Atacurile cibernetice din perspectiva articolului 2(4) din carta ONU. Studiu de caz: Stuxnet

Cătălina Pînzaru,
Relații Internaționale și Studii Europene,
promoția 2022-2025,
catalina.panzaru02@e-uvt.ro

ABSTRACT:

Siguranța cibernetică a devenit un subiect din ce în ce mai important în relațiile internaționale contemporane, având în vedere dependența tot mai mare a societății de tehnologie și conectivitate. Peisajul actual al relațiilor internaționale s-a schimbat dramatic. Având la bază mai multe precedente în care statele au utilizat mijloace cibernetice pentru a obține avantaje în agendele lor politice și militare, mulți cercetători și experți subliniază importanța recunoașterii atacurilor cibernetice ca o formă distinctă de război, cu implicații semnificative asupra dreptului internațional și securității globale. Atacurile cibernetice pot, în circumstanța îndeplinirii cerințelor din Tallinn Manual, constitui utilizări ale forței în sensul articolului 2(4) din Carta ONU, în special atunci când produc efecte comparabile cu cele ale forței armate convenționale. Cazul Stuxnet servește drept o ilustrare importantă a acestei realități, subliniind urgența adaptării continue a dreptului internațional la provocările complexe și dinamice ale erei digitale.

Cuvinte cheie: siguranță cibernetică, relații internaționale, drept internațional, operațiunea Stuxnet

INTRODUCERE

1. Contextul general al cercetării și importanța subiectului

Siguranța cibernetică a devenit un subiect din ce în ce mai important în relațiile internaționale contemporane, având în vedere dependența tot mai mare a societății de tehnologie și conectivitate. Peisajul actual al relațiilor internaționale s-a schimbat dramatic. Având la bază mai multe precedente în care statele au utilizat mijloace cibernetice pentru a obține avantaje în agendele lor politice și militare, mulți cercetători și experți subliniază importanța recunoașterii atacurilor cibernetice ca o formă distinctă de război, cu implicații semnificative asupra dreptului internațional și securității globale.

Sistemele informatice, rețelele de comunicații și infrastructura critică sunt indispensabile unui stat modern. Această dependență creează o vulnerabilitate semnificativă în fața atacurilor cibernetice, care pot perturba sau anihila funcționarea serviciilor esențiale, cum ar fi rețelele electrice, sistemele financiare sau infrastructura militară. Atacurile cibernetice reprezintă, prin urmare, o preocupare majoră pentru securitatea internațională și necesită o atenție sporită din partea statelor, organizațiilor internaționale și societății civile. Este esențial să se dezvolte un cadru juridic clar, să se consolideze capabilitățile de apărare cibernetică și să se promoveze cooperarea internațională pentru a atenua amenințările reprezentate de atacurile cibernetice. Cunoașterea modului legal de a reacționa asigură faptul că statele se pot proteja eficient împotriva activităților malițioase, fie acestea realizate de alte state sau de actori non-statali.

2. Obiectivul și ipoteza

Atacurile cibernetice ridică întrebări complexe cu privire la aplicarea dreptului internațional existent, inclusiv Carta ONU și legislația privind războiul. Există dezbateri intense despre când (și dacă) un atac cibernetic constituie utilizarea forței sau o intervenție interzisă. Se pune sub

semnul întrebării dacă atacurile cibernetice pot fi calificate drept acte (i)legale. **Obiectivul** acestei lucrări este de a stabili și analiza criteriile doctrinare pe care trebuie să le îndeplinească un atac cibernetic pentru a fi considerat o încălcare a articolului 2(4) din Carta ONU. **Ipoteza** acestei lucrări este că, cu cât un atac cibernetic corespunde mai mult criteriilor enunțate de *Tallinn Manual*, cu atât crește posibilitatea considerării sale drept *utilizare a forței* de către statele membre ale ONU.

Criteriile stabilite de doctrină sunt *severitatea*, *imediatitatea*, *directitatea*, *măsurabilitatea*, *caraterul militar*, *legalitatea presumptivă* și *implicarea statului*. Pentru a demonstra relevanța acestui model de analiză în calificarea atacurilor cibernetice moderne, studiul de caz a operațiunii Stuxnet oferă un exemplu elocvent pentru analiza acestor criterii.

3. Metodologia și delimitările cercetării

Prezenta lucrare își propune să analizeze, prin intermediul unui studiu de caz, modul în care un atac cibernetic de anvergură poate fi calificat în conformitate cu normele dreptului internațional privind utilizarea forței. Metodologia cercetării va consta în mai multe etape.

Se vor identifica și analiza criteriile propuse de doctrină pentru calificarea unui atac cibernetic drept uz de forță. Va urma o prezentare detaliată a operațiunii Stuxnet din perspectiva tehnică, a impactului produs și a reacțiilor internaționale. Se va evalua în ce măsură atacul Stuxnet a îndeplinit sau nu criteriile propuse de doctrină, argumentând pentru și contra calificării sale ca uz de forță. Iar, la final, se vor discuta consecințele calificării sau descalificării Stuxnet în calitate de uz de forță pentru dreptul internațional și securitatea cibernetică. Analiza va fi limitată la ipoteza unui atac cibernetic comis de un stat împotriva altui stat și va urmări stabilirea regimului juridic aplicabil acestui act, identificarea criteriilor doctrinare care ar permite calificarea sa drept utilizare a forței în sensul articolului 2(4) din Carta ONU, precum și explorarea alternativelor juridice în situația în care aceste condiții nu sunt îndeplinite.

DEFINITIA, TIPURILE ȘI NATURA ATACURILOR CIBERNETICE

1. Definiția atacurilor cibernetic

În domeniul relațiilor internaționale și al securității cibernetice, definirea precisă a unui atac cibernetic este fundamentală pentru aplicarea normelor de drept internațional, în special în contextul interdicției folosirii forței. Două perspective academice și doctrinare de referință, oferă perspective complementare, dar distincte, care modelează înțelegerea acestui concept. Aceste specificități vor fi, însă, explicate în detaliu în subsecțiunea 3 a acestui capitol, în această parte se vor expune doar definițiile propuse și rațiunea din spatele lor.

Conform analizei realizate Oona Hathaway și colegii săi din școala americană, un atac cibernetic este descris ca fiind „orice acțiune întreprinsă pentru a submina funcțiile unei rețele de calculatoare în scopuri politice sau de securitate națională”.[203] Această definiție pune accentul pe *intenția* atacatorului și pe *scopul strategic*. Contează anume, subminarea funcționalității sistemelor informatice pentru atingerea unor obiective politice sau de securitate. Este o definiție mai largă, care poate cuprinde o gamă variată de operațiuni cibernetice, de la spionaj electronic avansat și furt de date sensibile, până la sabotaj. Esențial este că nu impune în mod necesar un prag al daunelor fizice; simpla perturbare sau compromitere a funcțiilor, dacă este motivată politic sau de securitate națională, ar putea intra sub această umbrelă. Această perspectivă este valoroasă pentru a înțelege natura coercitivă a unor acțiuni cibernetice chiar și atunci când nu provoacă distrugeri imediate.

Pe de altă parte, *Tallinn Manual*, o lucrare elaborată de experți internaționali în drept internațional, sub egida NATO, propune o definiție mai specifică și orientată spre *consecințe*: un atac cibernetic este „o operațiune cibernetică, ofensivă sau defensivă, despre care se așteaptă în mod rezonabil să provoace vătămări sau moarte persoanelor sau daune ori distrugeri obiectelor”.[204] Această a două definiție introduce un prag de *impact fizic sau material*, legând conceptul de atac cibernetic de producerea unor vătămări corporale, decese sau distrugeri concrete de proprietate. Distincția este crucială, deoarece această limitare la efecte fizice severe este esențială pentru a diferenția un *atac cibernetic* (care ar putea declanșa dreptul la autoapărare conform Cartei ONU și obligația de la articolul 5 din Tratat) de *alte operațiuni cibernetice* mai puțin invazive, cum ar fi spionajul cibernetic, manipularea informațiilor sau perturbările temporare care nu cauzează daune ireversibile. *Tallinn Manual* încearcă astfel

[203] Hathaway, Oona A., et al. “The Law of Cyber-Attack.” *California Law Review*, vol. 100, no. 4, 2012, pag.. 822

[204] Schmitt, M-N., 2017, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press, pag. 106

să traseze o linie clară între acțiunile cibernetice care ar putea fi asimilate cu o *utilizare a forței* armate și cele care nu ating acest prag.

Interacțiunea dintre aceste două definiții reflectă dezbaterea continuă din dreptul internațional. Prima definiție oferă o perspectivă strategică amplă asupra amenințării cibernetice, punând accent pe obiectivele subiacente ale actorilor statali. În contrast, definiția din *Tallinn Manual* este mai restrânsă și mai practică pentru a determina momentul în care o acțiune cibernetică depășește sfera intervenției sau a spionajului și intră în domeniul utilizării forței, cu toate implicațiile juridice grave ce decurg din aceasta, inclusiv potențialul de a justifica răspunsuri militare tradiționale. Prin urmare, în timp ce Hathaway ne ajută să înțelegem *ce motivează* acțiunile cibernetice dăunătoare la nivel înalt, *Tallinn Manual* oferă criteriile pentru a evalua *când aceste acțiuni devin suficient de grave* pentru a fi considerate atacuri în sensul cel mai strict al dreptului internațional al conflictelor armate.

2. Tipurile de atacuri cibernetice

Înainte de a analiza consecințele legale și natura unei norme internațional obligatorii care ar putea fi aplicat atacurilor cibernetice, este esențial să clasificăm tipurile de atacuri cibernetice care pot fi efectuate.

Există nenumărate moduri de a utiliza mijloacele cibernetice, unele dintre ele fiind deja cercetate în doctrină:[205] (1) atacuri de tip *Distributed Denial of Service (DDoS)* – realizate în Estonia în 2007 și în Georgia în 2008; (2) *atacuri semantice* – introducerea de informații incorecte (de exemplu, viruși *malware*); (3) *infiltrarea unei rețele informatice securizate* – Stuxnet în 2010.

Atacurile DDoS[206] au fost cea mai răspândită formă de atac cibernetic în ultimii ani. În aceste atacuri, *botnet*-urile coordonate – colecții de mii de computere *zombie* preluate de viruși – atacă serverele vizitând sistematic site-uri desemnate. Atacurile DDoS cauzează de obicei doar inconveniente, dar atacul din 2007 asupra Estoniei[207] a produs și consecințe grave, deoarece țara depindea în mare măsură de tehnologia informației pentru tranzacțiile financiare. Atacul a vizat site-urile guvernamentale, site-urile ziarelor, băncile și sistemele de comunicație. Deși consecințele au fost suficiente pentru a determina mobilizarea unei reacții dipomatice din partea membrilor NATO, doar o minoritate de experți și țări au considerat că acest atac cibernetic ar putea fi suficient de serios pentru a declanșa obligația de apărare colectivă prevăzută la articolul 5.

Atacurile semantice (introducerea de informații incorecte), în care atacatorii introduc subtil informații eronate într-un sistem informatic,[208] sunt mai avansate decât atacurile DDoS. Aceste atacuri determină sistemul să pară că funcționează normal, deși, în fapt, eșuează. Atacatorii manipulează datele stocate sau codul operațional al sistemului, cu scopul de a face sistemul să funcționeze defectuos sau să ofere informații false, menținând în același timp iluzia autenticității. De exemplu, în 1999, Statele Unite au conceput un plan pentru a introduce date false referitoare la ținte în rețeaua de comandă a apărării aeriene a Serbiei,[209] perturbând capacitatea acesteia de a urmări aeronavele NATO. O abordare similară a fost utilizată de Forțele Aeriene Israeliene pe 6 septembrie 2007, în timpul unui atac aerian asupra unei instalații nucleare siriene. Avioanele israeliene au ajuns la țintele lor nedetectate după ce un atac cibernetic anterior a dezactivat sistemele de apărare aeriană ale Siriei.

Provocarea principală constă în identificarea momentului în care a avut loc atacul cibernetic,[210] deoarece perturbarea rămâne ascunsă până când este dezvăluită prin acțiuni cinetice ulterioare. Deoarece atacurile cibernetice semantice sunt adesea însoțite și facilitează operațiuni militare convenționale, este mai probabil ca acestea să fie recunoscute ca atacuri armate și drept utilizare a forței. Virusul Stuxnet[211] a fost un atac semantic, care s-a infiltrat într-un sistem securizat, ceea ce mulți experți consideră că a echivalat cu o utilizare a forței. Acesta corespunde abordărilor ce pun accent pe ținte, efecte și scopuri.

