

UNIVERSITATEA NICOLAE TITULESCU DIN BUCUREȘTI

FACULTATEA DE DREPT

ȘCOALA DOCTORALĂ

TEZĂ DE DOCTORAT

**ATACUL CIBERNETIC – O NOUĂ FORMĂ DE
AGRESIUNE ÎN DREPTUL INTERNAȚIONAL**

REZUMAT

Conducător de doctorat,

Prof. Univ. dr. Raluca Miga Beșteliu

Student doctorand,

Dan-Iulian Voitașec

București,

2017

Cuprins¹

Introducere

Necesitatea și actualitatea temei de cercetare

Obiectivele cercetării

Metodologia folosită pentru elaborarea lucrării de cercetare

Rezultatele cercetării și modalitățile de valorificare a acestora

Cap I –Atacul cibernetic- semnificații și calificarea juridică a atacurilor cibernetice

1. Atacuri îndreptate împotriva sistemelor informatice

2. Infrațiuni informatice

3. Terorismul cibernetice

4. Spionajul cibernetice

5. Atacuri informatice

6. Atacurile informatice care reprezintă folosirea forței conform dreptului internațional

Concluzii

Cap II - Atacul cibernetice ca formă de agresiune în dreptul internațional public

1. Agresiunea în dreptul internațional public

1.1. Privire istorică asupra incriminării agresiunii – Pactul Brian Kellog, Pactele de neagresiune, crimele împotriva păcii

1.2. Obligația statelor de a nu recurge la forță sau la amenințarea cu forță în relațiile internaționale

1.3 Excepții de la principiul interzicerii recursului la forță prevăzute de Carta O.N.U.

1.3.1. Dreptul la autoapărare

1.3.2. Recurgerea la forță în conformitate cu dispozițiile Capitolului VII din Carta ONU

¹ Lucrarea a beneficiat de suport financiar prin proiectul cu titlul „Studii doctorale și postdoctorale Orizont 2020: promovarea interesului național prin excelență, competitivitate și responsabilitate în cercetarea științifică fundamentală și aplicată românească”, număr de identificare contract POSDRU/159/1.5/S/140106. Proiectul este cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013. Investește în Oameni!

1.3.3. Folosirea forței în exercitarea dreptului la autodeterminare

2. Agresiunea în accepțiunea practicii ONU. Cazurile de agresiune conform art. 39 din Carta ONU.

2.1. Elementele faptului de agresiune potrivit Rezoluției 3314 din 14 decembrie 1974 a Adunării Generale O.N.U.

2.2 Deciziile Consiliului de Securitate în baza art. 39 din Carta ONU

3. Crima de agresiune în accepțiunea contemporană

3.1. Cadrul juridic internațional privitor la interzicerea crimei de agresiune

3.2. Sancționarea crimei de agresiune în cadrul Curții Penale Internaționale

3.3. Elementele constitutive ale crimei de agresiune

3.4. Problema exercitării jurisdicției asupra crimei de agresiune

3.5. Exercițarea jurisdicției conform art.15 bis

3.6. Exercițarea jurisdicției conform art.15 ter

4. Atacul cibernetic ca element material al crimei de agresiune

5. Conflictul armat declanșat prin atac cibernetic

5.1. Conflictul armat

5.2. Statutul participanților la conflicte armate declanșate prin atacuri cibernetice

Concluzii

Cap III – Mijloace și metode cibernetice de purtare a conflictelor armate

1. Aplicabilitatea normelor dreptului internațional umanitar în cazul atacurilor informatice

2. Mijloacele și metodele războiului cibernetic

2.1. Mijloacele războiului cibernetic

2.1.1. Calificarea armelor cibernetice drept arme de distrugere în masă

2.2. Metodele războiului cibernetic

2.2.1. Rău superfluu sau suferințe inutile

2.2.2. Mijloace și metode nediscriminante

2.2.3. Capcane cibernetice

2.2.4. Perfidia

2.2.5. Utilizarea necorespunzătoare a emblemelor de protecție

2.2.6. Represaliile

2.2.7. Înfometarea

Concluzii

Cap IV – Categoriile de persoane și obiecte protejate împotriva atacurilor cibernetice

1. Definiții

2. Protecția populației civile și a obiectelor civile

2.1. Protecția specială în timpul conflictelor armate

2.1.1 Protecția specială oferită femeilor în timpul conflictelor armate

2.1.2 Protecția specială oferită copiilor

2.1.3 Protecția jurnaliștilor în conflicte armate

Concluzii

Cap V – Răspunderea în dreptul internațional pentru atacurile cibernetice

1. Forme ale răspunderii pentru crimele internaționale

2. Răspunderea statelor

2.1 Răspunderea materială a statelor

2.2 Răspunderea politică a statelor

3. Răspunderea organizațiilor internaționale

4. Răspunderea penală internațională

4.1. Genocidul

4.2 Crime împotriva umanității

4.3 Crimele de război

4.4 Crima de agresiune

Concluzii

Capitolul VI – Concluzii

ANEXA I – Manualul de la Tallinn 2.0

Bibliografie Selectivă

Necesitatea și actualitatea temei de cercetare

Dacă la momentul adoptării Cartei Organizației Națiunilor Unite și a convențiilor care guvernează dreptul internațional umanitar, existența unor vehicule aeriene pilotate de la distanță cu ajutorul unor sisteme informatice interconectate părea de domeniul fantasticului, tehnologia actuală ne oferă posibilitatea controlării acestor vehicule folosind un dispozitiv pe care majoritatea populației din zone urbane îl poartă în buzunar, mai exact telefonul mobil.

