NICOLAE TITULESCU UNIVERISTY OF BUCHAREST

FACULTY OF LAW

DOCTORAL SCHOOL

DOCTORAL THESIS

Cyber-attacks – a new form of aggression in international law

SUMMARY

Thesis coordinator:
Professor Dr. Raluca Miga Beşteliu

Doctoral student:
Dan-Iulian Voitașec

BUCHAREST
2017

Table of content[1]

[1] This paper has been financially supported within the project entitled ***"Horizon 2020 – Doctoral and Postdoctoral Studies: Promoting the National Interest through Excellence, Competitiveness and Responsibility in the Field of Romanian Fundamental and Applied Scientific Research"***, contract number POSDRU/159/1.5/S/140106. This project is co-financed by the European Social Fund through the Sectoral Operational Programme for Human Resources Development 2007-2013. **Investing in people!**

1.3.2. The use of force in accordance with Chapter VII of the UN Charter

1.3.3. Use of force in exercising the right to self-determination

2. Aggression in the sense of UN practice. Cases of aggression according to art. 39 of the UN Charter
   2.1. Elements of aggression in accordance with Resolution 3314 of 14 December 1974 of the General UN Assembly
   2.2. Decisions of the Security Council based on Art. 39 of the UN Charter
3. The crime of aggression in the contemporary sense
   3.1. The international legal framework regarding the prohibition of aggression
   3.2. The crime of aggression according to the Statute of the International Criminal Court
   3.3. The constitutive elements of the crime of aggression
   3.4. The issue of exercising jurisdiction over the crime of aggression
   3.5. Exercise of jurisdiction under Article 15 bis
   3.6. Exercise of jurisdiction under Article 15 ter
4. Cyber-attack as a material element of the crime of aggression
5. Armed conflict triggered by cyber-attacks
   5.1. Armed conflict
   5.2. The statute of participants in armed conflicts triggered by cyber attacks

Conclusion

Chapter III – Means and methods of cyber-warfare

1. Applying International Humanitarian Law to cyber-attacks
2. Means and methods of cyber-war
   2.1. Means of cyber war
      2.1.1. Cyber weapons as weapons of mass destruction
   2.2. Methods of cyber war
      2.2.1. Superfluous injury or unnecessary suffering

2.2.2. Indiscriminate means and methods

2.2.3. Cyber boobytraps

2.2.4. Perfidy

2.2.5. Improper use of the protective indicators

2.2.6. Reprisals

2.2.7. Starvation

Conclusion

Chapter IV – People and objects protected against cyber attacks

1. Definitions
2. Protections of civilian population and civilian objects

2.1. Special protection granted during armed conflict

2.1.1. Special protection granted to women during armed conflict

2.1.2. Special protection granted to children during armed conflict

2.1.3. Special protection granted to journalist during armed conflict

Conclusion

Chapter V – Responsibility for cyber-attacks according to international law

1. Forms of responsibility for international crimes
2. State responsibility

2.1. Material responsibility of states

2.2. Political responsibility of states

3. Responsibility of international organizations
4. International criminal responsibility

4.1. Genocide

4.2. Crimes against humanity

4.3. War crimes

4.4. The crime of aggression

Conclusion

Chapter 6 – Conclusions

Annex I – The Tallinn Manual 2.0

Bibliography

Introduction

The necessity and timeliness of the research topic

At the time of adoption of the UN charter and the Conventions that govern international humanitarian law, it seemed in the realm of science fiction that unmanned flying vehicles could be controlled using a device found in the pocked of the majority of the urban population. But today that technology is no longer in the realm of science fictions, it is reality.

Technological evolution plays a central role in every state existing in the 21st century. Information systems almost entirely control services that are indispensable to our current society, such as electricity, water, rail transport even personal vehicles. In order to better understand the current technological advances, in Romania there are approximately 22,9 million mobile phone numbers for a population of less than 20 million inhabitants, 3.47 million internet subscriptions and 5.1 million internet subscriptions[2].

Given the cross-border nature of cyberspace, more and more states and international organization have begun to allocate more resources to develop cyber capabilities, both offensive and defensive.

This position was reaffirmed in the Declaration adopted by the Heads of State and Government participating in the NATO Summit held in Wales in September 2014. In art. 72 of the Declaration the Enhanced Cyber Defense Policy it is highlighted that cyber defense is part of NATO's core task on collective defense. Under this new policy,

[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

launching a cyber-attack against a NATO member state could lead to invoking art.5 of the North Atlantic Treaty. Also, art. 72 of the Declaration mentions that international law, including international humanitarian law and the UN Charter apply in the cyber field.