Infiltrarea unei rețele informatice securizate[212] permite atacatorilor să efectueze o varietate de acțiuni. Odată ajunși în interior, aceștia pot introduce informații false sau pot desfășura alte operațiuni, fiind uneori folosite doar ca instrumente de

[205] Hathaway, Oona A., et al. "The Law of Cyber-Attack." *California Law Review*, vol. 100, no. 4, 2012, pp. 817–885.
[206] *Idem*, pag. 837.
[207] *Idem*, pag. 838.
[208] *Idem*, pag. 839.
[209] *Idem*, pag. 838.
[210] Foltz, A., 2012, "Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate", JFQ, Issue 67, pag. 40-48.
Buchan, R., 2012. 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' *Journal of Conflict and Security Law*, *17*(2), pag. 211–227.
[211] Foltz, A., 2012, "Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate", JFQ, Issue 67, 4th quarter 2012, pag. 2;
Buchan, R., 2012. 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' *Journal of Conflict and Security Law*, *17*(2), pag. 2019.
[212] Hathaway, Oona A., et al. "The Law of Cyber-Attack." *California Law Review*, vol. 100, no. 4, 2012, pp. 839.

spionaj. Astfel de atacuri nu distrug întotdeauna rețeaua informatică sau infrastructura pe care o gestionează aceasta. Rețelele infiltrate includ nu doar computere, cum ar fi desktopuri și laptopuri, dar și sisteme critice, adesea neobservate, cum ar fi sistemele de control industriale care susțin infrastructura vieții moderne. Deși spionajul nu este considerat o acțiune legală în dreptul internațional, statele nu insistă asupra calificării spionajului ca o acțiune suficient de gravă pentru a fi considerată utilizare a forței sau ingerință. Cel puțin până când informațiile nu sunt folosite împotriva lor în moduri mult mai dăunătoare. Un exemplu de infiltrare a unei rețele securizate în scopuri diferite a avut loc în 2003, înainte de invazia SUA în Irak. Statele Unite au pătruns în sistemul de e-mail al Ministerului Apărării al Irakului pentru a trimite instrucțiuni ofițerilor irakieni, încurajându-i să se predea pașnic. Această operațiune este un exemplu de atac *command and control*,[213] termen utilizat pentru acțiuni destinate să perturbe capacitatea unui adversar de a-și gestiona și dirija forțele.

3. Natura evolutivă și impactul atacurilor cibernetice

Atacurile cibernetice au devenit o parte integrantă a planificării militare și a acțiunilor de război, așa cum s-a observat în conflicte precum războiul Rusiei împotriva Georgiei (2008), anexarea Crimeei (2014) și invazia Ucrainei (2022). Ele pot provoca daune fizice sau non-fizice și pot amenința securitatea individuală și suveranitatea statală.

Sistemele informatice, rețelele de comunicații și infrastructura critică sunt indispensabile unui stat modern, iar dependența crescândă de acestea creează o vulnerabilitate semnificativă în fața atacurilor cibernetice. Acestea pot perturba sau distruge funcționarea serviciilor esențiale, cum ar fi rețelele electrice, sistemele financiare sau infrastructura militară. Atacurile cibernetice sofisticate pot duce la pierderi economice semnificative, scurgeri de informații naționale sensibile și perturbări fizice ale infrastructurii critice, amenințând economia, confidențialitatea și încrederea cetățenilor în sistemele democratice, așa cum au demonstrat cazuri precum SolarWinds (2020)[214] și Heartbleed (2014).[215]

Michael Schmitt subliniază că, deși operațiunile cibernetice nu sunt cinetice și nu utilizează *arme* tradiționale, ele pot avea rezultate extrem de distructive, chiar letale, ceea ce le poate califica drept *armate* dacă duc la rănirea sau decesul persoanelor, sau la deteriorarea sau distrugerea proprietății. Chiar și o operațiune cibernetică ce *dezactivează* un obiect, fără a provoca daune fizice directe, poate fi considerată un atac, mai ales dacă necesită reparații complexe ale infrastructurii cibernetice.

Severitatea impactului este principalul aspect utilizat pentru a diferenția între diversele arme sau atacuri cibernetice, fiind adesea o abordare *post factum*. Dificultatea de a aplica definițiile tradiționale ale războiului, la războiul cibernetic provine din varietatea actorilor implicați (statali și non-statali) și din provocările legate de atribuire. Chiar și incidentele cibernetice de intensitate scăzută, care nu ating pragul unui atac armat, pot permite contramăsuri proporționale și fără implicarea forței. Cu toate acestea, efectul cumulativ al atacurilor frecvente și ușor perturbatoare ar putea, în anumite condiții, să atingă nivelul unui atac armat dacă distrug încrederea generală într-un sistem, ceea ce ar fi putut fi scopul lor principal.

Fundamentul normativ – Articolul 2(4) din Carta ONU. Interpretarea tradițională a interdicției utilizării forței

1. Introducere: Semnificația articolului 2(4) în ordinea juridică internațională

Articolul 2(4) din Carta Organizației Națiunilor Unite reprezintă o piatră de temelie a arhitecturii juridice internaționale post-1945, fiind recunoscut universal ca norma fundamentală a *jus contra bellum*.[216] Această prevedere interzice

[213] *Idem*, pag. 838.

[214] Atacul SolarWinds din 2020 a fost unul dintre cele mai semnificative și sofisticate atacuri de tip *supply chain* (lanț de aprovizionare) cunoscute. Atacatorii, despre care se crede că ar fi o grupă susținută de guvernul rus (Serviciul de Informații Externe)au compromis sistemele companiei SolarWinds. Ei au injectat un cod malițios (o denumit *SUNBURST*) într-o actualizare legitimă a platformei de management de rețea Orion, utilizată pe scară largă de agenții guvernamentale și companii private din întreaga lume.

[215] Heartbleed a fost o vulnerabilitate critică (denumită CVE-2014-0160) descoperită în biblioteca software OpenSSL în aprilie 2014. OpenSSL este o bibliotecă criptografică open-source larg utilizată pentru implementarea protocoalelor SSL/TLS, care asigură comunicarea securizată pe internet. Bug-ul se afla în implementarea extensiei *Heartbeat* a OpenSSL. O eroare de programare permitea unui atacator să trimită o cerere *heartbeat* formatată malițios unui server sau client vulnerabil. Acest lucru ducea la faptul că serverul trimitea înapoi mai multe date din memoria sa decât ar fi trebuit – până la 64 KB de memorie brută la fiecare cerere.

[216] *Dreptul împotriva războiului*, în latină.

statelor amenințarea cu forța sau utilizarea forței în relațiile internaționale, stabilind un pilon central al sistemului de securitate colectivă al ONU. Textul său este explicit: „Toți Membrii Organizației se vor abține, în relațiile lor internaționale, de a recurge la amenințarea cu forța sau la folosirea forței împotriva integrității teritoriale sau independenței politice a oricărui stat, ori în orice alt mod incompatibil cu scopurile Națiunilor Unite". Scopul primordial al acestei interdicții este menținerea păcii și securității internaționale, prevenind repetarea conflictelor devastatoare care au marcat prima jumătate a secolului XX.

Adoptarea Cartei ONU în 1945 a reprezentat un moment de ruptură paradigmatică în dreptul internațional. Înainte de această dată, sistemul juridic internațional era caracterizat de un *jus ad bellum*[217] permisiv, care acorda statelor un drept aproape nelimitat de a recurge la război ca instrument de politică externă.[3] Experiența tragică a celor două războaie mondiale a demonstrat însă eșecul acestui sistem și a generat o voință colectivă de a institui un cadru juridic mai restrictiv. Astfel, Carta a marcat o tranziție decisivă către un regim de *jus contra bellum*, unde utilizarea forței este, în principiu, interzisă.[218] Această schimbare nu a fost doar o ajustare minoră, ci o profundă transformare normativă, reflectând o traumă globală colectivă și un angajament ferm față de pace. Interdicția forței, cu excepția dreptului inerent la autoapărare (articolul 51) și a acțiunilor autorizate de Consiliul de Securitate al ONU, a devenit un principiu fundamental, a cărui universalitate și caracter de *jus cogens*[219] sunt consecința directă a lecțiilor învățate din conflictele catastrofale ale secolului al XX-lea.

2. Interpretarea tradițională a articolului 2(4) din Carta ONU

Articolul 2(4) din Carta ONU interzice atât *amenințarea cu forța*, cât și *utilizarea forței.*[220] Deși Carta nu oferă definiții explicite ale acestor termeni, interpretarea tradițională și jurisprudența internațională au contribuit la clarificarea lor. Amenințarea cu forța se referă la o declarație explicită sau implicită de a folosi forța, care este credibilă și are scopul de a constrânge un stat să acționeze într-un anumit mod. Nu orice demonstrație de forță militară constituie o amenințare; este necesar ca aceasta să transmită o intenție clară de a recurge la forță în cazul nerespectării unor cereri.[221]

Utilizarea forței, pe de altă parte, reprezintă acțiunea efectivă de recurgere la forță armată. Curtea Internațională de Justiție (CIJ) a subliniat într-o Aviz consultativ privind legalitatea amenințării sau utilizării armelor nucleare că interdicția „se aplică oricărei utilizări a forței, indiferent de armele folosite".[222] Această formulare este crucială, deoarece sugerează o interpretare mai largă a conceptului de *forță* decât simpla forță cinetică, deschizând calea pentru includerea unor forme non-tradiționale de forță, atâta timp cât efectele produse sunt comparabile cu cele ale unei acțiuni militare convenționale. Ambiguitatea deliberată a Cartei în definirea exactă a *amenințării cu forța* și *utilizării forței* permite o flexibilitate esențială în aplicarea sa la scenarii viitoare neprevăzute. Această flexibilitate, deși poate genera incertitudini, este vitală pentru relevanța pe termen lung a Cartei într-un peisaj tehnologic și strategic în continuă evoluție, permițând ca interpretarea tradițională să se adapteze noilor realități.

2.1. Conceptele de *integritate teritorială* și *independență politică*

Articolul 2(4) protejează în mod explicit *integritatea teritorială* și *independența politică* a statelor, subliniind legătura directă dintre interdicția forței și principiul fundamental al suveranității statale. Integritatea teritorială se referă la inviolabilitatea frontierelor și a teritoriului unui stat. Orice incursiune militară, ocupație sau achiziție teritorială rezultată din amenințarea cu forța sau utilizarea forței este strict interzisă și nu va fi recunoscută ca legală. Declarația Adunării Generale ONU privind principiile de drept internațional privind relațiile amicale și cooperarea între state, adoptată în 1970 (Rezoluția 2625 (XXV)), reiterează datoria fiecărui stat de a se abține de la amenințarea sau utilizarea forței pentru a viola frontierele internaționale existente.

Independența politică vizează dreptul inalienabil al unui stat de a-și determina propriul sistem politic, economic, social și cultural, fără interferențe externe.[223] Intervenția armată și toate celelalte forme de ingerință sau amenințări împotriva personalității statului sau împotriva elementelor sale politice, economice și culturale sunt con-

[217] *Dreptul la război* sau *dreptul de a merge la război*, în latină.
[218] "The Use of Force in International Law." *OpenLearn*.
[219] *Drept imperativ*, în latină.
[220] Schmitt, M-N., 2017, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press, pag. 45-54.
[221] Curtea Internațională de Jurstiție. *Legality of the Threat or Use of Nuclear Weapons*. Aviz consultativ din 8 iulie 1996, para. 47.
[222] *Idem*, para. 48.
[223] Adunarea Generală a ONU. *Declarația privind principiile de drept internațional privind relațiile amicale și cooperarea între state în conformitate cu Carta Organizației Națiunilor Unite*. Rezoluția 2625 (XXV) din 24 octombrie 1970.

siderate încălcări ale dreptului internațional. Declarația Adunării Generale ONU privind inadmisibilitatea intervenției în afacerile interne ale statelor și protecția independenței și suveranității lor, adoptată în 1965 (Rezoluția 2131 (XX)), condamnă explicit astfel de acțiuni. Această interconectare a suveranității cu interdicția forței demonstrează că sfera de aplicare a articolului 2(4) depășește invazia militară directă, incluzând și forme mai subtile de coerciție care subminează capacitatea unui stat de a se autoguverna. Această interpretare cuprinzătoare este esențială pentru menținerea păcii internaționale, în special în contextul apariției unor noi tipuri de amenințări non-cinetice.