Evoluția tehnologică joacă un rol central în fiecare stat existent în secolul XXI. Sistemele informatice controlează aproape în totalitate serviciile indispensabile societății actuale precum electricitatea, apa, transportul feroviar, chiar și autovehiculele personale. Pentru a înțelege mai bine avansul tehnologic actual, pe teritoriul României există aproximativ 22.9 milioane de numere de telefonie mobilă la o populație mai mică de 20 de milioane de locuitori, 3.47 milioane de abonamente de internet fix și 5.1 milioane de abonamente de internet mobil².

Având în vedere natura transfrontalieră a spațiului cibernetic, tot mai multe state și organizații internaționale au început să aloce un nivel mai ridicat de resurse dezvoltării capabilităților cibernetice atât defensive cât și ofensive.

Această poziție a fost reafirmată și în Declarația adoptată de șefii de stat și de guvern participanți la Summit-ului NATO ce a avut loc în Țara Galilor în septembrie 2014. În art. 72 al Declarației este consemnată adoptarea documentului “*Politica întărită în domeniul apărării cibernetice*” ce evidențiază faptul că apărarea cibernetică este parte a sarcinii de bază a NATO privind apărarea colectivă. Conform acestei noi politici,

² Asociația Națională pentru Administrare și Reglementare în Comunicații - http://www.ancom.org.ro/numarul-de-abonamente-de-telefonie-mobila-a-depasit-pentru-prima-data-numarul-de-cartele-preplatite-active_5762

lansarea unui atac cibernetic asupra unui stat membru NATO ar putea să conducă la invocarea art. 5³ al Tratatului Nord-Atlantic. De asemenea, tot în art. 72 al Declarației este menționat faptul că dreptul internațional, inclusiv dreptul internațional umanitar și Carta ONU, se aplică în domeniul cibernetic.

Cu toate că la nivel național și internațional au început să se dezvolte și să se adopte politici de securitate privind spațiul cibernetic, încă nu au fost dezvoltate instrumente internaționale specifice care să interzică sau să limiteze folosirea anumitor tipuri de atacuri cibernetic. Din cauza acestei situații trebuie identificate normele de drept internațional public și de drept internațional umanitar aplicabile atacurilor cibernetic. De asemenea, trebuie identificate situațiile în care folosirea atacurilor cibernetic atinge pragul de folosire a forței încălcând astfel dispozițiile art. 2 paragraf. 4 al Cartei ONU. În cazul lansării unor operațiuni cibernetic în timpul conflictelor armate, trebuie identificate normele de drept internațional umanitar aplicabile, limitele folosirii acestui tip de atacuri și statutul juridic al participanților la conflict.

Necesitatea și actualitatea temei propuse contă în cercetarea celei mai noi forme de agresiune, anume atacul cibernetic dar și a celei mai noi crime internaționale asupra căreia Curtea Penală Internațională va avea jurisdicție – crima de agresiune. În cadrul cercetării au fost folosite cele mai noi materiale disponibile la acel moment, ca exemplu, o parte din lucrare este axată pe cercetarea regulilor stabilite în prima ediție a Manualului de la Tallinn⁴ însă în momentul lansării celei de-a doua ediții a Manualului, cercetarea a fost revizuită pentru a reflecta noile reguli stabilite de grupul internațional de experți. Un alt element de noutate este îmbinarea dreptului internațional public, dreptului internațional umanitar și dreptului penal internațional cu anumite elemente din domeniul

³Art. 5 al Tratatului Nord-Atlantic: Părțile convin ca un atac armat împotriva uneia sau mai multora dintre ele, în Europa sau în America de Nord, va fi considerat un atac împotriva tuturor și, în consecința, sunt de acord ca, dacă are loc asemenea atac armat, fiecare dintre ele, în exercitarea dreptului la auto-apărare individuală ori colectivă recunoscut prin Articolul 51 din Carta Națiunilor Unite, va sprijini Partea sau Părțile atacate prin efectuarea imediată, individual sau de comun acord cu celelalte Parți, a oricărei acțiuni pe care o consideră necesară, inclusiv folosirea forței armate, pentru restabilirea și menținerea securității zonei nord-atlantice.

⁴Michael N. Schmitt – Tallinn Manual on the International Law Applicable to Cyber Warfare – Cambridge University Press, Cambridge, 2013

tehnologiei informației și comunicațiilor. Îmbinarea acestor elemente va permite analizarea cazurilor în care recurgerea la atacuri cibernetice poate fi catalogată drept agresiune, poate duce la declanșarea unui conflict armat sau situațiile în care o operațiune cibernetică va atrage răspunderea penală individuală pentru comiterea unei crime internaționale.

