conţinutul normativ al sancţiunilor cibernetice la nivelul Uniunii Europene

Decizia (PESC) 2019/797 a stabilit un cadru normativ pentru sancţiuni internaţionale specifice cu scopul de a *descuraja şi a răspunde la atacurile cibernetice care au efecte semnificative care constituie o ameninţare externă la adresa Uniunii sau a statelor sale membre.*[18]

Şi totuşi care sunt acele atacuri cibernetice care au efecte semnificative şi care constituie o ameninţare externă la adresa Uniunii sau a statelor sale membre? Răspunsul la această întrebare îl regăsim în prevederile art. 1 alin. (3) şi (4) din Regulamentul (UE) nr. 2019/796 al Consiliului.

În conformitate cu art. 1 alin. (3) din Regulamentul (UE) nr. 2019/796 al Consiliului sunt considerate atacuri cibernetice ce vor declanşa mecanismul de instituire a unor măsuri restrictive următoarele acţiuni (dacă nu sunt autorizate în mod corespunzător de către proprietar sau de către alt titular de drepturi asupra sistemului sau datelor ori asupra unor părţi ale acestora sau nu sunt permise în temeiul dreptului Uniunii sau al legislaţiei statului membru în cauză): accesarea de sisteme de informaţii; interferenţa cu sisteme de informaţii; interferenţa cu date sau interceptarea de date.

[17] Art. 215 alin. (1) din Tratatul privind funcţionarea Uniunii Europene, publicat în Jurnalul Oficial al Uniunii Europene 326/144 din 26.10.2012

[18] Regulamentul (UE) nr. 2019/796 al Consiliului din 17 mai 2019 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o ameninţare la adresa Uniunii sau a statelor sale membre

De asemenea, conform prevederilor art. 1 alin. (4) din Regulamentul (UE) nr. 2019/796 printre atacurile cibernetice care constituie o ameninţare pentru statele membre se numără cele care afectează sistemele informatice legate, printre altele, de: *1. infrastructura critică, inclusiv cablurile submarine şi obiectele lansate în spaţiul cosmic, care sunt esenţiale pentru menţinerea funcţiilor vitale ale societăţii sau pentru sănătatea, siguranţa, securitatea şi bunăstarea economică sau socială a oamenilor; 2. serviciile necesare pentru menţinerea unor activităţi sociale şi/sau economice esenţiale, în special în sectoare precum energia (electricitate, petrol şi gaze); transporturile (aerian, feroviar, pe apă şi rutier); bancar; infrastructurile pieţelor financiare; sănătatea (furnizori de asistenţă medicală, spitale şi clinici private); furnizarea şi distribuirea de apă potabilă; infrastructura digitală; precum şi în orice alt sector care este esenţial pentru statul membru în cauză; 3. funcţii critice ale statului, în special în domeniile apărării, al guvernanţei şi al funcţionării instituţiilor, inclusiv în ceea ce priveşte alegerile publice sau procesul de votare, al funcţionării infrastructurii economice şi civile, al securităţii interne şi al relaţiilor externe, inclusiv prin misiuni diplomatice; 5. stocarea sau prelucrarea de informaţii clasificate; sau 6. echipe guvernamentale de răspuns la situaţii de urgenţă.*

Cu privire la efectul semnificativ al unui atac cibernetic, Regulamentul prevede în art. 2 o serie de criterii în funcţie de care factorii decizionali trebuie să îi analizeze: *1. domeniul de aplicare, amploarea, impactul sau gravitatea perturbării cauzate, inclusiv în ceea ce priveşte activităţile economice şi societale, serviciile esenţiale, funcţiile critice ale statului, ordinea publică sau siguranţa publică; 2. numărul persoanelor fizice sau juridice, a entităţilor sau a organismelor afectate; 3. numărul statelor membre afectate; 4. valoarea prejudiciilor economice cauzate de exemplu de furtul de mari dimensiuni de fonduri, de resurse economice sau de proprietate intelectuală; 5. beneficiile economice obţinute de către autor, pentru sine sau pentru alţii; 6. volumul sau natura datelor furate sau amploarea încălcării securităţii datelor sau 7. natura datelor sensibile din punct de vedere comercial accesate.*[19]

Dacă aceste criterii prevăzute în art. 1 şi 2 din Regulament sunt îndeplinite atunci ne aflăm în prezenţa unui atac cibernetic cu efecte semnificative care constituie o ameninţare externă la adresa Uniunii sau a statelor sale membre.

Motiv pentru care, dacă sunt identificaţi autorii acestor atacuri (fie că vorbim de state, dar mai ales de actori non-statali), procedura prevede ca aceştia să fie incluşi pe o aşa-numită listă neagră ce se anexează la Regulamentul (UE) nr. 2019/796.

[19] Art. 2 din Regulamentul (UE) nr. 2019/796 al Consiliului din 17 mai 2019 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o ameninţare la adresa Uniunii sau a statelor sale membre

Competent să întocmească şi să modifice această listă este Consiliul, care va emite de fiecare dată o nouă decizie PESC şi un nou regulament care să completeze Anexa nr. 1 a Regulamentului (UE) nr. 2019/796, conform punctului nr. 4 din preambulul Regulamentului.

Aşadar, concret, se întocmeşte o listă neagră a persoanelor care au efectuat atacuri cibernetice importante asupra statelor U.E. Efectiv este o Anexă care se reînnoieşte periodic de către Consiliu.

Până în iulie 2020, această anexă, această listă, nu conţinea niciun nume şi nicio denumire. În iulie 2020, a fost adoptat un Regulament de punere în aplicare a Regulamentului 2019/796 prin care au fost adăugate 6 nume de persoane fizice şi de entităţi care au efectuat atacuri cibernetice. (Decizia Consiliului privind PESC nr. 2020/1127 din 30 iulie 2020 şi Regulamentul de punere în aplicare emis de Consiliu (UE) nr. 2020/1125 din 30 iulie 2020).