Although cyber security has begun to develop and national and international policies have been adopted, there are no international specific instruments developed to restrict or prohibit the use of certain types of cyber-attacks. Due to this situation, the rule on international public law and international humanitarian law applicable to cyber-attacks has to be identified. It is also necessary to identify situations in which the use of cyber-attacks reaches the threshold of use of force in violation of the provisions of art. 2 paragraph. 4 of the UN Charter. In the case of launching cyber operations during armed conflicts we have to identify the international humanitarian law rules applicable, the limits of using such attacks and the legal status of participants in the armed conflicts.

The necessity and timeliness of the proposed theme is in the research of the latest form of aggression, namely cyber-attacks and the latest international crime on which the International Criminal Court will have jurisdiction - the crime of aggression. During the research the most recent materials available at the time were used, for example, part of the paper is focused on researching the rules set out in the first edition of the Tallinn Manual, but when the second edition of the Manual was released, the thesis was revised to reflect the new rules set by the international group of experts. Another element of novelty is the merging of international public law, international humanitarian law and international criminal law with certain elements from the field of information and telecommunication technology. The combination of these elements will allow the analysis of cases where the use of cyber-attacks can be categorized as aggression, may lead to an armed conflict, or situations in which a cybercrime will entail individual criminal responsibility for committing an international crime.

Research objectives

The main objectives of this research are:

1. Identifying the evolution of the process of defining the crime of aggression and aggression in general;
2. Defining and identifying cyber-attacks in general;
3. Defining cyber-attacks that reach the threshold of use of force;
4. Identifying the law applicable to cyber-attacks;
5. Identifying situations where recourse to cyber-attacks can lead to armed conflict;
6. Identifying and analyzing the elements of the crime of aggression with cyber-attacks as the material element;
7. Identifying and analyzing forms of international responsibility for the crime of aggression and aggression;
8. Identifying and analyzing situations in which the launch of cyber-attacks may entail individual criminal responsibility for committing aggression;
9. Drawing up conclusions

Methodology used to study and complete the thesis

In order to develop the thesis, different methods of scientific research where used, among which we can mention the historical, comparative and logical method.

The historical method has been used, for example, to present the evolution of incrimination of aggression, the crime of aggression and the development of international criminal jurisdiction.

The logical method has been used to express conclusions and interpretations based on the study of relevant doctrine, legislation and jurisprudence in the field of international humanitarian law, international criminal law and emerging forms of aggression.

The comparative method has been used to present the formation of the doctrine on the applicability of international humanitarian law rules to the new means and methods of waging armed conflicts, in this case putting emphasis on cyber-attacks.

Results of the research and their means of dissemination

The results of the research will materialize in a unitary work. Also, the information obtained was and will be disseminated through participation in various scientific events: congresses, scientific sessions, conferences, as well as publication in various specialized journals. Thanks to my collaboration with the Romanian Red Cross Society, one of the main partners of the Romanian state in the field of international humanitarian law dissemination, I will try to share the results of the work during the training courses organized by SNCRR, both for volunteers and for other partners.

Paper structure

Conflict is a constant of mankind. Since the appearance of the first human settlements and hunting weapons, conflicts have also emerged. This is evidenced by archaeological discoveries, in 1964 a team of archaeologists discovered, near the Egyptian-Sudan border, a cemetery containing 59 whole human skeletons and several partial skeletons. The discovered skeletons are over 13,000 years old and show wounds caused by arrows and spears.[3]

This paper, structured in five chapters, aims to analyze the latest form of aggression in international law, namely cyber-attack. However, in order to deal with the most recent forms of aggression, various aspects of public international law, international humanitarian law and criminal international law must be considered. For this reason, the thesis is structured in one part.

Each chapter of the paper analyzes a different aspect of these branches of law, so the **first chapter of this paper** analyzes cyber-attack in general terms. The role of this chapter is to distinguish between different actions that can be directed against infrastructure and information systems. This initial chapter is structured in six subchapters, each of which deals with another aspect of current technological development.

[33] http://www.ancientmilitary.com/

Within this chapter various actions directed against information systems are analyzed, from cybercrime, cyber terrorism to cyber-attacks that reach the threshold of use of force according to international law. The scope of this chapter was to create a distinction between the various illegal actions directed against information systems to better understand the damage that can be caused by cyber-attacks. Cyber criminals can steal information or money from bank accounts while state sponsored cyber-attacks may cause damage to critical infrastructure, or even destroy uranium-enhancing centrifuges as was the case with the Stuxnet virus. There is no specific information on the origin of the virus but it is speculated that it was an operation of the United States of America and Israel directed against Iran, an operation known as Olympic Games. In this chapter the conditions that a cyber-attack must fulfill in order to be qualified as use of force according to international law are also presented.

The second chapter of the paper is also the most consistent and deals with the issue of cyber-attacks as a form of aggression in international law. The chapter is structured in five subchapters and deals with aggression in public international law, aggression in the sense of UN practice, the crime of aggression, cyber-attacks as a material element of the crime of aggression, and armed conflict triggered by cyber-attacks.