Obiectivele cercetării

Principalele obiective ale cercetării științifice sunt:

1. Identificarea evoluției procesului de defnire a crimei de agresiune și a actului de agresiune în general
2. Defnirea și identificarea atacurilor cibernetice în general
3. Defnirea atacurilor cibernetice ce ating pragul de folosire a forței calificabil pentru actul de agresiune
4. Identificarea normelor de drept aplicabile atacurilor cibernetice
5. Identificarea situațiilor în care recurgerea la folosirea atacurilor cibernetice poate duce la declanșarea unui conflict armat
6. Identificarea și analizarea elementelor crimei de agresiune având ca element material atacul cibernetic
7. Identificarea și analizarea formelor de răspundere internațională pentru crima de agresiune și actul de agresiune
8. Identificarea și analizarea cazurilor în care lansarea unor atacuri cibernetice poate atrage răspunderea penală individuală pentru săvârșirea crimei de agresiune
9. Formularea de concluzii

Metodologia folosită pentru elaborarea lucrării de cercetare

În scopul dezvoltării proiectului de cercetare au fost folosite diferite metode de cercetare științifică, între care putem aminti metoda istorică, comparativă și logică.

Metoda istorică a fost folosită, spre exemplu în privința prezentării evoluției incriminării actului de agresiune, a crimei de agresiune, și a dezvoltării jurisdicției internaționale penale;

Metoda logică a fost utilizată, spre exemplu pentru exprimarea propriilor concluzii și interpretări, pe baza studiului doctrinei, legislației și jurisprudenței relevante în domeniile răspunderii penale individuale, dreptului internațional umanitar și a apariției noilor forme de agresiune;

Metoda comparativă a fost folosită pentru a prezenta modul de formare al doctrinei privind aplicabilitatea normelor dreptului internațional umanitar noilor mijloace și metode de purtare a conflictelor armate punând în acest caz accent pe utilizarea atacurilor cibernetice.

Rezultatele cercetării și modalitățile de valorificare a acestora

Rezultatele cercetării efectuate s-au materializat într-o lucrare unitară. De asemenea, informațiile obținute au fost și vor fi diseminate prin participarea la diverse manifestări științifice: congrese, sesiuni științifice, conferințe, precum și publicarea în diverse reviste de specialitate. Datorită colaborării pe care o am cu Societatea Națională de Cruce Roșie din România, unul din principalii parteneri ai statului român în domeniul diseminării dreptului internațional umanitar, voi încerca să împărtășesc rezultatele lucrării în cadrul cursurilor de pregătire organizate de SNCRR, atât pentru voluntari cât și pentru persoane din afara organizației.

Structura lucrării

Conflictul este o constantă a omenirii. De la apariția primelor așezări omenești și a armelor pentru vânătoare a apărut și starea de conflict. Acest lucru este evidențiat și de descoperirile arheologice, astfel în anul 1964 o echipă de arheologi a descoperit, în apropierea graniței dintre Egipt și Sudan, un cimitir ce conținea 59 de schelete umane întregi și mai multe schelete parțiale. Scheletele descoperite au o vechime de peste 13.000 de ani și prezintă răni cauzate de săgeți și sulițe.⁵

Această lucrare, structurată în cinci capitole, are drept scop analizarea celei mai noi forme de agresiune în dreptul internațional, mai exact atacul cibernetic. Însă pentru a putea trata problema celor mai noi forme de agresiune trebuie analizate diferite aspecte ale dreptului internațional public, dreptului internațional umanitar și ale dreptului internațional penal. Din acest motiv lucrarea este structurată într-o singură parte.

Fiecare capitol al lucrării analizează un aspect diferit al acestor ramuri de drept, astfel **primul capitol** al acestei lucrări analizează atacul cibernetic la modul general. Rolul acestui capitol fiind acela de a delimita între diferite acțiuni care pot fi îndreptate împotriva infrastructurii și a sistemelor informatice. Acest capitol inițial este structurat în șase subcapitole fiecare dintre acestea tratând un alt aspect al dezvoltării tehnologice actuale. În cadrul acestui capitol sunt analizate diferite acțiuni îndreptate împotriva sistemelor informatice, de la infracțiuni ciberneticе, terorism cibernetic până la atacuri ciberneticе care reprezintă folosirea forței conform dreptului internațional. Am dorit să existe o delimitare a diferitelor acțiuni ilicite îndreptate împotriva sistemelor informatice pentru o mai bună înțelegere a daunelor care pot fi cauzate de atacurile informatice. Dacă

⁵<http://www.ancientmilitary.com/> - Accesat la 20.07.2015

infrafracțiunile informatice pot sustrage sume de bani din contul anumitor persoane, atacurile informatice pot duce la oprirea sau chiar distrugerea sistemului electric al unui stat sau la distrugerea unor centrifuge ce îmbunătățesc uraniul, situația cauzată de virusul Stuxnet. Nu există informații concrete privind proveniența virusului dar este speculat faptul că ar fi fost o operațiune a Statelor Unite ale Americii și a Israelului îndreptată împotriva Iranului, operațiune cunoscută sub numele de Olympic Games. În cadrul acestui capitol sunt prezentate și condițiile pe care un atac informatic trebuie să le îndeplinească pentru a putea fi calificat drept folosite a forței conform dreptului internațional.