2.2. Clauza reziduală: „Orice alt mod incompatibil cu scopurile Organizației Națiunilor Unite"

Clauza „ori în orice alt mod incompatibil cu scopurile Națiunilor Unite" extinde semnificativ sfera de aplicare a interdicției forței dincolo de cazurile specifice de încălcare a integrității teritoriale sau independenței politice. Această formulare flexibilă acoperă orice utilizare a forței care contravine scopurilor mai largi ale ONU, cum ar fi menținerea păcii și securității internaționale, dezvoltarea relațiilor amicale între națiuni și promovarea cooperării internaționale.

Această clauză reziduală funcționează ca un mecanism crucial de adaptare a Cartei. Recunoscând că redactorii Cartei nu puteau anticipa toate amenințările viitoare la adresa păcii și securității, această prevedere permite o interpretare evolutivă a conceptului de *forță*. Ea asigură că interdicția rămâne relevantă și aplicabilă chiar și în fața unor noi modalități de agresiune sau coerciție care ar putea apărea, chiar dacă acestea nu se încadrează strict în categoriile tradiționale de încălcare a integrității teritoriale sau a independenței politice. Această flexibilitate este deosebit de importantă în contextul amenințărilor emergente, cum ar fi cele din spațiul cibernetic, oferind baza legală pentru a argumenta că anumite acțiuni non-cinetice, dacă au efecte comparabile cu utilizările tradiționale ale forței și sunt incompatibile cu scopurile ONU, intră sub incidența interdicției articolului 2(4).

3. JURISPRUDENȚA ȘI PRACTICA STATELOR PRIVIND APLICAREA ART. 2(4) DIN CARTA ONU

3.1. Jurisprudența internațională relevantă.

Cazul *Activități militare și paramilitare în și împotriva Nicaraguei (Nicaragua v. Statele Unite ale Americii)* din 1986, judecat de Curtea Internațională de Justiție, reprezintă o hotărâre fundamentală în interpretarea articolului 2(4) din Carta ONU și a dreptului cutumiar privind utilizarea forței.[224] Această decizie a adus clarificări esențiale în ceea ce privește delimitarea dintre *utilizarea forței* și *atac ar mat*.

Curtea a stabilit o distincție crucială între aceste două concepte. A statuat că doar „cele mai grave forme de utilizare a forței" constituie un atac armat, care declanșează dreptul inerent la autoapărare, conform articolului 51 al Cartei.[225] Prin contrast, formele mai puțin grave de utilizare a forței, deși interzise de articolul 2(4), nu justifică un răspuns armat în autoapărare, ci pot permite adoptarea unor contramăsuri non-armate.

În acest caz, CIJ a considerat că finanțarea, antrenarea și aprovizionarea grupurilor de gherilă (*contras*) de către Statele Unite, care operau împotriva Nicaraguei, au constituit o *utilizare a forței* împotriva statului nicaraguan, dar nu au atins pragul unui *atac armat* direct.[226] În schimb, acțiunea de minare a porturilor nicaraguane de către SUA a fost calificată drept o utilizare directă a forței.[227]

Un aspect central al raționamentului CIJ, deși explicit menționat în contextul atacului armat, a fost importanța *scalei și efectelor* (*the scale and the effects*) unei acțiuni pentru a determina dacă aceasta atinge pragul de *utilizare a forței* sau *atac armat*.[228] Acest standard, bazat pe evaluarea cantitativă și calitativă a consecințelor unei acțiuni, a devenit fundamental pentru evaluarea legalității acțiunilor care nu implică neapărat forță armată convențională. Hotărârea CIJ în cazul Nicaragua ilustrează modul în care dreptul internațional, prin interpretare judiciară, se adaptează la noi provocări. Această decizie a oferit un cadru flexibil, bazat pe *efecte*, care este crucial pentru evaluarea formelor non-tradiționale de forță, chiar dacă speța în sine a vizat sprijinul convențional și indirect acordat grupurilor armate.

Deși articolul 2(4) al Cartei ONU utilizează termenul *forță* fără calificativul *armată*, interpretarea tradițională, susținută de *travaux préparatoires*[229] ale Cartei, a considerat că interdicția se referă în primul rând la forța armată. Propunerile de a include coerciția economică sau politică în sfera de aplicare a articolului 2(4) au fost respinse atât în timpul Conferinței de la San Francisco din

[224] CIJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, 1986.
[225] *Idem*, para. 191.
[226] *Idem*, para. 194-196.
[227] *Idem*, para. 268.
[228] *Idem*, para. 195.
[229] *Lucrări premergătoare*, din latină.

1945, cât și ulterior în cadrul discuțiilor pentru Declarația privind relațiile amicale.[230]

Prin urmare, coerciția economică sau diplomatică, deși pot încălca alte principii ale dreptului internațional, cum ar fi principiul non-ingerinței, nu sunt considerate, în general *uutilizări ale forței* în sensul articolului 2(4).[231] Declarația Adunării Generale ONU privind inadmisibilitatea intervenției în afacerile interne ale statelor din 1965 condamnă utilizarea măsurilor economice sau politice pentru a constrânge un stat, dar nu le califică drept *utilizare a forței* în sensul strict al Cartei. Această delimitare reflectă o alegere deliberată a statelor de a limita sfera de aplicare a interdicției la forța armată.

Cu toate acestea, evoluția tehnologică și apariția unor noi forme de coerciție au reaprins dezbaterile. Anumite operațiuni cibernetice, de exemplu, pot cauza consecințe economice severe, fără a implica neapărat forță cinetică.[232] Această capacitate a noilor tehnologii de a produce efecte comparabile cu cele ale forței armate tradiționale, chiar și prin mijloace non-cinetice, creează o tensiune cu interpretarea tradițională restrictivă. Această situație subliniază provocarea de a aplica un text juridic restrictiv unui peisaj de amenințări în continuă transformare. Deși interpretarea tradițională exclude în mare măsură coerciția non-armată, evoluția conceptului de *forță* se referă tocmai la modul în care această viziune restrictivă este contestată și potențial extinsă de gravitatea efectelor pe care noile tehnologii le pot produce.

3.2 Practica statelor

Declarațiile Adunării Generale ONU, deși nu sunt instrumente juridice obligatorii *per se*, joacă un rol crucial în cristalizarea dreptului cutumiar și în interpretarea normelor Cartei. Ele reflectă consensul statelor membre și oferă ghidare autoritară, validată uneori explicit de jurisprudența CIJ. Vor urma câteva declarații relevante pentru stabilirea practicii statelor din Organizația Națiunilor Unite.

Declarația privind inadmisibilitatea intervenției în afacerile interne ale statelor și protecția independenței și suveranității lor a fost adoptată prin Rezoluția 2131 (XX) din 1965). Această declarație condamnă intervenția armată ca fiind sinonimă cu agresiunea și contrară principiilor cooperării internaționale. De asemenea, interzice statelor să organizeze, să asiste, să finanțeze sau să tolereze activități subversive, teroriste sau armate îndreptate spre răsturnarea violentă a regimului unui alt stat. Aceasta extinde înțelegerea acțiunilor interzise dincolo de invazia directă.

Declarația privind principiile de drept internațional privind relațiile amicale și cooperarea între state în conformitate cu Carta Organizației Națiunilor Unite a fost adoptată prin în 1970. Această declarație, adoptată pentru a celebra a 25-a aniversare a ONU, a codificat principii fundamentale ale dreptului internațional, inclusiv interdicția utilizării forței și principiul non-ingerinței. Ea reiterează datoria statelor de a se abține de la amenințarea sau utilizarea forței împotriva integrității teritoriale sau independenței politice și de a nu organiza sau încuraja forțe neregulate sau bande armate pentru incursiuni pe teritoriul altui stat. Curtea Internațională de Justiție a făcut referire explicită la această rezoluție ca dovadă a obligațiilor cutumiare paralele cu cele din Carta ONU.

Declarația privind consolidarea eficacității principiului abținerii de la amenințarea sau utilizarea forței în relațiile internaționale din 1987 reconfirmă datoria fiecărui stat de a se abține de la amenințarea sau utilizarea forței împotriva integrității teritoriale sau independenței politice a oricărui stat și îndeamnă statele să soluționeze pașnic disputele internaționale. Ea subliniază importanța deplină a prevederilor Cartei ONU în domeniul menținerii păcii și securității internaționale.

Aceste declarații, prin reafirmarea și elaborarea constantă a principiilor articolului 2(4) și ale neintervenției, demonstrează o practică statală și un *opinio juris* consecvente. Acest lucru consolidează rigoarea interdicției, recunoscând în același timp implicit necesitatea adaptării sale la noi forme de coerciție. Prin clarificarea scopului tradițional al interdicției, ele pregătesc terenul pentru înțelegerea modului în care formele viitoare, neconvenționale de forță, precum atacurile cibernetice, ar putea fi evaluate.

Pentru a evalua dacă o acțiune, inclusiv o operațiune cibernetică, constituie o utilizare a forței, criteriul *scală și efecte* este fundamental. Acesta permite o analiză adaptată la realitățile contemporane, conform jurisprudenței CIJ și lucrărilor doctrinare precum *Tallinn Manual*.

Criteriul *scalei* se referă la amploarea și intensitatea acțiunii desfășurate, incluzând factori cantitativi precum numărul de sisteme afectate,

[230] Delerue, F. "The Threshold of Cyber Warfare: from Use of Cyber Force to Cyber Armed Attack." *Cyber Operations and International Law*, Cambridge University Press, 2020, Capitolul 6.

[231] Adunarea Generală a ONU. (1965). *Declarația privind inadmisibilitatea intervenției în treburile interne ale statelor și protecția independenței și suveranității acestora*. Rezoluția 2131 (XX).

[232] Valo, J. *Cyber Attacks and the Use of Force in International Law*. 2014. University of Helsinki.

durata operațiunii și resursele utilizate. O scară suficient de extinsă poate sugera o intenție coercitivă sau distructivă, aspect esențial pentru a încadra juridic o acțiune drept utilizare a forței, fiind susținut atât de jurisprudența CIJ în cauza *Activități militare și paramilitare*,[233] cât și de Regula 69 din *Tallinn Manual*.[234] Pe de altă parte, criteriul *efectelor* se concentrează pe consecințele calitative și cantitative ale operațiunii cibernetice. Acestea pot varia de la daune fizice semnificative și pierderi de vieți omenești, până la perturbări grave ale infrastructurii critice sau afectarea profundă a capacității de guvernare a unui stat. Dacă efectele unei operațiuni cibernetice sunt comparabile cu cele ale unui atac armat convențional, aceasta poate fi considerată o formă de utilizare a forței, indiferent de mijloacele tehnice folosite. Acest principiu este susținut de *Avizul consultativ* al CIJ privind armele nucleare,[235] de jurisprudența deja menționată,[236] dar și de doctrină.[237] Prin urmare, acest cadru analitic oferă o punte de legătură între normele tradiționale de drept internațional și noile provocări generate de evoluția tehnologică, permițând adaptarea regulilor existente la realitățile contemporane ale conflictului cibernetic.

4. CONCLUZII PRIVIND FUNDAMENTUL NORMATIV TRADIȚIONAL AL INTERDICȚIEI UTILIZĂRII FORȚEI

Articolul 2(4) din Carta ONU rămâne norma cardinală a dreptului internațional, instituind o interdicție aproape absolută a amenințării cu forța și a utilizării forței în relațiile internaționale. Această interdicție, care constituie fundamentul sistemului modern de securitate colectivă, este susținută de principiile suveranității statale și neintervenției. De-a lungul timpului, interpretarea sa a fost consolidată și nuanțată prin jurisprudența Curții Internaționale de Justiție, în special în cazul Nicaragua, și prin declarațiile Adunării Generale ONU, precum cele privind Relațiile Amicale și Inadmisibilitatea Intervenției.

