ATACUL CIBERNETIC CA FORMĂ DE AGRESIUNE ÎN DREPTUL INTERNAȚIONAL

CYBER ATTACK AS A FORM OF AGGRESSION IN PUBLIC INTERNATIONAL LAW

Daria ARMAN, masterand,
Universitatea de Stat din Moldova

Abstract: 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. Committing that kind of an attack one can steal the information that constitutes a state secret, violate the life support system of the state, and destroy the missile defence system what poses a threat to the security of the state and is a violation of universally recognized principles of international law.

Cuvinte-cheie: *atac cibernetic, agresiune, conflict, drept internațional umanitar, drept internațional public, tehnologii informaționale, informație, calculator, sisteme informatice, internet, securitate, hacker, crimă, răspundere.*

În legătură cu crearea de noi tehnologii și dezvoltarea sferei de informare pentru comunitatea globală, a apărut o amenințare nouă numită atac cibernetic.

Tehnologiile noi produc impulsuri noi în lege. Natura anonimatului și multijurisdicțională a spațiului informațional ridică probleme în reglementarea de stat care, în principiu, nu existau. Spațiul cibernetic nu are limite și, prin urmare, statalitate. Și aici problemele securității statului pot fi rezolvate doar ca probleme de securitate internațională.

De rând cu agresiunea directă, indirectă, economică și ideologică, aș fi de părerea de a specifica ca un tip aparte agresiunea cibernetică.

Conflictul cibernetic este, fără îndoială, unical: 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, restrângerea acestui teritoriu devine la fel de grea.

Atacurile cibernetice nu se încadrează în cadrul internațional tradițional, care guvernează utilizarea forței. Acestea reprezintă o nouă formă de război dezagregat, desfășurat în principal de echipe non-statale, care reflectă noi concepte de teritorialitate [1, p. 9].

Fără guvernare și constrângeri - din dreptul internațional, spațiul cibernetic va rămâne un câmp de luptă relativ nelegiuit. Multe întrebări dificile apar atunci, când încercăm să potrivim spațiul cibernetic unui regim de conflict, construit cu mult înainte ca cele mai previzibile politici să poată imagina armele cibernetice. Dar problemele generate de atacurile cibernetice sunt adesea similare cu problemele atacurilor convenționale. Diferențele dintre războiul convențional și războiul cibernetic sunt de grad, nu de natură. Astfel, regimul internațional de drept umanitar care guvernează războiul convențional poate fi transpus efectiv în atacurile cibernetice [2, p. 29].

Atacurile cibernetice reprezintă un test de greutate pentru angajamentul națiunii față de dreptul internațional. Problema atribuirii în spațiul cibernetic înseamnă că atacatorii cibernetici au capacitatea de a constrânge un stat fără responsabilitatea rezultantă. Prin urmare, atacatorul cibernetic poate experimenta o mare tentație de a încălca principiile și obligațiile dreptului internațional pentru a atinge scopurile atacatorului. Această amenințare a generat un interes substanțial în regândirea securității cibernetice. În timp ce unii experți au pledat pentru o mai mică anonimitate online și un control mai mult asupra guvernului, asupra infrastructurii cibernetice, există alte soluții care creează mai puține preocupări privind libertatea internă [3, p. 2].

Astăzi, statele se confruntă cu nevoia de a crea rezistență în infrastructura lor cibernetică. Răspunsul la amenințarea atacurilor cibernetice se află la fel de mult în domeniul atenuării, așa cum se întâmplă în domeniul atribuirii. Atenuarea înseamnă crearea unor sisteme de redundanță (cunoscute în mod colateral ca *backup*-uri) pentru a se asigura că sistemele rămân online.

Conflictele armate cresc din ce în ce mai mult dependența de calculatoare și fac ca armatele cele mai avansate și dotate din punct de vedere tehnologic, deci considerate cele mai puternice să devină și cele mai vulnerabile.

Ideea de securitate a dispărut odată cu progresul tehnologiei informației, din acest considerent se atrage o atenție tot mai sporită la tema securitatea în domeniul cibernetic.

Ca bază a dreptului internațional modern sunt principiile general acceptate consacrate în Carta ONU. În conformitate cu aceste principii, toate statele membre ale ONU ar trebui să rezolve conflictele care au apărut prin mijloace pașnice, împiedicând astfel comiterea de infracțiuni internaționale, dintre care cea mai gravă este agresiunea.

Carta Tribunalului Militar de la Nürnberg a stabilit severitatea acestei crime internaționale, însă agresiunea reprezintă o amenințare deosebită în prezent. 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.

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 aflate inofensiva, asigurând, în timp scurt, înfrângerea și capitularea inamicului [4].

În pofida deficiențelor existente, datorită complexității din ce în ce mai mari a situației geopolitice și apariției unor noi forme de agresiune, Rezoluția 3314 (XXIX) a Adunării Generale a ONU din 14 decembrie 1974, care afirmă definiția acestei crime grave internaționale și semnele sale, este principala sursă de standarde de responsabilitate pentru aceasta. Având în vedere faptul că acest act este de natură recomandativă, se desfășoară o activitate științifică constantă în domeniul elaborării de noi acte care să asigure responsabilitatea individuală a autorilor agresiunii, precum și a altor infracțiuni internaționale [5].