Cel de-al **doilea capitol** al lucrării este și cel mai consistent și tratează problema atacurilor cibernetice ca formă de agresiune în dreptul internațional. Capitolul este structurat în cinci subcapitole și tratează problema agresiunii în dreptul internațional public, agresiunea în accepțiunea practicii ONU, crima de agresiune, atacurile cibernetice ca element material al crimei de agresiune și conflictul armat declanșat prin atacuri informatice.

În primul subcapitol este tratată problema agresiunii din perioada evului mediu și până la actuala reglementare. Sunt prezentate o serie de tratate internaționale importante precum Tratatul de la Versailles din 1919, Tratatul Internațional pentru Renunțarea la Război ca Instrument de Politică Națională denumit și Pactul Kellogg-Briand din 1928, Convențiile „Titulescu-Litvinov” ce au avut drept scop definirea agresiunii și Statutul Tribunalului de la Nurnberg. Aceste tratate au dus la definirea agresiunii în Rezoluția 3314 a Adunării Generale ONU în anul 1974. Tot în cadrul acestui subcapitol este tratată și obligația statelor de a nu recurge la folosirea forței dar și excepțiile de la această regulă.

În cel de-al doilea subcapitol sunt analizate elementele faptului de agresiune prevăzut în Rezoluția 3314 a Adunării Generale ONU și sunt prezentate deciziile Consiliului de Securitate în baza art. 39 din Carta ONU. Ororile celui de-al doilea război mondial au schimbat modul în care statele recurg la folosirea forței. Acest fapt este

reflectat de interzicerea recurgerii la amenințarea cu forța sau folosirea ei de către art. 2 al Cartei ONU și de definirea agresiunii de către Adunarea Generală a ONU. Însă, statele sunt entități abstracte, împotriva statelor care încalcă aceste norme se pot lua anumite măsuri politice, economice sau militare dar responsabilitatea pentru luarea acestor decizii revine conducătorilor de facto a statului.

Din acest motiv, cel de-al treilea subcapitol analizează crima de agresiune așa cum a fost definită în art. 8 bis al Statutului Curții Penale Internaționale. În prima parte este analizat cadrul juridic internațional care a permis definirea crimei de agresiune în urma Conferinței Diplomatice de revizuire a Statutului CPI ce a avut loc la Kampala în anul 2010. Finalul celui de-al doilea război mondial a dus la apariția celor două tribunale militare internaționale de la Nuernberg și Tokio, reprezentând un moment important pentru definirea crimei de agresiune. Pentru prima oară, oficiali de rang înalt au fost trași la răspundere pentru comiterea unei crime internaționale. În art. 6 al Statutului TMI de la Nuernberg sunt definite crimele ce intră sub jurisdicția tribunalului, printre care regăsim și crimele împotriva păcii. După momentul Nuernberg și Tokyo nimeni nu a mai fost tras la răspundere pentru comiterea crimei de agresiune. Adoptarea Statutului CPI în anul 1998 a readus în discuție crima de agresiune. Inițial, definiția acestei crime nu se regăsea în Statutul CPI dar era specificat, în art. 5, că jurisdicția Curții se extinde și asupra crimei de agresiune. În urma Conferinței de la Kampala, a fost adoptat art. 8 bis ce a definit crima de agresiune. De asemenea, este tratată sancționarea crimei de agresiune în cadrul Curții Penale Internaționale și sunt analizate și elementele constitutive ale crimei de agresiune. Ca urmare a conferinței de la Kampala au mai fost adoptate două noi articole ce privesc modul de exercitare a jurisdicției asupra crimei de agresiune, art. 15 bis și 15 ter. Modul de exercitare a jurisdicției este tratat în partea finală a acestui subcapitol. Statutul Curții Penale Internaționale nu este recunoscut de toate statele, nu este recunoscut nici măcar de toate statele membre permanente ale Consiliului de Securitate al

ONU⁶ iar amendamentele de la Kampala au fost ratificate de doar 32⁷ de state, însă nu trebuie subestimat rolul CPI. Tocmai acest rol limitat pe care CPI îl are la nivel internațional a permis statelor, ca după mai bine de 60 de ani, să readucă în discuție și să definească crima de agresiune. Definiția crimei de agresiune în Statutul CPI marchează un moment important în dezvoltarea dreptului internațional și un semnal de alarmă pentru liderii ce consideră că nu vor fi trași la răspundere pentru acțiunile lor.

În ultimul subcapitol este analizată problema conflictelor armate declanșate prin atacuri cibernetice. Sunt prezentate modalitățile de declanșare a conflictelor cu și fără caracter internațional și statutul participanților la conflictele armate, mai exact statutul combatanților, prizonierilor de război, combatanților nelegali și participarea directă la ostilități.