Interpretarea tradițională a articolului 2(4) s-a concentrat în principal pe forța armată convențională. Cu toate acestea, dezvoltarea conceptelor precum *scala și efectele* unei acțiuni, derivate din jurisprudența CIJ, a conferit normei o flexibilitate necesară pentru a evalua noi forme de coerciție. Această adaptabilitate a permis ca o normă fundamentală, formulată într-o epocă pre-digitală, să rămână relevantă în fața provocărilor contemporane. Rezistența și capacitatea de adaptare a acestei norme fundamentale sunt demonstrate de modul în care ea a fost constant reafirmată și subtil ajustată prin decizii judiciare și declarații ale ONU. Această bază normativă solidă este esențială pentru abordarea provocărilor actuale, inclusiv a celor generate de operațiunile cibernetice. Deși natura *forței* poate evolua, interdicția și criteriile de evaluare a încălcării sale oferă un cadru juridic robust. Înțelegerea acestui fundament normativ tradițional este, prin urmare, o condiție prealabilă critică pentru analiza aplicabilității principiilor juridice stabilite la caracteristicile unice ale războiului cibernetic.

DREPTUL INTERNAȚIONAL APLICABIL ATACURILOR CIBERNETICE

1. Utilizare a forței. Criterii propuse de doctrină

Cum am menționat deja, utilizarea forței în relațiile internaționale este reglementată de articolul 2(4) din Carta Națiunilor Unite, care stipulează că statele membre trebuie să se abțină, în relațiile lor internaționale, de la amenințarea sau utilizarea forței împotriva integrității teritoriale sau independenței politice a oricărui stat sau într-o altă manieră incompatibilă cu scopurile Națiunilor Unite.

Curtea Internațională de Justiție (CIJ) a hotărât că articolul 2(4) din Carta Națiunilor Unite, care interzice utilizarea forței, și articolul 51, care abordează dreptul la autoapărare, se aplică *oricărei utilizări a forței, indiferent de armele folosite*. [238] Deși Carta Națiunilor Unite nu definește explicit forța, aceasta este în general înțeleasă ca incluzând forța armată, cu exemple oferite chiar

[233] CIJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, 1986, para. 195.

[234] Schmitt, M-N., 2017, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press, pag. 202.

[235] Curtea Internațională de Jurstiție. *Legality of the Threat or Use of Nuclear Weapons*. Aviz consultativ din 8 iulie 1996, para. 92.

[236] CIJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, 1986, para. 195.

[237] Buchan, R., 2012. 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' *Journal of Conflict and Security Law*, *17*(2);
Hathaway, Oona A., et al. "The Law of Cyber-Attack." *California Law Review*, vol. 100, no. 4, 2012.
Ducaru, S. "Can a Cyberattack Become an Act of War? European and Trans-Atlantic Perspectives.'' *Romanian Journal of European Affairs*, Vol.2, No.1 (2024).

[238] ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, 1986, para. 118.

în Carte. Articolul 42 permite Consiliului de Securitate al ONU să folosească forța armată în demonstrații, blocade și alte operațiuni aeriene, navale sau terestre atunci când măsurile pașnice se dovedesc a fi insuficiente.

The *Tallinn Manual*[239] face referire la un set de ghiduri și principii destinate înțelegerii modului în care dreptul internațional se aplică operațiunilor cibernetice. A fost dezvoltat de un grup de experți și academicieni internaționali, convocat de NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)[240] în Tallinn, Estonia. Manualul oferă o analiză a modului în care dreptul internațional existent, în special dreptul *conflictelor armate* și *dreptul internațional umanitar*, ar trebui să se aplice războiului cibernetic și operațiunilor cibernetice între state.

Grupul de experți internaționali care au lucrat la acest manual au decis asupra unui set de criterii[241] pe care un atac cibernetic ar trebui să le respecte pentru a constitui utilizare a forței. Aceste criterii sunt: (1) *severitatea*; (2) *imediatitatea*; (3) *nemijlocirea (directitatea);* (4) *invazivitatea*; (5) *măsurabilitatea efectelor*; (6) *legalitatea prezumptivă*; (7) *caracterul militar*; (8) *implicarea (vădită a) statului*.

Severitatea (*Severity*)[242]

Acest criteriu se referă la gravitatea consecințelor atacului cibernetic. Pentru a fi considerat o utilizare a forței, ar trebui să existe cel puțin daune fizice aduse persoanelor sau proprietății. De exemplu, atacul Stuxnet a fost considerat o utilizare a forței datorită daunelor fizice provocate programului nuclear iranian, care a fost întârziat cu câțiva ani. Atacurile cibernetice care duc la decese, răniri sau distrugere fizică se califică drept utilizare a forței. Michael Schmitt argumentează că operațiunile cibernetice care generează consecințe violente, cum ar fi rănirea sau decesul persoanelor, sau deteriorarea sau distrugerea proprietății, îndeplinesc criteriul de a fi *armate*. Un atac cibernetic ce provoacă explozia unei centrale electrice sau prăbușirea unor avioane ar putea constitui un atac armat, spre deosebire de cele care cauzează doar daune economice sau sociale. Nicholas Tsagourias subliniază că un atac armat este definit de gravitatea și efectele sale, nu de instrumentul utilizat, iar un atac cibernetic ce provoacă distrugeri umane și/sau materiale substanțiale poate fi echivalat cu un atac armat.[243]

Imediatitatea (*Immediacy*)[244]

Acest criteriu evaluează cât de repede se manifestă consecințele atacului. Cu cât efectele sunt mai rapide, cu atât statele au mai puține oportunități de a căuta soluții pașnice. În cazul Stuxnet, daunele s-au manifestat pe parcursul a săptămâni sau luni, permițând timp pentru măsuri de atenuare, ceea ce ar sugera că nu ar fi considerat o utilizare a forței pe baza acestui factor. De asemenea, este dificil de judecat iminența în contextul apărării preventive în cazul atacurilor cibernetice.

Directitatea (*Directness*)[245]

Se referă la conexiunea cauzală directă între acțiunile cibernetice și efectele produse. În cazul Stuxnet, a existat o conexiune cauzală directă între vierme și centrifugile deteriorate. Cu toate acestea, în general, stabilirea unei cauzalități directe poate fi dificilă în spațiul cibernetic, deoarece distrugerea este adesea realizată prin efecte indirecte.

Invazivitatea (*Invasiveness*)[246]

Acest criteriu măsoară gradul în care operațiunea cibernetică a pătruns în sistemele și infrastructura unui stat. Stuxnet a reprezentat o intruziune semnificativă în suveranitatea iraniană, vizând sisteme izolate fizic (*air-gapped)*.

Măsurabilitatea efectelor (*Measurability of effects*)[247]

Consecințele atacului ar trebui să fie evidente și cuantificabile. În cazul Stuxnet, consecințele au fost cuantificabile și identificabile, chiar și luând în considerare rata ridicată de eșec a centrifugilor. Cu toate acestea, în alte cazuri, efectele atacurilor cibernetice pot fi dificil de măsurat.

Legalitatea prezumtivă (*Presumptive legitimacy*)[248]

Acest criteriu sugerează că acțiunile ar trebui să fie, pe cât posibil, departe de acțiunile legale

[239] Schmitt, M-N., 2017, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press.
[240] CCDCOE, *The Centre is the first International Military Organization hosted by Estonia*.
[241] *Idem*, pag. 48.
[242] Schmitt, M-N., 2017, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press, pag. 48
[243] Tsagourias, N. "Cyber Attacks, Self-Defence and the Problem of Attribution." Journal of Conflict and Security Law, vol. 17, no. 2, 2012, pp. 235.
[244] *Idem*, pag. 49.
[245] *Ibidem.*
[246] *Idem*, pag. 49-50.
[247] *Idem*, pag. 50-51.
[248] *Idem*, pag. 51.

permise de ordinea internațională. Stuxnet a lipsit de legitimitate prezumtivă, deoarece nu există o acceptare internațională cutumiară pentru deteriorarea instalațiilor nucleare ale unui alt stat fără autorizarea Consiliului de Securitate al ONU sau în contextul autoapărării.

Caracterul militar (*Military character*)[249]

Este mai probabil ca o operațiune realizată prin mijloace militare să fie acceptată ca utilizare a forței. Michael Schmitt sugerează că respectarea aparentă a principiilor Legii Conflictelor Armate (necesitatea militară, distincția, proporționalitatea) ar putea fi un factor suplimentar luat în considerare de state. Deși operațiunile cibernetice nu sunt cinetice și nu folosesc *arme* tradiționale, ele pot avea rezultate extrem de distructive, chiar letale, ceea ce le poate califica drept *armate*.

Implicarea (vădită a) statului *(Involvement (evident of) the state)*[250]

Se referă la o conexiune mai strânsă între stat și operațiunea cibernetică. Deși niciun stat nu și-a asumat responsabilitatea pentru Stuxnet, scopul și designul viermelui sugerează puternic implicarea statală. Atribuirea este o precondiție crucială pentru analiza utilizării forței. Dificultatea atribuirii este o provocare semnificativă pentru declanșarea răspunsurilor colective, cum ar fi cele prevăzute de articolul 5 al NATO. Atribuirea poate fi tehnică, legală și politică, implicând identificarea atacatorilor, afilierile lor și legăturile cu statele.

Deși aceste criterii sunt utilizate de multe organizații, actori și experți, există unele criticifață de ele din cauza *maleabilității* lor.[251] Unele dintre acestea pot fi, de fapt, folosite într-un mod convingător pentru a nega impactul unui atac cibernetic. Există academicieni care au propus abordări diferite pentru a califica un comportament greșit ca utilizare a forței.

Unele dintre acestea sunt:[252] abordarea bazată *pe efecte* – efectele ar trebui să fie echivalente cu daunele cauzate prin mijloace cinetice (arme tradiționale); abordarea bazată pe ținte – scopul atacului (chiar dacă a eșuat) ar trebui să fie o țintă militară sau o infrastructură critică; abordarea bazată pe *instrumente* – cât de analogică este arma cu armele militare convenționale; abordarea *forței ca daune intenționate/* abordarea scopului[253] – scopul acestei abordări este de a se concentra pe intenție (nu pe efect).

După cum se poate observa în multe dintre strategiile naționale de securitate cibernetică ale statelor, există state care aplică principii similare cu cele din *Tallinn Manual* atunci când evaluează natura atacurilor cibernetice, în timp ce altele preferă abordări mai simple. Fragmentarea dreptului internațional actual și pozițiile politice asupra războiului cibernetic sunt cauzate de interesele naționale, situația geopolitică a fiecărui stat și modul în care își desfășoară politica externă.

2. Calificare juridică alternativă. Intervenția interzisă vs utilizare a forței.

Pe lângă propunerea doctrinei de a categoriza atacurile cibernetice drept utilizare a forței, există si o încadrare juridică alternativă plauzibilă, a cărei mențione o consider necesară. Intervenția unui stat în afacerile interne ale altuia are scopul de a impune voința acestuia din urmă asurpa unui alt stat suvernan. Astfel de intervenții pot lua forme diverse, inclusiv utilizarea forței, coerciția economică, spionajul sau propaganda.

Principiul non-ingerinței este recunoscut ca o normă a dreptului internațional cutumiar,[254] ceea ce înseamnă că este obligatoriu pentru toate statele, indiferent de obligațiile lor tratatale. Acest principiu a fost reafirmat în numeroase instrumente internaționale, inclusiv în Declarația Națiunilor Unite privind Principiile Dreptului Internațional referitoare la Relațiile Amicale și Cooperarea între State, în conformitate cu Carta Națiunilor Unite, în numeroase rezoluții ale ONU și în practica constantă dintre state.

Curtea Internațională de Justiție a definit principiul non-ingerinței în cazul *Nicaragua v. Statele Unite*,[255] hotărând că o intervenția ilegală referă la chestiuni în care fiecare stat are discreție suverană, cum ar fi alegerea sistemelor politice, economice, sociale și culturale, precum și formularea politicii externe. Intervenția devine ilegală atunci când folosesc măsuri coercitive pentru a

[249] *Idem*, pag. 51.
[250] *Idem*, pag. 51.
[251] Hathaway, Oona A., et al. "The Law of Cyber-Attack." *California Law Review*, vol. 100, no. 4, 2012, pp. 830; Nguyen, R.,"Navigating 'Jus Ad Bellum' in the Age of Cyber Warfare." *California Law Review* 101, no. 4, pag. 1124.
[252] Nguyen, R.,"Navigating 'Jus Ad Bellum' in the Age of Cyber Warfare." *California Law Review* 101, no. 4, pag.1117.
[253] *Idem*, pag. 1124.
[254] ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, 1986, para. 123.
[255] ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, 1986, para. 111.

influența aceste decizii, care trebuie să rămână libere. CIJ a mai declarat că un act care încalcă principiul cutumiar al non-ingerinței va încălca și principiul abținerii de la utilizarea forței în relațiile internaționale, dacă implică direct sau indirect utilizarea forței.