The first subchapter deals with the problem of aggression during the Middle Ages and up to the current regulation. A series of important international treaties such as the Statute of the Nurnberg Tribunal, the 1919 Treaty of Versailles, the International General Treaty for Renunciation of War as an Instrument of National Policy, also called the Kellogg-Briand Pact of 1928, the Titulescu-Litvinov Conventions aimed at defining aggression are presented and analyzed. These treaties have led to the definition of aggression in UN General Assembly Resolution 3314 from 1974. This subchapter analyses the obligation of states not to resort to the threat or use of force and also the exceptions to this rule.

The second subchapter analyzes the elements of aggression set out in the United Nations General Assembly Resolution 3314 and presents the decision of the UN Security Council under art. 39 of the UN Charter.

The horrors of the Second World War have changed the way states use force. This is reflected in the prohibition of resorting to the threat or use of force by art. 2 of the UN Charter and the definition of aggression found in the UN General Assembly's Resolution. But states are abstract entities, some political, economic or military measures can be taken against states that violate these norms, but the responsibility for making these decisions lies with the de facto ruler of the state. For this reason, the third subchapter analyzes the crime of aggression as defined in art. 8 bis of the Statute of the International Criminal Court. The first part presents and analyzes the international legal framework that allowed and led to the definition of the crime of aggression following the Diplomatic Review Conference of the ICC Statute held in Kampala in 2010.

The end of the Second World War led to the appearance of the two international military courts in Nurnberg and Tokyo, representing an important moment for defining the crime of aggression. For the first time, senior officials have been held responsible for committing an international crime. In art. 6 of the IMT of Nurnberg Statute defines crimes under the jurisdiction of the tribunal, among which we find the crimes against peace. After Nurnberg and Tokyo, no one was held accountable for committing a crime of aggression. The adoption of the ICC Statute in 1998 brought back the crime of aggression. Initially, the definition of this crime was not found in the ICC Statute, it was just specified in Art. 5 that the jurisdiction of the Court extends to the crime of aggression. Following the Kampala Conference, Art. 8 bis which defined the crime of aggression was adopted. This subchapter also deals with the sanction of the crime of aggression within the International Criminal Court and the elements of the crime. As a result of the Kampala conference, two new articles have been adopted regarding the way in which jurisdiction over the crime of aggression is exercised, art. 15 bis and 15 ter. The way in which jurisdiction is exercised is dealt with in the final part of this subchapter.

The Statute of the International Criminal Court is not recognized by all states, it is not even recognized by all the permanent member states of the UN Security Council and the Kampala amendments have been ratified by only 32 states, but the role of the ICC should not be underestimated. It is precisely this limited role that the ICC plays at the international level that allowed states to bring into discussion and define the crime of aggression after 60 years of inactivity in this field. The definition of the crime of aggression in the ICC Statute marks an important moment in the development of international law and an alarm signal send to all leaders who believe they will not be held accountable for their actions.

The last subchapter analyzes the issue of armed conflicts triggered by cyber-attacks. The subchapter presents the ways that an international and non-international armed conflict could be triggered by resorting to cyber-attacks, it also deals with the legal statute of combatants, prisoners of war, unlawful combatants and direct participation in hostilities.

The third chapter of this paper presents the cyber means and methods of armed conflict. The first subject analyzed is the applicability of international humanitarian law in the case of cyber-attacks. International law rules were designed in order to protect both persons directly participating in hostilities (combatants, members of organized armed groups, civilians involved in the conduct of hostilities), medical and religious personnel accompanying the armed forces and the civilian population. The right of states to resort to the threat or use of force is forbidden, but there are some exceptions to this rule. In 1949 the Geneva Conventions were created in order not to reach the situations encountered during the Second World War. From 1949 until now, a number of international treaties have been adopted that prohibit the use of certain means and methods of warfare. The norms of international humanitarian law have increased the protection offered during armed conflicts, but have not led to the eradication of abuses. Even though these rules exist, the way in which armed conflict are conducted has evolved, if at the moment of adoption of these treaties armed conflicted took place

between two or more states using conventional means and methods of warfare, in modern times most armed conflicts no longer have an international character and the means and methods of warfare have been adapted to these new situations. Technological advances have led to the emergence of new means and methods of waging war and therefore the current rules of international humanitarian law have to been analyzed to see if they apply irrespective of the space in which the conflict takes place. The last part of this chapter presents the prohibited methods of cyber conflicts and attempts to answer the question can cyber-attacks qualify as weapons of mass destruction?

Chapter Four presents the categories of people and objects protected from cyber-attacks, the protection offered to the civilian population and the special protection offered in the armed conflicts, as well as the protection of civilian objects such as indispensable goods, hazardous-force installations, cultural goods and the environment.