Cel de-**al treilea capitol** al lucrării prezintă mijloacele și metodele cibernetice de purtare a conflictelor armate. Primul subiect tratat este cel al aplicabilității normelor dreptului internațional umanitar în cazul atacurilor informatice. Normele dreptului internațional au fost concepute cu scopul de a proteja atât persoanele care participă direct la ostilități (combatanți, membri ai unor grupări armate organizate, civili care participă la desfășurarea ostilităților), personalul medical și religios care însoțește forțele armate cât și populația civilă. Dreptul statelor de a recurge la amenințarea cu folosirea forței sau la folosirea ei este interzis însă există și anumite excepții de la această regulă. Pentru a nu mai ajunge în situațiile întâlnite în timpul celui de-al doilea război mondial au fost create Convențiile de la Geneva din 1949. Din 1949 și până în prezent au mai fost adoptate o serie de tratate internaționale care interzic folosirea anumitor mijloace și metode de purtare a conflictelor. Normele dreptului internațional umanitar au mărit protecția oferită în timpul conflictelor armate dar nu au dus la eradicarea abuzurilor. Chiar dacă aceste norme există, modul de purtare a conflictelor armate a evoluat. Dacă la adoptarea acestor

⁶Doar Franța și Regatul Unit al Marii Britanii și Irlandei de Nord au ratificat Statutul CPI. Franța a depus instrumentele de ratificare a Statutului CPI la data de 9 iunie 2000 și Regatul Unit al Marii Britanii și Irlandei de Nord a depus instrumentele de ratificare a Statutului CPI la data de 4 octombrie 2001.

⁷<http://crimeofaggression.info/the-role-of-states/status-of-ratification-and-implementation/> - Accesat la 2.03.2017

tratate conflictele armate se purtau între două sau mai multe state, fiind folosite mijloace și metode convenționale de luptă, în prezent majoritatea conflictelor armate nu mai prezintă acest caracter internațional iar mijloacele și metodele de luptă s-au adaptat acestor noi situații. Avansul tehnologic a dus la apariția unor noi mijloace și metode de purtarea a conflictelor iar din această cauza trebuie văzut dacă normele dreptului internațional umanitar pot fi aplicabile indiferent de spațiul în care se poartă conflictul. Ultima parte a acestui capitol prezintă metodele interzise ale conflictelor cibernetice și încearcă să răspundă la întrebarea pot fi armele cibernetice calificate drept arme de distrugere în masă?

Capitolul patru prezintă categoriile de persoane și obiecte protejate împotriva atacurilor cibernetice, este prezentată protecția oferită populației civile și protecția specială oferită în cadrul conflictelor armate dar și protecția bunurilor civile precum bunurile indispensabile, instalațiile ce conțin forțe periculoase, bunurile culturale și mediul înconjurător.

Ultimul capitol tratează instituția răspunderii în dreptul internațional. Prima parte a acestui capitol prezintă formele răspunderii în dreptul internațional. Următoarea parte a capitolului analizează răspunderea statelor și a organizațiilor internaționale iar cea de-a doua parte analizează răspunderea penală internațională pentru comiterea crimelor de război, genocid și crimelor împotriva umanității. Răspunderea penală pentru comiterea crimei de agresiune este tratată în capitolul anterior. Trebuie să existe repercusiuni pentru faptele comise, altfel anumite state sau anumiți indivizi nu ar fi destul de motivați să le respecte. Chiar și în acesta situație, în care există instituția răspunderii, au fost numeroase cazuri în care normele dreptului internațional au fost încălcate și anumiți indivizi au ordonat comiterea unor crime odioase precum genocidul din Rwanda.

Lucrarea este finalizata de un capitol de concluzii care cuprinde opiniile autorului formulate ca urmare a cercetării materializate sub forma acestui studiu.

Bibliografie Selectivă

Tratate, monografii, cursuri

1. Raluca Miga-Beșteliu – Drept Internațional Public Volumul I, C.H.Beck, București, 2010, ISBN: 978-973-115-609-5
2. Raluca Miga-Beșteliu – Drept Internațional Public Volumul II, C.H.Beck, București, 2008, ISBN: 978-973-115-326-1
3. Beatrice Onica-Jarka – Drept International Umanitar, Universul Juridic, București 2010, ISBN 978-973-127-698-4 1
4. Beatrice Onica-Jarka – Jurisdictii Penale Internationale, CH Beck, București, 2008, ISBN: 978-973-115-223-3
5. Dumitra Popescu – Drept Internațional Public, Editura Univerisității “Titu Maiorescu”, București, 2005
6. Dumitra Popescu, Adrian Năstase – Drept Internațional Public, ediția revăzută și adăugită, Casa de editură și presă “:Șansa”, București, 1997, ISBN: 973-916-769-1
7. Michael N. Schmitt – Tallinn Manual on the International Law Applicable to Cyber Warfare – Cambridge University Press, Cambridge, 2013, ISBN 978-1-107-02443-4
8. Yoram Dinstein – War, Aggression and Self-Defence, Cambridge University Press, Cambridge, 2012, ISBN 978-1-107-00899-1 Hardback