Iar recent în 22 octombrie 2020, a fost suplimentată această listă cu încă două nume: Dmitri Badin a luat parte la un atac cibernetic cu efecte importante împotriva parlamentului federal german (Deutscher Bundestag) şi Igor Kostiukov este actualul şef al Direcţiei principale a Statului-Major al forţelor armate al Federaţiei Ruse (GU/GRU).[20]

Modul în care sunt implementate aceste sancţiuni cibernetice se face la nivelul fiecărui stat membru, prin legislaţia sa naţională.

3. Care sunt sancţiunile cibernetice?

Regulamentul Consiliului (UE) nr. 2019/796 prevede următoarele tipuri de sancţiuni:

1. Restricţii privind admisia – art. 4 din Regulament

Statele membre sunt obligate să ia măsurile necesare pentru a împiedica intrarea sau tranzitul pe teritoriul lor a: persoanelor fizice care sunt responsabile de atacuri cibernetice sau tentative de atacuri cibernetice; a persoanelor fizice 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; persoanelor fizice asociate cu acestea.

[20] Prin Regulamentul de Punere în Aplicare (UE) 2020/1536 al Consiliului şi prin Decizia (PESC) nr. 2020/1537 a Consiliului din 22 octombrie 2020 de modificare a Deciziei (PESC) 2019/797 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o ameninţare la adresa Uniunii sau a statelor sale membre, ambele publicate în Jurnalul Oficial al Uniunii Europene nr. LI 351/5 din 22.10.2020

2. Înghețarea fondurilor şi a resurselor economice – art. 5 din Regulament

Statele membre sunt obligate să înghețe toate fondurile şi resursele economice care aparţin sau se află în proprietatea, care sunt deţinute sau controlate de: persoane fizice sau juridice, entităţi sau organisme care sunt responsabile de atacuri cibernetice sau tentative de atacuri cibernetice; persoane 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; persoanele fizice sau juridice, entităţi sau organisme asociate cu acestea;

3. Suspendarea oricărei plăţi sau cereri de despăgubire – art. 8 din Regulament

Statele membre şi persoanele fizice şi juridice din statele membre ale Uniunii Europene sunt obligate să nu dea curs niciunei cereri în legătură cu niciun contract sau nicio tranzacţie a cărei executare a fost afectată, în mod direct sau indirect, în totalitate sau parţial, de măsurile impuse, inclusiv cererilor de despăgubire sau oricărei alte cereri de acest tip, cum ar fi cererile de compensare sau cele de chemare în garanţie, mai ales cererilor de prelungire sau de plată a unei obligaţiuni, a unei garanţii sau a unei indemnizaţii, în special a unei garanţii financiare sau a unei indemnizaţii financiare, indiferent de formă, în cazul în care este formulată de: o persoanele fizice sau juridice, entităţile sau organismele desemnate, enumerate în Anexa Regulamentul (UE) nr. 2019/796.

Concluzii

Concluzionând, sancţiunile cibernetice nu sunt nimic altceva decât nişte sancţiuni internaţionale ţintite (aşa numitele *targeted sanctions*) ce sunt luate de Uniunea Europeană împotriva unor state din afara Uniunii sau unor grupuri sau persoane fizice sau juridice care au lansat atacuri cibernetice cu efecte semnificative şi care constituie o ameninţare externă la adresa Uniunii sau a statelor sale membre.

Până în 1990, Consiliul de Securitate al ONU instituia sancţiuni internaţionale clasice (aşa numitele *comprehensive sanctions*) – care afectau întregul stat sau întreaga populaţie dintr-un stat sau dintr-un teritoriu, de exemplu – embargoul, neacordarea de vize tuturor cetăţenilor respectivului stat, etc.

Acestea aveau un efect destul de nociv asupra populaţiei şi nu asupra elitei conducătoare a statului respectiv, care se făcea responsabilă de acele fapte ilicite care încălcau dreptul internaţional public.

După 1990, practica Consiliului de Securitate şi practica statelor s-a axat în principal pe aşa-numitele *targeted sanctions*, sancţiuni internaţionale ţintite, care afectează mai mult elita conducătoare a statelor cu conduită ilicită. Şi aici întâlnim, în principal, sancţiuni precum: îngheţarea fondurilor, retragerea vizelor şi a permiselor de şedere pentru cei din elita conducătoare, interzicerea punerii la dispoziţie de fonduri sau resurse economice, ş.a.

Astfel, sancţiunile cibernetice, în substanţa lor, nu diferă prea mult de sancţiunile internaţionale ţintite, principala diferenţă dintre cele două tipuri de sancţiuni nefiind conţinutul acestor măsuri restrictive, ci acţiunile care au declanşat mecanismul de răspuns de către comunitatea internaţională.

În acest sens, ne raliem opiniei exprimate în doctrină de autorii Patryk Pawlak şi Thomas Biersteker, conform căreia în mod tradiţional şi mai ales în domeniul cibernetic, sancţiunile iau în general forma sancţiunilor ţintite împotriva unui stat, persoane fizice sau entităţi, acestea făcând parte din categoria de sancţiuni internaţionale a retorsiunilor.[21]

Aşadar, fără a încerca să diminuăm importanţa lor, sancţiunile cibernetice (cyber sanctions) sunt tot sancţiuni ţintite (targeted sanctions), doar că ele sunt instituite pentru un tip nou de faptă ilicită, şi anume atacurile cibernetice asupra unui stat membru al U.E. sau asupra unei instituţii a Uniunii Europene.

[21] P. Pawlak, Th. Biersteker, *op. cit.*, p. 47.