Unele atacuri cibernetice pot, de asemenea, să fie considerate intervenție interzisă dacă scopul acestora este de a forța un stat să-și schimbe politica. De exemplu, atacurile cibernetice care vizează infrastructura critică — cum ar fi rețelele electrice sau sistemele financiare — ar putea fi considerate o încălcare dacă acestea provoacă daune economice semnificative sau perturbă operațiunile guvernamentale. Deși aceste acțiuni de intervenție sunt ilegale, nu ating pragul utilizării forței decât dacă implică violență fizică sau distrugere care cauzează daune semnificative.

Distincția dintre aceste două categorii este importantă deoarece, deși intervenția interzisă implică un comportament greșit, aceasta nu comportă aceleași consecințe ca utilizarea forței. Acest lucru este în concordanță cu *principiul proporționalității* în dreptul internațional,[256] care previne escaladarea disputelor politice în conflicte militare. Astfel, utilizarea forței nu trebuie considerată un instrument sau o amenințare politică obișnuită. Potențialul său de a provoca daune ireparabile păcii și securității internaționale face ca aceasta să fie o ultimă soluție în abordarea conflictelor între state. CIJ și Carta ONU subliniază ambele că utilizarea forței trebuie abordată cu cea mai mare prudență, asigurându-se că mijloacele pașnice de rezolvare sunt epuizate înainte de orice recurs la acțiuni militare. Reacțiile permise la intervențiile interzise sunt *contramăsurile*, conform *ARSIWA*[257] - Articole despre responsabilitatea statelor pentru conduită interzisă de dreptul internațional, hotărârilor CIJ și Rezoluțiilor Adunării Generale a ONU.[258] *Principiile proporționalității* și *necesității* ar fi justificat (până acum) doar contramăsuri non-armate în cazul intervențiilor non-armate, spre deosebire de dreptul unui stat la autoapărare atunci când este supus utilizării forței. Dacă un stat abuzează de dreptul său de a recurge la contramăsuri sau autoapărare într-o manieră care depășește ceea ce este proporționat sau necesar, va fi (el însuși) responsabil pentru angajarea într-un comportament greșit internațional.[259]

STUDIUL DE CAZ STUXNET: ANALIZA UNUI ATAC CIBERNETIC CU IMPACT FIZIC

5.1. Prezentarea generală a atacului Stuxnet: obiective, cronologie și ținte

Stuxnet, descoperit pe 17 iunie 2010, reprezintă un vierme informatic de o sofisticare excepțională, considerat pe scară largă prima armă cibernetică din lume capabilă să genereze distrugeri fizice substanțiale infrastructurii critice.[260] Spre deosebire de formele tradiționale de *malware*, care se concentrează pe furtul de date, perturbarea rețelelor sau spionaj, Stuxnet a fost proiectat cu un scop precis: sabotajul fizic direct. Această capacitate de a traduce acțiuni digitale în consecințe cinetice a marcat un moment fundamental în evoluția amenințărilor cibernetice, transformând o ipoteză teoretică într-o realitate operațională.[261]

Apariția Stuxnet a modificat fundamental înțelegerea conflictelor cibernetice. Anterior, discuțiile se axau preponderent pe impactul asupra sistemelor informaționale – breșe de date, atacuri de tip denial-of-service sau spionaj digital. Stuxnet, prin distrugerea fizică a centrifugelor iraniene, a demonstrat o nouă dimensiune a agresiunii cibernetice: atacurile cyber-fizice, unde acțiunile din spațiul digital au consecințe directe și tangibile în lumea reală. Această schimbare nu se limitează la perturbarea digitală; ea semnalează o extindere a conceptului de *câmp de luptă* dincolo de domeniile fizice tradiționale, incluzând acum infrastructura digitală care susține societatea modernă.[262] Această realitate impune o reevaluare profundă a strategiilor de securitate națională, forțând statele să ia în considerare noi vectori de atac și să recunoască convergența tot mai accentuată dintre securitatea cibernetică și cea fizică, o separare care devine din ce în ce mai artificială.

[256] Hathaway, Oona A., et al. "The Law of Cyber-Attack." *California Law Review*, vol. 100, no. 4, 2012, pp. 841.

[257] International Law Committee, Responsibility of the States for International Wrongful Acts.

[258] Adunarea Generală a ONU. (1965). *Declarația privind inadmisibilitatea intervenției în treburile interne ale statelor și protecția independenței și suveranității acestora*. Rezoluția 2131 (XX).
Adunarea Generală a ONU. (1987). *Declarația privind îmbunătățirea eficienței principiului abținerii de la amenințarea sau utilizarea forței în relațiile internaționale*. Rezoluția 42/22.

[259] International Law Committee, Responsibility of the States for International Wrongful Acts.

[260] Kaspersky."Stuxnet Definition & Explanation."

[261] Chen, T., and Saeed A. "Lessons from Stuxnet." *IEEE Computer*, vol. 44, no. 4, Apr. 2011, pp. 91-93; "Lessons Learned From Stuxnet." *IBM's Security Intelligence*.

[262] Hollis, D. "Could Deploying Stuxnet be a War Crime?" *Opinio Juris*, 25 ianuarie 2011.

5.1.1. Contextul geopolitic

Atacul Stuxnet a fost profund ancorat într-o strategie geopolitică complexă, având ca obiectiv primordial împiedicarea sau, cel puțin, întârzierea programului nuclear iranian.[263] Acest program era perceput de actori internaționali cheie, în special Statele Unite și Israel, ca o potențială amenințare la adresa proliferării nucleare, generând tensiuni semnificative pe scena internațională.[264] Operațiunea, cunoscută sub numele de cod *Jocuri Olimpice* (*Operation Olympic Games*), a reprezentat un efort clasificat, inițiat sub administrația președintelui George W. Bush și continuat sub președintele Obama, deși nu a fost niciodată recunoscută oficial de către niciun stat.[265]

Se presupune că decizia de a utiliza Stuxnet a reflectat o abordare strategică nuanțată, vizând degradarea capacităților nucleare ale Iranului fără a recurge la o lovitură aeriană directă sau la o operațiune a forțelor speciale. Această strategie a poziționat Stuxnet nu doar ca un act de sabotaj, ci ca un instrument sofisticat de *diplomație secretă*. Natura sa clandestină și durata prelungită a operațiunii au permis autorilor să mențină o negare plauzibilă, controlând astfel narațiunea și atenuând potențialele reacții imediate.[266] Această abordare subliniază importanța crescândă a *zonei gri* în relațiile internaționale, unde statele pot urmări obiective strategice prin acțiuni care se situează sub pragul conflictului armat tradițional, estompând granițele dintre pace și război. Astfel, atacurile cibernetice devin o modalitate de a exercita presiune și de a obține avantaje strategice fără a declanșa un răspuns militar convențional.

5.1.2. Cronologia detaliată a dezvoltării, propagării și descoperirii Stuxnet

Dezvoltarea Stuxnet este estimată să fi început încă din anul 2005. Această perioadă extinsă de dezvoltare subliniază complexitatea inerentă și resursele considerabile necesare pentru crearea unei arme cibernetice de o asemenea anvergură. Prima variantă a virusul a fost detectată în iunie 2009. Ulterior, o a doua variantă, care a inclus îmbunătățiri substanțiale, a apărut în martie 2010, posibil ca răspuns la observațiile că Stuxnet nu se răspândea cu viteza sau impactul dorit. O a treia variantă, cu modificări minore, a urmat în aprilie 2010.Viermele conținea, de asemenea, o componentă cu un marcaj temporal de construcție din 3 februarie 2010.[267]

Descoperirea și identificarea viermelui au fost realizate pentru prima dată de compania de securitate VirusBlokAda la mijlocul lunii iunie 2010, iar jurnalistul Brian Krebs a publicat primul raport detaliat și larg citit pe 15 iulie 2010. Momentul în care Stuxnet a fost adus la lumină este atribuit unei erori de programare într-o actualizare, care a determinat viermele să se propage accidental dincolo de ținta sa inițială, ajungând pe un computer conectat la internet.[268] Această *scăpare* neintenționată a fost esențială, permițând analiștilor de securitate să-l detecteze și să-l discearnă. Un detaliu important al designului Stuxnet este că a fost programat să expire în iunie 2012, o caracteristică de tip *kill switch* menită să limiteze răspândirea necontrolată pe termen lung.[269]

5.1.3. Identificarea țintelor specifice și amploarea inițială a impactului

Ținta principală și specifică a Stuxnet au fost centrifugele de îmbogățire a uraniului din instalațiile nucleare iraniene, cu accent pe cele situate la Natanz. Atacatorii au vizat în mod deliberat sistemele de control industrial (SCADA) Siemens Step7, care erau responsabile de gestionarea și monitorizarea acestor centrifuge. Viermele a fost conceput pentru a manipula subtil viteza centrifugelor sensibile, inducând o uzură accelerată și, în cele din urmă, defectarea acestora pe termen lung, mai degrabă decât o distrugere fizică imediată și evidentă. Această abordare *de uzură* (*attrition*) a reprezentat o strategie calculată, menită să întârzie programul nuclear iranian fără a provoca o reacție armată directă și imediată.[270]

Se estimează că Stuxnet a deteriorat sau distrus aproape o cincime din centrifugele nucleare

[263] "Lessons Learned From Stuxnet." *IBM's Security Intelligence*.

[264] Joyner, D. "Stuxnet an 'Act of Force' Against Iran." *Arms Control Law*, 25 martie 2013; Roscini, M. "Did Stuxnet Breach the UN Charter's 'Principles'?" *Arms Control Law*, 28 septembrie 2012.

[265] "Operation Olympic Games: Cyber Sabotage as a Tool of American Intelligence Aimed." *Security and Defence*.

[266] Joyner, D. "Stuxnet an 'Act of Force' Against Iran." *Arms Control Law*, 25 martie 2013; Roscini, M. "Did Stuxnet Breach the UN Charter's 'Principles'?" *Arms Control Law*, 28 septembrie 2012.

[267] Kaspersky."Stuxnet Definition & Explanation."

[268] *Ibidem.*

[269] *Ibidem.*

[270] Kaspersky."Stuxnet Definition & Explanation."; Chen, T., and Saeed A. "Lessons from Stuxnet." *IEEE Computer*, vol. 44, no. 4, Apr. 2011, pp. 91-93; "Lessons Learned From Stuxnet." *IBM's Security Intelligence*.

ale Iranului, infectând peste 200.000 de computere și cauzând degradarea fizică a aproximativ 1.000 de mașini. Institutul pentru Știință și Securitate Internațională a estimat în 2010 că peste 1.000 de centrifuge au fost afectate, ceea ce reprezenta aproximativ 10% din capacitatea totală de îmbogățire a Iranului la acea vreme. Deși Stuxnet nu a fost conceput pentru a se răspândi dincolo de instalațiile nucleare iraniene, natura sa sofisticată și agresivă a dus la infectarea unor computere conectate la internet, deși a cauzat daune minime acestor sisteme externe datorită țintirii sale extrem de specifice.[271]

5.2. Analiza tehnică a Stuxnet: Mod de operare și efecte

5.2.1. Mecanismele sofisticate de propagare și infiltrare

Stuxnet a demonstrat o inginerie cibernetică de vârf, exploatând un număr fără precedent de patru vulnerabilități *zero-day* în sistemul de operare Microsoft Windows,[272] care erau necunoscute anterior dezvoltatorilor de software.[273] Acestea includeau un număr de vulnerabilități. Utilizarea simultană a multiplelor *zero-day*-uri a fost extrem de neobișnuită la momentul descoperirii Stuxnet și rămâne o raritate în peisajul amenințărilor cibernetice.[274]

Propagarea principală în rețelele *air-gapped* (izolate fizic de internet) ale instalațiilor nucleare iraniene s-a realizat prin intermediul unităților USB infectate, posibil introduse de agenți sau contractori care aveau acces fizic la aceste facilități securizate.[275] Acest vector de atac, aparent simplu, a demonstrat eșecul *mitului air-gap-ului* ca măsură de securitate singulară, subliniind că nici cele mai sigure instalații nu sunt imune la amenințări. Succesul infiltrării prin intermediul unităților USB a evidențiat o vulnerabilitate crucială: factorul uman. Indiferent de complexitatea tehnică a *malware*-ului, interacțiunea umană cu sistemele – cum ar fi utilizarea unităților USB de către ingineri – poate crea, în mod involuntar, puncte de intrare pentru amenințări avansate. Acest lucru implică faptul că strategiile de securitate cibernetică trebuie să depășească simplele apărări tehnice, integrând programe riguroase de instruire a personalului, protocoale operaționale stricte și măsuri robuste de securitate a lanțului de aprovizionare. Incidentul a demonstrat că chiar și facilitățile considerate *securizate* sunt susceptibile în fața adversarilor determinați.[276]

Odată pătruns în sistem, Stuxnet se putea propaga și prin partajări de rețea Windows și prin exploatarea vulnerabilităților menționate anterior[277] pentru a infecta computerele la distanță. Viermele conținea, de asemenea, capacități de auto-actualizare prin intermediul unei rețele *peer-to-peer* încorporate[278] și putea comunica cu servere de comandă și control (C2) pentru a furniza informații despre răspândirea sa și a primi actualizări.[279] Cu toate acestea, utilizarea unor astfel de funcționalități *zgomotoase* ar fi putut alerta personalul. Stuxnet a inclus și măsuri de siguranță pentru a-și limita răspândirea, infectând doar trei computere dintr-o unitate flash infectată și fiind codificat pentru a opri răspândirea după 24 iunie 2012.[280]

5.2.2. Modul de operare asupra sistemelor de control industrial și manipularea subtilă a datelor

Stuxnet a fost conceput cu o precizie remarcabilă pentru a afecta doar ținte specifice, minimizând daunele altor dispozitive sau rețele. Odată infiltrat, viermele căuta *software*-ul Siemens Step

[271] "Did Stuxnet Take Out 1000 Centrifuges at the Natanz Enrichment Plant?" *ISIS Online*.