9. Yoram Dinstein – The Conduct of Hostilities under the Law of International Armed Conflict, Cambridge University Press, Cambridge, 2004, ISBN-13 978-0-511-18682-0
10. Malcolm N. Shaw – International Public Law, Cambridge University Press, Cambridge, 2008, ISBN-13 978-0-511-45559-9
11. CyCon 2013 Proceedings – 5th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn, 2013, ISBN 978-9949-9211-5-7
12. Sergey Sayapin - The Crime of Aggression in International Criminal Law, Asser Press, Haga, 2014, ISBN 978-90-6704-927-6
13. Birgit Schlütter - Developments in Customary International Law, Koninklijke Brill NV, Leiden, ISBN 978-90-04-17772-7
14. William A. Schabas - An Introduction To The International Criminal Court, Cambridge University Press, Cambridge, ISBN 978-0-521-15195-5
15. Jeffrey Carr - Inside Cyber Warfare, O'Reilly Media, Inc, Sebastopol, 2010, ISBN: 978-0-596-80215-8
16. Paulo Shakarian, Jana Shakarian, Andrew Ruef - Introduction to Cyber-Warfare A Multidisciplinary Approach, Elsevier, 2013, ISBN: 978-0-12407-814-7
17. Richard A. Clarke, Robert K. Knake – Cyber War – The next Threat to National Security and What to do About it, HarperCollins Publishers, 2010, ISBN: 978-0-06-199239-1
18. Heather Harrison Dinniss - Cyber Warfare and the Laws of War, Cambridge University Press, 2012, ISBN 978-1-107-01108-3
19. Marco Roscini - Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, ISBN: 978-0-19-965501-4
20. Robert Cryer et all - An Introduction to International Criminal Law and Procedure, ediția a 2-a, Cambridge University Press, 2010, ISBN: 978-0-511-78934-2
21. CICR - Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law (Nils Melzer, 2009)
22. Nicoale Lupulescu – Drept umanitar, C.H. Beck , 2009, ISBN: 978-973-115-500-5

23. Dieter Fleck - The Handbook of International Law, Ediția a II-a, Oxford University Press, 2009, ISBN: 978-0-19-923250-5
24. Robert Kolb & Richard Hyde - An Introduction to the International Law of Armed Conflicts, Hart Publishing, 2008, ISBN: 978-1-84113-799-5
25. Gary D. Solis - The Law of Armed Conflict, Cambridge University Press, 2010, ISBN: 978-0-511-71253-1
26. Christine D. Gray – International Law and the use of Force, Oxford University Press, 2008, ISBN: 978-0-19-923914-6
27. M. Cherif Bassiouni – International Criminal Law: Sources, Subjects and Contents, 2008, ISBN: 978-1-107-00115-2

Studii, articole

28. David E. Graham – Cyber Threats and the Law of War, Journal of national security law & policy, University of the Pacific, 2010 - http://jnslp.com/wp-content/uploads/2010/08/07_Graham.pdf
29. Jackson Nyamuya Maogoto - Aggression: Supreme International Offence Still in Search of Definition, Southern Cross University Law Review, Vol. 5, Nr. 1, 2002
30. William H. Boothby - Methods and Means of Cyber Warfare, U.S. Naval War College, International Law Studies nr. 387, 2013
31. Michael Schmitt - Classification of Cyber Conflict, Oxford Journals, Journal Of Conflict And Security Law, Vol. 17, nr. 2, 2012
32. Andrew M. Colarik, Lech Janczewski D.Eng - Establishing Cyber Warfare Doctrine, Journal of Strategic Security 5, nr. 1 2012 - <http://scholarcommons.usf.edu/jss>
33. Claus Kress, Leonie von Holtendorff- The Kampala Compromise on the Crime of Aggression, Journal of International Criminal Justice nr. 8, Oxford University Press, 2010
34. Fred Schreier - On Cyberwarfare, DCAF Horizon 2015 Working Paper Nr. 7, DCAF, 2012
35. Matthew Gillett - The Anatomy of an International Crime: Aggression at the International Criminal Court, 2013