The fifth chapter deals with the institution of international law responsibility. The first part of this chapter presents the forms of responsibility in international law. The next part of the chapter analyzes the responsibility of states and international organizations and the second part analyzes the international criminal responsibility for committing war crimes, genocide and crimes against humanity. Criminal responsibility for committing the crime of aggression is dealt with in the previous chapter. There must be repercussions for the acts committed, otherwise some states or certain individuals would not be sufficiently motivated to respect them. Even in this situation, where there is the institution of liability, there have been numerous cases in which the rules of international law have been violated, and some individuals have ordered the commission of offensive crimes such as genocide in Rwanda.

The fifth chapters analyses the institution of international responsibility. The first part of this chapter presents the forms of responsibility according to international law. The second subchapter presents the material and political responsibility of state for committing international offenses attributable to them. This chapter also discusses the international responsibility of international organization. The last part of this chapter

analyses individual criminal responsibility for the war crimes, genocide and crimes against humanity committed using cyber capabilities. There must be repercussions for acts committed, otherwise some states or individuals will not be sufficiently motivated to respect international legal norms. Even if the institution of responsibility is deeply rooted in international law there are many examples where these rules have been violated and individuals have ordered the commission of horrific crimes such as the genocide in Rwanda.

The final portion of the thesis is dedicated to the conclusions formulated by the PhD candidate following the research process that materialized in this study.

Bibliography

Treaties, books, courses

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 Umaniar, 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 evăzută 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

Studies and articles in journals / collections of studies

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 Holtzendorff- 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 Şi Cunoştinţe, 2013 – Revista Română de Informatică şi 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 Deskilling 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

Legislation

70. Law 286/2009 - Romanian Penal Code, published in the Official Gazette no. 510 of 24 July 2009

71. Law 111/2002 for ratification of the International Criminal Court statute, adopted in Roma on 17 July 1998, Published in the Official Gazzete no. 211 of 28 March 2002

72. The 1949 Geneva Convention and Additional Protocols of 1977

73. Hague Convention

74. Decision no. 271/2013 for the approval of the Romanian Cyber Security Strategy and the National Action Plan on the Implementation of the National Cyber Security System

75. Seoul Framework for and Commitment to Open and Secure Cyberspace – document available at http://www.mofat.go.kr/english/visa/images/res/SeoulFramework.pdf .

76. A/68/98 - Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98

77. United Nations General Assembly Resolution 3314– 1974

78. UN Charter - 26July 1945

79. Amendments to the Rome Statute of the International Criminal Court – Kampala, 2010

80. United Nations Mechanism for International Criminal Tribunals Statute

81. Kosovo Specialist Chambers & Specialist Prosecutor's Office Statute

82. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, 1993

83. International Criminal Court State

84. International Criminal Tribunal for the former Yugoslavia Statute

85. International Criminal Tribunal for Rwanda Statute

Jurisprudence

86. International Court of Justice– Case concerning armed activities on the territory of the Congo - 2005

87. International Court of Justice - Legality Of The Threat Or Use Of Nuclear Weapons (Advisory Opinion) - 1996

88. International Court of Justice- Case Concerning Oil Platforms -2003

89. International Court of Justice - Case Concerning Military And Paramilitary Activities In And Against Nicaragua – 1986

90. International Criminal Tribunal for the former Yugoslavia – Prosecutor versus Dusko Tadic

91. International Criminal Tribunal for the former Yugoslavia - Prosecutor versus Goran JELIS

92. International Criminal Tribunal for the former Yugoslavia - Prosecutor versus Radislav KRSTIC

93. International Criminal Tribunal Rwanda - Prosecutor versus Jean-Paul AKAYESU

94. International Criminal Tribunal Rwanda - Prosecutor vs. Kayishema and Ruzindana

95. Rainbow Warrior Case (New Zeeland c. FRANCE), France-New Zealand Arbitration Tribunal

Webography

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. ICRC Resource Center – http://www.icrc.org/eng/resources/index.jsp

99. Oxford Journals - http://jcsl.oxfordjournals.org/

100. Social Science Research Network - http://www.ssrn.com/en/

101. International Criminal Court website - 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. Resolution 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. Department for Export Control – MAE website -www.ancex.ro

105. www.symantec.com/

106. International Criminal Tribunal for the former Yugoslavia website - www.icty.org

107. United Nations Mechanism for International Criminal Tribunals - http://www.unmict.org

108. Carsten Stahn -Tribunals are Dead, Long Live Tribunals: MICT, the Kosovo Specialist Chambers and the Turn to New Hybridity, 2016. http://www.ejiltalk.org/tribunals-are-dead-long-live-tribunals-mict-the-kosovo-specialist-chambers-and-the-turn-to-new-hybridity/