ATACUL CIBERNETIC – O NOUĂ FORMĂ DE AGRESIUNE ÎN DREPTUL INTERNAȚIONAL

Daria ARMAN

Advent of technology not only widens scientific horizon, but also poses constant challenges for the jurisprudence, legal system and legal world as a whole. Computers, Internet and Cyberspace – together known as Information Technology – presents challenges for the law. Challenges, which are not confined, to any single traditional legal category but in almost all established categories of law.

La etapa actuală, un atac cibernetic ar trebui să fie calificat nu doar o crimă împotriva resurselor informaționale, ci și o formă modernă de comitere a unui act de agresiune.

Prin efectuarea acestui tip de atac, pot fi furate informații ce constituie secrete de stat, se poate deteriora sistemul de susținere a vieții statului și se poate comite un sabotaj grav, precum distrugerea sistemului de apărare, care reprezintă o amenințare la adresa securității statului și este o încălcare a principiilor general acceptate ale dreptului internațional [1].

Actualitatea și necesitatea temei constă în cercetarea celei mai noi forme de agresiune, anume atacul cibernetic, dar și a celei mai noi crime internaționale asupra căreia Curtea Internațională Penală are jurisdicție – crima de agresiune. În cadrul cercetării au fost folosite materiale disponibile, ca exemplu, regulile stabilite în prima ediție a *Manualului de la Tallinn*. Un alt element este îmbinarea dreptului internațional public, dreptului internațional umanitar și dreptului internațional penal cu anumite elemente din domeniul tehnologiei informației și comunicațiilor. Îmbinarea acestor elemente va permite

analizarea cazurilor în care recurgerea la atacuri cibernetice poate fi catalogată drept agresiune, poate duce la declanşarea unui conflict armat sau situaţiile în care o operaţiune cibernetică va atrage răspunderea penală individuală pentru comiterea unei crime internaţionale.

Lucrarea dată are scopul de a efectua o analiză complexă a atacului cibernetic, şi în mod special a metodelor şi mijloacelor de purtare a conflictelor armate în spaţiul cibernetic. Asemenea identificare a normelor de drept aplicabile atacurilor cibernetice şi a situaţiilor în care recurgerea la folosirea atacurilor cibernetice poate duce la declanşarea unui conflict armat.

Recunoscând potenţialul de utilizare abuzivă, multe state au emis declaraţii cu privire la necesitatea reglementării comportamentului pe Internet. Adunarea Generală a ONU a emis numeroase declaraţii cu privire la posibilităţile abuzului cibernetic.

Apariţia atacurilor cibernetice reprezintă cea mai nouă parte a evoluţiei războiului şi continuitatea schimbărilor în război provocate de modificările tehnologice. Aceste modificări pun în mod inevitabil la îndoială cadrul de utilizare a forţei, precum şi alte aspecte relevante ale dreptului internaţional, dar şi ale dreptului internaţional umanitar. Reglementarea utilizării forţei este unul dintre aspectele cele mai controversate ale dreptului internaţional, iar ambiguitatea conceptelor de forţă şi atac armat nu este un fenomen nou şi nici nu este o limitare în contextul operaţiunilor cibernetice [2].

În măsura în care atacurile cibernetice sunt sub pragul unui atac armat, dispoziţiile legii spaţiale, neproliferarea armelor nucleare, Convenţia ONU şi drepturile de comunicare joacă un rol în crearea regimului juridic actual. Deşi această combinaţie este un regim imperfect, comunitatea internaţională trebuie să utilizeze toate instrumentele disponibile pentru a rezolva problema atacurilor cibernetice. Naţiunile folosesc din ce în ce mai mult potenţialul armamentului cibernetic, astfel sporind probabilitatea unui atac [3].

Atacul cibernetic este un atac hacking elaborat şi menit respectiv, de a submina sistemul de securitate a calculatorului, ca urmare pot fi distruse prin activitatea sa diferite tipuri de infrastructură a unui stat, inclusiv poate fi perturbat sistemul de securitate antirachetă. Acest tip de atac trebuie calificat drept o formă modernă de act de agresiune,

având în vedere severitatea consecințelor sale, comparabile cu un atac armat [4].

Agresiunea este cea mai gravă crimă internațională și reprezintă o amenințare pentru orice stat. Pentru a menține pacea și securitatea internațională, statele trebuie să colaboreze ca să dezvolte metode și acte juridice moderne și relevante care să vizeze prevenirea acestei infracțiuni în toate formele și manifestările sale.

Conflictul cibernetic este, fără îndoială, unic: în primul rând, acestea nu sunt asociate cu utilizarea armelor cinetice convenționale și, prin urmare, este destul de dificil să se determine locul desfășurării acțiunilor. Atacurile cibernetice pot apărea în diferite părți ale lumii, pot fi sub jurisdicția diferitelor state și uneori este destul de dificil să se definească așa-numitul teatru de război [5].

Modificările în legislațiile și politicile diferitelor state, cum ar fi adăugarea aplicabilității extrateritoriale la legile penale și planificarea utilizării contramăsurilor, reprezintă răspunsuri juridice valoroase la amenințarea atacului cibernetic. Totuși, „spațiul cibernetic este o rețea de domenii care include mii de furnizori de servicii internet de pe tot globul; niciun stat sau organizație nu poate menține apărarea cibernetică eficientă". Având în vedere caracterul transnațional al provocării, este posibil ca cooperarea internațională să fie necesară pentru a oferi o soluție proporțională cu problema.

Atacurile cibernetice oferă o tactică ieftină, la distanță, instantanee și puternică de constrângere sau distrugere, adesea fără a declanșa răspunderea. Aceste atribute garantează că statele și actorii nestatali vor continua să dezvolte și să săvârșească atacuri cibernetice în viitorul apropiat.

În cadrul viitoarelor conflicte armate, inteligența și tehnologia militară vor avea un rol hotărâtor, generând o cunoaștere aproape instantanee a situației militare globale și punctuale din lume, o reală superioritate informațională, o nouă dinamică, precizie și eficacitate a forțelor, asigurând, în timp scurt, înfrângerea și capitularea inamicului.

Interdicția juridică internațională ca sursă de răspundere în temeiul dreptului internațional este destul de relevantă ca și aplicarea în practică, inclusiv de Curtea Internațională de Justiție. Acest lucru este posibil, deoarece personajul este universal în natură pentru toate statele care se străduie să mențină pacea și securitatea universală, spre

deosebire de tratatele internaționale, în a căror adoptare poate fi făcută o rezervă pentru a evita regula responsabilității. Trebuie menționat că, în viitor, practica dreptului internațional personalizat în domeniul extrădării persoanelor implicate în comiterea agresiunii va îmbunătăți sistemul internațional de justiție, precum și va contribui la consolidarea relațiilor interstatale menite să mențină pacea și securitatea internațională.

Referințe:

1. ТИМОШКОВ, С.Г. Кибератака как современная форма совершения акта агрессии. В: *Вестник РГГУ. Серия Экономика. Управление. Право*, 2017, № (1), сс. 127-135.
2. RID, T.H. Cyber War Will Not Take Place. In: *Journal of Strategic Studies*, 2012, no. 1, vol. 35, pp. 5-32.
3. Carta nr. 1945 din 26.06.1945 a Națiunilor Unite, în vigoare pentru Republica Moldova din 2 martie 1992.
4. SCHMITT, M.N., elab. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013, p. 215.
5. ФЕДОРОВ, А.В., elab. *Информационная безопасность в мировом политическом процессе*. Москва: МГИМО-Университет, 2006, с. 220.