Indiferent de politicile pe care o națiune le pune în aplicare pentru a-și apăra infrastructura cibernetică de atacatori, dreptul internațional trebuie să joace un rol de descurajare a acțiunilor ilegale, făcând infractorii răspunzători de evaluarea internațională. Un tratat internațional care reglementează regulile de angajare online ar fi cu siguranță un plus de ajutor în corpusul legilor războiului. Cu toate acestea, în actualul climat internațional, o asemenea adăugire la legile războiului internațional este puțin probabil în viitorul apropiat. Din fericire, lipsa unui *addendum* de război cibernetic la legile de război nu înseamnă că atacurile cibernetice nu sunt reglementate. Statele pot continua să se bazeze pe regimul de drept internațional existent pentru reglementarea atacurilor cibernetice, în timp ce așteaptă răspunsul comunității internaționale la această formă modernă de luptă [6, p. 44].

Forma și funcția finală a regimului internațional de combatere a atacurilor cibernetice vor depinde în mare măsură de răspunsul comunității internaționale la circumstanțe specifice. Cel mai probabil, comunitatea internațională va fi mai concentrată asupra consecințelor unui atac de rețea computerizată decât asupra mecanismului său. Este puțin probabil ca sistemul juridic internațional să formeze un set complet de legi privind operațiunile de informare [7, p. 36].

În măsura în care atacurile cibernetice sunt sub pragul unui atac armat, dispozițiile legii spațiale, neproliferarea armelor nucleare, Convenția ONU și drepturile de comunicare joacă un rol în crearea regimului juridic actual. Deși, această combinație este un regim imperfect, comunitatea internațională trebuie să utilizeze toate instrumentele disponibile pentru a rezolva problema atacurilor cibernetice. Națiunile folosesc din ce în ce mai mult potențialul armamentului cibernetic, astfel sporind probabilitatea unui atac.

În consecință, pentru a stabili responsabilitatea internațională a unui stat pentru executarea sau ordonarea executării unui atac cibernetic, este necesar, ca un prim pas, să se arate regulii internaționale că un astfel de atac într-adevăr

încalcă. Al doilea pas al analizei constă în atribuirea unei astfel de acțiuni unei anumite stări.

Identificarea unei norme internaționale pe care atacurile cibernetice o constituie încălcarea este destul de simplă. După cum s-a explicat mai sus, art.2 alin. (4) al Cartei ONU interzice folosirea forței în relațiile internaționale și este considerat o normă imperativă. Pe baza documentelor ONU deja menționate (adică Declarația privind principiile dreptului internațional cu privire la relațiile prietenoase și cooperarea între state în conformitate cu Carta ONU și Carta drepturilor și obligațiilor economice ale statelor), se pot califica atacuri asupra infrastructurii cheie de stat realizate prin mijloace electronice ca „orice alt tip de măsură de constrângere a unui alt stat", constituind astfel o încălcare a dreptului internațional.

Efectuând o analiză în acest sens se pare clar că responsabilitatea statului trebuie să se bazeze mai degrabă pe o cerință de *duediligence* decât pe obligația de a prezenta o legătură formală între autoritățile statului și acțiunile făptuitorilor efectivi. Un element important al oricărui acord internațional privind responsabilitatea internațională pentru atacurile cibernetice ar fi o dezbatere privind succesiunea principiilor jurisdicției internaționale aplicabile actelor desfășurate prin Internet. Doar atingerea unui astfel de acord va permite evitarea unor analogii îndepărtate față de regimurile internaționale existente și reglementări naționale contradictorii. Un astfel de consens internațional ar putea constitui baza pentru un acord internațional mai larg privind limitele jurisdicției și competenței statului în spațiul cibernetic [8, p. 11].

Rezumând cele de mai sus, este necesar de menționat că problema legată de reglementarea spațiului cibernetic (și, în special, atacul cibernetic) este una dintre cele mai presante din lumea modernă. Rezoluția cea mai rațională a acestei probleme este adoptarea unei convenții care să reflecte toate aspectele acestor relații juridice. Cu toate acestea, este necesar să se înțeleagă că, în actuala situație geopolitică, adoptarea unei convenții poate fi amânată pentru o lungă perioadă de timp, ceea ce creează problema lipsei de reglementare a unuia dintre cele mai periculoase fenomene din lumea modernă.

Referințe bibliografice:

1. Rid Thomas. Cyber War Will Not Take Place, Journal of Strategic Studies, 2011;
2. Michael N.Schmitt. Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge: Cambridge University Press, 2013;
3. Jonathan A.Ophardt. Cyber Warfare and the crime of aggression: The need for individual accountability on tomorrow's battlefield. În: Duke Law & Technology Review (U.S.), 2010, Nr. 3;

4. Owens L.L. Justice and Warfare in Cyberspace. În: Boston Review A Political and Literature Forum (U.S.);
5. Rezoluția Adunării Generale a O.N.U. nr. 3314 (XXIX);
6. Solce. The Battlefield of Cyberspace: The Inevitable New Military Branch - The Cyber Force, ALB. L.J. SCI. & TECH, 2008;
7. Ventre D. Cyberespace et acteurs du cyber conflict, Hermes-Lavoisier, 2011.
8. Jeremy Malcolm. Appraising the Success of the Internet Governance Forum, 21 November 2008.