36. Noah Weisbord - The Mens Rea of the Crime of Aggression, Washington University Global Studies Law Review, Vol. 12, Nr. 3, 2013; Florida International University Legal Studies Research Paper Nr. 14-09, 2014
37. Robert Heinsch - The Crime of Aggression After Kampala: Success or Burden for the Future?, Goettingen Journal of International Law 2, 2010
38. International Committee of the Red Cross - International Humanitarian Law and the challenges of contemporary armed conflicts, Geneva, 2011
39. Michael N. Schmitt - Wired warfare: Computer network attack and jus in bello, International Review of the Red Cross, Vol 84, Nr 846, 2002
40. Michael N. Schmitt - The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis, Harvard National Security Journal, vol.1, 2010
41. Collin Allan - Direct Participation in Hostilities from Cyberspace, Virginia Journal of International Law, Vol. 54, No. 1, 2013
42. Michael N. Schmitt - Cyber Operations and the Jus in Bello: Key Issues, Naval War College International Law Studies, 2011
43. Christopher Greenwood - The Law of Weaponry at the Start of the New Millennium, International Law Studies – Vol. 71, 1998
44. Yearbook of the International Law Commission, 1950, Vol. II
45. Jerome Radcliffe – Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System, Black Hat USA, 2011,
46. Scott D. Applegate - The Dawn of Kinetic Cyber, 5th International Conference on Cyber Conflic, 2013
47. Ioan Dumitrache - Cyber-Physical-Systems (Cps) – Factor Determinant În Economia Bazată Pe Inovare Și Cunoștințe, 2013 - Revista Română de Informatică și Automatică, vol. 23, nr. 4, 2013
48. Karen L. Corrie - Pre-Trial Division of the International Criminal Court: Purpose, Powers, and First Cases
49. Matthias Schuster - The Rome Statute and the Crime of Aggression: A Gordian Knot In Search Of A Sword, Criminal Law Forum, 2003

50. Knut Dörmann - Computer network attack and international humanitarian law, The Cambridge Review of International Affairs "Internet and State Security Forum", Trinity College, Cambridge, 2001
51. William Church - Information warfare, International Review of the Red Cross, Nr. 837, International Committee of the Red Cross 2000
52. Wael Adhami - The strategic importance of the Internet for armed insurgent groups in modern warfare, International Review of the Red Cross, Vol. 89 Nr.868, International Committee of the Red Cross, 2007
53. Cordula Droege - Get off my cloud:cyber warfare, international humanitarian law, and the protection of civilians, International Review of the Red Cross, Vol. 94, Nr. 886, International Committee of the Red Cross, 2012
54. Herbert Lin - Cyber conflict and international humanitarian law, International Review of the Red Cross, Vol. 94, Nr. 886, International Committee of the Red Cross, 2012
55. Alan Backstrom, Ian Henderson - New capabilities in warfare: an overview of contemporary technological developments and the associated legal and engineering issues in Article 36 weapons reviews, International Review of the Red Cross, Vol. 94, Nr. 886, International Committee of the Red Cross, 2012
56. Hitoshi Nasu – Nanotechnology and challenges to international humanitarian law: a preliminary legal assessment International Review of the Red Cross, Vol. 94, Nr. 886, International Committee of the Red Cross, 2012
57. Tim Maurer - Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security, Science, Technology, and Public Policy Program Explorations in Cyber International Relations Project, Belfer Center for Science and International Affairs Harvard Kennedy School, 2011
58. Samuel Estreicher - Privileging Asymmetric Warfare?: Defender Duties Under International Humanitarian Law, Public Law & Legal Theory Research Paper Series Working Paper Nr. 10-28, 2010
59. Eneken Tikk-Ringas - Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012, ICT4Peace Publishing, Geneva, 2012
60. Nils Melzer - Cyberwarfare and International Law, UNIDIR, 2011

61. Kim Hartmann, Christoph Steup - The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment - 5th International Conference on Cyber Conflict PROCEEDINGS, NATO CCD COE Publications, 2013, ISBN 13 (pdf): 978-9949-9211-5-7
62. Igor Kotenko. Andrey Chechulin - A Cyber Attack Modeling and Impact Assessment Framework - 5th International Conference on Cyber Conflict PROCEEDINGS, NATO CCD COE Publications, 2013, ISBN 13 (pdf): 978-9949-9211-5-7
63. David Raymond, Gregory Conti, Tom Cross, Robert Fanelli - A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons, 5th International Conference on Cyber Conflict PROCEEDINGS, NATO CCD COE Publications, 2013, ISBN 13 (pdf): 978-9949-9211-5-7
64. Kaarel Kalm - Illicit Network Structures in Cyberspace, 5th International Conference on Cyber Conflict PROCEEDINGS, NATO CCD COE Publications, 2013, ISBN 13 (pdf): 978-9949-9211-5-7
65. Emilio Iasiello - Cyber Attack: A Dull Tool to Shape Foreign Policy, 5th International Conference on Cyber Conflict PROCEEDINGS, NATO CCD COE Publications, 2013, ISBN 13 (pdf): 978-9949-9211-5-7
66. Shannon Vallor - The Future of Military Virtue: Autonomous Systems and the Moral Deskillling of the Military, 5th International Conference on Cyber Conflict PROCEEDINGS, NATO CCD COE Publications, 2013, ISBN 13 (pdf): 978-9949-9211-5-7
67. Robert S. Dewar - The "Triptych of Cyber Security": A Classification of Active Cyber Defence, 6th International Conference on Cyber Conflict PROCEEDINGS, NATO CCD COE Publications, 2014, ISBN (pdf): 978-9949-9544-1-4
68. Stephen Cobb, Andrew Lee - Malware is called malicious for a reason: The risks of weaponizing code, 6th International Conference on Cyber Conflict PROCEEDINGS, NATO CCD COE Publications, 2014, ISBN (pdf): 978-9949-9544-1-4
69. Matteo Casenove, Armando Miraglia - Botnet over Tor: The Illusion of Hiding, 6th International Conference on Cyber Conflict PROCEEDINGS, NATO CCD COE Publications, 2014, ISBN (pdf): 978-9949-9544-1-4