[272] Vulnerabilitățile *zero-day* sunt defecte de securitate software sau hardware necunoscute anterior de către dezvoltatorul software-ului sau producătorul hardware-ului și, prin urmare, nedescoperite publicului larg sau nedetectate de producător.

[273] "Basic Attack Strategy of Stuxnet 0.5." *ISIS Online*.

[274] LNK (CVE-2010-2568); autorun.inf; MS10-061;SMB MS08-067.

[275] *Rețelele air-gapped* sisteme de securitate izolate fizic de orice altă rețea nesecurizată, în special de internet sau de rețelele publice. Conceptul de *air-gap* se referă la "golul de aer" care separă fizic o rețea de alta, împiedicând orice contact electronic direct.

[276] "Lessons Learned From Stuxnet." *IBM's Security Intelligence*.

[277] LNK (CVE-2010-2568); autorun.inf; MS10-061;SMB MS08-067.

[278] Rețelele *peer-to-peer (P2P***)** sunt un tip de arhitectură de rețea distribuită în care nodurile (participanții) funcționează atât ca clienți, cât și ca servere, partajând resurse și servicii direct între ele, fără a depinde de un server centralizat.
Conceptul de *rețele peer-to-peer încorporate* se referă la implementarea acestei arhitecturi P2P în sisteme sau dispozitive cu resurse limitate, adesea integrate în contexte specifice. Termenul "încorporate" (*embedded*) sugerează că funcționalitatea P2P este integrată direct în hardware-ul sau software-ul dispozitivului, mai degrabă decât să ruleze pe un computer general-purpose.

[279] *Serverele de comandă și control (C2 sau C&C)* sunt computere sau sisteme utilizate de atacatori cibernetici pentru a comunica și a gestiona de la distanță malware-ul instalat pe sistemele compromise (victime). Ele acționează ca un "cartier general" central pentru operațiunile malițioase.

[280] Kaspersky."Stuxnet Definition & Explanation."

7, utilizat de controlerele logice programabile (PLC) pentru a automatiza și monitoriza echipamentele electromagnetice în medii industriale. Viermele a actualizat codul pentru a trimite instrucțiuni distructive echipamentelor controlate, manipulând subtil viteza centrifugelor de îmbogățire a uraniului.[281]

Un aspect cheie al sofisticării Stuxnet a fost capacitatea sa de a trimite feedback fals controlerului principal. Aceasta însemna că, deși centrifugele funcționau defectuos și se autodistrugeau, monitoarele operatorilor afișau că totul funcționa normal, împiedicându-i pe aceștia să realizeze problema până când daunele fizice erau ireversibile. Această „mascare" a efectelor este o caracteristică definitorie a atacurilor semantice. Capacitatea Stuxnet de a manipula datele și de a prezenta feedback fals operatorilor umani ilustrează natura insidioasă a atacurilor semantice.[282] Această formă de atac depășește simpla perturbare; ea implică înșelăciune și subminarea încrederii în sistemele automate și în informațiile pe care acestea le furnizează. Dificultatea inerentă în detectarea unor astfel de manipulări subtile[283] până când daunele fizice devin incontestabile reprezintă o provocare semnificativă pentru securitatea cibernetică defensivă. Aceasta sugerează că detectarea tradițională a anomaliilor, care se bazează adesea pe abateri de la comportamentul așteptat, ar putea fi insuficientă. În schimb, o abordare mai robustă ar necesita monitorizare avansată a integrității, validare încrucișată a sistemelor și, potențial, analiză bazată pe inteligență artificială pentru a detecta alterările subtile și malițioase ale datelor înainte ca acestea să conducă la defecțiuni fizice catastrofale.

5.2.3. Descrierea efectelor fizice și impactul virusului

Stuxnet a manipulat valvele care pompau gaz de uraniu în centrifuge, accelerând volumul de gaz și suprasolicitând centrifugele rotative. Această suprasolicitare a dus la supraîncălzirea și, în cele din urmă, la autodistrugerea acestora.[284]Aceste acțiuni au cauzat degradarea și scoaterea din funcțiune a mii de centrifuge. Impactul fizic a fost cuantificabil și identificabil, chiar și luând în considerare rata ridicată de eșec preexistentă a centrifugelor.

[281] *Ibidem.*
[282] Capitolul II.
[283] "Lessons Learned From Stuxnet." *IBM's Security Intelligence*.
[284] *Ibidem.*

5.2.4. Componentele cheie ale malware-ului și caracteristicile sale avansate

Stuxnet era compus din trei părți principale: un vierme (*worm*) care realiza cea mai mare parte a lucrului malițios, un fișier de legătură (*link file*) care automatiza execuția copiilor propagate ale viermelui și un *rootkit* care ascundea fișierele de detecție.[285] Caracteristicile sale avansate includeau complexitatea, flexibilitatea, potențialul și combinația de funcționalități, făcându-l o *nouă specie* de vierme în peisajul *malware*. A fost conceput pentru a evita detectarea de către software-ul antivirus și de către operatorii umani, învățând despre mediul țintă și ajustându-și comportamentul.[286]

Arhitectura multi-componentă (vierme, fișier de legătură, *rootkit*), utilizarea fără precedent a patru exploatări *zero-day*, și capacitatea sa de a rămâne latent până la îndeplinirea unor condiții specifice demonstrează un salt semnificativ în sofisticarea armelor cibernetice. Acest nivel de complexitate și precizie indică o investiție substanțială de resurse, expertiză și timp, caracteristică capacităților la nivel de stat. Această evoluție sugerează că viitoarele arme cibernetice vor fi probabil și mai complexe, adaptabile și dificil de detectat și analizat, necesitând o creștere proporțională a capacităților defensive, a colectării de informații despre amenințări și a colaborării internaționale în cercetare și dezvoltare în domeniul securității cibernetice. [287]

[285] Un vierme (în engleză: *worm*) este un tip de program malware autonom (independent) care se reproduce și se răspândește de la un computer la altul, sau de la o rețea la alta, fără intervenția utilizatorului și fără a se atașa la un program gazdă existent (spre deosebire de un virus).
Un *fișier de legătură* (adesea numit și scurtătură, comandă rapidă) este un tip special de fișier care acționează ca un pointer sau o referință către un alt fișier sau director (folder) situat într-o altă locație. Rolul său principal este de a oferi acces rapid și convenabil la un fișier sau un folder fără a fi necesară navigarea la locația sa originală.
Un *rootkit* este un tip de software malițios sau un set de instrumente software care permit unui atacator să mențină acces privilegiat (adesea nivel de *root* sau "administrator") la un computer sau sistem de operare, în timp ce rămâne nedetectat. Este conceput pentru a ascunde prezența altor programe malițioase, procese, fișiere sau activități de rețea.
[286] Kaspersky."Stuxnet Definition & Explanation."
[287] Joyner, D. "Stuxnet an 'Act of Force' Against Iran." *Arms Control Law*, 25 martie 2013; Roscini, M. "Did Stuxnet Breach the UN Charter's 'Principles'?" *Arms Control Law*, 28 septembrie 2012.

5.2.5. Moștenirea tehnică a Stuxnet și apariția malware-urilor derivate

Deși Stuxnet a expirat în iunie 2012 și Siemens a emis remedieri pentru software-ul său PLC, moștenirea sa tehnică a continuat prin alte atacuri *malware* bazate pe codul său original sau pe metodologiile sale. Apariția rapidă a variantelor de *malware* precum Duqu,[288] Flame,[289] Industroyer[290] și Triton,[291] care fie au reutilizat direct codul Stuxnet, fie au adoptat tehnicile sale sofisticate [1], demonstrează un efect clar de copiere sau *proliferare* în domeniul cibernetic.

Această proliferare indică faptul că, odată ce o armă cibernetică extrem de eficientă și inovatoare este implementată și ulterior analizată, metodologiile sale pot fi invers-inginerizate, adaptate și reutilizate de alți actori statali sau non-statali. Acest fenomen implică o cursă continuă și accelerată a înarmărilor în spațiul cibernetic, unde tehnicile ofensive de succes devin rapid provocări defensive, necesitând inovație constantă în cercetarea securității cibernetice, partajarea informațiilor despre amenințări și dezvoltarea de mecanisme de apărare proactive pentru a rămâne înaintea amenințărilor în evoluție.

5.2.6 Implicațiile geopolitice și juridice ale atacului Stuxnet

Stuxnet a marcat un moment decisiv în istoria conflictelor cibernetice, demonstrând capacitatea fără precedent a unui atac cibernetic de a produce daune fizice substanțiale infrastructurii critice a unui stat.[292] A fost descris ca un *moment Oppenheimer* pentru războiul cibernetic, sugerând că potențialul său distructiv depășește cel al atacurilor cibernetice anterioare. Acest incident a catalizat o dezbatere globală intensă privind necesitatea unor noi norme și reglementări internaționale care să guverneze conduita statelor în spațiul cibernetic. A subliniat necesitatea urgentă a unui răspuns global colectiv pentru a securiza infrastructura critică împotriva amenințărilor cibernetice emergente. [293]

Înainte de Stuxnet, operațiunile cibernetice la scară largă, sponsorizate de state și care cauzau daune fizice, erau în mare parte teoretice sau limitate la colectarea de informații.[294] Execuția reușită a Stuxnet, în ciuda naturii sale secrete, a demonstrat fără echivoc fezabilitatea și eficacitatea mijloacelor cibernetice pentru a atinge obiective strategice semnificative (cum ar fi întârzierea unui program nuclear) fără a recurge la angajamente cinetice convenționale. Acest succes a contribuit, în mod argumentat, la o *normalizare* a războiului cibernetic ca instrument legitim și viabil al politicii de stat.[295] Acest lucru sugerează că operațiunile cibernetice nu mai sunt doar o nișă a informațiilor, ci o componentă centrală a securității naționale și a politicii externe, servind ca o alternativă sau o completare la acțiunile militare tradiționale. Această evoluție implică necesitatea ca statele să dezvolte doctrine clare, linii roșii și cadre de răspuns pentru operațiunile cibernetice, pe măsură ce *zona gri* a conflictului se extinde și devine tot mai centrală în relațiile internaționale.

Deși lucrarea de față nu include decât ipoteza unui atac cibernetic săvârșit de către un stat, a cărui responsabilitate este demonstrată, este necesară mențiunea cu privire la atribuirea propriu-zisă a atacurilor cibernetice unui stat și importanța probei.

Deși niciun stat nu și-a asumat oficial responsabilitatea pentru Stuxnet, scopul, designul extrem de sofisticat și țintirea precisă a viermelui sugerează puternic implicarea statală. Este larg acceptat în comunitatea de securitate cibernetică și în rapoartele independente că a fost o creație comună a agențiilor de informații din SUA și Israel.[296]

Atribuirea este o precondiție crucială pentru analiza utilizării forței și pentru declanșarea răspunsurilor colective, cum ar fi cele prevăzute de articolul 5 al NATO.[297] Dificultatea atribuirii

[288] Duqu (2011): Conceput pentru extragerea datelor din instalații industriale pentru potențiale atacuri viitoare.

[289] Flame (2012): Un spyware sofisticat care înregistra conversații Skype și colecta capturi de ecran.

[290] Industroyer (2016): A vizat facilități energetice și a cauzat o pană de curent în Ucraina.

[291] Triton (2017): A vizat sistemele de siguranță ale unei centrale petrochimice din Orientul Mijlociu, ridicând preocupări privind intenția de a provoca vătămări fizice sau chiar decese.

[292] Kettemann, Matthias C. "ENSURING CYBERSECURITY THROUGH INTERNATIONAL LAW." *Revista Española de Derecho Internacional* 69, no. 2 (2017): 281–90

[293] Hollis, D. "Could Deploying Stuxnet be a War Crime?" *Opinio Juris*, 25 ianuarie 2011.

[294] Nguyen, R.,"Navigating 'Jus Ad Bellum' in the Age of Cyber Warfare." *California Law Review* 101, no. 4, pag. 1081.

[295] O'Connell, M. "Cyber Security without Cyber War". *Journal of Conflict and Security Law*, Vol. 17, No. 2 (2012), pp. 187-209,

[296] Hollis, D. „Could Deploying Stuxnet be a War Crime?" *Opinio Juris*, 25 ianuarie 2011.

[297] Articolul 5 din Tratatul Atlanticului de Nord: "Părţile convin că un atac armat împotriva uneia sau mai multora dintre ele, în Europa sau în America de Nord, va fi considerat un atac împotriva tuturor părţilor şi, în consecinţă, sunt de acord că, dacă are loc un asemenea atac armat, fiecare dintre ele, în exercitarea dreptului la autoapărare individuală sau colectivă, recunoscut prin art. 51 din Carta Organizaţiei Naţiunilor Unite,

este o provocare semnificativă în spațiul cibernetic din cauza anonimatului, a naturii multi-stratificate a atacurilor și a vitezei mari de materializare a efectelor. Procesul de atribuire este un proces multifactorial, implicând aspecte tehnice (urmărirea mașinilor, geolocația), legale (standarde de probă) și politice (identificarea operatorilor, afilierile lor și legăturile cu statele, contextul geopolitic). Atribuirea tehnică, deși nu este absolut exactă, este completată de informații de *intelligence* și analize politice pentru a profila autorii și a stabili legăturile cu statele.[298] Dificultatea inerentă în atribuirea definitivă a atacurilor cibernetice către actori statali specifici creează o provocare profundă pentru aplicarea dreptului internațional.

Un aspect notabil al reacției internaționale la Stuxnet a fost lipsa unei rezoluții oficiale a Consiliului de Securitate al ONU sau a unei condamnări formale. De asemenea, tăcerea Iranului cu privire la atac a permis comunității internaționale să evite abordarea directă a problemei. Această situație subliniază complexitățile politice și lipsa unui consens clar în cadrul comunității internaționale privind modul de a răspunde la astfel de incidente cibernetice.

5.2.7. Impactul asupra interpretării articolului 2(4) din Carta ONU și a conceptului de <u>utilizare a forței</u>

Stuxnet a adus în prim-plan întrebarea fundamentală dacă un atac cibernetic poate constitui o utilizare a forței în sensul articolului 2(4) din Carta ONU.[299] Doctrina dreptului internațional, în special prin lucrările precum *Tallinn Manual*, a propus o serie de criterii care au fost deja discutate în Capitolul IV.[4]

Aplicând aceste criterii la Stuxnet, se pot observa îndeplinirea unor criterii și lipsa celorlalte. Acestea trebuie analizate atât individual, cât și global.

Severitatea atacului Stuxnet nu corespunde celei cerute de Tallinn Manual. Daunele fizice, rănirile sau decesele sunt considerate praguri pentru calificarea ca utilizare a forței.[300] A, însă, fost considerat o utilizare a forței datorită daunelor fizice provocate programului nuclear iranian, întârziindu-l cu câțiva ani.[301] **Imediatitatea** efectelor este un alt criteriu neîndeplinit. Stuxnet s-au manifestat pe parcursul a săptămâni sau luni, permițând - teoretic - timp pentru măsuri de atenuare, ceea ce ar putea sugera că nu ar fi considerat o utilizare a forței pe baza acestui factor.[302] **Directitatea** este confirmată. A existat o conexiune cauzală directă între vierme și centrifugile deteriorate.[303] **Invazivitatea** Stuxnet-ului s-a reprezentat printr-o intruziune semnificativă în suveranitatea iraniană, vizând sisteme fizic izolate (*air-gapped*), care fac parte din infrastructura critică a statului. [304] S-a remarcat de către grupul de experți, că intruziunea în sistemele de maximă securitate ale statului – legate de sfera militară, de *intelligence* sau (chiar) politică – reprezintă un argument adăugător în decizia unor state de a reprima atacurile cibernetice. **Măsurabilitatea efectelor** este asigurată de consecințele care au fost cuantificabile și identificabile, chiar și luând în considerare rata ridicată de eșec a centrifugelor. Dificultatea stabilirii extinderii efectelor nu se datorează unui caracter aleator al efectului virusul, ci tăcerii guvernului iranian cu privire la pagubele create de operațiune.[305] Stuxnet a fost lipsit de **legitimitate prezumtivă**, deoarece acțiunea deteriorarea instalațiilor nucleare ale unui alt stat fără autorizarea Consiliului de Securitate al ONU și în lipsă de contextul autoapărării.[306] Cum s-a menționat deja, **atribuirea** sau **implicarea statală** este considerată unanim drept o condiție îndeplinită. Deși niciun stat nu și-a asumat responsabilitatea, scopul și designul viermelui sugerează puternic implicarea statală. Este un fapt constatat deja că Stuxnet a fost o operațiune operată de SUA și Israel.[307]

Pe baza acestor criterii, majoritatea experților și participanți la redactarea *Tallinn Manual* și al altor lucrări de specialitate, au înclinat spre calificarea Stuxnet ca o utilizare a forței. Cu toate acestea, s-a făcut o distincție crucială între *utili-*

va sprijini partea sau părţile atacate, prin realizarea imediată, individual şi împreună cu celelalte părţi, a oricărei acţiuni pe care o consideră necesară, inclusiv folosirea forţei armate, în vederea restabilirii şi menţinerii securităţii în spaţiul Atlanticului de Nord.

Orice astfel de atac armat şi toate măsurile adoptate ca urmare a acestuia vor fi imediat aduse la cunoştinţă Consiliului de Securitate. Aceste măsuri vor înceta după adoptarea de către Consiliul de Securitate a măsurilor necesare pentru restabilirea şi menţinerea păcii şi securităţii internaţionale. "

[298] Schmitt, M-N., 2017, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press.

[299] Hollis, D. "Could Deploying Stuxnet be a War Crime?" *Opinio Juris*, 25 ianuarie 2011

[300] Schmitt, M-N., 2017, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press, pag. 49.

[301] *Idem*, pag. 49.

[302] *Ibidem.*

[303] *Idem*, pag. 49-50.

[304] *Idem*, pag. 50.

[305] *Idem*, pag. 50-51.

[306] *Idem*, pag. 51

[307] *Ibidem.*

zarea forței (articolul 2(4)) și *atac armat* (articolul 51), acesta din urmă declanșând dreptul la autoapărare. [308] În general, s-a considerat că Stuxnet a atins pragul de *utilizare a forței* datorită daunelor materiale semnificative, dar nu și pe cel de *atac armat*, ceea ce ar fi justificat doar contramăsuri non-armate din partea Iranului, nu un răspuns militar în autoapărare.[309]

S-a dezbătut, de asemenea, dacă Stuxnet a respectat principiile *jus in bello*, având în vedere țintirea sa precisă și minimizarea daunelor colaterale. Această precizie ar putea fi un indiciu suplimentar al sponsorizării statale și ar putea implica o intenție de a opera în limitele, chiar și extinse, ale dreptului conflictelor armate. Stuxnet a evidențiat faptul că statele iau în considerare factori dincolo de aderența strictă la articolul 2(4) atunci când caracterizează legalitatea operațiunilor cibernetice, având în vedere natura evolutivă a dreptului internațional și caracteristicile unice ale spațiului cibernetic.[310]

Lipsa unui cadru juridic internațional clar și obligatoriu pentru războiul cibernetic și atacurile cibernetice rămâne o provocare majoră.[311] Stuxnet a subliniat în mod dramatic această lacună, evidențiind urgența ca statele să elaboreze reguli specifice pentru operațiunile cibernetice și să consolideze cooperarea internațională în acest domeniu. Putem observa că, deși Stuxnet nu corespunde expres criteriilor cerute în Manual, lipsa unor criterii se compenseză puternic cu existența celorlalte și impactul *global* al acestora asupra formării unei opinii colective în rândul membrilor ONU. Deoarece fiecare atac cibernetic este unic în modul său de operare și din perspectiva efectelor și al scopului său, este ineficientă stabilirea unei liste de criterii restrictive și impunerea unor cerințe riguroase minime asupra tuturor situațiilor viitoare.

Ambiguitatea actuală în reglementarea cibernetică poate fi parțial explicată prin preferința marilor actori geopolitici, inclusiv SUA, China și Rusia, pentru un grad semnificativ de ambiguitate strategică. Această ambiguitate le permite o flexibilitate mai mare în dezvoltarea și rafinarea propriilor capabilități militare cibernetice, evitând angajamente internaționale obligatorii care ar putea restricționa acțiunile lor într-un domeniu în rapidă evoluție. Această situație este cu atât mai relevantă în contextul războaielor hibride și al dependenței ultra-tehnologice a societăților moderne.

Inițiative precum *Tallinn Manual*, deși nu sunt instrumente juridice obligatorii *per se*, joacă un rol esențial în furnizarea de ghidare și în promovarea unui consens asupra modului în care dreptul internațional existent se aplică operațiunilor cibernetice. Aceste eforturi sunt cruciale pentru a clarifica ce constituie un comportament acceptabil al statelor și care sunt consecințele potențiale ale ignorării normelor.

Incidentul Stuxnet a demonstrat în mod elocvent că, în timp ce dreptul internațional tradițional se concentrează pe daunele materiale și vieți omenești, noile forme de agresiune cibernetică pot provoca prejudicii non-materiale semnificative entităților și proceselor virtuale, care nu sunt pe deplin acoperite de cadrele juridice existente. Acest lucru subliniază inadecvatul continuu al definițiilor tradiționale și necesitatea de a adapta și dezvolta noi cadre legale care să țină cont de provocările unice ale dependenței crescânde de tehnologiile informației și comunicațiilor.

CONCLUZII

Lucrarea de față a abordat problematica atacurilor cibernetice din perspectiva articolului 2(4) din Carta ONU, analizând care sunt criteriile pe care acestea trebuie să le îndeplinească pentru a constitui o utilizare a forței în sensul normelor de drept internaționa. Ipoteza centrală a cercetării a fost că atribuirea criteriilor stabilite de Tallinn Manual unui atac cibernetic crește prograsiv șansa acestuia de a fi considerat o încălcare de articolului 2(4), iar studiul de caz Stuxnet a servit drept exemplu elocvent pentru a evalua aceste criterii.

Regimul juridic actual se bazează pe articolul 2(4) al Cartei ONU, care interzice amenințarea cu forța sau utilizarea forței. Curtea Internațională de Justiție a stabilit că această interdicție se aplică oricărei utilizări a forței, indiferent de armele folosite, subliniind importanța *scalei* și *efectelor* unei acțiuni în determinarea calificării sale. Această interpretare, adaptabilă la noile realități, permite evaluarea formelor non-tradiționale de forță, inclusiv a atacurilor cibernetice. Aplicarea acestor criterii la cazul Stuxnet a demonstrat complexitatea calificării, evidențiind, de exemplu, lipsa de legitimitate prezumtivă a acțiunilor care vizează

[308] Hollis, D. "Could Deploying Stuxnet be a War Crime?" *Opinio Juris*, 25 ianuarie 2011;
Joyner, D. "Stuxnet an 'Act of Force' Against Iran." *Arms Control Law*, 25 martie 2013; Roscini, M. "Did Stuxnet Breach the UN Charter's 'Principles'?" *Arms Control Law*, 28 septembrie 2012.

[309] Nguyen, R.,"Navigating 'Jus Ad Bellum' in the Age of Cyber Warfare." *California Law Review* 101, no. 4.