Legislație

70. Legea 286/2009 – Codul Penal Român, Publicată în Monitorul Oficial nr. 510 din 24 iulie 2009
71. Legea 111/2002 pentru ratificarea Statutului Curții Penale Internaționale, adoptat la Roma la 17 iulie 1998, Publicată în Monitorul Oficial nr. 211 din 28 martie 2002
72. Convențiile de la Geneva din 1949 și Protocoalele Aditionale
73. Convențiile de la Haga
74. Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică
75. Seoul Framework for and Commitment to Open and Secure Cyberspace – document disponibil la adresa <http://www.mofat.go.kr/english/visa/images/res/SeoulFramework.pdf> . Accesat la 2.03.2015
76. A/68/98 - Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – document disponibil la adresa http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98 . Accesat la 13.01.2015
77. Rezoluția 3314 a Adunării Generale ONU privind definiția agresiunii – 1974
78. Carta Națiunilor Unite din 26 iunie 1945
79. Amendamentele aduse Statutului Curții Penale Internaționale ca urmare a Conferinței de Revizuirea ce a avut loc în Kampala în 2010
80. Statutul Mecanismului Națiunilor Unite pentru Tribunale Internaționale Penale
81. Legea privind Camerele Specializate și Biroul Procurorului Specializat ale Tribunalului din Kosovo (Guvernul provinciei Kosovo)
82. Convenția privind interzicerea dezvoltării, producerii, stocării și folosirii armelor chimice și distrugerea acestora, 1993
83. Statutul Curții Penale Internaționale
84. Statutul Tribunalului Penal International pentru Fosta Iugoslavie
85. Statutul Tribunalului Penal International pentru Rwanda

Jurisprudență

86. Curtea Internațională de Justiție – Case concerning armed activities on the territory of the Congo - 2005
87. Curtea Internațională de Justiție - Legality Of The Threat Or Use Of Nuclear Weapons (Advisory Opinion) - 1996
88. Curtea Internațională de Justiție - Case Concerning Oil Platforms -2003
89. Curtea Internațională de Justiție - Case Concerning Military And Paramilitary Activities In And Against Nicaragua – 1986
90. Tribunalul Internațional Penal pentru Fosta Iugoslavie - Procurorul versus Dusko Tadic
91. Tribunalul Internațional Penal pentru Fosta Iugoslavie - Procurorul versus Goran JELIS
92. Tribunalul Internațional Penal pentru Fosta Iugoslavie - Procurorul versus Radislav KRSTIC
93. Tribunalul Internațional Penal pentru Rwanda - Procurorul versus Jean-Paul AKAYESU
94. Tribunalul Internațional Penal pentru Rwanda - Procurorul vs. Kayishema și Ruzindana
95. Cazul Rainbow Warrior (Noua Zeelandă c. FRANCE), France-New Zealand Arbitration Tribunal

Surse internet

96. Kai Ambos - The Crime of Aggression After Kampala, German Yearbook of International Law, Vol. 53, 2011 - http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1972173
97. Customary International Humanitarian Law Database – International Committee of the Red Cross - <http://www.icrc.org/customary-ihl/eng/docs/home>
98. Centrul de Resurse al Comitetului Internațional de Cruce Roșie – <http://www.icrc.org/eng/resources/index.jsp>
99. Pagina web a Oxford Journals - <http://jcs1.oxfordjournals.org/>
100. Pagina web a Social Science Research Network - <http://www.ssrn.com/en/>
101. Site-ul Curții penale Internaționale - www.icc-cpi.int

102. Report of the Special Working Group on the Crime of Aggression - ICC-ASP/6/SWGCA/INF.1 - https://asp.icc-cpi.int/iccdocs/asp_docs/SWGCA/ICC-ASP-6-SWGCA-1_English.pdf
103. Rezoluția RC/Res.1 din 8 iunie 2010. Document disponibil la adresa: https://asp.icc-cpi.int/iccdocs/asp_docs/Resolutions/RC-Res.1-ENG.pdf .
104. Site-ul Departamentului pentru controlul exporturilor - MAE
105. www.ancex.ro
106. www.symantec.com/
107. Site-ul Tribunalului Internațional Penal pentru Fosta Iugoslavie - www.icty.org
108. Site-ul mecanismului pentru Tribunale Internationale al ONU - <http://www.unmict.org>
109. Carsten Stahn -Tribunals are Dead, Long Live Tribunals: MICT, the Kosovo Specialist Chambers and the Turn to New Hybridity, 2016. Document disponibil la adresa: <http://www.ejiltalk.org/tribunals-are-dead-long-live-tribunals-mict-the-kosovo-specialist-chambers-and-the-turn-to-new-hybridity/>