[310] Hathaway, Oona A., et al. "The Law of Cyber-Attack." *California Law Review*, vol. 100, no. 4, 2012.

[311] Ducaru, S. "Can a Cyberattack Become an Act of War? European and Trans-Atlantic Perspectives.'' *Romanian Journal of European Affairs*, Vol.2, No.1 (2024).

instalații nucleare fără o justificare legală.

Prin analiza detaliată a cazului Stuxnet, lucrarea a demonstrat că anumite atacuri cibernetice pot într-adevăr atinge pragul de *utilizare a forței*. Stuxnet, un atac semantic care a vizat sistemul nuclear iranian, a cauzat daune fizice semnificative, reușind să întârzie programul cu câțiva ani. Acest aspect este crucial, deoarece criteriile propuse de doctrină, cum ar fi *severitatea*, indică necesitatea unor daune fizice pentru a califica un atac cibernetic drept utilizare a forței. Deși criteriul *nemijlocirii* nu a fost pe deplin îndeplinit în cazul Stuxnet, dată fiind manifestarea graduală a daunelor pe parcursul unor săptămâni sau luni, a existat o *conexiune cauzală directă* între vierme și centrifugele deteriorate, ceea ce a consolidat argumentul. Invazivitatea atacului Stuxnet, care a pătruns în sisteme fizic izolate, a reprezentat, de asemenea, o intruziune semnificativă în suveranitatea iraniană. Mai mult, măsurabilitatea efectelor atacului a fost clară, oferind o bază solidă pentru evaluarea impactului său.

Deși articolul 2(4) oferă un cadru juridic robust, natura evolutivă și rapidă a atacurilor cibernetice impune o necesitate continuă de clarificare și consolidare a reglementărilor internaționale. Ambiguitatea deliberată a Cartei în definirea exactă a *forței* permite o flexibilitate esențială în aplicarea sa la scenarii neprevăzute. Cu toate acestea, apar provocări semnificative în stabilirea atribuirii atacurilor cibernetice și în aplicarea principiilor de autoapărare în acest context. Este esențială promovarea cooperării internaționale și dezvoltarea unui cadru juridic clar pentru a atenua eficient amenințările reprezentate de atacurile cibernetice.

În concluzie, ipoteza cercetării a fost confirmată: atacurile cibernetice pot, în circumstanța îndeplinirii cerințelor din *Tallinn Manual*, constitui utilizări ale forței în sensul articolului 2(4) din Carta ONU, în special atunci când produc efecte comparabile cu cele ale forței armate convenționale. Cazul Stuxnet servește drept o ilustrare importantă a acestei realități, subliniind urgența adaptării continue a dreptului internațional la provocările complexe și dinamice ale erei digitale.

BIBLIOGRAFIE

1. "Basic Attack Strategy of Stuxnet 0.5." *ISIS Online*. Accesat la 21 Iul. 2025. Disponibil la: https://isis-online.org/isis-reports/basic-attack-strategy-of-stuxnet-0.5/.
2. CCDCOE. "Centre is the first International Military Organization hosted by Estonia." *CCDCOE*, 2008. Accesat la 12 Ian. 2025. Disponibil la: https://ccdcoe.org/news/2008/centreis-the-first-international-military-organization-hosted-by-estonia/.
3. ---. "European Union establishes a sanction regime for cyber-attacks'." *CCDCOE*, 2019. Accesat la 12 Ian. 2025. Disponibil la: https://ccdcoe.org/library/publications/european-union-establishes-a-sanction-regime-for-cyber-attacks/.
4. Chen, Thomas M., and Saeed Abu-Nimeh. "Lessons from Stuxnet." *IEEE Computer*, vol. 44, no. 4, Apr. 2011, pp. 91-93. Accesat la 18 Iul. 2025. Disponibil la: https://www.computer.org/csdl/magazine/co/2011/04/mco2011040091/13rRUB7a16w.
5. Consiliul UE. "Decizia (CFSP) 2019/797." 2019. Disponibil la: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32019D0797.
6. ---. "Regulament (EU) 2019/796." 2019. Disponibil la: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.LI.2019.129.01.0001.01.ENG&toc=OJ:L:2019:129I:TOC.
7. Delerue, François. "The Threshold of Cyber Warfare: from Use of Cyber Force to Cyber Armed Attack." *Cyber Operations and International Law*, Cambridge University Press, 2020. Accesat la 18 Iul. 2025. Disponibil la: https://www.cambridge.org/core/books/cyber-operations-and-international-law/threshold-of-cyber-warfare-from-use-of-cyber-force-to-cyber-armed-attack/18EED20277D22CAE25E71F63A27C8009.
8. "Did Stuxnet Take Out 1000 Centrifuges at the Natanz Enrichment Plant?" *ISIS Online*. Accesat la 21 Iul. 2025. Disponibil la: https://isis-online.org/isis-reports/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.
9. Ducaru, S., et al. "Can a Cyberattack Become an Act of War? European and Trans-Atlantic Perspectives." *Romanian Journal of European Affairs*, vol. 2, no. 1, 2024. Disponibil la: http://rjea.ier.gov.ro/wp-content/uploads/2024/06/Art.-1_Can-a-Cyberattack-Become-an-Act-of-War_Ducaru-et-al._2024_final.pdf.
10. Foltz, A. "Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate." *JFQ*, no. 67, 4th quarter 2012, pp. 40-48. Disponibil la: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_40-48_Foltz.pdf.
11. Hathaway, Oona A., et al. "The Law of Cyber-Attack." *California Law Review*, vol. 100, no. 4, 2012, pp. 817–85. Disponibil la: [suspicious link removed].
12. Hollis, Duncan B. "Could Deploying Stuxnet be a War Crime?" *Opinio Juris*, 25 Ian. 2011. Accesat la 18 Iul. 2025. Disponibil la: http://opiniojuris.org/2011/01/25/could-deploying-stuxnet-be-a-war-crime/.
13. Hughes, Rex B. "NATO and Cyber Defence - Mission Accomplished." *Atlantisch Perspectief*, no. 1/4,

2009. Accesat la 12 Ian. 2025. Disponibil la: https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/NATO%20and%20Cyber%20Defence%20-%20Mission%20Accomplished.pdf.

14. International Court of Justice. *Legality of the Threat or Use of Nuclear Weapons*. Advisory Opinion, 8 July 1996. 1996 I.C.J. Reports 226.
15. ---. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*. 1986. Disponibil la: https://www.icj-cij.org/case/70/judgments.
16. International Law Committee. *Responsibility of the States for International Wrongful Acts*. Accesat la 12 Ian. 2025. Disponibil la: https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.
17. "Lessons Learned From Stuxnet." *IBM's Security Intelligence*. Accesat la 18 Iul. 2025. Disponibil la: https://securityintelligence.com/lesson-learned-from-stuxnet/.
18. Joyner, Dan. "Stuxnet an 'Act of Force' Against Iran." *Arms Control Law*, 25 Mar. 2013. Accesat la 18 Iul. 2025. Disponibil la: https://armscontrollaw.com/2013/03/25/stuxnet-an-act-of-force-against-iran/.
19. Kaspersky. "Stuxnet explained: What it is, who created it and how it works?" *Kaspersky*, 28 Oct. 2021. Accesat la 10 Ian. 2025. Disponibil la: https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet.
20. Kettemann, Matthias C. "ENSURING CYBERSECURITY THROUGH INTERNATIONAL LAW." *Revista Española de Derecho Internacional*, vol. 69, no. 2, 2017, pp. 281–90. Disponibil la: [suspicious link removed].
21. NATO. "Cyber defence." *NATO*, 2020. Accesat la 12 Ian. 2025. Disponibil la: https://www.nato.int/cps/en/natolive/topics_78170.htm.
22. ---. "Defending the networks. The NATO Policy on Cyber Defence." *NATO*, 2011. Accesat la 12 Ian. 2025. Disponibil la: https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf.
23. NATO Strategic Communication Center of Excellence. *2007 cyber attacks on Estonia*. 2007. Accesat la 10 Ian. 2025. Disponibil la: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf.
24. Nguyen, Reese. "Navigating 'Jus Ad Bellum' in the Age of Cyber Warfare." *California Law Review*, vol. 101, no. 4, 2013, pp. 1079–1129. Disponibil la: [suspicious link removed].
25. *North Atlantic Treaty*. 4 Apr. 1949.
26. O'Connell, Mary Ellen. "Cyber Security without Cyber War." *Journal of Conflict and Security Law*, vol. 17, no. 2, 2012, pp. 187-209. Disponibil la: [suspicious link removed].
27. "Operation Olympic Games: Cyber Sabotage as a Tool of American Intelligence Aimed." *Security and Defence*. Accesat la 21 Iul. 2025. Disponibil la: https://securityanddefence.pl/Operation-Olympic-Games-nCyber-sabotage-as-a-tool-of-American-nintelligence-aimed,121974,0,2.html.
28. POLITICO. "Timeline: Europe under cyber seige in 2024." *POLITICO*, 2024. Accesat la 12 Ian. 2025. Disponibil la: https://www.politico.eu/article/europe-cyberattacks-russia-china-uk-ministry-of-defence-hacks/.
29. Roscini, Marco. "Did Stuxnet Breach the UN Charter's 'Principles'?" *Arms Control Law*, 28 Sept. 2012. Accesat la 18 Iul. 2025. Disponibil la: https://armscontrollaw.com/2012/10/09/did-stuxnet-breach-the-un-charters-principles/.
30. *Shanghai Cooperation Agreement*, Annex 1. Accesat la 10 Ian. 2025. Disponibil la: https://eng.sectsco.org/files/207508/207508.
31. Schmitt, M-N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017, doi:10.1017/9781316822524.
32. Schmitt, Michael. "Classification of Cyber Conflict." *Journal of Conflict and Security Law*, vol. 17, no. 2, 2012, pp. 245–60. Disponibil la: [suspicious link removed].
33. "Stuxnet Definition & Explanation." *Kaspersky*. Accesat la 18 Iul. 2025. Disponibil la: https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet.
34. "Stuxnet." *Wikipedia*, Wikimedia Foundation. Accesat la 18 Iul. 2025. Disponibil la: https://en.wikipedia.org/wiki/Stuxnet.
35. Tsagourias, Nicholas. "Cyber Attacks, Self-Defence and the Problem of Attribution." *Journal of Conflict and Security Law*, vol. 17, no. 2, 2012, pp. 229–44. Disponibil la: [suspicious link removed].
36. UN Cyber Command. Gen. James E. Cartwright. *Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations 5*. Nov. 2011. Disponibil la: https://nsarchive.gwu.edu/document/21369-document-10.
37. United Nations. *Charter of the United Nations*. 26 June 1945. Disponibil la: https://www.un.org/en/about-us/un-charter.
38. ---. "Declarația privind îmbunătățirea eficienței principiului abținerii de la amenințarea sau utilizarea forței în relațiile internaționale." G.A. Res. 42/22, 1987. Disponibil la: https://digitallibrary.un.org/record/152626?v=pdf.
39. ---. "Declarația privind inadmisibilitatea intervenției în treburile interne ale statelor și protecția independenței și suveranității acestora." G.A. Res. 2131 (XX), 1965. Disponibil la: https://digitallibrary.un.org/record/203886?ln=en&v=pdf.

40. ---. "Declarația privind principiile de drept internațional privind relațiile amicale și cooperarea între state în conformitate cu Carta Organizației Națiunilor Unite." G.A. Res. 2625 (XXV), 24 Oct. 1970. Disponibil la: https://www.auswaertiges-amt.de/blob/2165236/b03d8c5c0c74fc7c9947bee51cd27163/un-gv-res-freundschaftliche-beziehungen-data.pdf.
41. "The Use of Force in International Law." *OpenLearn*, The Open University. Accesat la 21 Iul. 2025. Disponibil la: https://www.open.edu/openlearn/society-politics-law/the-use-force-international-law/content-section-1.
42. Valo, Janne. *Cyber Attacks and the Use of Force in International Law*. 2014. Master's Thesis, University of Helsinki. *Helda*. Accesat la 18 Iul. 2025. Disponibil la: https://helda.helsinki.fi/bitstreams/9d3f583f-314b-4f89-978c-c4676002c446/download.
43. Weidemar, S. "NATO and Article 5 in Cyberspace." *CSS Analyses in Security Policy*, no. 232, Center of Security Studies, 2023. Disponibil la: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse324-EN.pdf.